3 Cybercrime: Mobile and Wireless Devices

Learning Objectives

After reading this chapter, you will be able to:

- Understand the security challenges presented by mobile devices and information systems access in the cybercrime world.
- Understand the challenges faced by the mobile workforce and their implications under the cybercrime era.
- Get an overview on mitigation strategy like the CLEW for possible protection of credit card users.
- Learn about security issues arising due to use of media players.
- Understand the organizational security implications with electronic gadgets and learn what organizational measures need to be implemented for protecting information systems from threats in mobile computing area.
- Understand Smishing and Vishing attacks in the Mobile World.
- Understand the security issues arising due to daily use of removable media such as pen/zip drives in this mobile environment.

3.1 Introduction

In this modern era, the rising importance of *electronic gadgets* (i.e., mobile hand-held devices) – which became an integral part of business, providing connectivity with the Internet outside the office – brings many challenges to secure these devices from being a victim of cybercrime. In the recent years, the use of laptops, personal digital assistants (PDAs), and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment. According to Quocirca Insight Report (2009),[1] by the end of 2008 around 1.5 billion individuals around the world had the Internet access. In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access. The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address. Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones. Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the *Smartphone*.

Smartphones combine the best aspects of mobile and wireless technologies and blend them into a useful business tool. Although IT departments of organizations as yet are not swapping employees' company-provided

PDAs (as the case may be) for the Smartphones, many users may bring these devices from home and use them in the office. Research in Motion's (RIM) Blackberry Wireless Hand-held is an alternate technology. According to Research in Motion Annual Report (2009),[2] there are over 175,000 organizations with BlackBerry Enterprise Server installed behind the corporate firewall (i.e., corporations that use the BlackBerry enterprise server and client/server software for data communication between corporate BlackBerry devices and other mail systems). Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity. Clearly, these technological developments present a new set of security challenges to the global organizations.

3.2 Proliferation of Mobile and Wireless Devices

Today, incredible advances are being made for mobile devices. The trend is for smaller devices and more processing power. A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities. A long list of options is available to the mobile users. A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls. A key driver for the growth of mobile technology is the rapid growth of business solutions into hand-held devices. Figure 3.1 shows some typical hand-held devices.

As the term "mobile device" includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices. Figure 3.2 helps us understand how these terms are related. Let us understand the concept of mobile computing and the various types of devices.

Figure 3.1 | Typical hand-held devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

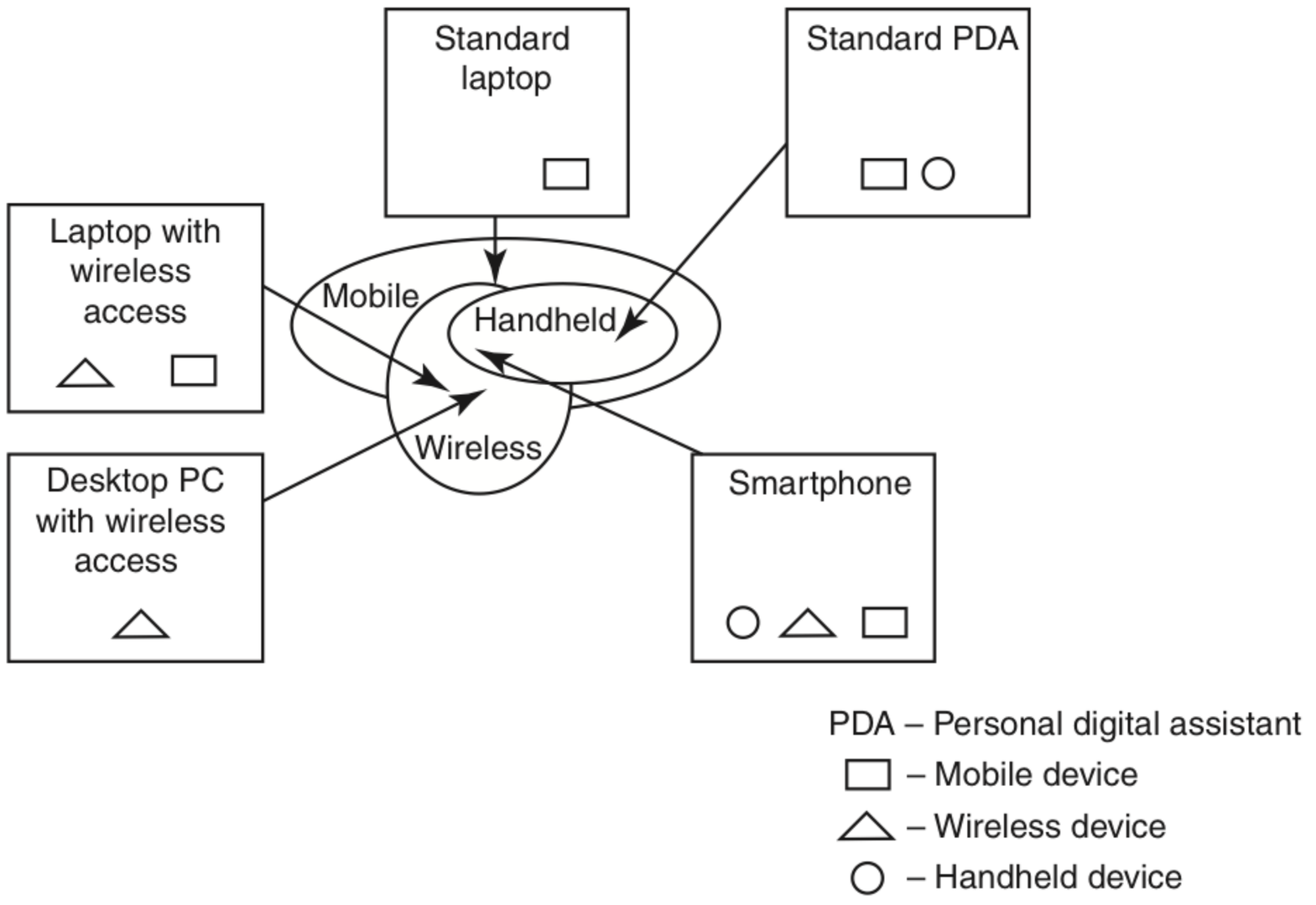


Figure 3.2 | Mobile, wireless and hand-held devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s.[3] They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch-screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. **Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. **Smartphone:** It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, *global positioning system* (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. **Fly Fusion Pentop computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

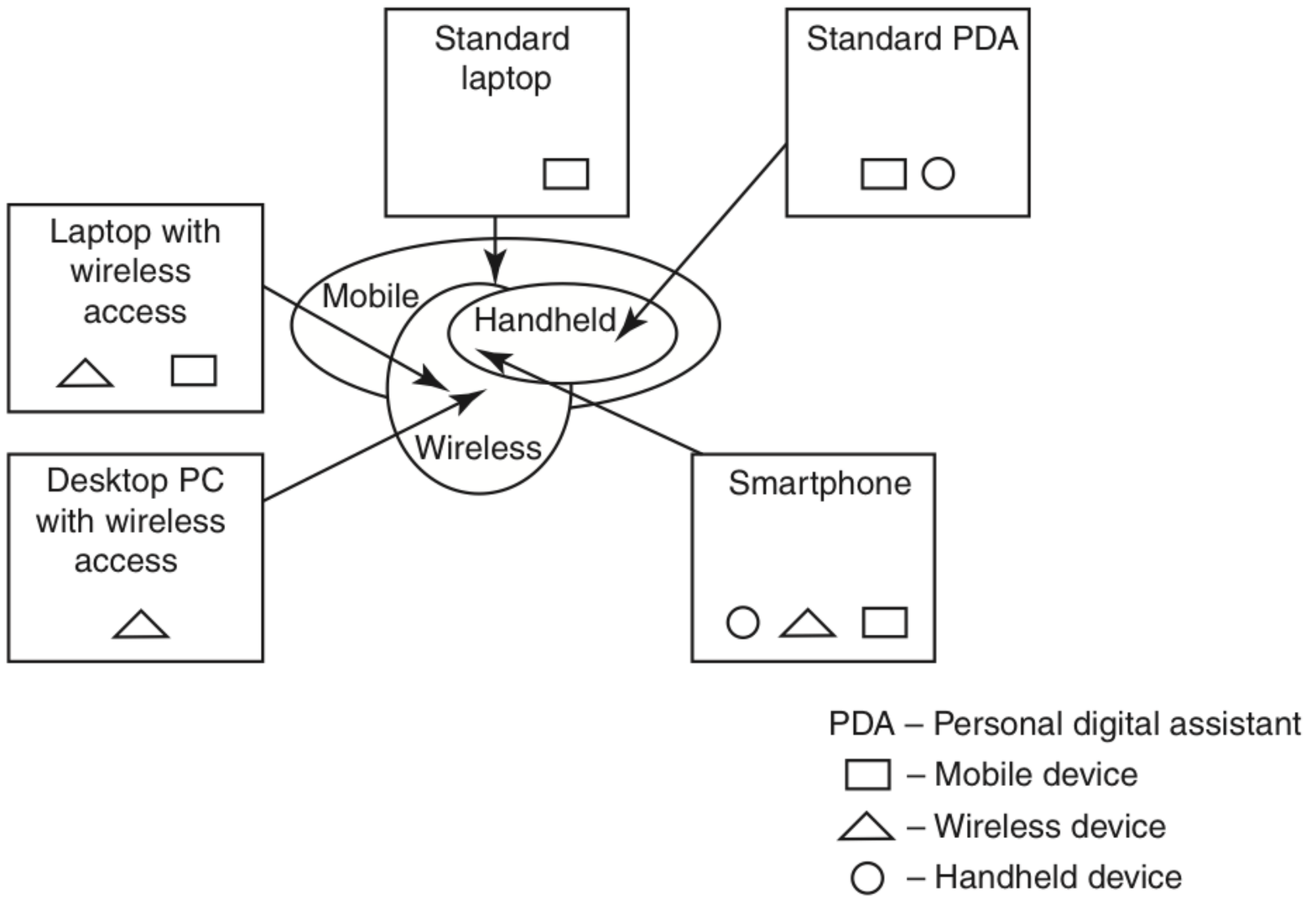


Figure 3.2 | Mobile, wireless and hand-held devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Mobile computing is "taking a computer and all necessary files and software out into the field." Many types of mobile computers have been introduced since 1990s.[3] They are as follows:

1. **Portable computer:** It is a general-purpose computer that can be easily moved from one place to another, but cannot be used while in transit, usually because it requires some "setting-up" and an AC power source.
2. **Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch-screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.
3. **Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.
4. **Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.
5. **Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).
6. **Smartphone:** It is a PDA with an integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.
7. **Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, *global positioning system* (GPS) and DVD player. It also contains word processing software and is Bluetooth compatible.
8. **Fly Fusion Pentop computer:** It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.

Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection. Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time. Mobile simply describes a computing device that is not restricted to a desktop, that is, not tethered. As more personal devices find their way into the enterprise, corporations are realizing cybersecurity threats that come along with the benefits achieved with mobile solutions.

Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all. Thus, while "wireless" is a subset of "mobile," in most cases, an application can be mobile without being wireless. Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smartphones. In this chapter the term "hand-held" is used as an all-embracing term.

3.3 Trends in Mobility

Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking. "iPhone" from Apple and Google-led "Android" phones are the best examples of this trend and there are plenty of other developments that point in this direction. This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.

It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain. Figure 3.3 shows the different types of mobility and their implications.

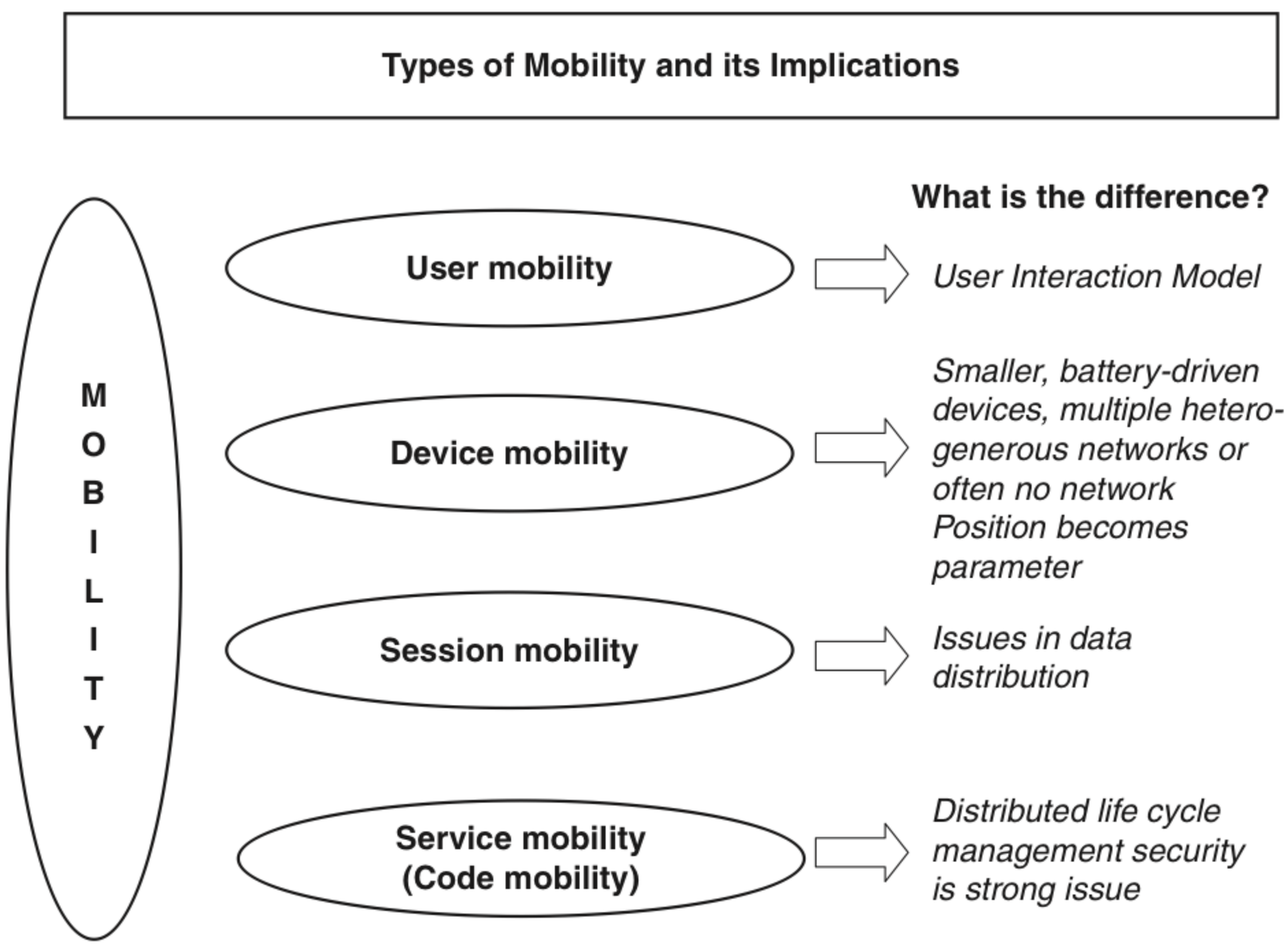


Figure 3.3 | Mobility types and implications.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

To assess major challenges in the mobility domain, let us see the statistics found during the surveys. In one such survey,[4] reported by Quocirca, employees working in government departments have lost or mislaid over 1,000 laptops, lost more than 500 phones or mobile E-Mail gadgets and lost over 700 other mobile devices (i.e., probably memory sticks, cameras, etc.). Another such survey, reported by Quocirca,[5] of the 2,853 respondents, 29% had a broad experience of wireless laptops, 14% had a broad experience of smart hand-helds, with around a further 60% in each case having a more limited or unofficial experience. Findings from surveys like these help us demystify many perceptions about mobile and wireless connectivities. The results of surveys like these indicate that we are grappling with a "perception problem"; most people have not as yet come to terms with the fact that the hand-held devices may look "harmless" but they can cause serious cybersecurity issues to the organizations (see Box 3.1).

The new technology 3G networks are not entirely built with IP data security. Moreover, IP data world when compared to voice-centric security threats is new to mobile operators. There are numerous attacks that can be committed against mobile networks and they can originate from two primary vectors. One is from outside the mobile network – that is, public Internet, private networks and other operator's networks – and the other is within the mobile networks – that is, devices such as data-capable handsets and Smartphones, notebook computers or even desktop computers connected to the 3G network.

Box 3.1 Key Findings for Mobile Computing Security Scenario

1. **With usage experience, awareness of mobile users gets enhanced:** Survey showed that those with broad wireless laptop experience place less emphasis on this aspect for the deployment of smart hand-helds. However, an experience of small hand-held deployment boosted the numbers seeing the need for increased provision of user support and training.
2. **People continue to remain the weakest link for laptop security:** Antivirus software, secured virtual private network (VPN) access and personal firewalls are deployed over two-thirds of IT professionals, but those with a broad wireless experience regard loss, damage or unauthorized use as their major concerns. These depend on the care taken by the users and well-communicated security policies.
3. **Wireless connectivity does little to increase burden of managing laptops:** The cost and complexity of device management is seen as an issue by around half of the IT professionals surveyed. However, the level of challenge perceived to affect security, device management and use support is unaffected by a broader experience of wireless laptop deployment.
4. **Laptop experience changes the view of starting a smart hand-held pilot:** The key concerns for starting a smart hand-held are security and the cost of devices, but these lessen for those with a broad wireless laptop experience. However, the concern over choosing the most appropriate devices rises with experience; users cite further concerns over interoperability and compatibility.
5. **There is naivety and/or neglect in smart hand-held security:** Although plenty of emphasis is placed on security, a large number of IT departments do not enforce security for smart hand-helds as well as for laptops or they leave it in the hands of the users. This is more prevalent in those with limited or unofficial smart hand-held activity, but even those with a broad experience (almost one-third of those surveyed) do not treat smart hand-held security as seriously as laptops.
6. **Rules rather than technology keep smart hand-helds' usage in check:** Businesses with an existing experience of smart hand-helds favored a policy of controlled deployment, with almost two-thirds of those surveyed providing a limited choice of devices, and only one-third of the surveyed population was user of technology solution based on continuous synchronization. However, broad experience increases the use of other automated solutions, such as centralized software management and remote device deactivation.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Popular types of attacks against 3G mobile networks[6] are as follows:

1. **Malwares, viruses and worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:
   - *Skull Trojan:* It targets Series 60 phones equipped with the Symbian mobile OS.
   - *Cabir Worm:* It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
   - *Mosquito Trojan:* It affects the Series 60 Smartphones and is a cracked version of "Mosquitos" mobile phone game.
   - *Brador Trojan:* It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conductive to traditional worm propagation vector such as E-Mail file attachments (refer to Appendix C).
   - *Lasco Worm:* It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir's source code and replicates over Bluetooth connection.
2. **Denial-of-service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable (we will address this attack in detail under Chapter 4). Presently, one of the most common cyber-security threats to wired *Internet service providers* (ISPs) is a distributed denial-of-service (DDoS) attack. DDoS attacks are used to flood the target system with the data so that the response from the target system is either slowed or stopped. Botnets/zombies are used to create enough traffic to impose that kind of damage (we have addressed zombies in Chapter 1 and Botnets in Chapter 2).
3. **Overbilling attack:** Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct or authorize to conduct.
4. **Spoofed policy development process (PDP):** These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].
5. **Signaling-level attacks:** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

To know more on this topic, readers may visit http://www.igr-inc.com/uploads/free_white_papers/3G_MobileSecurity_Jan07.pdf

Mobile Security Processing System (MOSES) is a programmable security processor platform that enables secure data and multimedia communications in next-generation wireless mobile computing. MOSES was developed to meet the security challenges in emerging mobile technology such as 3G and 4G mobile phones and PDAs. It is a security processing architecture to provide secure (i.e., tamper-resistant) and efficient (i.e., high performance, low power) execution of security processing functions. It constitutes three key components, such as Security Processing Engine (SPE), a hierarchical secure memory subsystem and security-enhanced communication architecture, from hardware perspective.

3.4 Credit Card Frauds in Mobile and Wireless Computing Era

These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M-Commerce) and mobile banking (M-Banking). Credit card frauds are now becoming commonplace given the ever-increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone. *Mobile credit card transactions* are now very common; new technologies combine low-cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.

Today belongs to "mobile computing," that is, *anywhere anytime computing*. The developments in wireless technology have fuelled this new mode of working for white collar workers. This is true for credit card processing too; wireless credit card processing is a relatively new service that will allow a person to process credit cards electronically, virtually anywhere. Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally. It is most often used by businesses that operate mainly in a mobile environment. These businesses include mobile utility repair service businesses, locksmiths, mobile windshield repair and others. Some upscale restaurants are using wireless processing equipment for the security of their credit card paying customers. Figure 3.4 shows the basic flow of transactions involved in purchases done using credit cards.[7] Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems (refer to Chapter 5) once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions (Box 3.2).

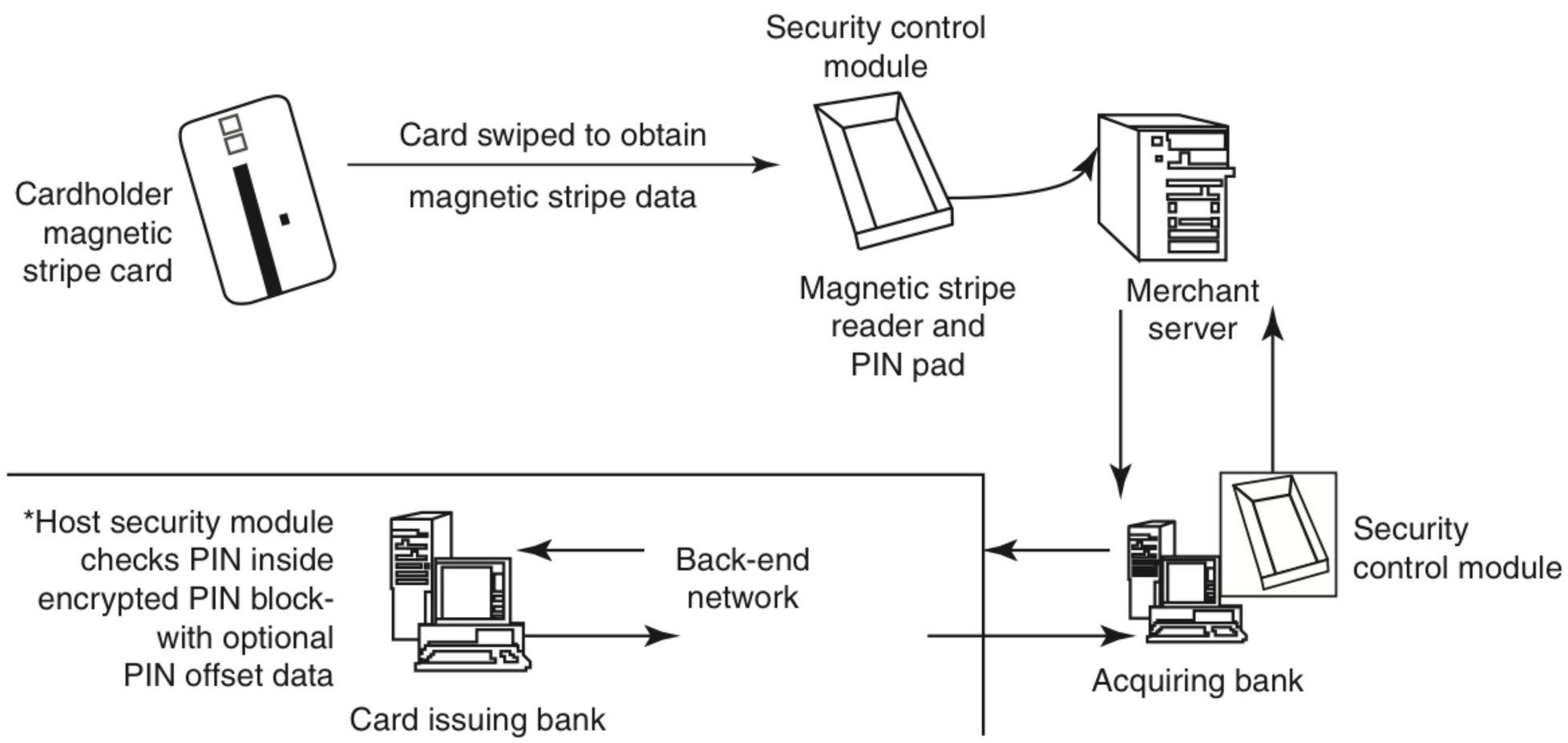


Figure 3.4 | Online environment for credit card transactions.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.2 Tips to Prevent Credit Card Frauds

The current topic is about credit card frauds in mobile and wireless computing era, however, we would like to include these tips to prevent credit card frauds[8] caused due to individual ignorance about a few known facts.

Do's

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
3. Change the default *personal identification number* (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.
7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.

Dont's

1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

Source: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm

There is a system available from an Australian company "Alacrity" called closed-loop environment for wireless (CLEW). Figure 3.5 shows the flow of events with CLEW which is a registered trademark of Alacrity used here only to demonstrate the flow in this environment.[9]

As shown in Figure 3.5, the basic flow is as follows:

1. Merchant sends a transaction to bank;
2. the bank transmits the request to the authorized cardholder [*not* short message service (SMS)];
3. the cardholder approves or rejects (password protected);
4. the bank/merchant is notified;
5. the credit card transaction is completed.

3.4.1 Types and Techniques of Credit Card Frauds

Traditional Techniques

The traditional[10] and the first type of credit card fraud is paper-based fraud – *application fraud*, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) (refer to Chapter 5) to open an account in someone else's name.

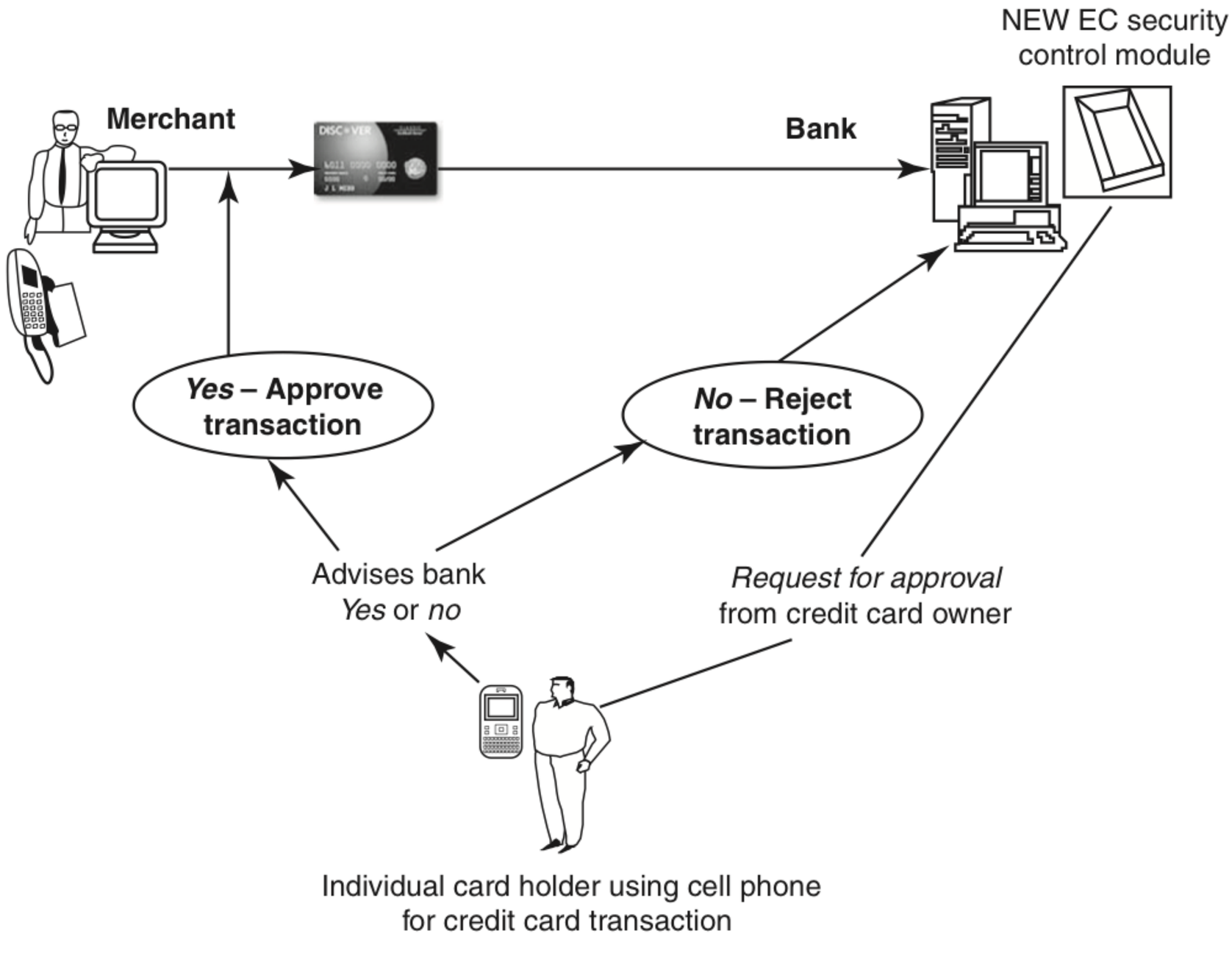


Figure 3.5 | Closed-loop environment for wireless (CLEW).
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.3 Potential Wireless Users – Beware!

Although wireless processing is a very good system for many companies, however, it is not for all mobile businesses. There are some drawbacks to wireless processing that many potential wireless users should be aware of before they venture into wireless processing. They are as follows:

1. **Wireless processing equipment is expensive:** There is no way to get around this. Wireless credit card machines are the most advanced processing terminals available. You get what you pay for! For a wireless terminal with a printer, expect to pay at least US$ 800 for a new terminal and US$ 700 for a refurbished terminal. If you are purchasing a terminal that is much cheaper than any other you find, it is most likely outdated equipment that uses outdated cellular networks. In other words, it is a scam, and you are about to buy a really expensive paperweight.
2. **Wireless processing comes with extra fees:** Just like a cell phone, wireless credit card machines operate on cellular networks. You have to pay for this cellular service in addition to the high cost of equipment. Luckily, wireless fees for processing are nowhere near what they are for cell phones. Expect to pay US$ 20–25 per month for a wireless service fee.
3. **Wireless credit card machines are subject to cellular coverage blackouts:** I know what you are thinking – "My cell phone works almost everywhere, so my wireless credit card machine will too." Sadly, this is not the case. Wireless credit card processing uses a business cellular network called the Motient or Mobitex network. Your cell phone may be using a network called code division multiple access (CDMA) or time division multiple access (TDMA) [global system for mobile communications (GSM)] or some other technology-based network. The coverage that your cell phone gets is much greater than the wireless processing network. There can be some states in your country with no coverage for wireless processing at all.

Box 3.3 Potential Wireless . . . (*Continued*)

4. **You cannot process checks or debit transactions over a wireless network:** Currently owing to federal regulations, it is impossible to process debit transaction or electronic checks over a wireless network. This is something that will probably end up being allowed in the future, but as of now there is not sufficient security or encryption to process these transactions wireless.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Application fraud can be divided into

1. **ID theft:** Where an individual pretends to be someone else (see more on ID Theft in Chapter 5).
2. **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit.

Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

Modern Techniques

Sophisticated techniques[10] enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud. Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another (see more on skimming frauds in Chapter 11 in CD). Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing (see more on this in Chapter 5). Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink/website (i.e., they have been scammed).

1. **Triangulation:** It is another method of credit card fraud and works in the fashion as explained further.
   - The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
   - The customer registers on this website with his/her name, address, shipping address and valid credit card details.
   - The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's website.
   - The goods are shipped to the customer and the transaction gets completed.
   - The crminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

   Such websites are usually available for few weeks/months, till the authorities track the websites through which the criminal has enticed the individuals to reveal their personal details, which enabled the criminal to commit the transactions by using the credit card details of these customers. The entire investigation process for tracking and reaching these criminals is time-consuming, and the criminals may close such fake website in between the process that may cause further difficulty to trace the criminal. The criminals aim to create a great deal of confusion for the authorities so that they can operate long enough to accumulate a vast amount of goods purchased through such fraudulent transactions.
2. **Credit card generators:** It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

3.5 Security Challenges Posed by Mobile Devices

Mobility brings two main challenges to cybersecurity: first, on the hand-held devices, information is being taken outside the physically controlled environment and second remote access back to the protected environment is being granted. Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure. When people are asked about important issues in managing a diverse range of mobile devices, they seem to be thinking of the ones shown in Fig. 3.6.

As the number of mobile device users increases, two challenges are presented: one at the device level called "microchallenges" and another at the organizational level called "macrochallenges." Of these, some microchallenges are discussed in this section and macrochallenges in the next section.

Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security*, *cryptography security*, *Lightweight Directory Access Protocol* (*LDAP*) *security*, *remote access server* (*RAS*) *security*, *media player control security*, *networking application program interface* (*API*) *security, etc*. In this section, we provide a brief discussion on these cybersecurity aspects. For most of the discussion here, the reference point is Windows mobile development given that the developers of the Windows OS are on the forefront of the technology in terms of their mobile computing technological initiatives. In view of the discussion in Section 3.4, the ID theft (we will address it in Chapter 5) is now becoming a major fraud in credit card business domain, wherein individual's *Personally Identifiable Information* (PII) is misused to open new credit accounts, take new loans or engage in other types of frauds, such as misuse of the victim's

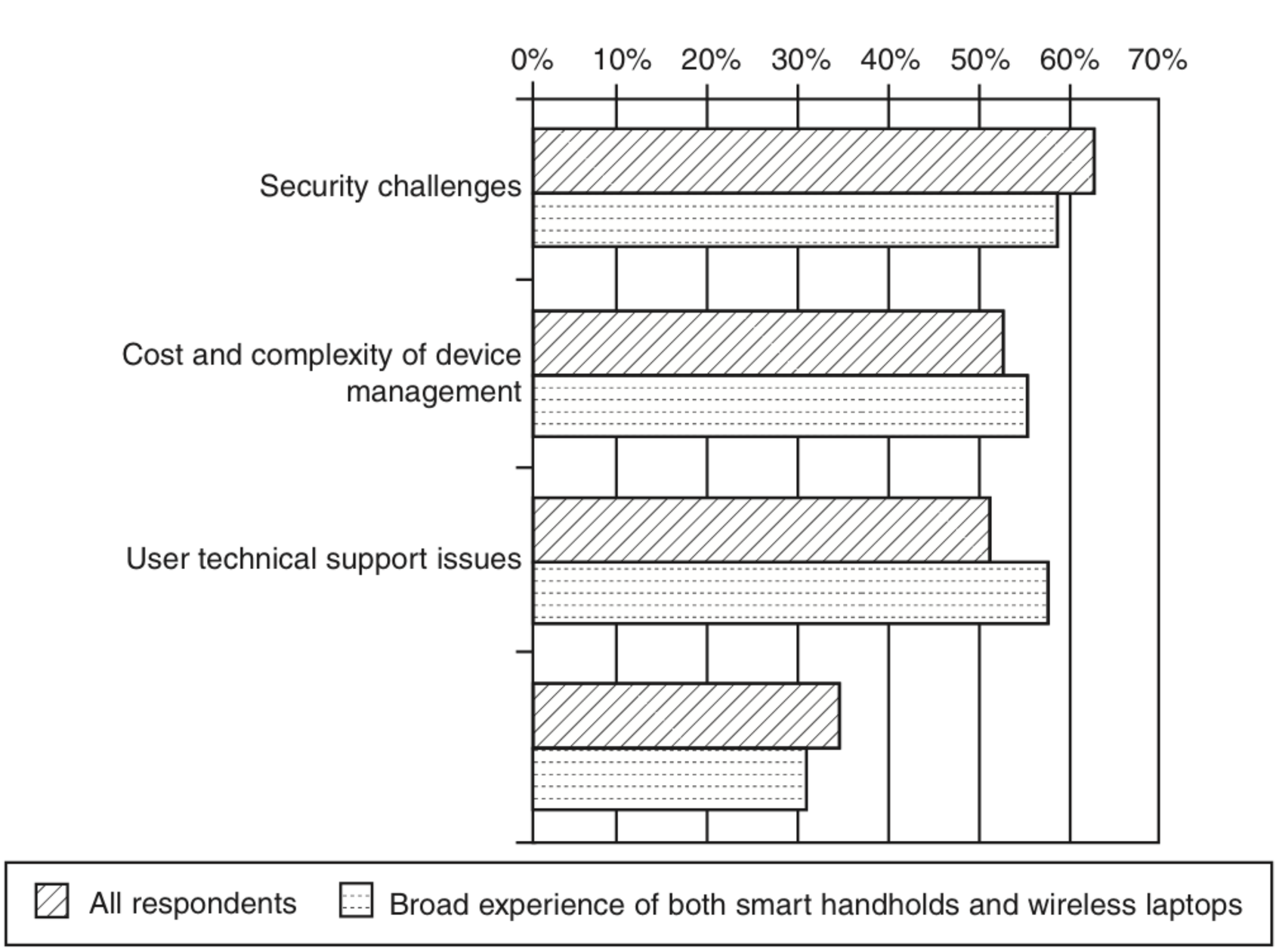


Figure 3.6 Important issues for managing mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

name and identifying information when someone is charged with a crime, when renting an apartment or when obtaining medical care.

3.6 Registry Settings for Mobile Devices

Let us understand the issue of registry settings on mobile devices through an example: Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook. ActiveSync acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device. In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs. In this context,

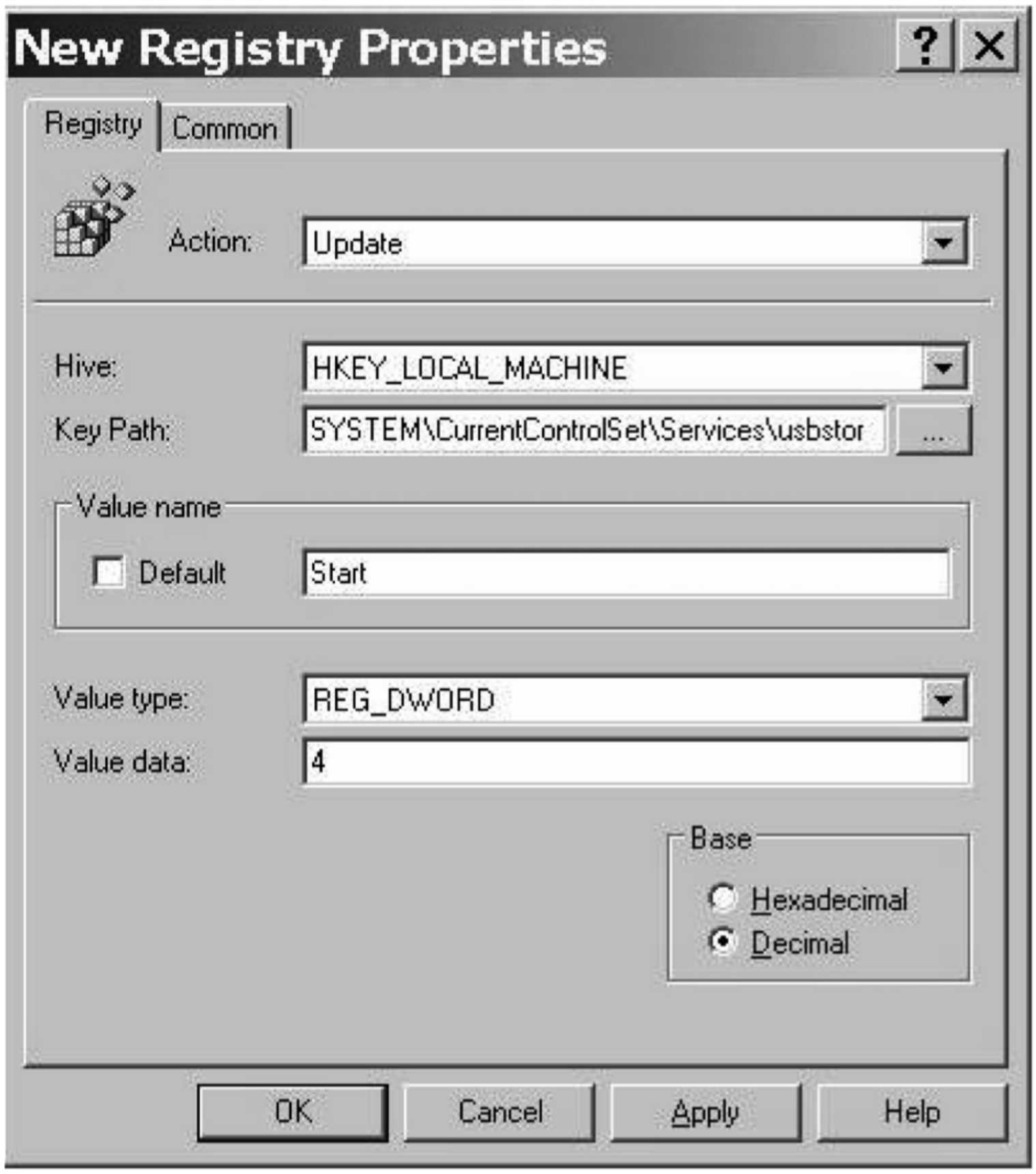


Figure 3.7 | Registry value browsing.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

registry setting becomes an important issue given the ease with which various applications allow a free flow of information.

Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within "group policy." Group policy is one of the core operations that are performed by Windows Active Directory. As a supporting point, consider the following: within the last 2 years, Microsoft has doubled the number of group policy settings that it ships with the OS. There are now nearly 1,700 settings in a standard group policy. The emphasis on most of the group policy settings is security.

There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against *Spyware, viruses, worms, malware* (we will address it in Chapter 4) and other Malicious Codes that run through the networks and the Internet. Microsoft and other companies are trying to develop solutions as fast as they can, but the core problem is still not being addressed. According to the experts, the core problem to many of the mobile security issues on a Windows platform is that the baseline security is not configured properly. When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every *Control Panel setting* and *group policy* option, they may not get the computer to the desired baseline security. For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional *registry* changes that are not exposed through any interface. There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.

Naive users may think that for solving the problem of mobile device security there are not many registry settings to tackle. However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of "registry hacks" that are discussed in Microsoft Knowledge Base articles. Figure 3.7 displays an illustration of how some tools allow users to browse to the desired registry value on their mobile devices.

3.7 Authentication Service Security

There are two components of security in mobile computing: *security of devices* and *security in networks.* A secure network access involves mutual authentication between the device and the base stations or Web servers. This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services. No Malicious Code can impersonate the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices. Some eminent kinds of attacks to which mobile devices are subjected to are: *push attacks*, *pull attacks* and *crash attacks* (see Figs. 3.8–3.10).

Authentication services security is important given the typical attacks on mobile devices through wireless networks: *DoS attacks*, *traffic analysis, eavesdropping*, *man-in-the-middle attacks* and *session hijacking*. We will continue further technical discussion on such topics in Chapter 4. Security measures in this scenario come from *Wireless Application Protocols* (WAPs), use of *VPNs*, *media access control* (*MAC*) *address filtering* and development in 802.xx standards.

3.7.1 Cryptographic Security for Mobile Devices

In this section we will discuss a technique known as *cryptographically generated addresses* (CGA). CGA is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address. The address the owner uses is the corresponding private key to assert address ownership

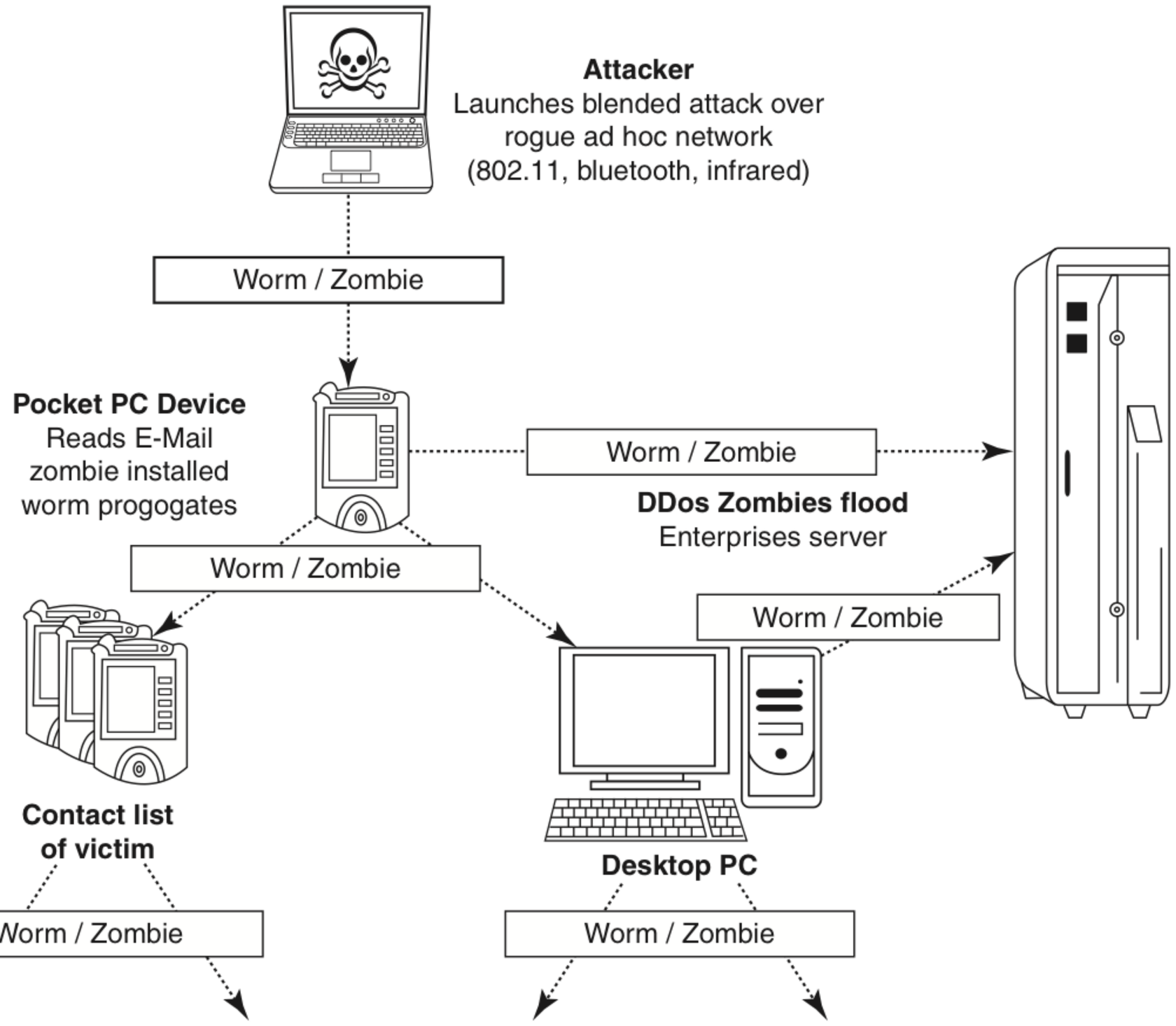


Figure 3.8 Push attack on mobile devices. DDoS implies distributed denial-of-service attack. *Source:* Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

and to sign messages sent from the address without a public-key infrastructure (PKI) or other security infrastructure. Deployment of PKI provides many benefits for users to secure their financial transactions initiated from mobile devices. CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in *context-aware mobile computing applications*) and mobility protocols. It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm, illustrated in Fig. 3.1) are one of the most common hand-held devices used in mobile computing. *Cryptographic security controls* are deployed on these devices. For example, the *Cryptographic Provider Manager* (CPM) in Palm OS5 is a system-wide suite of cryptographic services for securing data and resources on a palm-powered device. The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

3.7.2 LDAP Security for Hand-Held Mobile Computing Devices

LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organizations's Intranet). In a network, a directory tells you where an entity is located in the network. LDAP is a light weight (smaller

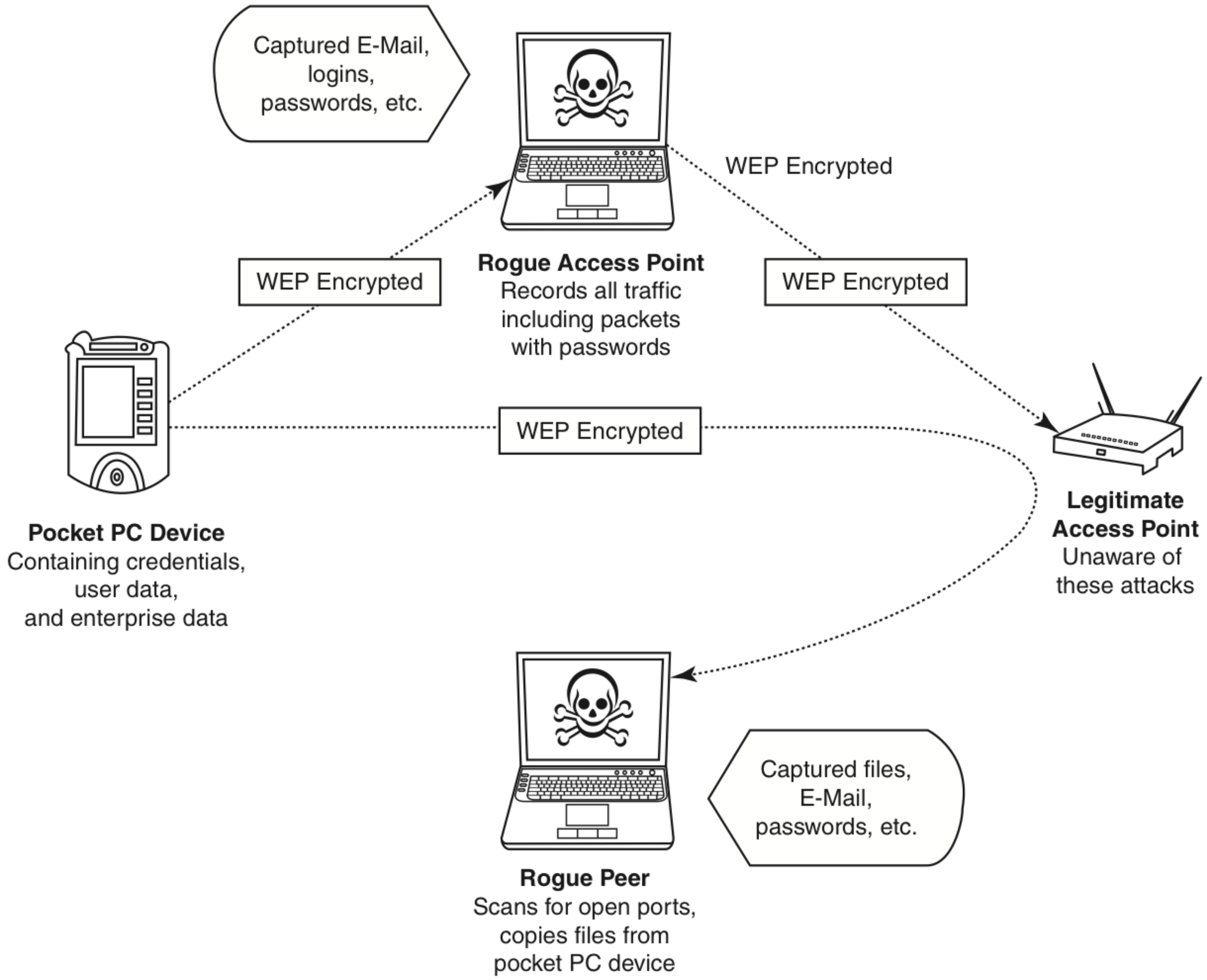


Figure 3.9 | Pull attack on mobile devices.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

amount of code) version of Directory Access Protocol (DAP) because it does not include security features in its initial version. It originated at the University of Michigan and has been endorsed by at least 40 companies. Centralized directories such as LDAP make revoking permissions quick and easy. Box 3.4 describes the directory structure of LDAP.

3.7.3 RAS Security for Mobile Devices

RAS is an important consideration for protecting the business-sensitive data (refer to Chapter 5) that may reside on the employees' mobile devices. In terms of cybersecurity, mobile devices are sensitive. Figure 3.11 illustrates how access to an organization's sensitive data can happen through mobile hand-held devices carried by employees. In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect. By using a mobile device to appear as a registered user (*impersonating* or *masquerading*) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.

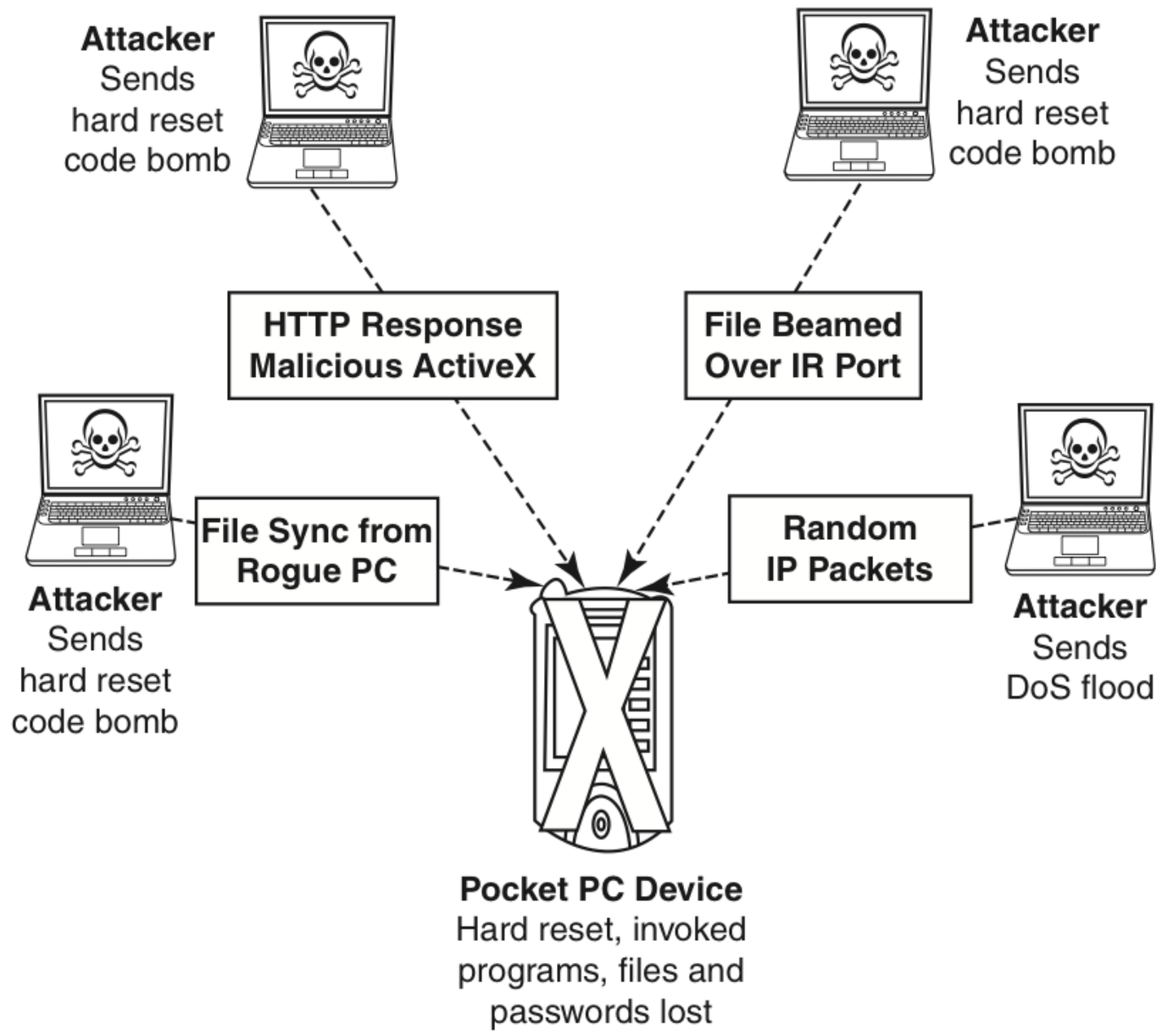


Figure 3.10 | Crash attack on mobile devices. DoS – Denial-of-service attack.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.4 LDAP Directory Structure

An LDAP directory is organized into a simple "tree" structure that consists of the following levels:

1. Root Directory (the source of the tree or the starting point) which branches out to
2. Countries, which branches out to
3. Organizations, which branches out to
4. Organizational units (divisions/departments and so forth), which further branches out to
5. Individuals (which, in turn, include files, shared IT resources such as printers and people)

An LDAP server is called a *Directory Systems Agent* (DSA). It receives a request from a user, takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user. An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically.

Source: http://www.csgnetwork.com/glossaryl.html

Another threat comes from the practice of *port scanning* (refer to Box 2.5 in Chapter 2). First, attackers use a domain name system (DNS) server to locate the *IP address* of a connected computer (either the mobile device itself or a gateway server to which it connects). A *domain* is a collection of sites that are related in some sense. Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls. For instance, *File Transfer Protocol* (FTP) transmissions are typically assigned to port 21. If this port is left unprotected, it can be misused by the attackers (see Box 3.5).

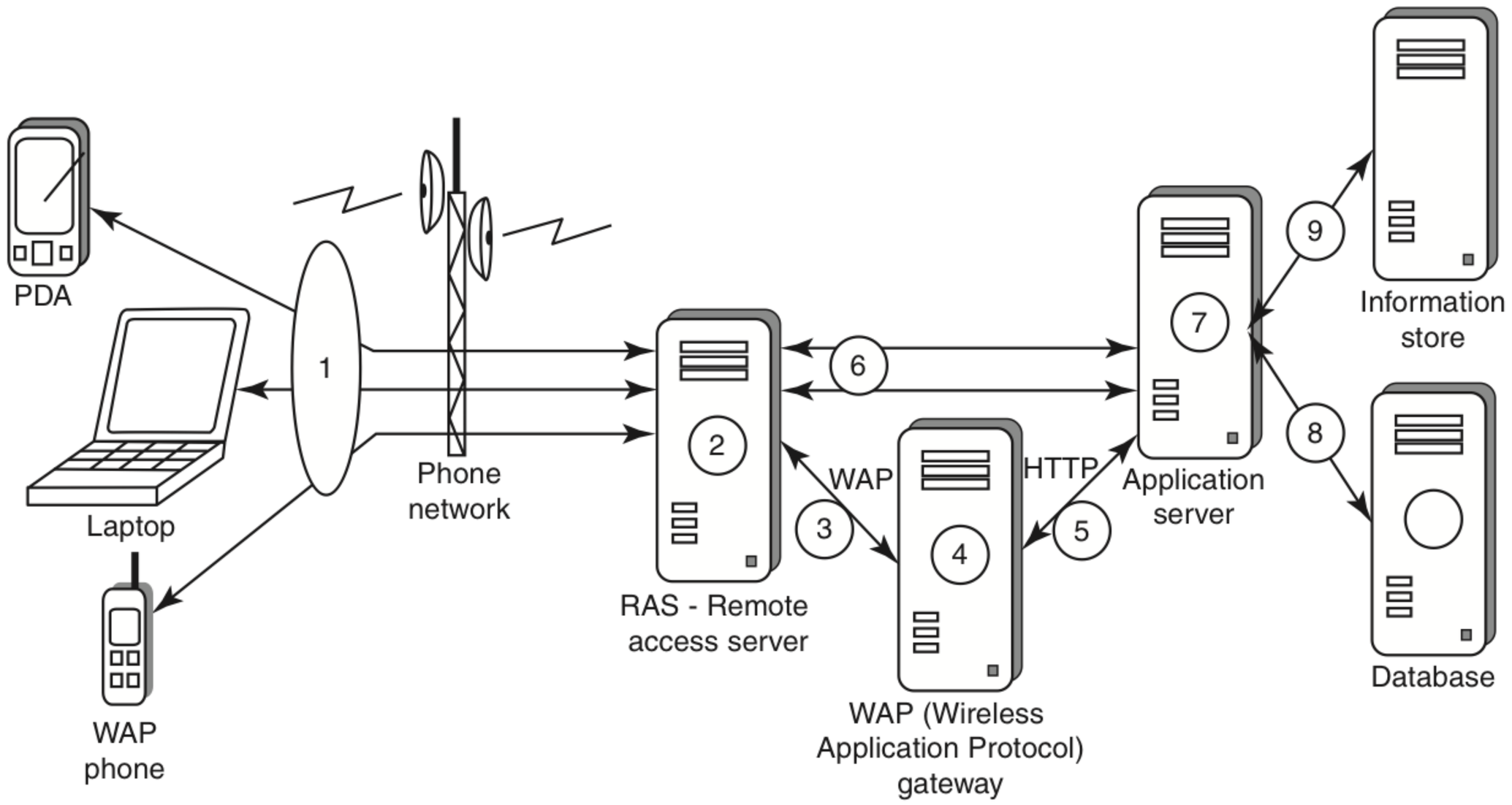


Figure 3.11 Communication from mobile client to organization information store.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Box 3.5 RAS System Security for Mobile Device Clients

The security of a RAS system can be divided into following three areas:

1. The security of the RAS server;
2. the security of the RAS client;
3. the security of data transmission.

Although the desired level of security of the RAS server can be controlled through implementation of local security guidelines, the RAS client (e.g., a mobile hand-held device) is typically not under the complete control of the IT personnel who is responsible for the local area network (LAN). The security of the data transmission media is generally completely out of their control. For this reason, protection of communications between the client and the server must be secured by additional means.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID. A *personal firewall* on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection. For situations where all connections to the corporate network pass through a gateway, placing the personal firewall on the gateway itself could be the simplest solution, because it avoids the need to place a personal firewall on each mobile device. In either case, deploying secure access methods that implement *strong authentication keys* will provide an additional protection.

3.7.4 Media Player Control Security

Given the lifestyle of today's young generation, it is quite common to expect them embracing the mobile hand-held devices as a means for information access, remote working and entertainment. Music and video are the two important aspects in day-to-day aspects for the young generation. Given this, it is easy to appreciate how this can be a source for cybersecurity breaches. Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the "music gateways." There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices. For example, in the year 2002, Microsoft Corporation warned about this.[11] According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people's computer systems and perform a variety of actions. According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer's owner is allowed to do, such as opening files or accessing certain parts of a network.

As another example, consider the following news item of the year 2004: corrupt files posing as normal music and video files could allow an attacker to gain control of the downloader's computer (see Ref. #5, Additional Useful Web References, Further Reading). With this happening, there are three vulnerabilities: (a) files could be created that will open a website on the user's browser (e.g., the user could be accessing from his/her hand-held device) from where remote JavaScript can be operated; (b) files could be created which allow the attacker to download and use the code on a user's machine or (c) media files could be created that will create buffer overrun errors. We will continue further technical discussion on "buffer overflow" in Chapter 4.

In Section 3.6, we have discussed registry settings in connection with the mobile devices' security. This topic becomes important in the context of the current section too. Registry of a computing device is an important concept; it stores information necessary to configure the system for applications and hardware devices. It also contains information that the OS continually references during an operation. In the registry, some keys control the behavior of the Windows Media Player control. Microsoft, through its developer network MSDN, describes details of registry value settings on the mobile devices. With the increase in our mobile workforce and the resulting increase in the number of mobile computing hand-held devices used by the young employees of most IT and software organizations, it would be quite common to expect such cybersecurity attacks and hence one should be ready for security measures.

3.7.5 Networking API Security for Mobile Computing Applications

With the advent of electronic commerce (E-Commerce) and its further off-shoot into *M-Commerce,* online payments are becoming a common phenomenon with the *payment gateways* accessed remotely and possibly wirelessly. Furthermore, with the advent of *Web services* and their use in mobile computing applications (see Ref. #3, Articles and Research Paper, Further Reading), the API becomes an important consideration.

Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications that can be used to target multiple security platforms present in a range of devices such as mobile phones, portable media players, set-top boxes and home gateways.

Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices). Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.

3.8 Attacks on Mobile/Cell Phones

3.8.1 Mobile Phone Theft

Mobile phones have become an integral part of everbody's life and the mobile phone has transformed from being a luxury to a bare necessity. Increase in the purchasing power and availability of numerous low cost handsets have also lead to an increase in mobile phone users. Theft of mobile phones has risen dramatically over the past few years. Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals. Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims. When anyone looses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)" (refer to Chapter 5), that really matter, are lost. Refer to Box 3.6 to learn about tips on securing mobile phone from being stolen and/or lost.

One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement. After PC, the criminals' (i.e., attackers')

Box 3.6 Tips to Secure your Cell/Mobile Phone from being Stolen/Lost

Nowadays, mobiles/cell phones are becoming fancier and expensive hence increasingly liable to theft. Criminals are interested in accessing wireless service and seek potential possibility to stealing the ID.

Ensure to note the following details about your cell phone and preserve it in a safe place[12]:

1. Your phone number;
2. the make and model;
3. color and appearance details;
4. PIN and/or security lock code;
5. IMEI number.

The International Mobile Equipment Identity (IMEI)

It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering *#06# from the keypad.

The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country. For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to "lock" the phone using its IMEI number. This will help to stop the usage of phone in that country, even if a SIM is changed.

Visit the weblink http://www.numberingplans.com/?page=analysis&sub=imeinr to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.

1. Add a security mark on your cell phone. Use permanent marker and print your alternate contact number and short address on your cell phone instrument as well as on battery. In case someone finds your handset, it is easier to contact you if the finder of your cell phone would like to return it you.
2. Set a password and ensure the password is strong enough so that a finder of your cell phone cannot easily guess it.
3. In case of loss of your cell phone, register a complaint with cell phone service provider immediately, using your IMEI number, to enable your service provider to block your cell phone and your account details. Preserve all the details of launched complaints, that is, obtain confirmation in writing from your service provider that your phone has been disabled.

Box 3.6 Tips to Secure your . . . (*Continued*)

4. In case of loss of your cell phone, register a complaint at the police station and obtain FIR. Preserve all the details for launched complaints, that is, FIR report.
5. Keep an eye on your phone while traveling. During the security check at the airport security, ensure to retrieve your cell phone immediately once it enters the x-ray machine – criminals often steal phones during these vulnerable seconds.
6. Keep Wi-Fi and Bluetooth OFF when it is not required to be in use. Airports, coffee shops, hotels and all other public places wherever free Wi-Fi zone is available, criminals always have an eye to seek the vulnerability to steal information.
7. Periodic backup is important and especially if you are traveling, backup before traveling is necessary. It takes only few minutes to take backup but it is always helpful in case you lose your cell phone during traveling.
8. Do not forget to apply all the updates for cell phone software/firmware, received from manufacturers, which are routinely provided to update vulnerabilities fixes.
9. Only download applications from reputable sources – specific care should be taken while downloading plug-in applications on the cell phone. It is always advised to use the recommendations provided by cell phone manufacturers' to download directly from the Web.

Install antitheft software on your cell phone

Antitheft software does not allow the criminal to use another SIM card in the stolen cell phone. When a SIM card is changed, the system asks for a verification code. Even if the criminal manages to break this code, the phone sends out a message regarding the change of SIM to two selected contacts from the cell phone contact directory with the new SIM number. So, it becomes easy to trace the address of the new cell phone number from the service provider and thus to trace the cell. Only the owners of the cell phone will know about the installed antitheft software, as it does not show any icons on the menu. Following are few antitheft software(s) available in the market:

1. **GadgetTrak:** http://www.gadgettrak.com/products/mobile/
2. **Back2u:** http://www.bak2u.com/phonebakmobilephone.php
3. **Wavesecure:** https://www.wavesecure.com/
4. **F-Secure:** http://www.f-secure.com/

Source: http://www.wikihow.com/Protect-a-Mobile-Phone-from-Being-Stolen

new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones. Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.

The following factors contribute for outbreaks on mobile devices:

1. **Enough target terminals:** The first Palm OS virus was seen after the number of Palm OS devices reached 15 million. The first instance of a mobile virus was observed during June 2004 when it was discovered that an organization "Ojam" had engineered an antipiracy Trojan virus in older versions of their mobile phone game known as Mosquito. This virus sent SMS text messages to the organization without the users' knowledge.
2. **Enough functionality:** Mobile devices are increasingly being equipped with office functionality and already carry critical data and applications, which are often protected insufficiently or not at all. The expanded functionality also increases the probability of malware.
3. **Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections. Therefore, unfortunately, the increased amount of freedom also offers more choices for virus writers.

3.8.2 Mobile Viruses

A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it. Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays. In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified. First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.

Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS. Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth-activated phones (i.e., if Bluetooth is always ENABLED into a mobile phone) whereas MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone's address book. Readers may visit http://symbianpoint.com/types-latest-list-mobile-viruses.html to know the list of latest mobile viruses (few viruses have been discussed in Section 3.3 Trends in Mobility).

It is interesting to note that, like Computer Virus Hoax, variants of Mobile Phone Virus Hoax[13] have been circulating since 1999. These hoax messages either will be sent through E-Mail or through SMS to the mobile users. The example of such hoax is given.

"*All mobile users pay attention!!!!!!!!!*

If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call, END THE CALL IMMEDIATELY, if you answer the call, your phone will be infected by a virus. This virus WILL ERASE all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now. You can also check this news in the CNN website.

PLEASE FORWARD THIS PIECE OF INFORMATION TO ALL YOUR FRIENDS HAVING A MOBILE PHONE."

How to Protect from Mobile Malwares Attacks

Following are some tips to protect mobile from mobile malware attacks[14]:

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

3.8.3 Mishing

Mishing is a combination of mobile phone and Phishing (we will address this in Chapter 5). Mishing attacks are attempted using mobile phone technology. M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam. A typical Mishing attacker uses call termed as *Vishing* or message (SMS) known as *Smishing*. Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details. Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

3.8.4 Vishing

Vishing is the criminal practice of using social engineering (refer to Section 2.3 in Chapter 2) over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V – voice and Phishing (we will address Phishing in detail under Chapter 5). Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.[15] (We will address ID Theft in detail in Chapter 5.)

The most profitable uses of the information gained through a Vishing attack include:

1. ID theft;
2. purchasing luxury goods and services;
3. transferring money/funds;
4. monitoring the victims' bank accounts;
5. making applications for loans and credit cards.

How Vishing Works

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. **Internet E-Mail:** It is also called Phishing mail (we will address this in Chapter 5).
2. **Mobile text messaging:** Refer to Smishing explained in Section 3.8.5.
3. **Voicemail:** Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.
4. **Direct phone call:** Following are the steps detailing on how direct phone call works:
   - The criminal gathers cell/mobile phone numbers located in a particular region and/or steals cell/mobile phone numbers after accessing legitimate voice messaging company.
   - The criminal often uses a war dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.
   - When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity. The message instructs the victim to call one phone number immediately. The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
   - When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
   - Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
   - Such calls are often used to harvest additional details such as date of birth, credit card expiration date, etc.

Some of the examples of vished calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

1. Automated message: Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.
   - Press 1 if you need to check your banking details and live balance.
   - Press 2 if you wish to transfer funds.
   - Press 3 to unlock your online profile.
   - Press 0 for any other query.

2. Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."
3. The victim enters his/her bank account number and hears the next prompt: "Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."
4. The caller enters his/her date of birth and again receives a prompt from the automated system: "Thank you. Now please type your PIN, followed by the pound key."
5. The caller enters his PIN and hears one last prompt from the system: "Thank you. We will now transfer you to the appropriate representative."

At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks[16]:

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

3.8.5 Smishing

Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing. The name is derived from "**SMS** Ph**ISHING**." SMS – Short Message Service – is the text messages communication component dominantly used into mobile phones. Refer to Box 3.7 to know how SMS can be abused by using different methods and techniques other than information gathering under cybercrime.

Box 3.7 Pretexting, Sexting and VoIP Spam

Pretexting

It is also a form of social engineering, wherein a pretexter hides his/her purpose and/or identity to get the personal information/sensitive data about another individual. For example, the pretexter may claim his/her affiliation with a survey agency, financial institute or bank. Usually, victims are targeted over the phone and enticed to reveal their information or perform an action. It is more than a simple lie as it most often involves some prior research or setup and the use of pieces of known information (e.g., for impersonation: date of birth, pet names of family members and last bill amount) to establish legitimacy in the mind of the target.[17]

This technique is often used to trick the executives to disclose the information about their customer and/or their competitor and is used by private investigators to obtain telephone records, banking

Box 3.7 Pretexting, . . . (*Continued*)

records, utility records and other information directly from junior representatives of an organization. However, nowadays, this technique is also used by the criminals through Vishing and Smishing attacks.

Sexting

It is the practice of sending sexually explicit text messages and photos over the cell phone. It is becoming an increasingly hot topic both in schools/colleges and in the workplace. Although most of the people think instantly of cell phones as sexting devices, digital photography, Internet (i.e., websites) and even few video game systems are also contributing sexting.[18]

Sexting is a complex topic and no one-size-fits-all solution is available, reason being that it embraces everything from gentle naughty-blue pictures to slimy pornography. Many teens (especially, girls) who believe they are sending a private message, may have their messages widely distributed, sometimes even immediately available on porno sites. So, it is important that parents should keep an eye on the cell phones provided to the kids. Kids should be made aware that "*Information shared electronically never dies*" and any message such as sexting may come back to haunt them even after months and years.

VoIP Spam

VoIP Spam is the proliferation of unwanted, automatically dialed and prerecorded phone calls using VoIP. Some pundits have taken to referring to it as "Spam over Internet telephony" (SPIT).[19] VoIP systems, such as E-Mail and other Internet applications, are susceptible to abuse by criminals to initiate unsolicited and unwanted communications. Increasingly, telemarketers, prank callers and other telephone system abusers are likely to target VoIP systems, particularly, if VoIP tends to supplant conventional telephony.

Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI. The popular technique to "hook" (method used to actually "capture" your information) the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI.

Smishing works in the similar pattern as Vishing. A few examples of Smishing are provided herewith to demonstrate how the victim is forced to disclose PI.

1. "We are happy to send our confirmation toward your enrolment for our 'xxxxxxxx Club Membership'." You will be charged ₹ 50/- per day, unless you reconfirm your acceptance of your membership on our "Membership Office Contact no. XXXXXXXXXX."
2. "[(Name of popular online bank) is confirming that you have purchased LCD TV set, worth of ₹ 90,000/- only from (name of popular computer company)]. Visit www.*abcdef*.com if you did not make this online purchase."

How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.

Box 3.8 SMS Blocker

India-based organization Optinno Mobitech Pvt. Ltd. has innovated and launched an application, *smsBlocker*, which runs on mobile phones and ensures 100% Spam blockage. smsBlocker is powered with a unique intuitive algorithm to detect and block Spam SMS automatically. However, mobile user can also customize the filtering levels as per his/her own privacy requirements. smsBlocker is configured to the unique mobile handset identification number, that is, IMEI. Thus, if a mobile user changes the mobile handset, smsBlocker will not work on the new mobile handset; however, if SIM card is changed it will not affect smsBlocker. smsBlocker is designed for all mobile handsets that support Symbian OS. It is interesting to note that smsBlocker does not require GPRS/Internet connection.

Source: http://www.smsblocker.in (30 July 2010).

3. Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

3.8.6 Hacking Bluetooth

Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile devices (see Box 3.9). Bluetooth is a short-range wireless communication service/technology that uses the 2.4-GHz frequency range for its transmission/communication. The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.

When Bluetooth is enabled on a device, it essentially broadcasts "I'm here, and I'm able to connect" to any other Bluetooth-based device within range. This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers. The attacker installs special software [see Table 3.1 for list of software(s) which are termed as *Bluetooth hacking tools*] on a laptop and then installs a Bluetooth antenna. Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth-enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

Box 3.9 Bluetooth

The word Bluetooth is an anglicized form of Danish *Blåtand* – Harald Bluetooth was king of Denmark in the 10th century, who managed to unite Denmark and parts of Norway into a single kingdom. The king was killed in 986 AD during a battle with his son. Choosing this name indicates how important companies from the Nordic region (nations including Denmark, Sweden, Norway and Finland) are to the communications industry, even if this name says little about the way the technology works. The implication is that Bluetooth does the same with communication protocols, uniting them into one universal standard. *blå* in modern Scandinavic languages means blue and (historically) correct translation of Old Norse *Harald Blátönn* could be Harald Bluetooth.

The Bluetooth logo is a bind rune merging the Germanic runes ᚼ (Hagall) and ᛒ (Berkanan).

Table 3.1 | Bluetooth hacking tools

Sr. No.	*Name of the Tool*	*Description*
1	BlueScanner	This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2	BlueSniff	This is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices.
3	BlueBugger	The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4	Bluesnarfer	If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5	BlueDiving	Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

Bluejacking, *Bluesnarfing, Bluebugging* and *Car Whisperer* are common attacks that have emerged as Bluetooth-specific security issues.

1. **Bluejacking:** It means *Bluetooth* + *Jacking* where Jacking is short name for *hijack* – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), for example, sending a visiting card which will contain a message in the name field. If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact. Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.
2. **Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.
3. **Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention. During initial days, the attacker could simply listen to any conversation his/her victim is having; however, further developments in Bluebugging tools have enabled the attacker with the ability to take control of the victim's phone and to conduct many more activities such as initiate phone calls; send and read SMS; read and write phonebook contacts; eavesdrop on phone conversations and connect to the Internet.
4. **Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo. Further reasearch is underway to know whether Bluetooth attackers could do anything more serious such as disabling airbags or brakes through this kind of attack. The reasearchers are also investigating about possibility of an attacker accessing a telephone address book once the connection gets established with the Bluetooth system through this kind of attack.

Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking. These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

Box 3.10 Hacking Mobile Phones

Chris Paget, a hacker, conducted a demonstration on how to intercept mobile phone calls using an equipment that costs not more than US$ 1,500, at a DefCon conference in Las Vegas.

The hacker used a simple antenna and some basic radio equipments to broadcast a GSM signal and pretend to be a telecom service provider. After this clever trick, it is possible for a hacker to forward his/her own calls and listen to any conversation that takes place within the network.

Although this demonstration is limited to GSM networks, the hacker is quite confident about causing disruption into 3G mobile networks with a simple noise generator and a power amplifier.

Smart readers can immediately conclude that although INTEGRITY is always challenged during the transmitting of the text messages, the threat of breaching the voice communication has also become important under cybersecurity.

Source: http://www.geekwithlaptop.com/hacker-demonstrates-powerful-mobile-interception-at-minimal-expense (3 August 2010).

"Bluetooth and Bluetooth Security" is a separate subject in itself. Readers may visit the following websites to explore more on this topic:

- https://www.bluetooth.org/apps/content/
- http://www.bluetooth.com/English/Pages/default.aspx
- http://www.bluetoothhack.info/

3.9 Mobile Devices: Security Implications for Organizations

3.9.1 Managing Diversity and Proliferation of Hand-Held Devices

In the previous sections we have talked about the microissues of purely technical nature in mobile device security. In this section, we focus on the macroissues at the organizational level. Given the threats to information systems through usage of mobile devices, the organizations need to establish security practices at a level appropriate to their security objectives, subject to legal and other external constraints. Some organizations will implement security procedures and tools extensively, whereas others will place more value on cost and convenience. Whatever approaches an organization chooses, it is important that the policy-making effort starts with the commitment from a Chief Executive Officer (CEO), President or Director who takes cybersecurity seriously and communicates that throughout an organization. The best security technology features will be found to be worthless if there is no organization policy or automated enforcement to ensure that they are actually used.

In some cases, for example, senior executives have been given special access rights to the corporate network which can circumvent standard security procedures. Cybersecurity is always a primary concern; even then, at times, there is still some short sightedness. Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices. Mobile devices of employees should be registered in corporate asset register irrespective of whether or not the devices have been provided by the organization. In addition (recall the microlevel technical issues discussed in the previous section), close monitoring of these devices is required in terms of their usage. When an employee leaves, it is important to remove his/her logical as well as physical access to corporate resources because employees (for malicious or other reasons) could be using their mobile devices to connect into the corporate networks. Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.

Box 3.11 TrustZone Technology for Mobile Devices – Toward Security of M-Commerce Applications

About 2 years back, *Trusted Logic Security Module* was announced for *Microsoft Windows CE 5.0*. With this, developers of Windows CE 5.0 can use Trusted Logic software to increase *electronic transaction security* in ARM-powered(R) devices, which is very pertinent in the M-Commerce paradigm.

The Windows CE 5.0 evaluation version of the security module, coupled with the ARM TrustZone technology, provides consumers with a more *secure environment for electronic transactions* such as *M-Banking, E-Commerce* and digital rights management (DRM) (refer to Appendix N). This security can be designed into ARM-powered consumer devices such as *mobile phones, payment terminals* and *set-top boxes*.

The security module implements the TrustZone APIs to enable smooth evolution and compatibility with future versions of the software running on ARM TrustZone technology-enabled processors. The software is part of a portfolio of embedded security products offered by ARM and developed under a recently announced agreement between Trusted Logic and ARM.

ARM TrustZone architecture extensions build security into the processor itself whereas TrustZone software provides trusted foundation software, protected by the hardware, enabling OS providers, handset vendors and silicon designers to expand and develop their own security solutions on top of an interoperable framework. Currently, security-aware applications must be rewritten for every security platform they run on. However, the new TrustZone Software API provides a standard interface for these applications to be partitioned and to communicate with a secure-side component independent of the actual system implementation.

According to experts, M-Commerce applications can now target multiple security platforms and speed up the development. Industry analysts say that this is a technical collaboration between Microsoft and ARM. This is being considered as a good step toward making mobile devices more secure and is critical to the success of next-generation mobile applications.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

In addition, employees should be encouraged to register with the IT department any devices they use for themselves, so that access can be provisioned in a controlled manner and de-provisioned appropriately when the employee leaves.

Younger workers (also referred to as Gen-Y) are pushing many enterprises to embrace mobility solutions. These younger workers prefer instant/text messaging instead of E-Mail, and frequently use social networking services such as Facebook, MySpace and Twitter. They often prefer to use personal, consumer-oriented devices (both laptops and mobile devices) in the work environment, and adapt quickly to new technology. In contrast, older workers are found to be slow to accept mobility solutions and rely almost entirely on voice communications and E-Mail. These old workers often do not see the benefit of instant messaging and social networking. Interestingly, at the same time these older workers are often found to be on the seat that provides authority and control for staffing and budget, and they can therefore greatly influence mobility policy. These different points of view between younger and older workers have created a mobility generational gap. Older workers sometimes see younger workers as being "spoiled" whereas younger workers sometimes see older workers as a barrier to progress.

3.9.2 Unconventional/Stealth Storage Devices

We have already mentioned about mobile phones and media players used by the employees. In this section, we would like to emphasize upon widening the spectrum of mobile devices and focus on secondary storage devices, such as compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees. As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes – unconventional/stealth storage devices available nowadays are difficult to detect and have become a

prime challenge for organizational security. It is advisable to prohibit the employees in using these devices [see Figs. 3.12(a) and (b)]. Their small size allows for easy concealment anywhere in a bag or on the body.

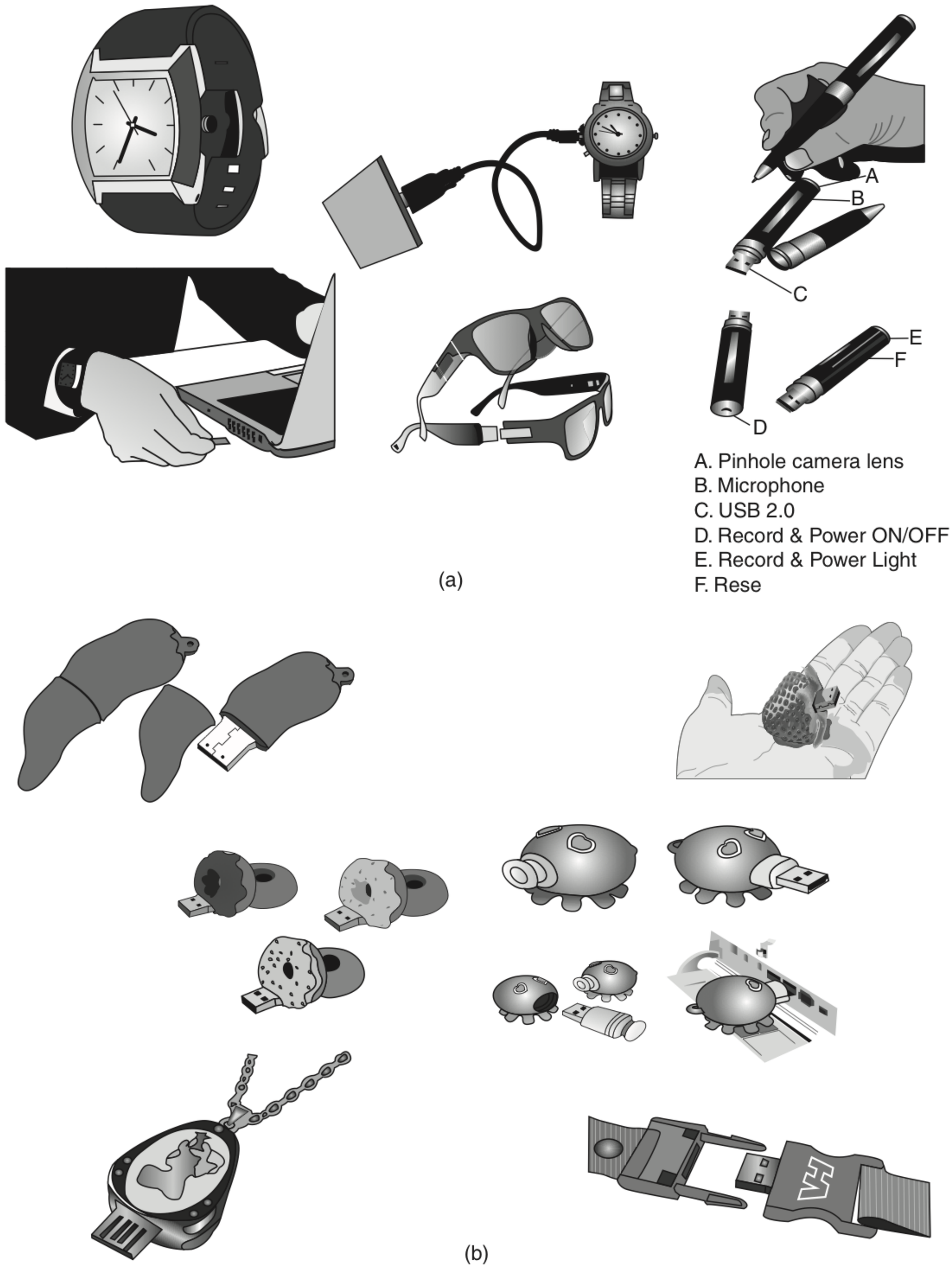


Figure 3.12 | Unconventional/stealth storage devices.

Firewalls and antivirus software are no defense against the threat of open USB ports. Not only can *viruses, worms* and *Trojans* (we will discuss more in Chapter 4) get into the organization network, but can also destroy valuable data in the organization network. Organization has to have a policy in place to block these ports while issuing the asset to the employee. However, sometimes the standard access controls with Windows OS do not allow the assignment of permissions for USB ports and restricting these devices becomes next to impossible. Disgruntled employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses. As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.

Using "DeviceLock" software solution, one can have control over unauthorized access to plug and play devices (for more details, visit http://www.devicelock.com/). The features of the software allows system administrator to:

1. Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
2. Control the access to devices depending on the time of the day and day of the week.
3. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
4. Set devices in read-only mode.
5. Protect disks from accidental or intentional formatting.

Another factor in cybersecurity complications with mobile devices is their falling cost. Until few years ago, mobile devices were considered as an office supply item instead of a powerful computing platform. Early hand-helds were *expensive* and *specialized*, so they were deployed only for specific applications, but more general-purpose models are now available at a relatively low cost, often bundled with a tariff for wireless connection. So, many organizations did not have policies concerning the usage of mobile/wireless devices at work/connected with work. Nowadays, because modern hand-held devices for mobile computing are, at times, good productivity tools, they cannot be precluded from use by employees, contractors and other business entities. Given this, it is important for the device management teams to include user awareness education; thus, they get encouraged to take some personal responsibility for the physical security of their devices, as many IT managers have learned from their bitter experience.

3.9.3 Threats through Lost and Stolen Devices

This is a new emerging issue for cybersecurity. Often mobile hand-held devices are lost while people are on the move. Lost mobile devices are becoming even a larger security risk to corporations. A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period. Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices. See Box 3.12 for some interesting facts on lost mobile devices.

The cybersecurity threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity, as most of the times the mobile hand-held devices are provided by the organization. Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators. Even if these lost devices are personal, the issue is no less serious given the resulting privacy exposures! Gartner Group had predicted that by 2003 there will be over one billion mobile devices in use globally. This is true going by the sales figures quoted in annual

Box 3.12 Getting Lost!!

Cities and countries in which drivers were surveyed were Chicago; Copenhagen, Denmark; Helsinki, Finland; London; Munich, Germany; Oslo, Norway; Paris; Stockholm, Sweden and Sydney, Australia.

1. Pointsec Mobile Technologies, Inc. has discovered where lost electronic devices go: they wind up in the back seats of taxis all around the world!!
2. A survey of 935 cabbies in 9 countries turned up 85 notebook computers, 227 PDAs and 2,238 cell phones lost in cabs in the last 6 months.
3. As per Gartner 2002 report, nearly 250,000 hand-held devices were left behind in the US airports in 2002, and of those, only about 30% were traced back and returned to their owners.
4. Copenhagen appears to have the most forgetful cell phone users, with 719 phones left behind in 100 cabs in a 6-month period. Chicago cab riders left behind 387 in the same period. In total, 97 PDAs and 20 notebooks were reported lost in Chicago. London cabbies reported 23 laptops left behind.
5. As per Gartner 2004 study, a company with 5,000 or more employees could save US$ 300,000–500,000 annually by tagging, tracking and recovering mobile phones and PDAs.

Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

reports published by Research in Motion. This shows that the popularity of mobile devices is increasing at a rapid rate; however, people have not been educated about the importance of securing them. The picture is indeed scary; mobile users are in an even worse position now because they are far more reliant on their mobile devices to store large amounts of sensitive information with very few concerned about backing it up or protecting it.

3.9.4 Protecting Data on Lost Devices

Given the above discussion, readers can appreciate the importance of data protection especially when it resides on a mobile hand-held device. At an individual level, employees need to worry about this. There are two reasons why cybersecurity needs to address this issue: data that are persistently stored on the device and always running applications. For protecting data that are stored persistently on a device, there are two precautions that individuals can take to prevent disclosure of the data stored on a mobile device: (a) encrypting sensitive data and (b) encrypting the entire file system (this may be useful when using data outside of a database, such as in a spreadsheet). Data that are stored on hard disks in persistent memory or on removable memory sticks (whether they are in or out of the device) should be protected. There are many third-party solutions/tools available to protect data on the lost devices, including encrypting the servers where a database file is residing. There are solutions using which individuals can enforce a self-destruct policy to destroy privileged data on a lost device or create a database action to delete the data on a user's device using a suitable tool.

A key point here is that the organizations should have a clear policy on how to respond to the loss or theft of a device, whether it is data storage, a PDA or a laptop. There should be a method for the device owner to quickly report the loss, and device owners should be aware of this method. Writing the emergency contact information on the device itself is unlikely to be very helpful.

3.9.5 Educating the Laptop Users

Often it so happens that corporate laptop users could be putting their company's networks at risk by downloading non-work-related software capable of spreading viruses and Spyware. This is because the software

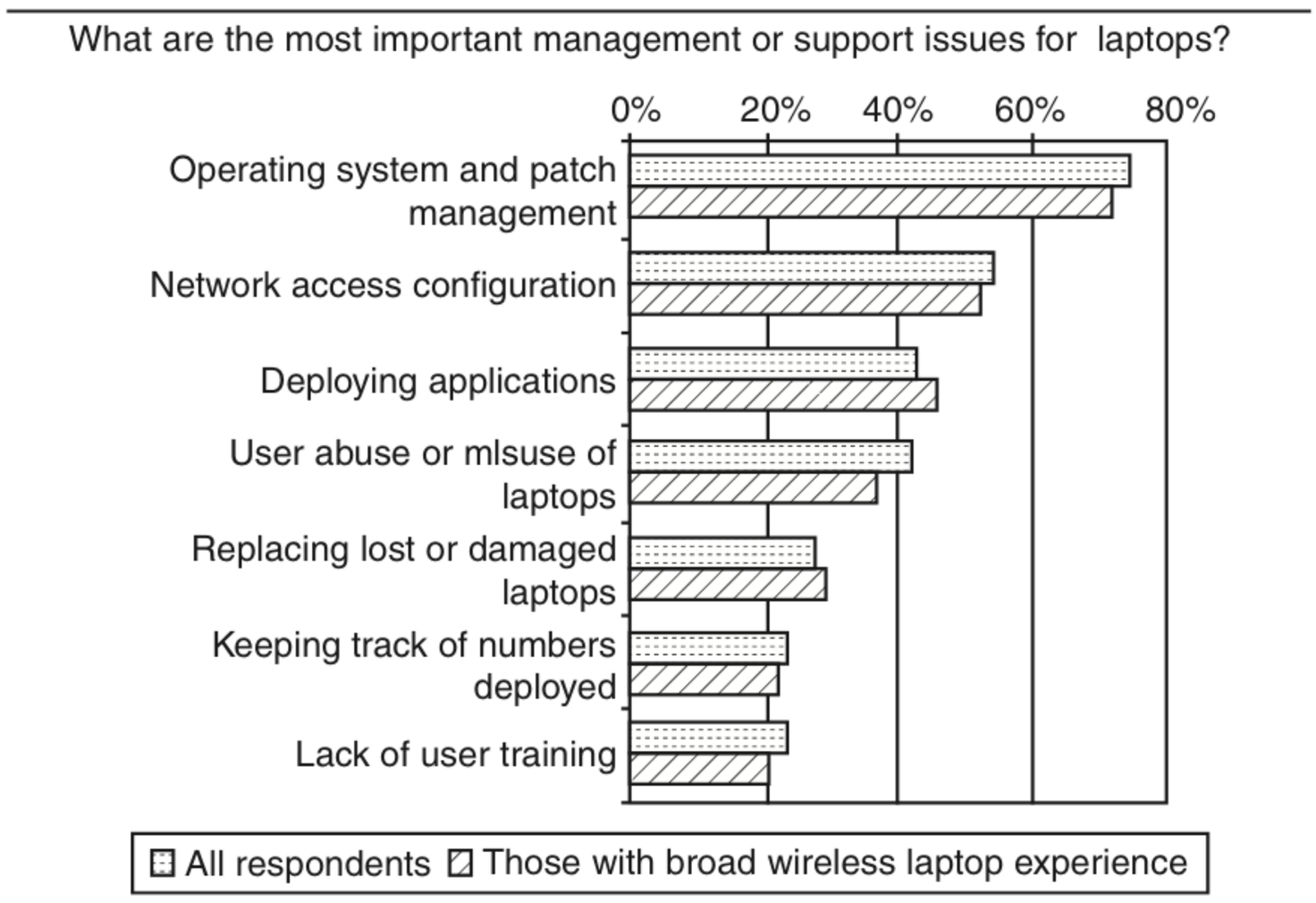


Figure 3.13 Most important management or support issues for laptops.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

assets on laptops become more complex as more applications are used on an increasingly sophisticated OS with diverse connectivity options.

According to year 2004 finding, through one survey, it was found that some 86% of employees with laptops admitted to installing software onto their machines when outside of the office, with many using their laptops to access peer-to-peer websites and downloading illegal music files and movies. As per one survey of 500 European business laptop users, Malicious Code, such as Spyware and viruses, is infecting laptops and consequently business networks when they are reconnected to the corporate systems.

The result from a survey quoted in Fig. 3.13 further supports this point on cybersecurity threats from corporate laptop users. However, despite the growth in corporate security risks, resulting from mobile working, the tone of most of the security-awareness surveys shows that only half of the companies have tools in place to manage the Internet access on laptops, with only one-quarter of businesses physically enforcing these policies. An important point to be noted is that the policies and procedures put in place for support of laptop have evolved over the years to be able to cope successfully with managing laptops, connected by wireless means or otherwise. This shows how much role "perception" plays in terms of most people perceiving laptops as greater culprits compared with other innocuous-looking mobile hand-held devices.

3.10 Organizational Measures for Handling Mobile Devices-Related Security Issues

So far, we have discussed micro- and macrolevel security issues with mobile devices used for mobile computing purposes and what individuals can do to protect their personal data on mobile devices. In this section, we discuss what organizations can do toward safeguarding their information systems in the mobile computing paradigm.

3.10.1 Encrypting Organizational Databases

Critical and sensitive data reside on databases [say, applications such as customer relationship management (CRM) that utilize patterns discovered through *data warehousing* and *data mining* (DM) techniques] and with the advances in technology, access to these data is not impossible through hand-held devices. It is clear that to protect the organizations' data loss, such databases need encryption. We mention here two algorithms that are typically used to implement strong encryption of database files: Rijndael (pronounced rain-dahl or Rhine-doll), a block encryption algorithm, chosen as the new Advanced Encryption Standard (AES) for block ciphers by the National Institute of Standards and Technology (NIST). (See Ref. #13, Additional Useful Web References, Further Reading). The other algorithm used to implement strong encryption of database files is the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio.

The term "strong encryption" is used here to describe these technologies in contrast to the simple encryption. *Strong encryption* means that it is much harder to break, but it also has a significant impact on performance. Database file encryption technology, using either the AES or the MDSR algorithms, makes the database file inoperable without the key (password). Encrypting the database scrambles the information contained in the main database file (i.e., all temporary files and all transaction log files) so that it cannot be deciphered by looking at the files using a disk utility. There is a performance impact for using strong encryption. A weaker form of encryption is also available that has negligible performance impact.

When using strong encryption, it is important *not* to store the key on the mobile device: this is equivalent to leaving a key in a locked door. However, if you lose the key, your data are completely inaccessible. The key is case-sensitive and must be entered correctly to access your database. The key is required whenever you want to start the database or you want to use a utility on your database. For greater security there is an option available that instructs the database server to display a dialog box where the user can enter the encryption key. This option is necessary because the encryption key should not be entered on the machine in clear text. To protect the scenario of information attack/stealing through the mobile devices connecting to corporate databases, additional security measures are possible through enforcing a self-destruct policy that is controlled from the server. When a device that is identified as lost or stolen connects to the organization server, IT department can have the server send a package to destroy privileged data on the device.

3.10.2 Including Mobile Devices in Security Strategy

The discussion so far makes a strong business case – in recognition of the fact that our mobile workforce is on the rise, organizational IT departments will have to take the accountability for cybersecurity threats that come through inappropriate access to organizational data from mobile-device–user employees. Encryption of corporate databases is not the end of everything. However, enterprises that do not want to include mobile devices in their environments often use security as an excuse, saying they fear the loss of sensitive data that could result from a PDA being stolen or an unsecured wireless connection being used. Their concerns are no longer viable. There are technologies available to properly secure mobile devices. These should be good enough for most organizations. Corporate IT departments just need to do their homework. For example, there are ways to make devices lock or destroy the lost data by sending the machine a special message. Also, some mobile devices have high-powered processors that will support 128-bit encryption. Although mobile devices do pose unique challenges from a cybersecurity perspective, there are some general steps that the users can take to address them, such as integrating security programs for mobile and wireless systems into the overall security blueprint. A few things that enterprises can use are:

1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.

2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
3. Develop a system of more frequent and thorough security audits for mobile devices.
4. Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company's overall IT strategy.
5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

In the next section, our focus is on security policies relating to mobile devices.

3.11 Organizational Security Policies and Measures in Mobile Computing Era

3.11.1 Importance of Security Policies relating to Mobile Computing Devices

Proliferation of hand-held devices used makes the cybersecurity issue graver than what we would tend to think. People (especially, the youth) have grown so used to their hand-helds that they are treating them like wallets! For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their hand-held devices (we have already discussed the threats through media player when we talked about microlevel technical issues for cybersecurity threats through these devices). One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization, merger or takeover plans and also other valuable information that could impact stock values in the mobile devices. Imagine the business impact if an employee's USB, pluggable drive or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information. Not only would this be a public relations (PR) disaster, but it could also violate laws and regulations. One should give a deep thought about the potential legal troubles for a public company whose sales reports, employee records or expansion plans may fall into wrong hands.

When controls cannot be implemented to protect data in the event they are stolen, the simplest solution is to prevent users from storing proprietary information on platforms deemed to be insufficiently secure. This sort of policy can be difficult to enforce, however, by increasing awareness of the user, it can be reasonably effective. Information classification and handling policy should clearly define what sorts of data may be stored on mobile devices. In the absence of other controls, simply not storing confidential data on at-risk platforms will mitigate the risk of theft or loss.

A survey[20] released by the Ponemon Institute, on behalf of Cellcrypt (www.cellcrypt.com), reveals that large and medium businesses are putting themselves at risk as a result of cell phone voice call interception. According to this survey of 75 companies and 107 senior executives in the US, it costs US corporations on average US$ 1.3 million each time a corporate secret is revealed to unauthorized parties. About 18% of respondents estimate such losses to occur weekly or more frequently, 61% at least monthly and 90% at least annually.

The survey asked the participants about the likelihood of six separate scenarios involving the use of cell phones to communicate sensitive and confidential information occurring in their organizations. The scenarios described the following:

1. A CEO's administrative assistant uses a cell phone to arrange ground transportation that reveals the CEO's identity and location.

2. The finance and accounting staff discusses earnings of press release and one participant on the call is using a cell phone.
3. A conference call among senior leaders in the organization in which cell phones are sometimes used.
4. A sales manager conducting business in Asia uses, his/her cell phone to communicate with the home office.
5. An external lawyer asks for proprietary and confidential information while using his cell phone.
6. A call center employee assists a customer using a cell phone to establish an account and collects personal information (including SSN).

3.11.2 Operating Guidelines for Implementing Mobile Device Security Policies

In situations such as those described above, the ideal solution would be to prohibit all confidential data from being stored on mobile devices, but this may not always be practical. Organizations can, however, reduce the risk that confidential information will be accessed from lost or stolen mobile devices through the following steps:

1. Determine whether the employees in the organization need to use mobile computing devices at all, based on their risks and benefits within the organization, industry and regulatory environment.
2. Implement additional security technologies, as appropriate to fit both the organization and the types of devices used. Most (and perhaps all) mobile computing devices will need to have their native security augmented with such tools as strong encryption, device passwords and physical locks. Biometrics techniques (retinal scans, iris scans, etc.) can be used for authentication and encryption and have great potential to eliminate the challenges associated with passwords.
3. Standardize the mobile computing devices and the associated security tools being used with them. As a matter of fundamental principle, security deteriorates quickly as the tools and devices used become increasingly disparate.
4. Develop a specific framework for using mobile computing devices, including guidelines for data-syncing, the use of firewalls and anti-malware software and the types of information that can be stored on them.
5. Centralize management of your mobile computing devices. Maintain an inventory so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices. This can often be simplified by integrating patching with syncing or patch management with the centralized inventory database.
7. Label the devices and register them with a suitable service that helps return recovered devices to the owners.
8. Establish procedures to disable remote access for any mobile devices reported as lost or stolen. Many devices allow the users to store usernames and passwords for website portals, which could allow a thief to access even more information than on the device itself.
9. Remove data from computing devices that are not in use or before re-assigning those devices to new owners (in case of company-provided mobile devices to employees). This is to preclude incidents through which people obtain "old" computing devices that still had confidential company data.
10. Provide education and awareness training to personnel using mobile devices. People cannot be expected to appropriately secure their information if they have not been told how.

3.11.3 Organizational Policies for the Use of Mobile Hand-Held Devices

The first step in securing mobile devices is creating company policies that address the unique issues these devices raise. Such questions include what an employee should do if a device is lost or stolen. We have talked about this in Section 3.9.4.

There are many ways to handle the matter of creating policy for mobile devices. One way is creating a distinct mobile computing policy. Another way is including such devices under existing policy. There are also approaches in between, where mobile devices fall under both existing general policies and a new one. In the hybrid approach, a new policy is created to address the specific needs of the mobile devices (such as what to do if they are lost or stolen) but more general usage issues fall under general IT policies. As a part of this approach, the "acceptable use" policy for other technologies is extended to the mobile devices. There may not be a need for separate policies for wireless, LAN, wide area network (WAN), etc. because a properly written network policy can cover all connections to the company data, including mobile and wireless.

Companies new to mobile devices may adopt an umbrella mobile policy but they find over time that they will need to modify their policies to match the challenges posed by different kinds of mobile hand-held devices. For example, wireless devices pose different challenges than non-wireless devices. Also, employees who use mobile devices more than 20% of the time will have different requirements than less-frequent users. It may happen that over time, companies may need to create separate policies for the mobile devices on the basis of whether they connect wirelessly and with distinctions for devices that connect to WANs and LANs.

It is never too early to start planning for mobile devices, even when a company, at a given point of time, cannot afford creating any special security policies to mitigate the threats posed by mobile computing devices to cybersecurity. It is, after all, an issue of new technology adoption for many organizations. By contemplating its uses, companies may think of ways they can use it and, perhaps just as important, how their competitors will use it.

3.12 Laptops

As the price of computing technology is steadily decreasing, usage of devices such as the laptops is becoming more common. Although laptops, like other mobile devices, enhance the business functions owing to their mobile access to information anytime and anywhere, they also pose a large threat as they are portable.

Box 3.13 Spy Phone Software!!!

Spy Phone software is installed on the mobile/cell phone of employees, if the employers wants to monitor phone usage. The Spy Phone software is completely hidden from the user, once it is intsalled and collects all the available data such as SMS messages, ingoing/outgoing call history, location tracking, GPRS usage and uploads the collected data to a remote server.

The employer can simply access the designated website hosted by Spy Phone vendor, and after entering his/her account details, he/she can have full access to all the data collected 24 hours a day, 7 days a week. The employer can access this website through the Internet; hence, he/she can keep an eye on their employees, regardless where he/she is in the world. The employer can read all SMS messages (both incoming and outgoing), know who they (employees) are calling or who is calling them and where they were when the call was received.

Following are few Spy Phone Software(s) available in the market:

1. **SpyPhonePlus:** http://www.spyphoneplus.com/
2. **FlexiSpy:** http://www.flexispy.com/
3. **TheSpyPhone:** http://www.thespyphone.com/spyphone.html
4. **Mobile Spy:** http://www.mobile-spy.com/

Wireless capability in these devices has also raised cybersecurity concerns owing to the information being transmitted over other, which makes it hard to detect. In this section, we provide an elaborate discussion as to what measures the organizations can take in the face of cybersecurity threat brought by the wide-spreading use of laptops.

The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics. Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market. Very few laptop thieves are actually interested in the information that is contained in the laptop. Most laptops contain personal and corporate information that could be sensitive.

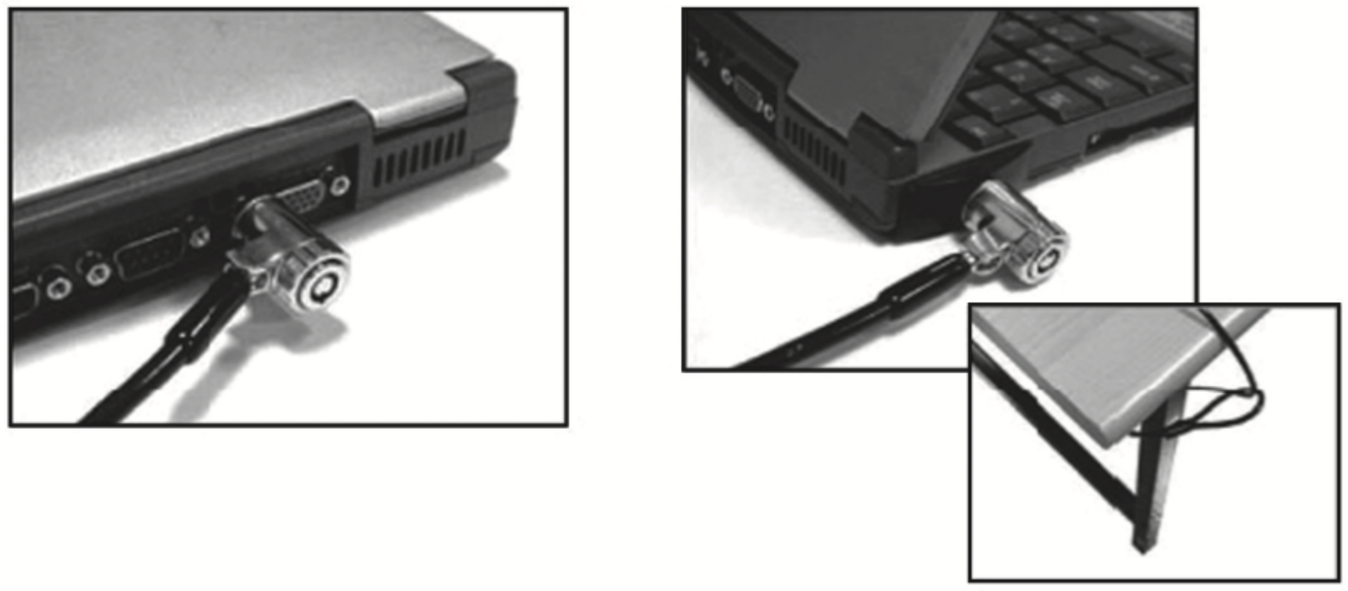
Such information can be misused if found by a malicious user. Senior executives commonly believe that the information stored on their laptops is only useful for them and would not be of any interest to others. Owing to this belief, most senior executives in an organization feel that it is unnecessary to protect the information stored on these laptops. However, this is not true. The following section provides some countermeasures against the theft of laptops, thereby avoiding cybersecurity exposures.

3.12.1 Physical Security Countermeasures

Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel. However, this mobility is putting organizations at risk of having a data breach if a laptop containing sensitive information is lost or stolen. Hence, physical security countermeasures are becoming very vital to protect the information on the employees' laptops and to reduce the likelihood that employees will lose laptops. Management also has to take care of creating awareness among the employees about physical security countermeasures by continuous training and stringent monitoring of organizational policies and procedures about these physical security countermeasures.[21]

1. **Cables and hardwired locks:** The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops. Kensington cables are one of the most popular brands in laptop security cables [see Figs. 3.14 (a) and (b)]. These cables are made of aircraft-grade steel and Kevlar brand fiber, thus making these cables 40% stronger than any other conventional security cables. One end of the security cable is fit into the universal security slot of the laptop and the other end is locked around any fixed furniture or item, thus making a loop. These cables come with a variety of options such as number locks, key locks and alarms. However, the downside of the security cables lies in the fact that one can easily remove detachable bays such as CD-ROM bay, Personal Computer Memory Card Industry Association (PCMCIA) cards (see Ref. #10, Additional Useful Web References, Further Reading), hard disk drive (HDD) bay and other removable devices from the laptop as the cable only secures the laptop from being stolen. The other disadvantage of security cables is when the laptop is locked to an object that is not fixed or is weak enough for anyone to break it. In certain cases of laptop thefts, the thief dismantled or smashed the fixed item to which the laptop was attached to.
2. **Laptop safes:** Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops. The advantage of safes over security cables is that they protect the whole laptop and its devices such as CD-ROM bays, PCMCIA cards and HDD bays which can be easily removed in the case of laptops protected by security cables.
3. **Motion sensors and alarms:** Even though alarms and motion sensors are annoying owing to their false alarms and loud sound level, these devices are very efficient in securing laptops. Once these devices are activated, they can be used to track missing laptops in crowded places. Also owing to

(a)



(b)

Figure 3.14 | (a) Kensington cable locks for laptops. (b) Closer view of cable locks for laptops. *Source:* Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

their loud nature, they help in deterring thieves. Modern alarm systems for laptops are designed wherein the alarm device attached to the laptop transmits radio signals to a certain range around the laptop. The owner of the laptop has a key ring device that communicates with the laptop alarm device. The alarm is triggered when the distance between the laptop alarm device and the key ring device crosses the specified range. Also available are security PCMCIA cards that act as a motion detector, an alarm system, and also have the capability to lockdown the laptop if the laptop is moved out of the designated range. They also secure the passwords and encryption keys and prevent access to the OS. These cards have batteries that keep them powered on even when the system is shutdown. Figure 3.15 shows some laptop alarm systems with sensors.

4. **Warning labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft. These labels have an identification number that is stored in a universal database for verification, which in turn makes the resale of stolen laptops a difficult process. Such lables are highly recommended for the laptops issued to top executives and/or key employees of the organizations.
5. **Other measures for protecting laptops are as follows:**
   - Engraving the laptop with personal details;
   - keeping the laptop close to oneself wherever possible;
   - carrying the laptop in a different and unobvious bag making it unobvious to potential thieves;

Figure 3.15 Laptop alarm systems with sensors.
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

- creating the awareness among the employees to understand the responsibility of carrying a laptop and also about the sensitivity of the information contained in the laptop;
- making a copy of the purchase receipt, laptop serial number and the description of the laptop;
- installing encryption software to protect information stored on the laptop;
- using personal firewall software to block unwanted access and intrusion;
- updating the antivirus software regularly;
- tight office security using security guards and securing the laptop by locking it down in lockers when not in use;
- never leaving the laptop unattended in public places such as the car, parking lot, conventions, conferences and the airport until it is fitted with an antitheft device;
- disabling IR ports and wireless cards and removing PCMCIA cards when not in use.

So far, we have discussed protection of corporate laptops in terms of physical access control. However, information systems security also contains logical access controls. This is because, information, be it corporate or private, needs high security as it is the most important asset of an organization or an individual. A few logical access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/open access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums/unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls/intrusion detection system (IDSs).
10. Encrypting critical file systems.
11. Other countermeasures:
    - Choosing a secure OS that has been tested for quite some time and which has a high security incorporated into it.
    - Registering the laptop with the laptop manufacturer to track down the laptop in case of theft.
    - Disabling unnecessary user accounts and renaming the administrator account.
    - Disabling display of the last logged in username in the login dialog box.
    - Backing up data on a regular basis.

Summary

Everyday mobile workers take laptop computers and hand-held devices outside of their organizations' secure environment. Cell phones, PDAs, Smartphones, laptop computers and other devices make it convenient to access information anywhere. However, the potential for confidential information to be exploited on these devices and the ability to access corporate networks from outside the firewall, as well as the susceptibility of these devices to loss and theft, create cybersecurity risks that must be addressed in order to protect the privileged data. Therefore, in this chapter, we have discussed the nature of mobile hand-held devices and how they have the potential to create exposure to information systems security in the organizations. We have emphasized and reiterated the key point that the

widespread use of mobile devices as well as information explosion calls for a higher-level security in the mobile devices. In this chapter, we have discussed cybersecurity challenges in mobile and wireless computing scenario. The challenge here is that IT departments and security professionals need to handle this issue with due seriousness. Mobile devices such as PDAs and Smartphones have become a key tool for traveling employees to help enable their digital lives both in the office and on the road. As more employees, including executives, begin to carry such devices, the amount of sensitive and confidential information at risk increases. Although PDAs and Smartphones can greatly enhance employee productivity, they can also be easily lost or stolen. Without protection, sensitive data stored on mobile devices may be breached, potentially resulting in damages, including lost revenue, regulatory penalties and loss of brand reputation and goodwill of the business enterprise. We have seen the different kinds of attacks launched on the mobile/cell phones by criminals and also some tips to avoid being victims of such attacks. Thus, the key point is that as mobile technology becomes ubiquitous, mobile security becomes increasingly important. Within a decade, mobile devices (PDAs, cell phones, wristwatches, etc.) will function as wallets, electronic banks (E-Banks), business cards, proximity keys, as well as the personal information managers (PIMs) and communicators they are today.

Our final key point in this chapter is that protecting the data on a device is just as important as protecting the information flowing between the device and the servers it interacts with. Device security is often something that is left up to the end-user to implement and maintain. Although this is often driven by corporate policy, enterprises often look for ways to take this responsibility out of the hands of end-users and place it under the enforceable control of an administrator.

Review Questions

1. What are the "mobility types"? Quote day-to-day examples of your familiarity that relates to them.
2. Discuss how "perception" makes people least suspect cybersecurity threats through mobile computing hand-held devices. What measures do you recommend against this situation?
3. What kinds of attacks are possible on mobile/cell phones? Explain with examples.
4. Explain the countermeasures to be practiced for possible attacks on mobile/cell phones.
5. What kinds of cybersecurity measures an organization should have to take in case of portable storage devices? Prepare security guidelines which can be implemented in an organization.
6. Explain the various measures for protection of laptops through physical measures and logical access control measures. Prepare a laptop security checklist using the guidelines provided in this chapter. Apply it to the laptop owner in your educational institute. If you are employed, then find out your organization's laptop protection policy and related procedures.

References

[1] Quocirca Insight Report (2009), *Addressing a Growing Problem: An Explosion of IP Addresses*, visit: http://www.quocirca.com (31 March 2010).

[2] Research In Motion Inc., *Research in Motion Annual Report*, 2009, visit: http://www.rim.com/investors/pdf/RIM09AR_FINAL.pdf (21 March 2006).

[3] To know more about mobile computing and types of mobile computing, visit: http://en.wikipedia.org/wiki/Mobile_computing (28 March 2010).

[4] To know more on *Mobile Security – Problem in Hand, Solution in Mind*, visit: http://www.it-analysis.com/blogs/Quocirca/2009/4/mobile_security_problem_in_hand_so_.html (31 March 2010).

[5] Quocirca Insight Report (2005), *Mobile Devices and Users*, visit: http://www.quocirca.com (15 May 2010).

[6] To know more about "3G Mobile Networks – Security Concerns," visit: http://fanaticmedia.com/infosecurity/archive/April09/3G%20Mobile%20Networks.htm (10 April 2010).

[7] To learn about credit card transactions using mobile cell phone, visit: https://www.frontlineprocessing.com/news/wireless-credit-card-processing/ (15 May 2010).

[8] To know how to avoid credit and charge card fraud, visit: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm (24 February 2010).

[9] CLEW Technology (*Closed-Loop Environment for Wireless*) comes from Alacrity, an Australian company who specifically created to deliver on the promise of mobile Internet. Alacrity's patented CLEW technology provides instant interactivity with their clients for time critical information. For further details, visit: http://www.alacritytech.com.au (15 May 2010).

[10] To know more about Types of Credit Card Fraud, visit:
http://people.exeter.ac.uk/watupman/undergrad/owsylves/page3.html (22 May 2010).
http://en.wikipedia.org/wiki/Credit_card_fraud (22 May 2010).

[11] For a news item *Microsoft Paves over Media Player Flaws*, visit: http://news.com.com/2100-1023-940050.html (19 May 2003).

[12] To know how to protect a mobile phone from being stolen, visit: http://www.wikihow.com/Protect-a-Mobile-Phone-from-Being-Stolen (20 February 2010).

[13] To know more about Mobile Phone Virus Hoax, visit: http://www.hoax-slayer.com/mobile-phone-virus-hoax.html (22 May 2010).

[14] To know more about Help protect against mobile viruses, visit: http://www.microsoft.com/uk/protect/computer/viruses/mobile.mspx (22 May 2010).

[15] To know more about Vishing, visit: http://en.wikipedia.org/wiki/Vishing (20 February 2010).

[16] To know more about how to protect from Vishing attacks, visit: http://news.cnet.com/8301-1035_3-10244200-94.html (18 February 2009).

[17] To know more about pretexting, visit: http://en.wikipedia.org/wiki/Social_engineering_(security) (18 February 2009).

[18] To know more about sexting, visit: http://en.wikipedia.org/wiki/Sexting (18 February 2009).

[19] To know more about VoIP spam, visit: http://en.wikipedia.org/wiki/VoIP_spam (18 February 2009).

[20] To know more about US Businesses Losing Millions from Illegal Interception of cell phone calls, visit:
http://www.darkreading.com/insiderthreat/security/perimeter/showArticle.jhtml?articleID=223101287 (22 May 2010).
http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100302006258&newsLang=en (22 May 2010).

[21] To know more about Laptop Security, visit: http://www.securitydocs.com/pdf/3399.PDF (22 May 2010)

Further Reading

Additional Useful Web References

1. Alexander, Z. (1997) *Is RAS Safe?*, WindowsITPro magazine – http://www.windowsitpro.com/article/networking/optimizing-nt-ras.aspx (15 May 2010).

2. To see interesting information in the article *Protecting your Laptop Computer*, visit: http://itso.iu.edu/Protecting_Your_Laptop_Computer (15 May 2010).

3. For *Windows Media Player Control Registry Settings*, visit: http://msdn.microsoft.com/en-us/library/ms909920.aspx (15 May 2010).
4. To study the projects done by the *Security Research Group*, visit: http://research.microsoft.com/en-us/groups/security/ (15 May 2010).
5. For another similar news item titled *Real Networks Warns of Media Player Security Flaws*, visit: http://www.networkworld.com/news/2004/0206realnwarns.html (15 May 2010).
6. For a very informative article on secure operation of the RAS system, visit: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm/s/s4112.htm (15 May 2010).
7. For an interesting article titled *Butter-Fingered Mobile Device Users create IT Risk*, visit: http://www.networkworld.com/newsletters/wireless/2005/0214wireless2.html?fsrc=rss-wireless (15 May 2010).
8. For an eye opening article titled *Corporate Laptop Users put Businesses at Risk*, visit: http://www.pcw.co.uk/computing/news/2071216/corporate-laptop-users-put-businesses-risk (15 May 2010).
9. For radio frequency identification (RFID), visit: http://www.rfidjournal.com/faq (15 May 2010).
10. To read about PCMCIA cards, visit: http://support.3com.com/infodeli/inotes/techtran/4bba_5ea.htm (15 May 2010).
11. Jackson, W. (2005) *GCN Staff, Survey: Digital Gadgets take a Back Seat – and Stay there*, available at: http://gcn.com/articles/2005/01/24/survey-digital-gadgets-take-a-back-seatand-stay-there.aspx (15 May 2010).
12. Middleton, J. (2001) Lost Mobile Devices drive Security Fears, Web article from the VNU Network VNU Business Publications, available at: http://www.vnunet.com/articles/print/2115935 (15 May 2010).
13. For further technical details of the AES algorithm, visit Rijndael home page at: http://csrc.nist.gov/archive/aes/index.html (15 May 2010).
14. Shriraghavan, S., Sundaragopalan, S., Yang, F., and Jun, J. (2003) *Security in Mobile Computing – Focus on Wireless Security*, November 25, available at: http://www.cc.gatech.edu/classes/AY2004/cs4235a_fall/presentations/NetSecPres. pdf (15 May 2010).
15. To learn about the RIM November 2006 report, visit: http://www.computing.co.uk/itweek/news/2169730/55-mobile-phones-left-london (15 May 2010). http://www.theregister.co.uk/2001/08/31/62_000_mobiles_lost/ (15 May 2010).
16. Strang, T. (2003) *Trends in Mobile Computing – From Mobile Phone to Context-Aware Service Platform*, German Aerospace Center (DLR), Oberpfaffenhofen, Germany, available at http://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/bt38/Bln_Release.pdf (15 May 2010).
17. For Windows advice on protecting sensitive information residing on mobile devices, *Windows Mobile-based Devices and Security: Protecting Sensitive Business Information*, available at: http://download.microsoft.com/download/4/7/c/47c9d8ec-94d4-472b-887d-4a9ccf194160/6.%20WM_Security_Final_print.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' (15 May 2010).
18. To know scams that target you or your small business, visit: http://www.scamwatch.gov.au/content/index.phtml/itemId/693900 (20 February 2010).
19. To learn about mobile device security, visit: http://www.securelist.com/en/analysis?pubid=170773606 (15 May 2010).
20. To know about PCI-DSS Standard, visit: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (18 July 2010).
21. For PCI compliance guide, visit: http://www.pcicomplianceguide.org/ (18 July 2010).

Books

1. Mallick, M. (2003) *Mobile and Wireless Design Essentials*, Wiley DreamTech (India) Ltd., New Delhi, India.
2. Nanvati, S., Thieme, M., and Nanavati, R. (2002) *Biometrics*, 1st edn, Wiley DreamTech (India) Ltd., New Delhi, India.
3. Unhelkar, B. (2006) *Handbook of Research in Mobile Business: Technical, Methodological, and Social Perspectives*, IDEA Group, Hershey, PA, USA.

4. Siegemund, F. and Flörkemeier, C. (2003) *Interaction in Pervasive Computing Settings using Bluetooth-enabled Active Tags and Passive RFID Technology together with Mobile Phones*, Institute for Pervasive Computing, Department of Computer Science, ETH Zurich, Switzerland.

Articles and Research Papers

1. Godbole, N. (2003) *Mobile Computing: Security Issues in Hand-Held Devices*, Paper presented at NASONES 2003 National Seminar on Management and Business, 13–16 February 2006, Sydney, Australia. The paper is available in the following link: http://www.au-kbc.org/bpmain1/Security/EMO_SecurityWhitepaper.pdf#search='RAS%20Server%20Security%20for%20Mobile%20Devices' for Ericsson Mobile Organizer (EMO) Security Whitepaper (15 May 2010).
2. Sadlier, G. (October 2003), Mobile Computing Security, INS White Paper.
3. Godbole, N. and Unhelkar, B. (2006) *Security Issues in Mobile Computing*, Proceedings of the 2nd International Conference on Information Management and Business, February 13–16, 2006, Sydney, Australia.

The appendices that serve as extended material for the topic addressed in this chapter are: A, B, D, E, L. These are provided in the companion CD.