Mobile Security

by Tharaka Mahadewa

Security for IT and IT for security are commonly used terms in the IT industry. While IT provides diverse technological solutions to ensure the security of day to day life, IT solutions become vulnerable to threats, so security for IT came to the subject. Since early 19s people were interested about this subject and came up with different solutions to protect data and systems. In fact the cryptographic algorithms were initially used as an encryption technique during civil wars. Earlier, IT security was refered only to the protection of desktops, laptops and servers. Now it has been quiet for a long time, and today's trending topic is mobile security. With the emergence of the mobile industry, individuals and businesses find themselves enjoying the divergence of mobile solutions, but at the same time the number of threats targeting mobile solutions increases.

Mobile security has become more of a concern, since data exchange through mobile applications can directly affect businesses, as today people use their personal smart phones for business purposes as well as for personal use, known as BYOD (Bring Your Own Device). In addressing this issue, what is suggested is having knowledge transfer sessions to educate the employees or people about possible threats, while implementing a proper mobile security system. The challenging part is to keep updating the security systems to the speed of the arrival of new mobile products or applications, with the cost of transformation.

Vulnerability Analysis

Here I will be discussing the current security issues relating to mobiles, based on some recent research papers and threat reports of anti-virus companies on mobile security. Some of the identified mobile insecurities based on the white paper by Acronis International are un-secure file transferring, stolen or lost mobile devices, open Wi-Fi networks and public hotspots, malware and viruses and unclear corporate policies. Among the possible mobile security vulnerabilities, malware has taken special attention and researches are finding new approaches to mitigate them spreading, specifically Android malware.

The worldwide smartphone market is invaded by Android and iOS over the other mobile OSs like Windows and Blackberry. Figure 7 shows the worldwide smartphone market share growth over the past few years based on different OSs, analyzed by International Data Corporation (IDC), USA. Since Android owns the largest market share, malware authors are more interested about Android.

According to the recent analysis, it is identified that the Android malware mostly exist and grows faster, yet the iOS has more vulnerabilities. The reason is due to the number of Malware families being higher in Android than iOS. The F-Secure Labs 2014 Threat Report says that their analysis found 275 new malware families on Android while only one new family identified on iPhone and Symbian. Their analysis had been carried on application samples from the Google Play Store, third-party app stores, developer forums and other sources. The Symantec 2014 Security Threat Report says that the average number of Android malware families discovered per month in 2013 is five.

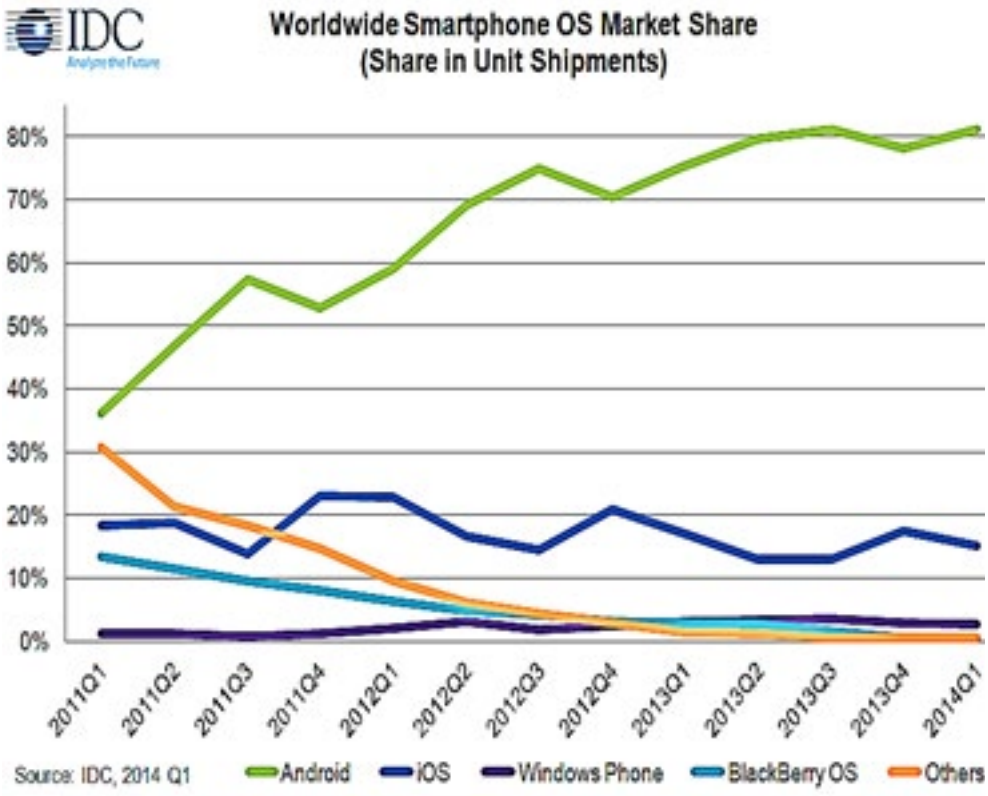


Figure 7 - International Data Corporation (IDC) USA, 2014

Why Malware Attacks? Why on Android?

The advantages gained by malware authors from infected devices are that they are able to monetize the devices, collecting personal information by spying on users and stealing the ad-revenue of application developers through embedded advertising libraries. Some facts which make the malware authors motivated on attacking mobile devices are the availability of cameras, near field communication (NFC), Bluetooth, wireless and GPS and other location services in most smartphones plus usage of mobiles for payments.

In addition to having a large market share, Android's open design which lets the users install apps from various sources is a fact for the malware authors to attack on Android. Even Android Google Play Store is vulnerable to malware attacks.

In fact some researches who had done a study on Android malware detection techniques, in their paper "Android Sandbox Comparison" at Mobile Security Technologies (MOST) 2014, states that Bouncer, introduced in Feb 2012 to analyze Play Store apps has a low rate in detecting malware and can be easily bypassed

"The risk of losing a device is still higher than the risk of malware infection."

Sophos Mobile Security Threat Report, 2014

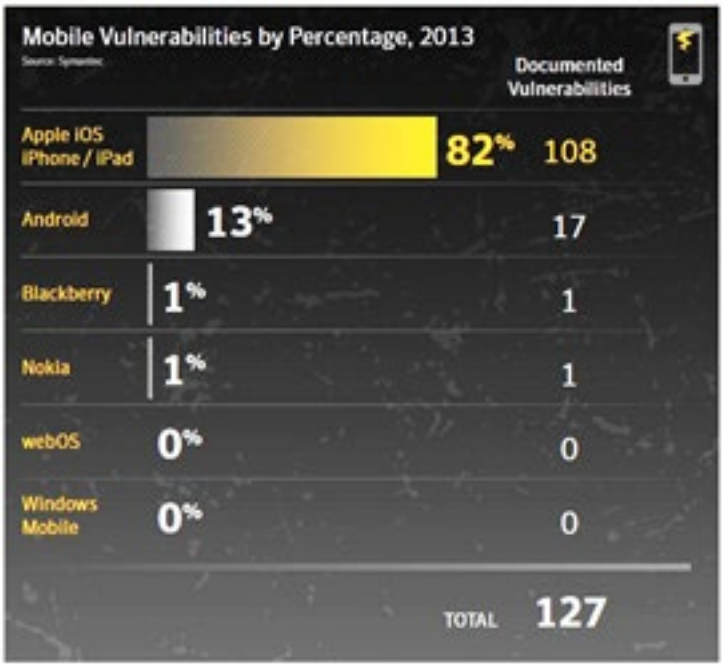


Figure 8 - Symantec's Internet Security Threat Report, 2014

How to Protect Your Device

1. When the device is lost or stolen

The basic approach is to have user authentication through a strong password, passcode or by locking the device. From business perspective a more strategic approach is required, such as the ability to remotely lock the device, wipe data remotely from the device or encrypt the data and having more control over data on the device.

2. From Malware and Viruses

Downloading applications from untrusted sources can make your device prone to be infected with malware. Android Google Play Store is considered a trusted source, yet the Play Store is also vulnerable to malware attacks.

"A good rule of thumb: if an app is asking for more information than what it needs to do its job, you shouldn't install it"

Sophos Mobile Security Threat Report, 2014

However, Android users can prevent installing non-Market apps by changing the settings, "Application > Unknown Sources", to unchecked. If you want to download an app from a third party or other source, using a reputable security software to scan can lessen the risk of been infected. When choosing a security software you

may consider the following features. Application scanner to verify downloaded apps are not malware infected, backup utility supporting remote storage to store your personal information, remote lock and remote wiping, parental control, etc.

Be aware when you give certain permissions to the application while installing it, since letting it dig into your personal information or giving more access is more or less similar to helping them achieve their target easily.

If you have "rooted" your device or "jailbroke" your iPhone, that means you have given full access to your device's OS and features. So a rooted device can be a great resource to malware authors. Since they can access data of other applications, devices used for business purposes should avoid being rooted or jail-broken and keep updating the OS to protect it from potential exploits.

In addition to the above, following are some best practices extracted from "Mobile Security Labware" which a smartphone user can adopt to prevent malware.

- Monitor Battery and Network usage, SMS or Call charges: infected device may have unusual usage of resources or charges.
- Check for suspicious behavior of device Settings: malicious apps can automatically turn on your GPS, Bluetooth, WI-FI or 3G.
- If your device overall performance is reduced or reboots frequently then most probably the device is infected with a virus unless it is a hardware problem.
- Make sure to turn off Bluetooth, WI-FI or Infrared when they are not been used.
- Do not install APK files directly from SD cards or any USB device unless you are an application developer. APK files should be digitally signed by developers that they are safe.
- Comprehensively read the reviews of the application before installing it.

Importance of Mobile Data Security

Personal User's Data Privacy

Recent studies have shown that personal smartphone users are more concerned about the privacy of their personal information while sharing them with applications and services. According to the findings by GSM Association based on the global research they carried out on more than 11,500 mobile users (including Brazil, Colombia, Indonesia, Malaysia, Singapore, Spain and the UK), in their report "MOBILE PRIVACY: Consumer research insights and considerations for policymakers" February, 2014 state that;

- 83% users *concern about sharing* their personal information when accessing the internet or apps from a mobile

- 65% users check *what info* an app wants to access and *why* before installing it
- 81% users think it is important to have the *option of giving permission* before 3rd parties use their personal information
- 41% users with privacy concerns *would limit their use of apps* unless they felt sure their personal information was better safeguarded.

So, as personal smartphone users, you should also consider the above factors before installing applications and prevent randomly installing apps just because you are interested. Usually we consider the following as sensitive information, a user must think twice before sharing or giving permissions to access.

- Sensor data: microphone, camera, GPS
- Personal data: password, email, SMS, contacts, calendars, photos, medical records
- Financial data: accounts and credit card numbers
- Authorizations to business data

Enterprise Level Data Privacy

The impact of BYOD to the data security of the organization is more significant than one would imagine. A single malware-infected device can lead the entire enterprise's network to be attacked. The cost of such an attack to the company is high and thus securing the sensitive information including proprietary and customer info has become a challenge to IT management.

The white paper on "The Business Case for Mobile Security and Management Solutions" by UBM Tech dated March, 2014 has extensively discussed the cost of mobile security breaches for an organization. Briefly, in addition to the various tangible costs the organization will have to address the problem of recovering intangible costs such as, lost employee-productivity, brand and reputation damage and lost customer-confidence.

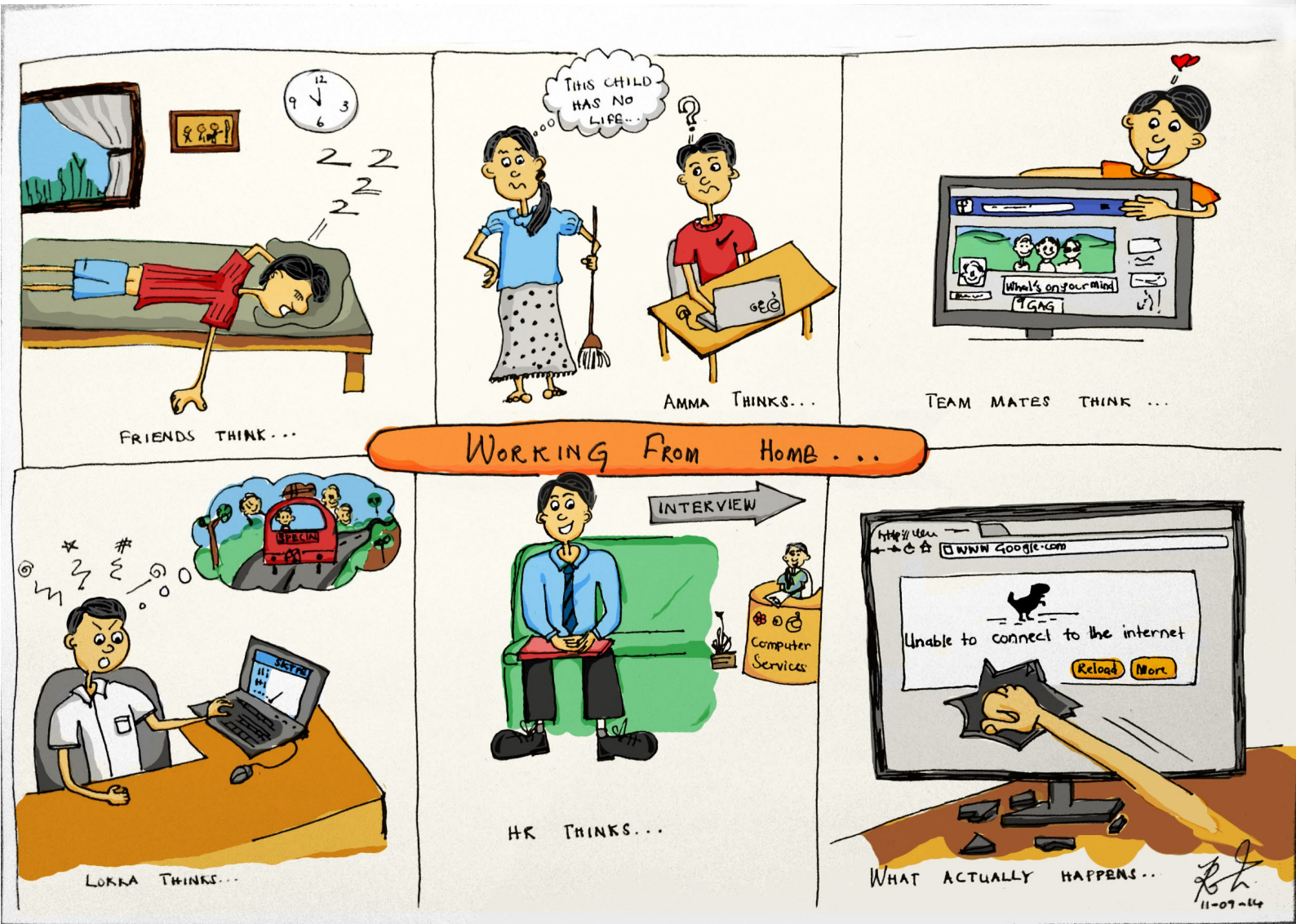
"A well planned mobile security strategy will bring a quick return on investment if it helps organizations avoid even one major security breach."

UBM Tech's Mobile Computing White Paper, 2014

The responsibility of securing company data is equally owned by the management and the employees of the organization. While organization implementing the security system plus access policies, employees will have to adhere to them. According to the survey report "Mobile Content Security and Productivity" by – "© AIIM 2013 www.aiim.org / © Accellion, Inc. 2013 www.accellion.com" only 18% of the sample participants believe that they are fully compliant with company policies, industry regulations or statutory government mandates.

Further they describe how a MDM (Mobile Device Management) platform can address the issue, since MDM supports managing the mobile devices use for business purpose, whether it belongs to the company or the employee. MDM can restrict the access-to-connect to the corporate data, monitor their usage, configure settings, deploy approved applications, wipe data remotely and even app store, can be used to store applications that use corporate data, free from malware.

Author of the survey report Nick Geddes recommend to combine the MDM platform with an ECM access and content management application to provide true mobile content management, since MDM has limited content capabilities.



Working From Home by Yasassri Rathnayake

Source Index

Topic	Reference	Page	Source
Becoming an IT professional	Figure 2	7	National ICT Workforce Survey - January 2010
	Figure 3	7	National ICT Workforce Survey - January 2010
	Content		http://www.bcs.org/category/17705
When to go Grails	Content	12	http://www.techempower.com/benchmarks
Who was Orson Welles and why he still matters?	Content		McBride, Joseph (2006) What Ever Happened to Orson Welles? A Portrait of an Independent Career Walsh, David (2013) The Sky Between the Leaves: Film reviews essays and interviews 1992-2012
Spring 4.0 – Evolution or Revolution	Figure 4	19	https://raw.githubusercontent.com/raffaelschmid/presentation-spring-4.0/master/docs/techevent-spring-4.0.pdf
Digital Games	Content		A.Garza & C.J.Ferguson, (2011). Call of (civic) duty: Action games and civic behavior in a large sample of youth. M.Schmierbach, (2010). "Killing spree": Exploring the connection between competitive game play and aggressive cognition. Effect of playing violent video games cooperatively or competitively on subsequent cooperative behavior D.A Gentile (2009). Pathological video-game use among youth D.A Gentile & J.R Gentile (2008). In-group versus outgroup conflict in the context of violent video game play N. Gill (2012). http://media.moddb.com/images/articles/1/94/93253/need_for_speed_world-wide.jpg http://assets.vg247.com/current//2014/05/call_of_duty.jpg
Mobile Security	Figure 7	32	Smartphone OS Market Share, Q1 2014: http://www.idc.com/prodserv/smartphone-ms-img/chart-ww-smartphone-os-market-share.png
	Figure 8	33	Symantec Corporation's INTERNET SECURITY THREAT REPORT 2014: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
	Content		Acronis's White Paper: Top Five Security Threats for the Mobile Enterprise and How to Address Them : http://promo.acronis.com/rs/acronis/images/WP_Top5_Mobile_Security_US_EN_130306.pdf Acronis's White Paper: Top Five Security Threats for the Mobile Enterprise and How to Address Them : http://promo.acronis.com/rs/acronis/images/WP_Top5_Mobile_Security_US_EN_130306.pdf International Data Corporation: Market research company, USA: http://www.idc.com/prodserv/smartphone-os-market-share.jsp F-Secure 's MOBILE THREAT REPORT Q1 2014: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014_print.pdf Mobile Security Technologies (Most) 2014 – Workshop: http://mostconf.org/2014/ Enter Sandbox - Android Sandbox Comparison: http://mostconf.org/2014/papers/s3p1.pdf Sophos Mobile Security Threat Report: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf Mobile Security Labware: https://sites.google.com/site/mobilesecuritylabware/4-mobile-malware/malware_prelab_activities Mobile Privacy: http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf UBM Tech Mobile Computing: http://www.informationweek.com/whitepaper/download/showPDF?articleID=191741382 Mobile Content Security and Productivity: http://www.informationweek.com/whitepaper/download/showPDF?articleID=191740910