

MOBILE TECHNOLOGIES SECURITY

July 2011

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Mobile Technology for Management	3
Introduction.....	3
Business Trends & The Impact on Business	3
Government Policy, and IT Governance	5
II. Mobile Technology for I.T. Practitioners	7
Types of Wireless Connectivity.....	7
Deployment Strategies	10
Security Considerations and Measures for Enterprises	11
III. Mobile Technology For End-Users	13

SUMMARY

As technologies advance, mobile phones, tablets and portable notebook computers are becoming commonplace. The computational power of these devices continues to increase, while at the same time they become ever smaller and lighter. A new spectrum of mobile products is emerging that combine a range of computational capabilities into one physical device. These mobile convergence capabilities enable people to remain online, accessing all their data, such as email and stock quotes, while on the move.

While there are many obvious advantages with these devices, they also affect traditional business processes, and there are security issues that need to be considered. Organisations need to be concerned about security, including theft or loss of mobile devices used by employees, corporate data leakage via these devices, possible virus infection, and possible unauthorised traffic interception. While enjoying the convenience and efficiencies brought about by new mobile technologies, appropriate security measures should be designed and implemented in order to counter any threats to sensitive data introduced by the use of mobile devices.

In this paper, we provide a brief overview of the most common mobile technologies, and outline the weaknesses around the use of these technologies. We also provide a set of general tips to end-users in maintaining personal security on mobile devices.

I. MOBILE TECHNOLOGY FOR MANAGEMENT

INTRODUCTION

Traditionally, desktop computers and telephones were considered to be two separate categories of device. As technology has advanced, the primary functions of such devices have become blurred. The merging of computation and communication technologies, or mobile convergence, has created a new spectrum of handheld devices that are a combination of a hand-held computer and mobile phone. Mobile computing devices (or mobile devices) are information systems capable of storing and processing large amounts of information without having a fixed physical location, and they can be carried around easily. Examples of mobile computing devices include mobile phones, smartphones, Personal Digital Assistants (PDAs), tablets and notebook computers.

Mobile technologies can change one's daily life; it is now possible to read and reply to emails by mobile phone, while Internet browsing by 3G and Wi-Fi enabled devices.

BUSINESS TRENDS & THE IMPACT ON BUSINESS

According to statistics from the Office of the Telecommunications Authority (OFTA), mobile subscriber penetration rate in Hong Kong had reached 194.3%, by March 2011. There are now more than 13.7 million mobile subscribers, and more than 6.8 million

2.5G and 3G mobile subscribers in the territory¹. In addition, OFTA statistics show that there are now more than 9000 public Wi-Fi access points (May 2011), facilitating access to free Wi-Fi services in certain areas of Hong Kong. Undoubtedly, these high figures indicate that Hong Kong is now a major wireless metropolitan city.

Enabling mobile device access to public and/or enterprise applications provides convenience to users. Advantages include improved efficiency, and increased capability to access information anytime or anywhere. However, these advantages do not come without shortcomings. New challenges are posed on both the server and client side. In this paper, we focus on the client side, that is, mobile devices themselves. Some of the security weaknesses with mobile devices include:

1. Theft or loss of the device. Confidential email messages or sensitive and personal data could fall into the wrong hands if such data was stored on the device.
2. Disgruntled employees or unauthorised personnel can take advantage of the small size and powerful capabilities of mobile devices (such as storage space and camera functions) to steal sensitive data while inside an organisation.
3. Viruses can also be spread across mobile devices. Mobile applications are susceptible to vulnerabilities and bugs just like any desktop software package.
4. The GSM/GPRS communication protocol does not have strong signal protection and it is relatively easy to intercept traffic on such networks.

Although the advantages of mobility and networking provided by mobile devices can increase productivity and improve communication turnaround time, those deploying mobile technologies within the organisation or enterprise need to seriously consider the

¹ http://www.ofa.gov.hk/en/datastat/key_stat.html

security implications. Appropriate security policies regarding the use of mobile devices should be defined.

GOVERNMENT POLICY, AND IT GOVERNANCE

The Hong Kong Government's *Digital 21* blueprint, along with the implementation of the "GovWiFi" programme, means that the use of mobile devices in business will inevitably increase. While mobile technologies make it easier to reach the individual, either by email, short message or voice call, there is also an increase of unsolicited messages being sent to mobile devices. The Hong Kong Government has been working with the industry to tackle the problem of unsolicited electronic messages since 2005. The "Unsolicited Electronic Messages Ordinance" (or UEMO), enacted in May 2007, aims to regulate the sending of commercial electronic messages (CEMs). The regulations cover electronic marketing messages promoting products or services sent as text and pre-recorded voice messages to telephones, fax machines or email addresses².

At the same time, mobile devices also bring with them other security challenges and risks. As an example, mobile devices often have a network connection capability, and they can be used to connect to an enterprise network. This could lead to a potential breach of security via the device if not properly checked and managed. This is why, when any enterprise is moving to adopt mobile technologies in business, a clear security policy on the usage of mobile phones/tablets/PDAs/notebook computers should be defined to handle, at a minimum, the following issues:

1. Physical handling of the device; guarding against loss or theft;

² <http://www.ofta.gov.hk/en/uem/main.html>

2. Mobile operating system issues; precautions against viruses or malicious codes should be implemented;
3. Sensitive data stored on mobile devices; a clear management policy that balances the risks of data leakage with convenience;
4. Other technical measures; security procedures and measures to protect mobile business applications and data.

II. MOBILE TECHNOLOGY FOR I.T. PRACTITIONERS

In this section, we briefly describe the key mobile technologies and protocols, including 1G, 2G, 2.5G, 3G and 4G, wireless LANs and wireless personal area networks.

TYPES OF WIRELESS CONNECTIVITY

Wireless Wide Area Network

The first generation (1G) mobile communication technology was introduced in the late 1970s. 1G was primarily an analogue system, and it was only used for voice transfer. In the late 1980s and early 1990s, second generation (2G) systems appeared³. Voice signals were then transmitted in digital form, offering better quality and lower cost. The well-known Global System for Mobile (GSM)⁴ communication protocol is classed as a 2G telephony system, and is based on a technology called Time Division Multiple Access (TDMA)⁵.

To extend the voice service to include the sending and receiving of data, GSM operators began providing General Packet Radio Services (GPRS)⁶, which is often referred to as

³ <http://www.itu.int/osg/spu/ni/3g/technology/index.html>

⁴ <http://www.etsi.org/WebSite/Technologies/gsm.aspx>

⁵ <http://www.privateline.com/Cellbasics/hart-ch3IS-136.pdf>

⁶ <http://www.etsi.org/WebSite/Technologies/gprs.aspx>

2.5G⁷; and Enhanced Data rates for GSM Evolution (EDGE)⁸, which is usually called 2.75G⁹. EDGE can provide a data rates up to 384 Kbps.

To further extend mobile technology to include multimedia communications (video, image, text, graphics and data), the International Telecommunication Union (ITU) developed standards for third generation (3G)¹⁰ mobile communication protocols¹¹. Data rates can now be up to 384kbit/s for subscribers on the move, and 2Mbps if they are in a stationery environment. The 3rd Generation Partnership Project (3GPP)¹² was formally established in December 1998, with the aim of producing globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support.

As data rates continue to increase, a new technology called High-Speed Downlink Packet Access (HSDPA)¹³, also called 3.5G¹⁴ has appeared. This can support a data rate up to a limit of 14.4 Mbps.

A fourth generation (4G)¹⁵ communication protocol is planned that will support high-quality multimedia services. Data rates up to 100 Mbps in mobile situations and 1 Gbps in stationary conditions are the target of this standard.

⁷ <http://en.wikipedia.org/wiki/2.5G>

⁸ <http://www.etsi.org/WebSite/Technologies/edge.aspx>

⁹ <http://www.mobileburn.com/term.jsp?term=2.75G>

¹⁰ <http://en.wikipedia.org/wiki/3G>

¹¹ <http://www.itu.int/newsarchive/press/PP98/Documents/Backgrounder2IMT2000.html>

¹² <http://www.3gpp.org/About/about.htm>

¹³ http://en.wikipedia.org/wiki/High-Speed_Downlink_Packet_Access

¹⁴ <http://en.wikipedia.org/wiki/3.5G>

Wireless Metropolitan Area Networks and Wireless Local Area Networks

While cellphone systems are improving in terms of data rate capabilities, other competing technologies such as Wi-Fi (or wireless LAN or WLAN) and WiMAX (Worldwide Interoperability for Microwave Access) are moving towards the same target of providing large bandwidth for integrated multimedia services. Wi-Fi is a wireless technology based on the IEEE 802.11 standard. Although Wi-Fi is limited somewhat in its range, it can support data rates up to 54Mbps, much faster than that offered by HSDPA at only 14.4 Mbps.

WiMAX, also called wireless Metropolitan Area Network (or wireless MAN), is a trademark of the WiMAX Forum, an industry-led, not-for-profit organisation formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonised IEEE 802.16 standard¹⁶. WiMAX can support much longer ranges than WLAN (Wi-Fi), and aims to provide a wireless alternative to wired broadband services like cable and DSL¹⁷. For stationary applications, WiMAX can deliver a capacity of up to 40 Mbps, while for mobile users WiMAX aims to offer up to 15 Mbps data rates within a typical cell radius of three kilometres.

For access control on WiMAX networks, digital certificates or pre-shared key authentication mechanisms are available. Strong encryption AES algorithms are also supported, and the design of the key management protocol has built in protection against

¹⁵ <http://en.wikipedia.org/wiki/4G>

¹⁶ <http://www.wimaxforum.org/about/>

¹⁷ <http://www.wimaxforum.org/technology/>

replay attacks. However, as WiMAX deployment is not yet on a large enough scale, its ability to withstand attacks is still subject to evaluation.

Wireless Personal Area Networks

In addition to the protocols above, mobile devices can also support Wireless Personal Area Networks (WPAN) such as Bluetooth and Infrared, which can connect and control various products and devices within a short distance (in the order of magnitude of metres, e.g. 1 metre or less).

Bluetooth is an open specification that is governed by the Bluetooth Special Interest Group (SIG). It provides a low bandwidth wireless connection supporting a range of about 10 meters, for both data (asynchronous) and voice (synchronous) communications with a total bandwidth of 1 Mb/sec¹⁸.

An Infrared link is a short-range wireless signal that acts like a cable so that a communication network can be established. Files and data can be passed bi-directionally, usually within a range of around 1 metre. However, if the line-of-sight infrared link is blocked, the connection is disconnected.

DEPLOYMENT STRATEGIES

Mobile devices are being used by enterprises in several areas, including mobile messaging and mobile web applications, etc. The most obvious use is access to email

¹⁸ <http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html>

while on the move. In addition, some commercial web applications have been developed to better serve customers using mobile technology.

When an enterprise decides to use mobile technologies in business, a clear security policy should be established to avoid possible internal network intrusion, virus infection and data loss due to the activities of mobile users.

SECURITY CONSIDERATIONS AND MEASURES FOR ENTERPRISES

The following security weaknesses are possible when enterprises deploy mobile technologies:

1. Theft or loss of small mobiles devices
2. Data leakage via mobile devices by disgruntled or unauthorised staff
3. Spread of viruses or other patch management issues
4. Possible snooping and interception on GSM communications

Before allowing staff to use hand-held devices to conduct business, the possibility of the device being lost or stolen should be considered. To defend against data leakage in this case, one possible solution is to enable a password-protection feature on each mobile device so that the device must be authenticated before it can be used. With this approach, a clear password management policy should be observed. Another possible solution is to use the remote data destruction function available on some devices. When the device is lost or stolen, the operator can destroy all the data and content in that device remotely. In addition, a list of authorised mobile computing devices allowed for business purposes should be maintained so that periodic inventory checks can be performed. If it is necessary to store sensitive data in the mobile device, encryption should be used to protect all data.

Data theft by disgruntled or unauthorised employees is always a weakness in an enterprise. When an employee is granted access to sensitive information, it is possible that data may be leaked, either deliberately or due to human error. Preventive measures are a must, including having all employees signed a confidentiality declaration and agreement. In some workplaces, such as call centres where staff have access to massive amounts of personal information, enterprises may need to institute a policy preventing staff from bringing belongings, including mobile phones, into the work environment.

Viruses are also a shortcoming on some mobile devices. The first proof of concept worm, known as Cabir, was reported to be able to infect phones and devices running the Symbian operating system back in 2004¹⁹. The worm propagated via Bluetooth technology and its solutions appeared later on affected operating systems. Enterprises should therefore consider developing a security policy to protect mobile phones. Install anti-virus software in mobile devices with updated virus definition signatures. Other necessary patch management policies should be implemented and updated regularly.

Although the original aim of GSM was to design a secure communication channel compared to earlier analogue voice transmission, it was found that GSM traffic was not as secure as expected, and interception of GSM traffic is still possible²⁰. This was exposed when a group of researchers in the US uncovered and cracked the secret COMP128 algorithm that is used for authentication and encryption in GSM²¹. Therefore, enterprises should consider one of the later communication protocols (such as 3G, Wi-Fi, etc.) for mobile devices used in business applications.

¹⁹ <http://news.bbc.co.uk/2/hi/technology/3809855.stm>

²⁰ <http://www.gsm-security.net/papers/securityingsm.pdf>

²¹ <http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html>

III. MOBILE TECHNOLOGY FOR END-USERS

From the point of view of end-users, there is a need to comply with at least a basic set of security precautions. For example, the US Defense Department has requested their staff encrypt all data stored on “*easily transportable computing devices*” including laptop PCs and personal digital assistants²².

A stolen or lost mobile device with unprotected storage allows an attacker to access the data on it. If the device is infected with malware, it may lead to hidden use of premium services, or leaking sensitive information. Here are some general tips for maintaining the security of your mobile device.

When configuring your mobile device

- Enable a power-on password or other device password management tool if available.
- Configure the mobile device in such a way that it locks automatically after some inactive time.
- Install mobile security software, such as anti-virus software and firewall on mobile device if available.
- Apply the latest patches and fixes for your mobile operating system and related backup/synchronisation software. Upgrade the software to its latest version where applicable.
- Scrutinise thoroughly all permission requests, for example those involving privileged access, when installing applications/services.
- Use encryption to lock sensitive data stored on the mobile device and removable media, if available.
- Set up a remote data wiping feature if available.

²² http://www.gcn.com/print/26_22/44923-1.html

- Turn off wireless connections such as Wi-Fi, Bluetooth and/or infrared connectivity when not in use.
- Turn off location services setting in your mobile device if it is not necessary to run location-based application.
- Do not jailbreak the mobile device (to override usage and/or access limitations).

When using your mobile device

- Do not leave a mobile device unattended, even for a moment.
- Do not process sensitive data in the mobile device unless with encryption feature on or secure end-to-end connection.
- Do not open or follow links in SMS/MMS or email from misleading URL, suspicious or un-trusted sources.
- Do not download or accept programs and content from unknown or un-trusted sources.
- Be cautious when connecting to publicly available Wi-Fi hotspots, and avoid access sensitive data unless with adequate security protection.

When backup data in your mobile device

- Turn on the encryption option in the backup/synchronisation software for storing the data in encrypted mode if available.
- Make sure the backup copies are encrypted no matter stored in desktop PC or in removable media.

When disposing your mobile device

- Completely clear all data and settings on your mobile device before disposal.

At ALL time

- Keep your mobile devices in a secure place, especially when not in use.
- Stay alert on security vulnerability on mobile devices, and apply the latest patches and fixes when available.
- Do not install illegal or unauthorized software on the mobile device.
- Do not allow wireless connections from unknown or un-trusted sources on your device.

While enjoying the convenience brought about by mobile technologies, appropriate security measures should be implemented, and mobile users should be aware of the risks in order to enjoy the benefits and convenience of Hong Kong as a wireless city.