What Kinds of Various Wireless Attacks Can Occur in Mobile and Wireless-Driven Devices?

Manuel Sanabria Andrade
Computer Science
Juan Ramírez, Ph.D.
Department of Electrical & Computer Engineering and Computer Science
Polytechnic University of Puerto Rico

Abstract *— Networks have been recently redefined by new devices in the market. These networks, comprised of a group of electronic devices, can be connected either using cables or using wireless technologies. Also, they have been implemented, not only in commercial places but also in households and home offices, among which reasons range from affordability to accessibility and ease of installation. However, these networks bear some significant risks when used: network attacks. Network attacks are one of the most common attacks to computer systems during these periods of time, where attackers are focusing on computers or other devices connected to a network, particularly if these are in wireless networks, and including cell phones, computers, and tablet pc, among others.*

Key Terms *— Attacks, Mobile Devices, Security, Wireless.*

INTRODUCTION

Wireless devices have become must-have devices among professionals and non-professionals, especially during these past years, where the necessity of always being in constant communication has arisen. Because of this, a large amount of devices currently hold wireless technology as part of their standard offerings; these devices range from personal computers (PCs), laptops, cellular phones (using both mobile and wireless networks), tablets, e-readers, among others. These wireless devices, however, have become a target for many attacks and that have paved the way for many attackers to create a diversity of security exploitations.

Wireless networks, being extremely similar to their wired counterparts, contain inherent risks associated with their outright implementation. Being that these technologies are associated with intercommunication between a diverse gamma of products and which may have their own security weaknesses and possibility of exploitation, security protocols and measure have been in an incremental development in these past few years. Moreover, this has caused many developers to create a large amount of security applications and additional methods to safely maintain and use information which must be used via these mediums. Additionally, development of encryption standards has also been a key measure to safeguard and to protect this information and which has been adopted in various technologies related to the wireless network field.

WIRELESS TECHNOLOGY

Wireless technology has been developed by a great number of companies throughout the years. This has caused a rapid evolution and a competition among many companies, boosting even further the capabilities once thought as limited. However, two of the wireless technologies most used nowadays as mediums to connect devices within networks are the mobile and Wireless Fidelity (Wi-Fi); the former is used with many devices, such as cellular phones, gaming devices, and certain tablet computers, while the latter can be used with most of the electronic devices used in day-to-day conventions.

Wireless Fidelity (Wi-Fi)

Wi-Fi technology works using radio waves to transmit data over the air. A computer or other Wi-Fi ready device communicates with a wireless access point which, in turn, communicates with the network. The radio frequencies used to communicate via Wi-Fi are extremely similar to those used to communicate

walkie-talkies and other similar devices. However, some differences can be shown between them, among which the most notable are that Wi-Fi transmits using 2.4 or 5 GHz frequencies, and that they transmit using 802.11 networking standards, created by the Institute of Electrical and Electronics Engineers (IEEE). This latter incorporates the 802.11a, b, g, and n networking standards [1].

These standards are based on the transmission capabilities of each one: 802.11a transmits at a 5GHz frequency and is able to move up to 54 megabits of data per second (Mbps), 802.11b transmits at a 2.4 GHz frequency and can transmit up to 11 Mbps, 802.11g transmits similarly to the 802.11b (at 2.4GHz) although it is able to transmit at speeds of up to 54 Mbps, and the 802.11n can transmit in both 2.4 and 5 GHz frequencies and with speeds of up to 300 Mbps; moreover, a new frequency is being developed, the 802.11ac, using the 5 GHz frequency and being able to transmit up to 7 Gigabits per second (Gbps) and which devices conforming to this standard are stated to be seen beginning on 2013 [2]. Refer to Figure 1 for an example.

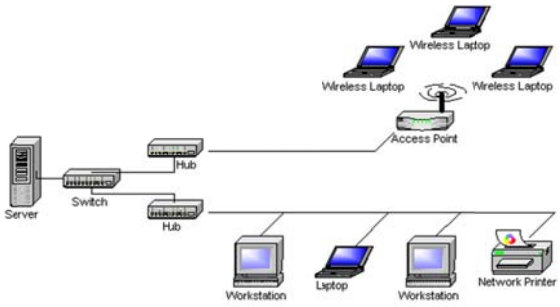

Figure 1
Example of a Standard Wireless Local Area Network (WLAN) Topology

Mobile Communications

Mobile communications, similarly to Wi-Fi, work using radio waves to communicate devices; these devices use radio towers to send and receive the different signals required to communicate with voice or data. These communications occur by using low power radio waves which communicate between them through a diversity of linked geographical places, called cells (hence the term cellular phones), up until it reaches its destination; Figure 2 presents an example of the mobile communication topology. As expressed before, this signals run through a series of radio towers, which are known as base stations, and which are responsible of transmitting these signals across and between cells; additionally, each cell is denoted by each base station. In other words, the distance covered by the base station is a cell. The most used technology for mobile communications is the Global System for Mobile Communications, also known as GSM, which was a communications standard developed by the European Telecommunications Standards Institute (ETSI). This standard was developed with the idea to replace the first generation analog cellular networks; it was originally designed and intended to be a digital, circuit-switched network optimized for telephony. However, this idea rapidly grew and data was added some time after that through the use of General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE).

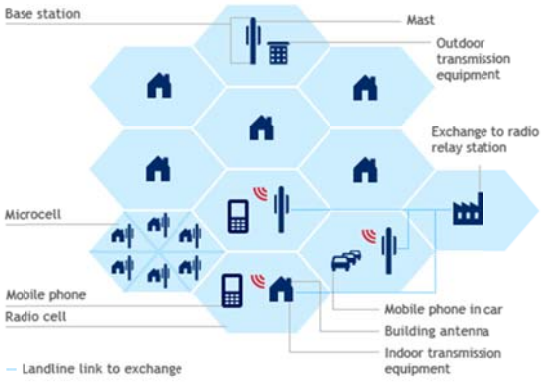

Figure 2
Example of a Mobile Communication Topology

Common Usage of Wireless Devices

Wireless devices have been incorporated into everyday life; recently, their uses have become increasingly peaked, especially among businesses where a need to communicate at all times have arisen exponentially. Moreover, data communications allow a much easier interconnectivity between people. This is essential for businesses who usually communicate

between numbers of people in order to ensure that services required are provided.

Tablets have become one of the most used mobile devices within enterprises. Some of these computers have been enabled with the ability to use mobile communication inherently; only a network service provider, also known as a network carrier, is needed to include a mobile communications plan to be used.

Additionally, tablet computers are capable of using Wi-Fi, a peculiarity not uncommon among mobile devices. Other mobile devices, such as cellular phones, are also known to have both mobile and Wi-Fi communication ability. This allows for a diversity of possible communication methods when not connected to a wired network. Moreover, new technologies allow for the creation of a mobile hotspot, where mobile devices make use of their communications and create a wireless access point where devices with Wi-Fi capabilities may connect and make use of such technology.

VULNERABILITIES, THREATS, AND RISKS

Mobile devices, based on the nature of their use, contain a number of vulnerabilities, threats, and risks that enterprises must be aware and address in order to ensure that security measures are taken so that they cannot be exploited.

Vulnerabilities

The following vulnerabilities can be identified within the mobile and wireless-capable devices:

- Sensitive information is traveled across wireless networks, making them more easily accessible through networks which are often less secured than wired networks.
- Mobility provides users with the opportunity to leave enterprise boundaries, thereby eliminating many security controls. These devices can be taken out of secured perimeters and onto unsecured areas.
- Unencrypted information stored within the device's memory may be accessible to unauthorized users of the device.
- Employee productivity may be affected if information kept within the devices is lost.
- Authentication requirements within mobile devices may not be as stringent as within computers, thus easier to be broken.
- Usually, the companies do not manage the device, especially those that contract third parties for their mobile services.
- Devices nowadays allow an innumerable amount of third-party applications to be installed within the devices for accessibility and other daily functions needed from the devices.
- Sensitive information is kept and safeguarded by the owners of the information within the enterprises. If this information is kept within mobile and wireless-capable devices, the users can easily make use of the information for other-than-work purposes.

Threats

The following lists the threats related to the vulnerabilities aforementioned:

- Outside sources may access in an easier manner information being transmitted through wireless equipment, whereas wired communication may need a physical tap in order to be accessed.
- Crossed-boundaries mobile devices may carry malware and other such software which may hinder the devices' security and allow for easier access to the information as well as propagating this software within the network.
- Readability of the information may be caused by unencrypted information within these mobile devices. If a malicious outsider were to intercept in-transit data or to steal a device, or if, otherwise, the employee were to lose the device, the data residing within it is readable and usable.
- Mobile devices, due to their portable nature, may be lost or stolen. Since data residing within these devices are usually not backed-up, if the device is lost, then its data is also lost.
- Since data residing within the device is not encrypted, in the event that the device is lost or stolen, outsiders may be able to access the device and all of its data.

- If, within an enterprise, no mobile device strategy exists, employees may choose to bring in their own, unsecured devices (bring-your-own-device, BYOD). While these devices may not connect to the virtual private network (VPN), they may very well interact with e-mail exchange services or store sensitive documents.
- Applications installed within the devices, especially those developed by third parties, may carry malware or other corrosive software that propagates Trojans or viruses; additionally, applications may also transform the device into a gateway for malicious outsiders to enter the enterprise network.
- Discovering the devices by hackers may cause them to access a device and/or launch attacks towards them.

Risks

The following vulnerabilities can be identified within the mobile and wireless-capable devices:

- A breach of information caused by its interception may impair the enterprise to work fluently and cause a downfall to the enterprise's reputation and legal actions toward it.
- Upon malware propagation, possible outcomes include data leakage, data corruption and unavailability of necessary data.
- Sensitive data exposed which may result in damage to the enterprise, customers or employees.
- Limitation of productivity of workers dependent due to an unavailability of the mobile devices if these become unable to work because they become broken, lost, or stolen and their data are not backed up.
- Data becoming exposed to unauthorized parties may result in damages to the enterprise and liability and regulation issues.
- Data leakage, malware propagation, and unknown data loss may occur if the device is lost or stolen.
- If devices become corrupted with malware, these may propagate along the enterprise's network and intrusion may be possible by outside sources.
- Device corruption, lost data, and call interception, may be possible, thus creating a higher probability of exposing sensitive information.

Risks, threats, and vulnerabilities are inherent within these types of technologies, especially when regarded to the information being transmitted and kept within the devices. Moreover, these risks, threats, and vulnerabilities are also known to many individuals outside of the corporations. This allows unauthorized users to launch attacks and exploit certain vulnerabilities that, if addressed correctly, would not leave the devices in an exploitable manner.

ATTACKS

Wireless communications, being part of networks, are susceptible to attacks very similarly to those found within their wired network counterparts. Additionally, a flurry of attacks has been found to be used on wireless devices and through the use of the different variations of technologies available.

Attacks on Wi-Fi

Wi-Fi attacks are not uncommon; many devices suffer attacks (or attempts) to be hijacked during the transmission of information. A number of attacks have been commonly used for this purpose, among which the following can be distinctively identified: War-Driving, Man-in-the-Middle, Plain Text, Packet Sniffing and Eavesdropping, Jamming, Network Hijacking, and Denial of Service (DoS) [3]-[5].

War-Driving attacks consist of using certain application software to detect and hijack a broadcasting wireless network with poor security parameters. Man-in-the-Middle (Figure 3) attacks consist of placing a rouge access point within range of an existing wireless network; users are ignorant of the fact that they are connecting to an illegitimate access point and succumb to the inadvertent scams and provide personal data, such as social security numbers, credit card information, and identification or authentication values. Plain-text attacks especially target Wired-Equivalent Privacy (WEP) security protocols and are based on decrypting WEP initial

authentication, which is sent in plain text. Packet sniffing and eavesdropping are usually used on wireless networks in order to monitor (sniff) the network traffic by use of legitimate network monitoring tools to ascertain if a network is insecure and available to be hacked into.

Jamming bases on flooding the radio waves with an undesired signal and disrupts the availability of a particular wireless signal, thus impeding its use. Network hijacking is when an active user session is taken controlled by an external source and where a hacker can insert himself/herself between the network server and the wireless client. Denial of Service attacks occur when unavailability of resources have occurred after a specific resource has been bombarded with an innumerable amount of requests.

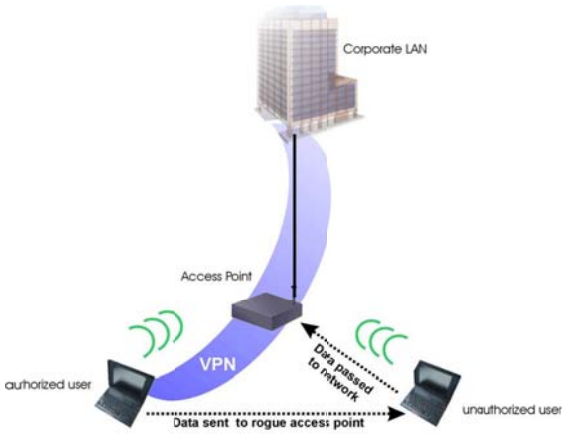

Figure 3
Graphical Representation of a Man-in-the-Middle Attack

Attacks on Mobile Networks and Devices

As of the first three quarters of 2010, more than 195 million smartphones were sold worldwide. However, smartphones have one major drawback: its ability to run applications, which makes users incredibly and increasingly reliable on them for computing needs.

Mobile attacks work in a similar fashion to wireless attacks. Some of them only use certain vulnerabilities in the network and exploit them in order to create the attack and acquire the data they want. However, since mobile devices have become less cellular phone-like and more computer-like, they have been endowed with the ability of using software applications specifically designed for them. These software applications are often developed by the Operating System (OS) markets. However, some of the applications available are developed by third parties.

One of the most common OS's in mobile devices is the Google's Linux kernel-based Android. This OS is available for smartphones and for tablets. The Android platform is composed of a total of four (4) layers:

- Applications – applications run at the very top of the platform.
- Application Framework – Services for applications, such as the Activity Manager (which controls activities for each application) and the Content Providers (which load the content provider defined by each application while restricting data accessibility across applications, are located in the Application Framework.
- Static Library – The Library/VM Layer contains static libraries and the Android runtime environment, and these static libraries provide common system and application libraries for applications. The Android runtime environment is composed of core runtime libraries and the Dalvik virtual machine (VM) – an optimized Android-specific Java virtual machine.
- Linux Kernel – the final layer within the architecture.

Android applications can be composed of a total of four component categories:

- Activity – focused windows in which the user interaction takes place, although only one activity can be active at a time.
- Broadcast Receiver – manages data for a certain application and controls the accessibility of the data
- Content Provider – listen and react to broadcast announcements.
- Service – Services run in the background while

users are running other applications. Moreover, a wide variety of applications have been created, with over 600,000 apps available for their download [6]-[7]. Furthermore, this ever-increasing number of available apps increases security threats exponentially. Reports have been provided by companies such as McAfee Labs, stating that each year mobile phones and tablets increase the likelihood of being attacked by malicious software. Additionally, types of threat aiming towards these devices have had significant changes.

Applications are constantly tested to verify if bugs or other security weaknesses can be exploited. Testing of the applications is performed using many tools and techniques. However, certain limitations exist for the testing of mobile applications, such as the physical constraints of these devices and the unfamiliarity of the developers with mobile platforms. Their high defect density has made these applications prone to bugs. These bugs allow the hackers to exploit the applications' security weaknesses in order to gain access to either confidential information or to resources found within the systems.

SECURITY

In order to ensure that security treats are assessed adequately and reduce the possibility of having confidential information stolen or compromised, companies involved in security-related applications have developed a significant amount of tools and utilities to protect the systems and the information within them. Additionally, these utilities provide many kinds of defense and backup tools so as to ensure that the information does not become irrecoverable. Among the possible security applications developed, some have been distinctly identified to work with either a mobile device or with a computer. However, new trends have made some of these developers to design and develop security applications that either work on both types of devices or provide a desktop and a mobile version.

Desktop Security

Security utilities have been created with the sole purpose of defending computers against threats. Among the most used security tools are the antimalware, antivirus, anti-spam, application-based firewall, and safe-browsing utilities.

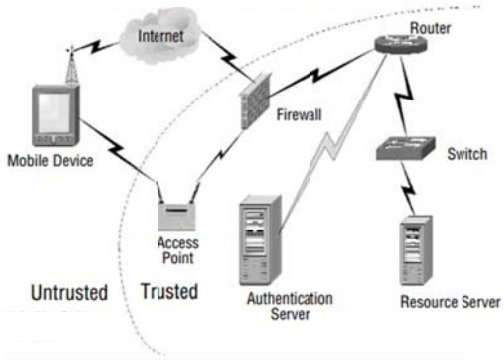

Figure 4
Graphical Representation of a Basic Security Model of a Wireless Network

However, additional security methods have arisen through the development of the threats. One such feat is the development of the WEP, the Wi-Fi Protected Access (WPA), and the Wi-Fi Protected Access II (WPA2, also known as 802.11i). WEP refers to the intent of creating a security for wireless network similar to that of a wired network. WEP functions as follows: each packet is encrypted separately with a RC4 cipher stream generated by a 64-bit RC4 key. The encrypted packet is generated using a bitwise exclusive OR (XOR) of the original packet and the RC4 key. However, this type of security had some apparent weaknesses, among which are the following:

- No key management is present within these standards and keys tend to prolong their existence, thus reaching a point of obsolescence.
- Messages used to authenticate can be easily forged.

Since the WEP standard became increasingly obsolete, the WPA standard was developed. Contrary to the WEP standard, the WPA was developed by the Wi-Fi alliance in order to address the shortcomings of the WEP standard; it bases on using the Temporary

Key Integrity Protocol (TKIP) to boost the encryption in wireless packets. Additionally, it uses a central authentication server, such as the Remote Authentication Dial-In User Service (RADIUS), in order to authenticate the user. Subsequently, the WPA2 functions as a product certification where it certifies that the device is compatible with the 802.11i standard. Many enterprises require this newer type of security standard to ensure that protection of wireless transmissions is at its optimum. Additionally, several other protocol implementations have been developed to replaces the WEP standard like, for instance, the Extensive Access Protocol-Transport Layer Security (EAP-TLS), Tunneling TLS (TTLS), and the Protected EAP (PEAP) [8]. The EAP protocol uses digital certificates within a public key infrastructure, otherwise known as PKI, in order to successfully authenticate users. Wireless devices have the ability to create secure connections to ensure that these are safely employed via the use of digital certificates. The users request either a digital certificate or an encrypted file to be stored within the device to be connected. This, in conjunction with a password or a personal identification number, otherwise known as PIN, functions as an authentication mechanism which ensures that the user requesting access to the network is really the user and not an unauthorized person, to a network server or an access point, which must also issue their own digital certificates back to the devices. However, because of the costs of this technology as well as the costs and complexity of its implementation, many enterprises have opted to not use this authentication mechanism. Because of this, the TTLS and the PEAP have been developed. Neither of these protocols requires the user to store a digital certificate within the device by incorporating older encryption protocols; Figure 5 depicts the authentication process of these protocols.

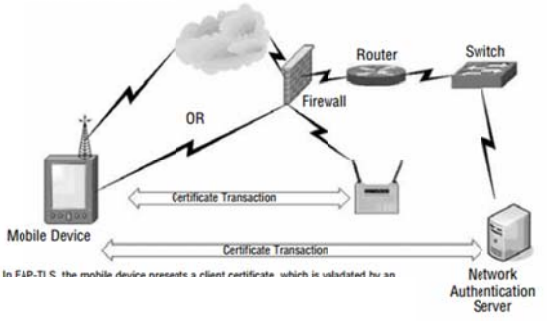

Figure 5

Graphical Representation of the EAP-TLS, PEAP, and TTL Protocols' Authentication Process

As previously explained, in the EAP protocol, the device presents a digital certificate which is validated by an authentication server. In turn, the authentication server (or the wireless access point, whichever the case), presents a certificate in order to validate itself to the device. Upon validation from both sides, the user may then gain access to the network resources. However, in the PEAP and TTLs, the authentication server (or wireless access point) will present the client a certificate first. The client will then, either present its own certificate, or authenticate via another authentication protocol.

An additional layer of security is sought by enterprises by the use of Virtual Private Networks (VPNs). These type of connections are used between the device and the enterprise's network and creates a "tunnel" used to connect the two. Every transmission performed through the use of this connection will be encrypted, thus the possibility of tapping and retrieving this information greatly decreases.

Mobile Security

Mobile security is enforced through some security tools, very similarly to the Wi-Fi utilities. Such utilities include additional methods of security, not only the protection against unwanted software, but also the ability to encrypt information. Such encryption is required to protect the information safeguarded within the devices, especially for those used within enterprises.

Firewalls have been developed also to protect the information within such devices. These firewalls filter accesses and prohibit unauthorized accesses to

the systems. Security utilities developed by companies such as AVG, AVAST, Comodo, Avira, Kaspersky, and McAfee are the most widely used to safeguard these devices.

Moreover, security policies should be implemented within the enterprises to ensure that maximum security is implemented within these devices. Also, some of the most common security measures taken within enterprises are the following:

- Encrypt local storage as well as removable media located within the devices.
- Enforce Virtual Private Networks (VPNs) to connect to sensitive networks.
- Perform backups of the data within the devices.

Perform centralized configuration and software upgrades "over the air" rather than relying on the connection to computers.

CONCLUSION

Devices with the ability to connect to the different networks have gained an incredible boost for the past few years. Additionally, daily uses have been developed where the necessity of always having an indisputable amount of availability is imperative. However, this need to always be connected opens the door to numerous security exploits. Moreover, third party technologies developed also allow security threats to be exploited more easily.

Information found within mobile and computer devices with connectivity to Wi-Fi or mobile networks require to always be protected and safeguarded from unauthorized access and appropriation. This raise in security concern has also made many of the security utilities developers to create applications which may ward-off possible threats. By doing this, secure communications between the networks are possible, including emails.

By using these new technologies, many costs can be significantly reduced. The necessity once apparent to invest a large amount of capital towards communications, especially long distance and multiple communications, have been greatly reduced and can now be limited to only those necessary within the enterprise. Even multinational corporations have found these technologies of great use to become increasingly competitive in their respective industries.

Recommendations

Mobile and wireless-enabled devices have become a significant and integral part of the Information Technology infrastructure within enterprises. However, in order to appropriately ensure that security risks and threats are being handled in an adequate and appropriate manner, certain security measures must be taken. Enterprises must begin by recognizing the significance of these devices among the enterprise community, along with all of its implications, both positive and negative. By assessing the positive ones, enterprise senior management may easily detect the use company employees have of the devices, thus making it possible to create policies and procedures to attend to their necessities as well as ensuring that company-wide requirements are met as well. Among the positive trends being attended by mobile devices, the following should always be recognized by senior management and related IT Governance bodies, such as the IT Steering Committee:

- Sales and field force automation and customer relationship management - Companies nowadays regularly use handheld devices for daily operations, including but not limited to recording deliveries and instantly updating the data on remote servers, accessible by mobile devices.
- "Dead-time" productivity - Mobile data connectivity and wireless capabilities improve productivity during dead times, such as periods of time when employees are waiting for a service or action, such as airports or meetings. Time used in these actions may very well be spent by these employees to check email communications, respond to urgent matters which otherwise may be answered after the required period of time.
- Travels - Maps and routes are now available and accessible on GPS-enabled mobile devices, thus speeding up travel time. Additionally, services are available which

trace the shortest and most direct routes to take in order to arrive at a destination, even if it is by foot or in some other method of traveling. Moreover, new additions to these services even include traffic reports to ensure that the fastest route possible is selected.

As part of the due process required to ensure safety among the users and the information retained within these devices, as previously mentioned, IT Governance bodies must ensure to include mobile devices among the frameworks within the enterprises, thus a necessity of developing a mobile technology governance framework has been created. The principles behind IT Governance should be used to manage IT risks of mobile devices. Senior management must be involved and committed to ensure that successful implementation is made of this strategy. This strategy must include a plan for obsolescence, since this technology is ever-changing and evolving.

A mobile policy should also be created and addressed. This type of policy should be implemented to govern the use of mobile devices within the enterprise. Moreover, it should include explanations such as proper behavior in relation to the use of these devices, their correct and incorrect uses, guidelines of usage, costs and reimbursements, and Human Resources perspectives, such as actions taken when a user leaves the organization.

Security policies must also be created to include wireless network and mobile devices. Because of the risks inherent to these technologies, such as the unauthorized access to information being transmitted by way of tapping the communication mediums, or the risk of the devices being stolen as well as the repercussions of this action, especially since the data retained by the enterprises is usually considered highly sensitive, the security policies established should address all of these possible scenarios where a security breach or communication of information without the required clearances has occurred. Additionally, security policies should address the corporation's view on mobility, permissible use, sourcing, chargeback, device standards, support and service levels, and governance. Other such aspects of the policy include:

- Enforceability on a myriad of devices.
- Managed in a centralized way by the enterprise itself.
- Simple framework used for support and implementation.
- Flexible, able to be adapted to various devices and situations.
- Focused on hindering the possibilities of loss and theft.
- Auditable in all of its parts.
- Tested and verified in disaster response tests.
- Attentive to possible external threats.

Also, strategies to address risks should be developed. Since many risks are inherent to these technologies, great care should be considered. The Information Systems Audit and Control Association (ISACA), has created and established a list of strategies to address risks, as explained below [9]:

- A lost or stolen mobile device – A strategy to address this risk would be to implement a central management console for device remote control such as location tracking, data wipe-out, password/PIN change, and/or strong user authentication. Additionally, always ensure that mobile devices are encrypted so information is unreadable and unusable in the event of loss or theft.
- Supporting various devices – Use cross-platform centrally managed mobile device managers to ensure that the myriad of devices available are included within the management system.
- Controlling data flow on multiple devices - Systems accessed through these devices should be secured with authorization, encryption, and privileges controls.
- Unauthorized synchronization of data to mobile devices must be restricted – Data

transfers to handheld devices should be monitored and restricted.

- Keep up with new developments of these technologies – Create user awareness trainings and provide them for the employees within the organization as a compulsory requirement.
- Promote accountability, responsibility, and transparency from device usage – Track and monitor the way these devices are used, and keep updated management with new trends as well as with existing ones.
- Demonstrate regulatory compliance – Implement a central management console which will manage all phases and stages of asset management.

REFERENCES

[1] Hutchison, K. "Wireless Intrusion Detection Systems", *GIAC Security Essentials Certification (GSEC) Practical Assignment*, October 18, 2004. Retrieved from http://www .sans.org/reading_room/whitepapers/wireless/wireless-intrusion-detection-systems_1543

[2] Smith, D. "What makes up a WLAN", May 3, 2002. Retrieved from http://www.techrepublic.com/article/what-makes-up-a-wlan/1048092

[3] Esposito, S. "Evolution of Wireless Security", *Y-12 National Security Complex*, August 9, 2007. Retrieved from http:// www.infragard-etn.org/wp/wp-content/uploads/2011/02/Evolution-of-Wireless-Security.pdf

[4] Low, C. "Understanding Wireless attacks & detection", *GIAC Security Essentials Certification (GSEC) Practical Assignment*, April 13, 2005. Retrieved from http://www. sans.org/reading_room/whitepapers/detection/understanding-wireless-attacks-detection_1633

[5] "Common Types of Network Attacks", *Microsoft TechNet Library*. Retrieved from http://technet.microsoft.com /en-us/library/cc959354.aspx

[6] Constine, J., "Google Play: 600K Apps, 1.5B Installs Per Month, 20B Total, Now With Byte-Sized Smart App Updates", *Techcrunch*, June 27, 2012. Retrieved from http://techcrunch.com/2012/06/27/google-play

[7] Fingas, J., "Google Play hits 600,000 apps, 20 billion total installs", *Engadget*, June 27, 2012. Retrieved from http://www.engadget.com/2012/06/27/google-play-hits-600000-apps/

[8] Smith, M., "Overview of Mobile Technology", *Journal Online*, Vol. # 1, 2006.

[9] "Securing Mobile Devices", *An ISACA Emerging Technology White Paper*, August 2010.