# Haking Mobie Security

# VIRTUALIZATION SECURITY INTERVIEW WITH SCOTT GORDON ANDROID MOBILE SECURITY

INTERVIEW WITH ARUN SOOD THE ULTIMATE HAT TRICK THAT WORKED OVER THE LAST COUPLE OF THOUSAND YEARS



# International forum on information security practices



MAY / 2012 MOSCOW / RUSSIA

#### organized by



WWW.PHDAYS.COM WWW.PHDAYS.BLOGSPOT.COM TWITTER @PHDAYS PHD@PHDAYS.COM

# In the program

learn all the latest - six streams of the conference, workshops, training and a hands-on lab keynoted **by Bruce Schneier** 

check your level - international competitions
Capture The Flag and HackQuest

show the world what you can do -Contest and challenges

crack your phone or laptop and get \$ - Hack2own

# How to get to PHDays

- make a report send us abstracts to Cfp by April 16
- participate in a hackquest from anywhere in the world
- organize and watch the online broadcast from anywhere in the world



## Haking Mobile Security

# Mobile Security

team

Editor in Chief: Grzegorz Tabaka grzegorz.tabaka@hakin9.org

Managing Editor: Piotr Kowalówka-Małkowski piotr.kowalowka-malkowski@software.com.pl

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

DTP: Ireneusz Pogroszewski

Art Director: Ireneusz Pogroszewski ireneusz.pogroszewski@hakin9.org

Proofreaders: Nick Baronian, Dan Dieterle, Bob Folden, Kelly Kohl, Michael Munt, Aby Rao, Jeffrey Smith

**Top Betatesters:** Keith Applegarth, Hammad Arshed, Ayo Tayo-Balogun, Manuel Boros, Amit Chugh, Dan Dieterle, Gregory Gallaway, M. Younas Iran, David Jardin, Michal Jáchim, Eder Lira, Rod MacPherson, Matteo Massaro, Rissone Ruggero, Antonio Saporita, Daniel Sligar, Jeffrey Smith, Arnoud Tijssen, Tom Updegrove, Dan Walsh, Robert Wood, David von Vistauxx

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

#### Senior Consultant/Publisher: Paweł Marciniak

**CEO:** Ewa Dudzic ewa.dudzic@hakin9.org

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

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

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

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

Mathematical formulas created by Design Science MathType™

#### DISCLAIMER!

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

#### Dear Readers,

In this issue of Hakin9 Mobile we are presenting articles focused on mobile security, cryptography and for the dessert we have cryptographic surprise. First, we start with the article dedicated to mobile device security by Parshant Verma and Sreenarayan A. The number of free Wi-Fi hotspots in the cities is going up - an additional incentive for the users to possess connected tablets and remain updated. The pace, at which Smart phones and tablets are being sold, is equally complemented by the availability of applications in the various market places or app stores and the increasing number of attacks. Next, you will read about Virtualization Security by Amar Wakharkar. This document tries to explain various factors affecting virtual security, security associated with full virtualization Technologies for server and desktop virtualization, and to provide recommendations for addressing these concerns. You will see what is inside Scott Gordon's mind in interview with him by Aby Ryo. "Bring your own device (BYOD), is gaining a lot of steam these days, why is that the case?" Next, we focus on Android Mobile Security in Vinay Gayakwad article. Android's profound impact on the mobile market has made it a prime target for criminals. And the operating system, which powers over half of the 60.5 million smart phones sold worldwide in the third guarter of 2011, is less safe than its rivals. Juniper Networks' Malicious Mobile Threats Report shows that Android malware instances increased by 400% between 2009 and 2010, while other platforms remained relatively secure, due mainly to fewer cybercriminals trying to break through their defenses, and in some cases, to stronger security features. Further in the issue, we prepared small cryptography surprise. First, Zsolt Nemeth and Jeffrey Smith find out how Arun Sood sees the future of cyber security, and then for promised dessert we will serve The Ultimate Hat Trick that Worked over Last Couple of Thousand Years by Zsolt Nemeth. This tutorial will help you understanding the concept of trojan dangers created - how they can invade computer, and therefore destroy you and your data. Keep safe and don't open e-mails from strangers ;)

Enjoy the reading!

Angelika Gucwa, Piotr Kowalówka-Małkowski and Hakin9 Team

### A Mobile Security



doos Lin

MAKE THE WORLD A SAFER PLACE

2012

D

# Your premium IT security event.

March, 19<sup>th</sup> - 23<sup>rd</sup> 2012 @ Heidelberg, Germany

ww.troopers.de ★ ★ www.troopers.de ★

That's how we opens

08 Mobile Device Security

by Prashant Verma

A lot of speculations these days are on the mobile devices and the security features they provide. The mobile phone and tablet usage has picked up on account of the numerous benefits, not to mention the comfort at fingertips and that too on the move. The number of free Wi-Fi hotspots in the cities is also going up – an additional incentive for the users to posses' tablets to be connected and remain updated. The pace, at which Smart phones and tablets are being sold, is equally complemented by the availability of applications in the various market places or app stores and the increasing number of attacks. A study by McAfee predicts more mobile attacks and fewer PC attacks in 2012.

#### **14** Virtualization Security

#### by Amar Wakharkar

Virtualization Security is the need for rapidly growing Virtualized environment. This document tries to explain various factors affecting virtual security, security concerns associated with full virtualization Technologies for server and desktop virtualization, and to provide recommendations for addressing these concerns.

#### 22 Android Mobile Security

#### by Vinay Gayakwad

Android's profound impact on the mobile market has made it a prime target for criminals. And the operating system, which powers over half of the 60.5 million smart phones sold worldwide in the third quarter of 2011, is less safe than its rivals. Juniper Networks' Malicious Mobile Threats Report shows that Android malware instances increased by 400% between 2009 and 2010, while other platforms remained relatively secure, due mainly to fewer cybercriminals trying to break through their defenses, and in some cases, to stronger security features.

#### CRYPTOGRAPHY

**28** The Ultimate Hat Trick that Worked over the Last Couple of Thousand Years

by Zsolt Nemeth

This tutorial will help you understanding the concept of trojan, dangers created by them, how they can come to your computer, how do they destroy you and your data. We will discuss that how many types of trojans exist and how they are attached to other applications (wrappers). And finally we'll disclose the most important issue: detection of trojan on your system, some common symptoms and prevention to safeguard your data.

### **INTERVIEW**

## 32 Interview with Scott Gordon by Aby Rao

Bring your own device (BYOD), is gaining a lot of steam these days, why is that the case?

Many employees use their personal devices at home, work and on the road. In addition, organizations need to provide network access to contractors and quests, who often arrive with their own personal devices. Although these devices are ultimately connecting to the network and introducing risk, IT Security must consider the productivity gains to be had. Security policies and practices need to be acceptable, unobtrusive and efficient for both users and IT, while fortifying necessary security mechanisms. What's important is to have realtime visibility and control over your network and the mobile devices connected to it, as well as a flexible way to enforce security policy. So we define BYOD as the extent to which an organization denies, tolerates, sanctions and endorses the use of personal and mobile devices on their network and the technical controls to manage operational risks.

#### 36 Interview with Arun Sood

by Zsolt Nemeth and Jeffrey Smith

What do you see as the future of cyber security?

Today we are mostly focused on Information Assurance – primarliy technology and policy issues. I think that there needs to be more focus on human factors, low cost solutions, and policy. In addition, Attribution deserves much more work.



000 0111

00 0

00 00

00 10

01 00

0000 

100

10 0

00 01 1

000 1

nn

000 0

1001 00

0001

0000 0 

0C

1 0000011

UAT's coveted Bachelor of Science degree in 000 001 Network Security is a vital national resource

> 0 00

> > 10 100

1000

1010000 0000 01 11 000001 0

100000100001 100 00 00 100

1000000 0 1 0 1 10010 000 0000

0 010

1 0000 00 000 1 01

00 10

010 1 000000 0 10100 010 1 0 010 1 0000000 0 1

One of the most prestigious Network Security programs in the country 100

0 00

O)

ÓĊ

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

0001

00 0

1101

10

100 0

17

00 10000

100

000 00

01 

001 00

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

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

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

**Bachelor of Science** Network Engineering Network Security **Technology Forensics**  Master of Science Information Assurance

Program accreditations, affiliations and certifications:



#### CLUSTERGEEK WITH CAUTION

LEARN, EXPERIENCE AND INNOVATE WITH THE FOLLOWING DEGREE STUDENTS: A ogy Studies, Virtual Modeling and Design, Web and Social Media <u>Tech</u> ologies Prepare to Defend! www.uat.edu 877.828.4335

# Mobile Device Security

There is a lot of speculation these days on mobile devices and the security features they provide. Mobile phone and tablet usage has picked up on account of the numerous benefits, not to mention the comfort of having that at fingertip and also on the move.

he number of free Wi-Fi hotspots in the cities is also going up – an additional incentive for the users to posses tablets that can be connected and remain updated. The pace at which smart phones and tablets are being sold is equally complemented by the availability of applications in the various market places or app stores and a side effect is an increasing number of attacks. A study by McAfee predicts more mobile attacks and fewer PC attacks in 2012.

There are various attack vectors to a phone / tablet. There are certain aspects of device security which needs to be understood and duly implemented by the users and enterprises to address the device related attacks and hacks. As an end user, you should try your best to stay protected by following the security best practices. As a supervisory control, an organization or enterprises would like to control their end mobile users, via a solution which provides them at least some control over end-users. We take a look at the end-user's perspective of device security and later on the organization's perspective of device security. But to understand those, let us first have a look at the threats the mobile device or tablet face.

#### **Threats to a Mobile Device**

A Mobile Device faces threats from multiple sources at multiple layers. On account of the different technologies used in the mobile devices, the threat source of each technology makes your mobile device and data vulnerable. Let us explore the various threat sources by means of the Figure 1.

#### **Threats at Web Layer**

A mobile user uses his device to connect to and surf the internet. There are numerous threats at the web layer. Some of the web layer threats / attacks are listed below:

- The Virus, Worms, Malware, Adware present in the wild gets downloaded to the mobile.
- The application data is sent over cleartext to the provider's server.
- The application data is weakly encrypted or encoded which could be reversed easily to read your sensitive data like password or PIN.
- The data in transit can be tampered to launch parameter manipulation related threats.
- Weaknesses in the Wi-Fi configurations may put user sessions at risk.

#### **Threats at Carrier Network**

The basic purpose of a mobile phone is to provide the user with call and messaging service. To provide this the phone utilizes the carrier network (telecom operator network).

User voice, SMS and other data over GPRS traverse the carrier network, which is also responsible for its security. Here are some of the threats /attacks at this layer:

- There are attacks which attempt to intercept the telecom tower's data.
- SMS interception has not been though very successful but can be attempted.
- There are attacks against GMS security too.
- SIM card forgery has been around for quite some time.
- Eavesdropping, Masquerading, Resource Exhaustion being some of the other attacks.

#### **Threats at NFC**

Near Field Communication (or NFC) is a communication media for the devices in very close proximity of few centimeters. The distance factor makes the attack probability lower at this layer as the attacker or the attacking device must be physically located nearby. Certain threats / attacks applicable in this case would be:

- Insecure Communications resulting into eavesdropping or data modifications.
- Unauthenticated NFC peers which can steal your data.
- Unauthenticated NFC peers who can install viruses or malware into your devices.

#### **Threats at Bluetooth**

Bluetooth is used for short distance communication within 100 meters. This is a very popular file transfer technology among mobile users. The threats / attacks at this layer include:

- Unauthenticated devices may send viruses, adware's, and malware to your Bluetooth device.
- Remote code execution types of attacks.
- Unknown device pairing puts your phone at risk.
- Bluejacking- sending unwanted messages to a Bluetooth device user.
- Bluesnarfing- unauthorized access of wireless device data via Bluetooth.
- Bluebugging- is used to install backdoors which can be used to listen to the user's voice conversation or enable call forwarding to hacker's number.

#### Threats via attached peripherals

Mobile devices can be accessed via data cables and connected to computers. There are peripheral devices that can be attached like the Credit Card Swipe accessory for iPhone, or a Smart Card Reader. All of these do pose threats to the mobile devices. Some of the relevant threats / attacks in this case are:

- Data theft / stealing via the attached cable.
- Interaction with Mobile OS in USB debugging mode.
- Virus / Malware infected device connected to phone, thereby risking the phone itself.
- Data frisking or stealing related attacks.

#### **Device Protection via Hardening** Lock your Device

One of the most basic instructions given in the security world is to lock your machine. The way you lock your home to safeguard against thieves and robbers; similarly you need to lock your mobile phones too. Locking the Phone prevents unwanted actions from happening. This can prevent casual presses and the attached actions. You may save a penny by locking the phone and prevent unnecessary calls being connected. You may prevent an unnecessary file being deleted accidentally. The locking method you use may have its own strength or weakness. We next discuss certain types of mobile device locks available.

#### PIN based Lock

The password or PIN based locking mechanism has been around for mobiles for a while now. These can



Figure 1. Threats to a mobile device

prevent or deter casual intruders only. The PIN is usually of 4 digits. The 4 digit PIN means the lower number of possible combinations, which is exactly why it is a weak password.

#### Image based passwords

Image based passwords are user friendly. They are quite secure to use and help protect the mobile from unauthorized use. One limitation with image based passwords can be the number of images available for selection.

#### Passcode

iPhone provides users with an option to use passcode. Simple passcodes are 4 digits long, which can be disabled in order to set alphanumeric passcodes. There are certain best practices with respect to passcode usage in iPhones. These are very well described by Apple at *http://support.apple.com/kb/HT4113*.

#### **Graphical Pattern Lock**

This is very popular among Android phone or Android devices users. A set of 9 dots are arranged in 3 \* 3 fashion to provide multiple touch screen drawing patterns. The number of possible combinations is sufficient enough to be termed as secure (Figure 2).

However this also can be attacked by inserting a film which gets the imprint of the touch pattern drawn by user. This same pattern can be then redrawn to unlock this phone.

#### **Face Detection Lock**

Android 4.0 introduced the face detection unlock feature. Your face picture is recorded and whenever you



Figure 2. Android Phone showing the Graphical Pattern Lock

come in front of your phone, you can unlock the phone. As always, every system has its own positives and negatives. There was an attack which demonstrated that this feature can be bypassed by showing the phone with another recorded digital image of the face.

#### **Device Autolock**

Every device including mobiles can be set to autolock at a certain period of inactivity. If the user has not used his mobile for a certain length of time, it may mean that he may be involved into something else now and forgot about his device. The unlocked phone puts the device at risk. If a person forgets to lock the phone, he is risking his data, unless he uses device autolock feature. Use the *protect by default* mantra and autolock your device. For mobile devices, 3 minutes of lockout interval should be sufficient in most of the cases.

#### **Device Encryption**

A full disk encryption is the only sound solution which can prevent your data even if your device is lost. The full disk encryption solution sets a password as key and locks your entire disk memory. For mobiles, several device encryption solutions are available. We do not come across such implementations very often but this is a sufficiently secure solution to implement. There are organizations which mandate their employees to use such solutions.

#### **Remote Wipe**

The Remote Wipe is very nice feature and it can be implemented in almost all types of smart phones. The feature provides the option of remotely wiping the data present in the user's phone. This is very handy option to use, often realized when the phone in lost. Blackberry offer this feature for their handsets. For other mobiles too, there are solutions available which can remotely wipe the data, whenever instructed to do so.

#### **Update Firmware**

The firmware controls the operations of the phones. The vendors from time to time release updates of firmware. There can be functionality or security or both related updates in a latest firmware release. The latest firmware may protect you against an attack revealed in your current firmware. It is in your best interest to apply such firmware updates to stay updated and protected. Vendors often provide the documentation of the update, which may be referred to for further information.

#### **Install Antivirus**

Antivirus prevents the device from being infected by viruses, worms, trojans and backdoors. For mobiles also, there are various antivirus solutions available now. The antivirus programs have become smarter and some of them also provide added features. These features include remote wipe, protecting your GPS coordinates, data leakage etc. Kaspersky, AVG and Lookout are some of the mobile antivirus solutions.

#### **Protect your Wi-Fi**

The HTTP data from your device travel via a local Wi-Fi to the destination server. This data may or may not be over SSL. A mobile device should be configured to use as many as possible of these settings for Wi-Fi connections. These include:

- Turn off Wi-Fi when not in use
- Use no auto reconnect
- Prefer WPA2 connections, over WEP
- Do not store the network password

#### **GPS Settings**

If you use Location Services or GPS related applications too much, you risk your coordinates being leaked out. Whenever you use Google maps, you share your current location with Google (Google knows where you are). While this feature may come handy at certain situations it also leaks out your current location, making you and your phone easily traceable. The feature should be used judiciously.

#### **Bluetooth connections**

Bluetooth is used for data or file transfer for up to distance of 100m with another Bluetooth device. This is a very commonly used feature among young people to share pictures or songs. The best practices to be followed safeguard against threats arising on account of Bluetooth connectivity are:

- Turn off Bluetooth when not in use
- Set to the device to non-discoverable mode by default
- Set a password for Bluetooth pairing
- Pair only with the devices which are trusted source
- Blackberry provides encryption over Bluetooth connections to use

#### **Secure Browsing**

Every mobile browser provides some features to protect the users. Mobile Safari in iOS 5 provides Private Browsing feature. When it is turned ON, browser history, cache, cookies, passwords are not saved. In other browsers, these settings can be configured manually. There are also options to delete the remembered data. If the phone is in auto remember mode for this data (it is not preferred to do so), then regular audits should be done to delete any sensitive data which was remembered unintentionally. As much as possible you should always send your private and sensitive data over SSL enabled websites only.

#### **Device data backup**

Mobile device data backup is often forgotten or not used by the mobile users. If you store valuable data in phones, you should regularly take back-ups. Blackberry provides a solution to take the Blackberry device data backups. There are backup solutions available for most of the other devices too. These may come handy when the phone gets corrupted or the phone is lost or stolen.

#### **Mobile Device Management**

Mobile devices vary from PDA, Mobile Phones, Net Pads, Mobile Laptops, etc. With the BYOD (*Bring Your Own Device*) coming at rapid pace and many employees working on the fly with the help of advanced technology. The challenge smart phones provide for the enterprises lays in meeting their demands in an efficient manner while not compromising on the data and device security. The answer to the question of enterprises security is Mobile Device Management.

#### **Underlying Technology**

Enterprises aim to secure data, which is their most valuable asset. This asset is present in employee's gadgets that may be beyond the control of the enterprise. These gadgets use internet connection to use their applications like Browsers, Emails, etc. The internet connection is established through cellular networks or Wi-Fi hotspots available at work/home/any other public place. With sensitive data being handled at such insecure locations a mechanism to securely manage the devices and data flowing in/out and stored is needed.

Mobile Device Management Solutions consists of two parts:

#### **Client Application**

These are applications are built for various types of platforms from Android, iOS, Windows Mobile and others that can be installed on the Employees Mobile Phone. These applications have capabilities of communicating with various servers located at the enterprise offices. These clients are basic command executors. They receive commands from the enterprise servers which are executed on the Mobile Phone. They also have features which can be used to send data and instructions/request to the server to trigger tasks like updating.

#### **Server Application**

The server side part of the MDM is the overall controller of the mobile devices. It is interface tuned to function on

its own or in the hands of administrators. This interface executes like a transponder which communicates with the Client over the internet in a secure manner and shows the activities taking place in the machine but also has the right to stop any task or change any configuration files of the Mobile Device. In short, it is a remote control for all the enterprise widely used Mobile Devices.

The Figure 3 is taken from the Apple Corporation Website, and it describes the way the configuration files are pushed onto the Apple Mobile Devices from the Servers. The configuration files are nothing but a list of settings that have been modified to function with the particular mobile service. From the diagram we can see that the servers and the clients may also belong to two different organizations. As long as the platform related configuration exchanges happen appropriately the vendors are irrelevant.

#### **Implementation Options**

Every enterprise has a different level of MDM implementation. These levels vary with the company policies. We shall try and cover the various features which different organizations can cover:

#### FOTA (Firmware Over The Air updates)

It is the feature of the MDM using which all the software and firmware updates on the mobiles can be done. Controlling all sorts of installations of applications and Operating System level patches can be achieved by making use of this component. It is highly recommended as forced installation of application and operating system level security patches can be executed through this level. FOTA support is available for platforms such as iOS, Android, Blackberry and Windows.

#### **Remote Configuration and Provisioning**

One of the biggest advantages of a mobile is its wireless freedom. You can go anywhere and are forced to carrying a heavy laptop or inserting an Ethernet cable for Internet. The MDM also implements management of the mobile remotely without causing any hassle to the user. Enterprises will be able to connect to their employees mobile devices anywhere in the world as long as the user has a network connection active on the device. The administrators will be able to remotely log into your phone or push configuration files which then will be used to change your mobile device settings.

#### Security

In the day to day tasks, every employee handles sensitive data in one form or another. Employees have sensitive documents, data and other information stored in their devices. Thus securing these mobile devices becomes a very important feature which must be included in the MDM. Updating antivirus and firewalls fall under this category. Implementation of encryption to encrypt all the data stored in the mobile devices also falls under the security umbrella. Usage of encrypted channel to communicate the data from the server to the client is covered in this element of the MDM.

#### Backup/Restore

As the mobile device is used day in/day out the chances of a application crashing increases. To avoid the loss of important information, regular backups should be done by every user on every device. This function of the MDM strengthens your employees data by taking regular backup's of all mission critical data and allows for instant restoration after failure/crash recovery of the mobile device. Usage of this feature helps in saving time and efforts too.

#### **Network Usage and Support**

Network usage gives the administrator a way to monitor the network traffic going in and out of the mobile device. By doing so, they can implement strong network level proxies and also check for non-legitimate traffic. MDM may have support provisions for all employees at any

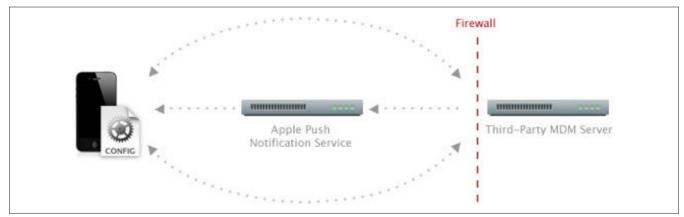


Figure 3. iPhone configuration file pushed by any Third party vendor MDM Server

time of the day. Support applications can be used of to generate and resolve problems.

#### **Mobile Asset Tracking and Management**

Enterprises can keep track of the location of the mobile device using the location based tracking feature. There is constant communication between the server and the client which can be used to check the location of the mobile device, thereby also keeping track of the employee's location at all times. Location based features are not only used for keeping track of the Mobile Devices but with additional plug-in, the client software will start pin-pointing out the location of the employees to the other team members (Managers etc.) giving an extra edge in features like arranging meeting places, connectivity, etc.

#### **Remote Lock and Wipe**

The enterprise can make use of the remote wipe feature and erase the entire phone memory and memory card in one click. This is a very useful command in circumstances when there is a report of theft or loss. Remote lock and unlock will help the enterprise manage a secure authentication mechanism on the mobile device. It is also possible to maintain the password policies used by the employees and will be able to unlock the phone after proper authentication of the user.

#### Logging and Reporting

Logging is a method of maintaining a record of all kinds of activity that is performed by an application or device. Logging is a day to day activity and logging of each and every activity running in a device is really a mandate. The main reason to log anything is that many other activities depend on that information. For example, incident handling tasks are heavily dependent on logs for perfection of the report. In the event of any suspicious activity the logs are extrapolated from the mobile device and can be sent to the server along with a report describing the reason for the alert. Logging and Reporting should be a must while implementing MDM for Enterprises.

#### **PRASHANT VERMA**

Prashant Verma is a Security Consultant. He currently leads the Mobile Security Service at Paladion Networks. He has conducted numerous application and network penetration tests. He is the co-author of "Security Testing Handbook for Banking Applications". He has authored security articles for Palisade and Hakin9. He loves to blog and tweets too. He has taken guest lectures and security trainings too. He is a "Digital Evidence Analyst". He also does Java and Android Security Code Reviews. With the predicted growth of mobile devices (enterprise distributed/personal) coming into the organizations and being used for official work, the threats associated to the security of the data in the devices also increases. Mobile Device Management is a good attempt which aims to focus on not only managing the mobile devices remotely but also keeping the device secure. MDM system try to provid an all in one Mobile Device Management Solution for the mobile devices, which is important when the globe is fast shifting from laptops/ desktops to mobiles!

#### Conclusion

Mobile Device security is of the utmost importance to users and organizations distributing or concerned about their employees using the mobile devices heavily for work purpose. It is in user's interest to follow the security best practices, apply the recommendations and harden their mobile to safeguard against the threats which surround their devices. At the same time organizations are worried more about the data security with the device into the picture, more than the device security itself. Data is the real asset for them and they would like to protect it by mandating certain policies for the employees using the mobile devices at work. MDM seems to address most of such issues. However an organization should evaluate an MDM solution that implements the policies they want to implement. Well evaluated and implemented MDM should play an important role going forward to address organizational concerns.

#### **SREENARAYAN A**

Sreenarayan A is a Security Analyst. He currently is Pen testing Mobile Applications and performing Secure Mobile Application Code Reviews at Paladion Networks. He has conducted numerous application and network penetration tests. He has authored security articles for Palisade and conducted Security Trainings at various Corporate and College level events. Partnering with the customers and fortifying their applications against latest Mobile Threats is his primary goal. He is a Certified Ethical Hacker and a Certified Security Analyst.

# Virtualization Security

This document assumes that readers have some operating system, networking, and security knowledge. Because of the constantly changing nature of full virtualization technologies, readers are encouraged to take advantage of other resources (including those listed in this document) for more current and accurate information.

irtualization Security is the need for rapidly growing Virtualized environment. This document tries to explain various factors affecting virtual security, security concerns associated with full virtualization technologies for server and desktop virtualization, and to provide recommendations for addressing these concerns.

\* All forms of virtualization other than server and desktop full virtualization are outside the scope of this document.

#### What is Virtualization?

Virtualization is anything that directly segregates any software resource from underlying hardware or system resource. It is done using Hypervisor, also known as VMM (*Virtual Machine Monitor*). Multiple operating systems, including multiple instances of the same operating system, can share hardware resources.

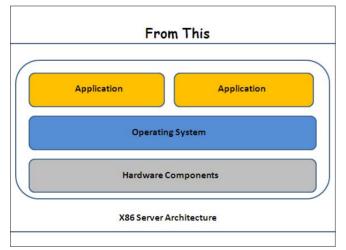


Figure 1. Virtualization

Unlike multitasking, which also allows applications to share hardware resources, the virtual machine approach using a hypervisor isolates failures in one operating system from other operating systems sharing the hardware. Example: Figure 1 and Figure 2.

#### **Virtualization Standard**

DMTF Open Standard for System Virtualization Management (*http://www.dmtf.org/standards/ovf*).

DMTF OVF Rel. 1.1.0 (*http://www.dmtf.org/standards/ published\_documents/DSP0243\_1.0.0.pdf*) The *Open Virtualization Format* (OVF) Specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

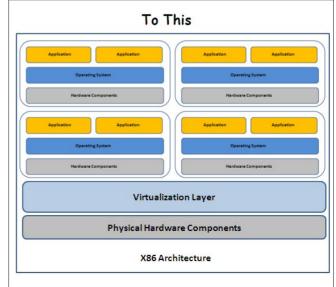


Figure 2. Virtualization

#### What is Virtualization Environment?

The virtualization environment is anything that directly or indirectly touches the virtualization host or virtual machines.

Virtualization Environment is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). There are many forms of virtualization, distinguished primarily by computing architecture layer. For example, application virtualization provides a virtual implementation of the application programming interface (API) that a running application expects to use, allowing applications developed for one platform to run on another without modifying the application itself. The Java Virtual Machine (JVM) is an example of application virtualization; it acts as an intermediary between the Java application code and the operating system (OS). Another form of virtualization, known as operating system virtualization, provides a virtual implementation of the OS interface that can be used to run applications written for the same OS as the host. with each application in a separate VM container.

#### **Types**

#### **Full Virtualization**

One or more OSs and the applications they contain are run on top of virtual hardware. Each instance of an OS and its applications runs in a separate VM called a guest operating system. The guest OSs on a host are managed by the hypervisor, also called the *virtual machine monitor* (VMM), which controls the flow of instructions between the guest OSs and the physical hardware, such as CPU, disk storage, memory, and network interface cards. The hypervisor can partition the system's resources and isolate the guest OSs so that each has access to only its own resources, as well as possible access to shared resources such as files on the host OS.

Also, each guest OS can be completely encapsulated, making it portable. Some hypervisors run on top of another OS, which is known as the host operating system. In full virtualization the hypervisor provides most of the same hardware interfaces as those provided by

the hardware's physical platform. This means that the OSs and applications running within full virtualization do not need to be modified for virtualization to work if the OSs and applications are compatible with the underlying hardware.

#### **Bare Metal VS Hosted Virtualization**

There are two forms of full virtualization. Bare Metal and Hosted Virtualization.

In bare metal virtualization, also known as native virtualization, the hypervisor runs directly on the underlying hardware, without a host OS; the hypervisor can even be built into the computer's firmware.



# hakin9 team!



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

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

### editors@hakin9.org

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

#### We look forward to hearing from you!

In the other form of full virtualization, known as hosted virtualization, the hypervisor runs on top of the host OS; the host OS can be almost any common operating system such as Windows, Linux, or MacOS. Hosted virtualization architectures usually also have an additional layer of software (the virtualization application) running in the guest OS that provides utilities to control the virtualization while in the guest OS, such as the ability to share files with the host OS. Hosted virtualization architectures also allow users to run applications such as web browsers and email clients alongside the hosted virtualization application, unlike bare metal architectures, which can only run applications within virtualized systems.

#### What is Cloud Computing?

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

#### Industry Virtualization, Cloud Implementations

- The Rackspace Cloud
- Amazon Elastic Compute Cloud
- VMWare Technologies
- Windows Azure
- Google App Engine
- SalesForce

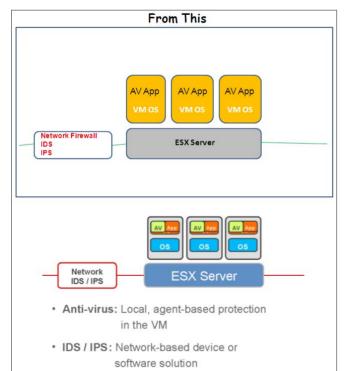


Figure 3. Traditional Security Approach

- Go Grid
- Oracle VM Virtual Box
- · Red Hat Enterprise Virtualization Manager

#### **Better Security**

Industries are adopting Virtualization because of its better security functionality over traditional network components.

- Cleaner and easier Disaster Recovery and Business Continuity Planning.
- Faster Recovery after attacks,
  - Compromised VM's can be reverted to Last known Good Snapshot OR Backup.
  - No need to rebuild from scratch.
  - Better forensics capabilities,
  - Take entire VM as opposed to just one image.
  - Contents of memory can be more easily captured.
  - Patching is safer and more effective,
    - Actually test patches on identical images of critical machine as opposed to the mocked up lab environment.
  - Failed patches can be easily recovered through snapshots or clones.
  - Patch offline virtual machines.
- No need of multiple images for every different piece of hardware in the environment.
- More "Cost Effective" Solution as Security devices can also be virtualized, so internal security becomes a real option because of low cost of software solution versus hardware.

#### **Traditional Security Approach**

This is the traditional security approach towards VM Implementations. It is does not secure VM Implementations as the security risks are different than traditional network setups (Figure 3).

#### **Security Risks in Virtualization**

#### Misconfiguration

As per Gartner security survey biggest security risk for virtual environment is Misconfiguration and mismanagement.

Following attacks are possible in misconfigured environment:

#### **MITM attack against Virtualization Admin**

It is possible if the virtualization admin in the organization lives in the same broadcast domain as other users and the admin is not careful about SSL Certificate implementation in VM. The main problem in VM is VM CLI Tools that do NOT warn about invalid certificates. All these make MITM attacks easier (example: vCLI, VIMA, VMWare Perl SDK).

#### Web Attack against Virtualization admin

It is possible if the admin uses same workstation to browse web that they use to administrate virtual environments. The attack is possible through phishing and other good old web attack techniques.

#### **Dormant VM**

We have 10 VM servers on a virtualized environment and our system administrator is performing a research by adding a new server to the environment and not deleting after his research. As time passes the server may miss some critical patches which could be used by attackers to compromise this research server and take control of others VM servers as the traffic is not filtered between VM's (Considering there is no virtual firewall or the traffic routed through physical firewall). There is also a heavy chance of deploying rogue guests on the virtualized environment.

#### **Resource Contention**

Resource contention can be problem with AV Full system scan on Virtual Environments as existing AV Solutions are not VM Aware. Simulation full AV Scans on the same host causes severe performance degradation. In Physical Environment all machines have independent hardware resource to distribute the load but in Virtual Environment resource are shared across multiple machines thus making it serious problem.

#### **VM Sprawl**

It is very easy to create virtual environments and most of the system administrators use VM technology because it is easy. But this ease of use can cause VM Sprawl which compromises security as vulnerabilities replicate quickly in VM and there is lack of visibility into, or integration with, the virtualization console.

#### **Inter-VM Traffic**

The major problem in Inter-VM Traffic is that the network IDS/IPS cannot see the Inter-VM Traffic; it is invisible to the IDS/IPS. This occurs because the VM operates the traffic in its own little network and the data does not come in contact with the network IDS/IPS.

Network traffic monitoring is particularly important when networking is being performed between two guest OSs on the host or between a guest OS and the host OS. Under typical network configurations, this traffic does not pass through network- based security controls, so host – based security controls should be used to monitor the traffic instead.

#### VM Mobility / vMotion

When one VM Machine moves from one ESX Server to another in the live environment it can cause an issue as the current solutions may not be capable of handling the new location and auto configure themselves accordingly to move the data or traffic through respective VM's. Live migration capability is major issue.

#### Malware / Rootkits

Virtualized environment are prone to various malware and root kits attacks which are specially developed for it. One example is Operation Blue Pill by Joanna Rutkowska. This Root kit has Common HVM layer architecture to support SVM and VT-x, on the fly loading and unloading, support for nested hypervisors on AMD

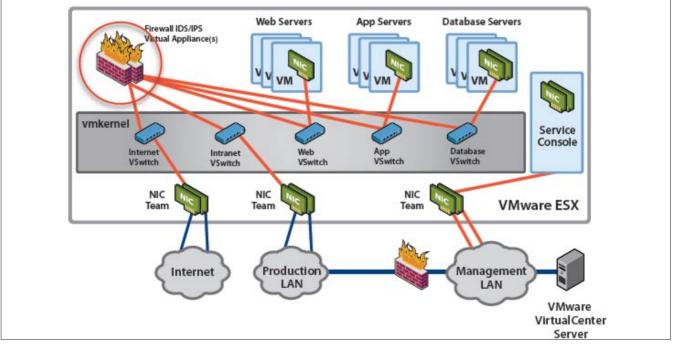


Figure 4. Ideal Virtual Network Breakup

#### Mobile Security 17

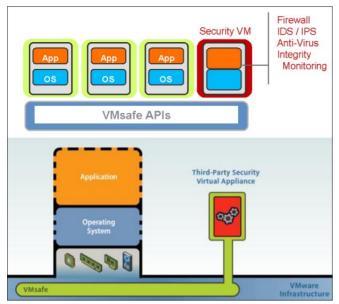


Figure 5. VMSafe API By VMWare

NBP inside NBP inside NBP, Virtual PC inside NBP, etc...

#### **Guest OS Monitoring**

The hypervisor is fully aware of the current state of each guest OS it controls. As such, the hypervisor may have the ability to monitor each guest OS as it is running, which is known as introspection. Introspection can provide full auditing capabilities that may otherwise be unavailable. Monitoring capabilities provided through introspection can include network traffic, memory, processes, and other elements of a guest OS. For many virtualization products, the hypervisor can incorporate additional security controls or interface with external security controls and provide information that was gathered through introspection. Examples include firewalling, intrusion detection, and access control.

#### **Image Management**

Creating guest machine images and snapshots does not affect the vulnerabilities within them, such as the vulnerabilities in the guest OSs, services, and applications. However, images and snapshots do affect security in several ways, some positive and some negative, and they also affect IT operations.

Note that one of the biggest security issues with images and snapshots is that they contain sensitive data (such as passwords, personal data, and so on) just like a physical hard drive. Because it is easier to move around an image or snapshot than a hard drive, it is more important to think about the security of the data in that image or snapshot. Snapshots can be more risky than images because snapshots contain the contents of RAM memory at the time that the snapshot was taken, and this might include sensitive information that was not even stored on the drive itself.

An operating system and applications can be installed, configured, secured, and tested in a single image and that image is then distributed to many hosts. This can save considerable time, providing additional time for the contents of the image to be secured more effectively, and also improve the consistency and strength of security across hosts. However, because images can be distributed and stored easily, they need to be carefully protected against unauthorized access, modification, and replacement. Some organizations need to have a

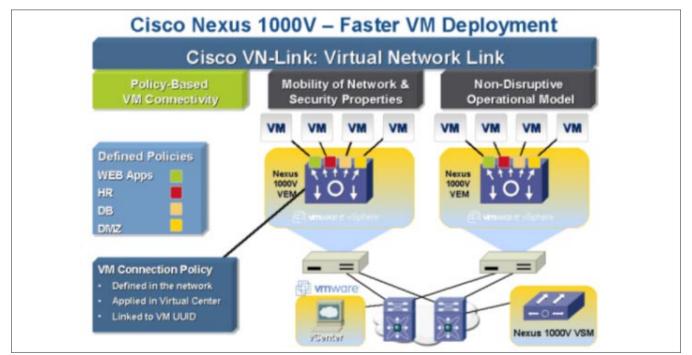


Figure 6. Cisco Nexus 1000V Virtual Switches

small number of known – good images of guest OSs that differ, for example, based on the application software that is installed.

#### Virtualization Security Assessment Tool VASTO Virtualization Assessment Toolkit

The framework consists of tools, libraries, modules, and user interfaces. The basic function of the framework is a module launcher, allowing the user to configure an exploit module and launch it at a target system. If the exploit succeeds, the payload is executed on the target and the user is provided with a shell to interact with the payload. Hundreds of exploits and dozens of payload options are available.

There are a number of open source modules that perform a number of different attacks from hijacking a connection to the virtual infrastructures web-based management consoles against VMware VI/vSphere, Server 1.x, Converter and even Citrix XenCenter to password bruteforcing against VMware and Xen platforms, up to a path traversal attack against VMware ESX, ESXi and Server web interfaces. VASTO even includes an attack against VMware Studio.

#### **VMInformer Assessment Toolkit**

#### **Best Practices for Virtualization**

#### **Hypervisor security**

The hypervisor is a piece of software, in many cases, unless it is integrated directly with the host platform (see the next section). The major virtualization vendors release patches for their products like any other software providers, and the key to mitigating the risk of hypervisor vulnerabilities is a sound patch management process.

Examples of sound patch management practices include maintaining the latest service packs for both guests and hosts, alleviating any unnecessary applications that have a history of vulnerabilities, and applying the latest security rollup patches if and when they are supplied by the virtual software vendor.

#### **Host/Platform Security**

The host platform, which connects the VMM and virtual guests to the physical network, can vary widely in the type of configuration options available. This is largely dependent on system architecture; for example, VMware's ESX Server platform has a number of similarities to Red Hat Linux. Given that many of these systems are able to be hardened significantly, a number of *best practice* configuration guidelines can be applied, including setting file permissions, controlling users and groups, and setting up logging and time synchronization. There are many freely available configuration guides from the virtualization platform vendors, the *Center for Internet Security* (CIS), NSA, and DISA.

#### **Securing Communications**

Securing communications between the host system and desktops or a management infrastructure component such as VMware's vCenter is essential in order to prevent eavesdropping, data leakage, and Man-in-the-Middle attacks. Most of the well-known platforms today support SSH, SSL and IPSec for any communications that are required, and one or more of these should be enabled.

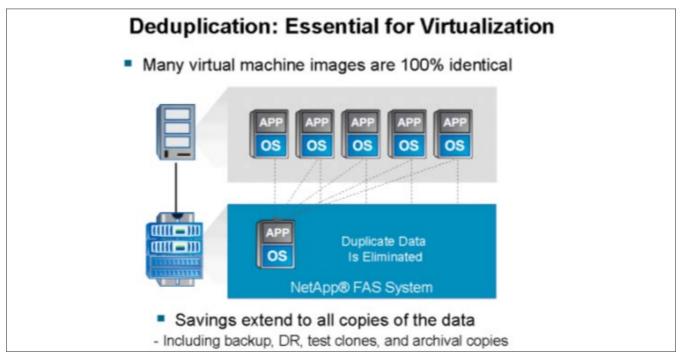


Figure 7. Backup Storage and Protection for Virtualized Environment

#### Mobile Security 19

WPA Cracker is a cloud cracking service for penetration testers and network auditors who need to check the security of WPA-PSK protected wireless networks.

WPA-PSK networks are vulnerable to dictionary attacks, but running a respectable-sized dictionary over a WPA network handshake can take days or weeks. WPA Cracker gives you access to a 400CPU cluster that will run your network capture against a 135 million word dictionary created specifically for WPA passwords. While this job would take over 5 days on a contemporary dual-core PC, on our cluster it takes an average of 20 minutes, for only \$17.

NEW :: We now offer Germany dictionary support, a 284 million word extended English dictionary option, and ZIP file cracking.

Simply upload your network capture, start your job, and WPA Cracker will email you the results within minutes! *Run It* ----

#### Figure 8. Cloud – Virtualization for Penetration Testers

#### Security between guests

One of the biggest security issues facing the virtualized enterprise revolves around the lack of visibility into traffic between quests. Inside a host platform is a virtual switch that each guest connects to - in essence, the host's physical NICs are abstracted into a switching fabric. In many organizations, network monitoring and intrusion detection solutions have long been established to gain visibility and security alerting on critical network segments. With the advent of the virtual switch, all inter-VM traffic on a host is contained entirely within the host's virtual switching components, so visibility and security is severely compromised. Fortunately, most enterprise-class virtualization solutions have traditional Layer-2 switching controls built in, so it's possible to create Mirror ports on the virtual switch to monitor traffic.

#### Security between host/guests

It is necessary to avoid *VM Escape*, where malicious code could *break out* of the VM Guest and execute on the underlying Host. The safest method for protecting against VM escape and other attacks that relate to guest-host interaction is to turn off services you don't need.

Normally virtual machines are encapsulated, isolated environments. The operating systems running inside the virtual machine shouldn't know that they are virtualized, and there should be no way to break out of the virtual machine and interact with the parent hypervisor. The process of breaking out and interacting with the hypervisor is called a VM escape. Since the hypervisor controls the execution of all of the virtual machines an attacker that can gain access to the hypervisor can then gain control over every other virtual machine running on the host. Because the hypervisor is between the physical hardware and

#### Reference

- Virtualization\_Security\_&\_Audit\_SF\_ ISACA\_03\_04\_2010 by Michael T Hoesing CISA,CISSP, CCP, ACDA, CIA, CFSA, CMA, CPA
- mcafee-key-security-ent-arch-wp
- Prism Microsystems VirtualizationSecuritySurvey2010 by Prism Microsystems
- VMWare virtual\_networking\_concepts
   from VMware site

the guest operating system an attacker will then be able to circumvent security controls in place on the virtual machine.

Ideal Virtual Network Breakup Figure 4.

#### **Products for Virtual Environment**

- VMSafe API By VMWare, (Figure 5)
- Cisco Nexus 1000V Virtual Switches, Nexus 1000 supports vMotion / VM Mobility (Figure 6)
- Backup Storage and Protection for Virtualized
   Environment

NetApp BEX – Using Data Deduplication (Figure 7) 11.4) Open vSwitch – Citrix

- VMWare vNetwork Distributed Switch Architecture
- Citrix XenServer 5.6 Free & Open source Hypervisor
- EMC Ionix ControlCenter

•

· EMC Rainfinity File Virtualization Appliance

#### **Cloud – Virtualization for Penetration Testers**

Many companies are now offering cloud, Virtualization for Penetration testers. One example can be Cloud base password cracking service. Many companies are coming forward to provide various security services via virtualization.

#### AMAR WAKHARKAR,

CEH, ECSA, LPT, ISO 27001 LI, CHFI, Consultant – Righshore Security Testing Team – Center of Excellence Amar has 5 years experience working in

the information security consulting field. He holds a CEH, ECSA, CHFI, LPT – EC-



Council, ISO 27001 LI – BSI, SANS Trained Web Application Pen Testing Hands-On Immersion – Level 5 Certifications and a Post Graduation Diploma in E-Business Administration from Welingkar Institute of Management, Mumbai, India. Amar is contactable on amarsuhas@hotmail.com.

### Do You Want to Become a Cyber Security Expert? OR ADVANCE YOUR IT SECURITY CAREER?

- Over Security has one of the largest market shares in IT
- Government & Compliance Regulations are more and more enforced
- Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand

#### THE CYBER 51 EXPERT COACHING FORUM

- Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- Networking with other community members and moderators
- Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more!

#### YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring
- Learn at your own pace at a fraction of the cost of regular courses

#### **CYBER 51 COACHING FORUM**

#### CYBER SECURITY FORUM



#### CONTENT:

- 1. General Topics
- 2. Service Assessment
- 3. Ethical Hacking
- 4. Cyber Threats
- 5. Mitigating Cyber Threats
- 6. Penetration Testing

#### **CYBER 51 INSTRUCTORS**



#### **OUR CERTIFICATION LEVELS:**

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

#### FEATURES



#### **ADDITIONAL FEATURES:**

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

#### WHY CYBER 51?

- Learn whenever you want to
- Dedicated 1-on-1 Coaching
- Information you will not find on public boards
- All Mentors work as Senior Security Consultants
- Frequent updates
- Great Value for money



#### CONTACT US TODAY

CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 0SH, MIDDLESEX, UNITED KINGDOM EMAIL: INFO@CYBER51.CO.UK WEB: WWW.CYBER51.CO.UK

# Android Mobile Security

Android's profound impact on the mobile market has made it a prime target for criminals. And the operating system, which powers over half of the 60.5 million smart phones sold worldwide in the third quarter of 2011, is less safe than its rivals.

Juniper Networks' Malicious Mobile Threats Report shows that Android malware instances increased by 400% between 2009 and 2010, while other platforms remained relatively secure, due mainly to fewer cybercriminals trying to break through their defenses, and in some cases, to stronger security features. Things have only gotten worse this year. Juniper says Android remains a top destination for malware in the mobile space, and that Google likely won't be able to stop the bad guys before things get totally out of hand.

If you are using the mobile not just as a mobile, but more than that like a computer, then be aware of the security issues you face in the mobile device. Also know the security implication of connecting your device to public Wi-Fi network, installing unknown apps into your device, malware attack, voice-call security, some facts of the mobile security and some precautions taken to make your device secured from all these.

#### Security for the apps you install:

An example of app permissions in Android Market.

Android applications run in a sandbox, an isolated area of the operating system that does not have access to the rest of the system's resources, unless access permissions are granted by the user when the application is installed. Before installing an application, Android Market displays all required permissions. A game may need to enable vibration, for example, but should not need to read messages or access the phonebook. After reviewing these permissions, the user can decide whether to install the application.

The numbers out of Lookout Mobile Security have to terrify Android smartphone users:

- Android users are two and a half times as likely to encounter malware today than 6 months ago.
- An estimated half million to one million people were affected by Android malware in the first half of 2011
- Android apps infected with malware went from 80 apps in January to over 400 apps cumulative in June 2011.

*There really is no secure platform. That's the fact*, said Roman Yudkin, CTO of Confident Technologies, a Solana Beach, CA computer security company.



Figure 1. App Download

The fast-paced growth in the Android smartphone market share is responsible for fueling the threats on the Android platform. The latest research, reported in late August by Port Washington, NY based NPD Group, pegs Android at 52 percent of the smartphone market in Q2. iPhone (iOS) share hit 29 percent. BlackBerry fell to 11 percent. Windows Mobile and webOS logged shares below five percent.

That muscular Android growth has attracted cyber criminals. But so far the damages inflicted have honestly been few. Android threats have mainly been nuisances but the threats have become more numerous, elaborated John Engels, an executive in Symantec's Mobility Group.

Leading the criminal parade is what Mahaffey refers to as *repackaging*, a threat that takes advantage of Android's open apps distribution policies where basically any site can set itself up as a distribution hub. This has created a thriving malware industry where criminals are taking popular, typically paid Android apps, then inserting malware, and, finally, making the app free (since it is stolen this involves no costs).

Bad as all this sounds, Mahaffey actually says there's good news here, too because *People are starting to realize they need to take precautions when they use an Android phone*.

One precaution: People have to understand that apps should be downloaded only from an approved short-list of sites, suggested Engels. On that list will be Android Market, possibly Amazon's Appstore, an enterprise's own Android downloads page if it has one and not much more.

The second precaution: Insist that users install and keep updated an antivirus app, suggested Mahaffey (whose company of course is a leader in that niche but there are many other player getting into that space). Android, unlike Apple's iOS, allows antivirus apps to run on the phones and so it is wise policy to require their use.

#### Attack of malware on your android device:

Mobile security researchers have discovered a server located in Germany that hosts more than 1,300 websites dedicated to distributing mobile malware as threat to mobile users continue to escalate.

The revelation comes amid signs of the increasing threat to the Android platform.

The German server hosts five categories of sites, based on the guise they use for distributing the malicious code: Android Market apps; Opera Mini apps, pornographic apps; app storage sites; and others that were inaccessible during the time of checking, said Paul Pajares, a fraud analyst with Trend Micro.

Earlier this week, Xuxian Jiang, a computer scientist at North Caroline State University posted details of a new piece of Android-based malware, dubbed RootSmart. RootSmart is notable because it appears to be one of the first examples of botnet malware targeted at Android handsets.

Once installed, the malware will surreptitiously contact command and control servers and attempt to download a root exploit, known as GingerBreak.

Analysis of RootSmart by Cathal Mullaney, at Symantec, suggests that the malware has been used to send premium rate SMS.

We can see the botmaster is generating anywhere between \$1,600 to \$9,000 per day and \$547,500 to \$3,285,000 per year the botnet is running, said Mullaney.

The malware comes bundled with a legitimate application for configuring phone settings that is available via a third-party app store. It has not yet been spotted in Google's official Android Market.

## Some measures taken by the companies to avoid malwares

With more and more mobile malware being directed at Android-based phones, you'd think the carriers and manufacturers would respond quickly to security and software updates to the underlying operating systems. According to a new survey that doesn't appear to be the case.

We've already been down this road before with PCs. In the early 2000s, malware infecting desktops primarily took advantage of software flaws in Microsoft Windows and Office. In response, Microsoft did issue patches, but the random nature didn't always work – a patch issued late on Friday wasn't installed until sometime the next week. And awareness of the patches wasn't very high. Starting in 2004, Microsoft standardized the process with *Patch Tuesdays*, the second Tuesday of every month, and I would venture to say that compliance is much higher today.

If the first step is creating a regular patch cycle, with mobile that's much harder to do. There are several more variables with Mobile. First, there's the underlying operating system (Android), then there's the unique chipsets and hardware of the handset, then finally there's the individual carrier's features and tweaks. The Android phones on the market may share the same name, but each are unique in significant ways that makes mobile patch distribution much more challenging.

Back in May 2011, Google formed the Android Update Alliance to address some of these concerns. Google partnered with the major US carriers, of course – AT&T, T-Mobile, Vodafone, Sprint, and Verizon. On the hardware side, Google partnered with HTC, LG, Samsung, Sony Ericsson, and Motorola. What these companies agreed to do was update their phones for at least 18 months after the hardware release.

That is roughly the average time a mobile phone customer keeps their phone before purchasing a new one. Before this, the manufacturers and carriers didn't patch the operating systems. If anything the alliance should reduce the time it takes for any Android phone to get the latest version. Apparently, that has not happened.

Flash forward to September 2011. According to the site Androidandme.com, Google is producing updates, but it seems both the carriers and the handset manufacturers aren't pushing these shiny new Android updates out to the end user. Android 2.3, for example, is only available on some – but not all – newer models of popular phones.

The manufacturer with the most Android 2.3 products on the market is HTC, followed by Samsung, then Sony Ericsson. If you add up the total number of phones offered, 32 of them offer Android 2.3, but 23 still run Android 2.2, and 6 still run Android 2.1. So the manufacturers are trying.

In terms of the carriers, here's where the ball gets dropped. The carriers with the most customers, Verizon and AT&T, aren't necessarily better at patching than the small guys. These two carriers still have a number of phones running Android 2.2. Smaller competitors like T-Mobile and Sprint are much better, with more of their phones running Android 2.3 than the big guys. But smaller carriers aren't necessarily the best: Boost, for example, still has phones running Android 1.5, and T-Mobile has one model that is still Android 1.6.

If anything, there doesn't seem to be a coherent pattern among the updates. Newer phones, such as Verizon's 4g HTC Thunderbolt, are still running Android 2.2, while older phones, like the Verizon Motorola Droid X, are running Android 2.3. That doesn't make sense.

Perhaps these numbers will turn around, and the next survey from *Androidandme.com* will show some progress from both the manufacturers and the carriers. And perhaps customers themselves will begin asking about updates to these new smaller form-factor computers – their smart phones and tablets. After all if they're already in the habit of updating their computers regularly, why not expect the same from their mobile devices? But wishful thinking isn't enough.

Even if Google pushed the updates out, the carriers could still block the installation on the handsets. All the mobile parties – Google, the manufacturers, and the carriers – need to work together at solving this problem. The real question is motivation.

#### Tips for you to avoid malwares in your device

An Android Trojan that security researchers brought to light this week – a piece of malware with the potential

to record your phone calls – made some waves on the creepiness scale, though it hasn't been spotted in the wild. This story brings up an unpleasant truth about today's mobile device security: It's sometimes still too hard for smartphone owners to know who to trust.

This Trojan would travel with an app from an untrustworthy source and ask for some unusually generous permissions from you. If you don't download the app and give the permissions, your phone does not get the malware. But how do you know whose apps to trust? Could you be fooled, as hackers get craftier? Apps marketplaces don't yet have foolproof controls to keep malware creators out. *InformationWeek.com*'s Robert Strohmeyer has 5 good pieces of advice.

#### **Lock Your Phone**

This should seem like a pretty obvious tip, but clearly most people need a good reminder, since the majority of smartphone users don't lock their phones at all. Putting a simple passcode on your phone is the first step – and could be the only step required – in protecting a device when it goes missing. But if a ne'er-do-well gets his hands on a phone with no passcode, as Symantec's Wilhelm pointed out, that's as good as an invitation to identity theft.

#### **Use Only Well-Known App Markets**

The most significant security factor that should give Android users pause, said Vamosi of Mocana, is that Android users can download apps from third-party sites not Google whereas iPhone users can only download from the App Store. So it's especially important to download apps from sources that are known for good security.

Wilhelm concurs. Only use app marketplaces hosted by well-known, legitimate vendors for downloading and installing apps, Wilhelm said.

Google's own Android Market certainly qualifies as well known source of apps, of course, but it's by no means a guarantee of any given app's safety. Amazon's Appstore for Android purports to vet apps for security. Wilhem suggests adjusting your Android device's settings to block app downloads from sources other than the Android Market.

#### Scrutinize Every App Download

Regardless of whether an app is free or paid, any given download is a potential threat to your phone's security. Take the time to scrutinize each app's market listing carefully before downloading it to your device.

Pay attention to the name of the app creator, said Wilhelm. An app that purports to be the legitimate version, but has a different author listed should be a definite red flag. An example of this appeared in the Android Market last year, when an author unaffiliated with any bank released apps for Wells Fargo and Bank of America. Those apps are no longer available in the Android Market, but showed up in searches for several months before Google took them down.

Vamosi and Wilhelm both recommend checking an app's ratings for good measure. *A bad guy can still game this*, Vamosi said, but if the app has been available for six months and has recent, positive comments, then it's probably safe.

Additionally, take a good look at the permissions the app asks for, and cancel the download if the app wants access to phone resources that seem disproportionate to its function.

#### **Beware Strange Texts and Emails**

As smartphones become increasingly PC-like, the range of potential threats grows beyond basic malware dangers. Smartphone users should be just as cautious of phishing scams as PC users, and resist opening any links from unknown or dubious sources.

Just like emails, attackers can use text messages to spread malware, phishing scams and other threats among mobile device users, said Wilhelm. So, the same caution users have become accustomed to applying to suspicious emails should be applied to opening unsolicited text messages, too.

#### **Use Mobile Security Software**

As the threat from mobile malware has grown, so has the number of good security offerings in the marketplace. Use one. There are several comprehensive device security apps in the Android Market that can help detect and protect against mobile malware, and it's increasingly wise to use one, according to Vamosi.

Because they involve a large number of mobile devices and users, businesses should be particularly vigilant on this front, according to Jeffrey Wilhem. *Enterprises should consider implementing a mobile management solution to ensure all devices that connect to their networks are policy compliant and free of malware.* 

#### Threat while you are using voice-call

As the story goes, reporters from the tabloid employed a hacking *trick* that relies largely on one basic given: that a lot of cell phone users haven't set a unique security PIN for voicemail access or haven't changed their standard four-digit default one either – often 1234 or 0000. The *trick* entails dialing the cell carrier's general voicemail access number, putting in the subscriber phone number and then the default password. In other words, guessing correctly that the target has left his or her voicemail box essentially open.

Another type of hack is caller ID spoofing and it involves placing a call to the targeted number from the same number. The *spoof* leverages pretty easily obtained software that essentially makes the cell phone carrier network think that an outside call to a phone's voicemail is actually coming from the phone itself – similar to dialing \*86 on your own mobile device to get messages. This type of attack specifically targets mobile users who have not set a voicemail password and, again, it allows easy access to inboxes.

No doubt you see a pattern here. And no doubt you see an easy fix to most voicemail vulnerabilities: Set a security PIN! Or, if you've already got one, make sure it's been updated from the easy-to-guess default.

To protect the sensitive personal information you maintain on your mobile phone, you should consider various options for security control. Your service provider or employer may offer some of these:

#### **For Consumers**

- Install an on-device anti-malware solution to protect against malicious applications, spyware, infected SD cards, and malware-based attacks on the device
- Use an on-device personal firewall to protect device interfaces
- Set a robust, unique password for device access
- Implement anti-spam software to protect against unwanted voice and SMS/MMS communications
- For parents, use device usage monitoring software to oversee and control pre-adult mobile device usage, and protect against cyberbullying, cyberstalking, exploitative or inappropriate usage, and other threats

#### **Enterprise Mobile Security**

Some ideas on how organizations can protect their network and precious, sensitive information from loss, theft or exploitation in today's mobile world:

- Employ on-device anti-malware to protect against malicious applications, spyware, infected SD cards and malware-based attacks against the mobile device
- Use SSL VPN clients to protect data in transit and ensure appropriate network authentication and access rights

#### Steps to follow if you are using public Wi-Fi

If you do allow mobile devices though, you should take the same approach as for any potentially hostile 3rd party network participant. Here are some measures to consider in terms of these mobile devices:

- Lock them down, restrict their access, sandbox them in. Really. Guest networks are long a staple of the security toolbox, and access control should be applied on a white-list, rather than a black-list basis
- Develop a Mobile Portal You may consider providing access to specialised mobile services, instead of letting users roam the holy of holies, the inner sanctum of the intranet. Web-based email services can be configured to prevent local storage of messages and files for example
- Limit functionality Access to Email is definitely an understandable need for a mobile user, but enabling mobile access to billing applications for users who don't require it is just asking for trouble.
- Create a concise Usage Policy and implement it

   Ensure that your users are sufficiently informed not to store company files or data on their phones without proper security controls and measures in place. Implement a punitive procedure for offenders and ensure enforcement

Aside from banning them outright, due to the utter lack of control over mobile clients, the user will be relied on more than ever. You may have to rely on their good judgment, their security awareness and their ability to follow security guidelines.

# Some of the examples of the virus found in android device and antivirus

Some Android malware incidents have been reported involving rogue applications on Android Market. In August 2010, Kaspersky Lab reported detection of the first malicious program for Android, named Trojan-SMS. Android OS. FakePlayer.a, an SMS trojan which had already infected a number of devices. In some cases applications which contained Trojans were hidden in pirated versions of legitimate apps. Google has responded by removing malicious apps from the Android Market, remotely disabling them on infected devices, and scanning newly-uploaded apps for potentially malicious software. Several security firms have released antivirus software for Android devices, in particular, AVG Technologies, Avast!, F-Secure, Kaspersky, McAfee and Symantec.

#### Conclusion

Finally, all the technology is here to make work much easier and faster. Everyhting has both advantages and disadvantages. Technology also has both flaws and benefits. But while using the same, use it in a secured way which should not affect your personalized works. More you use the technology be more secured.



Figure 2. Wi-Fi

#### VINAY GAYAKWAD Profession: Software Engineer Experience: 14 months Position: Technical Lead Company Details: Mpigeon, a startup company based in Bangalore, India. Qualification: Bachelor of Engineering in Computer Science. Date of Birth: 13th may 1987 Hands on experience in technologies: Android, Web technologies, Mobile Web technologies. Email: vinay gayakwad@yahoo.co.in



# ELIMINATE! Mobile App Security Issues

**Comprehensive Mobile Application Testing Solution From Your Trusted Information Security Provider** 

sales@paladion.net

# CRYPTOGRAPHY

# The Ultimate

### Hat Trick that Worked over the Last Couple of

### **Thousand Years**

This tutorial will help you understanding the concept of trojan, dangers created by them, how they can come to your computer, how do they destroy you and your data.

e will discuss that how many types of trojans exist and how they are attached to other applications (wrappers). And finally we'll disclose the most important issue: detection of trojan on your system, some common symptoms and prevention to safeguard your data.

#### What's the trojan?

A Trojan is a program that uses malicious code misguided as some trusted application. Trojans usually come wrapped into other appliactions and are being installed without the user's knowledge. Trojans are malicious pieces of code used to install hacking



Figure 1. Your computer is under siege

software on a target system and aid the Hacker in gaining and retaining access to that system. This makes trojans and their kind important pieces of a hacker's toolkit.

Trojans usually appear to perform a desirable and necessary function but in effect (due to the hidden and unauthorized code) performs functions unknown and unwanted by the user. The user just download these fake programs looking similiar to the original application, and damage is done. This tampered application may be a browser, monitoring program, system virus scanners, registry cleaners, computer system optimizers, or they may be applications like songs, pictures, screen savers, videos, masqueraded email links.

#### The process look like this:

- You execute that software or application; you will find the application running without any visible issues or you might get an error, but once executed the Trojan will install itself and compromise your system automatically.
- Once installed on a system, the program acquires system-level access on the target, where it can perform destructive and insidious tasks. They can leak data out, can cause system crashes or slowdowns. The most dreadful part is this: access generated by trojans can also be used as launching points for other attacks against your system.
- Many trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts.

#### The 7 main types of Trojans

- Remote Access Trojan (RAT): Designed to provide the attacker full control of the infected machine. Trojan horse usually masqueraded as a utility.
- Data Sending Trojan: Trojan horse that uses keylogger technology to capture sensitive data like passwords, credit card and banking information, and IM messages, and sends them back to the attacker.
- Destructive Trojan: Trojan horse designed to destroy data stored on the victim's computer.
- Proxy Trojan: Trojan horse that uses the victim's computer as a proxy server, providing the attacker an opportunity to execute illicit acts from the infected computer, like banking fraud, and even malicious attacks over the internet.
- FTP Trojan: This type of Trojan horse uses the port 21 to enable the attackers to connect to the victim's computer using File Transfer Protocol.
- Security software disabler Trojan: This Trojan horse is designed to disable security software like firewall and antivirus, enabling the attacker to use many invasion techniques to invade the victim's computer, and even to infect more than the computer.
- Denial-of-Service attack Trojan: Trojan horse designed to give the attacker opportunity to realize Denial-of-Service attacks from victim's computer.

In most of the cases trojan comes as a RAT and turns the Victim's computer into a zombie that can controlled remotely. Basically every trojan consists of two parts: server side and client side. The one that resides on the victim's computer is called the server part of the trojan and the one which is on the attacker's computer is called the client part. In order to perform its malicious tasks and function as a backdoor, the server component has to be installed on the victim's computer.

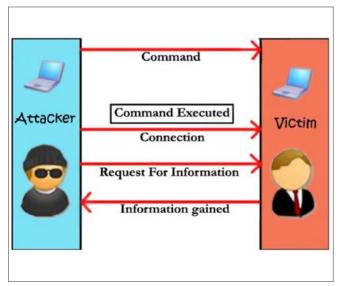


Figure 2. How trojans work?

#### Should I need a wrapper or a binder?

A wrapper is a program used to combine two or more executables into a single packaged program. The wrapper can turn a harmless executable (like a game or detecting tool) to a trojan's payload, the executable code that does the real damage, so that it appears to be a harmless file. Hackers use wrappers to bind the server part of the trojan behind any multimedia or document file. Wrappers are also known as binders.

In most of the cases games or other animated installations are used as decoys because they distract users' attention while the trojan in being installed. The user doesn't notice the slower processing or other unusual things that occur while the Trojan is being installed on the system.

#### The big picture

The main risk is this: a trojan can break through all security polices in a network, because an attacker can get access to a WorkStation with stored network credentials. With these credentials, an attacker can compromise the whole network. There is a type called reverse-connecting trojans that let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. Reverse www shell (in most of the cases) uses standard http. It's dangerous because it's difficult to detect - it looks like a client is browsing the Web from the internal network

C:\Program Files\PEBundle\pebmemc.exe     C:\Program Files\PEBundle\msvcp71.dll	<u>S</u> et Host
<ul> <li>C:\Program Files\PEBundle\pebmisc.dll</li> </ul>	Add <u>M</u> odules
	Add URL
	<u>R</u> emove
	<u></u> lear
Always extract to disk, even if target is newer. Delete this module when host terminates. Register ActiveX control Advanced bundle (Do not write module to disk)) xtraction Destination {Executable's folder}	Save project
	Bundle

Figure 3. Wrapper PE Bundle

File Options Process View Help						
■ A → Ø						
Process /	Protocol	Local Address	Remote Ad	State	^	
ALG.EXE:2344	TCP	CF22877W:1036	CF22877W:0	LISTENING		
🗂 AppleMobileDeviceServi	TCP	CF22877W:27015	localhost1030	ESTABLISHED		
AppleMobileDeviceServi	TCP	CF22877W:27015	CF22877W:0	LISTENING		
Cvpnd.exe:3432	TCP	CF22877W:62514	CF22877W:0	LISTENING		
Cvpnd.exe:3432	UDP	CF22877W:62514	н. н			
firefox.exe:5948	TCP	CF22877W:1073	localhost1074	ESTABLISHED		
firefox.exe:5948	TCP	CF22877W:1074	localhost1073	ESTABLISHED		
firefox.exe:5948	TCP	CF22877W:1063	localhost1062	ESTABLISHED		
firefox.exe:5948	TCP	CF22877W:1062	localhost1063	ESTABLISHED		
firefox.exe:5948	TCP	cf22877w.edfac.unim	89.202.172.10	ESTABLISHED		
firefox.exe:5948	UDP	cf22877w.edfac.unim	ж.ж			
firefox.exe:5948	UDP	cf22877w.edfac.unim	x. x			
firefox.exe:5948	TCP	cf22877w.edfac.unim	www.proxy.uni	ESTABLISHED		
firefox.exe:5948	TCP	cf22877w.edfac.unim	www.proxy.uni	ESTABLISHED		
firefox.exe:5948	TCP	cf22877w.edfac.unim	wwwproxy.uni	ESTABLISHED		
firefox.exe:5948	TCP	cf22877w.edfac.unim				
iTunesHelper.exe:124	TCP	CF22877W:1030	localhost:27015			
keyacc32.exe:1340	UDP	CF22877W:1039	*.*			
LSASS.EXE:1508	UDP	CF22877W:isakmp	×.×			
LSASS.EXE:1508	UDP	CF22877W:4500	*.*		~	

Figure 4. TCPView in use

#### Some common symptoms

- Wallpaper and other background settings autochanging
- Mouse pointer disappears
- Programs auto-loading and unloading
- Strange window warnings, messages and question boxes, and options being displayed constantly
- e-mail client auto sending messages to all on the user's contacts list
- Windows auto closing
- System auto rebooting
- Internet account information changing
- High internet bandwidth being used without user action
- Computer's high resources consumption (computer slows down)
- Ctrl + Alt + Del stops working

All above are indications of a trojan attack. In this case the only thing you can do is to check the applications which are making network connections with other computers. One of those applications will be a process started by the trojan.

#### Detection

You can also use the software named process explorer which monitors the processes executed on the computer with its original name and the file name. As there are some trojans who themselves change their name as per the system process which runs on the computer and you cannot tell the difference between the trojan and the original system process in the task manager processes tab, so you need a process explorer such as TCP View.

TCP View is a native Windows application that will show you detailed information about all TCP (*Transmission Control Protocol*) and UDP (*User Datagram Protocol*) endpoints on your system, including the local and remote addresses and status of TCP connections.

- TCP View also reports the name of the process that owns the endpoint.
- Active connections will appear in greenand you may right-click on the check the properties of the application.
- Once you got hold of the trojan application, you can disable the active connection and the running process.
- There is an option (which is recommended) to delete the physical application file. This will make you recover from the attack. There is a caveat though: in certain cases where the trojan is part of a system-critical file you'll set for hard times since the whole computer collapses immediately.

#### Countermeasures

Most commercial antivirus programs have anti-trojan capabilities as well as spyware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and trojan programs before they can cause damage. Once a system is infected, it's more difficult to clean, but you can do so with commercially available tools. It's important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, port monitoring tools can identify ports that have been opened or files that have changed. The key to preventing trojans and backdoors from being installed on a system is to not to install applications downloaded from the Internet or open Email attachments from untrusted parties.

#### **ZSOLT NEMETH**

Zsolt NEMETH is a serial entrepreneur who set up businesses in cyber security. His main interests are cryptography and network security. He founded MDS Ltd in the UK. He has done consulting



and penetration testing for financial institutions and built up bespoke solutions for them. Meanwhile he was the leader of a team of cryptographers that worked on creating an elegant cipher that will potentially solve some of the significant issues of the Vernam Cipher (aka one-time-pad). After selling MDS Ltd he has founded a holding that has scouted, bought and licensed technologies out.

Now he runs Camphora Llc with offices in Hungary and Luxemburg. He is doing ethical hacking and intrusion analysis for SMEs and a few selected big companies.

Zsolt holds a Master of Science degree in Economics from Szechenyi Istvan University and a Master of Science degree in Applied Mathematics from Ecole National Superieure, Paris. He is fluent in Hungarian, French and English.

He is a frequent speaker at conferences on fast symmetric ciphers and SCADA systems security.



Printer F

ATURES:

A.

✤ Covert tunneling SSH access over 3G/GSM cell networks NAC/802.1x bypass and more!

ndustry/

112

Sun:

Discover the glory of Universal Plug & Pwn

@pwnieexpress.com

**PWNIE EXPRESS** 

t) @pwnieexpress e) info@pwnieexpress.com p) 802.227.2PWN

THE

# INTERVIEW

# Interview with Scott Gordon

ForeScout enables its customers to unleash the full power of their network through enterprise-class security and control. ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. Because security solutions are easy to deploy, unobtrusive, intelligent and scalable, they have been chosen by more than 1,000 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. Headquartered in Cupertino, California, ForeScout delivers its solutions through its network of authorized partners worldwide. Learn more at www.forescout.com.



# Bring your own device (BYOD), is gaining a lot of steam these days, why is that the case?

Many employees use their personal devices at home, work and on the road. In addition, organizations need to provide network access to contractors and guests, who often arrive with their own personal devices. Although these devices are ultimately connecting to the network and introducing risk, IT Security must consider the productivity gains to be had. Security policies and practices need to be acceptable, unobtrusive and efficient for both users and IT, while fortifying necessary security mechanisms. What's important is to have realtime visibility and control over your network and the mobile devices connected to it, as well as a flexible way to enforce security policy.

So we define BYOD as the extent to which an organization denies, tolerates, sanctions and endorses the use of personal and mobile devices on their network and the technical controls to manage operational risks.

#### With employees being assigned Mobile devices as part of their work, how challenging is Mobile Device Management?

Before *Mobile Device Management* (MDM), companies already had processes for phones and phone management – most companies still do. With companyassigned and personal mobile devices, companies can leverage MDM for provisioning and configuration, billing and inventory management, as well as containerization and encryption to support security. Cloud based MDM solutions appear to be among the least complex to implement, albeit the subscription services are not inexpensive.

It's a different story with BYOD. Personal smartphones and tablets can do so many things and provide so much value in terms of productivity gains that companies need to get a grip on managing these devices from a broader security perspective. And MDM typically concerns smartphones and tablets, but there are plenty of users with notebooks. Other security mechanisms include *Virtual Desktop Interface* (VDI) or mobile application wrappers.

Even if a company has already deployed or intends to deploy an MDM system or other technologies to enable personal mobile device use, they still face security gaps unless they gain broader visibility and control over all network access, which industry analysts, and we feel NAC is best suited to provide.

# Why do you consider Network Access Control vital for protecting various mobile risks related to data within enterprises?

Many of the security risks that have long been a concern for laptops and notebook computers exist in mobile devices such as smartphones. Device mobility, wireless access, personal applications and the high risk of lost or stolen handhelds creates a need for added defenses against data loss, unauthorized access and malware.

Network Access Control has proven to be a best practice to manage data leakage risk, data privacy

issues and advanced threats brought about by increased user, contractor and guest connectivity, the influx of personal mobile devices on corporate networks and the move to support BYOD.

Network access control is an essential feature for mobile security. While inventory and software management are important, the means to enforce security policies based on identity, device (smartphone, tablets and notebook PC), configuration, security posture and network activity are crucial features for mobile security. These are capabilities available from NAC tools that are incomplete in MDM tools.

CounterACT today can identify all the personal and managed notebooks, smartphones and tablets and can apply broad policies – say to only allow web access for some and email access for others. With our new product, ForeScout Mobile, we introduce two plug-in modules to CounterACT. One module extends the level of control and remediation we can apply natively for Apple iOS and Android. And an MDM module offers broader coverage and even more advanced capabilities that leverage the customer's MDM platform. This gives organizations a flexible way to support their requirements wherever they sit on the BYOD maturity spectrum.

## Who are some of your competitors in the field of Mobile Security and Management?

IT organizations have alternatives. There is WAP to control the wireless access – which is OK for a guest network, but is not really that extensive. There is VDI, which can directly tunnel a user to a resource or application, but the user experience varies greatly, especially when using smartphones. Another option would be a mobile application wrapper that could secure the connection and application for the employee.

For really advanced protection, there is mobile device management. MDM offers great provisioning, inventory and cost management capabilities. The key factor is how intrusive the MDM mechanisms are, given the end user, device and risk. From a security perspective, the policy enforcement, encryption and containerization settings are an extremely strong approach for smartphones and tablets. MDM does not cover personal notebooks. MDM is also a heavy application and not so inexpensive per month, in terms of per device price tag. With NAC, and specifically CounterACT, we are in a great position to enable any of these technologies. We offer a broader, more unified view and level of control for the security operator. So really, ForeScout doesn't compete with WAP, VDI or MDM.

Tell us more about ForeScout Mobile and some of its top features? Does ForeScout Mobile support all platforms (iOS, WebOS, Symbian etc)?



In his business experience, Bryden say his involvement has always been as a

major shareholder and top executive, but in a company based on the vision of other people who he believed knew what they were doing, and whose dream had

commercial value.

Prophers. "I arrived here because of their invokation to find a warp ho invokation to find a warp ho invokation of the state of the state and the state invokation of the because a state invokation of the state of the sense full these as the because a state invokation of a hockey ground the condensity with the state of the sense of the state of the because a state of the state of the because of the sense of the state of the state of the sense of the state of the because of the sense of the state of the because of the sense of the state of the state of the sense of the state of the because of the sense of the state of the because of the sense of the state of the because of the sense of the state of the because of the sense of the sense of the state of the sense of the sense of the because of the sense of the because of the sense of the sen

> To have three young shiften in the main a with Sandy Dorting the week identy are a tot of themic, but the young 1 like to be with an entropy of the works of the source were than i would like to go to di had more avenuing free bod and works and the source of the source of the source of the bad more woungs free bod and the source of the source of the source of the source of the bad more woungs free bod the source of sourc

press done on the workner-dd, with workner-dd, with workner-tripe back to Cape Brents to oblight and when trends and donest Trendsant, A bit of tennis, weinting and history a sandvicture and bit were, and bit weintight and bit

addig old motionals, is just animal examples of the set of the case of Weeks of the case of Weeks of the set the set of the set of the set of the set the set of the

Haring

The constainty work that point if well-come the schemps, and i will be surprised if at that torus the search semasthing size to "says likeydam. Ha

### Security develo

Chryselle-ITS plans to increase its global ecommetrie market abare with a successful learth round of venture capital familing tailying more than 135420 soliton.

Securing virtual private net servicing and public key links structures (PDD) in a govering concern, in business transactions beginne (commonplace on the Web Chrysalls improves root key security of these network links structures with cryptographs andware.

Move Baker, president and CEO of Chryselle, asys rese that Y2K is over, security has been and the important base in 2008 and the proving Chryselle contenent

president and a says new that actly has become more to 2004 and

Join our Exclusive and Pro club and get: HEHINS Hakin9 one year subscription HEHINS Full page advertisement in Hakin9 every month! HEHINS Information about your company send to over 100,000 Hakin9 readers!

More information at en@hakin9.org

#### www.hakin9.org/en

# INTERVIEW



There are a lot of advantages to ForeScout Mobile when it comes to BYOD and mobile security. The key is enabling the security professional to have one powerful tool, one integrated console, to see and control in realtime all devices, wired and wireless, managed and personal, PC and mobile. And that's what we offer.

The CounterACT platform is able to identify and apply a basic policy for network access across the major handheld platforms including iOS, Android, WebOS and Symbian.

The ForeScout Mobile Security Module for Android offers a native Android app that can identify and apply access policies based on the user, the device, the applications and how the device is behaving on the network. The Module for iOS also offers these capabilities, but uses Apple's MDM and push notification services – so there is no app. And on iOS, we offer more remediation options such as remote wipe and lock, requiring apps or passwords, controlling Wi-Fi access and more.

Our ForeScout Mobile MDM Module will provide customers even broader coverage and remediation options leveraging their MDM platform. So organizations can support personal and mobile devices at work to the extent they need, while also enabling staff to reduce inherent security risks.

# Which industry will benefit the most with the release of ForeScout Mobile? What is the best approach for the customer?

ForeScout Mobile Security has very broad appeal and is not industry specific. It really comes down to the need to control network access, protect sensitive data and enforce policies. We see companies in all industries, as well as government agencies, benefiting from ForeScout Mobile Security.

## Are you partnering with anyone on the ForeScout platform?

ForeScout Mobile Security and ForeScout Mobile MDM were fully developed in house. We see a tremendous need in the marketplace as organizations ramp up their mobile security initiatives to support BYOD. It's not uncommon for an organization underestimate the number of to information workers using consumer devices to access business applications, by as much as 50%, so mobile security has become an integral component of a security program. Our ForeScout Mobile MDM module, available in a few months time, is based on our work with leading MDM vendors for specific interoperability, similar to what we have

done to support a customer's existing security and network infrastructure.

#### What size organizations are you targeting?

ForeScout offers significant security and economic value for the customer. What is interesting is that our customers and prospects are telling us that they want to offer a tiered mobile security strategy. Think of it as Mobile Security Rightsizing. Not all users will be allowed to use their personal mobile devices to access anything - most will be restricted to the Internet. Some will only need access to a certain application possibly using VDI or an app wrapper. A portion of specialized users, devices and apps will need more advanced security, which requires MDM. And the majority of other users will just need basic security, which includes Internet access, access to common applications (such as email) and modest configuration policy such as white listing, black listing, password management, etc. - but no provisioning or containerization.

This allows companies to deliver the appropriate level of required mobile security at an optimized expenditure of both capital and resources. Our ForeScout Mobile solution offers the right flexibility, features and price to directly support BYOD while enabling tiered mobile security services.

by Aby Rao

# CODENAME: SAMURAI SKILLS COURSE

# Penetration Test Training Samurai Skills

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites, Networks, Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos ( Course Updated Regularly )
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time, any where)
- Our Course is Totally Different from Other Courses ( new Techniques )

# INTERVIEW

# Interview with Arun Sood

Dr. Arun Sood is Professor of Computer Science in the Department of Computer Science, and Co-Director of the International Cyber Center at George Mason University, Fairfax, VA. His research interests are in security architectures; image and multimedia computing; performance modeling and evaluation; simulation, modeling, and optimization.

He and his team of faculty and students have developed a new approach to server

security, called Self Cleansing Intrusion Tolerance (SCIT). We convert static servers into dynamic servers and reduce the exposure of the servers, while maintaining uninterrupted service. This research has been supported by US Army, NIST through the Critical Infrastructure Program, SUN, Lockheed Martin, Commonwealth of Virgina CTRF (in partnership with Northrop Grumman). Recently SCIT technology was winner of the Global Security Challenge (GSC) sponsored Securities Technologies for Tomorrow Challenge. Dr Sood leads a university spin-off called SCIT Labs Inc, which is commercializing SCIT technology under license from GMU.

Since 2009 Dr. Sood has directed an annual workshop on Cyber Security and Global Affairs with Office of Naval Research support. The 2009 workshop was at Oxford, 2010 in Zurich and 2011 in Budapest. He was awarded grants by NATO to organize and direct advance study institutes in relational database machine architecture and active perception and robot vision.

Dr. Sood has held academic positions at Wayne State University, Detroit, MI, Louisiana State University, Baton Rouge, and IIT, Delhi. His has been supported by the Office of Naval Research, NIMA (now NGA), National Science Foundation, U.S. Army Belvoir RD&E Center, U.S. Army TACOM, U.S. Department of Transportation, and private industry.

Dr. Sood received the B.Tech degree from the Indian Institute of Technology (IIT), Delhi, in 1966, and the M.S. and Ph.D. degrees in Electrical Engineering from Carnegie Mellon University, Pittsburgh, PA, in 1967 and 1971, respectively.

His research has resulted in more than 160 publications, 4 patents, 2 edited books.

#### What's your background?

All my degrees are in Electrical Engineering – BTech (IIT, Delhi); MS and PhD (Carnegie Mellon). My dissertation research was in the area of control theory and motivated by the use of "small" computers like the early DEC mini-computers (PDP series). Currently, I am a Professor of Computer Science and Co-Director of the International Cyber Center at George Mason University at Fairfax, Virginia. My research is focused on modeling and designing resilient architectures; scalability of resilient systems; and metrics to evaluate resilience. I have worked for process engineering and consulting companies for about 10 years and have had academic

appointments at Indian Institute of Technology, Delhi (IIT, Delhi), Louisiana State University, and Wayne State University.

# When did you made the decision to get involved in cyber security?

For the last 10 years my research interests have shifted towards cyber security, and especially on recovery strategies. I got introduced to the complexity of the issues during a consulting assingment for a bank. This was the first time that I realized the expenses related to IDS alert processing. I see cyber security having many open and challenging problems, and yet opportunity to apply common sense solutions. I like to work at the edge of practice and research and cyber security provides an interesting place to be.

#### How do you stay up-to-date in cyber security? What sources do you use?

Conferences, workshops, technical publications. On line resources. Some IEEE publications that focus on this topic are well worth reading. IEEE Security and Privacy is a magazine style publication, that is designed for lay public. IEEE Transactions on Dependable and Secure Computing and IEEE Transactions on Information Forensics and Security are two key research publications. A number of papers provide information about the current status of the cyber incidents and cyber threat. Periodically I look at Financial Times, New York Times, SC Magazine, Wall Street Journal, Washington Post, Wired.

Do you believe that Moore's law will continue at its current rate and at one the point an evolution in cyber security will be necessary in order to protect digital assets in light of the processing evolution?

Moore suggested that transistors per chips will double every 2 years. I think that this will continue for sometime. Multiple cores per chip are helping achieve this. However, I expect that more compute cycles will be required to protect the digital assests. At some point more hardware assets will be used to manage key security problems like attribution and assurance.

#### Does the increasing use of distributed computing, new algorithms and new threats (especially APT) affects the way we do cyber security? How?

Cyber security can no longer rely on reactive approaches alone. It is necessary to take a information risk management view to the problem. Our solutions must include information sharing, proactive and threat independent approaches, agile defense approaches and continuous monitoring of the system status. We also need new approaches to forensics – maybe we should design systems with the expectation that forensic analysis may be necessary, thus reducing the time for trace back and other forensic analysis.

#### Is the growing use of computers and digital data leading to system downfall? At what degree are we dependent on digital information and processes?

We are increasingly dependent on digital info. I think that we are increasingly suffer from info overload. Take for example in the publishing world. The same article is replicated and published in many venues. If you subscribe to several publications, then the human has to act as the deduplicator. The same is true of the search results.

#### What are your main research topics?

The cyber security problem is an area of intense research. The current focus has been on reactive methods that are expected to defend against all the attacks. Enterprise systems process millions of transaction per day, and failure in even .01% of the cases provides for a challenging situation. This experience is supported by theory – detection theory suggests increasing probabilit of detection will increase probability of false positives which requires more cyber security analyst man hours to resolve. This reasoning, lead us to 3 principals that drive our research:

- Intrusions are inevitable
- Once in the system, intruders stay for long periods days, weeks and months
- Our current servers are sitting ducks

In my research I have focused on reducing the losses that are induced by a successful attack. We call this intrusion tolerance, and have developed SCIT – Self Cleansing Intrusion Tolerance architecture. SCIT uses a recovery oriented approach to achieve our goal of limiting losses. SCIT reduces the exposure time of the server to the internet, and restores the server to a pristine state every refresh cycle. In this way we reduce the time the bad guys have to induce losses. The limited goal of our research is to increase the work effort required by the attackers.

## What is your opinion of server security and how do you design secure systems?

Our current servers are sitting ducks. The bad guys install malware on the server, and this spreads the infection in the system. We need systems that will delete the malware as quickly as possibl. For this reason, I think that servers should be regularly taken offline and restored to a pristine state. The time the servers are exposed to the internet is called the server Exposure Time. If we can keep the Exposure Time low and restore the server to a pristine state at the end of this period, then the malware will have only a limited amount of time to do damage. We have built servers with an exposure time of 1 minute.

It is generally believed that a defense in depth approach is appropriate. I agree. If we can make the layers independent of each other then that will have additional protection characteristics. The SCIT technology easily integrates with the existing infrastructure without interfering with the existing security subsystems.

# What do you see as the future of cyber security?

Today we are mostly focused on Information Assurance – primarliy technology and policy issues. I think that there needs to be more focus on human factors, low cost solutions, and policy. In addition, Attribution deserves much more work.

#### In terms of players in cyber security, what do you expect? Small companies, lonely hackers, organized crime, cyber warriors? I assume this industry is dependent of financial resources or lack of them. Is it possible to small companies to prevail?

Most of the headlines are about successful attacks on large companies, especially financial services companies, and defense and government offices and contractors. However, small companies have also been hacked. Hackers have stolen data, and stolen commercial and business information like forthcoming bids which makes small companies particularly vulnerable. Rural comunities and small towns are also vulnerable to hacking. At the same time emerging nations are getting access to larger bandwidths and access to international traffic, with more danger of being targets and orginators of cyber attacks. For such organizations, the current approaches are too expensive, and low cost alternatives have to be developed.

Ont he other hand, small firms focused on a specific problems and solution can be very effective. However, usually enterprise solutions require extensive testing and hence the support of large companies. For successes in this space it in necessary to form strategic partnerships between large companies and small companies; between government and small companies; and this information sharing with the entrepreunerial drive of small companies will yield major dividends.

# What do you think about the future generation of cyber warriors and hackers?

Cyber warriors and hackers deserve more respect. We should not underestimate the value provided by the ethical hacking community. We need to build more trusting environments. We also need to switch from penetration testing, to measuring the consequences of bad guy actions.

# What's wrong with penetration testing? Do you feel it gives companies a fake confidence?

Penetration testing provides the status of the system at one point in time, New vulnerabilities are constantly being exposed, and thus systems that have recently successfully passed a penetration test, will find that they are vulnerable, In this sense the penetration test gives a false sense of confidence.

#### There are people who predict doomsday scenarios. Is it likely that eventually we get to a cyber cold war? What would it be like?

To some extent this has already occured in limited environments. The twin objectives of standardization and cost reduction, reduces the variety or hardware and software and makes all our systems vulnerable. There is a risk at the boundary of the cyber – physical connected systems. Protecting the national financial infrastructure from attack is critically important especially countries that are leading users of internet and mobile systems. Emerging countries are pushing for using mobile devices to perform financial transactions, especially low value monetary transactions. Most Critical Infrastructure Protection projects include water and electric utilities.

#### Has it already started?

It appears that Estonia and Georgia events are examples of code ware. There are reports of the Israel adn Palestinan conflict leading to cyber security incidences. There is widespread speculation that the Stuxnet attack on the Iranian nuclear infrastructure was linked to a foreign government.

## Are you optimistic or pessimistic of our ability to mitigate the cyber threat?

On the whole I am optimistic that the world will successfully manage and navigate through the cyber threat.

by Zsolt Nemeth and Jeffrey Smith

# zebNet

### Protect your important data before it is too late!



No-one likes to consider the worst case scenario, but are you prepared for a loss of all computer assets?

Computers are easily replaced, but your critical data and files are something money can't buy.

zebNet offers powerful, easy-to-use and leading backup solutions for all major web browsers and email clients which are designed to protect you as much as possible.

With a backup solution from zebNet you will always be protected from the worst case scenario at an affordable price, starting at just \$9.99

#### Visit www.zebnet.us to be protected!

#### Highlighted features at a glance:

- Fast and reliable backup and recovery
- Self-restoring backup files
- Backup reserve copies
- Backup to any FTP server
- Scheduled backups on a regular basis
- Data migration between different computers
- Support for portable editions of your web browser/email client
- Create a portable edition of your web browser/email client
- And many more



#### **Exclusive limited-time offer for you as a Hakin9 subscriber:**

Get a **50% DISCOUNT** off any zebNet backup solution you wish by simply entering the discount code "**Hakin9**" in our store at **www.zebnet.us** 

zebNet backup solutions are available for Microsoft Outlook, Windows Live Mail, Microsoft Internet Explorer, Mozilla Firefox, Mozilla Thunderbird, Mozilla Seamonkey, Google Chrome, Opera, Apple Safari, Postbox and IncrediMail.



# **Classroom & Distance Learning Programs on**

# Information Security & Ethical Hacking

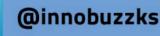
# Web Application Security

# Network Security

# Exploit Development

# Reverse Engineering & Malware Analysis

www.innobuzz.in mag@innobuzz.in





/innobuzz



/innobuzz





May 20th - 25th @ Okura Hotel Amsterdam

# **REGISTER ONLINE**

http://conference.hitb.org/hitbsecconf2012ams/