# HAKIN9 EXTRA

# Mobile Hacking

WINDOWS PHONE 8 APPS

PENTESTING ESSENTIALS

MOBILE PHONE SPYING, DETECTION AND COUNTERMEASURES

MOBILE NETWORK TRAFFIC ANALYSIS

Issue 02/2013 (20) August ISSN: 1733-7186

PLUS

WHEN IS TABLET SAFER THAN PC?

*“We specialize in Information Security Solutions including Penetration Testing, Forensic Analysis and Computer Investigations to a diverse range of clients worldwide”*

Cyber Investigations N.I. Ltd.

Northern Ireland Science Park
Queens Road
Queens Island
Belfast BT3 9DT
United Kingdom

Email:
info@cyberinvestigationsni.com

Telephone:
+44(0)28 9079 6983

*For a free security consultation, then please contact us by either mail or phone and one of our security experts will be happy to assist you.*

Please visit us on: [www.cyberinvestigationsni.com](http://www.cyberinvestigationsni.com)

HAKIN9 team

**Editor in Chief:**
Julia Adamczewska
*julia.adamczewska@hakin9.org*

**Editorial Advisory Board:**
Hans van Beek, Peter Harmsen, Leighton Johnson, Casey Parman, Dan Smith

**Proofreaders:** Julia Adamczewska, Krzysztof Samborski

*Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.*

**Publisher:**
Paweł Marciniak

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

**Product Manager:**
Krzysztof Samborski
*krzysztof.samborski@hakin9.org*

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

**Marketing Director:**
Julia Adamczewska
*julia.adamczewska@hakin9.org*

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

**DTP:**
Ireneusz Pogroszewski

**Publisher:**
Hakin9 Media Sp. Z o.o. SK
02-676 Warszawa, ul. Postępu 17D
NIP 95123253396
Phone: 504927626
*www.hakin9.org/en*

Whilst every effort has been made to ensure the highest quality of the magazine, the editors make no warranty, expressed or implied, concerning the results of the content's usage. All trademarks presented in the magazine were used for informative purposes only.

**DISCLAIMER!**
**The techniques described in our magazine may be used in private, local networks only. The editors hold no responsibility for the misuse of the techniques presented or any data loss.**

**Dear Readers,**

*And here it comes – the edition on Mobile Hacking. In this issue we will focus on hacking/security matters of those tiny computers everyone has with him or her almost everywhere and most of the time.*

*When it comes to an ordinary PC or laptop safety it is no wonder to anybody that such devices should be protected against viruses, hackers and all potential threats. But in their everyday life people tend to forget about possessing a little computer that is used for calling, texting, sending e-mails, surfing on the Net, working and whatever other stuff they do on their mobiles. They can be hacked too, so it is well worth finding out how, and how to counteract.*

*So let's start with the Attack section and the article 'Mobile Phone Spying, Detection and Countermeasures' providing fine examples of these. The other article in this section deals with Sim Card Hacking. Then from the Defense section you will learn about the Windows Phone 8 security features and pentesting, and also what can be mobile network traffic analysis used for. Because many of our target readers have their families and children, they will definitely benefit from the article 'Mobile Kids Safety' written by the specialist involved in Online Child Safety program, who is also interviewed in this issue. In our Extra section there is somewhat controversial paper titled 'When is a Tablet safer than PC?' So let's find out the author's answer and check if you agree...*

*Hakin9's Editorial Team would like to give special thanks to the authors, betatesters and proofreaders.*

*We hope our effort was worthwhile and you will find the Hakin9 Mobile Hacking issue appealing to you. We wish you a nice read.*

*Julia Adamczewska*
*and the Hakin9 team*

## ATTACK

## DEFENSE

## PLUS

## INTERVIEW

# Mobile Phone Spying, Detection and Countermeasures

Mobile Security have been a much discussed field in IT security due to the wide spread use of mobile devices. This article aims at exposing Mobile Phone Spying (or Track and Trace), how it's done with reference to concept and available tools, Detection and Countermeasures. It presents Mobile Spying in its real offensive light so that IT security professionals can put in proactive measures to combat this threat.

Over the past two decades, improvements in engineering (both software and hardware) in the mobile computing space has given birth to high end mobile devices having capabilities of PCs. Initially limited to voice communication, mobile phones have become smarter and smarter. Higher processing speed, larger screens, touch input features, wireless facility and GPS location awareness have paved the way for even more improvements in deployable custom and third party mobile Apps. The proliferation of software and the advancement in Engineering have increased the attack space for mobile devices over the years- ranging from simple to more advanced attacks. Despite this, mobile devices form the fastest growing consumer technology with worldwide sales exceeding 650 million in 2012 alone with brands like Apple's iPhone enjoying "Super" patronage. Human life tends to revolve around the mobile phones.

In addition to their use for conventional services like Voice communication and Web surfing, mobile devices now store tremendous amounts of financial, personal and commercial data that is juicy enough to attract both targeted and mass-scale attacks. Over the years, we have seen various attacks been launched at mobile devices; some OS independent while others are device dependent. Threats like Viruses, Worms, Trojans and single target spying applications have gained ground; Buffer overflow (iOS about 2007), SMS fuzzing (iOS 2009), Application Permission escalation (Android 2010), OS rootkit (Android 2010). Though compared to their PC counterpart we are yet to see threats like rootkit (except on Android devices in 2010), distributed spyware and self-propagating worms – worms availability requires user interaction to propagate. New Threats are growing at 42% yearly though. We can't stop here without mentioning mobile phone and tablets theft.

Of all the attacks launched at mobile devices (Smart Phones and Tablets) the most common is "Mobile Phone Spying" for obvious reasons. One is the ease at which this can be done (availability of tools and the low technical know-how needed to execute an attack) and the motivation for such action ranging from emotional to financial or simply for outright damage as a phone wipe can be executed remotely with relative ease.

## Mobile Phone Spying

### The Concept

A spy attack to mobile phone varies in concepts and means, but there seems to be a common factor underlying most methods. The most common is the use of a client -server like concept unlike bluejacking which is a client – client concept. An intrusive application is installed on the mobile device which in turn communicates to a remote server through an internet connection sending details such as SMS, call logs, phone books, GPS location, browser history, camera pictures, voice call recording, available applications etc. to the remote server. Keylogging can also be implemented. The attacker then logs into a web interface over the internet to view all retrieved information from the user or the application sends SMS messages to the attacker. The application works by hooking all messaging API and also reads contents of application data files. This appears to be viable for organizations trying to enforce policies or monitor staff, but it can also mean the ability for a blackhat eavesdropping on important information which can be used for further attacks. The situation can become worse if local data storage is insecure (encryption, caching of information not intended for long term storage) and poor authorization and authentication schemes lead to privilege access issues.

The spy application is installed on the victim's mobile device like any other mobile application after which it hides itself by running as a process in the background. It will not be visible in the applications' task list, user interface or application manager. All local logs of information sent over the internet to the attacker are erased as soon as the spy message have been sent – making it uneasy to detect the presence of the spying application. Most of these applications are available for free in the wild and for sale off-the-shelf and over the internet. It should be noted that legit mobile applications can also be "trojanised" with Spyware.

## Spying Tools

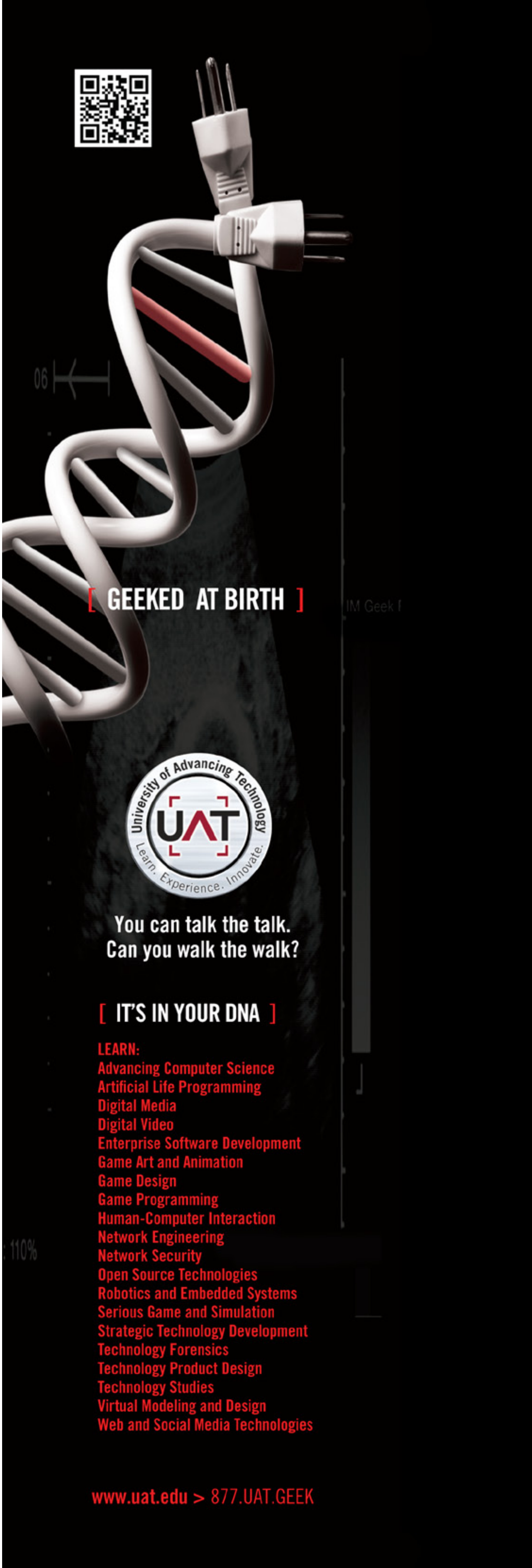
There are so many tools available such that I can't mention all of them in this write up. Few that stand out are Neo-Call spy, Mspy, FlexiSpy, Stealthgenie, Cell phone Spy and Mobile spy. I'll give brief feature list of the tools below:

### Neo-Call Spy

Initially created to spy on Symbian phones, its features have now been extended to cover iPhone, Blackberry, Android and Windows Phones. It sends information directly to another mobile phone. The software is based on the IMEI number – this means that the attacker must know the target. It offers the following spying features SMS, Call List, Location, Remote Listening, Key logging, It is also covert in operation. Commands are sent from the Master phone to the Target to obtain information from the target through hidden SMS messages.

### Mspy

It runs on Smart Phones and Tablets. It allows you to spy on calls, SMS messages, Emails, GPS lo-



cation, browsing history, calendar, address books, IM Messages, Record Surroundings, Control Installed Apps and programs, view Multimedia files, remote control features including device wipe and excellent reporting feature. It's covert in operation and uses the Client – server behaviour with a web based front end. You can view all the spied information online through a secured online account.

**FlexiSpy**
This was initially classified as a mobile device trojan due to its invasive nature but later the classification reduced as variants were released. It helps spy on mobile phones and tablets. It offers about 130 features which when categorized fall within the coverage of Mspy. Additional features like camera spying and Wallpaper viewing are invaluable to an attacker. It's also covert in operation and can often go undetected. This also uses a Client – Server architecture with a web based front-end. You can view all the spied information online through a secure online account.

**Stealthgenie**
This is also operated covertly and works similarly to FlexiSpy and Mspy – with the same feature set.

**Mobile Spy**
This has most of FlexiSpy's features set with additional Application Blocking, remote Install abilities and live control panel abilities. Multimedia files can be downloaded from the front end panel.

Other tools are (Source: *http://cell-phone-monitoring-software-review.toptenreviews.com/*):

**HIGHSTER MOBILE**
An easy-to-use cell phone monitoring software; Text messages, call recordings, call logs…all sent from the target phone right to the user email, cell phone or`online web account immediately.

**All-in-one Spy Software**
Top quality spy phone software since 2006. Cell phone tracking & surveillance. Secure SMS. Voice Encryption and PC monitoring software.

**Easy Spy**
Easy-to-use program for monitoring cell phones. Provides instant access to text messages, calls and more. Right from the user own cell phone, computer or tablet, undetected.

**Spybubble**
Powerful yet covert cell-phone monitoring software that tracks and aecords all information in real-time. It is wel-known cell phone monitoring and tracking system with call listening and environment listening.

**MobShield (Mobile Shield)**
Highly advanced cell phone application that allows the user to restrict the use of the cell phone while monitoring the phone's activities. MobShield is the best way to protect your kids, aged parents, spouse, or employees from danger and temptation.

**Phone Spy**
Monitoring conversations of a spouse, lovers, children, employees and anybody else that the user chooses. Once the phone makes connection with the target phone, its user can start listening to what is happening around the target phone.

**MobileSpy**
The next generation of smartphone spy software. Silently monitoring text messages, GPS locations, call details, photos and social media activity; viewing the screen and location live.

**Spyera**
The software that is installed on a smart phone to monitor everything happening on the phone. SPYERA secretly records events (sms, call history, phone book, location, emails, What's App messages, IM, Facebook Chat, Skype, see photos taken and many more...) that happen on the phone and delivers these information to a web account, where the user can view these reports 24/7 from any Internet enabled computer or mobile phone.

**OX for Android MobileSpy**
Cell phone spy for smart Android version phone also provides users a free trial process, it can be download to the mobile phone to learn what the children are secretly talking and texting, smoking, drugs, or what the employees are really doing away from office with this mobile spy.

**VspyMe**
Are you are spending sleepless nights worrying about where your kids are or what they are up to? Look no further. vSpyMe Children and family is a powerful cell phone spy software designed to ease your burden and give you better visibility, transparency and control of what's going on in your home and the lives of people you care about.

**MerrySpy**
A spy software to turn ordinary Nokia S60 phones into spy phones.

### SpyMaster Pro

World's most efficient and advanced cell spying software, works 100% in hidden mode without leaving any indication of detection.

### EasilySpy

100% Safe and easy to use, yet powerful enough to get the needed information.

### PhoneSheriff

The next generation of parental control software for mobile phones and tablets. If you are worried that your children are using their phones and tablets inappropriately, then use PhoneSheriff (Figure 1-4).

### Case Study

Todd's suddenly sounds all religious and stuff. He claims to live righteously and proves that others are not as good as him. Edwin hates this and being a blackhat, he wants to prove otherwise to him and his mates, that Todd is not a saint after all. He starts looking for ways to provide evidence that that's not the case. Appropriate tool: Mobile Spy, FlexiSpy and Mspy. Method:

- Edwin opens an account with any of the three tools.
- He downloads the application, "Trojanises" it with a gaming application or just transfers it to *Todd's phone* through Bluetooth since he has access to *the* phone.
- He installs the application, logs on to the portal online. Monitors the phone for porn and illicit pictures, downloads it and presents it to *Todd* and his friends. What an embarrassment for *Todd*... and a good lesson learnt.

These tools though having a legal ground for usage are potential black hat delight since information gathered from the phone can be used for malicious purposes. Care must be taken to understand the way Mobile phone Spying works and how to Detect and/or prevent this imminent threat.

## Detection

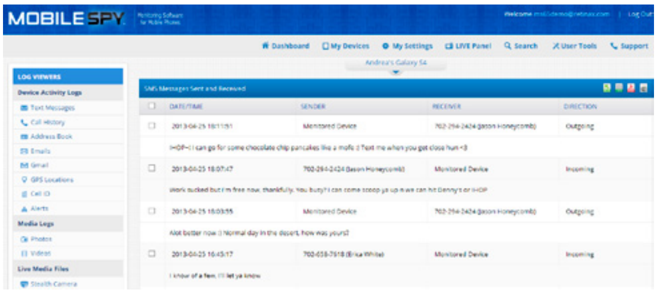
Like in any other investigation, careful attention is paid to some basic phone behavior like increased data charge due to usage, strange behavior of the phone like sudden phone reboot, flashing screen, locked down applications.

Analysis of the compromised phone can be categorized into three:

- Traffic analysis
- Process Analysis
- File System Analysis

### Traffic analysis

Most spy tools communicate with the attacker through SMS, MMS or over the data channel. So even if the tool is able to evade the user, it can't bypass the operator's billing system. Most of the time, phone users are on a monthly Data and SMS plan making it even more difficult to detect. In this senerio an investigation SIM is used (A SIM that is not used for any other purpose obtained from the mobile phone operator). The SIM is installed in the phone and up to 10 or more SMS are sent to the phone. – This of course should be free to the phone's user, so if there are charges, then the phone is likely a victim of phone spying. Similarly, disable all automatic update feature and observe the GPRS/EDGE icon after an SMS is sent. Check the data bill again and very unusual then this is a call to be suspicious. The TCP/IP traffic can also be sniffed using Wireshark, a PC, Wireless Router (Pro-



SMS Messages Sent and Received

| □ | DATE/TIME | SENDER | RECEIVER | DIRECTION |
|---|---|---|---|---|
| □ | 2013-04-25 18:11:51 | Monitored Device | 702-294-2424 (Jason Honeycomb) | Outgoing |
| | IHOP~I can go for some chocolate chip pancakes like a mofo :) Text me when you get close hun <3 | | | |
| □ | 2013-04-25 18:07:47 | 702-294-2424 (Jason Honeycomb) | Monitored Device | Incoming |
| | Work sucked but I'm free now, thankfully. You busy? I can come scoop ya up n we can hit Denny's or IHOP | | | |
| □ | 2013-04-25 18:03:55 | Monitored Device | 702-294-2424 (Jason Honeycomb) | Outgoing |
| | Alot better now :) Normal day in the desert, how was yours? | | | |
| □ | 2013-04-25 16:45:17 | 702-658-7918 (Erica White) | Monitored Device | Incoming |
| | I know of a few, I'll let ya know | | | |

**Figure 1.** *Front End: SMS captured using Mobile Spy*

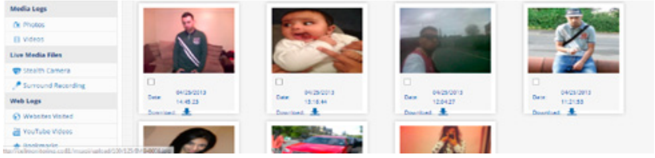
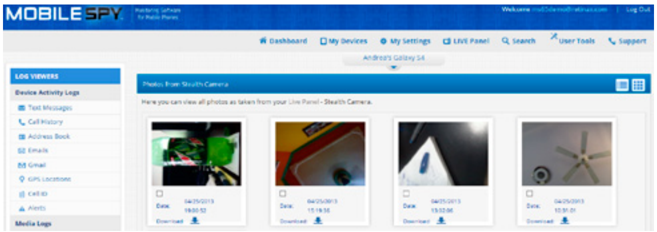


**Figure 2.** *Front End: Photos Captured using Mobile Spy*



Photos from Stealth Camera

Here you can view all photos as taken from your Live Panel - Stealth Camera.

**Figure 3.** *Front End: Stealth Camera*

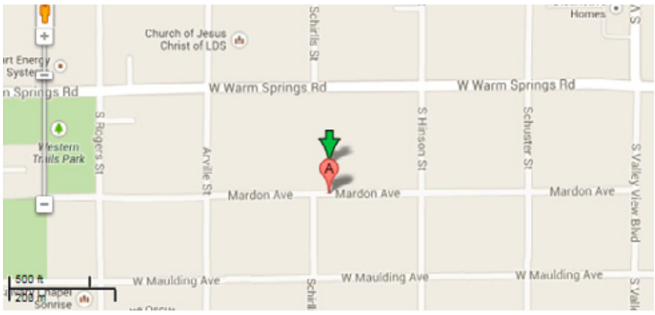


**Figure 4.** *Front End: GPS Location*

visioned for internet Access) and Switch – do this at your own risk as this is illegal in some countries. I will not give details here. Sorry. Some spying tools insist on the use of the Phone's Data instead of WLAN, they tend to create their own form of access visible on the phone after connection to WLAN – this is a clear indication of Mobile Spying application's presence on the phone. An example is FlexiSpy (Figure 5).

### Process Analysis

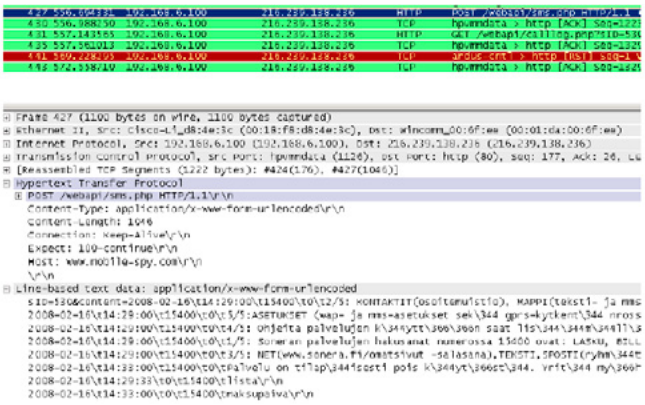
Get another Phone, list out all processes running on that phone. Access the process List of the suspected phone and list them out. Compare the two lists for any suspicious processes. For any process that is suspected not to be an OS process or a legitimate application process further investigation should be done on that process. This analysis is based on that fact that most Spy tools do not hide their processes. For Windows mobile the registry is the best place to search for anomalies.

### File System Analysis

Compare the file system of the phone to another phone which is clean. It is advisable to install a file monitor application to monitor processes accessing the file system when receiving and sending SMS, MMS, incoming and outgoing calls or emails. F-explorer, EzFileMon are applications that can be used for Symbian Phones. Once the process is found, kill it and see if any spying continues. After this, try to locate the file and delete it. Check the location of installed applications. Any application that is not installed within the right path is a suspect.

## Prevention / Countermeasures

- Do not jailbreak or root your phone iPhone or Android phones respectively – this removes most of the security features on the phone – Charlie Miller, SyScan 2009.
- Use a good mobile antivirus – This detects commonly used spy tools. This is one of the sure protection against Mobile Device spying.
- Set access security on the Phone e.g password lock, pattern lock etc. This will help reduce the possibility of an attacker gaining access for installation of the application on your phone.
- Update you Mobile OS – Keep you Mobile OS updated. Security Patches are released with OS upgrades and updates.
- If possible implement an OS re-installation policy in your organization. – this will ensure that undetected compromised phones are corrected.
- During crucial meetings, power down you phone – an attacker may have gained access to the camera and may be doing surround recording.
- Keep your phone close to yourself at all times.
- Install only signed application – this is the only sure way to prevent "trojanised" applications from being installed.



```
427 556.694331 192.168.6.100   216.239.138.236   HTTP   POST /webapi/sms.php HTTP/1.1
430 556.988250 192.168.6.100   216.239.138.236   TCP    hpvmmdata > http [ACK] Seq=122
431 557.143565 192.168.6.100   216.239.138.236   HTTP   GET /webapi/calllog.php?SID=53
435 557.561013 192.168.6.100   216.239.138.236   TCP    hpvmmdata > http [ACK] Seq=132
441 569.228295 192.168.6.100   216.239.138.236   TCP    ardus-cntl > http [RST] Seq=1
445 572.558710 192.168.6.100   216.239.138.236   TCP    hpvmmdata > http [ACK] Seq=132

⊞ Frame 427 (1100 bytes on wire, 1100 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_d8:4e:3c (00:18:f8:d8:4e:3c), Dst: Wincomm_00:6f:ee (00:01:da:00:6f:ee)
⊞ Internet Protocol, Src: 192.168.6.100 (192.168.6.100), Dst: 216.239.138.236 (216.239.138.236)
⊞ Transmission Control Protocol, Src Port: hpvmmdata (1126), Dst Port: http (80), Seq: 177, Ack: 26, Le
⊞ [Reassembled TCP Segments (1222 bytes): #424(176), #427(1046)]
⊟ Hypertext Transfer Protocol
  ⊞ POST /webapi/sms.php HTTP/1.1\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    Content-Length: 1046
    Connection: Keep-Alive\r\n
    Expect: 100-continue\r\n
    Host: www.mobile-spy.com\r\n
    \r\n
⊟ Line-based text data: application/x-www-form-urlencoded
    SID=530&content=2008-02-16\t14:29:00\t15400\t0\t2/5: KONTAKTIT(osoitemuistio), KAPPI(teksti- ja mms
    2008-02-16\t14:29:00\t15400\t0\t5/5:ASETUKSET (wap- ja mms-asetukset sek\344 gprs-kytkent\344 nross
    2008-02-16\t14:29:00\t15400\t0\t4/5: Ohjeita palvelujen k\344ytt\366\366n saat lis\344\344\344ll\3
    2008-02-16\t14:29:00\t15400\t0\t1/5: Soneran palvelujen hakusanat numerossa 15400 ovat: LASKU, BILL
    2008-02-16\t14:29:00\t15400\t0\t3/5: NET(www.sonera.fi/omatsivut -salasana),TEKSTI,SPOSTI(ryhm\344t
    2008-02-16\t14:33:00\t15400\t0\tPalvelu on tilap\344isesti pois k\344yt\366st\344. Yrit\344 my\366h
    2008-02-16\t14:29:33\t0\t15400\tlista\r\n
    2008-02-16\t14:33:00\t0\t15400\tmaksupaiva\r\n
```

**Figure 5.** *Monitored traffic from a Mobile Spy infected Phone (Jarno Niemela)*

Mobile phone spying applications are easy to get in the wild. This has dramatically increased the occurrence of spying and its consequences. Mobile phones are gradually taking over from PCs as people are being drawn because of the feature rich yet portable nature of mobile devices. Spying remains one of the major threats in the industry and should be given careful attention within the security space.

## References

- Jarno Niemela: Detecting Mobile Phone Spy Tools
- Paul Ruggiero and Jon Foote: Cyber Threats TO Mobile Phones 2012
- Dr. Mohamed Hossam Ahmed: Mobile Phone privacy Report: March 2009
- Mike Klipstein Rafael Cedeño: Your Smart Phone Hates you 2012

### AKINFE OLUWAFEMI G

***Is the President of Iris Computer Solutions, which specializes in the provision of various IT services ranging from Networking and Security to Software development. He has over 10 years of practical IT experience and holds a degree from the prestigious Federal University of Technology, Akure. He has 5 certifications; CCNA, CCNA Security, CEH, ECSA and A+ IT Technician. He has a passion for innovation in the Networking and Network Security Space. He is also an IT infrastructure support Professional. He can be found online at the following sites: http://www.iriscomputersolutions.com/ and http://247infotech.wordpress.com/.***

# IRIS COMPUTER SOLUTIONS

*Complete IT Solutions ... applicable Worldwide*

IT Security Solutions
Secure E-Commerce Implementation
IT Security Consultancy and Training
IT Security Risk Management
Technology Support Services
Business IT Automation

Email: info@iriscomputersolutions.com
Telephone: +2347031360963; +2348036907067
Facebook: facebook.com/Iriscomputers
Website: www.iriscomputersolutions.com

**Iris Computer Solutions rebranding soon.... watch out**

# SIM Card Hacking

SIM cards were believed to be the most secure part of a mobile phone but recent researches have proved otherwise. An expert cryptographer within security research labs has found a way to trick mobile phones into granting access to the device`s locations, SMS functions, and allow changes to a person`s voicemail number.

SIM (Subscriber Identification Module) is a small card inserted into a device that ties it to a phone number and authenticates software updates and commands. There are more than 7 billion SIM cards are in use worldwide. To ensure privacy and security, SIM cards use encryption when communicating with an operator, but the encryption standards used vary widely.

Recent studies have shown that just under a quarter of all the SIM cards that were tested, could be hacked. Given that encryption standards vary widely between countries, it has been estimated that an eighth of the world's SIM cards could be vulnerable, or about half a billion mobile devices (FIgure 1). The SIM card hacking flaw was discovered by German programmer Karsten Nohl,

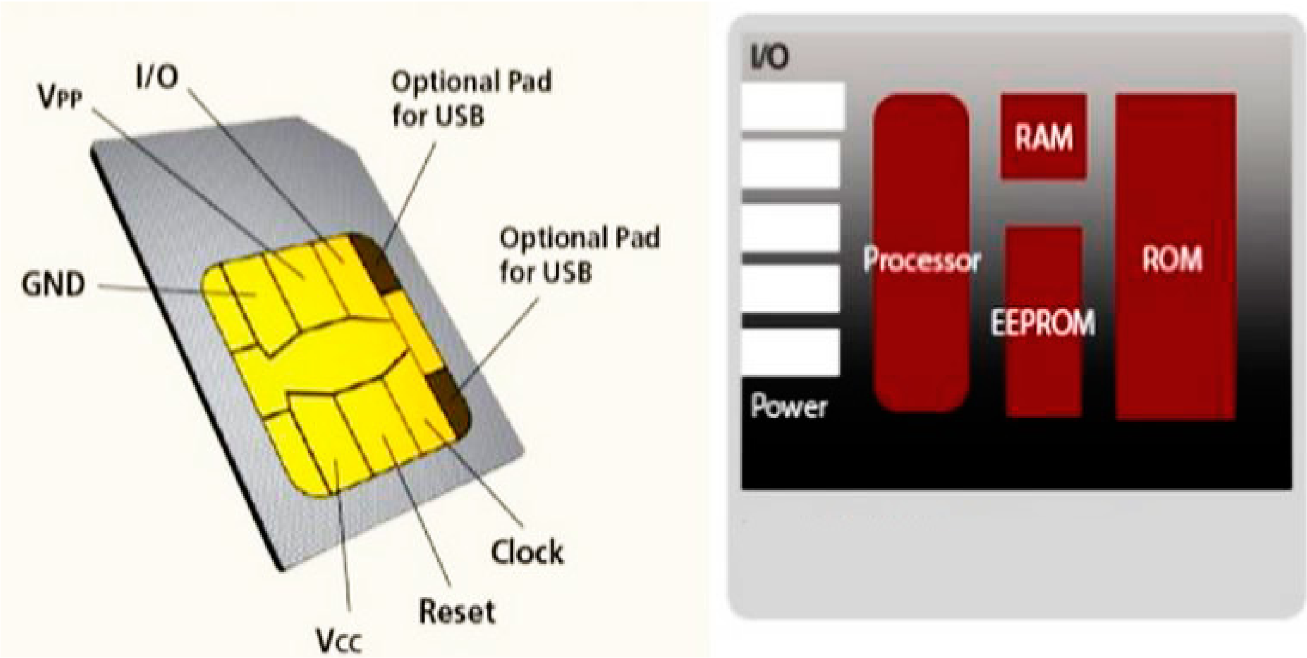


**Figure 1.** *Smart Chip in a card*

who has informed mobile operators of the potential danger. After that all, the Mobile phone users have been put on an alert that their SIM cards can be hacked anytime which may lead to fraud and soaring premium rate bills.

On the other hand, if we talk about the mobile operators they say that they are already aware about this flaw and are taking steps to patch the flaw before customers are hit.

Worldwide, mobile phones are the major source used in accessing online banking and other sensitive personal information. If the discovered flaw is used by Hackers, it may lead to a privacy disaster. This flaw also makes some noise for the mobile customers who use their Smartphone's to pay bills and transfer money.

Flaw Researcher (Karsten Nohl) says something about his Flaw:

"Give me any phone number and there is some chance I will, a few minutes later, be able to remotely control this SIM card and even make a copy of it,"

However, the international umbrella mobile operator organization, the GSMA, said that the flaw was limited to a minority of SIM cards and that newer SIM cards may not be affected. It said that it had advised operators of the security risks involved.

## Major Causes of SIM Card Hacking

See Figure 2.

## Outdated Encryption Standard

Researchers have indicated that many SIMs use a weak encryption standard dating from the 1970s called DES (*Data Encryption Standard*). DES has long been considered a weak form of encryption, and many mobile operators have upgraded to more secure Encryption. It is relatively easy to discover the private key used to sign content encrypted with DES.

## Cracking SIM Update Keys

OTA commands, such as software updates, are cryptographically-secured SMS messages delivered directly to the SIM. While the option exists to use state-of-the-art AES or the somewhat outdated 3DES algorithm for OTA, many (if not most) SIM cards still rely on the 70s-era DES cipher. DES keys were shown to be crackable within days using FPGA clusters, but they can also be recovered much faster by leveraging rainbow tables similar to those that made GSM's A5/1 cipher breakable by anyone [1].

In an experiment conducted at the Security Research Labs, researchers sent a binary code over SMS to a device using a SIM with DES. Since the binary code wasn't properly cryptographically signed, it would not run on the device.

But while rejecting the code, the phone's SIM makes a crucial mistake: it sends back over SMS an error code that carries its own encrypted 56-bit private key, according to the company. Because DES is considered a very weak form of encryption, it's possible to decrypt the private key using known cracking techniques.

Security Research Labs did it in about two minutes on a regular computer with the help of a rainbow table, a mathematical chart that helps convert an encrypted private key or password hash into its original form faster.

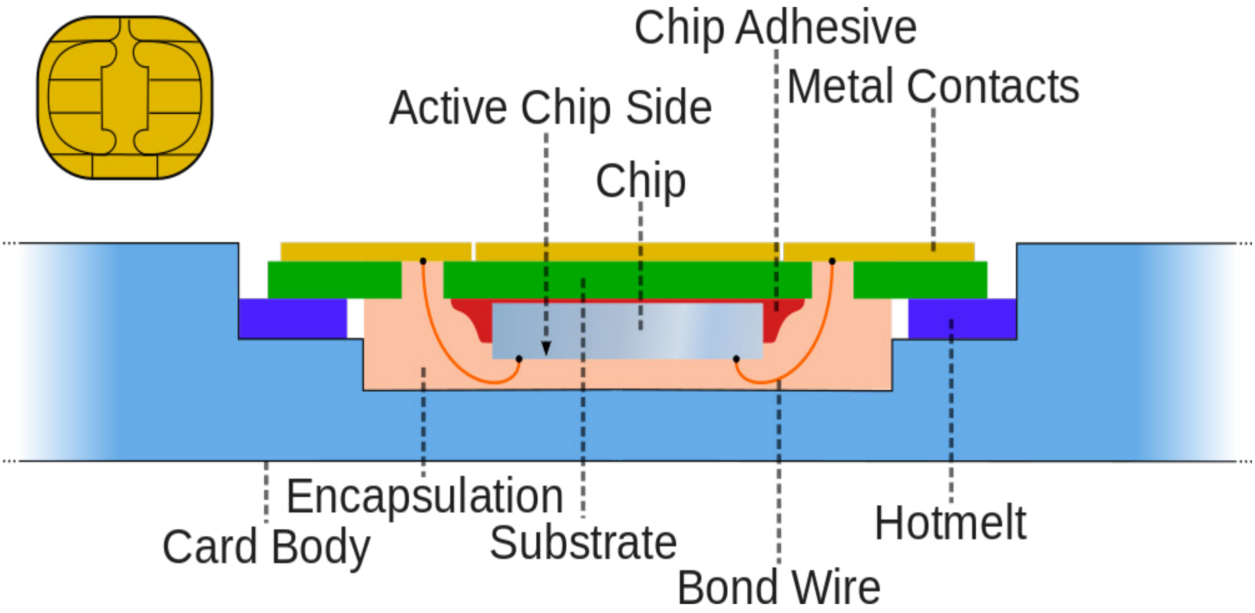


**Figure 2.** *How a Sim card is read*

With the private DES key in hand, it is then possible to "sign" malicious software updates with the key, and send those updates to the device. The device believes the software comes from a legitimate source and then grants access to sensitive data.

Using the SIM's private key, an attacker could force the SIM to download Java applets, which are essentially very small programs that perform some function. Those applets would be "allowed to send SMS, change voicemail numbers, and query the phone location, among many other predefined functions."

With the all-important (and till-now elusive) encryption key, it is even possible to send a virus to the SIM card, which could then send premium text messages, collect location data, make premium calls or re-route calls. A malicious hacker could eavesdrop on calls, albeit with the SIM owner probably noticing some suspiciously-slow connections.

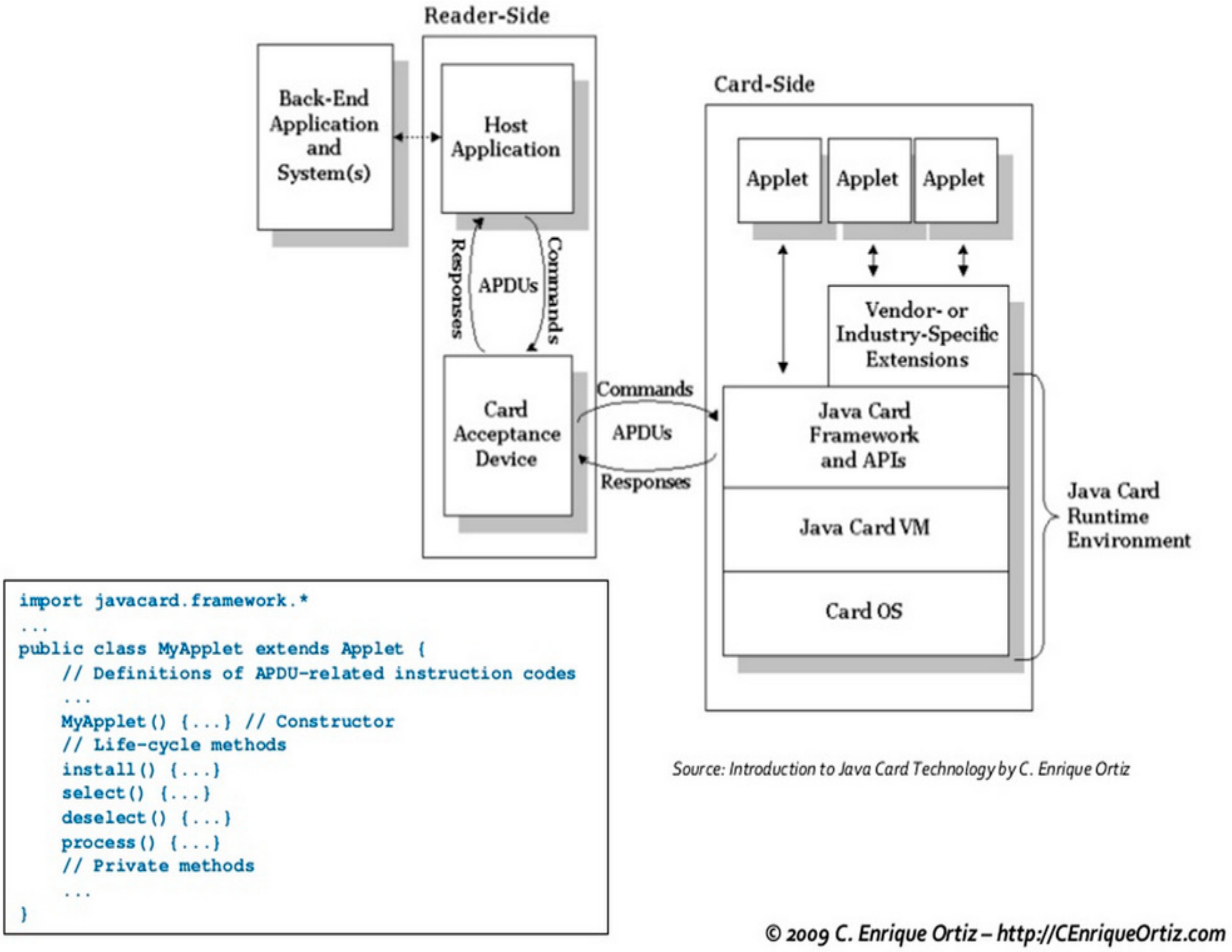
The company outlined an attack scenario against SIM cards that run some form of Java virtual machine, a software framework for Java applications.

## Java Sandboxing

A second bug has also been found. Unrelated to the weak encryption key, it allows even deeper hacking on SIMS and is caused by mistake on the part of SIM card manufacturers. In principle, the Java virtual machine should assure that each Java applet only accesses the predefined interfaces.

Key to the hack is Java Card (2), a general purpose programming language used on 6 billion SIM cards. If operators need to update something on your SIM, for instance allowing interoperability with a carrier in another country, it will execute the right Java Card programs on your SIM by sending your mobile a binary SMS (Figure 3).

Java Card uses a concept called sandboxing, in which pre-installed programs like a Visa or PayPal app are shielded from one another and the rest of the SIM card. The term comes from the idea of only allowing programs to "play with their own toys, in their own sandbox," "This sandboxing mechanism is broken in the most widely-used SIM cards." The researcher said he found a few instances where



```
import javacard.framework.*
...
public class MyApplet extends Applet {
    // Definitions of APDU-related instruction codes
    ...
    MyApplet() {...} // Constructor
    // Life-cycle methods
    install() {...}
    select() {...}
    deselect() {...}
    process() {...}
    // Private methods
    ...
}
```

Source: Introduction to Java Card Technology by C. Enrique Ortiz

© 2009 C. Enrique Ortiz – http://CEnriqueOrtiz.com

**Figure 3.** *Java Card Technology*

the protocols on the SIM card allowed the virus he had sent to a SIM, to check the files of a payment app that was also installed on the card.

In sum, a malicious hacker who wanted to use this method might start with a list of 100 phones. They could send a binary SMS to all of them, using a programmable cell phone connected to a computer. They might get 25 responses with cryptographic signatures, and dismiss the half that uses a stronger security standard. From the rest, Nohl surmises they could crack the encryption key of perhaps 13 SIM cards, and send them a virus that breaks through the Java Card sandbox barriers and reads payment app details, as well as the master key of the SIM card.

## Who Is To Be Blamed?

Gemalto which made about half [3] its $2.5 billion revenue [4] in 2012 selling SIM cards, said in an email to Forbes that its SIMs were consistent with state-of-the-art and applicable security guidelines, and that it had been working closely with GSMA and other industry bodies to look into the earlier research.

Despite this, it is believed that badly-configured Java Card sandboxing "affects every operator who uses cards from two main vendors," including carriers like AT&T and Verizon who use robust encryption standards. Are SIM cards with these 3DES standards vulnerable? Some people suggest they might be but are still unsure about the details.

## iPhone, Android, BlackBerry

The mobile industry has spent several decades defining common identification and security standards for SIMs to protect data for mobile payment systems and credit card numbers. SIMs are also capable of running apps.

Nohl said Security Research Labs found mobile operators in many countries whose phones were vulnerable, but declined to identify them.

All types of phones are vulnerable, including iPhones from Apple Inc, phones that run Google Inc's Android software and BlackBerry Ltd Smartphone's, he said.

BlackBerry's director of security response and threat analysis, Adrian Stone, said in a statement that his company proposed new SIM card standards last year to protect against the types of attacks described by Nohl, which the GSMA has adopted and advised members to implement

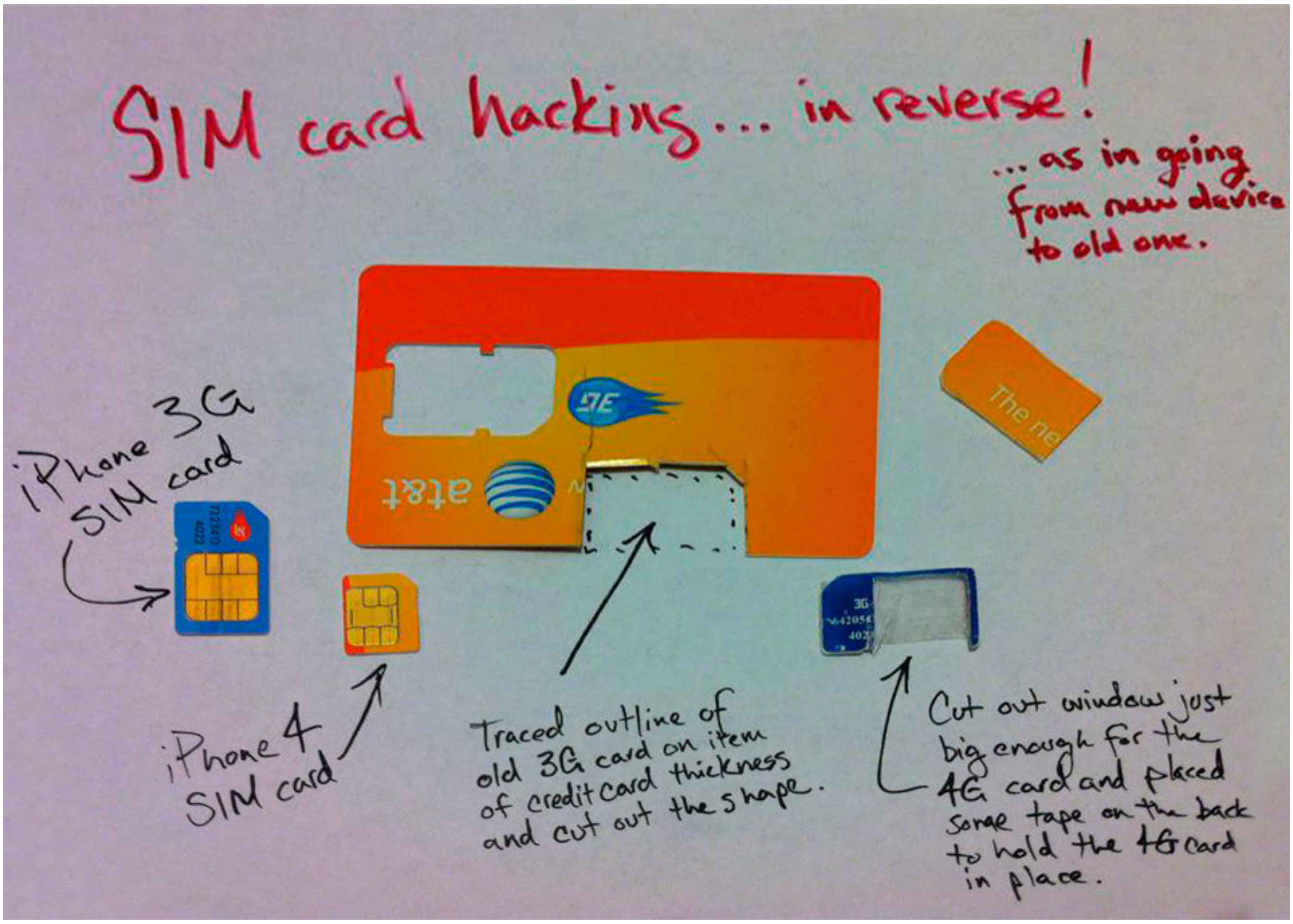

SIM card hacking... in reverse!
... as in going from new device to old one.
iPhone 3G SIM card
iPhone 4 SIM card
Traced outline of old 3G card on item of credit card thickness and cut out the shape.
Cut out window just big enough for the 4G card and placed some tape on the back to hold the 4G card in place.
at&t
The ne

**Figure 4.** *Sim Card Hacking In Reverse*

"We understand the vulnerability and are working on it," said CTIA Vice President John Marinho. "This is not what hackers are focused on. This does not seem to be something they are exploiting."

## SIM Card Hack Could Affect Millions Worldwide!

A United Nations group that advises nations on cyber-security plans to send out an alert about significant vulnerabilities in mobile phone technology that could potentially enable hackers to remotely attack at least half a billion phones (Figure 4).

The bug discovered by German firm, allows hackers to remotely gain control of and also clone certain mobile SIM cards.

Hackers could use compromised SIMs to commit financial crimes or engage in electronic espionage, according to Berlin's Security Research Labs, which will describe the vulnerabilities at the Black Hat hacking conference that opens in Las Vegas on July 31.

The U.N.'s Geneva-based International Telecommunications Union, which has reviewed the research, described it as "hugely significant."

"These findings show us where we could be heading in terms of cyber-security risks," ITU Secretary General Hamadoun Touré told Reuters.

A spokeswoman for the GSMA, which represents nearly 800 mobile operators worldwide, said it also reviewed the research.

"We have been able to consider the implications and provide guidance to those network operators and SIM vendors that may be impacted," said GSMA spokeswoman Claire Cranton.

Nicole Smith, a spokeswoman for Gemalto NV, the world's biggest maker of SIM cards, said her company supported GSMA's response.

"Our policy is to refrain from commenting on details relating to our customers' operations," she said.

## SIM Card Hack – Severe Implications for Business

The impact of hacked SIM cards, one of the few stalwarts in the high-tech industry that has not seen a serious exploit, could be monumental.

For individuals, the risk of someone hijacking your phone and listening in on calls or making phony purchases is bad enough. For business users, these problems may soon be compounded considerably (Figure 5).

As business data continues to move from the desktop PC to mobile devices, even rank-and-file employees are finding themselves walking around with a mountain of sensitive data in their pocket or purse. Lost and stolen phones have become an epidemic [5] for the corporate world, and solutions to this dilemma have been unbearably slow in presenting themselves. Compound that with the risk that a large number of business devices may also be able to be attacked via a remote exploit and cell phones are looking increasingly like the weak link in any business's infrastructure.

Let's say a business does take steps to secure its handsets and ensure that SIM cards are properly patched and safe from attack. What then? Even if businesses correct company-owned devices, plenty of risks are sure to remain, thanks to the rise of BYOD (bring your own device) programs. BYOD, for the uninitiated, is the policy of allowing employees to use their own phone or tablet for work – often in lieu of issuing them a company-owned mobile phone or even a landline. This saves the company money but remains a serious security risk – doubly so given the current news, since BYOD devices can't be easily patched or protected from a central location.

Finally, as phone-based commerce becomes increasingly popular, this opens up yet another avenue where businesses will face risks. Hackers could theoretically redirect payments or change the amounts involved, potentially leaving merchants high and dry at the end of a transaction.

## Remedies

The risk of remote SIM exploitation can be reduced by the following measures:

### Improved SIM cards

Cards need to use state-of-art cryptography with sufficiently long keys, should not disclose signed plaintexts to attackers, and must implement secure Java virtual machines. While some cards already come close to this objective, the years needed to replace vulnerable legacy cards warrant supplementary defenses.

**Figure 5.** *Hacked 3G*

## References

[1] *https://srlabs.de/decrypting_gsm/*
[2] *http://en.wikipedia.org/wiki/Java_Card*
[3] *http://www.businessweek.com/news/2012-06-14/linkedin-s-stolen-passwords-spell-profit-for-gemalto*
[4] *http://www.gemalto.com/press/archives/2013/2013-03-14_Gemalto_FY_2012_Earnings_PR_EN.pdf*
[5] *http://www.businessweek.com/articles/2012-03-08/data-security-most-finders-of-lost-smartphones-are-snoops*
[6] *http://events.ccc.de/congress/2008/Fahrplan/events/2997.en.html*

### SMS firewall

One additional protection layer could be anchored in handsets: Each user should be allowed to decide which sources of binary SMS to trust and which others to discard. An SMS firewall on the phone would also address other abuse scenarios including "silent SMS."

### SMS filtering

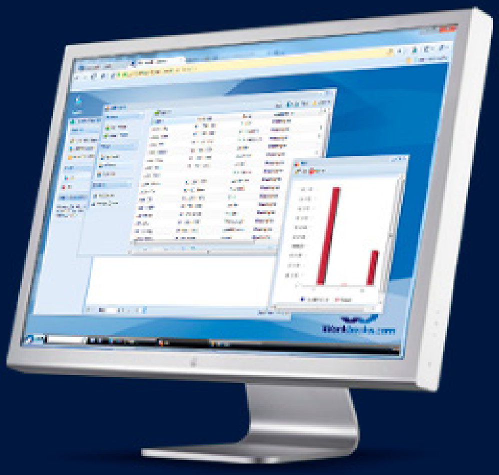
Remote attackers rely on mobile networks to deliver binary SMS to and from victim phones. Such SMS should only be allowed from a few known sources, but most networks have not implemented such filtering yet. "Home routing" is furthermore needed to increase the protection coverage to customers when roaming. This would also provide long-requested protection from remote tracking [6].

To sum up, the carriers should upgrade to newer encryptions quickly, not just for the safety of their subscribers, but future revenue too. Payment providers like MasterCard and Visa will need to use the OTA protocol to fill SIM cards with Java applications, like credit card applets, and enable NFC-based payments on phones in the future – and they'll pay carriers for the privilege of being on the SIM.

To conclude, SIM card hacking also projects a serious threat for mobile phones and therefore it must not be taken for granted and necessary measures and counter techniques need to be encouraged.

### ANUPAM SHARMA

***Sharma Lives in Shimla, Himachal Pradesh, co-founder of Aorso Technologies and Unhacks Inc. He previously served at Demagogue as a director of Network and Security for 1 year. He is Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT), Certified Hacking Forensics Investigator (CHFI) from EC Council University California, USA. From long time he have been into security research and tracking tactics of hackers and intruders. He is currently working network checkpoint software which is to be launched in upcoming year. His main interest are in Mobile hacking and web application pentration testing.***



# Windows Phone 8 Application Penetration Testing Essentials

This article will provide an overview of the Windows Phone 8 operating system security features and how to conduct penetration tests of Windows Phone 8 applications.

Android and iOS are the market leaders in terms of mobile platforms and mobile applications. Microsoft is hoping to gain more market share again with their latest mobile operating system. Microsoft's mobile operating system Windows Phone, previously known as Windows Mobile, overtook Blackberry in market share in February 2013 [1] and IDC analysts predicted that by 2016 Microsoft's mobile operating system will gain a market share of more than 10% [2]. As a result, organisations are developing more applications for Microsoft's mobile platforms; as such, IT security professionals should understand how these applications can be assessed and secured.

This article will provide an overview on Windows Phone 8 security and will outline how to perform security assessments of Windows Phone 8 applications.

## Windows Phone, Windows RT and Windows 8

Microsoft introduced a new Application Programming Interface (API) called WinRT in its latest operating systems in addition the Win32 API that was supported in Windows operating systems since Windows 95. Applications developed using the WinRT API are known as Windows Store applications, or Metro-style applications.

Windows RT, Microsoft's operating system launched to support devices with ARM chipsets, only supports the WinRT API and is, by default [4, 5], not able to run Win32 applications.

Windows Phone 8 supports the Windows Phone RT API, which is only a subset of the WinRT API.

Microsoft changed the kernel of the Windows Phone platform from Windows CE in Windows Phone 7 to Windows NT in Windows Phone 8. This allowed Microsoft to inherit the security controls we are familiar with from modern Windows desktop operating systems to their mobile platform.

**Table 1.** *Overview of Microsoft's latest operating systems*

| | Hardware Architecture | Applications Architecture | OS Kernel |
|---|---|---|---|
| Windows 8 | X86/x64 | Win32/WinRT | Windows NT |
| Windows RT | ARM | WinRT | Windows NT |
| Windows Phone 7 | ARM | Silverlight/ XNA | Windows CE |
| Windows Phone 8 | ARM | Windows Phone RT | Windows NT |

## Windows Phone 8

As a result of adopting the Windows NT kernel, Windows Phone 8 inherited key security features that were missing from prior Microsoft mobile platforms:

- NTFS file system support
- BitLocker device encryption
- Sandboxed applications: Applications run in their own sandboxed virtual environment
- UEFI Secure boot: Unified Extensible Firmware Interface (UEFI) is the successor to the legacy BIOS firmware interface. UEFI relies on the Trusted Platform Module (TPM) 2.0 standard requiring unique keys to be burned into the chip during production to restrict software without correct digital signature to execute.
- All Windows Phone 8 binaries must have digital signatures signed by Microsoft to run

The older Windows Phone 7 operating system was built on the Windows CE kernel and did not have the above security features and as such, unlocking and running arbitrary ROM's and applications was much easier. Windows Phone 8 applications are downloaded through a central app store Windows Phone Store.

## Preparing your test environment

Mobile application penetration tests can be conducted in 2 ways: using a physical Windows Phone 8 device, or using emulators. Some of the prerequisites before you can start assessing your Windows Phone 8 applications are outlined next.

### Using a physical Windows Phone 8 mobile phone

When using a physical phone an unlocked phone is required. At this stage, unlocking your phone can only be accomplished by either:

- Registering a developer account and developer-unlock your phone for $99/year. On a developer unlocked phone you can install up to ten applications that are not digitally signed by Microsoft
- Registering a student account: Students can install up to three applications that are not digitally signed by Microsoft
- Register a company trusted certificate for Enterprise app stores for $399/year

It is likely in the future it may become possible to unlock Windows Phone 8 devices using different means. For Windows RT, a jailbreak tool was released [4] that disables code signing in the operating system's boot loader and allows the execution of arbitrary applications. From preliminary analysis of the boot loaders of Windows 8, Windows RT and Windows Phone 8, they appear identical (Figure 1).

There are some other limitations that make it more difficult, but not impossible for this to happen in the future [3].

### Using an emulator

To test applications using emulators, the Windows Phone SDK that can be downloaded from dev.windowsphone.com will automatically install the Windows Phone emulator. After installing the SDK, the emulator is available from:

```
C:\program files (x86)\ Microsoft XDE\8.0\XDE.exe
```

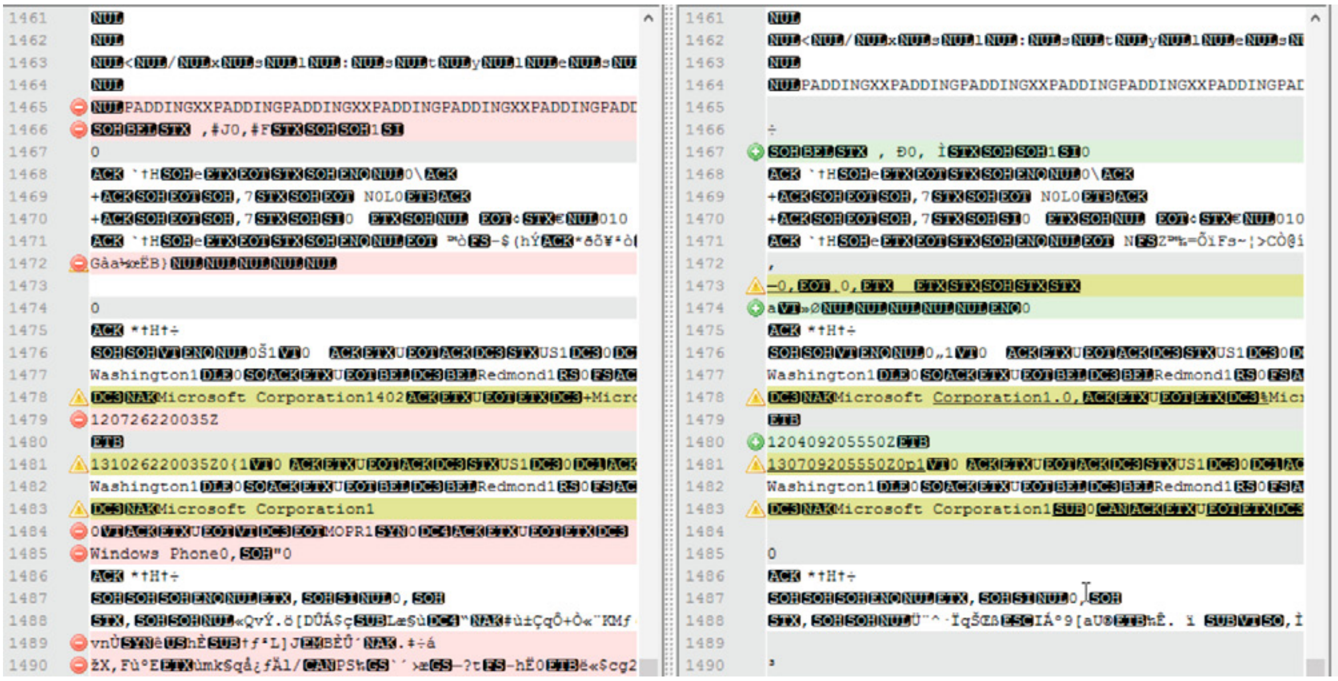


**Figure 1.** *Comparison of Windows Phone 8 and Windows RT boot loaders*

You also need a copy of the following tools:

- Visual Studio or Visual Studio Express – *http://www.microsoft.com/express/*
- Windows Phone Power Tools – *http://wptools.codeplex.com/*
- ILSpy – *http://ilspy.net/*
- Tangerine – *https://github.com/andreycha/tangerine*

Some commercial alternatives for ILSpy and Tangerine that are worthwhile exploring:

- XAML Spy – *http://xamlspy.com/*
- .NET Reflector – *http://www.reflector.net/*

## Hyper-V configuration settings

- Windows Phone 8 emulators are Hyper-V virtual machines each instance having their own IP addresses. When using an emulator for testing, a system with core i3, i5 or i7 or equivalent AMD processor supporting newer hardware virtualization features is required.
- First of all, make sure your hypervisor settings are enabled in your system BIOS. Next, validate that Hyper-V settings are enabled in Windows.

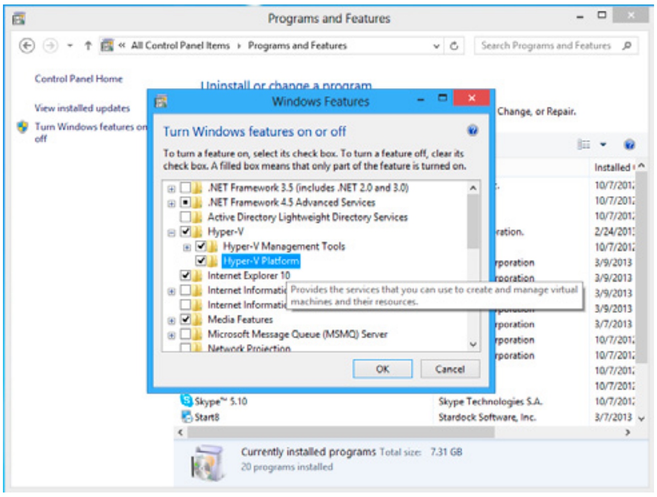
## VMware configuration

- It is often advantageous to perform penetration tests from a virtualized environment. In order to conduct Windows Phone 8 penetration tests using VMware, a number of virtualization settings need to be configured. In VMware Fusion:
- Enable the VT-x/EPT hypervisor option (Figure 2)
- Open your .vmx file in a text editor and add the following setting (Figure 3), if not already there:

```
mce.enable = “TRUE”
```

## Windows Phone applications

Windows Phone 8 applications are stored in the XAP file format. A XAP file is, similar to an Android APK file, a compressed zip archive containing all the application's supporting files such as DLL's. The AppManifest.xaml file defines the assemblies that get deployed with the client application.


Programs and Features

All Control Panel Items › Programs and Features

Windows Features

Turn Windows features on or off

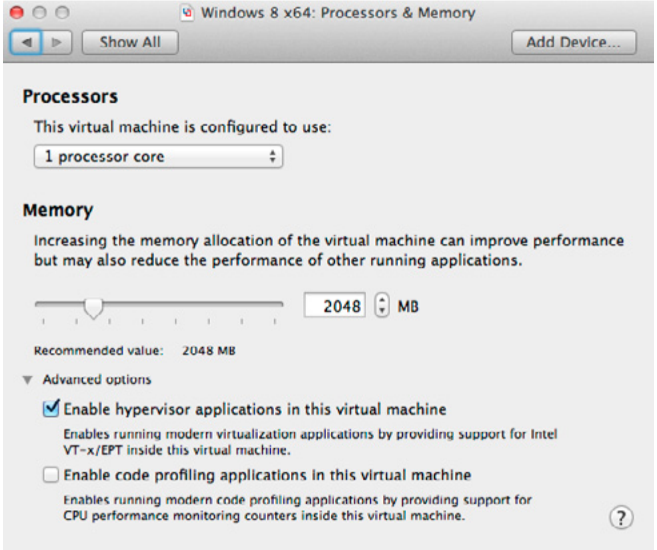
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☐ .NET Framework 3.5 (includes .NET 2.0 and 3.0)
- ■ .NET Framework 4.5 Advanced Services
- ☐ Active Directory Lightweight Directory Services
- ☑ Hyper-V
  - ☑ Hyper-V Management Tools
  - ☑ Hyper-V Platform
- ☑ Internet Explorer 10
- ☐ Internet Informati…
- ☐ Internet Informati…
- ☑ Media Features
- ☐ Microsoft Message Queue (MSMQ) Server
- ☐ Network Projection

Provides the services that you can use to create and manage virtual machines and their resources.

Currently installed programs Total size: 7.31 GB
20 programs installed

**Figure 2.** *Windows Hyper-V configuration*


Windows 8 x64: Processors & Memory

**Processors**

This virtual machine is configured to use: 1 processor core

**Memory**

Increasing the memory allocation of the virtual machine can improve performance but may also reduce the performance of other running applications.

2048 MB

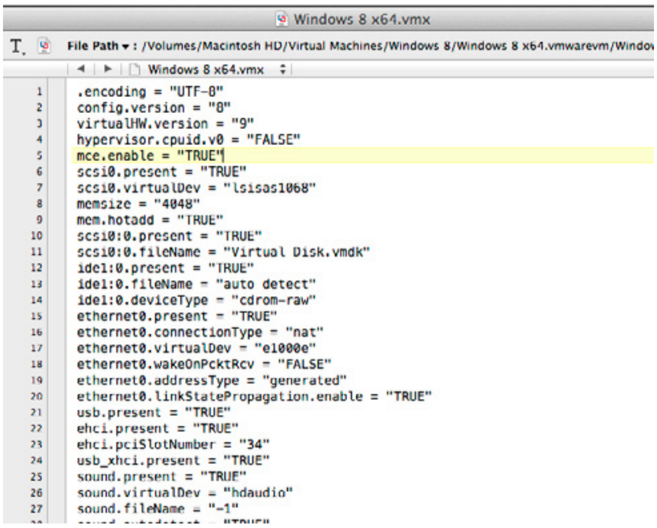
Recommended value: 2048 MB

Advanced options

☑ Enable hypervisor applications in this virtual machine
Enables running modern virtualization applications by providing support for Intel VT-x/EPT inside this virtual machine.

☐ Enable code profiling applications in this virtual machine
Enables running modern code profiling applications by providing support for CPU performance monitoring counters inside this virtual machine.

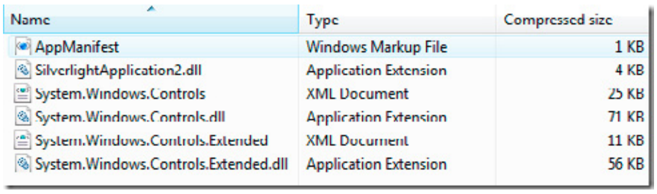
**Figure 3.** *VMware hypervisor configuration*


Windows 8 x64.vmx

File Path : /Volumes/Macintosh HD/Virtual Machines/Windows 8/Windows 8 x64.vmwarevm/Windo

```
.encoding = "UTF-8"
config.version = "8"
virtualHW.version = "9"
hypervisor.cpuid.v0 = "FALSE"
mce.enable = "TRUE"
scsi0.present = "TRUE"
scsi0.virtualDev = "lsisas1068"
memsize = "4048"
mem.hotadd = "TRUE"
scsi0:0.present = "TRUE"
scsi0:0.fileName = "Virtual Disk.vmdk"
ide1:0.present = "TRUE"
ide1:0.fileName = "auto detect"
ide1:0.deviceType = "cdrom-raw"
ethernet0.present = "TRUE"
ethernet0.connectionType = "nat"
ethernet0.virtualDev = "e1000e"
ethernet0.wakeOnPcktRcv = "FALSE"
ethernet0.addressType = "generated"
ethernet0.linkStatePropagation.enable = "TRUE"
usb.present = "TRUE"
ehci.present = "TRUE"
ehci.pciSlotNumber = "34"
usb_xhci.present = "TRUE"
sound.present = "TRUE"
sound.virtualDev = "hdaudio"
sound.fileName = "-1"
```

**Figure 4.** *Enable hypervisor support within your virtual machine .vmx file*



| Name | Type | Compressed size |
|---|---|---|
| AppManifest | Windows Markup File | 1 KB |
| SilverlightApplication2.dll | Application Extension | 4 KB |
| System.Windows.Controls | XML Document | 25 KB |
| System.Windows.Controls.dll | Application Extension | 71 KB |
| System.Windows.Controls.Extended | XML Document | 11 KB |
| System.Windows.Controls.Extended.dll | Application Extension | 56 KB |

**Figure 5.** *Unencrypted XAP file content*

**Listing 1.** *Full PlayDRM header of encrypted XAP file*

```
<WRMHEADER xmlns="http://schemas.microsoft.com/DRM/2007/03/PlayReadyHeader" version="4.0.0.0">
<DATA><PROTECTINFO><KEYLEN>16</KEYLEN><ALGID>AESCTR</ALGID></PROTECTINFO><KID>w3i0edJP7EOqQ6aQzdA
oSQ==</KID><LA_URL>http://microsoft.com/</LA_URL><CUSTOMATTRIBUTES xmlns=""><S>9FcV5qmfIsMc+X2MVmX
3Hw==</S><KGV>0</KGV></CUSTOMATTRIBUTES><CHECKSUM>Hu3+fizBvKU=</CHECKSUM></DATA>
</WRMHEADER>
```

This file is updated when compiling an application (see Figure 5).

Whilst publishing an application to the Windows Store, Microsoft will encrypt the content and digitally sign XAP file using PlayDRM. As a result, it's not possible to extract the XAP file you download from the official app stores.

The difference between a XAP file from the app store and an unencrypted XAP can be inspected by opening the XAP file headers in a text editor: Figure 6, 7 and Listing 1.

A limitation of encrypted XAP files downloaded from the app store is that they cannot run in emulators. When conducting penetration tests of a Windows Phone application using emulators it is required to obtain the XAP files of the application compiled by the developer, not from the Windows Store.

- Side-loading is the process of installing applications on a device without using the official app store. Apps can be side-loaded by copying them on a Micro-SD storage card. Windows Phone Power Tools also allows us to side-load apps to an emulator on the fly.
- Some important limitations to keep in mind:
  - Only apps signed with trusted certificates will run (on locked phones)
  - Your Windows phone will validate with the Windows Phone store that the app on the storage card is the latest release

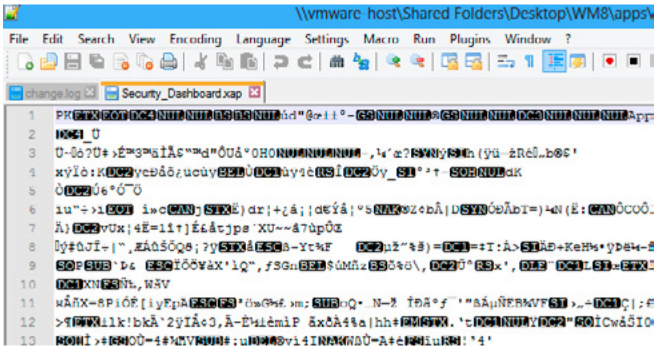

\\vmware host\Shared Folders\Desktop\WM8\apps\
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
change.log
Security_Dashboard.xap

**Figure 6.** *PK file header of unencrypted XAP file*

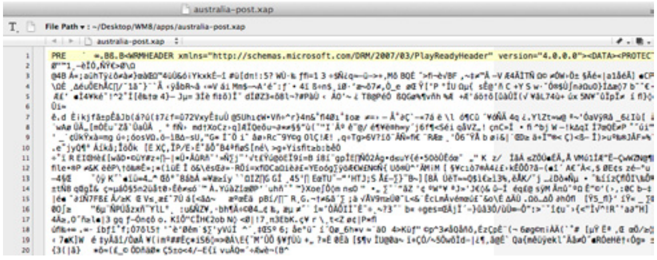
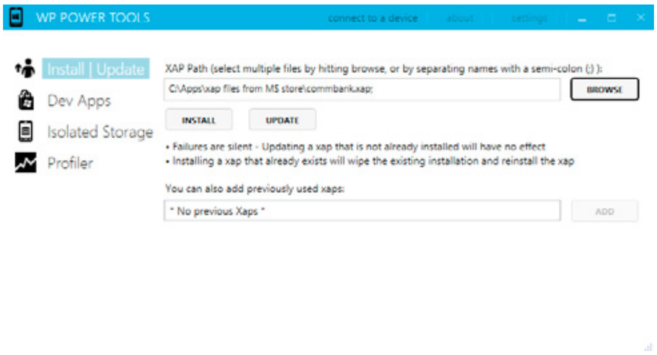


**Figure 7.** *PlayDRM header of encrypted XAP file*

## Application penetration testing

### Local file storage analysis

Applications have their own individual isolated storage space. Using Windows Phone Power Tools, we can extract and modify local configuration files of our Windows Phone application to check for information disclosure vulnerabilities or to attempt to tamper with configuration data (Figure 8 nad Figure 9).



XAP Path (select multiple files by hitting browse, or by separating names with a semi-colon (;) ):

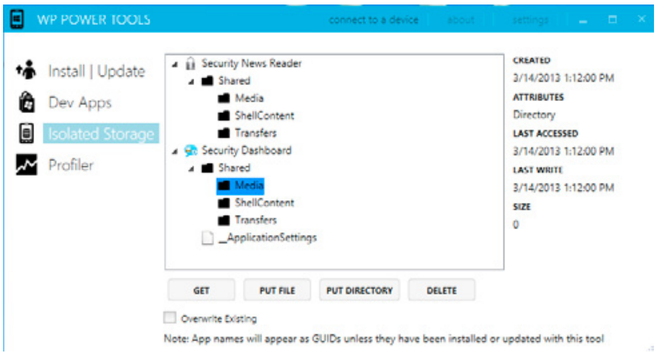
C:\Apps\xap files from MS store\commbank.xap;

- Failures are silent - Updating a xap that is not already installed will have no effect
- Installing a xap that already exists will wipe the existing installation and reinstall the xap

You can also add previously used xaps:

* No previous Xaps *

**Figure 8.** *Side-loading apps in Windows Phone Power Tools*



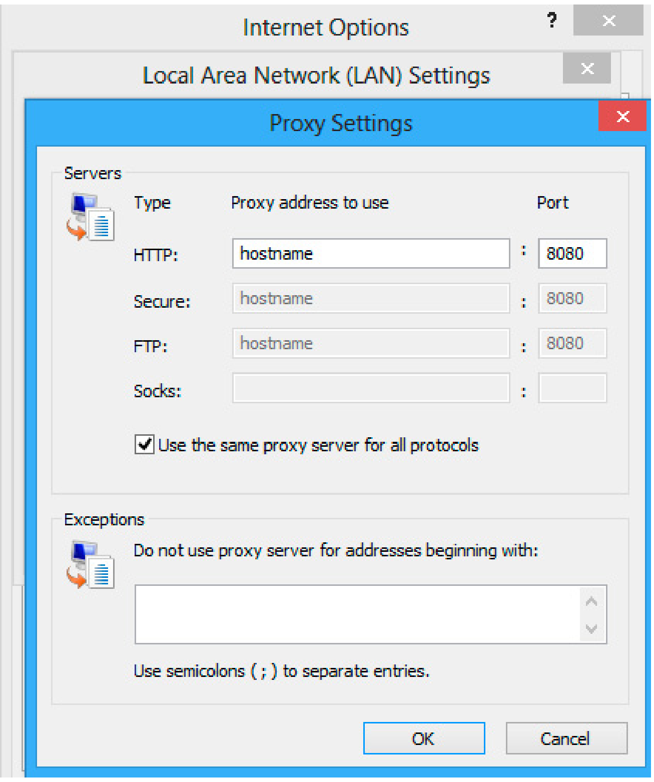
```
Security News Reader
  Shared
    Media
    ShellContent
    Transfers
Security Dashboard
  Shared
    Media
    ShellContent
    Transfers
  __ApplicationSettings
```

CREATED
3/14/2013 1:12:00 PM
ATTRIBUTES
Directory
LAST ACCESSED
3/14/2013 1:12:00 PM
LAST WRITE
3/14/2013 1:12:00 PM
SIZE
0

□ Overwrite Existing

Note: App names will appear as GUIDs unless they have been installed or updated with this tool

**Figure 9.** *Local file system analysis using Windows Phone Power Tools*



HTTP: hostname : 8080

Secure: hostname : 8080

FTP: hostname : 8080

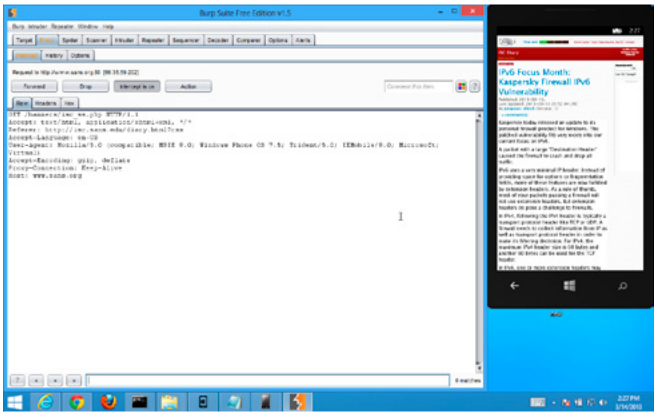
Socks: :

☑ Use the same proxy server for all protocols

Do not use proxy server for addresses beginning with:

Use semicolons ( ; ) to separate entries.

**Figure 10.** *IE proxy configuration settings*

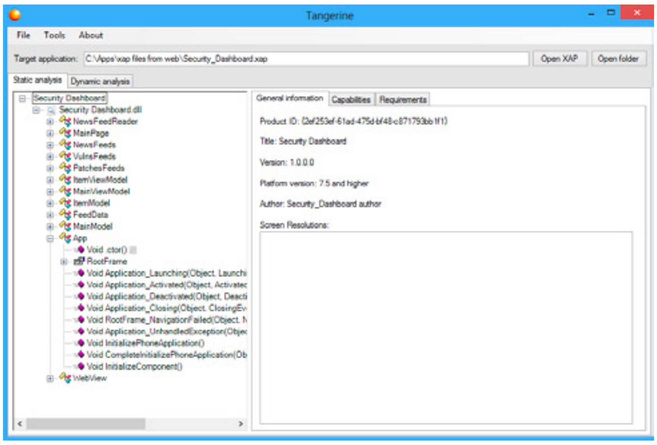


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Forward
Drop
Intercept is on
Action
Raw Headers Hex

Request to http://www.sans.org:80 [66.35.59.202]

```
GET /banners/imc_ws.php HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://isc.sans.edu/diary.html?rss
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows Phone OS 7.5; Trident/5.0; IEMobile/9.0; Microsoft;
Virtual)
Accept-Encoding: gzip, deflate
Proxy-Connection: Keep-Alive
Host: www.sans.org
```

**Figure 11.** *Analysing network traffic of your WP8 application using Burp Proxy*



Target application: C:\Apps\xap files from web\Security_Dashboard.xap

```
Security Dashboard
  Security Dashboard.dll
    NewsFeedReader
    MainPage
    NewsFeeds
    VulnsFeeds
    PatchesFeeds
    ItemViewModel
    MainViewModel
    ItemModel
    FeedData
    MainModel
    App
      Void .ctor()
      RootFrame
      Void Application_Launching(Object, Launchi
      Void Application_Activated(Object, Activatec
      Void Application_Deactivated(Object, Deacti
      Void Application_Closing(Object, ClosingEv
      Void RootFrame_NavigationFailed(Object, N
      Void Application_UnhandledException(Objec
      Void InitializePhoneApplication()
      Void CompleteInitializePhoneApplication(Ob
      Void InitializeComponent()
    WebView
```

Product ID: {2ef253ef-61ad-475d-bf48-c871793bb1f1}

Title: Security Dashboard

Version: 1.0.0.0

Platform version: 7.5 and higher

Author: Security_Dashboard author

Screen Resolutions:

**Figure 12.** *Decompiling source code using Tangerine*

## Application traffic analysis

To understand the internals of the application, we need to be able to intercept, analyse and modify information exchanged between our application and the server systems communicated with. Similar to when testing web applications, we will use our favorite web application proxy software to accomplish this. We need to keep a couple of things in mind to be able to accomplish this:

Since Windows Phone 8 emulators are Hyper-V virtual machines having its own IP address. Network traffic needs to route from the Hyper-V virtual machines through the Hyper-V host (i.e. our test machine). As a result, we need to ensure our proxy software is configured not to only listen on the LOCALHOST interface you would typically intercept on whilst assessing regular web applications, but explicitly on your HOSTNAME: Configure your IE proxy settings to proxy through your HOSTNAME, not 127.0.0.1 or LOCALHOST (Figure 10).

A restart of the emulator is required each time IE proxy configuration settings are modified as the Windows Phone emulator does not update proxy settings on the fly.

The OWASP Mobile Security Project is a good starting point outlining what your tests should focus on during mobile penetration tests, in addition to the tests you typically would conduct on other web applications (Figure 11).

## Decompiling applications

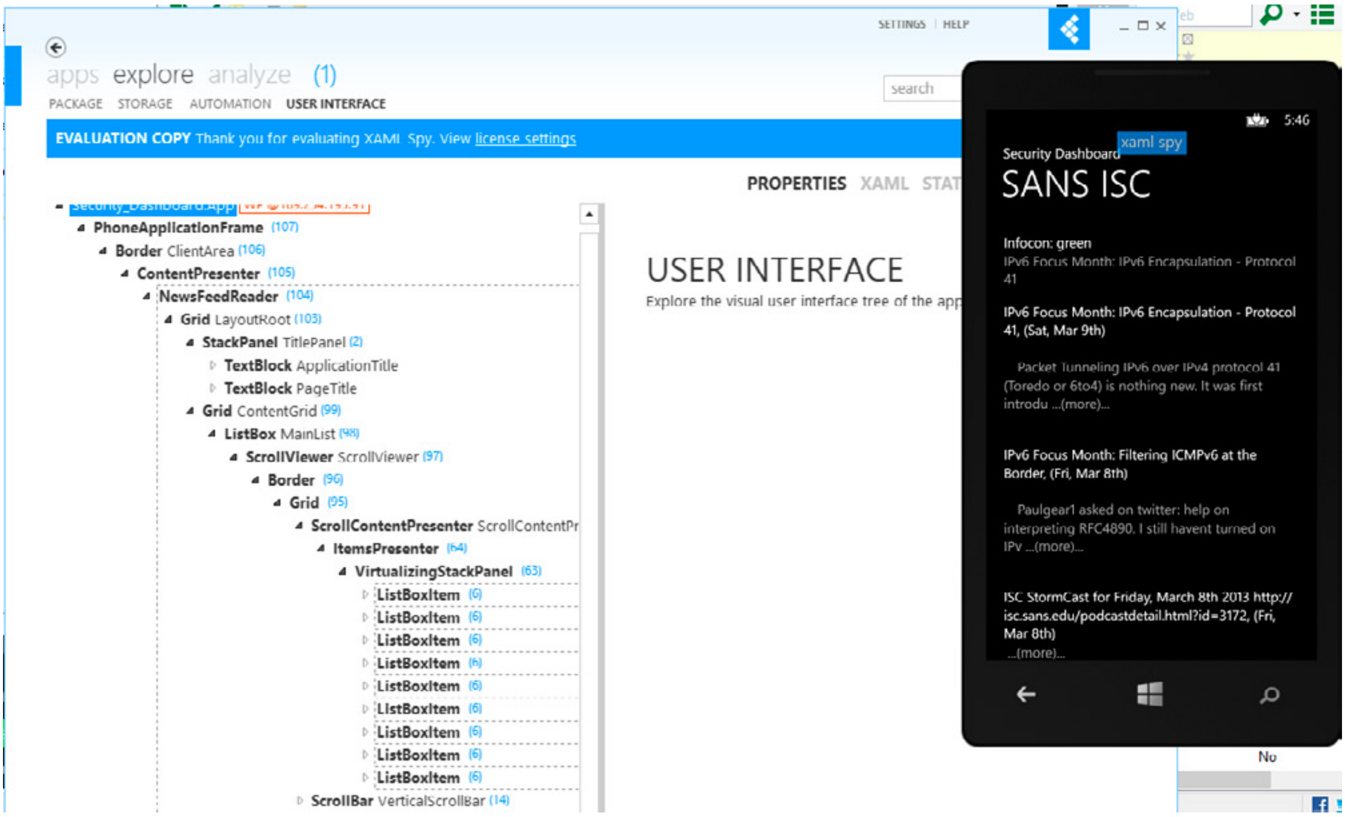
Tangerine is free software that can be used to decompile your Windows Phone applications to have a closer look at the source code for security vulnerabilities using static and dynamic analysis. Take note again that to be able to decompile the application, the XAP file of the application to test needs to be obtained from the developer, not from the Windows Store due to the PlayDRM encryption.

XAML Spy ($79, free trial) is a good commercial alternative. XAML Spy relies on third party decompilers; a prerequisite is to have one of the following three .NET decompilers installed:

- ILSPY (free), *http://ilspy.net/*
- JustDecompile (free), *http://www.telerik.com/products/decompiler.aspx/*
- Reflector ($95, free trial) *http://www.red-gate.com/products/dotnet-development/reflector/*

## Summary

This concludes the article on Windows Phone 8 security testing essentials. In summary:



EVALUATION COPY Thank you for evaluating XAML Spy. View license settings

USER INTERFACE

Explore the visual user interface tree of the app

```
Security_DashboardApp
  PhoneApplicationFrame (107)
    Border ClientArea (106)
      ContentPresenter (105)
        NewsFeedReader (104)
          Grid LayoutRoot (103)
            StackPanel TitlePanel (2)
              TextBlock ApplicationTitle
              TextBlock PageTitle
            Grid ContentGrid (99)
              ListBox MainList (98)
                ScrollViewer ScrollViewer (97)
                  Border (96)
                    Grid (95)
                      ScrollContentPresenter ScrollContentPr
                        ItemsPresenter (64)
                          VirtualizingStackPanel (63)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                            ListBoxItem (6)
                      ScrollBar VerticalScrollBar (14)
```

5:46

Security Dashboard xaml spy

SANS ISC

Infocon: green
IPv6 Focus Month: IPv6 Encapsulation - Protocol 41

IPv6 Focus Month: IPv6 Encapsulation - Protocol 41, (Sat, Mar 9th)

Packet Tunneling IPv6 over IPv4 protocol 41 (Toredo or 6to4) is nothing new. It was first introdu ...(more)...

IPv6 Focus Month: Filtering ICMPv6 at the Border, (Fri, Mar 8th)

Paulgear1 asked on twitter: help on interpreting RFC4890. I still havent turned on IPv ...(more)...

ISC StormCast for Friday, March 8th 2013 http://isc.sans.edu/podcastdetail.html?id=3172, (Fri, Mar 8th)
...(more)...

**Figure 13.** *Decompiling source code using XAML Spy*

- Black box Windows Phone 8 application penetration testing can be conducted using a physical Windows Phone 8 device but not using emulators since emulators cannot run XAP files downloaded from the Windows Store.
- White box Windows Phone 8 application penetration tests should be conducted using emulators: It is only possible to decompile XAP files of non-PlayDRM encrypted XAP files. Since there's no jailbreak yet for Windows Phone 8, analyzing local file storage only appears possible at this stage with emulators.

## References

- *http://www.neowin.net/news/windows-phone-overtakes-blackberry-in-market-share* – Windows Phone overtakes BlackBerry in usage share
- *http://www.neowin.net/news/idc-windows-phone-market-share-up-to-116-percent-by-2016* – IDC: Windows Phone market share up to 11.6 percent by 2016
- *http://forum.xda-developers.com/showthread.php?t=2340643* – Porting the Windows RT jailbreak
- *http://forum.xda-developers.com/showthread.php?t=2092158* –Windows RT jailbreak
- *http://forum.xda-developers.com/showthread.php?t=2095934* – Win86emu: Running x86 apps on WinRT devices

## WOUTER VEUGELEN

***Wouter is a cyber security consultant with nearly ten years of experience assisting organisations with information security services, including penetration tests, security architecture & design and security transformation services.***

***Wouter teaches as a mentor for SANS Institute, is exam proctor for GIAC certification exams, and is advisory board member of the ISA99 Committee on Industrial Automation and Control Systems Security and SANS GIAC. He is member of Australian Information Security Association (AISA), Information Systems Audit and Control Association (ISACA), and Information Systems Security Association (ISSA).***

***Wouter obtained his Master of Science degree in Information & Communication Security from KTH Royal Institute of Technology, Scandinavia's largest technical university. He wrote his thesis for Microsoft, where he was involved with the integration of the Belgian Electronic Identity card middleware with Windows CardSpace.***

***His Twitter handle is @veugelenw, and he is infrequently updating his blog at voipsec.eu. Contact him at wouter.veugelen@gmail.com with any questions or comments.***

# Mobile Network Traffic Analysis

Mobile network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening "under the hood". Monitoring network traffic is important in most mobile app penetration testing, yet fun to mess around with.

Nowadays the popularity of mobile app markets is higher than that of smart phones. It is exceedingly clear that most of the apps require internet connection in order to perform properly. Since the end user only sees the client front end, it is not possible to see the POSTs and GETs that the app sends to an external server in an easy manner.

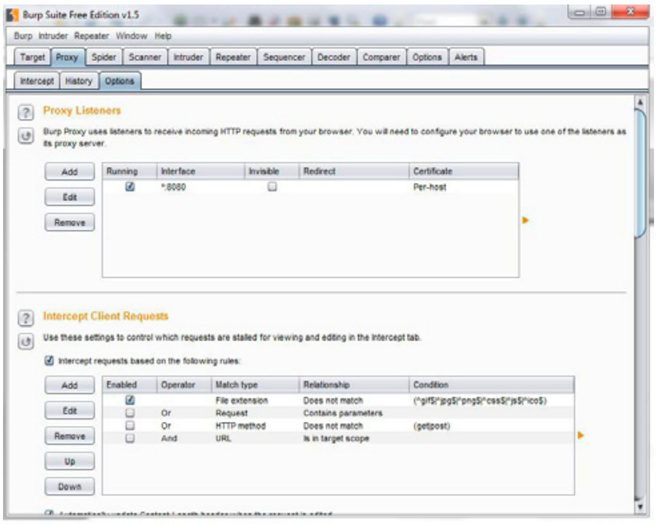
In order to monitor the traffic, 3rd party software must be used to sit in between the device and modem, as a proxy. There are many proxies in order to carry out this mission such as Fiddler, Paros and the Burp suite. In this article the Burp suite was chosen as the proxy. Burp suite is ~~a~~ Java based software that can be used to record, analyze, test, and tamper with traffic.

## Setting up the proxy

To use the Burp suite as a proxy there is a small configuration required within the software. Firstly the software can be download from it official website: *http://www.portswigger.net/burp/download.html*, Since the Burp suite written in the Java language, Java runtime environment is required to run the tool and it can be downloaded from Oracle's Sun website: *http://www.oracle.com/technetwork/java/javase/downloads/index.html.*

Additional information about the Burp suite and java applets in general can be found here: *http://www.portswigger.net/burp/help/suite_gettingstarted.html*.

After downloading and installing the Java runtime environment, we can now run the .jar Burp suite in 2 different ways. The first is to run Burp directly by double-clicking the Burp JAR file. However, it is preferable to launch Burp from the command line, as this gives you more control over its execution, in particular the amount of memory that your computer assigns to Burp. To do this, in your command prompt type a command like:



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

| Running | Interface | Invisible | Redirect | Certificate |
|---|---|---|---|---|
| ☑ | *:8080 | □ | | Per-host |

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

| Enabled | Operator | Match type | Relationship | Condition |
|---|---|---|---|---|
| ☑ | | File extension | Does not match | (^gif$\|^jpg$\|^png$\|^css$\|^js$\|^ico$) |
| □ | Or | Request | Contains parameters | |
| □ | Or | HTTP method | Does not match | (get\|post) |
| □ | And | URL | Is in target scope | |

**Figure 1.** *Burp Suite interface*

```
java -jar -Xmx1024m /path/to/burp.jar
```

where 1024 is the amount of memory (in Mb) that you want to assign to Burp, and `/path/to/burp.jar` is the location of the Burp JAR file on your computer. The first screen you see after starting the Burp suite is: Figure 1.

There are many menu tabs and features in the Burp suite, but we are not required to use any of these in this article as we are using the Burp suite just as a proxy, so after proceeding to the Proxy tab and the Options, we will be seeing a screen like this: Figure 2.

At the moment of running the Burp suite the proxy has been started to intercept traffic by default on port 8080 as we can see, but we have to change the settings to get the external traffic from the network. We need to edit the existing listener on the port 8080: after clicking the Edit button we must check the 'All interfaces' radio button in order to get this work on other devices (Figure 3).

After this stage the proxy is ready to capture all the traffic within the network on the 8080 port, but the device is not on port 8080 by default, so a small change is required on the device to alter the proxy setting.

Along with the target port we need to point the device to the machine IP address that is running the Burp suite proxy on, so we need to identify the machine's IP address first by executing `ipconfig` command in CMD on Windows and `ifconfig` in Linux/UNIX operating systems (Figure 4).

Now we have identified the IP address as *192.168.0.5* and the proxy port as *8080,* we are ready to point the mobile device to the Burp suite proxy, this can be done in iPhone and iPad by going to the Settings, Network and then change the HTTP Proxy to Manual and enter the gathered information as shown: Figure 5.

We have now connected the device to the Burp proxy and then to the internet. To test this let's

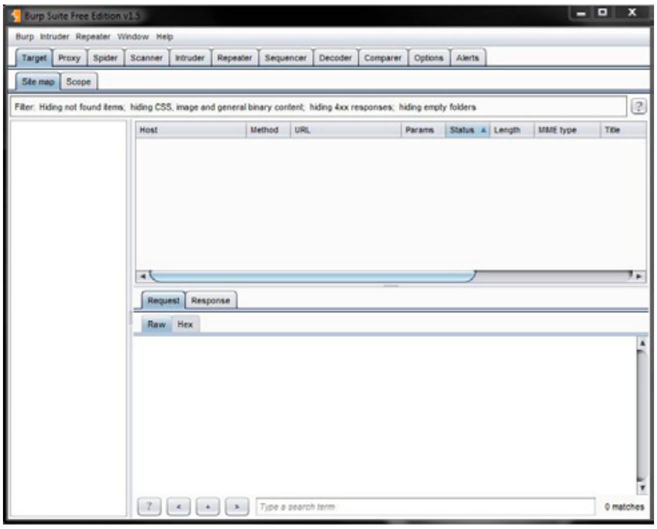
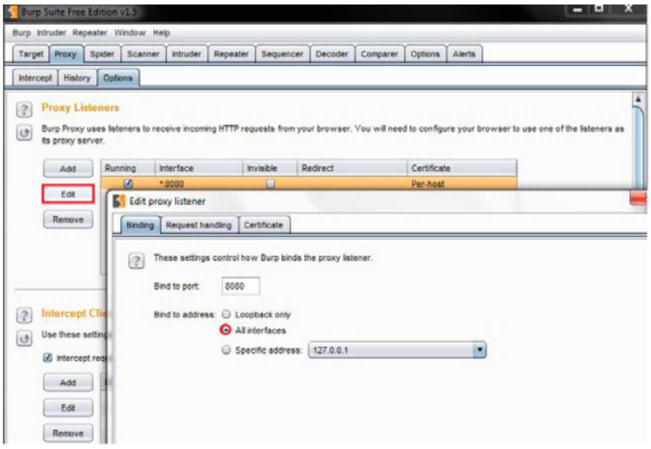

Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Site map Scope
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Status Length MIME type Title
Request Response
Raw Hex
Type a search term
0 matches

**Figure 2.** *the Proxy tab*


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Add
Edit
Remove
Intercept Cli
Use these settin
Intercept req
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

| Running | Interface | Invisible | Redirect | Certificate |
|---|---|---|---|---|
| ☑ | *:8080 | □ | | Per-host |

Edit proxy listener

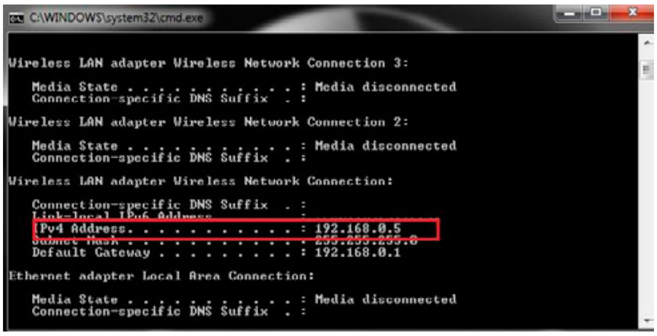
Binding | Request handling | Certificate

These settings control how Burp binds the proxy listener.

Bind to port: 8080

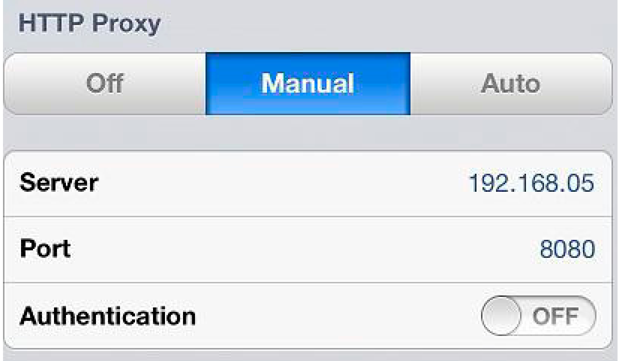
Bind to address: ○ Loopback only
● All interfaces
○ Specific address: 127.0.0.1

**Figure 3.** *Configuring the proxy*



```
Wireless LAN adapter Wireless Network Connection 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

**Figure 4.** *Identifying machine's IP address in Windows OS*



HTTP Proxy

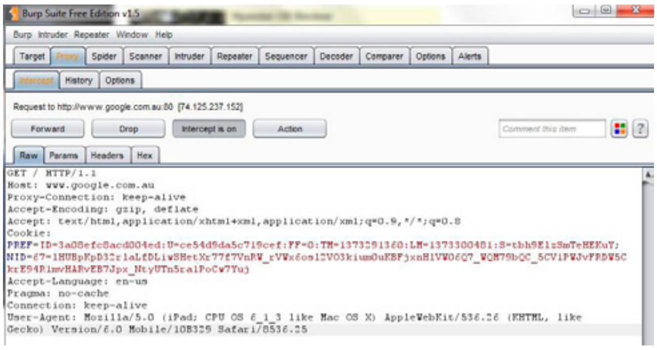
Off | [✓ Manual] | Auto

Server 192.168.05

Port 8080

Authentication OFF

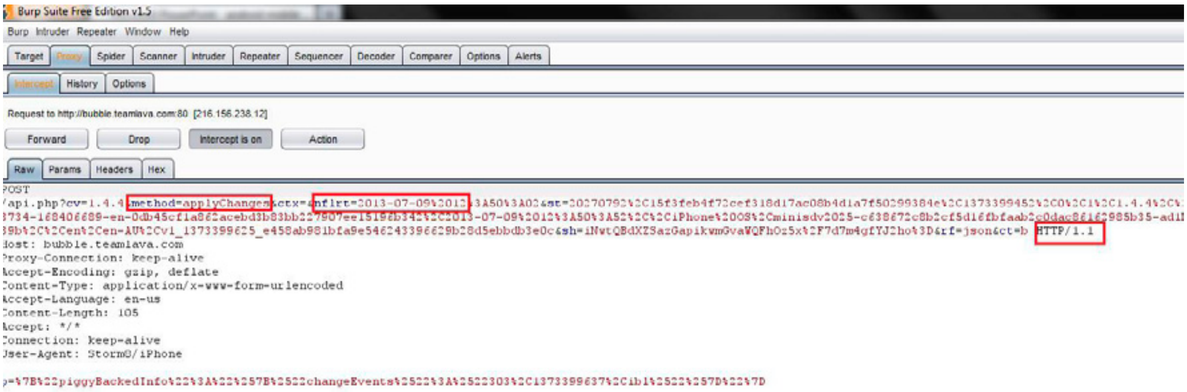
**Figure 5.** *Configuring the device*


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

Request to http://www.google.com.au:80 [74.125.237.152]

```
GET / HTTP/1.1
Host: www.google.com.au
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Cookie:
PREF=ID=3a08efc8acd004ed:U=ce54d9da5c719cef:FF=0:TM=1373291360:LM=1373300481:S=tbh9E1zSmTeHEKuY;
NID=67=1HUBpKpD32rlaLfDLiwSHetXr77f7VnRW_rVWx6os12VO3kiumOuKBFjxnH1VW06Q7_WQM79bQC_5CViPWJvFRDW5C
krE94RimvHARvEB7Jpx_NtyUTn5ra1PoCw7Yuj
Accept-Language: en-us
Pragma: no-cache
Connection: keep-alive
User-Agent: Mozilla/5.0 (iPad; CPU OS 6_1_3 like Mac OS X) AppleWebKit/536.26 (KHTML, like
Gecko) Version/6.0 Mobile/10B329 Safari/8536.25
```

**Figure 6.** *Burp Suite capturing the first session visiting google.com.au*


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Intercept History Options
Forward
Drop
Intercept is on
Action
Raw Params Headers Hex

Request to http://bubble.teamlava.com:80 [216.156.238.12]

```
POST
/api.php?cv=1.4.4&method=applyChanges&ctx=&nflrt=2013-07-09%2012%3A50%3A02&st=20270792%2C15f3feb4f72cef318d17ac08b4d1a7f50299384e%2C1373399452%2C0%2C1%2C1.4.4%2C%
3734-168406689-en-0db45cf1a862acebd3b83bb227907ee1519eb342%2C2013-07-09%2012%3A50%3A52%2C%2CiPhone%2008%2Cminisdv2025-c638672c8b2cf5d16fbfaab2c0dac86162985b35-adil
39b%2C%2Cen%2Cen-AU%2Cv1_1373399625_e458ab981bfa9e54624339662 9b28d5ebbdb3e0c&sh=iNwtQBdXZSazGapikwmGvaWQFhOz5x%2F7d7m4gfYJ2ho%3D&rf=json&ct=b HTTP/1.1
Host: bubble.teamlava.com
Proxy-Connection: keep-alive
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-us
Content-Length: 105
Accept: */*
Connection: keep-alive
User-Agent: Storm8/iPhone

p=%7B%22piggyBackedInfo%22%3A%22%257B%2522changeEvents%2522%3A%2522303%2C1373399637%2Cib1%2522%257D%22%7D
```

**Figure 7.** *Bubble Mania communication*

browse the net via the device, if everything has been set correctly this should be our first capture with the Burp suite: Figure 6.

Now we are capable of peeking under the hood and view any device its communication with the internet. This can be very useful when it comes to pentesting an app as we can check for:

- Unprotected communications (SSL and no encryption )
- Insecure file system permissions (Writing program files with poor permission)
- Exploiting buffer overflows within an app
- Insecure file system storage (such as storing sensitive data by the app; passwords, credit cards and keys on an external server
- Phone identifiers used in authentication
- Local web vulnerabilities (Tampering data with attacking vectors)
- Unauthorized access to paid-for resources

In this article we are going to discuss and analyze an issue of unprotected communication within a game, called Bubble Mania which is the most popular free game on the app store.

This is a network traffic capture taken using Burp suite when starting a level inside the game: Figure 7.

Firstly as it can clearly be seen the app using HTTP as communications protocol which is not safe when dealing with a customer's personal details, as this app offers many in-app purchases. Secondly if you have played this game you have a limited time to play the game each day, five tries everyday. This app uses the device's time and sends it to the `bubble.teamlava.com` server without encryption, this allows us to modify the date and gain extra tries every time playing this game.

Other apps behav exactly the same. For example: some apps allow a limited number of characters to be typed in their text field using a mobile device but when capturing the traffic we can edit the text field area and bypass this validation for buffer overflow exploitation since all of the iOS apps are written in objective C.

## Summary

As mentioned earlier, mobile phones are devices containing various types of personal information. As the popularity of these devices and their applications increase, so does the interest of the hackers to find and exploit vulnerabilities in these devices and apps and acquire data. Their potential attacks are aided by the functionality provided by the operating system running in the smart phones, most of the recent mobile phone application attacks are done via using only the client side of view and most pentesters ignore the network side of apps. This article demonstrated the importance of capturing and analyzing the traffic on mobile devices and how this can be useful when pen-testing an app.

**R. MILAD HOSSENI**

***R. Milad Hosseni is the founder of Austation.com, an information security web application consulting and web-service provider in Brisbane, Australia. Over the past decade, Milad Hosseni has worked as an Application Security Specialist on several large private and high-profile companies, while working on a degree in Computer Systems and Software Engineering at QUT Australia.***

# Mobile Kids Safety

## What do you need to know when your kid is using a mobile phone

In this article I will try to explain Mobile Safety. I will not go into history of mobiles and communication technology cause it is not so important for this topic.

When mobiles hit the market, we changed the way we communicate with each other. Today, smartphones have changed everything. Now, using a smartphone we can:

- Shoot videos and images
- Send and receive e-mails
- Browse the Web
- Connect with friends and family

And much more.

For businesses or private use, smartphones are just so easy and fun to use and still they are powerful and feature-rich.

Even better, you can access a hundred of thousands mobile apps to be installed on kid's phone.

There are a great and helpful apps for kids that should be installed on they mobile phone and they are free also.

Unfortunately, using smartphone can be very dangerous too. Smartphones like iPhone are almost like PC. You can do almost everything you usually do on your laptop or PC.

9 of 10 kids use social networks like Facebook on their mobile phones which is good to stay connected with known friends and family but it can be dangerous without parent supervision. In today's modern world, kids and teenagers are practically not accepted as a part of the community by their peers if they don't have a smartphone.

### What do you need to know

- Does mobile phone have Internet access
- Is Bluetooth disabled
- Is location services turned off

Let's try to give a short description:

**Does the phone have internet access?**
All UK mobile phone companies have to provide an internet filter on their phones to help block potentially harmful stuff like pornography. But, and this is the important bit for parents, most operators don't activate the filter unless you ask them to.

**Is Bluetooth enabled?**
Bluetooth enables your child's mobile phone to find and talk to other Bluetooth-enabled mobile phones in the vicinity. If it's activated, it means your child could receive unexpected and unwanted messages, and any personal information stored on your child's phone – for example, their contact list – could be vulnerable. Switching off the Bluetooth option makes the phone 'invisible' to other Bluetooth users.

### Is the phone registered for a child or adult user?

If the phone is registered to a child user, it will automatically not be able to access content rated 18+. But if your child has a phone that has been passed down to them from you or another adult, no such block will be in place. Brave the piped music and endless wait and talk to your mobile phone operator to find out if the internet filter is activated.

Scary stats

- 52% of nine year olds and 95% of 15 year olds have a mobile phone
- By 2020 most of us will connect to the internet via our mobile

Check whether parental controls are set as default on your child's mobile – if not, ask for them to be switched on.

### Can the phone access chatrooms or games where users chat to one another?

Are these moderated? Chatrooms provided by your child's mobile operator or its partners which do not have 18+ age-restrictions must be moderated. Find out about the operator's moderation policies and systems. Be aware that chatrooms accessed on the internet via your child's mobile (ie which are not provided by the mobile operator or its partners) may not be moderated.

### Is 'location services' switched off?

If you agreed to get your child a mobile precisely so that you could keep tabs on where they are, then you've got to weigh up the pros and cons, safety-wise, of your child's phone having location services switched on. It's a tricky one – Vodafone has a detailed parents' guide on the safety and privacy issues raised by location services.

Essentially, mobile phone location apps aren't necessarily provided by mobile networks and both GPS and WiFi can locate and communicate your child's location without their mobile phone operator being aware of it. Check the phone's settings, so you know where location services are on or off. Alternatively, disable the GPS or WiFi on your child's mobile.

With your teenagers, stress to them that if they use a location service alongside their social networking profile, eg Facebook, everyone on their 'friends' list will know where they are at any time, so that they

have to be 100% certain they only allow ‘real’ friends who they know and trust to locate them.

**Does your child know that they should never give out their mobile number to strangers?**
Our parents told us never to talk to strangers and we in turn need to stress to our children that they mustn’t give away any personal information to people they’ve never met before via their mobile and the internet.

### Agree on what features kids can use

Based on the age and maturity of each child, agree on phone features. Define clear rules for sensible use and the consequences for breaking them. Talk about usage: who they can talk to or text and when, the websites they can visit, and so on. With older kids, discuss cyberbullying and sexting.

From time to time, ask your kids to show you what is on their phones. Periodically re-examine rules as children mature and mobile technologies evolve.

### Teach kids safe and responsible phone use

Help kids understand the following:

- Share their phone number only with family and close friends. Do not put it on social network pages, use it to enter contests, or give it to just anyone who asks for it.
- Lock the phone with a PIN that your child keeps secret (even from best friends) to prevent others from snooping or misusing it.
- Don’t say, text, or post anything that would hurt or embarrass someone.
- Don’t make, send, or accept provocative texts, photos, or videos.
- Avoid clicking links in ads, contests, text messages (even from friends) offering free prizes and the like.

### Get help from technology

Clearly explain why you are using safety tools and what they will do for your children’s information security. Consider setting them up together.

Some protections are provided through the carrier’s service; others can be set on the mobile phone. The most reliable are those on the phone, because when a phone uses a wireless network, it bypasses the carrier and its tools.

Filter or block websites and content as appropriate for your child’s age and maturity:

- Consider blocking Internet access for the youngest; for teens, think about restricting access to gambling, adult, and other inappropriate sites.
- Filter lyrics, video, and other content that is violent or explicit.
- Restrict access to forums (including in games) unless they are moderated by humans.

Use GPS cautiously. If you use a family location service to monitor your kids’ whereabouts, make sure others cannot locate them. Otherwise, consider disabling the location feature on your child’s phone; at the very least, turn it off in the phone’s camera.

Manage contacts, which can include blocking callers and restricting contact to approved numbers only.

## What to do if there are problems

Immediately report:

- Physical threats, persistent cyberbullying, or any form of exploitation to the police and the carrier.
- Inappropriate content or behavior to the carrier or app.

## 5 Apps you can use to keep kids safe

### Sygic Family

Sygic Family keeps your family safe by allowing you to check the real-time location and the battery levels of your family members’ smartphones. You can also track your children’s whereabouts, or have them check-in periodically to let you know where they are and if they have arrived at their destination safely.

**Figure 1.** *Family by Sygic*

The app also has an in-built messaging system which lets you send messages for free over an Internet connection. You can also set Safe or Unsafe zones – a notification will be sent to you when they enter or leave these zones. There is also an SOS button available in this app, which lets you send out your exact location at the tap of the button. You never know when you might need it.

Platform: iOS | Android

### Life360

Life360 has pretty much the same things Sygic has: GPS locations of your family members via their smartphones, a panic button, and alerts when some one enters a preset zone (e.g. gets home). It also lets you check where they have been (location history), where to get help in an emergency (hospitals, police stations), and allows you to have group chats.

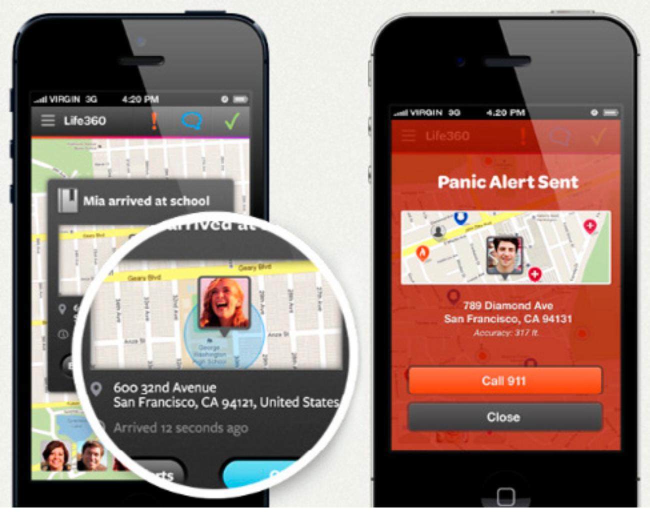


**Figure 2.** *Life360 App*

If you don't have a smartphone, you can still use this with a mobile phone at RM4.99 per month, for up to 5 mobile phones (only in the U.S.). A text message will be sent to them and once they consent to it, their location would be tracked and sent back to you. The app tries its best to not be a monitoring app but more of a communication tool to help bring families closer together and safer too.

Platform: iOS | Android | Blackberry

### mamaBear

Here is another great app for keeping your children safe; the difference is, it also helps keep your child safe online. MamaBear has a feature to keep watch over your child's Facebook feed. You will be alerted to any signs of bullying or use of crude language as well as when they check-in or get tagged on their friends' photos. The team is working on doing the same for Twitter and Instagram profiles.

Offline, you will receive alerts for when they leave a place, when they need to be picked up, when they are driving or riding past a certain speed limit, or when they explicitly need you in an SOS cry for help. This app will give you either peace of mind or great conversation starters on talking about speeding, truancy, open communication channels, and how to stay safe at all times.

Platform: iOS | Android

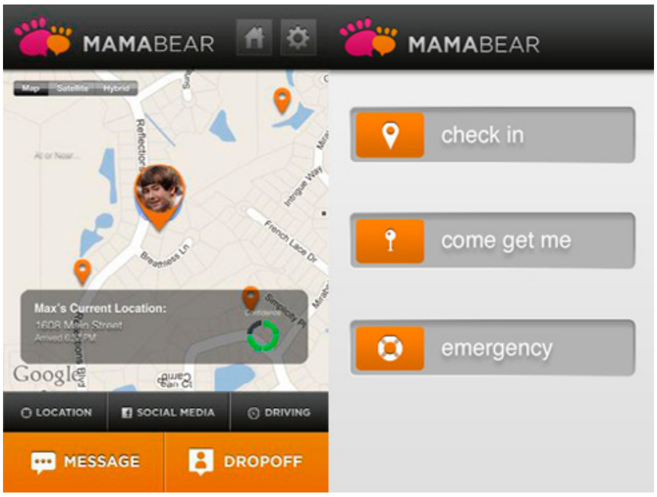


**Figure 3.** *MamaBear App*

### Google Latitude

Google Latitude is less of an app and more of a tracking tool. It allows you to see where your family members are on a map, and easily keep in touch with them. To use it, sign in to Google Latitude and start adding your family members via their Gmail contacts. When they accept, you can see their locations on Google Map on your phone.

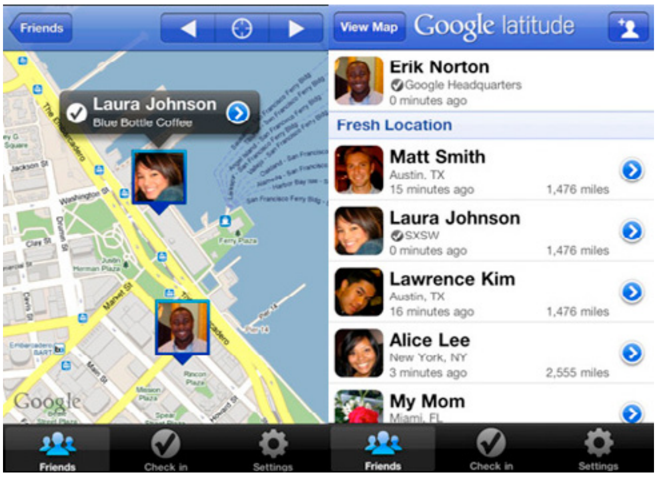


**Figure 4.** *Google Latitude App*

Their locations will be at the background even when the app is closed or when your smartphone is locked. Android users have a widget they can setup. You can also get the app to check you in automatically at a preset place. As this is not restricted to family members you can use it to check just about anyone's whereabouts, provided they are on Google Latitude.

Platform: iOS | Android

### MobileKids

This is the odd one out, but some parents may require this level of monitoring for their children. Receive alerts when your kids have been using their mobile phones in the middle of the night, when they add a new unrecognized contact, or when they download a new app. Parents will also get statistics about their children's mobile usage, which they can use to set usage limits (premium account).

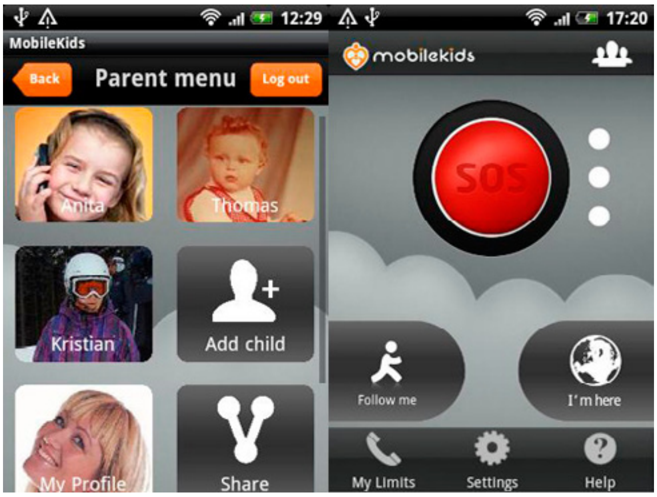


**Figure 5.** *MobileKids App*

There is still the much sought-after location feature, with a slight twist. The SOS button and Check-In feature is in but more interestingly, the child can request for their parents to track their movement live via GPS tracking, something like remotely 'walking' them to their destination.

Platform: iOS | Android

## Net Nanny Mobile Safety

Great iOS app for kids:

Net Nanny is a customizable safe Internet browser – intended to replace the Safari browser. Use a world-class Internet filter from the market leader.

Choose from 3 Safety Settings:

**HIGH**

- Blocks pornography, nudity, death, gore, abortion, mature, lingerie, swimsuits
- Masks profanity

**MEDIUM**

- Blocks pornography, nudity
- Warns for death, gore, abortion, mature, lingerie, swimsuits
- Masks profanity

**LOW**

- Blocks pornography, nudity

**IMPORTANT**

For Net Nanny to be effective, Safari and other web browsers should be removed/disabled. To disable Safari, go to Settings > General > Restrictions. In the same menu, turn off "Installing Apps" to ensure other non-filtered browsers are not installed.

**NOTE ABOUT HYPERLINKS**

Browsers other than Safari cannot open when you click hyperlinks within emails, texts, or apps. Instead, you must copy the hyperlink URL and paste it into Net Nanny. This is a limitation for all third-party browsers, not specific to Net Nanny.

PRODUCT FEATURES

- Filters Web Content
- Profanity masking
- Safe Search enforcement
- Protection on Wi-Fi, 3G/4G networks

BROWSER FEATURES

- Cut and Paste
- Pinch and Zoom
- Landscape Mode
- Multiple Tabs
- Bookmarks
- URL browsing history and suggestions
- Persistent Cookies
- Alternative Search with Google, Yahoo!, Bing

### DALIBOR VLAHO

***Dalibor Vlaho, born in 1985, in town Vukovar, Croatia. I have 15 years of computer experience and I'm holding CEH – Certified Ethical Hacker Certificate and Information Security Engineer issued by Information Security Agency. In the year 2008 I founded ISA – Information Security Agency that consists of more then 7000 Engineers Worldwide. Some of the biggest things I've done was decrypting message from Al-Qaeda. I am constantly fighting against terrorism and online child abuse. I was a part of a team who hunted down well-known On-line child abusers and reported them to the FBI. Now I am Director of Information Security Agency and Security Engineer in two companies in Abu Dhabi and Dubai.***

INFORMATION SECURITY AGENCY
ISA

# When is a Tablet safer than PC?

Magicians have just one tool for all their plans: Abrakidabra! Despite the security admins whos every day game is to "compare" various settings and equipment, and "select" the securest ones. In this article we discuss when choosing a tablet is safer than a PC and how this device helps us to upgrade our organizational security.

It is said that tablets and smartphones are not smart enough in security and since vulnerabilities rely on "security stupidity", it is judged that these new born appliances are not safe to use. The judgment has become so bold that recently some organizations preferred NOT to use smartphones and tablets. The question is: "are laptops always safer than smartphones and tablets?" The answer is No!

In this article we discuss about how a smartphone or tablet can be safer than a laptop or desktop computer. For shortening in writing, until it is not specifically mentioned we use the term Tablet generally addressing smartphones, palm pc, tablets and as the like in this category although there are differences in functionality and security.

## Main Security Advantages

### Safer Internet Network

Certain methods of data capturing and sniffing are based on LAN and traditional computer networks. For instance methods such as MAC Spoofing or Arp Poisoning are effective on a connected network, or methods like DNS poisoning works if the hacker can alter the DNS configuration of the victim which is really hard to do in a tablet using its own mobile data. In other word, while the user is not using the wired or wireless internet access it's instead using the mobile data. Since techniques for MITM or other usual sniffing methods are very hard to perform on mobile data infrastructure, therefore in some cases it is safer to use a tablet rather than a pc or laptop.

For instance, to check bank account with the application supplied by the bank on a tablet is much safer than opening the website of the bank on the laptop which is connected to a LAN with hundreds of computers especially in a guest network.

The prepared Mobile Data access on tablets can create an isolated internet access for certain purposes which such an isolation would be very hard to be designed amongst the LAN.

### More secure in the nature

In the first days when the primitive computers came into existence, nobody could even imagine that one day there would be a software which can harm the computer itself and there would be specialists who intentionally create these harmful applications. This means that the term "Security" was added to the IT dictionary long after the Operating Systems had started to work publicly. The computers and features of them grew much faster than the security systems and such different growth rate has caused a big gap between functionality and security, a gap that is still is a cozy safe house for vulnerabilities, security breaches and hackers of course!

However the cellphone manufacturers made the first smartphones in 2000, although the first real smart one came to the market in 2004. Considering the manufacturing year of first iPad which is 2010, we can come to the conclusion that when the smartphones and tablets were being designed, designers had deeper and more experienced knowledge about security. Hence the tablets platform and infrastructure are based with more security considerations. In other word, security has been present in their designing process from very scratch.

### SIM Card base design

To be SIM card based is another advantage of tablets. SIM card brings the benefits of privacy and security along with trust functionality. Currently the SIM card security, is one of the most secure and trustful technologies in the world. Nowadays when the strongest encryption and security methods are needed, SIM card comes into the picture first.

Another security benefit is that a digital signature generated base on the SIM card can be used for assuring the integrity. This signature is different from the popular signatures we use for SSL and is inserted in the presentation layer of the OSI and therefore brings higher and stronger levels of security (Ref.: “The SIM card as an Enabler for Security, Privacy, and Trust in Mobile Services” Carsten RUST, Stefano SALSANO, Lars SCHNAKE).

The point is that although laptops can use a SIM card as well as mobiles and tablets, however mobile is solely manufactured based on the SIM card. The Operating System and even the hardware of a tablet and smartphone design is involved in working by a SIM card and the SIM security roles on very low levels of the system.

The other benefit of SIM card based functionality is the uniqueness of a SIM card. Replicating a SIM card is almost impossible while replicating the MAC address as one of the most unique IDs of network can be done in a glance! Hence by using a tablet or smartphone as a SIM card based device, we can secure the network by getting much closer to confidentiality and authenticity (in the security triangle).

### Fewer Malwares

Currently there are roughly 24,000,000 virus signatures for known viruses, just known viruses! A small portion of these are related to mobile viruses and especially the known viruses for tablets and mobiles are not so very strong and destructive yet and still we haven’t experienced serious events such as viruses like Chernobil and Stuxnet. In additions there are numerous polymorphic and metamorphic computer viruses which exist in the world and change every now and then and occasionally we see various versions of them.

In addition to the fact that the number of viruses written dedicatedly for tablets are very low, we have good news that those detected tablet viruses nowadays are not effectively a real virus. In terminology, a worm is an unwanted application which can distribute itself from one client to another host automatically, a virus requires the user interaction. However for tablets, since the communication over the network and especially from one tablet to another tablet is strictly controlled by the OS and is not as smooth like in computers, the “distribution rate” of mobile malwares are dramatically slower.

Generally speaking most of tablet malwares are rather a Trojan Horse than a real distributive worm or virus and until the user dose not trust any third party application and dose not install them at all, the presence probability of malwares on his or her tablet would be reduced close to zero percent.

Furthermore, many computer viruses rely on vulnerabilities and act by leveraging intrusion attacks. Although tablets can be vulnerable to intrusions, however it is not reported yet that a serious and successful intrusion attack has occurred and is distributing from tablet to tablet! In contrast this report is very common in computers like stuxnet, Duqu, Confiker and as the like.

Overall we can say due to the low number of existing malwares for tablets and smartphones, we can be safer while surfing the internet, working with unknown files, and doing such activities.

## Other Security Benefits of Tablets

### Pocket sized

Amongst portable computer devices, the number of stolen laptops is bigger than tablets since they are handier to carry and smartphones of course can be preserved in the pocket.

### Internal Memory

Data resided in the hard disk drive of a laptop is safe guarded by the applications and OS, while they are present! By detaching the hard disk and connecting it to another computer as slave, all the security applications would be inactive and then it is much easier to crack into the hard disk data. However, typically the data of a tablet and internal memory of a smartphone is not accessible without the tablet itself, and some simple configuration can be set to wipe the data after couple of try and error for infiltration.

The size of tablets is a considerable advantage in physical security.

### Simpler applications

Tablets' applications are generally simpler. Obviously the simplicity is the first rule of security. Furthermore while the applications are simpler, there would be less vulnerabilities in them and of course there would be less security breaches.

### Wiper and Tracker

Nowadays by default many tablets are equipped to wiper and tracker features. Using this feature we can be sure if by any reason the tablet is lost or stolen, there is a way to find the device or even erase all the data in it.

Let's see of what could be found on a stolen tablet from a sales manager:

- access to his mailbox, since the username and password is saved on it, and access to the customer list and latest prices which are attached to the sent emails!
- the phone book, of all customers and…
- confidential data such as maps or technologies or other valuable assets (I had a customer who had lost four maps of a product with overall cost of $500,000 and after a month their competitor start manufacturing the same product and broke their monopoly. They were all stolen from a lost laptop)
- lots of confidential data such as pictures, SMS, banking information,…
- and so on…!

In such a case, the owner can easily track the device and if found out it is not recoverable sends an SMS command to wipe the whole data. Even if it was not feasible to send the command, the phone can be configured to wipe the whole data after five continues wrong unlock passkey.

## Tablets vs. General Threats

There is a rule: "If a hacker wants to get inside your system, he/she will and there is nothing you can do about it. The only thing you can do is to make it harder and longer to get in". However, there are some general methods which by applying them on the network we can prevent significant amount of attacks and security breaches. The reason is that there are certain attack methods which are more common due to applicability and the rest of hacking techniques are practical and feasible in very special situations.

Below we talk about some of the common hacking methods and why using a tablet can protect our data and network against them.

### Trojans and Backdoors

One of the easiest and most effective methods of hacking a system or a network, is by sending a Trojan to a computer to collect and forward sensitive data of the victim or open a Backdoor for further abuse. This technique not only is a used by hackers, but also is a common method of many malwares crawling around the internet.

Base on the different functionality of Trojans and Backdoors, a tablet resist against each in a different behavior:

#### Trojans

Trojans are harmful applications which usually contain an entertaining or useful section, and a harmful and destructive section which resides behind it. The point about a Trojan is that this malware functions only "on demand", meaning that it should be activated and run by the user. Hence if the user dose not run or install any sort of third party application at all, we can say that the user will never become a victim of a Trojan. What is important about the tablet applications in the market is that thanks to the factory preinstalled applications, tablets can survive usable without any other application at all!

#### Backdoors

Backdoors have two segments: Server and Client. The client resides on the hacker system. The hacker then puts the server segment on the victim host, then the server opens a port and starts listening to it. Communicating to that port by the client application, hacker sends command to the victim host and receives data from it.

What is important is that these sort of applications are mostly prepared packages ready to use, and of course they are made base on computer operating systems such as Microsoft Windows or Linux. Until now, researches haven't shown any existence evidence for such a malware for tablets and mobile devices.

Additionally, controlling network traffic on tablets are much easier than computers, especially an unwanted transaction can be detected and terminated faster and easier.

Therefore using a tablet is a proper defensive method against backdoors as well as Trojans.

### MAC Spoofing and Arp Poisoning

For sniffing and data capturing, two of the most effective methods are MAC Spoofing and ARP Poisoning. ARP Poisoning is used to redirect the data between two hosts to pass through another host which is the hacker system so that the hacker can see and read the sent and received data. This methodology is called as “man in the middle (MITM)”. In the MAC Spoofing, the hacker imitates an already captured MAC address of a system as its own MAC address and therefore his system would be in place of the victim host.

Both the above methods resides on LAN access and work on one broadcast domain. There are different defensive methods against data sniffing, however the final solution is to isolate and separate the data from the public network. When the isolation is the matter, we usually plan a separate wireless access point, separate switches or VLAN, separate cabling, separate ISP, and internet link and so on. However using a tablet with a mobile operator data plan will avail us all the foregoing situation already prepared and of course with less administration headache.

Note that this solution works fine when the purpose of internet usage is working with specific applications or surfing private and secure internet, and shouldn’t become a secondary risk point.

### Exploit and Intrusion

Most of applications are published containing several bugs although companies try to avoid them. Due to lack of knowledge or developers’ mistakes or many other reasons bugs remain in an application and cause it behaves irregular and act unwantedly in an especial circumstance. For instance allow a user level request to perform with administrative level privilege so that an ordinary user creates a system level service! In the most dramatic result a bug may allow a hacker to run arbitrary code (run a custom command whatsoever) or maybe crashes the application.

The good news about tablets is that there are fewer running applications in memory and it is not very common that the user keeps an application always running. Furthermore the number of active system services in a tablet is much less than a computer.

Overall we can say a tablet is less engaged with numerous applications and services and therefore is less exposed to vulnerabilities and exploits.

### Web browsers vulnerabilities

One of the most popular applications used in all the computers is the web browser. A web browser is nothing other than an application which sends and receives traffic of internet web sites. Therefore amongst all the applications on a computer, the web browser is the most exposed application to the internet traffic. Hence any vulnerability or weakness in this application is a significant exposure to the threats. The bad news is that none of the current web browsers in the marked is bug-free.

Compared to computer web browsers, tablet web browsers are quite lighter and smaller and they are not as versatile as the computer web browsers. Although this sounds like a disadvantage, however due to shorter codes and fewer number of features, bug occurrence and therefore vulnerability occurrence is less probable.

## Security Strategies

There are two popular security strategies which are usually used as the security guidelines when making any decision about the network:

- layered security strategy,
- end to end security strategy.

In this section we discuss about each of the strategies and see how we can meet the guideline by using a tablet instead of a PC.

### Layered Security Strategy

In Layered Security scenario -in a practical view-we divide the network to several layers of access or risk. Then, for each layer we create a security layer or security circle to protect that portion of the network. Sometimes in this method the portions and divisions are mistaken by the security techniques or features such as the Antivirus, IPS or Firewall and so on. The Layered Security methodology, however, divides the whole network to several points of risk such as below:

- Physical Security
- Network Security
- Host Security
- Application Security
- Data Security

These are just examples for the network portions and risk circles in the layered security plan. Each organization may have its own plan and there is no certain predefined methodology to be deployed on a network. Since the Layered Security is a complex and expensive method, this method is not very popular amongst the security designers.

After defining the segments, we assign security teams to manage the security of one or more segments and we decide what sort of equipment, hardware or software should be used in the segments. The steps which we decide whether a tablet can raise the security level of the segments or not.

Below we discuss when to choose a tablet in each layer of security:

### Physical security

It is easier to protect a tablet from thieves. If physical access is a concern, a tablet and especially a smartphone can be a good choice. As mentioned before, wiping the data of a tablet is quick and easy, and since this device can be kept in pocket we won't have to remind the client every day that: "lock you system when you leave it!"

### Network Security

When the data leaves the host, we have no more control over it, so it is vital to be sure that they go out in a correct path, toward correct destination and of course reach the destination intact. Sometimes instead of securing the network in order to make it a safe place, it is easier to change the network from a public network to a private one. If this method helps, swaping the PC with a tablet for certain tasks would be wise.

### Host Security

Generally speaking, any entity in a network which can send and receive data is called a host. One group of hosts are Endpoint Systems such as PCs, Laptops and if chosen, Tablets. In most cases, a tablet performance is not sufficient for all the client needs, however tablet can be a workaround for many complicated security scenarios which cost a lot to deploy or in some cases the best solution.

### Application Security

Patch management, updates, upgrades, checking certificates and trustability of third party applications is a part of controlling the application security. Additionally resolution of the changes and probable conflicts is another duty in this security section. Although the security administrators try to tune it up to the highest security levels, nonetheless sometimes keeping an application and its transactions secured relies on isolation and/or simplicity. In this case choosing a tablet would be a significant help.

### Data Security

Protecting the data means to have control on where they are cumulated, where they are sent, and who from where has access to them. The data are usually collected on servers on shared resources, and on the clients' computers as a private resource. Sometimes users share their private data with other users which such private resources become another publicly shared resource.

Nowadays although new features of the tablets allow the users to share their data on their tablets, however tablets and especially the smartphones are rather a private appliance and from base they are made to be private and isolated. Followed by the built-in countermeasure capabilities in these devices, protecting some critical data on a tablet looks much easier and safer than a PC or especially a laptop.

## End to End Security Strategy

In the End to End security strategy, at the first step all the gates which the data step into the network as one end, and the points in which data terminates as the other end, should be listed and categorized separately. This categorization can be based on the use or functionality. Commonly the two main ends in the networks are the internet gateway as the front end and the client computers as the endpoint.

Base on the needed security level, we should select proper solutions along with suitable equipment for that category. Deciding between a Tablet as the endpoint system or a PC and Laptop should be made in this section.

In order to protect an endpoint computer, we need to apply various security considerations which below is some examples:

- Antivirus
- Firewall
- IPS
- Physical security
- Internet Security

By changing the endpoint host from a pc or laptop to a tablet, since the hardware and especially the OS changes, we may be more secure depend on the situation.

### Antivirus

As explained before, there are less viruses for tablets and compared to the computer viruses they are considerably less destructive. Benefiting from this advantage, instead of a laptop we can use a tablet to be on a safer side. In addition, antiviruses for tablets are not as complicated as for desktops and need less management to work best. Hence just installing an antivirus for a tablet can reassure us a bit more that it will work properly! By the way most of the managed and enterprise antiviruses nowadays can control and monitor client applications installed on tablets and smartphones as well as desktop computers.

**Firewall**

A firewall task is to block unwanted ports and just allow transactions from defined known ports. The reason for using a firewall is that backdoors most of the time use irregular ports for transacting to the hacker and benefiting from a firewall will certainly block any similar harmful traffic.

However since applications on tablets work much more isolated than a pc, and whereas accessing data and files by an application on a tablet needs more permissions from the user, to have a firewall on a tablet is not as necessary as on a desktop computer or laptop. Note that to have a firewall on a tablet is of course a necessity however the absence of it will harm the tablet less than a computer.

**IPS**

Intrusion is a sort of attack which exploits a vulnerability in an application and can escalate its privilege to execute a command or cause a crash. However as mentioned before in this article, there are less known vulnerabilities in tablet's applications and therefore to use a tablet would protect us against these sorts of attacks.

In addition, there are much more built-in applications on a tablet which we can work with it without so many applications like we have on our computers. Obviously less applications means less vulnerabilities and of course more security.

**Physical security**

It is said that: "When there is physical access, there is no security". Of course there are many solutions and techniques to keep a laptop or computer safe when it is stolen or there is an unauthorized access to it. However there are some built-in security features to protect a tablet against unauthorized access and the size of most of smartphones is definitely a considerable advantage in physical security.

**Internet Security**

It is important to have a tough security plan while surfing the internet. In an endpoint host, it is necessary to define for what purpose the client will access the internet and per the need allow the user to surf the internet and define an absolute security guideline base on it. There are cases that it is a real risk to flow the user's internet traffic over the intranet, or we are worried about the potential risks in a computer or overall we need an isolated internet access for a certain user. In addition to all these reason we can add the vulnerabilities in the computer web browsers which in a computer, may lead to a sever security breaches. Considering all these, we may judge that a tablet would make a safer environment for user's internet surfing. Moreover sometimes we need a separated internet access for a particular application and not all the internet surfing. In this case, slower but safer mobile internet for just an account checking is more beneficial than a fast public internet which brings lots of security concerns.

## Conclusion

There is no final solution for security and no security scenario can be definitely more secure than others. However, a good security consultant always have a good collection of various answers for various conditions.

Tablets and smartphones as new populated devices, have first stepped in the market as Gadget devices but recently they are dramatically developed and upgraded so that they can be used for business and office use. These devices are invented when the IT industry had suffered enough from security ignorance and hackers attacks, so that they are equipped with outstanding security features.

Due to the capabilities and special environmental conditions they have, in some cases they can be a good choice to be a good substitute for a desktop computer or a laptop.

**FARZAD GHAFOURIAN**

***Farzad Ghafourian has been working as a security specialist since 2006 and has been in the information technology market from 1997. He was involved in security matters of many enterprise companies in the Middle East and Iran, the most popular targets of cyber-attacks. He has experienced the attack of Stuxnet and Wiper, two of the famous historical attacks, and wrote several articles about computer and network security.***

# Interview with Akinfe Oluwafemi

Is the President of Iris Computer Solutions, which specializes in the provision of various IT services ranging from Networking and Security to Software development. He has over 10 years of practical IT experience and holds a degree from the prestigious Federal University of Technology, Akure. He has 5 certifications; CCNA, CCNA Security, CEH, ECSA and A+ IT Technician. He has a passion for innovation in the Networking and Network Security Space. He is also an IT infrastructure support Professional. He can be found online at the following sites: http://www.iriscomputersolutions.com/ and http://247infotech.wordpress.com/.

## Could you please introduce yourself briefly?

Akinfe Oluwafemi G., the President of Iris Computer Solutions soon to be known as Roche Consulting Nigeria, which specializes in the provision of various IT and consulting services ranging from Networking and Security to Software development. I have over 10 years of IT experience and hold a degree from the prestigious Federal University of Technology. I have 5 certifications; CCNA, CCNA Security, CEH, ECSA and A+ IT Technician. I have a passion for innovation in the Networking and Network Security Space. I am also an IT infrastructure Professional. I also do some form of blogging at *http://247infotech.wordpress.com/*. I love technology writing and music. I love nature and traveling…What else can I say about me apart from my unique management style.

## Present your company and yourself within its structures.

Firstly, I would like to say that I operate Iris Computer solution with partners and we are soon to make a big transition into a full services and consulting firm which will be referred to as Roche Consulting with a renewed vigour and culture that will transform the face of IT business and consulting in Nigeria. The Transformation process has begun… Watch out!

Now to the question. Iris Computer Solutions (Soon to be known as Roche Consulting Ng) is an IT service delivery firm. I am responsible for the daily technical operations of the firm, supervising processes from IT Project commencement to commissioning and support. Projects ranging from IT Infrastructure Management, Application Design and Implementation, Security, IT risk management and Technical Support Services.

## What does your company deal with?

We service a variety of customers ranging from SMEs to Multi-nationals. We are essentially into automation using IT platforms as a tool to drive our customer's business for maximum benefit in terms of value addition. We also provide IT Security Services. This is the summary of what we do.

## Describe the team you work with.

We have a team of IT professionals with several years of experience in Applications Development, Security and Risk management, Service Management, Hardware and Software, Ethical Hackers and IT Security Professionals, Engineers, Project Managers and Accountants. All our staff are customer centered. We believe that customer is a KING and treat them as such. Every member of the team is committed to put a smile on the face of our customers at first experience – we know that there may not be a second chance.

## What services do you provide?

We provide E-commerce Services, IT Security Training, IT Risk Management and Policy development, Vulnerability testing and Management, Applications Development and testing, ERP solutions (Hospitals, FMCG, Hospitality Orgs etc.), IT Consultancy services for Government Agencies and Multinationals, IT Project Management and IT Technical Support Services.

## What are your target clients?

We provide services for SMEs, Government agencies, Banking, oil and Gas, MNCs, FMCGs and Private Organisations.

## Do you look for new employees? If so, What kind of candidates do you look for?

Yes we do. We are constantly repositioning our workforce to meet Human Resource demands. Our ideal candidate must be passionate about customer service. The techies must be professionally sound, innovative and solutions driven. People who can think outside the box and take the organization to the dream heights of success…we call this innovative ideas.

## What distinguishes you from other companies?

I will say we stand out in two things. Our passion for creating a customer experience that is positively unmatched in the market and our unparalleled innovative products and services that can be jaw-dropping most times.

## What do you think about Hakin9 Magazine and its readers?

Hackin9 Magazine overall is a good read for any in the IT security space. The offensive must be understood before the defensive can be put in place. This is what I call "Proactive Security". Hackin9 Magazine helps you understand the offensive and advices good defensive options also. A good read indeed for security newbies and professionals.

## What message would you convey to our readers?

Discard the norm of reactive security and open up to the concept of Proactive security. This is the key to success within the security space. Keep subscribing to and reading Hackin9 Magazine.

*by Julia Adamczewska*

# Interview with Dalibor Vlaho

### Could you please introduce yourself briefly?

My name is Dalibor Vlaho and I am 28 years old Security Engineer from Croatia.

I am current director of ISA – Information Security Agency and I'm working for Abu Dhabi And Dubai corporations.

In the year 2008 I founded ISA – Information Security Agency that consists of more then 7 000 Engineers Worldwide. Some of the biggest things I've done was decrypting message sent from Al-Qaeda.

I constantly fight against terrorism and Online child abuse and any other Online crime act.

I was a part of a team who hunted down well-known online child abusers and reported them to the FBI.

In 2013, I developed high quality Online Child Safety Education and Abuse-Prevention Program.

### Present your company and yourself within its structures.

For more than 5 years, ISA has existed to provide valuable intelligence to world's largest government and non-government organizations.

Today, ISA is the country's top technology agency, as well as the world's largest employer of computer security experts world-wide.

ISA was in completely secrecy but in 2013 it became publicly known.

### What does your company deal with?

ISA deals with terrorism and criminals who use computer and telecommunication technology to harm and steal sensitive information from Governments and other Organizations.

### Describe the team you work with.

Team I work with is a group of highly trained security professionals from all around the world.

They are present in more than 75 countries and they are playing a big role in the ISA.

### What services do you provide?

- Penetration Testing
- Web Application Security
- High Quality Training
- Facility Security
- Background Check

And many more

### What are your target clients?

- Government
- Non-government Organizations
- Large Corporations
- Medium Businesses

### Do you look for new employees? If so, What kind of candidates do you look for?

We are always looking to hire new engineers but as for now we have enough employees.

### What distinguishes you from other companies?

ISA is completely different and can't be compared with other agencies.

Why? ISA started as a secret organization with more than 7 000 engineers working for the ISA.

ISA's role is to monitor network traffic and search for malicious users.

When we do our work, we report it to the FBI and take steps to hunt them down.

There is no building, there is no office – We are present in the whole world to protect nations from criminals and terrorism.

### What do you think about Hakin9 Magazine and its readers?

Hakin9 Magazine is far better than other magazine we can find on the market.

It is based on Step-by-Step tutorials that are very helpful and interesting for those who try to understand how things work.

I really enjoy reading it and writing for it.

Hakin9 should be the choice number one for any of the IT Experts.

### What message would you convey to our readers?

Now at the age of 28, I have 15 years of experience in development and information security.

At the beginning of my career it was not so hard to learn new things. But spending sometimes more than 12 hours a day on it was hard.

Internet was the first place for me to find answers to my questions. Unfortunately, in my country (Croatia) there are not so many guys who can help you in learning so I was on my own in that time.

Now I am experienced and skilled enough to teach others how stuff works and I am able to conduct operations that I was not able to do before.

Use your head and your fingers to grow your knowledge and put it on higher level.

Spread your word and help other to gain more skills because good hackers are always welcome to the community.

Use your skills for good things, don't do anything stupid and remember …

***There is no exploit to get you out of the jail!***

*by Julia Adamczewska*