**Telecommunications and Network Security (Cell Phones/Wireless)**

**Technology – Standards – Attacks - Recommendations….etc**

Written By

**Lance West**

**Table of Content**

**Telecommunications and Network Security – Cell Phones/Wireless……………………...3**

CIA – Confidentiality/ Availability/ Integrity for cell phones

 Two main cell phone networks are used in the USA

 1) Code Division Multiple Access (CDMA) **– See CDMA PowerPoint**

 2) Global System for Mobile Communications (GSM) **– See GSM PowerPoint**

**Wireless Technology Communication Methods…………………………………………….6**

* + Frequency Hopping Spread Spectrum - p6
	+ Direct Sequence Spread Spectrum - p7
	+ The different types of 802 Technologies - p9
	+ Wireless Standards - p10
	+ Bluetooth Wireless - p12

**Open Systems Interconnection (OSI)……………………………………………………….12**

**Tying the Layers Together…………………………………………………………………..14**

**Security Concerns for Mobile Networks/Wireless Technology…………………………...16**

* + Vulnerabilities c - p17
	+ Mal-Ware & Viruses - p19
	+ Fake-Installer, the leader in attacks on Android phones - p20
	+ [First Ever Windows Malware that can hack your Android Mobile](http://thehackernews.com/2014/01/first-ever-windows-malware-that-can_23.html) – p21

**How to tell if your phone is infected………………………………………………………...22**

**Strategies for Addressing Mobile Device Risk……………………………………………..22**

* + Step 1: Upgrading your phone – p22
	+ Step 2: Down loading Apps – p23
	+ Step 3: Developing Your Own Apps – p23
	+ Step 4: Cell Phone Audits - p24

**Conclusion……………………………………………………………………………………26**

**References…………………………………………………………………………………….27**

**Telecommunications and Network Security** – Cell Phones/Wireless:

Fundamental security for any system begins with the basics “confidentiality, integrity, availability.” This is a simple concept that will help you protect critical assets like your personal data as you use your cell phone, because it is now evident that companies for the most part are not protecting you from identity theft. Their mission is to make money, and collecting your personal data is just a means to an end for most businesses. So here are a few things to keep in mind when you use your cell phone in public places.

Confidentiality – don’t use open Wi-Fi systems to transmit data, switch your phone to use its 3G or 4G network. This will give you an extra level of secrecy and added level of encryption to prevent unauthorized disclosure. Attackers can thwart confidentiality mechanisms by network monitoring, shoulder surfing, stealing password files, breaking encryption schemes, and social engineering.

Basic Personal Cell Phone Protection:

1. Create a stronger password on your phone beyond the four digit ones that come as a default, something with uppercase and lowercase letters, numbers, and symbols.
2. Turn off tracking use it only when you need it, because people, stores and even others around you can hack that functionality to their advantage and know your movements.
3. Use only trusted networks when transmitting person data. Example: Your Home Network.

Train yourself and your business people to use proper data protection procedures, on and off the job. Since these days a lot of people are using their personal cell phones to access their business accounts through all types of public networks.

Availability - reliable and timely access to data and resources is needed but should only be authorized individuals, and a well designed 3G and 4G networks is a lot better than a public Wi-Fi network. Every company should have guideline on how to access the business network from outside of the company. Since any App you download can lead to a potential risk have vetted IT policies and procedures in place that outline what you can and cannot download.

Integrity – you must establish protection protocols for your network to ensure the integrity of the data it holds. This will also ensure accuracy and reliability of the information and help guard against any unauthorized use or modification of critical systems or the data it stores. Cell phone development is relatively new leaving to the door open for a hacker to take advantage of weak standards and protocols.

**Two main cell phone networks are used in the USA**

The two most dominant types of digital cellular networks in the U.S. are known as Code Division Multiple Access (CDMA) and Global System for Mobile Communications (GSM) networks. There are other common cellular networks within the U.S., including Time Division Multiple Access (TDMA), Frequency division multiple access (FDMA), and Integrated Digital Enhanced Network (iDEN). The iDEN network uses a proprietary protocol designed by Motorola, while the others follow standardized open protocols. A digital version of the original analog standard for cellular telephone phone service, called Digital Advanced Mobile Phone Service (D-AMPS), also exists, but is slowly being replaced. I am limiting the research to the two most common CDMA and GSM and the different technologies used in transmitting information.

* **Frequency division multiple access (FDMA)**

FDMA puts each call on a separate frequency.

* **Time division multiple access (TDMA)**

TDMA assigns each call a certain portion of time on a designated frequency.

* **Code division multiple access (CDMA)**

CDMA gives a unique code to each call and spreads it over the available frequencies

**FDMA** separates the spectrum into distinct voice channels by splitting it into uniform chunks of bandwidth. To better understand FDMA, think of radio stations: Each station sends its signal at a different frequency within the available band. FDMA is used mainly for analog transmission and is not considered to be an efficient method for digital transmission.

**TDMA** is the access method used by the Electronics Industry Alliance and the Telecommunications Industry Association for Interim Standard 54 (IS-54) and Interim Standard 136 (IS-136). Using TDMA, a narrow band that is 30 kHz wide and 6.7 milliseconds long is split time-wise into three time slots. TDMA refers to a digital link technology whereby multiple phones share a single-carrier radio-frequency channel by taking turns—using the channel exclusively for an allocated time slice, then releasing it and waiting briefly while other phones use it. The 3G evolutionary step for GSM is known as Universal Mobile Telecommunications System (UMTS) and involves enhancing GSM networks with a Wide-band CDMA (W-CDMA) air interface.

The **CDMA** refers to a technology designed by Qualcomm in the U.S., which employs spread spectrum communications for the radio link. Rather than sharing a channel, as many other network air interfaces do. **CDMA** takes an entirely different approach from TDMA. CDMA, after digitizing data, spreads it out over the entire available bandwidth. Multiple calls are overlaid on each other on the channel, with each assigned a unique sequence code. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over a number of the discrete frequencies available for use at any time in the specified range. Verizon, Sprint and most other U.S. carriers use CDMA, which means no SIM card **– See “CDMA Network Structure and Components – Powerpoint.”**

The **GSM** (Global System for Mobile communications) network is, at the start of the 21st century, the most commonly used mobile telephony standard in Europe. It is a so-called "second generation" (2G) standard because, unlike the first generation of portable telephones, communications occur in an entirely digital mode. Called "Group Special Mobile" when first standardized in 1982, it became an international standard called "Global System for Mobile communications" in 1991.

In Europe, the GSM standard uses the 900 MHz and 1800 MHz frequency bands. In the United States, however, the frequency band used is the 1900 MHz band. For this reason, portable telephones that are able to operate in both Europe and the United States are called **tri-band** while those that operate only in Europe are called **bi-band**. The GSM is a cellular system first designed in Europe, primarily by Ericsson and Nokia. Cingular and T-Mobile operate nationwide networks in the U.S. GSM uses a TDMA air interface. The GSM standard allows a maximum throughput of 9.6 kbps, which allows transmission of voice and low-volume digital data, for example text messages (**SMS**, for Short Message Service) or multimedia messages (**MMS**, for Multimedia Message Service) - **See ”GSM Network Structure - PowerPoint**.”

**Wireless technology Communication Methods**

Wireless technology can use a number of different methods to communicate to devices across a network. Frequency Hopping Spread Spectrum (FHSS) takes the total amount of bandwidth (spectrum) and splits it into smaller sub-channels. The sender and receiver work at one of these sub-channels for a specific amount of time and then move to another sub-channel. The sender puts the first piece of data on one frequency, the second on a different frequency, and so on. The FHSS algorithm determines the individual frequencies that will be used and in what order, and this is referred to as the sender and receiver’s hop sequence.

Direct Sequence Spread Spectrum this spread spectrum (DSSS) takes a different approach by applying sub-bits to a message. The sub-bits are used by the sending system to generate a different format of the data before the data are transmitted. The receiving end uses these sub-bits to reassemble the signal into the original data format. The sub-bits are called chips, and the sequence of how the sub-bits are applied is referred to as the chipping code. The sub-bits provide error-recovery instructions, just as parity does in RAID technologies. If a signal is corrupted using FHSS, it must be re-sent; but by using DSSS, even if the message is somewhat distorted, the signal can still be regenerated because it can be rebuilt from the chipping code bits. The use of this code allows for prevention of interference, allows for tracking of multiple transmissions, and provides a level of error correction.

The SSID is required when a wireless device wants to authenticate to an AP. For the device to prove it should be allowed to communicate with the wired network it must first provide a valid SSID value. The SSID should not be seen as a reliable security mechanism because many APs broadcast their SSIDs, which can be easily sniffed and used by attackers. The wireless device can authenticate to the AP in two main ways: open system authentication (OSA) and shared key authentication (SKA). OSA does not require the wireless device to prove to the AP it has a specific cryptographic key to allow for authentication purposes. In many cases, the wireless device needs to provide only the correct.

One a related subject a newer wireless standards is on the horizon called Near Field Communications (NFC), a short-range point-to-point wireless communication technology, has been issued, and devices are starting to appear with this capability that allow them to function as a connectionless identity card for credit and debit transactions and other purposes, such as interacting with NFC-enabled advertisements. This is a newer type of wireless system, but the differences in payment instruments and payment protocols used by various service providers and concerns about security have so far limited widespread adoption of any one scheme.

WLAN Security - The first WLAN standard, IEEE 802.11, had a tremendous number of security flaws. These were found within the core standard itself, as well as in different implementations of this standard. The three core deficiencies with WEP are the use of static encryption keys, the ineffective use of initialization vectors, and the lack of packet integrity assurance. This is like having everyone in your company use the exact same password. Not a good idea! So that is the first issue—static WEP encryption keys on all devices. In most WEP implementations, the same IV values are used over and over again in this process, and since the same symmetric key (or shared secret) is generally used, there is no way to provide effective randomness in the key stream that is generated by the algorithm. The appearance of patterns allows attackers to reverse-engineer the process to uncover the original encryption key, which can then be used to decrypt future encrypted traffic. So there are many weaknesses within wireless technology. A skilled attacker can even change data within the wireless packets by flipping specific bits and altering the Integrity Check Value (ICV) making the receiving end oblivious to these changes. The ICV works like a CRC function; the sender calculates an ICV and inserts it into a frame’s header. The receiver calculates his own ICV and compares it with the ICV sent with the frame. TKIP addresses the deficiencies of WEP pertaining to static WEP keys and inadequate use of IV values. Two hacking tools, Air-Snort and WEP-Crack, can be used to easily crack WEP’s encryption by taking advantage of these weaknesses and the ineffective use of the key scheduling algorithm within the WEP protocol

**The different types of 802 Technologies**:

802.1X standard is a port-based network access control that ensures a user cannot make a full network connection until he is properly authenticated. This means a user cannot access network resources and no traffic is allowed to pass, other than authentication traffic, from the wireless device to the network until the user is properly authenticated. An analogy is having a chain on your front door that enables you to open the door slightly to identify a person who knocks before you allow him to enter your house. The 802.1X technology actually provides an authentication framework and a method of dynamically distributing encryption keys. The three main entities in this framework are the supplicant (wireless device), the authenticator (AP), and the authentication server (usually a RADIUS server).

**The disadvantage** of the original 802.11 standard is that mutual authentication is not possible. When using WEP alone, the wireless device can authenticate to the AP, but the authentication server is not required to authenticate to the wireless device. This means a rogue AP can be set up to capture users’ credentials and traffic without the users being aware of this type of attack. 802.11i deals with this issue by using EAP. EAP allows for mutual authentication to take place between the authentication server and wireless device, and provides flexibility in that users can be authenticated by using passwords, tokens, one-time passwords, certificates, smart cards, or Kerberos. This allows wireless users to be authenticated using the current infrastructure’s existing authentication technology. The wireless device and authentication server that are 802.11i-compliant have different authentication modules that plug into 802.1X to allow for these different options. So, 802.1X provides the framework that allows for the different EAP modules to be added by a network administrator. The two entities (supplicant and authenticator) agree upon one of these authentication methods (EAP modules) during their initial handshaking process.

**A large concern** with current WLANs using just WEP is that if individual wireless devices are stolen, they can easily be authenticated to the wired network. 802.11i has added steps to require the user to authenticate to the network instead of just requiring the wireless device to authenticate. TKIP was created as a quick fix to WEP’s overwhelming problems. It does not provide an overhaul for the wireless standard itself because WEP and TKIP are still based on the RC4 algorithm, which is not the best fit for this type of technology. The use of AES is closer to an actual overhaul, but it is not backward-compatible with the original 802.11 implementations. In addition, we should understand that using all of these new components and mixing them with the current 802.11 components will add more complexity and steps to the process.

**Wireless Standards:** Standards are developed so that many different vendors can create various products that will work together seamlessly. Standards are usually developed on a consensus basis among the different vendors in a specific industry. The Institute of Electrical and Electronics Engineers (IEEE) develops standards for a wide range of technologies—wireless being one of them. Below is some of the current wireless security standards build on IEEE guidelines.

|  |
| --- |
| **Characteristics of Wireless Security Structures Currently in Use** |
|  | **802.1x Dynamic WEP** | **Wi-Fi Protected Access (WPA)** | **Wi-Fi Protected Access 2 (WPA2)** |
| Access Control | 802.1x | 802.1x or Pre-shared Key | 802.1x or Pre-shared Key |
| Authentication | EAP methods | EAP methods or Pre-Shared Key | EAP Methods or Pre-Shared Key |
| Encryption | WEP | TKIP (RC4) | CCMP (AES Counter Mode) |
| Integrity | None | Michael MIC | CCMP (AES CBC-MAC) |

**802.11b -802.11b** provides a transfer rate of up to 11 Mbps and works in the 2.4GHz frequency range. It uses DSSS and is backward-compatible with 802.11 implementations.

**802.11a -** This standard uses a different method of modulating data onto the necessary radio carrier signals. Whereas 802.11b uses DSSS, 802.11a uses OFDM and works in the 5GHz frequency band. OFDM is a modulation scheme that splits a signal over several narrowband channels. The channels are then modulated and sent over specific frequencies. Because the data are divided across these different channels, any interference from the environment will degrade only a small portion of the signal. This allows for greater throughput. Like FHSS and DSSS, OFDM is a physical layer specification. It can be used to transmit high definition digital audio and video broadcasting as well as WLAN traffic

**802.11e -** This standard has provided QoS and support of multimedia traffic in wireless transmissions. Multimedia and other types of time-sensitive applications have a lower tolerance for delays in data transmission.

**802.11f -** When a user moves around in a WLAN, her wireless device often needs to communicate with different APs. An AP can cover only a certain distance, and as the user moves out of the range of the first AP, another AP needs to pick up and maintain her signal to ensure she does not lose network connectivity.

**802.11g – j, n, and I6 -** We are never happy with what we have; we always need more functions, more room, and more speed. The 802.11g standard provides for higher data transfer rates—up to 54 Mbps. This is basically a speed extension for 802.11b products. If a product meets the specifications of 802.11b, its data transfer rates are up to 11 Mbps, and if a product is based on 802.11g, that new product can be backward-compatible with older equipment but work at a much higher transfer rate.

**Bluetooth Wireless:** The Bluetooth wireless technology is actually based upon a portion of the 802.15 standard. It has a 1- to 3-Mbps transfer rate and works in a range of approximately ten meters. If you have a cell phone and a PDA that are both Bluetooth-enabled and both have calendar functionality, you could have them update each other without any need to connect them physically. A real security risk exist when transferring unprotected data via Bluetooth in a public area, because any device within a certain range can capture this type of data transfer. One attack type that Bluetooth is vulnerable to is referred to as Bluejacking. In this attack, someone sends an unsolicited message to a device that is Bluetooth-enabled. Bluejackers looks for a receiving device (phone, PDA, tablet PC, laptop). Bluejackers is a simple technique because instead of creating a legitimate name in the other users address book, the bluejacker's message takes the place of the name. The prank essentially erases the "from" part of the equation, allowing a user to send any sort of comment he wishes without identifying him or herself.

**Open Systems Interconnection (OSI)**

The OSI is made up of seven layers, and each is used by wireless devices in different ways. **Application Layer:** The application layer, layer 7, works closest to the user and provides file transmissions, message exchanges, terminal sessions, and much more. This layer does not include the actual applications, but rather the protocols that support the applications. When an application needs to send data over the network, it passes instructions and the data to the protocols that support it at the application layer. This layer processes and properly formats the data and passes the same down to the next layer within the OSI model.

**Presentation Layer:** The presentation layer, layer 6, receives information from the application layer protocol and puts it in a format all computers following the OSI model can understand. This layer provides a common means of representing data in a structure that can be properly processed by the end system. This layer also handles data compression and encryption issues. If a program requests a certain file to be compressed and encrypted before being transferred over the network, the presentation layer provides the necessary information for the destination computer. It provides information on how the file was encrypted and/or compressed so that the receiving system knows what software and processes are necessary to decrypt and decompress the file

**Session Layer:** When two applications need to communicate or transfer data between themselves, a connection may need to be set up between them. The session layer is responsible for establishing a connection between the two applications, maintaining it during the transfer of data, and controlling the release of this connection. Session layer protocols are the least used protocols in a network environment; thus, many of them should be disabled on systems to decrease the chance of them getting exploited. RPC and similar distributed computing calls usually only need to take place within a network; thus, firewalls should be configured so this type of traffic is not allowed into or out of a network.

**Transport Layer:** How do I know if I lose a piece of the message? Response: The transport layer will fix it for you. When two computers are going to communicate through a connection-oriented protocol, they will first agree on how much information each computer will send at a time, how to verify the integrity of the data once received, and how to determine whether a packet was lost along the way.

**Network Layer:** The main responsibilities of the network layer, layer 3, are to insert information into the packet’s header so it can be properly addressed and routed, and then to actually route the packets to their proper destination. In a network, many routes can lead to one destination.

**Data Link Layer:** The data link layer is divided into two functional sub-layers: the Logical Link Control (LLC) and the Media Access Control (MAC). The LLC, defined in the IEEE 802.2 specification, communicates with the protocol immediately above it, the network layer. The MAC will have the appropriately loaded protocols to interface with the protocol requirements of the physical layer.

**Physical Layer:** The physical layer, layer 1, converts bits into voltage for transmission. Signals and voltage schemes have different meanings for different LAN and WAN technologies.

Tying the Layers Together

Tying the Layers Together so pick-up all of these protocols from the floor and put them into a stack—a network stack. The OSI model is used as a framework for many network-based products and is used by many types of vendors. Various types of devices and protocols work at different parts of this seven-layer model. The main reason that a Cisco switch, Microsoft web server, a Barracuda firewall, and a Belkin wireless access point can all communicate properly on one network is because they all work within the OSI model.

Graphics OSI model shows what level of the OSI each type of device works within.



The IP address acts as the doorway to a computer, and the port acts as the doorway to the actual protocol or service - below is a diagram of how each port functions within the network structure. To communicate properly, the packet needs to know these doors. This diagram shows how packets communicate with applications and services through ports. Example Email defaults to Port 25, Http to port 80, and Https port defaults to 443.



The table below points out the differences between TCP and UDP and can also be seen in the message formats. Because TCP offers more services than UDP, it must contain much more information within its packet header format, as shown in the below table.

|  |  |
| --- | --- |
| **TCP Format** | **UDP Format** |
|

|  |  |
| --- | --- |
| Source Port | Destination Port |
| Sequence Number |
| Acknowledgment Number |
| offset | Reserved | Flags | Windows |
| Checksum | Urgent Pointer |
| Options | Padding |
| Data |

 |

|  |  |
| --- | --- |
| Source Port | Destination Port |
| Length | Checksum |
| Data |

 |

**Security Concerns for Mobile Networks/Wireless Technology**

Security threats and vulnerabilities mobile handheld devices include the following items, which are discussed in more detail below:

* Loss, theft, or disposal
* ­Unauthorized access
* ­ Malware
* ­ Spam
* ­ Electronic eavesdropping
* ­ Electronic tracking
* ­ Cloning
* ­ Server resident data.
* Application Development

Everyone should know someone at sometime will lose their phone which will open up the person/company to unauthorized access. Moreover, if the phone is not password protected with a strong password can even open you up to identity theft to various phone scans. Most security concerns listed above are a no brainer and should be addressed with policies and procedures to protect the data within. I will focus on the more misunderstood threats like malware, and viruses.

**Vulnerabilities** Is a lack of a countermeasure or a weakness in a countermeasure that is in place. It can be software, hardware, procedural, or human weakness that can be exploited. Vulnerability may be a service running on a server, unpatched applications or operating systems, an unrestricted wireless access point, an open port on a firewall, lax physical security that allows anyone to enter a server room, or unenforced password management on servers and workstations.

**This table presents some known vulnerabilities and associated threats that need to be understood when dealing with mobile devices**.

|  |
| --- |
| **Mobile Device Vulnerabilities, Threats and Risks** |
| **Vulnerability** | **Threat** | **Risk** |
| Information travels across wireless networks, which are often less secure than wired networks | Malicious outsiders can do harm to the enterprise | Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation, legal action |
| Mobility provides users with the opportunity to leave enterprise boundaries and thereby eliminates many security controls. | Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network. | Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data. |
| Bluetooth technology is very convenient for many users to have hands-free conversation; however it is often left on and then is discoverable. | Hackers can discover the device and launch and attack | Device corruption, lost data, call interception, possible exposure of sensitive information. |
| Unencrypted information is stored on the device | In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable. | Exposure of sensitive data, resulting in damage to the enterprise, customers or employees. |
| Lost data may affect employee productivity. | Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up. | Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices and data that are not backed up. |
| The device has no authentication requirements applied. | In the event that the device is lost or stolen, outsiders can access the device and all of its data. | Data exposure, resulting in damage to the enterprise and liability and regulation issues. |
| The enterprise is not managing the device. | If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with e-mail or store sensitive documents. | Data leakage, malware propagation, unknown data loss in the case of device loss or theft. |
| The device allows for installation of unsigned their party applications. | Applications may carry malware that propagates Trojans or viruses; the applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network. | Malware propagation, data leakage, intrusion on enterprise network. |

Ten years ago it seemed possible to understand and secure a network and everything that resided within it. As technology grew in importance in every aspect of our lives over the years, however, almost every component that made up a traditional network grew in complexity. We still need to know the basics (routers, firewalls, TCP/IP protocols, cabling, switching technologies, etc.), but now we also need to understand data loss prevention, web and e-mail security, mobile technologies, antimalware products, virtualization, cloud computing, endpoint security solutions, radio-frequency identification (RFID), virtual private network protocols, social networking threats, wireless technologies, continuous monitoring capabilities, and more. A network used to be a construct with boundaries, but today most environments do not have clear-cut boundaries because most communication gadgets are some type of computer (smart phones, tablet PC, medical devices and appliances)

**Mal-Ware & Viruses**

One of the first viruses to hit a cell phone was in 2004 “EPOC.cabir” hit the Nokia Series 60 phone that uses the Symbian OS, Dubbed EPOC.cabir. The virus transmits its code via a Symbian OS distribution file disguised as a security manager utility. Once installed, which it had to be invited to install. It appeared as a message each time the phone turned on. Since it first came out in 2004 it has morphed into at least 15 varieties, and affected cell phones in over 14 countries. There is no payload, apart from the vastly shortened battery life caused by the virus constantly scanning for Bluetooth-enabled devices once you turn on your phone.

**Toll Fraud Malware**: Android Phones now encompasses a large share of the cell phone market, which is why major hackers are writing a lot of malware apps to attack them. The most prevalent form of Android malware scrapes small amounts of money from smartphone owners by making secret charges to their phone bills. This type of malware is called “Toll Fraud,” and it has the potential to fool plenty of people who don’t pay close attention to their phone bills every month. But how does toll fraud work if the carriers control our bills? The process is actually not that complex. First, it helps to understand a legitimate transaction involving text messages. Say, for example, a person wants to send a text message to a service to buy a new ringtone. When this happens, the cellular network forwards the text message to a middleman service, which handles the transaction between the wireless provider and the ringtone provider. The ringtone provider then shoots a message to the cellphone owner asking for confirmation of the order. When the customer confirms the order, he receives the ringtone, his cellphone bill is charged, and the carrier takes a cut and gives the rest of the money to the ringtone provider and the middleman service.

How “Toll Fraud” SMS messages work (**Graphic Below**) A person downloads a malicious app. The app invisibly sends a text message to a service that uses a middleman service that has a relationship with the malware author. A confirmation message is sent back to the malware, which blocks it from being seen by the customer and confirms the charge. The charge goes to the user’s bill, and the carrier takes its cut and gives the rest of the money to the service and the middleman, and thus the malware author gets his/her due.



**Fake-Installer - the leader in attacks on Android phones**

The Fake-Installer family is one of the most prevalent malware apps now on the networks. More than 60 percent of Android samples processed by McAfee are Fake-Installers. The deception starts when users search for a popular application and access a fake official site or fake market via search engines or social networks. Applications appear to be legitimate, including screenshots, descriptions, user reviews, videos, etc. Victims fall into the trap of downloading and installing the malware. Now SMS Premium Rate Numbers for previous versions of Fake-Installer were created only for Eastern European users, but malware developers have expanded their fraud to other countries–adding instructions into the code to get the Mobile Country Code and Mobile Network Code of the device. Based on that information, Android/Fake-Installer selects the premium-rate numbers and the text for SMS messages.

[**First Ever Windows Malware that can hack your Android Mobile**](http://thehackernews.com/2014/01/first-ever-windows-malware-that-can_23.html)

Around January of this year the first windows based Malware app that attacks Android phones, it showed up in South Korea in January, but is now gaining ground in the US. If your system is running a windows operating system, then it’s a bad news for you. It’s a malware program that tries to install mobile banking malware on Android devices while syncing. The Windows Trojan then parses this configuration file and downloads a malicious APK (an Android application) from the following location on the infected device.

**%Windir%\CrainingApkConfig\AV-cdk.apk**

In the next step, the trojan downloads all the necessary tools including Android Debug Bridge and the moment you connect an android device having USB debugging Mode enabled, it initiates the installation process and repeats it until it ensure that the connected device has been infected and install an app that will appear as a fake Google App Store image (**to the right**) on your phone. When it first showed up it would look for certain Korean online banking applications on the compromised device.

**How to tell if you phone is infected**

On a PC the signs are pretty obvious. Your computer slows to a screeching halt and your browser re-directs you to random websites. Users of mobile devices usually don't discover something's wrong until they look at their phone bills and don't recognize the numbers of text message recipients. Premium rate SMS Trojans are the most common type of mobile malware. This malware disguises itself in a legit-looking app, and secretly sends SMS short codes that bill the caller. In addition, nor will an average user really be able to tell by checking apps permissions. Android developers can choose from dozens of permissions, and as it's often impossible to guess which are legitimate and which are warning signs.

**Strategies for Addressing Mobile Device Risk**

Mobile devices offer enterprises the ability to keep their employees connected at all times. These devices afford people the ability to conduct business anywhere—whether they are at home, in the office, or traveling between destinations, but there is a few simple steps you can take to start.

**Step 1**: **Upgrading your phone**: For a simple yet vivid example of the device risks introduced by an employee-owned phone, just consider the likely scenario of an employee upgrading from an iPhone 4 to an 5s. "There will almost certainly be corporate information on the old phone, and the person who that phone is handed to is not trusted. A company should invest in a “Mobile Device Management (MDM)” platform that can control which devices can access specific applications on your network. An MDM solution can also carry out activities such as:

* device provisioning and configuration
* software distribution
* encryption and password management
* remote wipe and lock

**Step 2: Down loading Apps:** Reduce app download risks through policy and training. When it comes to risks introduced by downloaded apps, it's important to understand the potential for damage. Part of the problem is that mobile operating systems don't consistently enforce controls on what apps can and cannot do. In February last year, the Path social app for iOS was found to upload the user's address book to Path servers without asking permission – a practice that was subsequently found to be a common practice among many legitimate apps. Then it was also revealed that it granted an iOS app access to location data also inadvertently gives the app access to upload the user's photo library, should the app developer choose to exploit that privilege.

**Step 3: Developing Your Own Apps**? Scan the code for security vulnerabilities. Many organizations are now developing and launching their own mobile apps as a new channel for acquiring, communicating with, and doing business with customers. These apps often provide an authenticated mechanism for accessing privileged resources such as company databases. The risk here is that developers can inadvertently introduce security vulnerabilities when developing custom mobile apps for organizations – often because they are new to the platform, inexperienced with security issues, or unaware of the possible risks for example?

1. insecure data storage
2. weak server-side controls
3. insufficient transport layer protection
4. client-side injection
5. poor authorization and authentication
6. improper session handling
7. security decisions via untrusted inputs
8. side channel data leakage
9. broken cryptography
10. sensitive information disclosure

One big problem with Developers is they often try to roll their own crypto, or they make a mistake like hard coding the key into the app so that it can be used offline." To minimize these risks, companies that develop their own apps should engage a mobile security consultancy that was not involved in the development process – an "external pair of eyeballs," to check for security vulnerabilities.

**Step 4: Cell Phone Audits:** Conduct a Company-Wide Mobile Security Audit. No comprehensive mobile security strategy is complete without an audit that examines your mobile infrastructure, devices, and apps to identify current weaknesses and help guide your organization's next steps.

A typical security audit methodology might include:

* Evaluating your organization's overall mobile infrastructure;
* Conducting penetration tests on your mobile clients and the servers that control them;
* Assessing the security of your mobile devices and apps to determine their susceptibility to data breaches;
* Evaluating the gap between your current policies and procedures and known best practices.

Other Strategies to conceder

• Defining allowable device types (enterprise-issued only vs. allowing personal devices)

• Defining the nature of services accessible through the devices, taking into account the existing IT architecture

• Identifying the way people use the devices, considering the corporate culture as well as human factors and how the non-deterministic execution of processes through the use of mobile devices may lead to unpredictable risks

• Integrating all enterprise-issued devices into an asset management program

• Describing the type of authentication and encryption that must be present on the devices

• Outlining the tasks for which employees may use the devices and the types of applications that are allowed

• Clarifying how data should be securely stored and transmitted

|  |
| --- |
| **Strategies to Address Risks** |
| **Risk** | **Strategy** |
| A lost or stolen mobile device | Implement a central management console for device remote control, location tracking, data wipe-out, password/Pin change or strong user authentication. Ensure that mobile devices are encrypted so information is unusable in the event of loss or theft |
| Providing support to various devices | Turn to cross-platform centrally managed mobile device managers |
| Controlling data flow on multiple devices | Secure the systems that are accessed with authorization, encryption and privileges control. |
| Preventing data from being synchronized onto mobile devices in an unauthorized way | Monitor and restrict data transfers to handheld or removable storage devices and media from a single, centralized console. |
| Keeping up with the usage of the latest and greatest devices | Create Keen user awareness on information assets, risks and value to the enterprise |
| Promoting accountability, responsibility and transparency with device usage | Track the way devices are used, and provide regular feedback to management |
| Demonstrating regulatory compliance | Implement a central management console to manage all stages of asset management, from installation to retirement |

**Some special considerations for auditors**

• Policy—does a security policy exist for mobile devices? Does it include rules for appropriate physical and logical handling? The enterprise should have a policy addressing mobile device use and specifying the type of information and kind of devices and information services that may be accessible through the devices.

• Antivirus updates—Auditors should verify that the enterprise updates the mobile device antivirus software to prevent perpetuation of malware.

• Encryption—Auditors should verify that any data labeled as sensitive are properly secured while in transit or at rest.

• Secure transmission—Auditors should determine whether mobile device users are connecting to the enterprise network via a secure connection. VPN, IP security (IPsec) or Secure Sockets Layer (SSL) can offer some levels of assurance.

• Device management—Auditors should determine whether there is an asset management process in place for tracking mobile devices. This asset management program should also detail procedures for lost and stolen devices as well as procedures for employees who have been terminated or have resigned from the enterprise.

• Access control—Auditors should verify that data synchronization of mobile devices is not set to receive access to shared files or network drives that contain data that are prohibited for mobile use by the policy.

• Awareness training—The auditor should verify that the enterprise has an awareness program in place that addresses the importance of securing the mobile devices physically and logically. The training should also make clear the types of information that can and cannot be stored on such devices.

• Risk—Mobile devices have the capability to store large amounts of data and present a high risk of data leakage and loss. As such, mobile device policies should be created and enforced to ensure that information assets are not exposed.

**Conclusion**

Technical innovation has paved the way for mobile device assimilation into the workplace. These devices have acted as a catalyst for improving efficiency, productivity and availability in business operations. While many enterprises have chosen to utilize this technology, they have often not considered the business risk or the governance implications associated with these devices. Loss, theft or corruption of sensitive or confidential data; malware that can affect not only the mobile device itself, but also the enterprise network; and the way in which employees use the devices are just a few of the risks involved with this type of technology. In addition to the governance and security that already exist within the enterprise, risks and associated controls (if they exist) that accompany this boundary less technology must be assessed to ensure that enterprise information assets are protected and available. Enterprises that have been considering the use of mobile computing devices in their environment should calculate the benefits that the technology can offer them and the additional risks that are incurred. Once benefits and risks are understood, businesses should utilize a governance framework to ensure that process and policy changes are implemented and understood, and that appropriate levels of security are applied to prevent data loss.

**References:**

*Harris, Shon. (2013). All-In-One CISSP Exam Guide Sixth Edition*

*Publisher: McGraw Hill*

Vanquish the cell-phone virus. (2005, 05). *Technology Review, 108*, 16-17. Retrieved from <http://ezproxy.metrostate.edu/login?url=http://search.proquest.com/docview/195344054?accountid=12415>

NOKIA CELL PHONES CONTRACT VIRUS. (2004). *InfoWorld, 26*(25), 22. Retrieved from <http://ezproxy.metrostate.edu/login?url=http://search.proquest.com/docview/194355188?accountid=12415>

Roberta Bragg, C. I. S. S. P., & Rhodes-Oulsey, M. (2004). *Network security: The complete reference*. The McGraw-Hill/Osborne.

Neuhaus, S., & Gheorghe, G. (2013, November). POSTER: Critique of the CISSP common body of knowledge of cryptography. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 1355-1358). ACM.