Mobile Devices - Future Security Threats & Vulnerabilities

V.Sklikas and N.L.Clarke

Network Research Group, University of Plymouth, Plymouth, United Kingdom.
e-mail: info@network-research-group.org

Abstract

The success of the Internet technologies made telephony companies realise the advantages of the adoption of IP technologies over circuit switched networks. Now both the telecommunication and Internet technologies converge and integrate for the creation of an 'all-IP' wireless infrastructure, able to support mobile data and multimedia applications, resulting in making available all known Internet services to the forthcoming wireless networks. However, beyond the numerous benefits that arise, factors such as mobility, the compact size of the various mobile devices, the ease of their connectivity and their open nature increase the threats and the risks being posed, rendering the future wireless security an increasing problem. This paper reviews the threats introduced by traditional networking technologies and examines the way in which they could be adopted by the wireless technology, investigating possible threat scenarios and taking into consideration future technology capabilities.

Mobile technologies are a target for many threats that exist in traditional wired networks, in addition to many wireless specific threats. The underlying communications medium is open to intruders and is easier to eavesdrop as no physical access is required. Unauthorised access to a network through wireless connections, by bypassing any firewall protection, interception of unencrypted information, and the tracking of the mobile users are some of the most critical threats concerning the owners and the users of mobile networks and devices.

This paper introduces a number of network topologies and discusses the relatively advantages and disadvantages of implementing each. Generally security of mobile devices can be viewed from a central server or network centric perspective, managed by trusted third party authorities, offering security at the network and covering all security tasks needed on the devices with no end-user interaction.

Keywords

Mobility, security, wireless

1. Introduction

The two major fields that target in their convergence that will lead to a unified wireless IP infrastructure, are the cellular telephony and the Internet. Wired networks evolve into wireless and wireless networks evolve into wireless Internet Protocol (IP) networks, as the latter is a more suitable approach for supporting the forthcoming mobile data and multimedia applications. The workplace is being decentralised and the level of electronic mobility able to overcome the limits of traditional wired

devices, is given by new technologies for communicating, entertaining, and accessing information that introduce with incredible pace. Portability, flexibility and productivity increase, while the numerous mobile devices introducing, allow data synchronisation with network systems and application sharing between the devices. Remote users are allowed to synchronise personal databases and are provided access to network services such as wireless e-mail, Web browsing and Internet access, though, the receiving, modification and transferring of information over networks, while roaming, becomes feasible. Public access points are growing daily in number to serve mobile users and provide them with connectivity. The prerequisite to this scheme, so that Internet services become available to wireless networks, is the integration of the IP technologies into mobile devices.

On the other hand, until now we used to be concerned only about security associated to wired local networks especially due to the highly vulnerable IP protocol. Unfortunately the aforementioned convergence brings IP technologies and mobile devices together, setting new security problems. In more detail, wireless IP networks operate over the IP, resulting in them inheriting all known vulnerabilities of the Internet Protocol. Lack of strong network security provision and a number of flawed services are some of the IP's weaknesses that make it vulnerable enough to exploitation and specifically to misuse and spoofing. Additionally, the numerous mobile devices required and used to bring the wireless services to the end-user, have many critical weaknesses, making them vulnerable to security threats. Mobile communication and wireless technologies became a target for already existing weaknesses within fixed networks. However, the mobility offered through these technologies, the variety, the minimal physical size and the ease of mobile devices' connectivity make security risk levels to rise. Moreover, the open nature of the wireless technologies due to the airborne waves they use for data transport and some different protocol deficiencies than those introduced in wired networks, make some security aspects to occur in a different form than they occur in fixed environments. Current threats are able to compromise wireless vulnerabilities, making the future unsure for everything and everyone. But in which manner could wireless technologies be compromised? Which and how already existing vulnerabilities could be exploited in order for someone to hijack telecommunications? Which are the techniques already followed in wired networks and now adopted, modified and applied to mobile devices, for someone to serve his purpose? If the future is going to be so insecure, is there any security mechanism that could counteract the forthcoming threats and risks?

2. Possible Future Threats and Vulnerabilities

The numerous mobile devices, the enhanced wireless capabilities, the increased computational power, the integrated IP technologies and a majority of security unaware consumers that will be using these devices make a very risky combination for the advanced IP services that will be offered widely through the Internet. But how this combination renders the future mobile domain insecure?

2.1 How could Mobile Devices be compromised

The increased use of wireless devices, Personal Devices, PDAs and smart phones running an operating system in combination with the 3G technology that brings Internet services on these devices, increase the potential for attacks. Their open operating systems and the lack of antivirus and detection tools, make the devices capable of being infected by any kind of malicious code. Their data storage, their transfer capabilities and their support for executable files, add to the problem and will make them even more susceptible to worms, viruses and spammers, while they introduce new exposures for hackers and crackers to target. The numerous wireless access technologies they support open a new avenue, due to their open nature, and increase the potential for a number of attacks. Moreover, their compact size encourages them being stolen, while the lack of authentication mechanisms facilitates the unauthorised access to the devices.

Furthermore, mobile devices integrate office functionality making it more possible for Malware to widespread by exploiting their wireless ports. In addition, they are very often strictly associated with critical data and applications, but as mentioned before, not accompanied by any security facilities or data integrity mechanisms. The ultimate goal, though, will involve the collection, alteration or loss of financial and other confidential data. The devices' direct ties to systems that deal with purchases and other transactions (LLet and Hines, 2004), and the fact that the number of users that engage wirelessly in online banking increases, will make mobile devices a tempting financial offer to exploit.

Moreover, 3G technologies and the increased number of the multimedia applications, games and screensavers available for downloading, combined with the fact that providers usually allow all kinds of content to be sent to the handsets, will pose hidden risks. Malware will be able to spread through all these facilities infecting both network services, such as Short Messaging Service (SMS) or Multimedia Messaging Service (MMS), and mobile devices. Infected devices will make their numerous wireless access technologies available for Malware to distribute. In addition, the increased access technologies that will be supported within Wi-Fi networks, including wireless networking cards, wireless access points, and Bluetooth will increase the potential for attacks. The combination of the access technologies used by the devices and the enhanced Wi-Fi networks open handhelds up to a variety of attack scenarios.

Another issue concerns the variety of the mobile operating systems that ensures that the widespread Malware is minimised. The lack of a dominant operating system requires Malware to be specifically written for each individually. The most popular operating system to date, is Symbian, hence most of the attacks have been focused upon Symbian PDAs. But how long will this be for, until mobile devices adopt one common operating system?

Finally, technology improves and the devices are equipped with enhanced and accurate built-in capabilities, like cameras and microphones. This makes anything supposed to be safe and private within the physical perimeters of a user's location, office or room susceptible to eavesdropping. In addition, mobile IP and the numerous

location-aware services used by mobile devices, like GPS that has already started to be used, could provide unauthorised parties with information, which reveal end-users' location, resulting in the violation of end-user privacy.

2.2 Mobile Devices – An Attacking Tool

Mobile devices will not always be the victim; it will equally be the attacker. Intranets are expanding beyond the traditional enterprises' limits out into the Internet, through mobile and wireless access technologies increasing not only external but also internal threats (Greenfield, 2002). Threats within wireless networks could be born and occur in any form, with passive or active attacks, malicious codes or software tools that assist an intruder using a mobile device to compromise any security weaknesses. Mobile Malware will be able to cause widespread damage. Such devices will be possibly used within enterprises without being noticed, enabling someone to gain unauthenticated access in the network. Attached to network connections, they could constitute a backdoor threat from the outside world. Operating as hidden 'Zombies' (Gilbert, 2005), they could launch attacks and distribute Malware to other PCs or networks, aiming to the alteration or disclosure of any sensitive data or the affection of the network's reliability and availability through Denial of Service (DoS) attacks.

Furthermore, future handhelds with enhanced communication capabilities, processing power and executable files support, will open a new avenue for easily compromising various Internet services that are considered to be secure enough. Therefore, Voice over IP (VoIP) sessions will be spoofed, eavesdropped, or even disrupted. Voice packets will be possible to be recorded, or IP phones could become unstable and finally unavailable. Having physical access to the main servers will give the opportunity to disrupt any services integrated with VoIP applications, like unified messaging. In the same way, using a mobile device within the network to compromise and launch DoS attacks to the VoIP gatekeeper, could lead to limited bandwidth or no service availability. Every component of the VoIP network infrastructure becomes susceptible to distribution of viruses, DoS attacks and eavesdropping, since handhelds will be almost everywhere and without control within a company or a core network. Unfortunately, VoIP will become feasible to be compromised outside an intranet too. Hot Spots are increasing in number and such public access points are preferred by a number of uneducated end-users, resulting in increasing any potential of attacks, making such places risky too. Public access points will be using the Mobile IP, proved to be vulnerable, increasing, though, the possibility for VoIP ongoing sessions to be monitored and disrupted, while providing the adroit user with free voice services and charging the unaware consumer.

The conclusion is that mobile devices are going to become an increasing problem for everyday life, affecting it in all sections; financial attacks, thefts, and users' privacy. Thus, there is no need for more evidence that enhanced security mechanisms have to be proposed, designed and deployed as a counteract to the forthcoming problems.

3. Future Security Solutions

The need for mobile security mechanisms and improved device management is undeniable. A complete security solution should look for weaknesses, focusing independently on protocols, mobile technologies, software and the end user security knowledge, while it needs to commensurate with the threats posed against it and the cost of securing it. The ultimate security solution should rely on a centric framework that improves the network and the terminal security management.

There is a range of mechanisms that could enhance security on mobile devices. An appropriate BIOS configuration could constitute the primary level of security, involving authentication prior to system boot and locking mechanisms for preventing any configuration alteration. Enhanced solutions include third party audit tools installed on the devices that provide with log mechanisms able to monitor actions taken on them, while antivirus, firewall and detection tools increase security. In addition, technologies are improving in terms of reliability and accuracy and biometric devices (Silicon Trust website) will eventually become the preferred choice for user authentication, preventing identity fraud. Moreover, the numerous services that will be offered should be able to detect any kind of misuse by illegitimate users, making end-users feel confident about the services they use. Though, third party services that digitally certify the authenticity and integrity of an application (Meserve, 2005), could be considered an appropriate mechanism. End-to-end encryption methods imposed to all the network's nodes that the devices might connect to, advances the protection level. IPv6 and IPsec (Ford, 2005) that is contained in the new version of IP, is more viable than Secure Sockets Layer (SSL) when it comes to traffic from a large number of applications. Additionally, IPv6 would enhance security in the public access networks. Finally, the implementation of encryption mechanisms makes VoIP and Mobile IP related services more secure both within enterprises and public access points, eliminating the possibility of eavesdropping. Finally, the large number of mobile devices on the market, and the uneducated consumers who have little to no knowledge of the security threats that are posed, makes it an imperative need that enterprises and the market precipitate into technical education solutions that incorporate a level of education and security knowledge of the end users. Specific policies should be imposed, within enterprises and public access points, on the way mobile devices are used.

Unfortunately, common security solutions used to date are possibly insufficient for future security demands; on the contrary the above review and propositions, show that some advanced security is required; how this could be achieved or possibly approached, is from a centric perspective. The existences of centric frameworks introduce an advanced level of protection by using network resources.

One approach could be a network centric model that uses network resources in protecting the devices. A network centric model, suggests the provision of security solutions at the network and not at the client device side; the future Internet will be secure as long as it will rely on third parties that provide with the necessary services to filter and monitor the content that flows inside the core network, preventing from Malware's spread at the client devices. Third parties could use the appropriate

antivirus, firewall and detection tools to provide a gateway level protection, in order to successfully block any malicious or unsolicited code in the network. Centric solutions do not require any end-user interaction, facilitating amateur consumers.

The central server model implies a centralised management of security on the device. It could refer to a model that involves a third party agency or authority, equipped with a range of central servers, providing the corresponding security services, like password security, biometric information security, and the provision of sensitive data storage behind a firewall. A central management console interacting with the devices, could provide terminal monitoring and its security configuration, while patches, updates and any kind of fixes concerning the various operating systems that mobile devices use, are downloaded automatically. All security tasks taking place on the devices are time consuming and complex, discouraging amateur users who do not have the appropriate knowledge to engage in such processes; thus, the ultimate aim of a central server framework is to impose security services at a terminal level, with no end user interaction.

However, a number of disadvantages arise within each of these centric models. The nature of a network centric model renders it weak when it comes to any kind of failure (Karygiannis, 1998). The system becomes unable to monitor any component of the network and all the nodes being protected before, become available and easy to penetrate. On the other hand, although a central server framework is fail-safe, it is vulnerable to security weaknesses since an intruder can disable local security mechanisms on the terminal that report back to the central system; thus a device cannot always be trusted to diagnose itself with a host-based monitor alone (Karygiannis, 1998). Both the network centric model's and the central server model's weaknesses imply that there is a need for a hybrid model that inherits and combines most of their advantages eliminating any deficiencies. A hybrid model is illustrated in Figure 1.

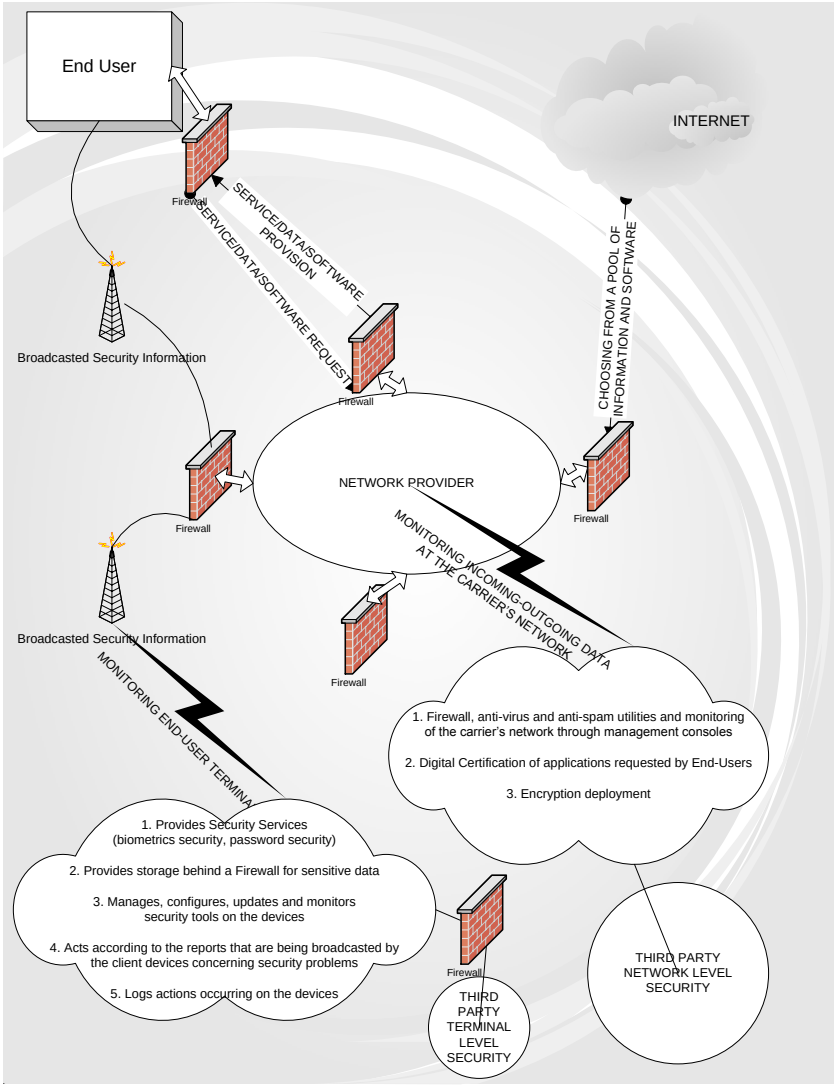

Figure 1. Hybrid Model

4. Conclusion and Future Work

The success of the Internet technologies made telephony companies realise the advantages of the adoption of IP technologies over circuit switched networks. Now both the telecommunication and Internet technologies converge and integrate for the creation of an 'all-IP' wireless infrastructure. Mobile devices introduce everyday, equipped with utilities and facilities to exploit the forthcoming networks. All known Internet services and multimedia applications will be delivered to mobile devices since future wireless networks are designed to support IP technologies. Unfortunately, an IP infrastructure inherits all known vulnerabilities occurring within

the traditional networks that operate over IP, in addition to factors like mobility, the variety of the devices that are used and their compact physical size. All these factors make it easy for current threats in traditional networks to be adopted and be applied to wireless technologies, in different forms due to their open nature. Mobile Malware will become an increasing problem for mobile devices, compromising network services to propagate. Attacks will be launched with the goal of financial gain and sensitive data disclosure.

The need for mobile security mechanisms and improved device management is undeniable though. A possible future security infrastructure should call for the following:

1. An end-to-end solution for all mobile devices within a carrier's network

    - Network centric security services maintained by trusted third parties;
      A gateway level security solution in the network is required to be able to
      flexibly filter the traffic. Intelligence lying on the network will always be
      better than any solution at device level.
    - Central server security approaches also maintained by trusted third parties

2. Mass coverage over all devices and geographic regions
3. Transparent security that requires no end-user involvement
4. Cooperation between network carriers, device manufacturers and technology providers, such as software companies that write applications for smart phones.

4.1 Future Work

Some of the issues that a future research could focus on, could be associated with the enhancement of the security mechanisms required to counteract the forthcoming threats, proposing the technologies and specifications that should be used.

Networks that consider the different access technologies including their advantages and disadvantages could be researched, combined with a study of the types of network infrastructures, able to protect mobile devices that might be applicable. A detailed report on suggested systems' configuration followed by network diagrams and simulations would be very useful for network administrators who focus on blocking the threats at the network rather than at the devices.

The detailed actions of trusted third parties, bearing in mind the nature of mobile devices and their technical requirements such as processing and memory needs should accompany a research on possible required equipment. Finally, the major topic, though, that should accompany the aforementioned possible future research topics, could negotiate with an investigation that defines the best choice and combination of future security frameworks and the proposed security mechanisms,

the equipment and technical specifications; it should best reflect in the most profitable way both for the authorities and the end users, financial issues and the quality of services that will be provided.

5. References

Ford, M. (2005), "Security and IPv6", http://www.ipv6.bt.com/tutorials/security.html, (Accessed July 2005)

Gilbert, A. (2005), "Botnets and Spyware still on the rise", http://news.zdnet.co.uk/internet/security/0,39020375,39208661,00.htm, (Accessed July 2005)

Greenfield, D. (2002), "New Public Network: Crystal Ball Gazers", http://www.networkmagazine.com/shared/printableArticle.jhtml?articleID=8703365, (Accessed 2 September 2005)

Karygiannis, T. (1998), "Network Security Testing Using Mobile Agents", http://csrc.nist.gov/mobilesecurity/Publications/Agents_PAAM98.pdf

LLet, D. and Hines, M. (2004), "Skulls program carries Cabir worm into phones", http://news.com.com/2100-7349_3-5469691.html, (Accessed July 2005)

Meserve, J. (2005), "Is your cell phone at risk?", http://www.networkworld.com/research/2005/041805-mobile-virus.html, (Accessed July 2005)

"HP Wireless Security", http://h200007.www2.hp.com/bc/docs/support/SupportManual/C00290881/C00290881.pdf, (Accessed August 2005)

"PKI: Future Trends", Silicon Trust website, http://www.silicon-trust.com/background/sp_pki_future_trends.asp, (Accessed August 2005)