International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 1, January- 2013

Current Security Issues posed by Mobile Devices

Syed Abdul Wahab Asif
Associate Professor,
Nizam Institute of Engineering and Technology.

Dr.D.Vasumathi
Associate Professor,
JNTU College of Engineering and Technology.
JNTUH,Kukatpally.

Zeeshan Fatima Armeen
Assistant Professor,
Nizam Institute of Engineering and Technology.

Shaik Abdul Rasheed
Assistant Professor,
Nizam Institute of Engineering and Technology.

Abstract

The majority of mobile and remote user devices, including home PCs, notebooks, PDAs and smartphones, are not adequately protected. The growing business use of personally owned equipment, and improvements in personal device functionality and storage capabilities, are making mobile security an increasingly serious problem for enterprises. The greater the functionality of the device, and the lower the level of influence that the IT organization has over the device and its user, the greater the risk. User-owned IT is a reality, even in the most-conservative and risk-averse organizations, but its risks can be contained — if they are understood.
Enterprises' greatest concern about mobile devices is the potential for data leakage caused by an unauthorized person gaining access to sensitive information. Loss of access to information — whether temporary or permanent — represents a greater risk.
The good news is that a growing variety of technical controls are available to safely accommodate the urgent demand for the greater flexibility and convenience offered by mobile devices, including those that are not owned or directly controlled by the enterprise.

Keywords: Mobile Security Issues in a Corporate Environment, The Perfect Protection Strategy, Protecting Yourself against Attacks

1. INTRODUCTION

As you might expect, mobile data users move faster than the rest of the business world. They adopt new tools quickly. They adapt to new policies and protocols readily. They overcome obstacles with pragmatism and speed. Keeping up with the mobile workforce has kept network administrators on their toes. But looking ahead, IT departments are looking far beyond their role as fleet managers for a fringe group. They must now address the growing number of mobile users at all levels of their organization and look to provide more than simply access. They must now reach this mobile workforce through specialized services and custom-developed applications.

At the heart of all mobile activity is the paramount importance of security. As users take on multiple devices (tablets, smart phones, etc.), connect to an increasing menu of wireless peripherals (storage drives, printers, etc.) and flirt with an explosion of exciting new applications, the need to secure every endpoint has forced IT directors to reassess their entire mobile strategy and architecture.

To help you plan for the coming year, Good Technology has identified six trends that will drive mobile security issues.

1.1 Data Security

Data security is keeping all the information the enterprise controls safe, including everything stored on cell phones, laptops and other devices in the field. Sound hard? Well, it is - and getting harder. The best approach is defense in depth, which relies on many approaches at many levels. While the details are complex, defense in depth relies on the common-sense assumption that malware or intruders that elude one level will be caught by another.

1.2 Mobile Device Security

Mobile devices have their own characteristics and unique security issues. Security threats that go hand in hand with mobility include data exposure through the WLAN, exposure of your network through unsecured public-access points, lost or stolen devices, mobile viruses and other malware. Mobile-device management software offers an umbrella solution, but strong user policies and basics, such as data encryption, remain key elements in a successful mobile security plan.

1.3 Mobile Devices

Mobile devices are aimed at workers and consumers not working from a wired outlet. The mobile device category is expanding by leaps and bounds, and includes everything from cell phones, feature phones and smart phones to laptops, mobile Internet devices (MIDs), tablet computers and ultra-mobile PCs (UMPCs). Mobile devices are benefiting from the growth of 3G networks and will become even more ubiquitous as 4G grows. There is more diversity in the types of devices and operating systems than in the desktop world.

1.4 Network Security

Network security is a broad term that encompasses the protection, integrity and continuity of network-based assets, which include hardware, software and data, along with related network services. Key elements of network security include strong user policies, network-access controls, and intrusion-prevention systems, which fend off malicious attacks through the Internet or determine access to shared network software. Wireless networks require an even more intricate security matrix.

1.5 Security Policy

An organization's security policy is its basic plan to protect data, devices and its network. The key is to determine what data and devices are the most sensitive and work backward to data and devices that are less critical. Among many other elements, security policies cover access rights of employees and outsiders, how to handle mobile workers, procedures for quickly terminating access rights of people who are fired or quit and security maintenance procedures such as updates and patches.

1.6 Strategic Planning

Simply put, strategic planning determines where an organization is going over the next year or period of time, how it's going to get there, and how it will know if or when it gets there. Often even more important than the actual plan produced, the process helps the organization clarify its plans and ensure that key leaders are all on the same page. Beyond merely defining the organization's purpose and goals, such planning also includes ways to measure whether and how those goals are achieved.

2. Top Five Privacy Issues Facing Mobile In 2013

Given the personal nature of mobile as well as its ability to collect data about users, 2013 will be a perilous time as the industry faces growing scrutiny around mobile privacy from regulators.

The mobile industry could see greater enforcement around mobile privacy this year on a couple of different fronts, including location-based data and privacy policies for children. In an interview with Mobile Marketer, director of The Future of Privacy Forum Jules Polonetsky talks about why privacy is such an important issue in 2013.

“The reason I think privacy is going to be critical to mobile is that we are seeing such robust use of data,” Mr. Polonetsky said. “We are starting to see companies emerging that are appending third-party data, tracking users across many apps and integrating smarter uses of location.

“Making sure that users feel mobile devices are becoming more useful to them and are not tracking them is important,” he said. “We cannot afford for consumers to have a nagging sense of lack of control for a device that is so personal.

“People already feel this way about their PCs but they tolerate it. It seems less likely that people will tolerate a device that is in their pocket as being anything less than something they are in control of.”

One specific areas of focus is likely to be reaching children via mobile devices, with the Federal Trade Commission expected to address how children use mobile apps and smartphones. New rules or guidelines could significantly impact mobile marketing.

Location-based services and apps will also be an important part of the discussion surrounding mobile and privacy in 2013 as the need for geo-based information to provide certain mobile services clashes with consumer desire for privacy.

Below, Mr. Polonetksy addresses what will be the top five privacy issues facing the mobile industry in 2013.

What are the challenges in mobile privacy?

Folks are struggling to figure out what identifiers should be used because there are no ubiquitous cookies in mobile as there are for desktop. This has helped create an infrastructure for desktop that provides controls for users.

In mobile, people have cobbled together what they can but the opt-out framework is not there. People are looking for digital fingerprints, something that allows tracking and gives users a choice.

It is important to address this issue because the data is there, people are building databases. But, to opt out today in mobile can be challenging.

In some cases, you have to copy the 40 character unique identifier code for a phone and submit it.

What is the mood in Washington towards mobile and privacy?

On the Hill, everyone is sitting on the edge of their seats because we expect the release of two major privacy documents in the upcoming weeks and months. This could be the first time any White House has gone on record supporting a comprehensive privacy law.

Previously, the White House supported self-regulation for everything other than healthcare and financial services The White House is expected to endorse a privacy framework that would see stakeholders in specific sectors coming up with self-regulation.

If the Federal Trade Commission thinks the rules determined by a sector are adequate, it would endorse them and have the authority to enforce them as if they were law.

How might any changes to COPPA affect mobile companies?

The FTC has proposed an update to Children's Online Privacy Protection Act. Folks were worried that they would raise the age but they are keeping the age at 13. The FTC is proposing changes around tracking on a children's Web site that deems the information personal, so children would need a parent's permission.

If you are going to collect personal information from those who are under the age of 13, you are going to have to get permission.

The FTC has said it does not think mobile is any different from the Web when it comes to privacy policies. They do not care what kind of device is used, they are complaining about Web site privacy policies and that covers any place, including mobile.

We are already seeing some companies that track mobile and Web usage dropping kid's sites because suddenly it is too risky.

What do marketers need to know about location and privacy?

Location services are one of the big trends in mobile this year but, are these services likely to run afoul of regulators? How is location being shared is that something that needs to be resolved.

If I am an app developer and I don't need location for my service, should I be asking for location? If I am asking just for the ads, should I be making that clear to users?

If I do have geographic integration, can I give the information to my ad network and let them use it and sell it?

There is not yet a good set of rules for what you can do with location to make advertising more effective and this is where companies are going to invite controversy.

Companies should not sell and trade away this information so that other services can build a profile of where a user has been over time. Let us make the ad smarter for the user but let us not lose control of the user's history.

What's the best way to do mobile-friendly privacy policies?

Some companies are working on these issues. Google apps enable users to request that AdMob not track their behavior while the iPhone gives users an option to not send their location to iAds.

There are still some problems around executing privacy policies in mobile, however. For example, an app developer who wants to provide a privacy policy might have a hard time doing so in the Apple Store because of the way the content is controlled.

There is a whole range of issues around giving notice adequately, having a privacy-friendly way to tailor ads and good practices around location that the Direct Marketing Association and the Mobile Marketing Association are working on.

In a recent survey, we found that free apps were twice as responsible as paid apps in terms of having privacy policies. Free apps, because they are ad supported, are more likely to be explaining this to users with a privacy policy.

Overall, there is still a low rate of mobile app developers that have privacy policies.

If you do have a privacy policy, make sure it is easily findable.

3. Mobile Security Issues in a Corporate Environment

The smartphone market is accelerating at a rapid rate. According to current estimates by the industry association BITKOM [1], the global IT and communications market will grow by 4.8 percent this year. Mobile communication devices – and smartphones in particular – are leading this charge, with experts predicting a huge 11.5 percent increase in their sales. Sales of smartphones have even overtaken those of PCs, and the devices are becoming increasingly popular for both business and private use.

As a result, companies which don't necessarily require their staff to use smartphones are becoming obliged by their employees' usage and personal experience of these practical devices to implement them for business purposes.

In many companies, employees are also given their choice of end device as an incentive. The European Information Technology Organisation (EITO) predicts global sales of 1.4 billion mobile phones for 2011.

3.1 The Dynamic Smartphone Market

Anyone looking closely at the smartphone market will notice that there is currently no operating system which predominates, to the extent that Windows does for computers. Instead, as Canalys' latest market analysis shows, several providers are well-positioned and are helping themselves to respectable pieces of the smartphone pie. Thanks to a wide range of devices which span the price spectrum, the Android platform has profited most from the recent market growth. With 33.3 million Android smartphones, Google has secured itself a market share of 32.9 percent, making it the market leader. Second place is, however, not occupied by Apple and its ubiquitous iPhone. Instead, Symbian's market share of 30.6 percent (31 million devices) puts it right behind Google and clearly ahead of Apple. Only then does the iPhone operating system iOS enter the field, with 16.2 million devices and a market share of "just" 16 percent.

Next come the BlackBerry devices so popular with business users, with a market share of 14.4 percent. Bringing up the rear is Microsoft with its current Windows operating systems and a total market share of 3.1 percent. The smartphone market also presents a challenge for analysts, as predicting it is extremely difficult. Just a year ago, iOS's market share (16.3 percent) was similarly high.

Last year, BlackBerry devices still retained a fifth of the market, while Android, the current leader, was bobbing around at the back with 8.7 percent. This put it just in front of Windows Mobile which, at the time, had 7.2 percent. A year ago, Symbian was still the market leader – and by a very large margin, with 44.4 percent of the market share.

As a current survey carried out by Forbes Insights shows, however, the smartphone share of the business market is now quite different. 87 percent of management in US companies use laptops, and 82 percent also own smartphones. 28 percent are "dual-device owners" who, in addition to a BlackBerry – the classic corporate mail machine – also own an Android-based mobile device or an iPhone. The smartphone is the communication device of choice for more than half of those surveyed.

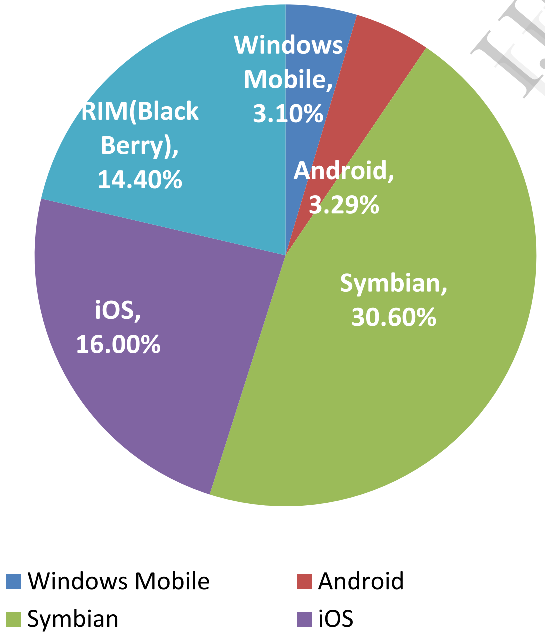


Fig 1: Survey of Smart Phones

3.2 Smartphone Protection Is Mandatory

Why, though, should companies incorporate smartphones into their security strategies? The simple answer is that smartphones have many uses, making it important to protect these mobile platforms.

In companies, smartphones are most commonly used to access communications networks – primarily phone and email systems, but also (and increasingly) other messaging systems, including scheduling management systems. They are also used to gain comprehensive access to contact databases.

In such cases, the confidentiality of sensitive company data must be ensured. Third parties should not be permitted access to business emails, nor – of course – should they be able to access customer or vendor information.

The next step involves accessing corporate networks. Employees usually use a VPN connection to dial into the corporate network, from where they can access files and business applications like ERP systems (Enterprise Resource Planning).

It is important that companies must take action here to prevent unauthorized users from accessing internal company information, siphoning off data, or manipulating existing applications.

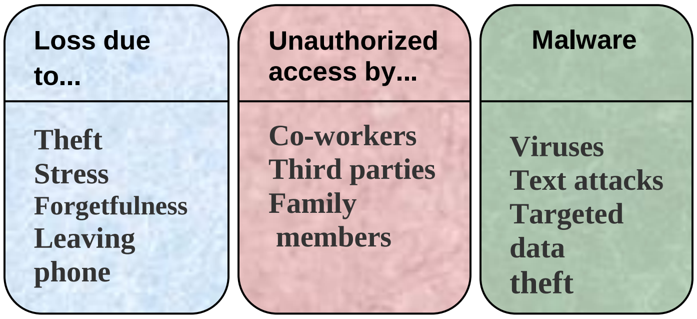
For years, it has been common practice for companies to have protective strategies in place to cover their servers, workstations and other IT components. Protecting smartphones used for business purposes is, unfortunately, not yet a fixed component of corporate security policies. Given the various smartphone uses listed above, protecting your company's smartphones would be a wise move.

14:18
McAfee Security
McAfee
Mobile Security
Security Scan
Protect against viruses and other threats
Data Backup
Backup personal data and media
Data Restore
Restore contacts and SMS
Lock Device
Lock the device now! (You can unlock i with your PIN)
Wipe Data
Wipe all personal data, media and memory card
SiteAdvisor
Browse and search securely
menu

Fig 2: Smart phone Security

3.3 The Perfect Protection Strategy

There are three basic scenarios against which smartphones should be protected. The most common is Case1: loss or theft. According to BITKOM studies, 10 million Germans have already lost a mobile phone [4] and in a recently conducted survey during January 2011 across 4 European countries, targeting mobile users from the age of 14 and upwards, 20% said their mobile devices had either been stolen or lost. Case 2 is similar to Case 1: someone else gains complete access to your mobile device for a short time. Let's take a popular example: an employee leaves his smartphone lying on his desk during the lunch break, and a co-worker or third party picks it up. Here, too, the risk of misuse of corporate information through unauthorised access is a real one. Case 3 combines all the other threat scenarios – including malware specifically designed for mobile devices, SMS attacks, and targeted data theft via specially-designed emails or websites. What makes this case different, however, is that the attackers do not have physical access to the device.



Loss due to...	Unauthorized access by...	Malware
Theft Stress Forgetfulness Leaving phone	Co-workers Third parties Family members	Viruses Text attacks Targeted data theft

Fig 3: Three basic scenarios of protecting smartphone

3.4 Protecting Yourself against Loss and Theft

If your smartphone is lost or stolen, a third party gains physical access to your device. If the finder is dishonest, he or she now has all the time in the world to access the information stored on the smartphone. Not only is the data stored on the mobile device itself valuable, but login information for corporate networks or communications services is also of interest. If VPN or mail server passwords are stored in your phone, the thief only has to touch the appropriate application to gain access. Protective software like Kaspersky Endpoint Security 8 for Smartphone contains special anti-theft functions to prevent third parties from accessing information on missing devices. Lost smartphones can even be blocked remotely using special management software. Devices with GPS receivers – a feature which is already built into most business smartphones – can also be located. Alternatively, you could take more drastic measures and use a delete command to restore the device completely to its factory settings.

While the lost device itself must still be replaced, doing so does not pose a problem for most companies, and resetting it prevents sensitive corporate data from falling into the wrong hands.

A professional thief will quickly take measures to avoid being detected. One of his or her first acts, therefore, will be to remove the SIM card. Here, too, however, Kaspersky Endpoint Security for Smartphones has a solution: the SIM Watch function enables management software to keep track of the device, even if the SIM card is removed. Even the new mobile number is automatically texted to the phone's rightful owner.

But what if the smartphone can't be locked down in time? In such cases, encryption comes in handy. This tried and tested method has proven effective in protecting data on laptops for years. Files, folders and storage media can be irrecoverably encrypted using Kaspersky Endpoint Security, insuring that only those with the correct password can access the data.

3.5 Protecting Yourself against Attacks

The perfect protective software for mobile devices:

- Access blocks
- Encryption
- Privacy protection
- "Over-the-air" management
- Support for rules
- Multi-platform support

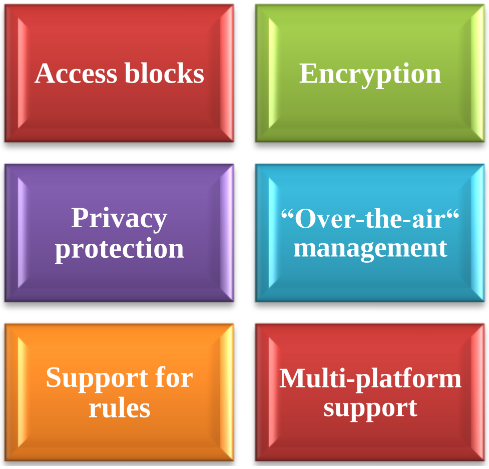


Fig 4: Six perfect protective softwares for mobile devices

The problem of mobile malware is one which is often dismissed. After all, the numbers cannot possibly compare to the current Windows situation. While malware for diverse mobile platforms do exist – such as Trojans which send texts to premium services in order to run up huge bills for the phone owners, for example – there have only been a few major virus outbreaks to date. Caution is, however, advised, as the increasing popularity of smartphones and tablets is making them interesting targets for malware authors. It is also worth noting that not all virus attacks are necessarily aimed at causing media sensations. Security experts have been observing the malware scene's increasing professionalization for years now. Quality comes before quantity, and if someone is interested in the data on your field sales team's smartphones, a targeted attack is a genuine risk. Our advice is to take precautions using mobile virus protection. Kaspersky Endpoint Security 8 for Smartphone protects mobile devices in real time and performs scheduled malware checks of entire devices. This can prevent data thieves gaining a head start, thus nipping major threats in the bud. In addition to a mobile protection solution, an anti-spam module is also important. Its functionality should not be limited to emails – instead, it should also filter unsolicited texts and calls.

3.6 Additional Security Measures

While access blocks and encryption will help to conceal information, sophisticated protection software also has other useful tricks up its sleeve, including privacy protection features. Kaspersky Endpoint Security 8 for Smartphone, for example, enables users to hide individual contacts, call lists and texts.

3.7 Simple smartphone security

Smartphones can do a great many things, and the threats affecting them are diverse. Luckily, protecting these mobile all-rounders is very easy to do. When choosing appropriate protective software for smartphones, companies should take into account the following points.

3.8 Management Functions

Configuring one smartphone manually is easy. Configuring five or more can be a nuisance, and configuring more than ten is uneconomical without a centralized management interface which allows access to mobile devices for maintenance purposes. This is precisely what Kaspersky Endpoint Security 8 for Smartphone provides. As administration can also be performed remotely, the IT team retains total control of the devices at all times. This enables updates and new programs to be installed easily and in a targeted manner. When choosing a mobile security suite, you should also bear in mind that, as well as being managed through

the Kaspersky Administration Kit, Kaspersky Endpoint Security can also be integrated seamlessly into existing management environments for mobile devices –such as Microsoft's mobile device manager, for example, or Sybase Afaria.

3.9 Protection for All Platforms

Don't compromise when it comes to smartphone security. The protective software you choose must support all the mobile platforms your company currently uses. Kaspersky Endpoint Security 8 for Smartphone currently supports Black-Berry, Windows Mobile, Android and Symbian devices

Highlights

- Ensure Robust Data Protection
- Get Multi-Platform Support
- Deploy With Ease
- Manage Effectively

System Requirements

Supported Management Platforms:

- Kaspersky Administration Kit 8.0 (version 8.0.2121 or higher)
- Microsoft System Center Mobile Device Manager 2008 SP1
- Sybase Afaria 6.5

Supported Operating Systems:

- Symbian S60 9.1-9.4 (only Nokia)
- Windows Mobile 5.0-6.5
- BlackBerry 4.5-5.0
- Android 1.5-2.3

References

1. http://research.microsoft.com/apps/pubs/default.aspx?id=133031

2. http://www.enisa.europa.eu/act/it/privacy-and-trust/eid/mobile-eid

3. http://www.geek.com/articles/mobile/99-of-android-devices-vulnerable-to-authentication-attack-20110517/

4. http://www.linkedin.com/answers/technology/information-technology/information-security/TCH_ITS_ISC/117191-15928281

5. http://csrc.nist.gov/groups/SNS/mobile_security/mobile_forensics.html

6. http://www.confidenttechnologies.com/news_events/new-mobile-authentication-technology-protects-online-businesses-and-their-customers-frau