Mobile Security Strategies
Juniper Research Special Report
for
Computer Weekly

... information you can do business with
Mobile Security ~ Safe and Secure Devices

1. Introduction

This special report for readers of Computer Weekly is based on Juniper Research’s recent report:


Smartphones currently possess many of the powerful capabilities similar to a PC and as new features and functionalities are being added, smartphones are becoming more vulnerable to certain kinds of attack. As smartphones are increasingly used for accessing remote data and carrying sensitive business and personal data, security apps are becoming an essential and integral part of the smartphone to make it less vulnerable to the different types of threats. Similarly, as both consumer and enterprise adoption of tablets has risen – following the success of Apple’s iPad – there is a pressing need to provide security solutions for these devices.

We have summarised the factors that contribute towards the need for security as shown below.

**Figure 1: Need for Mobile Security**

Source: Juniper Research
The proliferation of downloadable free and paid apps that can be easily installed on mobile devices along with their high volume of data usage opens up the device towards possible threats and risks. Also, the increasing adoption of mobile commerce (mainly banking, payments and ticketing) by users means that distinct security measures are required for the different types of threats and risks they face.

Consumers are adapting to new environments and are familiarising themselves with their new habitats. While for laptops or netbooks using the more traditional data connections (cable broadband or Wi-Fi), the presence of security suites has been a common practice for quite some time, the situation is markedly different for smartphones or tablets where the concern for a secure and safe environment has been highlighted to a greater extent in recent times.

On the corporate side, mobile network usage by enterprise devices has historically raised concerns amongst system administrators since this has implications for corporate network infrastructure, network integrity and data security. When it comes to mobile data connections, questions are being raised regarding unauthorised system or resource access, leading to difficulties when dealing with devices using mobile broadband, data breaches and identity or corporate confidential data theft.

While the mobile environment has been largely successful thus far in eluding the wide spread threats and attacks faced by the PC world, it is becoming both more appealing to cyber criminals and is inherently vulnerable to other security issues. A combination of safe practice and modern software to counter these threats is becoming more important by the day.

2. Security Issues & Trends

This section examines some of the primary security issues surrounding mobile devices. Smartphone and tablet users use their devices for emailing, instant messaging, mobile banking, payments and social networking. Sending and receiving confidential corporate emails, accessing payments and checking bank accounts and storing confidential personal and business details on devices—all requires a secure environment. While the number of mobile threats identified today is relatively small, it is on the increase.

Mobile security has become very important in the wake of accelerating data usage and smartphone adoption:

- The mobile device memory is just as capable of storing sensitive data as other memory storage devices, which means attackers or hackers can access data easily—whether maliciously or accidentally.
- Mobile devices increase the “surface area” for attacks with more access points for hackers to gain entry.
- Applications for mobile devices have given hackers a new avenue for malware. Furthermore, there are multiple platforms (Apple, Android, BlackBerry) and maintaining security across the devices, for each app has to be secure across each platform.

The major security issues that call for mobile security management are discussed below.

2.1 Storage of Confidential Information

Many users store confidential personal and business information on their mobile devices. Personal smartphones owned by users can be configured to access corporate email and data and can be synchronised easily. Also, the introduction of mobile banking, payments and ticketing solutions require secure transmission and storage of sensitive financial data, and social data is often compromised by content sharing third party applications and online gaming.

Mobile devices transport data via wireless networks, which are comparatively less secure than wired networks. This presents users with the risk of leaving confidential information to be intercepted. Most data stored in the mobile devices is unencrypted, so the information stored in these devices is at risk of being misused if intercepted while in transit or when the device is stolen or lost.
### Table 1: Confidential Information Classification Examples

<table>
<thead>
<tr>
<th>Business</th>
<th>Personal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Details</td>
<td>Personal Contacts</td>
</tr>
<tr>
<td>Business Schedules</td>
<td>Personal Calendar</td>
</tr>
<tr>
<td>Documents/Spread sheets</td>
<td>Entertainment – Music/Videos etc.</td>
</tr>
<tr>
<td>Banking and Payments</td>
<td>Store PINs/Passwords</td>
</tr>
<tr>
<td>Business Emails/Instant messaging</td>
<td>Bank Account Details/Banking</td>
</tr>
<tr>
<td>Corporate/Client Information</td>
<td>Personal Email/Social Networking</td>
</tr>
</tbody>
</table>

Source: Juniper Research

### 2.2 Device Protection

According to the industry body ISACA (Information Systems Audit and Control Association), mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls. This could provide malwares and viruses with access to the enterprise network through the user’s smartphone, which may cause data to be lost or intercepted.

Mobile devices therefore require the same level of protection as is available to other end point devices such as laptops and netbooks and which includes:

- Malware protection
- Firewall
- Antivirus Protection
- Spam protection
- Phishing protection

### 2.3 Mobile Apps & Software Downloads

Mobile applications are of major concern from a security perspective as they introduce a number of threats into the enterprise network. Most users download both free and paid apps from application stores. Uncertified third party applications that are downloaded are sometimes malwares or spyware that can retrieve emails, messages, call history, client list and other corporate data. There are different types of unsecure mobile applications available for download from app stores which are marketed as useful business or personal applications.

The application carrying malwares can either transform the device into a gateway for Trojans and viruses to enter the enterprise network or may cause data leakage or exposure.

In addition, new applications installed on mobile devices can locate the device on a map and track the movements of the device and the user. The most attacked applications include games, social networking, search, news and other apps such as weather and music.

### 2.4 Device Loss or Theft

As a smartphone accumulates more features, it becomes more desirable to thieves both in terms of the value of the device and as a means of accessing identity. Devices such as smartphones and tablets have the
capability to store personal as well as confidential corporate information in a single source. This in turn attracts thieves and fraudsters as it provides them with one-stop access to that information. It then becomes easy to work out who they bank with, where they have recently made transactions, the names of their family and to glean other details from emails or other documents. Our interviews and research confirm that device loss or theft continues to be the biggest threat vector.

As smartphones users increasingly store personal and business data, then the risk of crimes such as identity theft, made possible by phone theft, will be a strong motivator in using mobile security suites. The US Federal Trade Commission recently announced that identity theft was the leading consumer complaint that they had received in 2011. Out of the 1.8 million complaints filed in 2011, 279,000 (15%) were reported as identity theft complaints.

It is worth noting that user irresponsibility has a role to play in increasing the risk and this is why device loss or theft will have an impact on enterprise security policies. Inadequate policies to guard against device loss could lead to:

- Data breach leading in turn to identity theft
- Fraudulent calls and billing
- Enterprise data for sale leading in turn to financial losses

According to the latest Junos Pulse mobile security statistics¹, in 2011, almost 17% of security suite users used the ‘locate’ command to find a missing device and over 6% requested to remotely lock those devices to guard against inappropriate use.

### 2.5 Always-On access and User Owned Devices

A majority of enterprise users use smartphones for accessing corporate emails and data and since some of these devices are being bought by the user themselves and not the organisation, the protection of these mobile devices become even more important. Additionally, most mobile devices are always connected to the Internet either via cellular networks or through WiFi networks. This means not only that the device is exposed to the Internet but that other devices can also connect to it.

### 2.6 BYOD Trend

BYOD (Bring Your Own Device) is an emerging and inevitable trend today, but from the security perspective, it is considered as an insecure policy which could damage a company’s reputation and business. If every employee has his/her own device Android or iOS device, it becomes increasingly difficult to manage different devices and to implement common security solutions and policies, because devices, applications, platforms and users are different.

Even though security vendors describe it as a ‘security nightmare’ for businesses, they noted that it is possible to deal with the associated security implications and that it is much safer ‘by default’ when a company provides unified devices for all employees to access corporate accounts.

Juniper Research believes that there is a need to consider consumer owned devices used to access corporate data or email as well as devices that are connecting to the corporate wireless network while considering the BYOD trend. However, in both cases the level of compromise depends on the malware in question.

---

¹ Source: Juniper Networks; Mobile Threat Report, 2012
3. Threats

The following table provides an outline of the key information and security threats to mobile device users.

Table 2: Security Threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Loss/Theft</td>
<td>When the smartphone/tablet is lost by the user or stolen, it can provide the attacker with access to unprotected data stored in the device.</td>
</tr>
<tr>
<td>Phishing</td>
<td>The practice of sending emails or text messages at random to users with the aim of fooling them into disclosing sensitive information to bogus applications or websites operated by fraudsters.</td>
</tr>
<tr>
<td>Malware and Viruses</td>
<td>Malware or malicious software is specifically designed to infect devices without the user’s knowledge, thereby leaking sensitive information and providing full remote access of the device to the attacker.</td>
</tr>
<tr>
<td>Spyware</td>
<td>A general name for the type of malware that can be installed on devices which monitors all the user activities on the device.</td>
</tr>
<tr>
<td>Worms</td>
<td>Malicious programmes that replicate themselves continuously over the device, its memory card and spread themselves via email, messages and through the Internet.</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Network spoofing involves an attacker setting up a rogue network access point using WiFi or GSM: it invites users to connect to the network enabling the attacker to intercept and leak sensitive information.</td>
</tr>
<tr>
<td>Spam</td>
<td>The use of messaging media such as texts, instant messaging, and emails to send unsolicited bulk messages to random users.</td>
</tr>
<tr>
<td>Denial of Service Attack</td>
<td>A DoS (Denial of Service) attack is an attack on a device or mobile network that causes a loss of services to users, typically the loss of network connectivity and services by consuming bandwidth of the victim network or overloading the computational resources of the victim system.</td>
</tr>
</tbody>
</table>

Source: Juniper Research

Note: The list is not exhaustive.

4. Mobile Security Stakeholders & Opportunities

Although most mobile security threats can be seen as malevolent and illegal (with some exceptions in the case of malware and viruses), the effect that a given threat has differs, depending on what stake different groups have in the mobile ecosystem.

4.1 The Individual Subscriber

In terms of numbers, by far the largest group of stakeholders in the mobile security landscape is the individual end user or subscriber. They have the right to assume the mobile device is safe, and that activities such as searching the mobile internet will not result in harm to their phone or to their finances. Increasingly, and by virtue of fundamental changes to the mobile industry, users’ activity is becoming more sophisticated.

This is bringing about the need for security products which are not necessarily related to the protection of the device from malware, such as the ability to encrypt information held on the handset and SIM card as
Mobile Security: Special Report for Computer Weekly

well as the ability to back up important data remotely if necessary and even remotely wipe a handset if it is known to be lost or stolen.

This in turn has also led to the development of sophisticated security management products both from OS vendors such as Apple, RIM and applications security vendors.

Interestingly, while individual user activity is becoming more sophisticated, user attitudes towards protection seems to have so far remained largely unchanged since the days of less sophisticated phones. End users are making few attempts to mitigate the increasing risk to their mobile security or that of the organisation to which they are affiliated. As evident from employee and consumer surveys, security has been often raised as a concern by end users, but only few have adopted some kind of security solutions to negate the same.

4.2 The Corporate Subscriber

An equally important “end user” that has a vested interest in keeping the mobile device safe is the corporate business. Increasingly the mobile device is becoming a “window” onto the corporate network. Organisations are therefore beginning to buy protection to avoid their information and intranet security being compromised.

By using security packages, organisation-wide policies can be set governing how data is encrypted and what access to the corporate network is permitted for different device sets.

Coupled with this, the industry has developed a “remote wipe” facility as a last resort which means that all the data on a corporate device can be cleared if necessary. In some cases the data can be backed up to avoid it being lost altogether.

For the corporate end-user, over the air (OTA) security policy management has become an important part of the security suite offered by both operators and security applications providers. This allows corporate IT managers to assert organisation-wide security policies such as banning access to certain websites or the application of antivirus software.

4.3 Mobile Network Operators

Arguably the most important stakeholder is the mobile network operator. The operator relies heavily on the security of the phone network and its identification mechanisms that allow them to bill a given customer for calls. Key to the success of an operator is the ability to have confidence in its SIM data and billing software. Perhaps equally important, is its reputation among end users. This means that it is in its interests to avoid security breaches that may affect those end users. Even allowing spam to get through to the end user can have an adverse effect on the business as high spam levels are likely to lead to high levels of churn.

End-users place the responsibility for mobile security squarely on the shoulders of the operator with whom they have a relationship. Ultimately since mobile operators own the customer relationship, Juniper believes that in the future they are also likely to be in the front line of providing security services, often via a third party applications security vendor from which they purchase a white label security suite.
5. Market Drivers

Mobile security is rapidly becoming as essential on a handheld as it is on a desktop or notebook computer. The increasing popularity of smartphones makes this particularly relevant, as many users are now becoming accustomed to accessing e-mails and websites and performing online transactions on the move, thereby storing more and more potentially sensitive data on a phone.

**Figure 2: Mobile Security Market Drivers**

The market drivers for mobile security have been explained in detail below.

5.1 Adoption of Open Operating Systems is Increasing

Open operating systems such as Android allow developers to take source code and develop applications from it which essentially represents a lessening of the control that operators have over their own infrastructure. Even though allowing third party application developers’ access to its source code has its own benefits, it makes the OS vulnerable to malicious applications created by third party developers.

This means that mobile devices running on open operating systems can be easily targeted by criminals or malware developers.

5.2 Increased Smartphone Penetration

The considerable numbers of consumers still using non-smartphones, combined with the fact that the combination of smart mobile devices equipped with intuitive touchscreen interfaces, allied to the onset of readily accessible consumer oriented apps means that the installed base for smartphones will continue to grow and reach almost 2 billion by 2016.

Growth in developed markets will continue as ever more consumers upgrade from outdated featurephones to higher performance smartphones with greater functionality. While smartphones now account for the majority of mobile devices in the US, there remains significant scope for growth both here and in other markets with production costs expected to fall further for vital components such as
processors and touchscreens. Furthermore, a lowering of the minimum price of smartphones will increase their affordability in emerging markets with 3G networks, such as China and India.

In addition to offering greater potential for browsing, most smartphones come equipped with attractive cameras, with the result that end users often store hundreds, if not thousands, of images, allied to other features including email access, calendar and document storage.

### 5.3 The Rise in mCommerce

Over the past 12 to 18 months there has been significant activity and growth in mobile payments (particularly digital and physical goods purchases), and mobile banking. In addition these services and applications, along with contactless NFC (Near Field Communication), mobile money transfer, ticketing and coupons are forecast to grow rapidly over the next five years. However, security concerns are one of the reasons why mobile commerce has not expanded as fast as expected.

This rapid development in mCommerce means that storing more potentially sensitive data on a phone makes it more likely to attract a cyber-criminal’s attention as a target for hacking or breaching into. Hackers are able to access sensitive information stored in the device such as account details or PIN codes used for mobile banking, transaction codes and credit card details.

### 5.4 Increased Data Usage and Availability of Apps

Mass adoption of smartphones that offer ubiquitous internet access allied to a host of other Internet capable devices, including tablets, has driven a dramatic growth in data usage over the past four years. This in turn has been accelerated by the availability of large (in some cases unlimited) data bundles allied both to the increasing availability of HSPA+ and LTE connectivity and of free WiFi coverage.

End-users are receiving seamless access to their personalised set of services irrespective of their location and through both mobile and fixed networks. Also, the increasing pervasiveness of broadband and high speed connections at home and at work provides users with the ability to access data and information any time and from anywhere.

Applications and services available now and in the future from the numerous application stores in the market are going to be key drivers of mobile security as they provide the potential for malware and viruses to be spread via downloaded – fake and infected – malicious apps.

The increased penetration of smartphones has spiked the total data traffic on cellular networks globally. According to our recent Mobile Data Offload & Onload\(^2\) report, the average smartphone user generates over 8 times the amount of traffic produced by the average featurephone user. Other high bandwidth requiring data application and services available to the consumers also contribute towards higher multiples of traffic.

### 5.5 Increase in Device Sophistication

Greater device sophistication accelerates the need for mobile device security in several ways. First, with larger volumes of mobile payments there may be an increased incentive and motive to attack the mobile device for financial gain. Secondly, increased processing power means that mobile devices will be able to “support” attacks, from a memory and processing power perspective, which previously they would not have been able to do. Perhaps most important, however, is that more sophisticated devices, led by the iPhone, are finally opening the broader Internet to the handset, at a time when viruses and other malware are increasingly delivered over the Internet.

\(^2\) Source: Mobile Data Offload & Onload: WiFi & Small Cell Strategies 2012-2016
6. The BYOD Trend

6.1 What is BYOD?

BYOD or bring your own device refers to the practice of consumers getting accustomed to bringing their own mobile computing devices such as smartphones and tablets into the enterprise and accessing corporate assets. Such assets range from company documents to financial data, from calendar and contact details to company emails.

Traditionally, enterprise smartphones were classified as devices with access to enterprise IT systems and Intranets. Historically, if organisations used devices with the same mobile operating system they were able to rely on in-built operating system security. However, with the increasing BYOD trend, organisations now have a need to re-assess their mobile device as well as security strategies. The increasing popularity of smartphones and tablets makes this particularly pertinent as many users are now accustomed to accessing e-mails, websites and performing online transactions on the move, thereby storing more and more potentially sensitive data. The fact that most services themselves are now cloud-based and thus accessible via multiple devices is another factor contributing towards this growing trend.

Thus, enterprise mobile IT policies will become increasingly complex as multiple device types need to be managed and employees now have a wider array of handsets. These devices need to be detected as they attempt to access the corporate network. Several factors feed into this growing trend of BYOD – the development of the corporate mobile device market and increased penetration (and usage) of mobile devices within the enterprise; wide network connectivity and always-on devices providing access to files and emails anywhere and everywhere; the availability of a greater variety of mobile apps and solutions designed for the enterprise.

Companies are looking into quickly and smoothly incorporating mobile network connected devices into the corporate network since that is the easiest way to enforce policies and to audit such devices. Juniper Research recommends that Enterprise and IT managers audit the security status of their corporate mobile device deployments and take remedial action where necessary.

While this trend will redefine enterprise connectivity, by anticipating such changes, working towards efficiently integrating devices connected to enterprise networks and by dealing with network security concerns and issues, organisations can prevent unpleasant situations generated by security breaches in the corporate network environment.

6.2 Security Implications

The BYOD trend is something that CIOs and IT directors or managers cannot ignore as there is an increasing number of employees bringing their own devices to the enterprise – whether such activity is officially endorsed or not. There are a number of issues and implications that need to be addressed and measures have to be taken via new device management policies and security measures. Enterprises need to be aware of the different activities on their employees’ mobile devices (including emails, files and documents stored and installed apps) and so we expect the mobile device management platform to be the umbrella, under which important security and management functions will fall, including policy management, secure access based on strong authentication, data protection and device protection.

In summary, the security implications arise from the following factors:

- The lack of a unified perspective on mobile platform risks
- A standard unified set of rules - Do’s and Don’ts
- A generic view on their practical uses
- OS and device manufacturers trying to get the biggest market share by incorporating more features on smartphones leading to more potential security holes
• Vendors trying to get greater numbers of computer users to migrate to mobile devices by porting computer facilities on smartphones and tablets

Consequently, there is a need to consider mobile devices as just another endpoint. They should be integrated with existing management platforms and there is a need to educate or inform enterprises of what solutions they should adopt. Apart from the benefits of BYOD, enterprises have to face a number of challenges from updating traditional device management to adopting new security measures.

It is thus imperative that if an enterprise allows an employee to use his or her device to access corporate networks, that enterprise must ensure that (a) it has IT policies in place to cover such usage and (b) that the employee understands and has signed up to those IT policies.

A number of vendors have been developing packages deliberately designed to cope with the use of consumer devices within the enterprise space. In summary, there is a need to:

• maintain a secure access to the enterprise network from the consumer owned device
• identify new consumer owned devices connected to the enterprise network and to monitor them
• enforce company policies and to protect confidential company data
• ensure productivity and improve efficiency

Knowing who is accessing your network and ensuring that only authorised users can access information in a secure manner are the two most important steps that need to be managed by the enterprise. Most of the respondents confirmed that along with mobile device management, malware and data protection is necessary to secure corporate data and to protect against malicious applications and websites.

**Figure 3: BYOD Management Needs**

BYOD is actually blurring the line separating business devices from consumer devices - this consumerisation of business devices reflects the change in consumer attitude towards bringing in their own devices to the work place.

The following forecast on BYOD devices including smartphones and tablets, provides context to the current use of employee owned devices in the work place. Juniper anticipates that the global number of consumer smartphone and tablets brought into the enterprise will more than double by 2014, reaching 350 million by 2014, compared to almost 150 million this year. This represents almost 23% of the total installed base of consumer owned tablets and smartphones.
Figure 4: Number of Consumer Owned Smartphones & Tablets in the Enterprise (m) 
Split by Region, 2014: 350 million

Source: Juniper Research

7. Mobile Security Software Market

The threats to mobile phone users from theft, phishing, viruses, malware, spam and unauthorised access are emerging at an unprecedented pace; a rate that is emerging to be faster than that previously seen with the PC industry. Juniper Research has found that only 5% of global smartphones and tablet devices have security software installed, despite a steadily increasing threat from malware, fraud and device theft.

Juniper Research forecasts that both corporate and personal users will begin to recognise the need to protect their data and the demand for mobile security products will increase over the next five years to a point where 1 in 5 mobile devices will be protected by third party security software.

We anticipate that a number of high-profile security alerts for mobile phone users will publicise the risks of using a mobile phone for data-centric applications and services and result in the revenue growth. Initially driven by the data hungry mobile business or enterprise user who has seen the benefits of data services such as email, we will see mobile security products become mainstream by late 2013 crossing the $1 billion annual revenue barrier.

Just as consumers are currently purchasing and installing internet security products, e.g. Symantec’s Norton Security suite, on their PCs and laptops, mobile device users will also add their mobile devices to the list of electronic devices they must secure. The number of protected consumer devices will overtake protected enterprise devices by 2015, driven by BYOD trends.
Order the Full Report


- BYOD Trend Analysis & Forecast
- Mobile Device Authentication
- Enterprise vs. Consumer Analysis

This exciting 2nd edition study provides the most detailed view of the opportunities for connected device security to date.

Juniper’s unique forecast suite for the mobile security landscape includes:

- Number of protected vs. non-protected devices
- Mobile security product sales revenue
- Consumer and Enterprise owned mobile devices
- ‘Bring Your Own Device’ Forecasts
- Mobile Handsets used for Commerce Authentication Mechanisms

Key Questions Answered:

1. How many mobile devices will have security products installed in them by 2017?
2. How is the mobile security market developing among enterprise users and consumers?
3. What will drive the demand for third party security applications among enterprise and consumers?
4. What is driving the BYOD trend and what are its security implications?
5. What is the adoption of mobile devices in mCommerce authentication?

Juniper Research Limited

Juniper Research specialises in providing high quality analytical research reports and consultancy services to the telecoms industry. We have particular expertise in the mobile, wireless, broadband and IP-convergence sectors. Juniper is independent, unbiased, and able to draw from experienced senior managers with proven track records.

Publication Details

Publication date: August 2012

Author: Nitin Bhas

For more information, please contact: Michele Ince, General Manager michele.ince@juniperresearch.com

Juniper Research Ltd, Church Cottage House, Church Square, Basingstoke, Hampshire RG21 7QW UK

Tel: +44 (0)1256 830001/475656

Fax: +44(0)1256 830093

Further executive briefings and whitepapers can be downloaded at www.juniperresearch.com