

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

HACKING RFID

RFID SECURITY AND PRIVACY ISSUES

PASSIVE RFID TAG SECURITY

THE RFID AND NFC RADIO FREQUENCY

RFIDIOT FOR MAC OSX

AN INTERVIEW WITH DR. ANN CAVOUKIAN

Vol.6 No.8
Issue 08/2011(44) ISSN: 1733-7136

PLUS

2 NEW COLUMNS!

(IL)LEGAL

WHEN IS PRIVATE NOT PRIVATE? MAKING SENSE OF EUROPEAN PRIVACY LAW

TOOL TIME

MITM USING CAIN: CLIENT SIDE ATTACKS



It's here! Penetration testing for Students



Click here
To enter the
early bird list

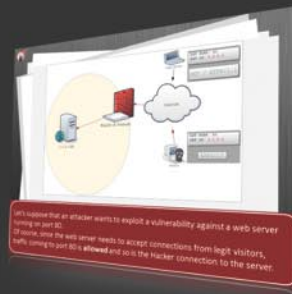


80% of beginners remain beginners or give up completely

We know the pain of being a beginner. You either don't have the foundational skills or you don't have a clear path to follow. Don't give up. There is a better way. Our course will teach you basics of networks and web apps.

It's not just about 1337 instructors

Expert teachers hardly remember what took them to the expert status. It's a fact. There is no way to effectively teach beginners other than help them building strong foundations and showing them the correct path.



You can do it

If you keep studying without a clear learning path you are probably wasting time. Secret is path and perseverance. Better a single step in the correct direction than 10 random steps. Our course will save you months of struggling and frustrations.

You gotta see this.

www.elearnsecurity.com



Still hacking virtual machines?



Coliseum Lab is here!

The most epic web app hacking lab
you have ever seen

CLICK HERE

14 educational challenges
in a multi-platform
environment.

Epic!

www.coliseumlab.com



HAKIN9 team

Editor in Chief: Ewa Dudzic
ewa.dudzic@hakin9.org

Managing Editor: Patrycja Przybyłowicz
patrycja.przybylowicz@hakin9.org

Editorial Advisory Board: Rebecca Wynn, Matt Jonkman,
Donald Iverson, Michael Munt, Gary S. Milefsky, Julian Evans

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Marketing Manager: Małgorzata Bocian
m.bocian@hakin9.org

Proofreaders: Donald Iverson, Michael Munt, Elliott Bujan, Bob
Folden, Steve Hodge, Jonathan Edwards

Top Betatesters: Ivan Burke, Aby Rao, John Webb, Nick Baronian,
Chris Brereton, John Hammond, Keith Lee, Felipe Martins,
Alexandre Lacan

Special Thanks to the Beta testers and Proofreaders who helped
us with this issue. Without their assistance there would not be a
Hakin9 magazine.


Senior Consultant/Publisher: Paweł Marciniak


CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of
the magazine, the editors make no warranty, express or implied,
concerning the results of content usage.
All trade marks presented in the magazine were used only for
informative purposes.

All rights to trade marks presented in the magazine are
reserved by the companies which own them.
To create graphs and diagrams we used smardcrow.com program
by  SmartDraw

The editors use automatic system 
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only
be used in private, local networks. The editors
hold no responsibility for misuse of the presented
techniques or consequent data loss.

Dear Readers,

This month we have dedicated the issue to RFID Security. It's
not a new technology, however it has become more popular
to common folks recently because of introducing biometrics
passports and Contactless Credit Cards. And even more
popular, because of a range of vulnerabilities that has been
discovered just after it. The threat of being robbed of money
or identity scares more that having the smartcard hacked in
the phone. Some companies smell the new business and
offer special sleeves for cards and passports. The fear is the
best marketing campaign. The RFID aimed to be a future
technology known from sci-fi movies. One is sure – RFID
infrastructure introduces the new privacy and security risks.
We, the specialist, as well as common folks need to be aware
of them.

In the Basics section you will find the article: *RFID for
Newbies, Sauce Security*, it's a great background, worth your
attention before reading the rest of the articles. The author
Gildas Avoine is a founder of *RFID Security & Privacy Lounge*
(<http://www.avoine.net/rfid/>). I recommend you also the articles
written by Michel Barbeau – *Passive RFID Tag Security:
Electronic Product Code E-Passport and Contactless Credit
Card*, and by Gary S. Milefsky – *RFID Security and Privacy
Issues*. Both texts are dealing with the most popular and
current issues in RFID security. Don't dare miss the Israel
Torres article titled *RFIDIOT for Mac OSX*. As usual, Israel has
written for us a description of his own experiments. I think the
Interview With Dr. Ann Cavoukian prepared by Rebecca Wynn
doesn't need any special recommendations. You just won't be
able to skip it.

Since August issue you can enjoy two new columns. The
Tool Time is the "how to" column, where each time you will find
the description of different tools and tricks that can be done
using it. The presented material will be of interest for beginners,
as well as for more advanced readers. The (Il)legal column will
be dealing with law regulations in IT security world and some
case studies from this area. I hope you will like them!

Wish you enjoy the reading!
Patrycja Przybyłowicz
& Hakin9 team

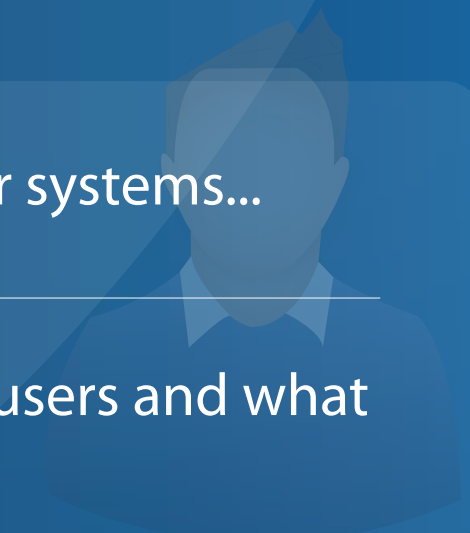
Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

Visit: <http://id-theftprotect.com>

IN BRIEF

08 Latest News From the IT Security World

By Armando Romeo, eLearnSecurity and ID Theft Protect

STORIES

10 Security by Hiding!

By Ali Hadi

I was once talking to a friend of mine about client side attacks, and how they can lead to a full compromise of the companies private network. He told me that they were safe because: first – they use a third party to host their website, and second – no one knows what IP address ranges they are using for their local LAN! When he finished I asked him if he accepts a challenge? I told him I would send him an email containing their ISP name and full IP address ranges they are using. He accepted the challenge! It was really one of the simplest tasks I've ever done in this field. Read how simply the hidden network can be found!

BASICS

14 Basics: RFID for Newbies, Sauce Security

By Gildas Avoine

Everyone knows what RFID means. However, details behind this word are usually unknown or misunderstood. We provide in this article an introduction to the Radio-Frequency IDentification technology and highlight the related security and privacy issues related to this ubiquitous technology. This is an introducing article to RFID security issues. Read it before enjoying the rest of the content!

ATTACK

20 RFIDIoT for Mac OSX

By Israel Torres

RFID when first introduced years ago convinced many that it would be the way of the future. Inventory systems would be smarter, tracking things and even people would be simpler. One could simply walk into a store, pick up their items they needed and walk out comforted by the thought that this exchange automatically deducted whatever they walked out with from their established accounts. Cars could pull up to gas stations fuel up, be automatically detected and billed accordingly. People could walk right into their office building or homes without ever have to worry about spilling their coffee looking for keys. Then the fear came...

DEFENSE

24 RFID Security and Privacy Issues

By Gary Milefsky

Here's a real-world scenario: You're a successful

executive at a large software company. You're about to be robbed but it won't be through cyber-crime or zero-day malware exploiting CVEs, as I usually write about. As you walk into your local Starbucks to pick up your favorite cup of coffee, a young man bumps into you, says excuse me and heads to his car with his cup of coffee. Next thing you know, while you're out having coffee, this young man has actually cloned your RFID card for building access and access to your office... Read what are the threats and how to secure yourself against them.

30 Passive RFID Tag Security: Electronic Product Code E-Passport and Contactless Credit Card

By Michel Barbeau

Because on their impact on the applications, security vulnerabilities of RFID tag technologies, when they are uncovered, easily draw media attention. The wireless security and access control of some key recent RFID-based technologies have been, although, interestingly designed. From this article you will learn what three key RFID-based applications are doing to secure their wireless communications and chip access.

ID EXPERTS SAYS...

38 The RFID and NFC Radio Frequency – Enabled Security Threat

By Julian Evans

A discussion on how radio frequency-enabled technology could leave people vulnerable to identity theft and then potential identity fraud. Read the article and find out why Expert Julian Evans claims, that it's only a matter of time before someone or a cybercrime gang finds a method that steals both the personal and business data from the many material objects that will in the future use RFID and NFC. This article is a very good update of the most current issues in RFID security.

INTERVIEW

44 RFID and Privacy – An Interview With Dr. Ann Cavoukian

By Rebecca Wynn

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is protected in Ontario – and around the world. Dr. Cavoukian is Ontario's first Information and Privacy Commissioner (IPC) to be re-appointed for an unprecedented third term. On July 15th 2011 our long time contributor, Rebecca Wynn, ask Dr. Cavoukian about her views on Radio Frequency Identification...

TOOL TIME

46 MITM using Cain: Client Side Attacks

By Bharath Siva Kumar

As a Boss, have you ever tried to find out what your employee is working on with his office desktop? As a network admin, have you thought of finding who is flooding the network with trivial issues? As a parent, are you eager to know what sites your kid is browsing? If your answer is yes to any one of the above, then the solution is right here. It is obvious that you just have to behave as a Man-in-the-Middle (MITM) to sort out the things. Let us have a panoramic view of MITM and how to perform it in a stealthy way.

(IL)LEGAL

50 When is Private Not Private? Making Sense of European Privacy Law

By Drake

The EU has recently changed the law regarding the saving of cookies on users' computers by websites. The Privacy and Electronic Communications Regulations (PECR) have been updated to increase privacy for website visitors and require websites to obtain consent from visitors prior to storing a cookie on the visitor's computer. Let's think about this for a moment – this is a piece of European legislation. The internet, by contrast, is not limited to the realms of the EU. So, in effect, the law applies to everyone with a website, whether or not they are hosted inside the EU. On the face of it, this makes little sense – the legal aim is clear, but the aim does not coincide with practical realities. Read the article to find out how do we get to the situation where laws are passed that no-one seems to understand...

COMMUNITY

54 The Astalavista Experience

By Sven Adelt

Astalavista.com is an IT News & Security community. It serves as a starting point for IT and security news with its continuous news stream on the main page. But Astalavista is much more, for the technical interested and IT savvy people there are a multitude of tools which can be used. These range from diagnostic tools like dig, ping and traceroute to information gathering tools, DNS tools and encryption/decryption routines. Finally you can test your IT security skills on the Wargames section. Read more about it and find out how to make advantage of all mentioned above.

CARTOONS

58 The Asylum

By Jim Gilbert

Jim's cartoons are non-figurative. The reason of this lies in his long search, how to combine words and graphics. As a result he started to draw cartoons. Specifically he is excited about The Asylum because of its minimal nature, minimal drawing, minimal words, minimal characters... maximum content. Enjoy the last set of series The Asylum by Jim Gilbert. Since September issue, we welcome a new cartoonist.

Learn
Web Application Security
with...



Coliseum

Virtual labs
100% practical hands on
training
by eLearnSecurity

FIND OUT

14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

ANONYMOUS IS BACK WITH SOME LULZ

While LulzSec has disbanded, the Anonymous group is still there fighting its Antisec battle against US government and its information security contractors.

90,000 records belonging to U.S. military personnel have been announced and released thereafter in early July. The records seem to be stolen from Booz Allen Hamilton a *leading consulting firm, helps government clients solve their toughest problems with services in strategy, operations*, another contractor indeed.

Anonymous and the other groups fighting the Antisec battle, have realized that contractors might not only hold the most sensitive data belonging to governments but they are also, most of the times at least, the weakest link.

In the meantime Anonymous is in talks with Al Jazeera journalist Yasmine Ryan to negotiate a release of what they claim to be gigs of emails of Middle Eastern Royal Families (Qatar, Bahrain, UAE).

The data, due to imminent release should contain, among other things, *their SCADA oil pipeline access and their exploitation of money*.

Source: Armando Romeo,
www.elearnsecurity.com

BROWSERID IS THE NEW SIGN IN PROTOCOL BY MOZILLA

Over the years a number of technologies, more or less sophisticated, have come up to try to replace the old and ever-green passwords. While each technology has its pros and cons in terms of security, on the web you have to face another challenge: usability.

Web developers, between the two, tend to like usability: it increases adoption and interaction with their products. So with time and the web 2.0 era, single sign on and Facebook or Twitter based authentication has become a widespread alternative to passwords.

Mozilla, is not taking it a step further: trying to avoid using OpenID's and social network based authentication and instead using email and public key cryptography to determine the identity of a website visitor.

The project named BrowserID, requires that the email is tied to the accounts you own on the web and be verified through a pair of keys (public and private), with the private key being stored within the web browser.

Basically the data and the authentication keys are only shared between the browser, the email service that will have to implement this new feature and the website you wish to sign on. No data would be shared with Facebook and similar. Mozilla

claims BrowserID to be secure, cross-browser and user-friendly.

Is this going to be the new way to sign in?

Source: Armando Romeo,
www.elearnsecurity.com

VODAFONE NETWORK HACKED THROUGH FEMTOCELL, OR MAYBE NOT

A breaking-through news has circulated on the internet for days: Vodafone network has been hacked through buggy Femtocell.

Femtocell are small base stations, sized as a residential DSL router, that telecommunication companies sell to residential or business customers to increase the coverage of the cellular network in indoor environments.

These devices connect to the service provider and implement a series of features, sometimes even critical, that deal with the identification of the subscriber among the other things. The Hacker's Choice, historic hacking group, has claimed to have reverse engineered a Sagem-manufactured femtocell (Sure Signal Femto) sold by Vodafone UK to its residential and small business subscribers.

The hack would allow anyone with a bit of experience in hackery, to intercept calls or impersonate subscribers. And even make calls at the expenses of the victim. What's scary is the possibility to perform a remote attack against a device in the range of 50 meters. Far enough to hide in a car right?

The security issue seems to be architectural: the insecure device implements features that should be of competence of the carrier core's network authentication systems and as such easy to hijack once compromised.

A detailed wiki post has appeared on the THC website explaining the hack step by step, however Vodafone, a few days after this release, claims these vulnerabilities have been fixed in 2010 and that they are no more an issue.

Research on Femtocell seems to be on the rise and we should expect more breakthroughs in this field.

Source: Armando Romeo,
www.elearnsecurity.com

PORTUGUESE HACKERS REVENGE AGAINST MOODY'S

Moody's is the credit reference agency that gives ratings to countries economy and their ability to pay back debt. In a recession period that is seeing many European countries in serious difficulties, these agency look like more the weapon of speculators that a serious and trusted source of information for investors.

Moody's has indeed rated Portugal bonds as *junk*, the day before bonds would have been out for sale.

Surely a curious coincidence but this drastically decreased the chances for the bonds to be ever sold, making Portugal situation even worse.

Portuguese hackers have not been indifferent. A sarcastic defacement depicted first Portuguese king Afonso ranking Moody's website as Z- – and Portugal as A++.

Source: Armando Romeo,
www.elearnsecurity.com

Firefox 5 Following Chrome Release Cycle

Firefox 5 was launched on June 18th by Mozilla. Let us get the bad news out of the way concerning those of you who currently use Firefox 4 – Mozilla doesn't plan on maintaining version 4, so you will have no choice but to download/upgrade to version 5.0. It appears Mozilla is following the quick release cycle (and security improvement plan) used by Google with Chrome, so expect to be forced to upgrade to the next release – version 6.0, which is understood to be in alpha right now.

Source: ID Theft Protect

Google Plus To Default All Profiles To 'Public'

Google is about to launch a social network called Google Plus (+), which allows people with Google profiles to manage their online identity. Most people don't actually know that their Google profiles are *public* (check out this post). Google wants users to find and connect with others online – if users have a private profile this will not work, so Google will default all profiles to the 'public' setting.

Only your full name and gender will be displayed on your profile, and you will be able to edit or remove any other information that you don't want to share. If you have a *private* profile and do not wish to make your profile to be seen by others, Google suggests you delete your profile. All private profiles will be deleted after July 31st, 2011. Facebook allows users to hide their profiles from others; Google Plus isn't taking this approach. Social networks don't work if your profile is private (hidden), but you can certainly control the data that is viewable by friends and others.

Source: ID Theft Protect / julianevansblog.com

IE Remote Code Execution Vulnerability

It appears that hackers are targeting the remote code execution vulnerability that was presumably patched by Microsoft last week (CVE-2011-1255). A leading security vendor identified the flaw has been exploited in the last few days in limited attacks launched from compromised websites. The security company: Symantec said *It appears that a duplicate of the top page of the website was either hacked to include a hidden iframe tag linking*

to an exploit page or was prepared from scratch, which, if run successfully, the included shell code downloads an encrypted malicious file from the same site.

The malware connects to a command and control server on 3322.org via the HTTP protocol and waits for commands. The compromised website and websites are being distributed via e-mail. ID Theft Protect suggests users deploy the CVE-2011-1255 patch immediately.

Source: ID Theft Protect

Microsoft Update Hotmail And Windows Live With SSL

Microsoft updated SSL protection for Hotmail and Windows Live services last week (7th July) when they expanded the SSL protection to include Windows Mail and Outlook Connector. Note: the SSL encryption feature is only applicable to those of you who have Hotmail accounts.

Source: ID Theft Protect

Windows 7 bluetooth stack vulnerability

Microsoft has released a small number of patches for July (July 12th). There is one patch which is a critical update for Windows 7 and Windows Vista. Additionally there are three security bulletins rated as *important* that impact Windows and Microsoft Office.

The critical Windows 7 and Vista exploit/bug affects the Windows Bluetooth Stack. This driver enables Windows to connect with Bluetooth devices. The exploit will only work if the vulnerable system has the bluetooth set to *discoverable*

Source: ID Theft Protect

MICROSOFT WINDOWS KERNEL Win32k.sys VULNERABILITIES

Microsoft Windows is exposed to multiple security issues that occur in the Windows kernel *Win32k.sys* kernel mode device driver. Multiple local privilege escalation issues are caused by a NULL pointer reference error that occurs due to a failure to properly manage pointers to certain kernel driver objects. Multiple local privilege escalation issues occur because an use-after-free error occurs due to improper driver object management.

A local information disclosure issue occurs because it fails to properly validate certain function parameters. This vulnerability currently affects the following: Windows XP SP3 and x64 SP2, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 and Server 2008 SP2, Windows 7 and Windows 7 SP1, Windows Server 2008 R2 x64 and x64 SP1 are affected.

Source: ID Theft Protect

Security by Hiding!

Sometimes companies or lets say their IT decision makers staff think that by hosting their companies websites or services at a different physical location, than their company location is, they will make their private network more safe!

What you will learn...

- Why you need to keep your eyes open,
- Why hiding your network isn't the solution,
- Educate your staff and use security policies,
- Security Awareness.

What you should know...

- System Administration basics,
 - Familiar with security social engineering.
-

This is never true, and never will be. Because of their laziness in doing a proper lock down to the companies environment and network, they make a decision to out source their website hosting. Now look, if you can't afford resource to host your companies website locally – that's okay, but even then you have to do your job in the right way.

There has also been a big argumentation about security by obscurity. Most the time in security by obscurity, people admit, for example the presence of an FTP server, but only that they have changed its port from 21 to something else. They did a lock down to the service, but changed the port as another step in the lock down or hardening process in order to make it far from reach, especially bots. But they never say, that they rely on changing the FTP servers port for reaching or making it secure. They are hiding their services port, but they are not depending only on that! This topic is not about security by obscurity, its security by hiding in the closet!

Hiding yourself will bring you no benefit, sooner or later they will get to you, and then what? Start crying? I really think IT personnel need to start thinking and doing their jobs in the right way.

Hide and Seek

You can hide yourself, your network, but not forever. Hackers through the years have gained lots of techniques and ways to get to their target, whether

they want to get to them physically or just over the cyber space. They can get there, and it's only a matter of time. We have seen how some of the cyber attacks were done by injecting code within a website and luring employees of the target company to browse to that website. Other types of attacks where done by injecting code in the companies website itself, and by that they not only managed to reach their private network, but broke the trusty relationship between them and their website. Imagine you don't even trust your own website! Wow, that's really hard to accept, but unfortunately it's true, and it happened. Client side attacks today are the most successful types of attacks that are really hard to defend against, especially if you have those lazy admins running your office, and not to forget those employees who think that what they have on their PC's is useless and worthless, so they use the lamest passwords such as 123, or their phone numbers! But wait, I don't want you to forget that there is also some other way of seeking you – *Social Engineering!*

Making you my Engineer!

What? Yes, I can re-engineer you to benefit from you and information you have. I was once talking to a friend of mine about client side attacks, and how they can lead to a full compromise of the companies private network. He told me that they were safe because: first – they use a third party to host their website, and second – no one knows what IP address ranges they are using for their

local LAN! When he finished I asked him if he accepts a challenge? I told him I would send him an email containing their ISP name and full IP address ranges they are using. I told him, that it should be enough to convince him, that hiding isn't the proper way to defend the network. He accepted the challenge! It was really one of the simplest tasks I've ever done in this field. All I had to do was to call the target company (the one my friend is working in) and ask anyone who was working there, the following:

Me: Hello, I'm from ISP ABC. We are doing a survey about our services, and wish to know what do you think about it??

Employee: Sorry, from where?

Me: ISP ABC.

Employee: But we are a client of ISP XYZ, not ABC!

Me: Oh, sorry then. But anyway won't you be thinking of doing the move to ABC? We can give you a better offer?

Employee: Sorry, you have to talk to the IT department about that.

Me: Okay, I will be in touch with them soon.

Just like that, I've managed to find out which ISP they are using. Because, I didn't hang up the phone, when their employee told me which ISP they are using – my call wasn't considered as a suspicious one. I let him/her think I was really doing a survey for ISP ABC. Honestly, I could have done it also in another way. Just by sending my friend an email or checking any of the emails he has sent me in his official working hours. It would be easy for me to know his IP address from the email's headers that are exposed to me!

Anyway, now I had their ISP name, it was easy to use a tool or any of the websites that provide IP address tools to get at least one IP address, that belongs to their ISP XYZ. I only needed one IP to dig further and get their full IP address range. I got one IP address and then went to phase two of my friends challenge.

I picked up the phone and called their ISP (XYZ). And had the conversation below:

Me: Hello, I'm Engineer XXXXX (gave my friends real name) from company example.com, and I have a set-up that I need to do for my manager's tomorrow seminar, he will be holding. I want to host the set-up on one of our IP addresses you gave us. We have 8 IP addresses from you, but I can only know one of them! Can you help me with that?

ISP: Yes sure, what was your companies name again please?

Me: It's example.com, and one of our IP addresses is XX.XX.XX.XX (XX is used as IP addresses to represent the example).

ISP: Sir, sorry but that IP doesn't even belong to you!

Me: What? I beg your pardon? (shouting a bit)

ISP: Yes sir, that IP address is for someone else. Your companies IP Address range is: (XX.XX.XX.XX to XX.XX.XX.YY), and you only have four IP addresses not 8!

Me: I knew there was something wrong. Thank you very much, my manager will be really happy with me tomorrow.

ISP: No problem at all, your more than welcome any time.

Just as simple as that, I passed the challenge or as we say in the security world – *I captured the flag*. Now I wrote my friend a nice letter with the IP address range I've challenged him with. He was shocked!

I can see you, I know where you are!

Hiding is never a proper way to defend yourself. Do the security measure first, then hiding would have been another security layer on the top, but it won't be the only layer to your organization or company's network. People, including IT as well, need to know that every PC, device, server, and asset within a company's network is important and needs to be secured from outsiders. They need to take out of mind that only the government agencies need to care about security, and not them. I know lots of people, who whenever you tell them about security and the importance of even their simple data, they either start laughing or start telling you that they are not the CIA!

Security in its basic level is just like the doors and the windows to our homes. Why don't we have homes without doors? Or homes with open windows? Leave them open then, and I'm sure the next day you will find your wallet (if not something bigger) has been stolen, just like the hacker stole your email. It's the same idea, only implemented differently!

Finally, if security was for those agencies only? Why do most of these people come crying after their email has either been stolen or been abused by someone? Why don't they just say: *its okay, my email wasn't very important, in the end I'm not a CIA agent?* The reason is, that they all are lying in one way or another, everything that belongs to us is important, but it's the matter of whatever I want to spend some tiny winy time for protecting myself or not?

Governments, companies and institutes must start security awareness campaigns in their area. People need to know about the risks of the Internet and what could come from it. People need to be aware, about how they can be misused and even robbed. How many times did you get that African Bank Manager who has millions of dollars and doesn't know where to go with them (hehehehe)? Do you really think that a person,

On the 'Net

- <https://addons.mozilla.org/en-US/firefox/addon/noscript/> – NoScript Firefox Addon,
- <https://addons.mozilla.org/en-US/firefox/addon/flashblock/> – Flashblock Firefox Addon,
- http://www.sans.org/security-resources/policies/Acceptable_Use_Policy.pdf – InfoSec Acceptable Use Policy – SANS.

who was able to become a bank manager is so naive that doesn't know where to go with all those millions? What a dumb manager he is then! Wake up! You are in the middle of a social engineering attack. How we can defend against such attacks depends on our awareness level. So really, I think that security awareness is the next step we all need to go through.

With people not appreciating what the security threat can cause them or their organization, it will be really nearly mission impossible. But wait, I don't believe in impossibility, especially in the Computer World.

I don't want to be Hypnotized?

If you really don't, then please consider the following points below:

- Harden or lock down your network properly, and don't leave it to chance and hiding, because hiding won't serve you well.
- Always monitor carefully even the trustworthy appliances or services that your company owns. Who knows you might be compromised from them. Use tools such as NoScript, FlashBlock, etc. with your Firefox browser to check the running scripts (java scripts or whatever is running in the background). These will really help you whenever you browse a website, or not. It will also help you to check if the code is harmful. Today most of the attacks are targeting clients by malicious scripts and flash in websites content. These tools will really help you mitigate some of them, if not all.
- Never use your company's assets such as emails for your own personal needs. I've seen lots of people use them in public forums and stuff like that. This is very dangerous and can lead in the attackers profiling phase.
- The weakest point in any secure environment is the personnel. Start by giving your company's employees sessions about awareness and why it is very important. Security Awareness is a growing topic in the industry not because of nothing, but because there is real need of it. We need to be educated whether we are IT guys or not, we all have important assets we need to protect. Grown-ups and kids today know that doors are for their security, so why not make them all know that the computer security awareness is needed for their electronic assets?

- I always say that your life can be easier by documenting everything and using a proper security policy for the company. The policy or guidelines will really help you a lot. And one of the most important policies in our companies today is the *Acceptable Use Policy* (AUP). I highly recommend working on one, and enforcing it on your network users.
- Finally, don't come crying when you loose your photo or email. Your mother and father warned you, and it's up to you now :)

Summary

I don't know if you ever heard about the Joke that says: *In year 2020 if you loose your car keys, you can ask Google for it, and it will tell you it's on the table!* It's a joke sure, but if you think about it, you will find it close to reality. So, if Google can know where is your car keys, can't the bad guys know where you are? I leave that thought up to your consideration. Even though it's a joke, but it's the one that you really need to think about.

ALI HADI

The author has been working as a network security officer for different large companies for more than five years. His day to day activity is related to firewall auditing, IDS/IPS, and policy enforcement. He holds a Ph.D. degree and MS.c. degree in Computer Information Systems (CIS), and a BS.c. degree in Computer Science. Throughout his working career he managed to gain a couple of well known technical certificates such as: OSCP, ECSA, CEH, CNI, CLP10, CLA10, CLDA, IBM Certified Specialist – System Administration, Novell Linux Specialist, and RHCE.



UAT's coveted Bachelor of Science degree in Network Security is a vital national resource

One of the most prestigious Network Security programs in the country

We will teach you the concepts of security by design, and layered security to protect against exploitation of networks and data

UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency

THEY SELDOM SMILE AT THE NSA. CAN YOU MAKE THEM GRIN?

Learn how to synthesize and apply these vital skills and leadership ability to succeed in the fast moving field of Network Security.

Bachelor of Science
Network Engineering
Network Security
Technology Forensics

Master of Science
Information Assurance

Program accreditations, affiliations and certifications:



⚠️ CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREE STUDENTS: Advancing Computer Science, Artificial Life Programming, Digital Media, Digital Video, Enterprise Software Development, Game Art and Animation, Game Design, Game Programming, Human-Computer Interaction, Open Source Technologies, Robotics and Embedded Systems, Serious Game and Simulation, Strategic Technology Development, Technology Product Design, Technology Studies, Virtual Modeling and Design, Web and Social Media Technologies

Prepare to Defend!

www.uat.edu

877.828.4335

RFID for Newbies, Sauce Security

Everyone knows what RFID means. However, details behind this word are usually unknown or misunderstood. We provide in this article an introduction to the Radio-Frequency IDentification technology and highlight the related security and privacy issues related to this ubiquitous technology.

What you will learn...

- Basics about RFID technology,
- security issues in RFID systems.

What you should know...

- Basics about integrated circuits,
- cryptographic authentication,
- ISO standards.

Our aim is not to provide a handbook, but a concise article that presents the background required to instill interest and read more focused and detailed technical articles. We so suggest for each topic, some links and further readings.

Foretaste

There is not a single day where we do not use RFID. *Radio Frequency Identification* (RFID) is indeed a pervasive technology deployed in many applications to identify or authenticate objects and subjects with neither physical nor visual contact. As illustrated on Figure 1, an RFID system usually consists of tags, i.e., a microcircuit with an antenna, carried by the object or subject, some readers that allow to remotely query the tags, and a back-end system that can be centralized or distributed into the reader(s).

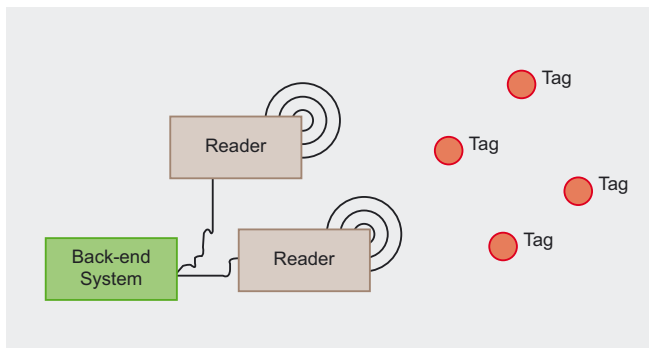


Figure 1. Entities involved in an RFID system

Toward a Unified Definition

A common idea is that an RFID tag is just a transponder that backscatters a unique identifier, used for supply chains, libraries, and pet identification. An RFID tag can actually do much more than simply backscattering an identifier, and it is even tricky to define the limits between RFID and the other evolved technologies. In a recommendation published in 2009, the European Commission considers that *RFID means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.* [1] According to this definition, contactless smartcards also belong to RFID.

Some Reasons to Move to this Technology

RFID has a lot of advantages that make it a very promising technology. First of all, the fact that no contact is needed to read an RFID tag allows to use it where traditional smartcards are not invited: pet identification, electronic passports, but also access control for ski lifts as you do not have to remove your gloves and take out your tag when passing the turnstiles! More interestingly, RFID allows for real-time localization and inventory in warehouses and libraries. In warehouses, putting RFID on palettes, boxes, or items clearly reduces unknown losses. RFID also brings advantages in access control

applications by speeding up the flow of customers. This is especially desirable in mass transportation and already deployed in many cities like Brussels, Boston, London, New York, Paris, and Singapore to name a few.

Flashback to World War II

Contrarily to what one may think, RFID is not a technological revolution that appeared during the last decade. A regularly cited application as being the first real deployment of RFID is the *Identify Friend or Foe* system used by the *Royal Air Force* during World War II to identify Allied aircrafts. Today's RFID no longer looks like those of Grandpa, although the physical principles are still the same. With the advances in microelectronics and the introduction of smartcards in the 70s, RFID tags early became very small (see Figures 2 to 4) and cheap devices capable of computations. As highlighted by Mark Roberti in the *RFID Journal*, Charles Walton seems to be the first one who got a patent related to passive transponders, in 1973 [2].

Commercial applications really started in the 80s and growing up in the 90s with the commercialization of some famous products like Mifare by NXP Semiconductors (formerly Philips Semiconductors) used for public transportation passes, loyalty cards, access control badges, etc. One billion Mifare-based products have been sold from 1995, according to NXP [3]. Another notable event in the RFID history is the creation in 1999 at the MIT of the Auto-ID Center [4], yielding to EPC Global Inc. [5], whose goal is to promote and standardize RFID in supply chains.

Nowadays, the cost of a tag can be as low as 15 cents and as small as a grain of rice. We will see nevertheless that most of tags are bigger and more expensive than that.

Focus on the Communication Distance

There exists a wide range of tags with many different characteristics. The characteristics of the tags mostly depend on the application they are used for. A common point, though, is that most of them are passive, meaning



Figure 2. RFID tags for logistics



Figure 3. RFID tags for animal identification

that they do not contain any battery; instead, they catch their energy from the electromagnetic field of the reader. Except when explicitly stated, RFID always means passive RFID in the common language. We will also use this convention in what follows. The main characteristic to point out is the communication distance between the reader and the tag. It obviously depends on several parameters, one of them being the frequency band of the tag. We consider three main frequency bands in RFID [6]: LF (125-134 kHz), HF (13.56 MHz), and UHF (860-960 MHz). The communication distance with LF is not longer than a few centimeters. This kind of tag is, for example, used for pet identification as LF can easily cross liquids (and a dog or a cat, as us, is nothing but a bag of water). UHF is the new trend as the communication distance can be as long as a few meters. This makes it an ideal candidate for applications related to the supply chain industry. Finally, HF is in practice the frequency band almost always used for secure applications: its communication distance is between a few centimeters to a few decimeters depending on the standard that is used in the low layers of the communication model, especially ISO 14443 [7] or ISO 15693 [8].

Typical Configurations and Performances

Establishing a classification of tags is not easy as many parameters must be considered at the same time: memory type and size (RAM, ROM, EEPROM), computational



Figure 4. RFID tags for various applications

capabilities (w/o processor), communication rate, etc. Instead of a classification, we provide three typical configurations we can encounter in our everyday life.

- **Supply Chain.** In such environment, UHF tags are typically used in order to benefit from their long communication distance. The tags can be compliant with EPC Gen 2 [9] with a cost as low as 15 cents. Of course, they have almost no calculation capabilities, except an anti-collision scheme and the ability to check a password to definitively disable the tag. EPC Gen 2 is a standard developed by EPC Global Inc. [5] especially to target this application.
- **Passport.** HF tags are used, compliant with ISO 14443, which implies a communication distance less than 10 centimeters (with legal readers). Such tags embed a processor, although they are passive, and are able to perform heavy cryptographic operations typically RSA1024 or ECC [10]. Typically, they contain a 70-KB EEPROM.
- **Ski lift.** HF is also used in this case, with tags compliant to ISO 15693, which allows reading tags at a distance of about 50 centimeters. Cryptographic functions can be available on such tags, but usually implemented without any processor. The cost of such a tag is about 70 cents. Typically, they contain a 1-KB EEPROM.

Playing with Tags

It is really surprising to see that most of graduated students in computer science never played with RFID tags (nor smartcards) during their studies, while an RFID tag is nothing but a miniaturized computer. LF tags are usually compliant with proprietary specifications and playing with them implies to use the provided software. Some standards exist, though, for example for pet identification [11][12]. Hence, one can easily read the ID of his dog using open-source libraries or softwares, for instance RFIDiot [13].

UHF tags are not very fun as they usually contain only an identifier, and UHF readers are more expensive than LF or HF readers.

To play with RFID, HF devices probably constitute an easy and interesting starting point. Currently, the most interesting tags to play with are the HF tags

compliant with either ISO 14443 [7] or ISO 15693 [8]. These documents standardize the physical and communication layers. This greatly helps the quick deployment of RFID solutions as many readers and tags comply with these standards, for example ACR122 (ISO 14443) and Omnikey 5321 (both ISO14443 and ISO15693), compatible with Windows, Mac OS, and Linux, and available for less than 60 euros.

Interacting with a tag can be easy (but limited) using off-the-shelf softwares provided by the manufacturer or any other RFID expert. For example, one can easily play with the application Touchatag [14] or read his own electronic passport using ePassport Viewer [15]. However, interacting with an integrated circuit can be done using the commands defined in ISO 7816 [16] when it complies with this standard. Mifare tokens are partly compliant with ISO 14443 and ISO 7816 and are so good candidates to start playing with RFID. One can play with a Mifare Classic, which are just memory cards whose access is protected with a stream cipher (broken in 2008) or more evolved tags, for example Mifare UltralightC or DESfire, which allow to manipulate cryptographic protocols through ISO 7816-compliant commands. Some others will prefer to recover the keys of their Mifare Classic tag and will use appropriate tools, like mfoc and mfcuk [17]. Finally, designing its own evolved RFID solution can be pretty cheap using Java cards, like JCOP to name one of them.

We provide below a simple example to illustrate the query of a Mifare Ultralight tag called *touchatag* [14], using the tools `pcsc_scan` and `gscriptor`.

The first test is `pcsc_scan` used with Linux. It regularly scans every PC/SC readers connected to the computer, and displays, as illustrated in Figure 5, the detected ones (in this case an ACR122, although named ACR38U).

In Figure 6, we can observe that we communicate with the tag using some APDUs [16] [18]. First we poll the tag with the command `ff 00 00 00 04 d4 4a 01 00` and then we get the remaining answer with the command

`ff c0 00 00 11`. Its answer is `D5 4B 01 01 00 44 00 07 04 A1 71 F9 23 25 80 90 00` where:

- `01` is the number of tags found.
- `01` is the target number.
- `00 44 00` are anti-collision data.

```
avoine@rantanpan:~$ pcsc_scan
PC/SC device scanner
V 1.4.16 (c) 2001-2009, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.5.3
Scanning present readers...
0: ACS ACR 38U-CCID 00 00

Sat Jun 18 17:33:27 2011
Reader 0: ACS ACR 38U-CCID 00 00
Card state: Card inserted,
ATR: 3B 00

ATR: 3B 00
+ TS = 3B --> Direct Convention
+ T0 = 00, Y(1): 0000, K: 0 (historical bytes)
```

Figure 5. Detecting RFID readers using the tool `pcsc_scan`

```
avoine@rantanpan:~$ gscriptor
No reader given: using ACS ACR 38U-CCID 00 00
Using T=0 protocol
Reading commands from STDIN
ff 00 00 00 04 d4 4a 01 00
> ff 00 00 00 04 d4 4a 01 00
< 61 11 : 0x11 bytes of response still available.
ff c0 00 00 11
> ff c0 00 00 11
< D5 4B 01 01 00 44 00 07 04 A1 71 F9 23 25 80 90 00 : Normal processing.
```

Figure 6. Pooling the tag using the tool `gscriptor`

- 07 is the length of the tag identifier.
- 04 A1 71 F9 23 25 80 is the tag identifier.
- 90 00 means that the command ended properly.

In Figure 7, we read the first four of 16 memory pages contained by the tag, by sending the command ff 00 00 00 05 d4 40 01 30 00 then ff c0 00 00 15 to get the remaining data. One can easily observe that the first two pages contain the tag identifier (where 5C is a checksum): D5 41 00 04 A1 71 5C F9 23 25 80 7F 48 FF 7F E1 10 06 00 90 00. The same command could be sent to read the remaining pages, replacing 00 by 04, 08, and 12.

To go further in practical handling, many open-source libraries are available on the Internet. The website YobiWiki [17] references the most widely used ones, for example librfid, libnfc, rfidiot, and many others.

Considering Security and Privacy

While RFID has been around for several decades, RFID security only became recently a major concern in the information security community. Expertise in security of smartcards was already well-established but the RFID technology raised new problems unexplored until then. The fact that most of tags are batteryless and resource-constrained leads to new challenges on lightweight cryptographic designs and implementations. Also, tags are pervasive, communicate wirelessly, sometimes without awareness of their holders. This clearly modifies the threat model compared to smartcards with contacts.

RFID security issues are commonly classified into 3 families that are described below: impersonation, privacy, and denial of service.

Impersonation

Many evolved applications require authentication and not only identification. This security objective does not refer to RFID environments only, but low-capability tags make this objective hardly reachable. An *impersonation is a deception whereby one entity purports to be another*. [19]. A key-recovery attack is more powerful as the adversary obtains the credential, which is stronger than only impersonating the entity. In RFID, cloning is even stronger as it consists in copying the public and private data of a given tag into another one. Even when the

credentials are known, the cloning attack is hard to put into practice with cheap means as commercial blank tags usually store a unique ID that is not modifiable. These attacks can be due to weaknesses in the authentication protocols, in the cryptographic algorithms, in the key generation, in the physical protections of the integrated circuit, or to many other means.

Security Flaws in the Press

Many deployed RFID solutions expected to provide security are weak. Usually, these weaknesses would be very easily discovered with the specifications of the product. Unfortunately, security by obscurity is still too often applied in RFID and so security audits are done without the technical specifications.

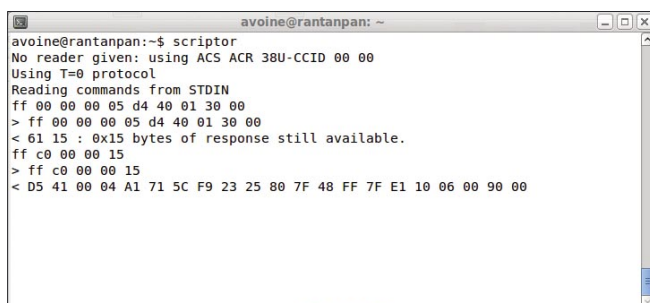
Nevertheless, practical impersonation attacks hit the headlines for a few years. One may cite the attacks against the Texas Instruments' Digital Signature Transponder, the Keeloq ignition car system [20], the Mifare Classic card, among the most famous ones. Real-life frauds based on these attacks are rare or, more precisely, not so much publicly known. However, frauds can also rely on failures in the policies, for example in the manufacturing process of the cards, as recently discovered in Boston's mass transit system [21].

Relay attacks

Another major concern is the relay attack, thoroughly detailed in [23]. The relay attack, introduced by Desmedt, Goutier, and Bengio in 1987 [23], defeats any classical authentication protocol by relaying the low-layer communication between the parties involved in the protocol. Hence, encryption cannot thwart the attack. In RFID, the aim of this attack is to make the reader think that the tag is in its neighborhood while it is not. Consequences of such an attack can be quite serious when considering payment systems.

The relay attack takes root in the famous *Postal chess grandmaster* problem introduced by John Conway in 1976 [24] where a little girl, Anne-Louise, plays two chess correspondence games with both Bobby Fisher and Boris Spassky. Anne-Louise simply mirrors the moves of the two grandmasters and eventually wins against one of them, or draws with both of them. Obviously, the two grandmasters are not aware of the trick, thinking they play with Anne-Louise. This attack is illustrated in a video where an illusionist, Derren Brown, challenges nine top-level chess players simultaneously [25].

The relay attack has been successfully implemented in RFID by Gerhard Hancke in 2005 [26] over a 50-meter radio channel between two accomplices. Since then, ready-to-use tools have been published, for example the LibNFC library allows to perform a relay attack on ISO 14443-compliant tags over a channel created between two computers.



```

avoine@rantanpan:~$ scriptor
No reader given: using ACS ACR 38U-CCID 00 00
Using T=0 protocol
Reading commands from STDIN
ff 00 00 00 05 d4 40 01 30 00
> ff 00 00 00 05 d4 40 01 30 00
< 61 15 : 0x15 bytes of response still available.
ff c0 00 00 15
> ff c0 00 00 15
< D5 41 00 04 A1 71 5C F9 23 25 80 7F 48 FF 7F E1 10 06 00 90 00

```

Figure 7. Reading the tag using the tool scriptor

Countermeasures to relay attacks and variants are based on the calculation of the round-trip time of a message between the reader and the tag. This countermeasure suggested in 1993 by Brands and Chaum [27], called *distance bounding or proximity check*, is still an experimental one that is not used in commercial products. We nevertheless raise that NXP announced that Mifare Plus contains a proximity check [28], which is a simplified one.

Privacy

RFID also raises controversial questions about privacy. Privacy advocates claim that RFID endangers individual liberties and consider it as a way of obtaining information about citizens without their consent. Among them, CASPIAN [29] is an active group of *Consumers Against Supermarket Privacy Invasion and Numbering*, created in 1999 by Katherine Albrecht, and very active in the USA.

Beyond Human rights organization, authorities are aware of the privacy issues and address them. For example, in its recommendation SEC(2009) 585/586 about RFID, the European Commission states: *Because of its potential to be both ubiquitous and practically invisible, particular attention to privacy and data protection issues is required in the deployment of RFID. Consequently, privacy and information security features should be built into RFID applications before their widespread use (principle of security and privacy-by-design)* [1].

Among privacy, one may distinguish *information leakage* where the tag or the back-end reveals some personal information, from *illicit tracking* that consists in tracking a tag and so its holder.

Information leakage

Information leakage can arise from the tag or from the back-end system. For example, an ID card or a

Bibliography

- Viviane Reding, Commission Recommendation of 12.05.2009 – SEC(2009) 585/586, 2009 [1],
- Mark Roberti, The History of RFID Technology [2],
- <http://www.nxp.com> [3],
- <http://www.autoidlabs.org/> [4],
- <http://www.gs1.org/epcglobal> [5],
- Information technology – RFID for item management, 2008 [6],
- ISO/IEC 14443 Identification cards – Contactless integrated circuit cards [7],
- Identification cards – Contactless integrated circuit(s) cards [8],
- EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID v1.2.0, 2008 [9],
- DOC 9303 – Machine Readable Travel Documents [10],
- Identification d'un transpondeur évolué, 1996 [11],
- Identification des animaux par radiofréquence – Concept technique [12],
- <http://www.rfidiot.org> [13],
- <http://www.touchatag.com> [14],
- <http://sites.uclouvain.be/security/epassport.html> [15],
- Identification cards – Integrated circuit cards, 1994 [16],
- <http://wiki.yobi.be/wiki/RFID> [17],
- Application Programming Interface – ACR122 Version 1.0, 2008 [18],
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, 1996 [19],
- Mid-Atlantic Ravelco & CarThiefStoppers.com, <http://www.carthiefstoppers.com/> [20],
- Eric Moskowitz, Many conspired in T pass fraud, May, 21st, 2011, 2011 [21],
- Avoine, Bingöl, Kardas, Lauradoux, and Martin, A Framework for Analyzing RFID Distance Bounding Protocols, 2011 [22],
- Yvo Desmedt, Claude Goutier, and Samy Bengio, Special Uses and Abuses of the Fiat-Shamir Passport Protocol, 1987 [23],
- John H. Conway, On Numbers and Games [24],
- Derren Brown, <http://www.youtube.com/watch?v=evZmpsI3jI0>, 2007 [25],
- Gerhard Hancke, Practical Attacks on Proximity Identification Systems, 2006 [26],
- Stefan Brands and David Chaum, Distance-Bounding Protocols, 1993 [27],
- Marc Vauclair, MIFARE Plus & Privacy Preserving Technologies, 2009 [28],
- <http://www.nocards.org/> [29],
- <http://wiki.yobi.be/wiki/MOBIB> [30],
- <http://www.abiec-bvirh.be/> [31],
- http://en.wikipedia.org/wiki/RFID_Zapper [32],
- Lukas Grunwald, <http://www.dn-systems.com/company/team/>, 2007 [33],
- <http://en.wikipedia.org/wiki/Rfid> [34],
- Klaus Finkenzeller, RFID Handbook, 2010 [35],
- <http://wiki.yobi.be/wiki/RFID> [36],
- Ari Juels, RFID Security and Privacy: A research Survey, 2006 [37],
- <http://www.avoine.net/rfid/> [38],
- <http://www.rfid-sec.org> [39],
- Katherine Albrecht and Liz McIntyre, Spychips, 2006 [40].

passport may leak some personal information. A public transportation pass may reveal the last locations where the holder passed [30].

Encrypting the data or requiring an authentication of the reader may solve the problem, but protecting the data in the database is also required. To illustrate the problem, one may consider the case of pet registration in Belgium. Electronically tagging his dog is mandatory to move within the Schengen Space. In Belgium, this registration is managed by ABIEC [31], which offers on its website some search tools to query the database. Unfortunately, these tools allow anyone knowing a dog's tag identifier to get sensitive information about the owner (name, address, phone number, etc.). Such a tag identifier can be obtained for example from Google, and then some other tag identifiers can be guessed as they are simply sequential numbers, which allows to enumerate all the dogs' owners in Belgium.

Illicit tracking

Illicit tracking consists in tracking a tag in different places or at different times without the agreement of its holder. Avoiding this problem is quite hard as everything sent by the tag can potentially allow to track it.

People are probably less worried by this kind of attack, but researchers work a lot on this topic as no nice solution exists yet. Roughly speaking, the tag should not send any intelligible information, including its identity, in the clear when it tries to be authenticated. This implies that the reader authenticating the tag does not know which cryptographic key should be used to perform this authentication. Either all the tags use the same key, which is basically an insecure option, or the reader tests all the keys it knows, which is an inefficient option in large-scale systems. Designing privacy-friendly RFID solutions is still a challenging task which many research works focus on.

Denial of service

Denial of service, which is far less considered by the research community, may have awful consequences in large-scale or sensitive RFID applications, for example when tags are used to control a supply chain. A denial of service can be done using some electromagnetic means to noise the tag-reader channel or to kill the tags [32], but it can also be applied in the higher layers. For example, one may exploit a bug in the reader firmware

to crash the system as suggested by Lukas Grunwald [33] against ePassport readers, or erase the tag's memory when not protected against illegal writing.

Summary

RFID is a wide and quickly evolving technology that cannot be completely presented in a few pages. After this short introduction, we recommend some readings to allow readers to strengthen their knowledge.

- A large view of existing RFID applications can be obtained on the Wikipedia RFID page [34]. It also presents some standards related to RFID, although this reference is not the best one for those who look for technical details.
- A technical approach of RFID is available in the excellent *RFID Handbook* by Klaus Finkenzeller [35]. It will soon become your bedside book.
- Geeks will enjoy the really unavoidable website YobiWiki [36] that references all libraries, tags, readers, that allow you to play with RFID. It also provides many practical tips to make your readers properly running.
- The first hardware one may purchase to get fun with RFID could be an ACR122 reader and a few Mifare cards (Ultralight, Classic, and UltralightC), available on Internet for a hand of dollars.
- For a research-oriented view, a comprehensive state of the art paper [37] written by Ari Juels is probably a good starting point. It is nowadays a bit outdated but still provide some strong background before moving to more recent publications.
- References toward scientific publications about RFID security and privacy can be found on the RFID Security & Privacy Lounge [38]. About 800 researchers are registered to this lounge.
- The major research-oriented workshop about RFID security and privacy is *RFIDSec* [39] organized since 2005 in USA and Europe. There is also an IEEE conference organized in the USA since 2007, that mainly addresses antennas, circuits, softwares, protocols, and security.
- Finally, liberty rights defenders may find their *alter ego* in *Spychips* [40], written by Katherine Albrecht and Liz McIntyre.

GILDAS AVOINE

Gildas Avoine is a professor of information security and cryptography at the UCL in Louvain-la-Neuve (Belgium), where he launched in 2008 the Information Security Group (GSI). The GSI addresses many theoretical and practical research topics, including (but not limited to) the security and privacy problems in Radio-Frequency IDentification (RFID). Gildas Avoine also founded the RFID security and privacy lounge (www.avoine.net/rfid/), a scientific

portal that references research-oriented publications related to the domain. Before joining the UCL, he was researcher at the MIT (USA) and at the EPFL (Switzerland), where he obtained a PhD degree in cryptography. Previously, he studied at the University of Caen (France) where he received a Bachelor degree in mathematics and Bachelor and Master degrees in computer science. Prof. Avoine is also an independent expert in cryptography and information security. He leads training and consulting for companies.

RFIDIOT for Mac OS X

RFID when first introduced years ago convinced many that it would be the way of the future.

What you will learn...

- How to install RFIDIOT on Mac OS X 10.6.8 via automation

What you should know...

- RFID theory, simple shell programming

Inventory systems would be smarter, tracking things and even people would be simpler. One could simply walk into a store, pick up their items they needed and walk out comforted by the thought that this exchange automatically deducted whatever they walked out with from their established accounts. Cars could pull up to gas stations fuel up, be automatically detected and billed accordingly. People could walk right into their office building or homes without ever have to worry about spilling their coffee looking for keys.

Then the fear came – the number of the beast and all that... talks of a *national id card* (NID); citizens being injected with a tiny bead of trackable information now



Figure 1. Bootable Live RFID Hacking system (OpenPCD)

became a sign of apocalypse instead of technology. Paranoia called for more privacy and security (both fantastic illusions that many still believe in today). More questions came, less progress achieved.

For the average consumer RFID still hasn't arrived. The only real chance of finding RFID mechanisms to play with are slim to none. Places that one would think would have them don't. The only real place RFID is seen is in the corporate world where they are used for proximity security, vehicle transponders, library systems, anti-theft devices, wholesale inventory.

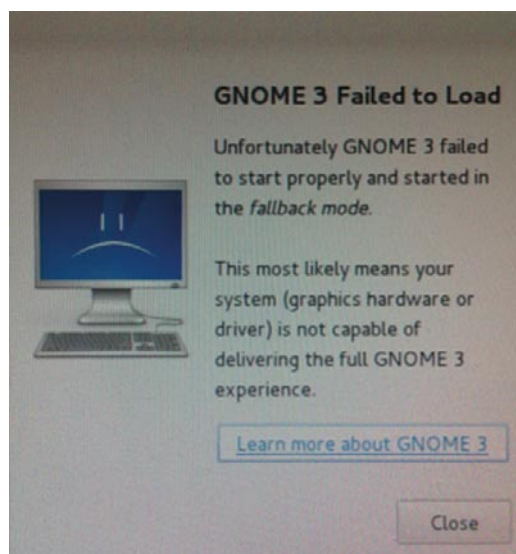


Figure 2. Gnome3 Fail

To the naked eye it is obvious that the world is still hung up on analog devices such as magnetic stripes, and barcodes – even multidimensional barcodes that only machines can read anyway (at least effectively).

RFID Hacking

RFID Hacking for the most part has come to a standstill; googling the phrase itself brings up old information from a few years back; when it seemed it was at its peak. I was quite excited to see mention of a Bootable Live RFID Hacking system (OpenPCD) the other day (link below). I downloaded the ISO and burnt it using my Mac, then booted up my Mac Mini to play away. Unfortunately my playtime started to crumble when I saw a crash screen when using the default configuration, on the reboot used the basic mode (Figure 1); things were looking good until I got the Gnome3 fail screen (Figure 2) As described on the support site I looked around for the tools, and played with them a bit before realizing it was still in development; also it didn't appear my RFID reader was supported so I moved on (perhaps to return to it another day).

I looked around the Mac App store and to my surprise saw a new app recently recently; named ReadRFID for 11.99\$USD. (Figure 3) I read the description and perused the support site and the support files for the integration. I purchased it downloaded it in the blink of an eye; plugged in my reader put the RFID token on top of the reader put the RFID token on top of the reader (although it has a 5 inch proximity detection range) and pressed the Read RFID button. Much to my chagrin the error returned *No RFID Reader found* (Figure 4). I searched around the preferences and support documents and nothing positive resulted (again perhaps to return to it another day).

I cursed at my USB RFID reader; *Y U NO WORK?!* perhaps the reader was too old or somehow broke? I had a stack of laptops that I used to test with it a few years ago when I bought it at a LayerOne conference

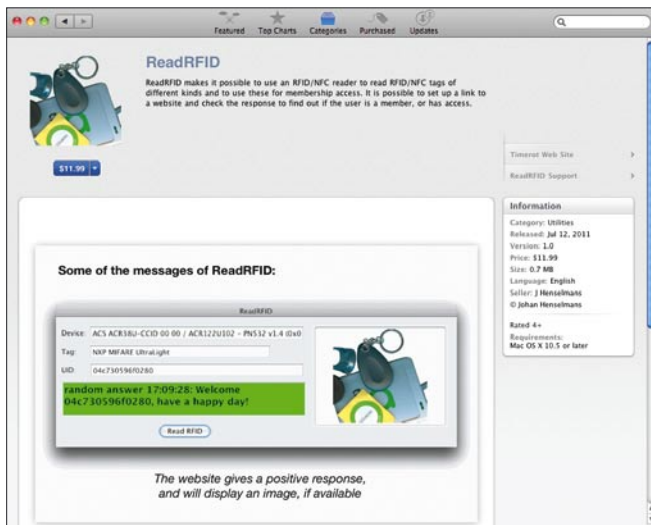


Figure 3. ReadRFID Mac App Store

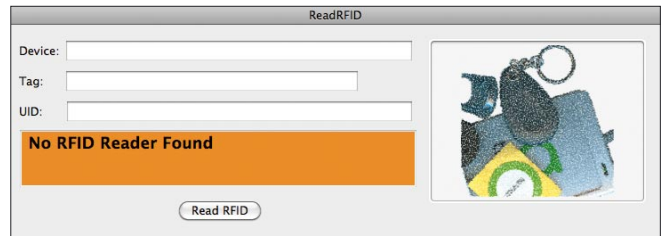


Figure 4. ReadRFID No RFID Reader Found

from Adam Laurie (himself). That's when I figured I'd give his site a visit and see what could be done with RFIDIoT. The site looked the same as what I remember of it. The page stated it was last updated July 12th 2011; but the latest update was marked March/June 2011 for ubertooth-one. Anything else seemed to still have a 2009 timestamp on it. The documentation page was last updated March 20th 2010. I'm running the latest version of Mac OS X (10.6.8 as of this writing) and the site is referencing 10.2; the latest stable release *RFIDIoT-1.0a.tgz* dated November 30th, 2009 and the beta *RFIDIoT-1.0b-beta.tgz* dated May 6th 2010. The beta mentioned the word broken so I installed the stable version. Note that I switched to Mac March 13, 2009 so this would be the first time I've used RFIDIoT on the Mac platform; my previous experience with it was using linux. (I never tried the windows version).

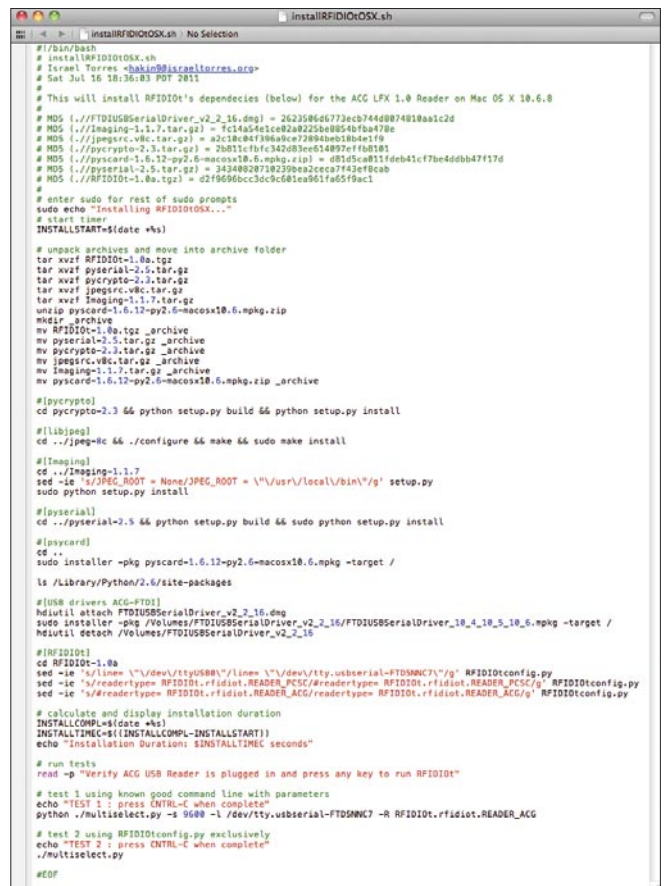


Figure 5. InstallRFIDIoTOSX Script

Versions Used

RFIDiot 1.0a
 pyserial 2.5
 pycrypto 2.3
 pycard 1.6.12
 libjpeg 8c
 Imaging 1.1.7

Site Download

RFIDiot <http://rfidiot.org/>
 pyserial <http://pypi.python.org/pypi/pyserial>
 pycrypto <http://www.dlitz.net/software/pycrypto/>
 pycard <http://sourceforge.net/projects/pycard/>
 libjpeg <http://www.ijg.org/files/>
 Imaging <http://www.pythonware.com/products/pil/>

Python 2.6.1 and Python 2.7.2
 XCode 3.2 (10M2518) and 4.0.1 (4A1006)

I also downloaded the dependencies however a lot of the links on the page were no longer valid; a lot of them were redirecting or just plain dead. I had to google and search out what would be the best guess. I built many packages over and over again; getting a lot of bad error messages. I was figuring this was going to be 0 for 3 of failure. I googled around some more not giving up hope as RFIDiot was the most promising hacking tool for RFID I had seen in person. So I persevered and found a site that mentioned instructions for building RFIDiot for Mac OS X! [link below] Aptly named RFIDiotOSX – reading more of the one page wiki it talked about running on 10.6 (certainly better). I ran through the instructions on my Macbook Pro but in the end wasn't a happy camper. I also noticed the driver link pointed to HID so it's possible this works great for an HID reader but the instructions couldn't take me all the way through.

Spending a day going over each line and reading the RFIDiot's documentation I exploded everything and started from scratch. Grabbing all the packages and dependencies I could find for each item mentioned as several versions have appeared to pass and change slowly through time. I knew for a fact that I didn't want to have to keep reinstalling things over and over so I hopped over to my test system (Mac Mini); re-imaged the Mac with an updated image of OS X using Carbon Copy Cloner, then tried to build each dependency line by line in the terminal; taking notes as I went along the way. Turns out the notes ended up getting more

```
Installation Duration: 130 seconds
Verify ACG USB Reader is plugged in and press any key to run RFIDiot.
multiselect v0.1m (using RFIDiot v1.0a)
Reader: ACG LFX 1.0 (serial no: 00070045)

Tag ID: U003B220400 Tag Type:EM 4x02 (Unique)
Tag ID: U003B220400 Tag Type:EM 4x02 (Unique)
Tag ID: U003B220400 Tag Type:EM 4x02 (Unique)
Tag ID: U003B220400 Tag Type:EM 4x02 (Unique)
Tag ID: U003B220400 Tag Type:EM 4x02 (Unique)
No card present.
```

Figure 6. Script Post Tests

```
Terminal — bash — 80x24
PIL.pth serial
README smartcard
pycrypto-2.3-py2.6.egg-info
Checksumming Driver Descriptor Map (DDM : 0)...
Driver Descriptor Map (DDM : 0): verified CRC32 $FFFE7A78
Checksumming Apple (Apple_partition_map : 1)...
Apple (Apple_partition_map : 1): verified CRC32 $7831DE93
Checksumming disk image (Apple_HFS : 2)...
.....
disk image (Apple_HFS : 2): verified CRC32 $9271EAB7
Checksumming (Apple_Free : 3)...
(Apple_Free : 3): verified CRC32 $00000000
verified CRC32 $072DA0F3
/dev/disk1 Apple_partition_scheme
/dev/disk1s1 Apple_partition_map
/dev/disk1s2 Apple_HFS /Volumes/FTDIUSBSerialDr
iver_v2_2_16
installer: Package name is FTDIUSBSerialDriverInstaller
installer: Installing at base path /
installer: The install was successful.
"disk1" unmounted.
"disk1" ejected.
Installation Duration: 130 seconds
Verify ACG USB Reader is plugged in and press any key to run RFIDiot.
```

Figure 7. Script Automation

optimized and eventually into the bash file you see here (Figure 5). I wrote this solely for the ACG LFX 1.0 Serial USB RFID Reader/Writer; it's 100% automated via the shell script including the driver install (Apple has CLI tools that to install GUI driven installers via CLI). The overall installation from start to finish takes an average of 130 seconds, and you only have to type your sudo password in at the beginning (on a default system) – the installation is long done before you would ever be prompted again due to timeout. All

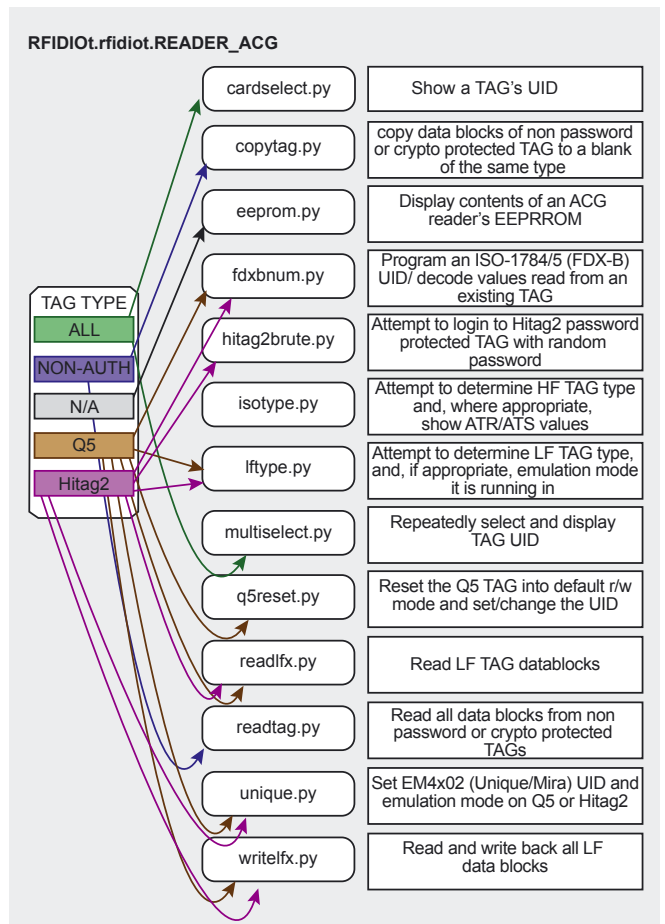


Figure 8. Useful Python Scripts

Web Links and References

<http://rfidiot.org/documentation.html>
<http://code.google.com/p/appleguru/wiki/RFIDiotOSX>
http://www.openpcd.org/Live_RFID_Hacking_System
http://en.wikipedia.org/wiki/Radio-frequency_identification
http://en.wikipedia.org/wiki/Near_field_communication

Notes

All source code created and tested on:
 Macmini3,1 and MacBookPro5,1
 Mac OS X 10.6.8 10K540
 Darwin Kernel Version 10.8.0
 GNU bash, version 3.2.48(1)-release
 Python 2.6.1 and Python 2.7.2
 XCode 3.2 (10M2518) and 4.0.1 (4A1006)

is done without rebooting and you can even plug the reader in ahead of time to run the tests immediately :) (Figure 6).

As time passes this article will also age but I'd like to describe the versions used that the script calls during the install (the script also contains all the MD5 hashes to verify the expected 'happy path' versions tested).

After all is said and done the reader is installed as `/dev/tty.usbserial-FTD5NNC7` on Mac OS X 10.6.8 and needs to be called thusly; the installer actually modifies the necessary `RFIDiotconfig.py` (configuration file) to accommodate for this reader. If you have a different reader you'll need to modify the script accordingly



Figure 9. ACG LFX 1.0 Serial USB RFID Reader/Writer

including the driver install itself. I've laid out how to call the dmg and package installers via CLI (Figure 7) so you probably just need to replace those lines. Naturally test it first one line at a time before running it via an automated process.

RFIDiot supports a slew of readers (available on the site for purchase <http://rfidiot.org/#Hardware>) but the focus of this article is the ACG LFX 1.0 (non-PCSC) so I've extrapolated this information from the documentation visually which of the python scripts is useful for this combination (Figure 8).

The RFID reader used in this demonstration is an ACG LFX 1.0 Serial USB RFID Reader/Writer covering 125 / 134.2 kHz that supports the following tags: EM4x02, EM4x50, EM4x05 (ISO 11784/5 FDX-B), Hitag 1 / 2 / S, Q5, TI 64 bit R/O & R/W, TI 1088 bit Multipage (Figure 9).

I had originally attempted to run all the builds on my *Macbook Pro* (MBP) before starting from scratch on the Mini and after the installer was tested on the mini several times after several re-images I decided to run it on my MBP to see if it would fix whatever was broken... and it did! the only caveat is that in Python 2.7.2 which is what the MBP is running the pycrypto package (pycrypto-2.3-py2.7.egg-info and Crypto and its subfolders) gets installed on `/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/site-packages` and need to be moved to `/Library/Python/2.6/site-packages` and that's it.

Conclusion

Open source software (or really just any software that allows for modification at the nth level) is super great; unfortunately as authors get busy with something new (as many of us do in the hacker realm) as well as disinterested in former projects projects slowly wither and die leaving it up to the visitors of sites to further evolve and keep the dream alive.

This further reflects how RFID has fallen away from the idea of the mainstream consumer. Reinvigoration is necessary. The future holds things via the smartphone some already come built in with the necessary electronics for NFC (*Near field communication*) but a lot of the implementations aren't optimized for use and the common folk have no idea how to use them or that it even exists. We as a whole are still far away from living a Star Trek lifestyle walking through doors that swish or communicators that know where you are, if you are hungry, what kind of food you prefer. Let's keep on trying to get there :)

ISRAEL TORRES

Israel Torres is a hacker at large with interests in the hacking realm.

hakin9@israeltorres.org, http://twitter.com/israel_torres

Got More Time Than Money?

Try this month's crypto challenge:

<http://hakin9.israeltorres.org>

RFID Security and Privacy Issues

Proactively deploy RFID in stronger and more ethical ways

Radio Frequency IDentification (RFID) is a wireless technology used to share data through radio waves. With RFID, you can transfer data between a reader and an electronic tag attached to an object for the purpose of identification and tracking.

What you will learn...

- RFID Basics
- RFID Hacking
- RFID Defense

What you should know...

- Social Engineering Basics
- Multifactor Authentication Methods
- Multilayered Security Basics

Unlike BARCODEs, RFID is used to share information without having to show the tag to the reader device.

Some RFID tags can be read from several meters away and beyond the line of sight of the reader. The application of bulk reading enables an almost-parallel reading of tags. Most RFID tags contain at least two parts: one is an integrated circuit for storing and processing information, modulating and demodulating a *radio-frequency* (RF) signal, and other specialized functions; the other is an antenna for receiving and transmitting the signal.

RFID uses hardware readers, hardware tags and software for communications into networks such as

government identification databases, retail ecommerce systems, inventory tracking, shipping and monitoring solutions. RFID can be either passive (using no battery), active (with an on-board battery that always broadcasts or beacons its signal) or *battery assisted passive* (BAP) which has a small battery on board that is activated when in the presence of an RFID reader. Passive tags are very popular and are a fraction of the cost of active tags. You'll find passive tags in *Physical Access Control* (PAC) systems, passports and retail outlets. Active tags are usually used for tracking containers or expensive medical equipment and even for monitoring environmental conditions in data centers.

Some of the most popular RFID applications are:

- Access control and management
- Tracking of goods in retail
- Tracking of persons and animals
- Toll collection and contactless payment
- Machine readable travel documents
- Passport verification and identity lookup
- Tracking sports memorabilia to verify authenticity
- Smart dust for massively distributed sensor networks
- Airport baggage tracking logistics

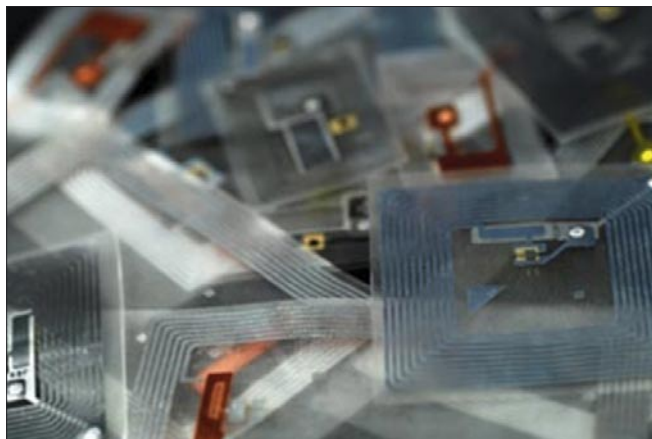


Figure 1. RFID Tags – Tiny, Portable, Easy to Deploy

History of RFID

Way back in 1945, Léon Theremin invented an espionage tool for the Soviet Union which retransmitted

incident radio waves with audio information. Sound waves vibrated a diaphragm which slightly altered the shape of the resonator, which modulated the reflected radio frequency. Even though this device was a covert listening device, not an identification tag, it is considered to be a predecessor of RFID technology, because it operated like a Passive RFID tag, being energized and activated by waves from an outside source. Similar technology, such as the IFF transponder developed in the United Kingdom, was routinely used by the allies in World War II to identify aircraft as friend or foe. Transponders are still used by most powered aircraft to this day. Another early work exploring RFID is the landmark 1948 paper by Harry Stockman, titled *Communication by Means of Reflected Power*. Later, in 1973, Mario Cardullo's device was the first ancestor of modern RFID, as it was a passive radio transponder with memory. The initial device was passive, powered by the interrogating signal, and was demonstrated in 1971 to the New York Port Authority and other potential users and consisted of a transponder with 16 bit memory for use as a toll device. The basic patent filed by Mario Cardullo covers the use of RF, sound and light as transmission media.

An early demonstration of reflected power (modulated backscatter) RFID tags, both passive and semi-passive, was performed by Steven Depp, Alfred Koelle, and Robert Freyman at the Los Alamos National Laboratory in 1973. The portable system operated at 915 MHz and used 12-bit tags. This technique is used by the majority of today's UHFID and microwave RFID tags. The first patent to be associated with the abbreviation RFID was granted to Charles Walton in 1983.

The largest passive RFID deployment is the enterprise-wide deployment performed by WalMart which installed over 25,000 reader systems at over 2800 retail stores.

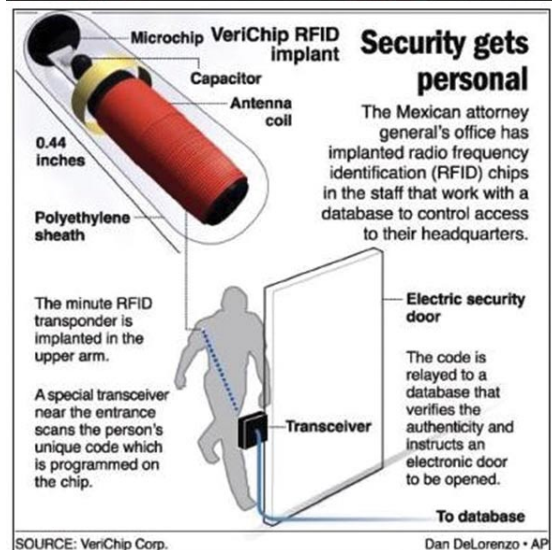
The largest deployment of active RFID is the US Department of Defense use of Savi active tags on every one of its more than a million shipping containers that travel outside of the continental United States. (Source: Wikipedia)

Security and Privacy Concerns

Here's a real-world scenario: You're a successful executive at a large software company. You're about to be robbed but it won't be through cyber-crime or zero-day malware exploiting CVEs, as I usually write about. As you walk into your local Starbucks to pick up your favorite cup of coffee, a young man bumps into you, says excuse me and heads to his car with his cup of coffee. Next thing you know, while you're out having coffee, this young man has actually cloned your RFID card for building access and access to your office. Within minutes, he's been in the building, in your office

and stealing everything he needs without tripping off any alarms. Could this actually happen to you? Yes. It's called RFID CLONING and it's easy.

This is why I always argue for two or even three factor authentication. By needing not only your badge but a secret combination, or your biometrics such as a



Thu Jul 15, 9:33 AM ET



Figure 2. Authentication Options – Black Box Intellipass or VeriChip Human Implants

fingerprint or retina scan, then this hacker would have been stopped at the front door. Take a look at Black Box Corporation's new product for both Data Center cages and for the front door – it's called Intellipass and it does just what I'm suggesting (See: <http://www.blackbox.com/go/intellipass>).

Is RFID the Orwellian Nightmare Come True?

PositiveID has been attempting to convince everyone that they need to be VeriChipped. They claim it will help speed patients through hospitals, executives through secured access and consumers through grocery and retail outlets.

Governments are forcing employees to be chipped just to keep their job. For example, the Mexican Attorney General's office requires all employees to be 'veri-chipped' for access to their offices.

Just this month, PositiveID announced that it has completed development of its RFID glucose-sensing microchip, GlucoChip, which will accurately measure glucose levels in individuals with diabetes. The lab tested a stable and reproducible closed cycle, continuous glucose sensing system that functions in the human blood fractions that are relevant to glucose sensing in the human body. According to the 2011 National Diabetes Fact Sheet, more than 25 million children and adults in the U.S. have diabetes, or over 8 % of the population. GlucoChip is FDA cleared and based on PositiveID's VeriChip microchip used for patient identification. The embedded bio-sensor system utilizes RFID technology and includes a remote transponder in wireless communication with an implantable passively-powered on-chip transponder. The company believes the measurement of glucose levels through this system will allow individuals with diabetes to monitor glucose levels in a less invasive manner.

The ultimate question is this – who benefits the most if we are all chipped. One could argue that the Globalists who control the banking infrastructures of

the world will gain the control they want over all of us – maybe it's a conspiracy, maybe not – but here's the theory – you get chipped, your money supply goes electronic. One day, if you do something someone doesn't like, instead of being added to a *no fly* list, like the new TSA control grid in the USA over air travel, your chip no longer has any access to your money – it gets electronically locked up for some reason...is it possible? If you let yourself be chipped, the answer is yes. Some religious factions call human barcoding and human RFID chipping the *mark of the beast* – there's a real heated debate here way beyond what I want to discuss in Hakin9 Magazine but the privacy concerns are as big, maybe bigger than the security concerns.

Key Privacy Issues

Without bringing these issues to the forefront, then the Orwellian *Big Brother* watching you system will be in place. We've tolerated cameras on every street corner, arguments globally for *national ID* cards and now the RFID technology can and will enable additional losses of privacy, potentially in the name of *Homeland Security* or for retailers, in the name of *Commerce*. Merchants must be prohibited from forcing or coercing customers into accepting live or dormant RFID tags in the products they buy. There should be no prohibition on individuals to detect RFID tags and readers and disable tags on items in their possession. RFID must not be used to track individuals absent informed and written consent of the data subject. Human tracking is inappropriate, either directly or indirectly, through clothing, consumer goods, or other items. RFID should never be employed in a fashion to eliminate or reduce anonymity. For instance, RFID should not be incorporated into currency.

While there are beneficial uses of RFID, some attributes of the technology could be deployed in ways that threaten privacy and civil liberties:

RFID tags can be embedded on objects and documents without the knowledge of the individual who obtains those items. As radio waves travel easily and silently through fabric, plastic, and other materials, it is possible to read RFID tags sewn into clothing or affixed to objects contained in purses, shopping bags, suitcases, and more.

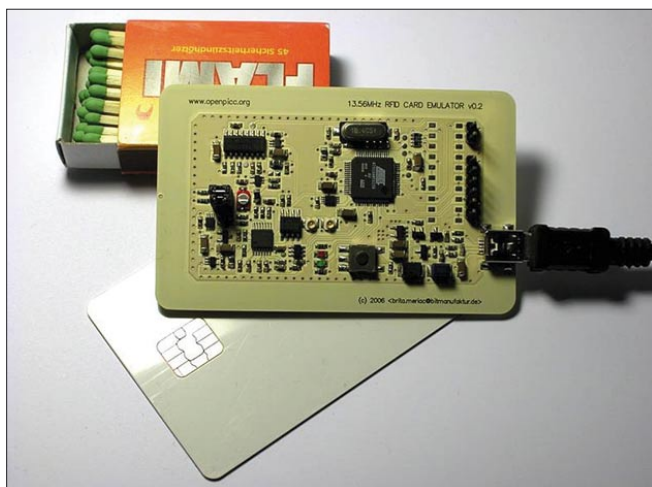


Figure 3. RFID Hacker Toolkit – Card Simulator



Figure 4. RFID Protection – ID Stronghold Card Sleeve

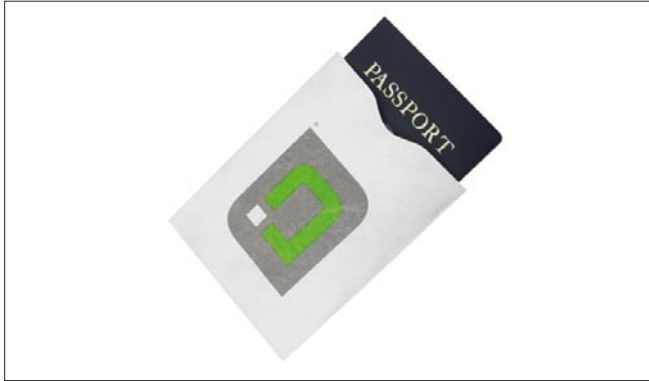


Figure 5. RFID Protection – ID Stronhold Passport Sleeve

Unique identifiers for all objects worldwide. The Electronic Product Code potentially enables every object on earth to have its own unique ID. The use of unique ID numbers could lead to the creation of a global item registration system in which every physical object is identified and linked to its purchaser or owner at the point of sale or transfer.

Massive data aggregation. RFID deployment requires the creation of massive databases containing unique tag data. These records could be linked with personal identifying data, especially as computer memory and processing capacities expand.

Hidden readers. Tags can be read from a distance, not restricted to line of sight, by readers that can be incorporated invisibly into nearly any environment where human beings or items congregate. RFID readers have already been experimentally embedded into floor tiles, woven into carpeting and floor mats, hidden in doorways, and seamlessly incorporated into retail shelving and counters, making it virtually impossible for a consumer to know when or if he or she was being scanned.

Individual tracking and profiling. If personal identity were linked with unique RFID tag numbers, individuals could be profiled and tracked without their knowledge or consent. For example, a tag embedded in a shoe could serve as a de facto identifier for the person wearing it. Even if item-level information remains generic, identifying items people wear or carry could associate them with, for example, particular events like political rallies. (Source: PrivacyRights.org – see <https://www.privacyrights.org/ar/RFIDposition.htm>)

Hacking RFID

The RFID chip in a credit card emits the account number, expiration data and other information. About 100 million credit cards now have this technology embedded into them. However, over the next 2-3 years, it is expected that credit card issuers will replace every single magnetic stripe credit and debit card with a new contactless smartcard, and why shouldn't they? The new cards seem to make it all easier. So much easier that some folks are reading your credit cards before you even take them out of your wallet. Those folks are called identity thieves, and the unfortunate truth is that RFID technology has made identity theft quite literally a stroll in the park. Where credit card *Skimming* used to require the thief to get his hands on your card, acquiring your personal data is now as easy as passing you on the street.

The bootable Live RFID Hacking System contains a ready-to-use set of hacking tools for breaking and analyzing MIFARE Classic RFID cards and other well known card formats. It is built around PCSC-lite, the CCID free software driver and libnfc that gives you access to some of the most common RFID readers.

To learn more about this RFID hacking tool, visit the website, here: http://www.openpcd.org/Live_RFID_Hacking_System.



Figure 6. RFID Protection – Wrap Your Wallet in Aluminum Foil



Figure 7. RFID Protection – Wrap your Passport in Aluminum Foil

Another project is called *The OpenPICC project* for *Proximity Integrated Circuit Cards* (PICC) and is the counterpart to OpenPCD. It is a device that emulates 13.56MHz based RFID transponders/smartcards. OpenPICC can be used to e.g. simulate ISO 14443 or ISO 15693 transponders, such as those being used in biometric passports and FIFA worldcup tickets.

To learn more about this RFID hacking tool, visit the website, here: http://www.openpcd.org/OpenPICC_RFID_Emulator_and_Sniffer_Project.

Another RFID hacking utility is called RFDump. It is a backend GPL tool to directly interoperate with any RFID ISO-Reader to make the contents stored on RFID tags accessible. This makes the following types of audits possible:

- Test robustness of data-structures on the reader and the backend-application
- Proof-of-concept manipulations of RFID tag contents
- Clone/copy & paste User-Data stored on RFID tags
- Audit tag-security features

To learn more about this RFID hacking tool, visit the website, here: <http://www.rf-dump.org/>.

Defending RFID

One company, ID Stronghold, has created a patented Secure Badgeholder® and patent pending Secure Sleeve® and Secure Wallets, which are designed to shield all contactless credit cards, passports, drivers licenses, ISO 14443A/B and EPC Gen1/Gen2 contactless smart cards; any contactless card that operates at 13.56 Mhz and above. It does not shield

non-smart cards (older 125khz proximity cards). On cards that include a secondary 125 khz antenna added for backward compatibility only the new 13.56 Mhz interface is shielded. The 13.56 Mhz interface is generally the only one with personal data.

To learn more about ID Stronghold's products, visit them online at <http://www.idstronghold.com>.

My favorite method for real hackers is real simple – wrap your cards in Aluminum foil for the same results – you could wrap the inside of your wallet with this foil for the cost of a few cents.

To learn how to do this on your own, visit this website: <http://www.i-hacked.com/index.php?option=content&task=view&id=208>.

Conclusion

Like all other identity management technologies, RFID is powerful and enabling. This wireless technology is used to share data through radio waves. With RFID, you can transfer data between a reader and an electronic tag attached to an object for the purpose of identification and tracking. However, there is an immeasurable amount of risk when using wireless technologies. It can be used for eavesdropping, tracking, stealing identities and so much more. With great power comes great responsibility – so if you are deploying RFID, you need to consider both security and privacy issues.

For Privacy rights, you should consider RFID technology and its implementation in a way that is guided by strong principles of *fair information practices* (FIPs). The eight-part Privacy Guidelines of the *Organisation for Economic Co-operation and Development* (OECD) provides a useful model (See: <http://www.oecd.org>). In addition, for Security consider multiple factors of authentication, where RFID is only one of these methods. Make sure you and your personnel understand the risks of eavesdropping on passive RFID such as access id cards, company credit cards and passports – especially for those employees who travel frequently.

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine and a frequent contributor to NetworkWorld, CIO Magazine, SearchCIO and others. He is also a frequent speaker at network security events and trade shows throughout the globe. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at <http://www.netclarity.net>. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org and a CISSP®. Miliefsky is a Founding Member of the US Department of Homeland Security (<http://www.DHS.gov>), serves on the advisory board of MITRE on the CVE Program (<http://CVE.mitre.org>) and is a founding Board member of the National Information Security Group (<http://www.NAISG.org>).

RFID in Defense and Security

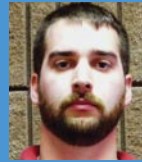
Nov. 15, 2011 Doubletree Hotel Crystal City—National Airport, Arlington, Va.

**LEARN HOW
DEFENSE
COMPANIES ARE
USING RFID TO
IMPROVE SECURITY,
STREAMLINE
PROCESSES AND
CUT COSTS**

HEAR FROM THESE AND
OTHER INDUSTRY LEADERS:



Paul
Hunter



Jeremy
Mercer



David
Blackford



Ismail
Uysal,
Ph.D.



BY ATTENDING THIS EVENT, YOU WILL:

- › Hear real-world case studies from leaders in defense
- › See the latest RFID technology solutions
- › Better manage your supply chain
- › Increase the security of shipments
- › And so much more!

HAKIN9 MAGAZINE VIP DISCOUNT:

SAVE 15% OFF RFID IN DEFENSE AND SECURITY—USE PROMO CODE AWAY
FOR MORE INFORMATION, VISIT www.rfidjournalevents.com/defense.

Passive RFID Tag Security:

Electronic Product Code, E-Passport and Contactless Credit Card

Because on their impact on the applications, security vulnerabilities of RFID tag technologies, when they are uncovered, easily draw media attention. The wireless security and access control of some key recent RFID-based technologies have been, although, interestingly designed.

What you will learn...

- what three key RFID-based applications are doing to secure their wireless communications and chip access.

What you should know...

- basic computer and network security.

What is a *Radio Frequency Identification* (RFID) tag? It is an electronic wireless technology for automated identification of objects, animals and people. Most impressive is the physical size of the technology. At the core of every paper thin RFID tag is a tiny integrated circuit, of a few millimeters on the side, containing a processor, memory and a transceiver. A RFID tag can be non self-powered or self-powered. A non self-powered, or passive, RFID tag gets its energy, to activate its circuitry, from the electromagnetic field produced by a reader accessing it. The captured electromagnetic energy is converted into electricity by the antenna of the tag. The wireless link between a reader and a tag can use spectrum in the *Low Frequency* (LF) range (124 to 135 KHz), *High Frequency* (HF) range (13.56 MHz) or *Ultra High Frequency* (UHF) range (868 MHz in Europe, 915 MHz in North America or 950 MHz in Japan). Hence, direct contact between a reader and a tag is not required. The workable separation distance varies from a few centimeters (with LF and HF) to a few meters (with UHF). A HF RFID reader and a few tags are pictured in Figure 1. Applications of passive RFID tags include inventory tracking (e.g., library, supply chain), electronic passports, contactless credit cards and office keys.

Self-powered RFID tags, or active tags, have their own internal source of energy. Workable distances are much longer than for passive tags, i.e., several tens of meters. They are well suited for automatically

taking tolls on highways. Active tags are more costly to produce than passive tags, by a factor of hundred. Note that longer workable distance doesn't mean better for all applications. For instance at the gas station, you don't want to be billed for the fill-up of your neighbor because you *smart* payment card happened to be in range of the reader. Short range RFID is best suited for that type of applications. On the other hand, long range RFID scans highly shelved items without the need to climb.

The RFID concept has effectively been implemented in several different incompatible ways by various manufactures. RFID systems could be proprietary. For the sake of interoperability between different

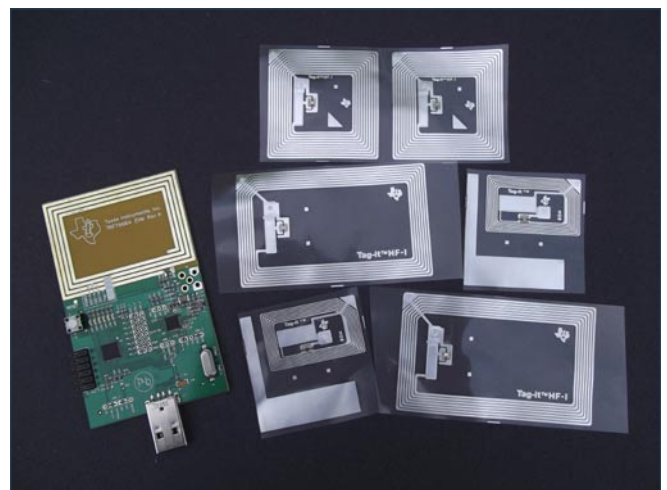


Figure 1. A RFID reader and tags

manufacturer products, notable standardization efforts include *Electronic Product Code* (EPC), e-passport and *Europay MasterCard Visa* (EMV) contactless credit cards. EPC is aiming to replace barcodes, e-passport, the passport with optically readable data and EMV contactless credit card, the magnetic stripe credit card.

Discovery of new security vulnerabilities in the design of RFID systems instantly grabs media attention because of the potentially affected large number of users. On the one hand, because of their low cost and limited hardware capabilities, security in RFID tags had been often absent or minimal. On the other hand, users of RFID applications expect confidentiality, integrity and authentication of communications between readers and tags.

In this feature, we focus the attention on the security of the communications between RFID readers and passive tags in EPC, e-passport and EMV contactless credit card applications. We review the security mechanisms that have been recently implemented and their vulnerabilities. This feature has been prepared solely using literature available from the public domain.

Electronic Product Code

EPC is a standardized technology developed by EPCglobal Inc. EPC is a realization of the concept of *Internet of Things*. Objects with RFID tags have presence on the Internet. EPC is a system for connecting objects with related information and organizations. Readers

get the identity of tagged objects. Using the identity, a lookup service is accessed to obtain associated information, such as a description of the tagged object and its manufacturer.

For keeping the cost low (i.e., a few cents per tag), each tag stores a 96-bit identifier, which is used as a key to access detailed information from databases, i.e., the EPCglobal Network. EPC aims at replacing the barcode technology with a more efficient system. A barcode determines a product type. In contrast, an EPC RFID tag determines a product type and contains a unique product serial number. That means that information about a product can be retrieved as well as the history of a particular exemplar of that product. EPC RFID tags also read faster than barcodes. Line-of-sight with the reader is not required. Several tags are simultaneously readable. We hereafter focus on the reader-to-RFID tag interaction, in particular the for EPC UHF Class 1 Generation 2 tags. The reading and writing procedures are matter for consideration.

The reading protocol is depicted in Figure 2. The reader sends an inventory query to power and activate the tag. The tag generates, stores in memory and returns a 16-bit random number (RN16). The next transmission of the reader is an acknowledgement (ACK) loaded with a copy of RN16. Upon reception of the ACK with a RN16 matching the one stored in memory, the tag transmits its EPC.

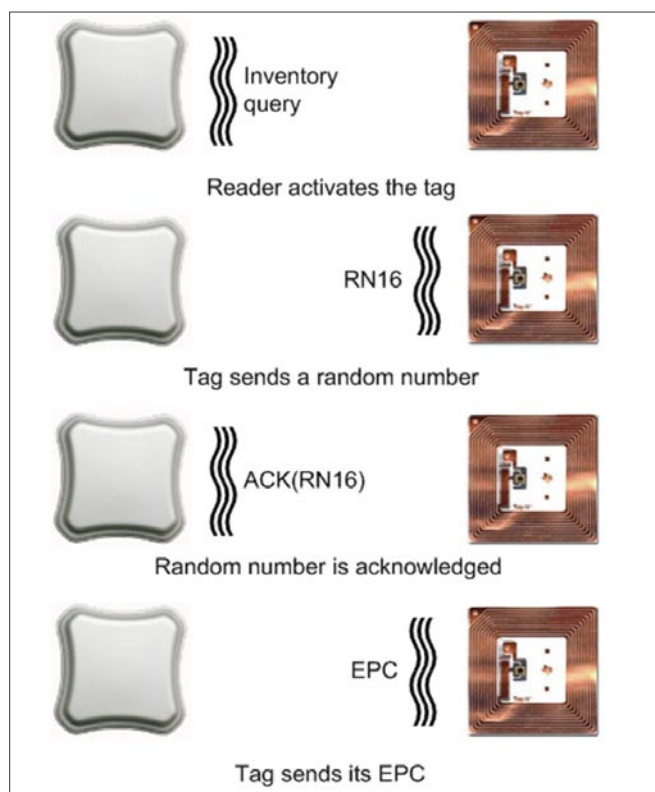


Figure 2. Reading protocol of an EPC Gen2 tag

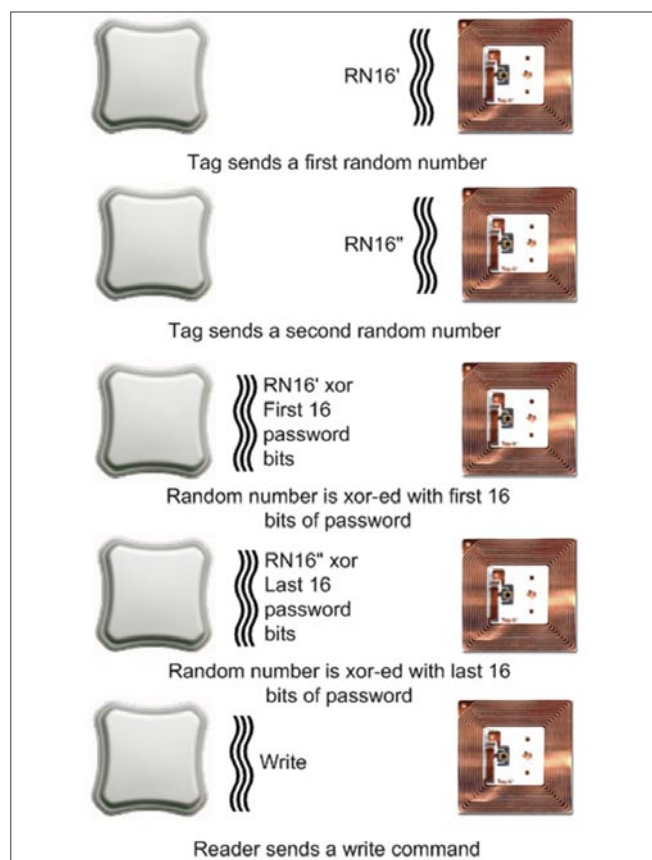


Figure 3. Writing procedure of EPC Gen2 tags

In this context, desirable but non-present security properties are message confidentiality, integrity protection, origin authentication and replay protection. *Confidentiality* is keeping secret to a source and a destination the content of their message. *Integrity protection* intends to provide to a destination assurance that a message has not been altered during its transmission. *Message origin authentication* means that the destination receives assurance of the identity of the source. Replay protection forces the origin of a message to demonstrate to the recipient that the message is new and is not a retransmission of a previously sent message.

The random number-based handshake is a pairing technique, but not a security mechanism. Eavesdropping of signals and interception of EPCs are possible. A lookup service may be accessed to gain further information about the tagged objects. The EPCs can also be used for counterfeiting and creating clones of the original objects. Location tracking and surveillance of objects are also possible. The absence of message origin authentication enables scanning attacks.

Every EPC Gen2 tag is write-protected by a 32-bit password. Writing must be preceded by a successful inventory query. The write procedure is illustrated in Figure 3. Two new 16-bit random numbers, RN16' and RN16'', are generated and sent to the reader by the tag. Afterwards, the reader must prove ownership of the 32-bit password to the tag. The reader sends the password into two separate segments of 16 bits. The first transmission is scrambled by xor-ing the first 16 bits of the password with RN16'. The second part is obfuscated by xor-ing the last 16 bits of the password with RN16''. The reader can then send the write command to the tag. Writing can also be permanently disabled.

Because of the mathematical properties of the xor operation, i.e., $(a \text{ xor } b) \text{ xor } b = a$, an eavesdropper who successfully intercepts RN16', RN16'' and the two obfuscated password transmissions can retrieve the password. There are neither theoretical difficulties nor complex problems to solve. The feasibility of the attack has already been demonstrated. An adversary



Figure 4. The e-passport (note the e-passport symbol at the bottom)

can intercept the password and reuse it to rewrite a tag with its own data. Note also that this rudimentary form of authentication is asymmetric. The reader password ownership is verified, but not the tag.

A reader can command a tag self-destruction operation. The protocol is very similar to the write procedure. It is guarded by the 32-bit password that is sent scrambled into two segments using two 16-bit random numbers. The protocol is equally vulnerable to eavesdropping attacks.

E-Passport

US, Canada and several other countries have or are about to adopt the electronic passport (e-passport). The e-passport is HF RFID tag-based, see Figure 4. In every e-passport, a RFID tag stores the name, nationality, gender, date of birth, place of birth and portrait of the owner. The e-passport technology has been standardized by the *International Civil Aviation Organization* (ICAO) under the name *Machine Readable Travel Documents* (MRTD).

E-passports are using the ISO/IEC 14443 standard. It is an international standard for communicating with RFID devices at 13.56 MHz. The standard covers four aspects: physical characteristics (e.g., device size), radio frequency power and signal interface (e.g., modulation and coding), initialization and anti collision (e.g., frame format, device activation procedure, device identification procedure) and transmission protocol (i.e., activation and deactivation of data transfer). The ISO/IEC 14443 standard does not define the data transfer protocols, other than their activation and deactivation.

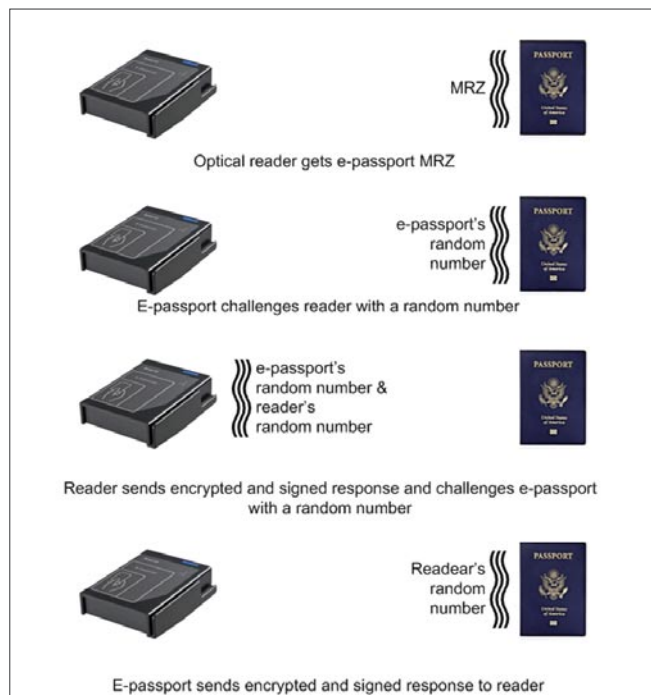


Figure 5. BAC mutual authentication and session key establishment

For situations requiring data protection, it has to be supplemented with application specific security protocols.

The MRTD *Basic Access Control* (BAC) protocol establishes a secure channel between a reader and an e-passport RFID tag. Data transfer is protected with Triple-DES encryption. Symmetric keys, for data confidentiality and integrity protection are generated. They are derived using the *Machine Readable Zone* (MRZ), which are two lines of characters at the bottom of the passport data page that holds the portrait of the owner. They contain the passport number, owner's date of birth and passport expiry date.

The BAC is a two-phase procedure, see Figure 5. The reader has combined optical reading and wireless communications capabilities. An e-passport is not readable unless opened. In a first phase, an optical reader obtains the MRZ of the opened e-passport. Then, a RFID reader accesses the electronic content of the passport. The content consists at least of the MRZ and photograph, which resolution may be higher than the printed one. It may also contain fingerprints and iris biometrics.

In the second phase, the reader and e-passport demonstrate to each other that they own the MRZ. The MRZ is not sent over the air. A challenge and response protocol, with encryption and digital signature, is used. The MRZ plays the role of seed for secret symmetric key derivation. It is used on each side as an input to a one-way hash function, i.e., SHA-1, that outputs an encryption (K_e) and a *Message Authentication Code* (MAC) computation key (K_m). The e-passport sends to the reader a new random number. The reader returns the same value as a response to the tag, encrypted and signed using Triple-DES, K_e and K_m . The response is accompanied with a new reader's random number. If the first received random number matches the value sent to the reader, then the reader is authenticated and authorized by the tag. The tag also calculates a response that is returned to the reader as the reader's random number encrypted and signed using Triple-DES, K_e and K_m . The reader does verify the response, i.e., it must match the random number that was sent. At the end of a successful authorization procedure, the same symmetric session encryption key and session MAC computation key are derived on each side, using SHA-1 and another pair of random numbers exchanged during the BAC. They session keys are used to protect the confidentiality and integrity of the data traffic between the tag and reader.

The protocol can be attacked by first intercepting the RF communications then running an offline dictionary attack. An eavesdropper may intercept the signal between a legitimate reader and an e-passport tag.

The digital data is encrypted. To decrypt the data, the adversary has to generate and try key seeds, i.e., possible MRZ values, one by one until it hits the right one. Since MRZs are not totally random and are constructed from people names and dates, a dictionary of names that can be tried first may help to reduce the search space. Again, adversaries don't have to go through theoretical problems that are complex and difficult to solve. Lab demonstrations have been able to run successful dictionary attacks in few hours. So far however, to the best of our knowledge the documented attacks are either fictional or have been done solely in lab environments. Because of the low power and short distance propagation of HF RFID signals, their interception *in the field* is not impossible in theory but challenging in practice. For instance, conditions for wave propagation are not ideal in an airport terminal environment.

Tampering the actual content of an e-passport is possible, but the challenge is to regenerate a valid *Public Key Infrastructure* (PKI) digital signature that matches the new content.

Contactless Credit Card

Contact versus Contactless Card

There are currently two kinds of smart credit card technologies: contact and contactless. Every *contact card* has an embedded three by five millimeters integrated circuit. The contact card is easily recognizable because of the connection pads placed middle left. They enable electronic access to the chip, see Figure 6. In itself, this technology is not RFID based, although it can be combined with it. Payment is done by inserting the card into a reader and entering a *Personal Identification Number* (PIN).

The *contactless* cards are HF RFID tag based. MasterCard PayPass and Visa payWave are contactless credit card systems. Such cards are distinguishable by the technology symbol printed on them, see Figure 7. Note that PayPass is not limited to contactless card applications. It is the system that has been adopted by Google wallet. Payment is done by tapping a card over a terminal, which embeds a RFID reader. Optionally, the type of transaction is selectable (credit or debit) and a PIN may be entered.



Figure 6. A contact smart card (note the contact pads placed middle left)

Contactless Card Security

Contactless credit cards are developed according to the ISO/IEC 14443 and EMV published standards. The adoption and use of standards in this context are important for interoperability and compatibility between systems of different payment card issuers. EMV defines the components of a payment system into four books. In regard to security, the books two and four, entitled *Security and Key Management* and *Application Specification*, are the most relevant. At the outset, it is interesting to note that every card issuer (e.g., Visa or MasterCard) may have its own payment application, determined by an Application IDentifier (AID). Look at your paper receipts; the AID may be printed at the bottom (e.g., A0000000031010 or A0000000041010). The PayPass contactless application is named M/Chip. The payWave application is *Visa Smart Debit/Credit* (VSDC). For greater interoperability, there is also the *Common Payment Application* (CPA) recognized by Visa, MasterCard, JCB and other payment card issuers. The actual application, which is used between a card and a terminal, is determined at the beginning of a transaction.

In spite of the existence of several payment applications with their own peculiarities, one can get a good idea of the kind of security contactless payment cards are using by reading the EMV books, two and four, and CPA specification. In fact, the CPA is a model of a family of payment applications. There are several implementation alternatives left open to make CPA general enough to suit different payment needs. The specification defines the peer-to-peer interface between a payment card and a terminal.

Figure 8 is a model of a payment application transaction as recommended by the CPA specification. Firstly, the terminal sends a SELECT command and chooses an application. The selection is according to the type of transaction and applications that are both supported by the terminal and card. Secondly, a transaction is initiated. The terminal pulls from the card, using READ RECORD commands and responses, the static data that is needed to process the transaction. There are several kinds of static data items. The exact static data pulled from the card depends on the actual type of transaction, e.g., payment versus PIN update.



Figure 7. A contactless smart card (note the payWave symbol, top left)

For a payment transaction, let us assume that the pulled static data includes at least the 16-digit *Primary Account Number* (PAN), i.e., the card number, PAN Sequence Number, which distinguishes cards that have the same PAN, and expiry date. A public key certificate, employed for the next step, is also part of the static data. Thirdly, the card static data is offline authenticated by the terminal. Offline authentication means that a back-end system of the card issuer is not involved in the process. There are three forms of authentication, which are discussed in more details in the sequel. The most complete form of authentication is accomplished using the GENERATE AC (Application Cryptogram) command and response. The terminal then independently checks if the static data verifies a number of restrictions, such as the validity of the card expiry date. Afterwards, the terminal confirms the legitimacy of the person holding the card. Choices of PIN-based methods are available. There are two offline methods, plain text or encrypted PIN, where the card does the actual validation. It stores a copy of the PIN and can determine the correctness of the PIN entered by the cardholder. It can also be done by contacting an online back-end system. Cardholder verification may also be omitted. PIN encryption for the offline case is described in more details in the sequel. For credit and fraud protection purposes, the terminal may contact an online back-end system to get a transaction authorization, either for high-value

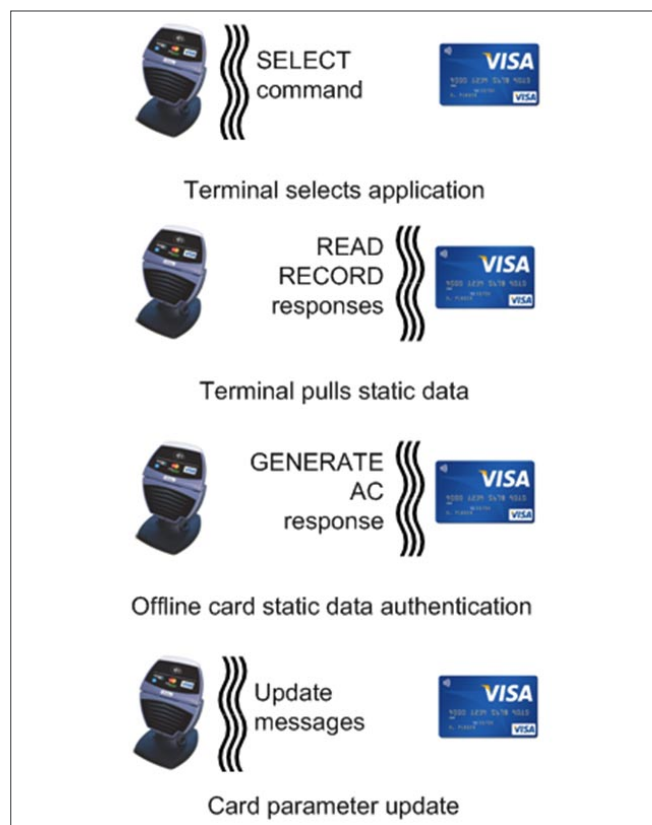


Figure 8. CPA model of a payment transaction

transactions or on a periodic basis. Consistency of the transaction with respect to non-static data stored in the card is also performed (e.g., an amount accumulator). Before completion of the transaction, the terminal may issue update messages to change data stored in the card, such as the PIN. These updates are sent using secure messaging, discussed in more details in the sequel.

Both encryption and authentication use a session key, valid for the duration of one transaction. The session key is derived from a *Master Key* (MK). Card static data authentication and derivation of the MK and session key, very important aspects in the security of contactless credit cards, are discussed hereafter.

Offline Static Data Authentication

Offline authentication signifies that the card issuer is not involved in the procedure. The forms of authentication that may be implemented by contactless payment cards are *Static Data Authentication* (SDA), *Dynamic Data Authentication* (DDA) and *Combined DDA/Application Cryptogram Generation* (CDA). SDA guarantees that the static data stored in a card has not been modified. DDA provides as SDA, confidence that the static data stored in a card has not been tampered plus assurance the card is not counterfeited. CDA provides the assuredness of DDA, plus certification that encrypted application data, transferred between the card and terminal, hasn't been changed.

Offline data authentication is done using RSA public key cryptography. The card stores and provides to the terminal an issuer public key certificate. With SDA, all the static data provided by the card to the terminal is signed using a one-way hash function and an issuer private

key. With DDA, the card is challenged to compute a hash value over the static data and two random values determined at the beginning of a transaction, one by the terminal, one by the card. This is to assure that the card has not been cloned from another card, through a skimming attack for instance. The card can't replay previous challenge responses and has to prove that it owns the issuer private key matching the issuer public key certificate. With, CDA the calculation of the one-way hash value is done over the dynamic data and application data.

PIN Encryption During Cardholder Verification

Cardholder verification consists of verifying a match between a PIN entered on the terminal by the person holding the card and the PIN stored in the card. For this verification to happen, the terminal needs to communicate the PIN to the card. It can be done using RSA encryption.

The PIN verification protocol is illustrated in Figure 9. Upon request, the card generates and sends to the terminal and eight-byte challenge random number. The terminal conceals the received random number and PIN together using a RSA recovery function and a PIN encryption public key. The cryptogram is sent to



Figure 9. PIN verification protocol

Acronyms

AC	Application Cryptogram
ACK	Acknowledgement
AID	Application Identifier
BAC	Basic Access Control
CDA	Combined DDA/Application Cryptogram Generation
CPA	Common Payment Application
DDA	Dynamic Data Authentication
DES	Data Encryption Standard
EMV	Europay MasterCard Visa
EPC	Electronic Product Code
Hz	Hertz
LF	Low Frequency
HF	High Frequency
ICAO	International Civil Aviation Organization
IEC	International Electrotechnical Commission
IMK	Issuer Master Key
ISO	International Organization for Standardization
RF	Radio Frequency
UHF	Ultra High Frequency
MAC	Message Authentication Code
MK	Master Key
MRTD	Machine Readable Travel Documents
MRZ	Machine Readable Zone
PAN	Primary Account Number
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RN16	16-bit random number
RSA	Rivest, Shamir, and Adleman
SDA	Static Data Authentication
SHA	Secure Hash Algorithm
VSDC	Visa Smart Debit/Credit

On the 'Net

- The web site RFID Security and Privacy Lounge references technical works on RFID security published in the literature: www.avoine.net/rfid.
- For information about the EPC tag technology and EPCglobal Network, including the standards, visit the following web site www.gs1.org/epcglobal.
- Information about the e-passport standards (MRTD) is available at the web site: www2.icao.int/en/MRTD.
- For information about EMV, i.e., the four-book standard, the contactless and CPA specifications, check out the web site: www.emvco.com.
- For technical documentation specific to PayPass go to paypass.com (some information available only to licensees).
- Technical information about PayWave can be obtained at partnetwork.visa.com/vpn/global/category.do?categoryId=28&documentId=57&userRegion=1 (some information available only to licensees).

the card in a VERIFY message. The card recovers the PIN and random number using a RSA signing function and PIN encryption private key. The recovered PIN must match the PIN stored in the card. The recovered random number must be equal to the one that was generated. The random number has a replay protection purpose, i.e., an adversary cannot replay a previously intercepted VERIFY message. The PIN encryption public key, part of the static card data, is signed using a card issuer private key.

Secure Messaging

Secure messaging is used to assure the confidentiality, integrity and authentication of five different types of commands that can be sent by a terminal to a card, that is, application unblock, PIN change, PIN unblock, put data and update record. They all update data stored in the card. Confidentiality is achieved using encryption, followed by the computation of a four-byte MAC for the sake of integrity and authentication. The MAC is meant to be a proof that the origin of a message is from a legitimate terminal. Message payload is encrypted and MAC is calculated using DES or Triple DES.

DES or Triple DES is used in conjunction with a session key valid for the duration of a single transaction. The session key is generated as the Triple DES encryption of a transaction counter, using the MK. The transaction counter makes the session key different from transaction to transaction.

The MK is 128-bit long. The method suggested by EMV uses the 16-digit PAN, PAN Sequence Number and 128-bit *Issuer Master Key* (IMK). In a nutshell, the MK is defined as the Triple DES encryption of the PAN and PAN Sequence Number, using the IMK. The PAN Sequence Number is not always available. When the case arises, a null value is used.

Conclusion

The highlights of the three RFID applications reviewed in this article are given in Table 1. It is interesting to note that the security of people identification and payment applications doesn't not rely solely on cryptographic techniques, but also on the RF characteristics of the devices and the environment they are meant to operate in.

The EPC reading protocol sends data in plain text. Interception of EPCs is possible. A lookup service may be accessed to retrieve further information. Enabled attacks include tag counterfeiting, location tracking and scanning. The writing and killing protocols are password protected. The reader sends to the tag the password scrambled using two random numbers and the xor operation. The interception of the random numbers and scrambled password and an application of the xor operation are all that is required to capture the password.

A secure channel is established to assure confidentiality and integrity of communications between an e-passport and a reader. Block cipher-based

Table 1. Summary of RFID application characteristics

	Technologies		
	EPC	E-Passport	Contactless Credit Card
Standard	EPCglobal Inc.	MRTD	EMV
Frequency	UHF (860-960 MHz)	HF (13.56 MHz)	HF (13.56 MHz)
Distance	10 m	10 cm	10 cm
Application	Supply chain	Border crossing people identification	Electronic payment
Security	Scrambled 32-bit password protected write/kill	- Mutual authentication - Encrypted traffic - Public key encryption signed content	- Card static data authentication - PIN encryption - Card update message confidentiality, integrity and authentication

encryption is used. Symmetric keys are established during mutual authentication using the optically read MRZ. Dictionary attacks are theoretically possible.

Static data pulled from a contactless credit card is sent plain text, according to the CPA model. The static data is signed using RSA public key cryptography. The terminal verifies the person holding the card and static data pulled from the card, but not the opposite. The card, however, does not authenticate the terminal. The PIN is sent from the terminal to the card encrypted using RSA public key cryptography. Static data authentication and PIN encryption are well designed. They both use asymmetric key cryptography. The public key of a card can be known by anyone. Recovering the corresponding card private key is, although, intractable.

Triple DES and session keys are used to encrypt and sign terminal messages that update card parameters. The messages trigger the operations *application unblock*, *PIN change or unblock*, *put data* and *update record*. They are encrypted and authenticated using a block cipher, i.e., symmetric key cryptography, which is considered to be strong. A 128-bit session key is renewed for each transaction. The session key is derived from a MK. The 128-bit MK is, in principle, long enough to make brute force attacks intractable. The PAN can be intercepted over the air, since it is sent plain text from the card to the terminal. Determined by the card issuer, the 128-bit IMK is shared by both the terminal (or a back-end system accessible by the terminal) and card. The search space is astronomical in size. The drawback of symmetric key cryptography is that any authenticator and any supplicant must know the IMK. Any insider device that has the IMK can impersonate a legitimate terminal and send commands to a card. Finally, since the security is not end-to-end, but terminal-to-card, attacks are possible by subverting terminals.

MICHEL BARBEAU

Michel Barbeau is a professor of Computer Science. He got a Bachelor, a Master's and a Ph.D., in Computer Science, from Universite de Sherbrooke, Canada ('85), for undergraduate studies, and Universite de Montreal, Canada ('87 & '91), for graduate studies. From '91 to '99, he was a professor at Universite de Sherbrooke, Canada. Since 2000, he works at Carleton University, Canada. He focuses his efforts on network and wireless security, vehicular communications, wireless access network management, ad hoc networks and RFID.

Join

hakin9 team!



If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

editors@hakin9.org

and give us a brief description of your field of interest.

We look forward to hearing from you!

The RFID and NFC Radio Frequency-Enabled Security Threat

A discussion on how radio frequency-enabled technology could leave people vulnerable to identity theft and then potential identity fraud. (Updated)

Identity theft and identity fraud is a growing business. The crime itself is very much still in its infancy in most countries in the world with the exception of the US, where it continues to be a major problem for both the general population and the authorities. So you will not be surprised to hear that from the US comes yet another type of identity theft called *non-contact identity theft* or what is sometimes referred to as *Wireless identity theft*.

Wireless identity theft is a relatively new type of identity theft that uses radio frequency to gather important personal information from someone's store, access control, credit, debit, passports or identity cards. There are two particular types of wireless identity theft which involve *Radio-frequency identification* or *RFID* and *NFC* (*Near Field Communication*) with the latter becoming very popular with recent smartphone developments.

Radio-frequency Identification and Near Field Communication

Radio-frequency identification (RFID) is an object (or TAG) that is incorporated into say a passport or debit/credit card that sends out radio waves for identification and tracking. Most RFID tags can only be read from several meters away – most can also be read from beyond the line of sight of the reader as well. The RFID tag contains two elements. The first element (circuit) is used for storing and processing information and the other is an antenna for receiving and transmitting the signal.

Near Field Communication (NFC) is a subset of RFID that limits the range of communication to within 10 centimeters or 4 inches. Objects that are tagged with NFC are usually passive because it does not require that much range. Some have even employed shielding

to further reduce the chance of other people being able to read the information. NFC is basically *cashing in on cashless*. NFC is expected to replace the cards in your wallet, discovering content on the go, using a smartphone as a content reader and so on. Consumer interest is expected to be rapid, but businesses might need greater incentives to adopt NFC. Cost and security are two prime issues right now.

RFID Tags

RFID tags come in three distinct types. The first type contains a small battery that can transmit signals autonomously; the second type is called passive RFID tags – these have no battery and need an external device to activate a signal handshake. The third type is a battery assisted passive RFID which requires an external device to activate (wake up). The last type has a greater range.

FACT

RFID active tags have been used on more than a million shipping containers that travel outside of the United States. (US Department of Defense) – 2007

RFID technology is developing rapidly, however there are some obvious engineering limitations. RFID technology is miniaturizing as the technology advances, but the advances appear to be currently limited to the radio frequencies available. The antennas themselves are difficult to attach, which in turn limits the reading range. There are new developments in this area which look to overcome these technical difficulties most notably photovoltaic components, but this is some way off. So what about NFC technology?

NFC Technology Use

In the UK, the London Oyster card already uses NFC and many VISA cards use NFC and most people don't even know it. NFC technology lets consumers pay for items by passing their smartphone over a small reader. The NFC chip would be able to hold a consumer's bank account information, gift cards, loyalty cards and coupons.

Google is one reputable company that is leading the way with NFC. Google Wallet is available via a mobile app. Users will need to set up the service by affiliating their GWallets with a Google account, creating a PIN code and then adding a credit card to the account. A security company called First Data will vet and approve the cards. Once activated, spending privileges are activated for each and every card. Shoppers will need to *tap and go* on their smartphones to be able to use GWallets. The system cannot work without the support of retailers who will need to offer PayPass checkouts. To date (June 2011) 120,000+ retailers have signed up in more than 300,000 locations.

A number of smartphone devices with the NFC feature have started to appear including the Google Nexus S and BlackBerry 9900 and there appears to be strong rumors that NFC might be built into the iPhone 5, tablets and other devices. The market could be worth \$670 billion (L420 billion) by 2015 claimed Juniper Research report (June 2011). *

Statistic: Worldwide NFC transactions will near \$50 billion by 2014.

Reference: Juniper Research report, June 2011

Western Europe is among the top three regions contributing to this growth and will account for 75 per cent of gross mobile payment transaction value in 2015. North America and the Far East and China will sit alongside Western Europe in making up this dominant figure. Contactless payments, mobile ticketing and transfers will become much more the norm in both developing and developed countries, helping to fuel the growth, according to Juniper.



Figure 1. Example: UK Biometric Passport with computer chip

RFID Technology Use

RFID technology use is without doubt on the increase within industry, in particular the financial industry – where it is used in debit and credit cards. There are several good reasons why business is looking at this technology. One of which is decreased cost of the RFID devices and tags, increased performance and a stable international standard. A number of industries are looking to RFID technology for asset tracking. It is this last point of *tracking* that provokes widespread alarm bells in privacy circles.

With RFID becoming more and more prevalent in everyday life, most people will be unaware of the impact that this technology has on their lives. One particular RFID technology use is with *Biometric Passports*. Most citizens of a country will have one, especially if they want to travel. The Passport is one of the most important *identities* an individual can ever have.

Biometric Passports

The biometric passport is simply a paper document that contains biometric electronic information that can be used to identify travellers. All biometric passports use contactless smart card technology (which uses a computer chip – see Figure 1) and antenna for both computer chip power and hand shaking with a device.

The computer chip (can be seen at the bottom right on the Passport image above) contains exactly the same personal information that is found on the same page as the individual's personal information. Below (Table 1) is an example of the data stored on a UK Biometric Passport.

All biometric passports use a PKI to authenticate the personal data stored on the passport smart card. Authorities claim that the PKI used cannot be broken. The biometrics used for identification includes facial, fingerprint and iris recognition. Each computer chip stores a JPEG or JPEG2000 format image of one of the above identification options. Every time you cross borders a biometric comparison is performed by e-border systems.

Biometric Passport Security Issues

The biometric passport has been designed to have non-traceable computer chip characteristics as well as a number of preventative technologies including *Passive Authentication (PA)* and *Active Authentication (AA)*

Table 1. Personal data encrypted in biometric passport

Passport Type	Date of Birth
Country Code	Sex type
Passport Number	Place of Birth
Surname	Valid from to dates
First and middle names	Country of Authority
Nationality	Signature

just to name a few. The real issue with PA is that not all border systems appear to check the cryptographic signature on a passport computer chip. AA also appears to have problems with security, mainly concerning a hacker's ability to alter the anti-cloning mechanism functionality. By altering this functionality it would be possible to be in two places at once.

In March of this year a security expert in the UK claimed to siphon data off an RFID chip from a passport in a sealed envelope, but the UK Home Office maintains that even if a biometric passport is cloned, airport scanners will pick up a fake chip. However, some experts claim that although British airport scanners have the technology to identify chips which are not genuine, those in other countries do not.

Non-contact Technology

One of the main concerns with non-contact technology (RFID and NFC included) is the ability to have your information swiped from your passport or card without you ever knowing. The same problems exist with Bluetooth technology but the Bluetooth security issue has been handled by offering a *passkey*. The Passkey is an encrypted password – normally four digits which allow the user to accept or deny a communication with another Bluetooth enabled device. Unfortunately, this process is likely to never appear on passports or credit or debit cards.

The RF enabled Cards Threat

RF enabled cards (whether they be store, debit or credit cards) allow organisations and retail outlets for example to learn more about their customers. They provide valuable personal data as well as collect profile data on customer behaviour both from what an individual purchases to tracking their every movement.

The RFI chip responds to certain radio frequencies. When an individual's tag comes into contact with these radio frequencies there is a handshake and the data is parsed. There is an opportunity here to harvest the sensitive data in which a hacker or identity thief could program their own cards using already well documented cloning techniques. Websites can easily be found which supply the necessary tools and software to commit *non-contact identity theft*.

NFC security issues – case story: Google Wallet

Google Wallet uses something called *Secure Element*. A user's data is protected and saved away from the main operating system and hardware, so if anyone who attempts to find a way into your device will not be able to access it. At the users level the NFC chip/antenna turns off when the phone screen is black. The protocol also uses a PIN code for transactions which are also further

protected by settings that prohibit transactions without the app being launched. This appears very secure, but is it?

Google Wallet is an *android* app – this is an open source community (think Marketplace) and given recent Android app malware exploits, you'd be hard pressed to find a good reason why consumers will *trust* Google Wallet at all. The back-end of processing and storage of credit card data is protected by the PCI-DSS (*Payment Card Industry Data Security Standards*) – so this isn't the security weakness.

Android smartphones have a separate chip that stores the sensitive card data, which is encrypted and the chip is tamper proof. But then what comes is the real weak link – the Android app (as mentioned above). All you have to do to open the app is remember a PIN – how many people uses *1234* or *6789* or something like a data of birth? **Update:** Google say they have developed *password logic* whereby they will detect and reject obvious weak passwords i.e. *1234*. If the Google Wallet becomes widely adopted, then there are some security researchers who wonder whether Google will retain the PIN. If the PIN was abandoned then this would open a whole new can of worms (pun was unintentional).

What if Android malware writers could spoof the Google Wallet? It's possible once you have access say via the PIN to access the data and reverse engineer the Google Wallet app to extract the key. Creating a malicious app that emulates the Wallet app to fool the secure element chip to give up the user credentials is possible. The attacker can then collect information for sale or for attempts at cloning the data to new NFC assets.

RFID Applications

The financial industry has been very active in the RFID market. In the US, most of the debit and credit card providers are migrating away from swipe cards – mainly due to the time it takes to complete a transaction – to the more speedy RFID tagged transaction process. The RFID issuing organisations dispute the RFID identity theft threat. So why have some cards had individuals names and other data removed by some credit card companies? Various white-hat hackers believe RFID is not safe and have produced reports to prove it.

Credit and Debit Card RFID Technology

In the US millions of contactless credit cards have been received – in fact some 250 million Americans have RFID technology. The RFID technology associated with credit and debit cards can never be switched off. The idea behind the RFID is that you don't have to hand over your card. All you do is, wave your card in front of a scanner and that's that. A particularly good method of protecting your RFID privacy is to purchase RFID-blocking sleeves for your contactless cards or use just aluminium foil to block the radio waves.

The continuing RFID threat may well be a problem especially given the cyber security issues that we read about concerning stolen financial records and identity theft. Admittedly there has been no identity theft or cyber crime committed using RFID – not just yet. Most of the threats have been developed in controlled environments using proof-of-concept which demonstrates the supposed RFID vulnerabilities. There does appear a concerted effort to provide high level encryption to RFID contactless technology – but the real question of *has anyone had their data or identity stolen yet?* is something that might happen in the future. Why discount it?

The Malware and DDoS Threat

Consider the number of malware (computer worms and viruses) that are being constantly developed in the online world. Some attempt to steal your personal and financial data; others serve no purpose other than to destroy your PC or data. When computers first appeared it took years for the first virus to appear. If you were to put the clock back – one wonders what foresight would have given us – it wouldn't have given us one of the biggest industries in the world – internet security!

RFID Car Immobilizers

Ever wondered how your car automobile immobilizers work? Well, the car key uses RFID. The immobilizer has a chip in the key which is encrypted which sends an RF wave to the car to open or lock the car including the immobilizer. As yet there is no real purpose for hacking into a car but given the amount of computer technology that is being built into cars – one day hackers will have a reason to crack into a car (using Bluetooth, RFID or Satellite) maybe to stop your car from working (similar to a DDoS attack).

You can actually purchase a \$50 kit from the internet that will read 125-Khz RFID chips. The kit includes; open source software for reading, storing and re-transmitting card data and decoding software. The decoding software decodes the RFID encryption used in car keys for several car models. This would allow a hacker to scan an unsuspecting car-owners' key, decrypt and the data and open the car.

Mitigating the RFID Security Risk

The real security risk for RFID is mainly the opportunity to steal the data as to date no one hacker has admitted to being able to hack an RFID system or crack an RFID card. For individual users of RFID, solid tag and system data security should actually address the privacy concerns while at the same time allowing for greater efficiency and enhanced security.

If you want to understand more about RFID technology and the obvious threats, then you only need to visit the *Communications of the Association Machinery (CAM)*.



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.

[IT'S IN YOUR PULSE]

LEARN:

Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering

Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Games and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

Have a read of this:

For successful data retrieval the perpetrator's antenna must catch two different interactions: the forward channel, which is the signal being sent from the RFID reader to the RFID token; and the backward channel, which is the data being sent back from the RFID token to the RFID reader. . . .

. . . the perpetrator would need only an antenna and an amplifier to boost the signal capture, a radio-frequency mixer and filter, and a computer to store the data. The amplifier itself would not even need to be that powerful, since it would need to boost the signal over only a short distance of three to five meters. . . . These RFID "sniffers" can then be plugged into a laptop via a USB port.

The 52-bit encryption key can be easily broken, so one can only be baffled as to why the CAM has made the above statement. Some experts are perplexed as to why 3D barcodes are not used as they can safely store data which is hard to crack.

Last year at DefCon NSA intelligence officers were gathering – what they didn't know what that an RFID scanner was searching for them also using a wireless Bluetooth webcam, which also took their picture. The RFID reader sniffed data from their RFID-enabled ID cards and other documents they were carrying in their backpacks and pockets. Obviously no crime was committed. The project was only to raise awareness.

The Department of Commerce's *National Institute of Standards and Technology* (NIST) in the US is leading the way on RFID security. It understands the risks and has highlighted specific recommendations. Its list of recommended practices for ensuring the security and privacy of RFID systems includes:

- firewalls that separate RFID databases from an organization's other databases and information technology (IT) systems;
- encryption of radio signals when feasible;
- authentication of approved users of RFID systems;
- shielding RFID tags or tag reading areas with metal screens or films to prevent unauthorized access;
- audit procedures, logging and time stamping to help in detecting security breaches; and
- tag disposal and recycling procedures that permanently disable or destroy sensitive data.

NIST will no doubt play a significant role in determining RFID standards for organisations and manufacturers from now and into the future.

Government and Business RFID Strategies

As yet there doesn't appear to be any plans from government or businesses to develop strategies that allow for the future threat that RFID might impose on

individuals and organisations. A thorough examination of the threats would be required (see below). This would have to look at existing and new potential threat approaches, malware trends, the value of the data held on RFID cards and how the threats are to be mitigated.

Government and businesses will need to consider both the Privacy and Forging elements. Therefore we can divide RFID security threats into two distinct elements:

Element 1: Privacy

Inventorying – collecting tag data with a suspicious reader

Tracking – Illicit tracking using a tag's serial number

Element 2: Forging

Cloning – Physical replication of an existing tag to introduce to the system

Simulation – Tampering with an RFID system using simulation devices

(c) S.Nair, O. Al Ibrahim

Final Thoughts

The technology for analyzing, hacking and cloning RFID tags will only improve over time. The mass production machinery behind the tags cannot keep up with the security threats. This is the same story in the PC world whereby malware is always one step ahead. Will we ever learn from our history? One doubts it.

So what about NFC? Right now Android is the weak link (if you were to use Google Wallet as the template) – not iPhone or Blackberry. The biggest question right now has to be – will users accept financial data and credentials stored on the same device? While RFID/NFC can certainly provide bulletproof cryptographic protection, most deployments still choose proprietary technology instead. The NFC chips in upcoming phones support both the old and the new standards. Right now, if you are reading this, you are probably saying to yourself *I'm not so sure*.

It's only a matter of time before someone or a cybercrime gang finds a method that steals both the personal and business data from the many material objects that will in the future use RFID and NFC.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect. IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.

RFID JOURNAL LIVE! Europe

18-19 Oct. 2011 * Dorint Hotel, Amsterdam, The Netherlands



LEARN HOW YOU CAN USE RFID TO IMPROVE THE WAY YOU DO BUSINESS

HEAR HOW THESE AND OTHER INDUSTRY LEADERS ARE BENEFITING FROM RFID TODAY:

KEYNOTE SPEAKERS:



GERRY WEBER
INTERNATIONAL AG

Christian von Grone



Soren Moller Sorensen



Carlo K. Nizam

FEATURED SPEAKERS INCLUDE:



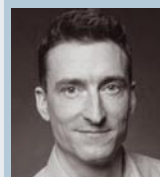
Mike Haley



Rimantas Damanskis



Asif Latief



Andreas Schroers, Ph.D.



RFID JOURNAL

**HAKIN9 MAGAZINE VIP DISCOUNT:
SAVE 15% OFF RFID JOURNAL LIVE! EUROPE
USE PROMO CODE AEBD**

**SPECIAL
WAREHOUSE
AND INVENTORY
MANAGEMENT
SEMINAR**

www.rfidjournalevents.com/europe

RFID and Privacy

An interview with Dr. Ann Cavoukian

Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada



Dr. Ann Cavoukian took a Bachelor of Arts (B.A.) at York University in Toronto and then received a *Masters of Arts (M.A.)* and *Doctorate of Philosophy (Ph.D.)* in psychology from the University of Toronto, specializing in criminology and law.

In the 1980s, she headed the Research Services Branch for the provincial Attorney General. Joining the Ontario provincial Office of the Information and Privacy Commissioner in 1987, Dr. Cavoukian served as its first Director of Compliance followed by her appointment as Assistant Commissioner in 1990.

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is protected in Ontario – and around the world. Dr. Cavoukian is Ontario's first *Information and Privacy Commissioner (IPC)* to be re-appointed for an unprecedented third term. Initially appointed in 1997, her role in overseeing the operations of the freedom of information and privacy laws in Canada's most populous province has been extended to 2014. Like the Auditor General, she serves as an Officer of the Legislature, independent of the government of the day.

Noted for her seminal work on Privacy Enhancing Technologies in 1995, her mantra of *privacy by design* seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protections.

Dr. Cavoukian published two books on privacy with co-authors:

- Tyler Hamilton: *The Privacy Payoff: How Successful Businesses Build Customer Trust*, 2002.

- Don Tapscott: *Who Knows: Safeguarding Your Privacy in a Networked World*, 1997.

Awards include:

- 2011 – Information Access and Protection of Privacy Award (University of Alberta)
- 2011 – Privacy Professional of the Year (SC Congress)
- 2011 – Kristian Beckman Award (IFIP)
- 2008 – Privacy Hero and Leadership Award (WiredSafety)
- 2007 – Top 100 most powerful women in Canada (Women's Executive Network)
- 2007 – Dr. Barbara Wand Award (Ontario Psychological Association)
- 2006 – Outstanding contribution to the protection of privacy rights in Ontario (Ontario Bar Association)
- 2006 – IABC All-Star speaker (International Association of Business Communicators)
- 2005 – Privacy Innovation Award (International Association of Privacy Professionals)
- 2003 – Privacy Manager of the Year (Privacy Manager Magazine)

Memberships and affiliations include:

- Chair, IPSI Advisory Board
- International Biometric Advisory Council
- IBM Privacy Management Council
- European Biometrics Forum
- Future of Privacy Forum
- RIM Council

- Distinguished Fellow of the Ponemon Institute
- Women of Influence

When asked on July 15, 2011 her views on Radio Frequency Identification (RFID) Dr. Cavoukian stated:

RFID tags are the next evolution in technology from barcodes. Containing microchips and tiny radio antennas that can be attached to products, RFIDs can transmit a unique identifying number to an electronic reader, which in turn links to a computer database where information about the item is stored. To manufacturers, suppliers and retailers, RFIDs can be a valuable tool in managing inventory but for consumers they can also pose as a potential risk to privacy if linked to personal information.

RFID tags are becoming more prevalent in our everyday lives from security access cards to ignition immobilizers to highway toll systems and other electronic pass systems. Further, the ubiquitous presence of RFID tags for consumer level items is rapidly approaching. From cans of shaving cream to sweaters, RFIDs will soon be found on almost every product as companies look to optimize their inventory control and supply-chain management practices. However, for RFID technology to fully realize its potential for consumers, retailers and suppliers, it is vital that privacy concerns be addressed while establishing principles for dealing with the evolution and implementation of the advancing technology.

Although RFID technology deployed in the supply chain management process poses little threat to privacy, item-level use of RFID tags in the retail sector, when linked to personally identifiable information, can facilitate the tracking and surveillance of individuals.

The IPC's work on RFID and privacy has involved numerous publications with key overarching principles addressing key privacy issues regarding the use of RFID technology at an item-level in the retail sector.

The first principle places a focus on RFID information systems rather than on the technology. Like all technological developments, the technology itself is neutral and the problem often lies in the way which it is deployed.

The second principle advocates building privacy and security from the outset while still in the design stage. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This comes directly from Commissioner Cavoukian's concept of Privacy by Design (PbD), which refers to the philosophy and approach of embedding privacy directly into the design specifications of information technologies, accountable

business practices and physical design and networked infrastructure. In short, it is taking the proactive approach by making privacy the default by building it in at the very beginning.

The third principle encourages the maximization of individual participation and consent. RFID systems should be open and transparent and allow consumers with the opportunity to make informed decisions about their role in the use of RFIDs.

Smart businesses will always employ technology to improve productivity, cut costs and increase their bottom line. However, one must begin to question just how smart businesses are when they deploy technology that requires consumers to relinquish their personal information in return for greater convenience or simply for the sake of the businesses to operate more cost effectively.

Businesses must begin to understand that there are various benefits to privacy beyond the need to fulfill the minimum legal obligations. Consumers who are informed and in control of their personal information are faithful customers and most importantly, they are repeat customers. The issue with RFIDs ultimately comes down to consumer empowerment and trust which in reality translates into market share. Simply said, any amount of money saved on implementing cost-effective technologies is a futile initiative if consumers do not even trust you enough to spend their money with you.

For more information on Commissioner Cavoukian's Privacy by Design please visit www.privacybydesign.ca or contact the Information and Privacy Commissioner of Ontario directly at info@ipc.on.ca / 416-326-3333

REBECCA WYNN

Rebecca Wynn, DHL, MBA, CISSP, CRISC, LPT, CIWSA, MCTS 2005, LPT, GSEC, CCSK, NSA/CNSS NSTISSI 4011-4016 is a Lead/Principal Security Engineer with NCI Information Systems, Inc. She has been on the Editorial Advisory Board for Hakin9 Practical Protection IT Security Magazine since 2008.

MITM using Cain: Client Side Attacks

As a Boss, have you ever tried to find out what your employee is working on with his office desktop? As a network admin, have you thought of finding who is flooding the network with trivial issues? As a parent, are you eager to know what sites your kid is browsing?

What you will learn...

- Use of Cain and Abel tool to launch MITM attack
- Protecting yourself from MITM Attacks

What you should know...

- Basic computer and Internet skills
- A little about Address Resolution Protocol (ARP)

If your answer is yes to any one of the above, then the solution is right here. It is obvious that you just have to behave as a *Man-in-the-Middle* (MITM) to sort out the things. Let us have a panoramic view of MITM and how to perform it in a stealthy way.

What is MITM

Man-in-the-Middle (aka *Monkey-in-the-Middle*) is a process in which the attacker intercepts or observes the conversation between two hosts by creating individual connections with the victims and relay the messages between them, giving them the feel of direct conversation. The attacker can behave in a passive or active mode in which he can simply observe the conversation by sniffing network traffic or modify the conversation by injecting the new ones respectively.

MITM attack can be performed by using a simple GUI based window tool known as Cain and Abel. You can download the tool for free from <http://www.oxid.it>.

Cain and Abel

Knowledge of how to use a tool is as important as selecting a perfect tool for particular task. C&A is windows based GUI tool used mostly for password recovery through network sniffing, cracking passwords using Dictionary and Brute-force attacks, VOIP conversation recordings etc. It has been developed for use of network administrators, forensic staff, security

professionals, pen testers and others who use it exclusively for ethical reasons.

The latest version of C&A comes with capability of MITM using APR (*ARP Poison Routing*). APR is the major feature of the program which enables hijacking the IP traffic between hosts by sniffing on switched networks. Even though C&A is a framework for many other tasks, for now we will stick to only MITM.

APR (ARP Poison Routing)

This kind of attack is based on the manipulation of host's ARP caches. On an Ethernet/IP network when

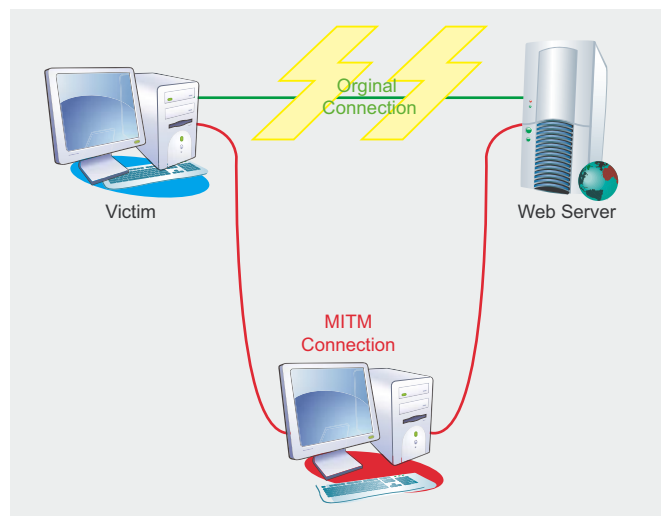


Figure 1. Men in the middle

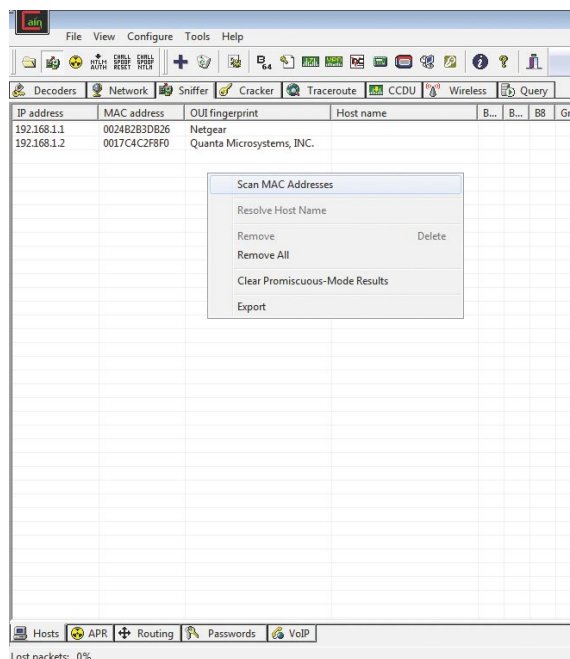


Figure 2. Scanning for Hosts

two hosts want to communicate to each other they must know each other's MAC addresses. The source host looks at its ARP table to see if there is a MAC address corresponding to the destination host IP address. If not, it broadcasts an ARP Request to the entire network asking the MAC of the destination host. Because this packet is sent in broadcast it will reach every host in a subnet; however, only the host with the IP address

specified in the request will reply its MAC to the source host. Conversely, if the ARP-IP entry for the destination host is already present in the ARP cache of the source host, that entry will be used without generating ARP traffic.

How to perform APR

To start APR, you should be in a network with computers connected. APR can be done with single host or group of hosts inside a network (Intranet). ARP poisoning cannot be done in WAN or Internet. Now we will go with step by step procedure of how to APR using C&A.

Step 1:

Install C&A in your windows systems. Start C&A and select the sniffer tab.

Step 2:

Next step will be to scan the no.of active hosts present in your network. The result provides you with each IP-MAC associations in the network. Click the configure button from control panel and ensure that *Use real IP and MAC addresses* is selected under *APR* tab and click OK. While scanning, you should use your real IP and MAC to avoid conflicts. Right click on empty space and scan MAC addresses.

The result will be of all the active hosts in the network excluding yours. My IP is 192.168.1.3 which is not shown in the scan results.

a d v e r t i s e m e n t



HAKIN9

Subscribe to our newsletter and stay up to date with all news from Hakin9 magazine!

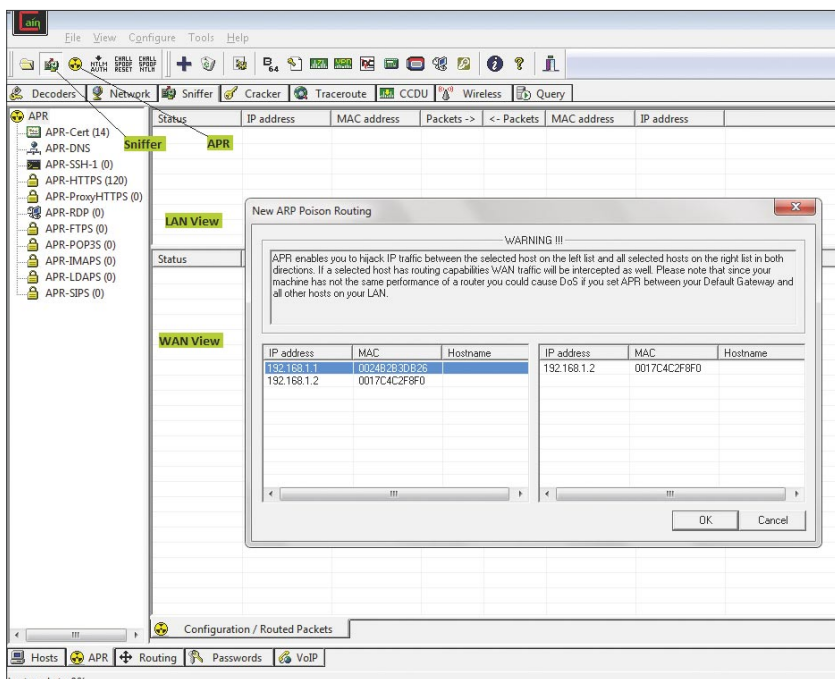


Figure 3. Adding the hosts

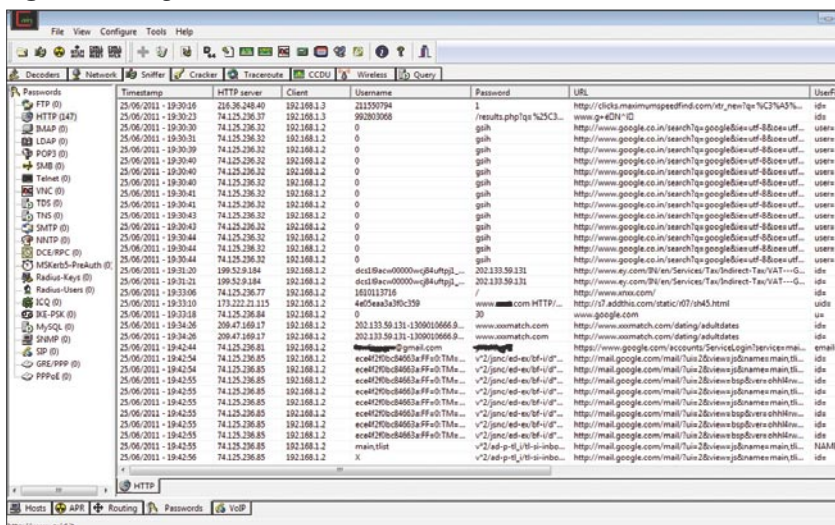


Figure 4. Result of APR

Step 3:

Go to *configure* again and use spoofed IP-MAC addresses (IP-MAC should be different from the one present in network to avoid confusion) to conceal your actual IP. Start the sniffer by clicking on the icon in control panel. Find out the router IP (default gateway) in your network from the scan results.

Go to APR tab (present at bottom of sniffer window) and click on LAN view. Add the Hosts by clicking on blue plus sign. The popup window will allow you to select the IP's which you want to poison. From the left panel select the router IP and from the right select the IP which you want to sniff (thus you can be able to listen the conversation between the router and the selected victim).

In my example 192.168.1.1 is my network router and 192.168.1.2 is the victim which I want to monitor.

Step 4

Click OK and start APR (yellow nuclear symbol) to begin poisoning and listen to their conversation. In the WAN view it shows full-routing conversation between victim computer and router. Go to *Passwords* tab (adjacent to APR tab), select HTTP and look at the astonishing results.

In my example, it is evident that my employee is accessing restricted sites and I am also able to capture his email id and passwords (look and forget).

Protecting from MITM attacks

Who knows if your computer is vulnerable to MITM attacks. So make sure that you are protected in the following ways to mitigate the risks. MITM attacks can be avoided to a maximum extent by:

- Use SSL and HTTPS wherever possible.
- Update the Antivirus and Firewall regularly which notifies you when someone attempts to sniff your network.
- Make use of the latest version of web browsers.

Conclusion

The effective way to protect oneself from particular attack is to possess a deeper insight on how to perform that attack, thus leaving you with the knowledge of vulnerabilities and exploits which you can patch. This tool is made up with the motivation for ethical reasons and there is no perception of unethical issues.

BHARATH SIVA KUMAR

Bharath Siva Kumar is a Master's student in Information and Communication Systems Security at KTH in Sweden. He is mainly interested in Cloud Security, Network and Application Security. He is also a bibliophile and pianist. Contact: bharath17@aol.com.

The background of the entire page is a dark blue/black color with several bright white lightning bolts striking downwards. The bolts are jagged and have a glowing effect.

In the next issue of
HAKIN9 magazine:

Secure Coding

**Available to download
on September 1st**

Soon in Hakin9!

BitCoin, DDOS, TOR Project, Botnets, Social Network Security, Hacking Apple, Biometrics, Rootkits, Debugging/Fuzzing, SQL Injection, Stuxnet, Hacking Facebook, Port scanner, IP scanners, ISMS, Security Policy, Data Recovery, Data Protection Act, Single Sign On, Standards and Certificates, Biometrics, E-discovery, Identity Management, SSL Certificate, Data Loss Prevention, Sharepoint Security, Wordpress Security

If you would like to contact Hakin9 team, just send an email to en@hakin9.org. We will reply a.s.a.p.

When is Private Not Private?

Making Sense of European Privacy Law

A judge is a law student who marks his own examination papers.

H. L. Mencken

American Journalist

We all know that it is important to stay within the law. The problem is, laws change less quickly than the world in which they must be applied. But laws do change – and so do our legal responsibilities, either as individuals or as parts of bigger organisations. With super-injunctions for celebrities such a prominent feature of the headlines in the UK recently, it's been easy to miss privacy issues which have a much wider impact.

There are a number of legal arguments that state there is no specific right – but this is clearly not the case when we examine the recent developments in the law around this point. In general terms, privacy can be seen to be assigned as both a right specific to individuals (as per the super injunction instance) and a general right (for example, applying to consumers in the EU). Privacy has, de facto, become a real consideration in the application of technology; furthermore, the impact of this applies not just to large organisations, but also the behaviour of individuals. Therefore, there is a responsibility to respect the right to privacy.

The EU has recently changed the law regarding the saving of cookies on users' computers by websites. The *Privacy and Electronic Communications Regulations* (PECR) have been updated to increase privacy for website visitors and require websites to obtain consent from visitors prior to storing a cookie on the visitor's computer. Let's think about this for a moment – this is a piece of European legislation. The internet, by contrast, is not limited to the realms of the EU. So, in effect, the law applies to everyone with a website, whether or not they are hosted inside the EU. On the face of it, this makes little sense – the legal aim is clear, but the aim does not coincide with practical realities.

The CEO of one major online luxury retailer, when interviewed by the author, stated that he was *vaguely*

aware of the legislation, but *was unsure how it applied to him*. Therefore his intended action was to ignore it. This is potentially a minefield for organisations – cookies may be an integral part of the design and functionality of many websites, but the risks and legal implications may not be fully understood by management. If a big organisation can't keep on top of this, what about small businesses? Or individuals?

We should expect that legislation in this area to increase and become more focussed as time progresses – taking steps now diminishes the risk of becoming a test case, with all the negative attention that would bring.

So how do we get to the situation where laws are passed that no-one seems to understand – let alone knows how to comply with?

The significance of legislation – the law of unintended consequences

The root of the issue is what the purpose of laws are. They are in essence tools- enacted by governments to address what is perceived to be an issue. The problem comes when the world changes. Whether the original issue still remains, or even was completely understood in the first place, the law remains on the books. Hence, the tool can be repurposed – to do something that it was not originally intended for.

The Anglo-American legal tradition directs a court to look to past decisions for guidance on how to decide a case before it. This means that the legal rules applied to a prior case with facts similar to those of the case now before a court should be applied to resolve the legal dispute.

The use of such precedent has been justified as providing predictability, stability, fairness, and efficiency in the law. Reliance upon precedent contributes predictability to the law because it provides notice of

what a person's rights and obligations are in particular circumstances.. It also means that lawyers can give legal advice to clients based on settled rules of law. Since the start of the twenty-first century, Russia's legal institution has been gradually shifting from a Continental codified law-based legal system to the Anglo-Saxon precedent-based system.

All fine in theory – but what happens when there is no clear precedent? This is frequently the case where technology is involved. This creates the risk of being the test case – the first instance in which the law is applied, and which in effect forms the precedence. If the law has not been interpreted before, there is no benchmark – where the circumstances around the case change, because of a changing technology landscape, for instance, there is the risk of rolling interpretation. In effect, every time is the first time.

To illustrate this problem, it's worth considering two case studies – one to illustrate the evolution of an older piece of legislation, and the second to illustrate the issue of personal liabilities.

Case Study: The Data Protection Act

The UK's Data Protection Act came into force in 1998. It is fairly typical of Data Protection legislation within the EU. The Act covers any data about a living and identifiable individual. Anonymized or aggregated data is not regulated by the Act, providing the anonymization or aggregation has not been done in a reversible way. Individuals can be identified by various means including their name and address, telephone number or Email address. The Act applies only to data which is held, or intended to be held, on computers (*equipment operating automatically in response to instructions given for that purpose*), or held in a *relevant filing system*.

In practical terms, all sorts of data could be covered by the Act – even an address book could be classified as a *relevant filing system*, for example diaries used to support commercial activities. At the Act's core are eight principles:

- Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - at least one of the conditions in Schedule 2 is met, and
 - in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- About the rights of individuals e.g. You have the right to have data about you removed.
- Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The body responsible for enforcing the terms of the DPA is the *Information Commissioner's Office (ICO)*. For many years, the Act was more of a notional threat than a practical risk to organisations. However, the ICO has become increasingly active over the last few years. This has principally taken the form of increasingly hefty fines in April 2010. Since the Criminal Justice and Immigration Act 2008, the ICO has had the power to impose fines of up to £500,000 on organisations that deliberately or recklessly commit serious breaches of the DPA What is of more note is how these fines have been applied – not just to organisations, but to individuals within them.

Four examples include:

- The ICO fined two ex T-Mobile employees for having stolen customer data for financial gain. In a statement the ICO said that the two former employees picked 'select customer data' in 2008 and have been fined for their actions. The two workers, David Turley and Darren Hames, were ordered to pay a total of £73,700(US \$120,000) in fines and confiscation costs. Failure to do so could result in prison time.
- In 2010 the ICO announced a £100,000 (US \$162,000) penalty was handed to Hertfordshire County Council in the UK. The council was reprimanded for two serious incidents when employees faxed highly sensitive personal information to the wrong recipients. In one case, details relating to child sex abuse meant to go to lawyers were sent to a member of the public.
- Later in 2010, employment services company A4e was hit with a £60,000 (US\$ 97,000) fine A4e had an unencrypted laptop stolen, which contained personal data on 24,000 people who had

used community legal advice centres in Hull and Leicester. There was apparently an unsuccessful attempt to access the data on the laptop after it was stolen *The laptop theft... nothing less than a monetary penalty as thousands of people's privacy was potentially compromised by the company's failure to take the simple step of encrypting the data*, the Information Commissioner, Christopher Graham, stated.

- The latest fine, of £120,000 (US \$195,000), imposed on Surrey County Council, is the largest to date, was imposed for the exposure of the details of *vulnerable* individuals through a series of three misdirected e-mails. None of the e-mails were encrypted.

In none of these cases did the activity which caused the fine relate per se to the processing of data. All the data in question was either *at rest* or being transmitted. Similarly, the Act does not specify encryption. The Act was designed to make organisations accountable – but we can see individuals being fined and threatened with jail time.

It's also worth noting that privacy law is not a uniquely EU phenomenon. Even countries such as Uganda have, in recent years, created legislation in this space – so it is a reasonable expectation that this will come into play whatever legal jurisdictions you live or operate in.

Case Study 2: Gary McKinnon: UFOs, the Department of Defence and...

Gary McKinnon is a 45 year old Scottish systems administrator and, in his spare time, a hacker. He also has abiding interests in UFOs and various conspiracy theories. He is accused of hacking into a number of United States military and NASA computers over a 13-month period between February 2001 and March 2002, using the name *Solo*. The computer networks he is accused of hacking include networks owned by NASA, the US Army, US Navy, Department of Defense, and the US Air Force. McKinnon claimed that he was able to get into the military's networks simply by using a Perl script that searched for blank passwords

It is claimed that by disrupting operating systems, he shut down the US Army's Military District of Washington network of 2,000 computers for 24 hours. In addition it is claimed he deleted US Navy Weapons logs, rendering a naval base's network of 300 computers inoperable after the September 11th terrorist attacks. McKinnon is also accused of copying data, account files and passwords onto his own computer.

In his defence, McKinnon denied causing any damage. He arguing that, while looking for UFO-related material, he accessed open, unsecured machines with

no passwords and no firewalls. Furthermore, he claims he alerted the relevant authorities numerous times pointing out their many security weaknesses. The US claimed he caused over \$700,000 worth of damage – his counterclaim is that the US claim is inflated to justify his extradition to the United States. While not admitting that it constituted evidence of destruction, McKinnon did admit leaving a threat on one computer:

US foreign policy is akin to Government-sponsored terrorism these days ... It was not a mistake that there was a huge security stand down on September 11 last year ... I am SOLO. I will continue to disrupt at the highest levels ...

His case has attracted support from a wide range of celebrities, including Sting, Pink Floyd, and Marillion, political parties including the UK's Conservative Party (part of the country's ruling coalition), and the UK's National Autistic Association (Asperger's Syndrome forms a key part of his defence).

So here we have a situation where a super-annuated *script kiddie* has had his career ruined, was threatened with extradition to the US, and has lasting notoriety – all resulting from a misplaced interest in conspiracy theories. Definitely a case of unintended consequences – but a great example of how *private* activities can spill outside those bounds- and into dangerous legal territory. The real significance of the case is yet to emerge – it will likely form a precedent for how the US will expect to treat other hackers. Given the increasing frequency and sophistication of such attacks, this should be watched with real interest around the world.

An ounce of prevention...

There is very little we can do to educate lawmakers directly. Nor should we seek to create a test case – this would be expensive and dangerous. But there is plenty we can do to ensure that neither we, nor the organisations we work for, fall foul of the law. Here are five easy steps to take:

Know who's responsible for what you say and do

This is easy to work out – it's you. Even in a work context, you have responsibility for avoiding legal problems that you can see.

Drop the distinction between the private and the public

The internet – and the law – doesn't make an easy distinction between your public and your private personas. It is easy for people to make a link between you and your Twitter alter ego for example – so avoid saying things you would not like to repeat in a court of law. This is underlined by the super injunction issue in the UK. People felt they were saying things *in*

private or in the public interest, but this is likely to be an area where the law will evolve.

Make sure you understand what's relevant

Knowing what you have is critical. Are you handling personal data? This immediately translates into a need to comply with relevant privacy legislation. Running a small business online? Take steps to comply with PECR. Taking card payments? Ensure you know what the relevant regulation (Payment Card Industry- Data Security Standards [PCI-DSS]) say. Ignorance of the law is not a viable legal defence.

Take sensible steps in advance

We started the article talking about PECR and cookies, and the difficulty of interpreting law. However, there are reasonable steps that can be taken to make sure you are well positioned to comply with law, even poorly understood ones. In this case, avoid using flash cookies. Flash cookies make it intrinsically difficult for users to opt-out from behavioural targeting (as flash cookies re-spawn even where a user has deleted them). Therefore they are more likely to breach the requirements of PECR, as it will be difficult to claim the user has given valid consent when a flash cookie re-spawns despite a user's attempt to delete it.

Keep a watching brief

There is lots of easily digestible comment on legal developments. Pinsent Mason, an international law firm, provides free news and comment, as well as well as advice on issues around IT law (www.out-law.com).

DRAKE

Drake has worked on information security and strategy with government agencies, the military, financial institutions, and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.

Join

PenTest Mag team!



PenTest Magazine is looking for regular contributors. If you want to be a part of the first magazine devoted to penetration testing, now's your chance to join us. We especially need:

- news contributors – send in a piece of news of an interest for a pentester and make your own comment on it.
- “point of view” section writers – short articles (800 words tops) with you discussing an issue you think should be discussed.
- “vulnerability check” writers – what a pentester can use in his work.
- reviewers – found an interesting tool? Review it for us.
- betatesters – read an article before it's published in the magazine and share your opinion on it with us.

Regular contributors are given free subscription to the magazine and – if they represent companies – free advertising in the mag. And, of course, an earned mention in the magazine.

Worth it? Ask for details:

sebastian.bula@software.com.pl

The Astalavista Experience

Astalavista.com is an IT News & Security community. It serves as a starting point for IT and security news with its continuous news stream on the main page. More in-depth information is provided on the forums, blogs and multimedia sections.

What you will learn...

- You can use Astalavista for Diagnostics
- You can use Astalavista for Information Gathering
- You can use DNS Tools and Encryption/Decryption routines
- You can use Wargames to improve your security skills

What you should know...

- Basic to good knowledge of security tools and issues

But Astalavista is much more, for the technical interested and IT savvy people there are a multitude of tools which can be used. These range from diagnostic tools like dig, ping and traceroute to information gathering tools, DNS tools and encryption/decryption routines. Finally you can test your IT security skills on the Wargames section...

Astalavista has been around for some time now. It was founded in 1997 by a computer enthusiast. The name of the site stems from the unforgettable line in the Terminator 2 movie – *Hasta La Vista Baby*. Today Astalavista focuses on a community part, a multitude

of internet security tools, the Wargames section (where you train your IT security skills) and IT news!

This article features on the tools and wargames section, the most sophisticated parts on *Astalavista.com* (Figure 1) The tools page itself is divided into Diagnostics, Information Gathering, DNS Tools and Encryption/Decryption.

Tools Page – The Diagnostics part

On the diagnostics part Astalavista offers basic tools you need in IT security and a good collection of more sophisticated tools. Most of the tools on Astalavista

are free of use – you only need to join the community. More sophisticated tools are open to premium users with a monthly, yearly or lifetime membership. The tools range from Dig, Ping, Traceroute to SNMP Check and Proxy Checker. We want to showcase here Dig and Ping to also involve

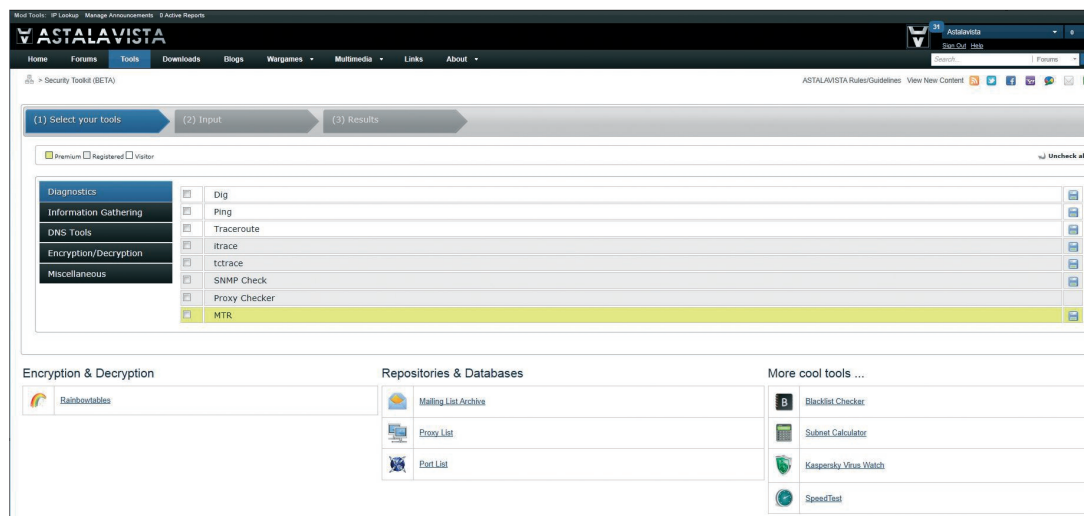


Figure 1. Astalavista Tools Page

readers with a basic knowledge of IT security in our Astalavista experience.

Dig and Ping

Certainly most of you have worked with Dig or heard the expression once, even though you are not an IT expert. So to reiterate, what is it exactly? Dig is a network administration command line tool. It requires the *Domain Name System* (DNS) name servers for any desired DNS record. If you want to check an URL or IP address, please make sure you have the legal permission to do so. Just put in the format of your information into the query box, either the IP address or the URL and start the process (Figure 2). Unless there is some kind of protection by the owner of the IP address or URL you get the typical result, that looks more or less like the one in Figure 3.



Figure 2. Dig input

Another classic query everyone performs is ping. The ping utility is used to see if a computer is operating and also to see if network connections are intact. How does it work? A small packet is sent through the network to a particular IP address. If a result is being received one can tell the number of hops that lie between two computers and the amount of time it takes for a packet to make the complete trip between the computer and the IP address. You see a typical result on Figure 4.

Tools Page – Information Gathering

Here Astalavista features nine important information gathering tools. These range from Whois, Banner Grabber to Portscan and Netcraft.

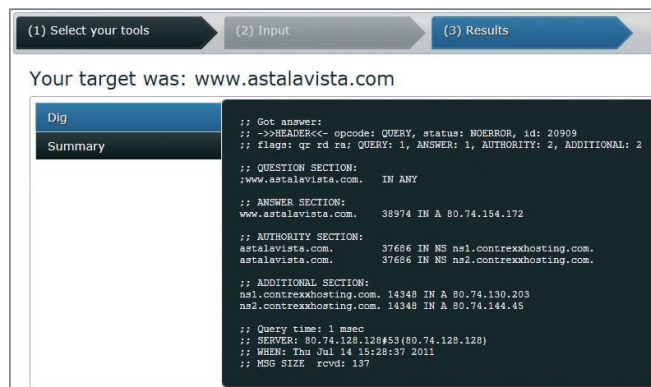


Figure 3. Dig result

a d v e r t i s e m e n t

In the Next Issue of PenTest Magazine ...

Pentesters! (Ab)Use Their Cloud!

Available to download on August 1st

The August issue of PenTest Magazine will be devoted to penetration testing in the cloud. If you are interested in this delicate subject, don't miss it.

In the upcoming issues of PenTest Magazine you will find:

Pentesting Mobile Applications, Client Side Exploits, Social Engineering And Pentesting, Nessus Scanner and more...



If you would like to contact PenTest Magazine team, just send an email to sebastian.bula@software.com.pl
We will reply a.s.a.p.

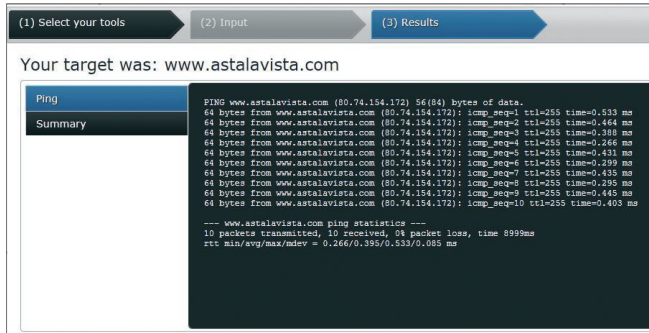


Figure 4. Ping result

Tools Page – DNS Tools

The DNS Tools Page features five important tools. These are DNS Host, DNS Tracer, DNS Map, DNS Enum and Zone Check.

Tools Page – Encryption/Decryption

On the encryption/decryption section we want to highlight Rainbowtables (Figure 5) Rainbowtables allow

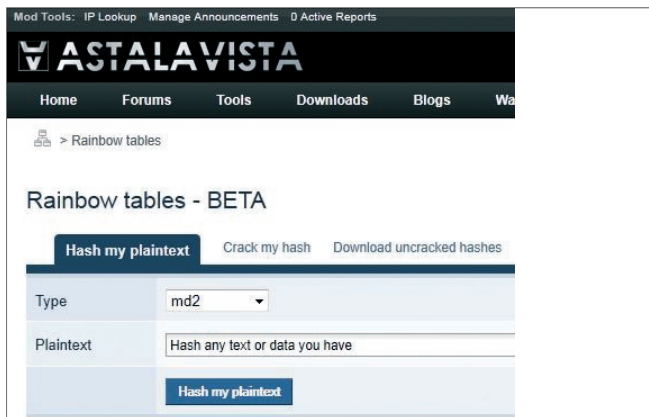


Figure 5. Rainbow tables

you to convert any possible variable-sized amount of data into a small datum. On Astalavista you can choose between more than forty types of hash conversions. So, try it out yourself. Just put in any kind of text or other data, choose your hash type and with one click you have created your own hash text (Figure 6) On Rainbowtables you also find other features like crack



Figure 6. Plaintext to hash result

my hash, download and upload cracked hashes. So if you are able to get back the plain text from our hash result example in Figure 6, please drop us a line.

Wargames

The Wargames section on Astalavista.com is the real challenge for anyone who sees himself as an IT savvy or IT professional and is willing to test his security and ethical hacking skills (Figure 7). The purpose of a



Figure 7. Wargames – Real Missions overview

wargames server is to allow you to practice hacker tricks, without actually damaging anyone or breaking the law. With this technique, gaps in security can be discovered and the necessary precautions can be taken. To get started first look to the access details (Figure 8). You will

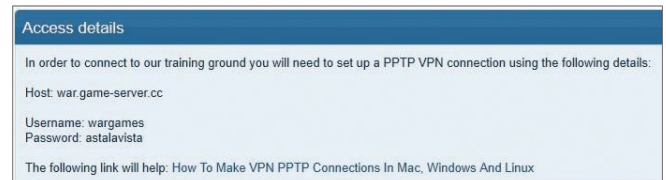


Figure 8. Real Missions – access details

need to setup a PPTP VPN connection to our server and give the password information. On the system status you find 14 interesting challenges, click on every one of them and choose your favourite. For example you could try the World Gold Reserve Challenge. Here you find yourself with the fictitious task to access the World Gold Reserve and to transfer 1000 Gold bars to your own account. If you enjoy the wargames challenge you may even want to write a whitepaper about your experience and address it to wargames@astalavista.com.

SVEN ADELT

Sven Adelt is the Community Manager for Astalavista.com. He has a marketing background and a masters degree in English, Business and Political Science. His affinity to IT and the security world stems from years of experience at a telecommunications provider in Germany. He joined the Astalavista Project in February 2011 and quickly absorbed the Astalavista spirit.

Join Today Free!



Go Premium to support & enjoy the full potential!

New

Astalavista - The IT News and Security Community

- Forum Posts SHOW
- Downloads SHOW
- Events HIDE
- Official Blog SHOW
- News SHOW
- Jobs SHOW

Astalavista has taken another step into the future.

Stay Up-to-date

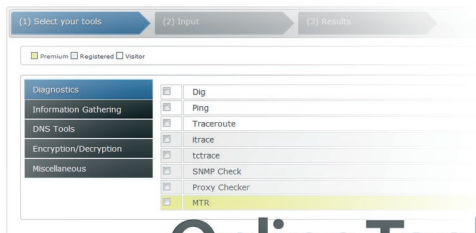
With our relaunch we focus even more on the IT & Security world.

Our continuous news stream on the main page gives you all the information you need – 24/7. What do you think about that? Give us a shout on our Astalavista Blog, you find it by clicking on the first news item on our news stream.

Join Today

www.astalavista.com

Go Premium!



Online Tools

The new **Online Tools** overview page features nearly 50 tools covering typical IT needs, like Whois, Dig, Proxy List or Encryption.

The **Rainbow tables** section lets you hash your plain text in more than forty different types and crack your hashes. The **blacklist checker** runs your domain against the most important black lists and checks if your IP/Domains are flagged as spam.



Wargames

Wargames by its broad definition is a military drill under real life conditions. It is about testing strategies without the actual combat.

The **“World Gold Reserve”** is where most of the world's gold is stored. The combat in IT is virtual. Here the purpose of a wargame server is to allow you to practice hacker tricks without damaging anything or violating the law. The aim is to find gaps in security and to learn the necessary precautionary actions to prevent this.

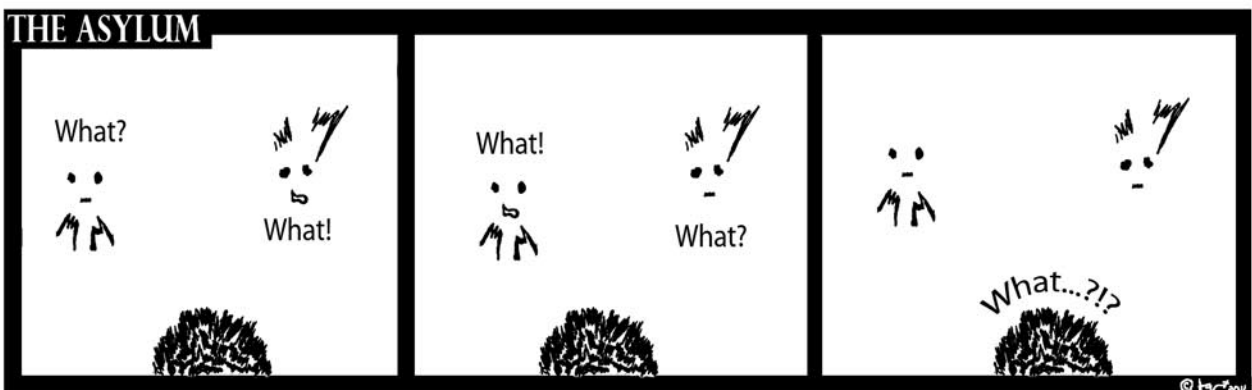
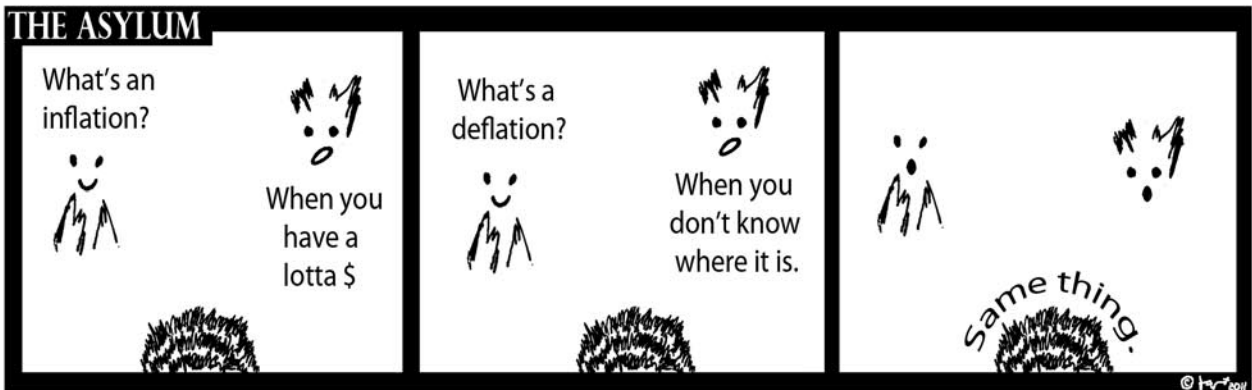
Go Premium to support & enjoy the full potential!

Astalavista.com

No There is no fingerprint, but there is a secret code that gives you a sweet discount: hakin9astadiscount

IT News and Security Community

Notes on The Asylum



Hacker | Halted

**U S A
2011**

**Oct 21-27, 2011
Intercontinental Hotel. Miami, Florida**

*Its more than just a conference.
Its the Convergence of the Best at
a World Class Event*

Jeremiah
Grossman

Bruce
Schneier

Philippe
Courtot

Charlie
Miller

George
Kurtz

www.hackerhalted.com

Join the National Information Security Group (NAISG)

FREE ANNUAL MEMBERSHIP FOR HAKIN9.org SUBSCRIBERS

FACT SHEET



Overview

The National Information Security Group (NAISG) is a non-profit organization that promotes awareness and education of information security through the support of local and regional chapters. Members include IT administrators, managers, law enforcement personnel, the media, educators and students and anyone else interested in getting or staying on the cutting edge of information security.

NAISG:

- › OPEN YOUR OWN CHAPTER ANYWHERE IN THE GLOBE.
- › MONTHLY MEETINGS AT EACH CHAPTER – VISIT ONE WHEN YOU CAN – FREE.
- › SECURITY VENDOR NEUTRAL – NO PRODUCT PRESENTATIONS.
- › MEMBERS ARE IT SECURITY PROFESSIONALS, LAW ENFORCEMENT, STUDENTS, EDUCATORS AND OTHERS.
- › EDUCATIONAL VENUE ON NEW SECURITY TECHNIQUES AND OTHER INFORMATION SECURITY ISSUES.
- › FREE DAILY TECHTIPS – EMAIL AND ONLINE FORUM FOR FREE SUBSCRIPTION TO SOLVE ANY SECURITY OR IT RELATED QUESTION OR PROBLEM YOU ARE HAVING...

No formal security experience required. Come to learn, share tips and tricks and network with IT professionals!

Leadership

- › **Bradley J. Dinerman**, founder and president - Brad is the founder and president of Fieldbrook Solutions LLC, an IT and MIS and consulting firm in Massachusetts. He is a CISSP and a Microsoft MVP in Enterprise Security, holds a number of technical certifications, is an active member of the FBI Infragard and the Microsoft IT Advisory Council and earned a Ph.D. in physics from Boston College. Brad frequently contributes to online TechTips sites and gives user group and conference presentations around the country. More information is available at <http://www.naisg.org/About/>.
- › **Board of Directors** . A six-member board of directors provides direction for the group. Members of the board represent various segments of the IT/security community, including academia, law enforcement, defense and the legal sectors. Bios of the board members may be found at <http://www.naisg.org/Board/>.
- › **National Advisory Council** This council includes the leaders of each chapter and provides inter-chapter support.

U.S. Chapters

As of April, 2011, NAISG maintains the following chapters in addition to its online presence, for a total of more than 5,000 members:

Atlanta, GA; Boston, MA; Dallas, TX; Houston, TX; Midland, MI; Orlando, FL; Seattle, WA; Little Rock, AR

Key Sponsors

Astaro – <http://www.astaro.com>

NetClarity – <http://www.netclarity.net>

SECURANOIA – ANNUAL SECURITY CONFERENCE

– TO BE HELD THIS FALL IN BOSTON, MA, USA

NAISG is the legal trademark of the National Information Security Group, Inc. All Rights Reserved.

NAISG is a NON-PROFIT ORGANIZATION.