IJCSN International Journal of Computer Science and Network, Volume 3, Issue 4, August 2014
ISSN (Online) : 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

A Review of Challenges and Solutions of Wireless Security

[1] Achi Ifeanyi Isaiah, [2] Agwu Chukwuemeka Odi

[1] Department Of Computer Science, Our Saviour Institute Of Science And Technology

[2] Department Of Computer Science, Ebonyi State University-Abakaliki

Abstract - The need for wireless connectivity has increasingly become the order of the day because of the convenience it offers to the end users. As a result of this every individual, organizations, ministries and so have preference for it. To this end, in recent years, most devices come with wireless LAN [5] which enables them to see and get connected to an existing wireless network. The growing corporate appetite for Internet, intranet and wireless LAN services will drive the need for advanced information security services as technologies for circumventing network security systems continue to keep pace with the technologies designed to defend against them. Because of this ever increasing awareness and demand for wireless network, there is need to secure, safeguard this wireless network to ensure the authorized users are the ones gaining access to it. In this paper, we will deliberate on the challenges users encounter in securing a wireless network with wireless devices and the solutions.

Keywords - *Wireless LAN, Wired Equivalent Privacy, Cryptography, Encryption, Biometrics, Network, Wireless Security, Algorithm, Authentication, VPNs, PKIs*

1. Introduction

Wireless data communications have transformed not only the business world but also the whole human society by improving efficiency, flexibility, convenience and above all productivity besides providing access to a flexible mobile user and device a time-independent connectivity. These days, companies and individuals have started to use wireless devices for important communications such as personalized email, mobile commerce activities, corporate data transmission and other net activities. Apart from voice communication, data communication is also being done through mobile devices. This is possible due to very high advancement going on in wireless technology industry [1],[8]. At the same time, as wireless platforms mature, grow in popularity and store valuable information, hackers are also stepping their evil efforts on these new gadgets. As any other medium of communication and commerce, wireless has not been spared of insidious attacks. The wireless industry has been hit particularly hard by the illegal use of resources and the violation of privacy and access to confidential data. One major reason for this insecurity is due to the fact that these tiny, Internet access-capable and intelligent devices were not designed at the beginning with security [6] aspect as a top priority. That means, security issues on most intelligent mobile and in-mobile devices was not considered initially where this wireless data communication network will be deployed.

Therefore, as a part of grand vision of ubiquitous computing, providing information and services on demand in secured manner for a mobile flexible user at a desired quantity and quality, at any location through these devices remains paramount. Wireless security such as with wireline security boils down to protecting information and preventing unauthorized system access.[6] The challenge here is to implement security in small-footprint devices with low processing power and small memory capacities and that use unreliable, low bandwidth wireless networks. This is because in the traditional wired LAN, security can be enforced by protecting and managing the workstations and physical links.

On the contrary, in the wireless LAN the communication is not through a physical link but through wireless channel; hence it is highly vulnerable to all kinds of security threats. In deploying wireless LAN on devices, it requires a software based solution to manage the channels and provision of needed security for data exchange. In this regard, wireless security has been an important area of product research and development.

Therefore, in this paper we x-rayed the major wireless technologies, security challenges and how they are implementing the security aspect.

2. Wireless Technologies and Security Flaws

2.1 LAN Standard

The IEEE 802.11 [5]wireless LAN standard is rapidly gaining popularity. The protocols, algorithms and technologies involved with improving the 802.11 standard security are complex and very independent. This technology's security mechanism is the wired equivalent privacy (WEP) protocol. Encrypting data with WEP protects the wireless link between clients and access points. Wireless network administrators provide a WEP-algorithm-based key for each authorized user, thereby denying access to anyone without an assigned key.

Flaws in the WEP algorithms used in these networks can open the wireless intranets to frauds of various types. If access to intranets using wireless Virtual Private Networks (VPNs) is not guarded adequately at the handset level using access passwords and other security mechanisms, technical frauds like cloning or handset thefts can leave corporate networks vulnerable[3],[12].

2.2 Wireless Application Protocol (WAP)

WAP-compliant devices can access the Internet resources. WAP specifies the Wireless Transport Layer Security (WTLS) protocol, which is similar to the Internet's transport layer security protocol. WTLS provides authentication [14], data integrity, and privacy services within wireless technologies' limited processing power, memory capacity and bandwidth. WTLS generally uses Ron Rivest Adi Shamir (RSA)-based cryptography and it can also use elliptic-curve cryptography (ECC), which provides a high level of security while demanding fewer computing and memory resources than other encryption approaches. Many e-commerce and corporate sites use Secure Socket Layer (SSL)-based security[15]. Therefore, a transmission to such a site from a WAP phone must first pass through a gateway that converts the encryption formatting from WTLS to SSL. During the conversion process, the message is very briefly unencrypted and hence interception by hackers is possible.

3. Types of Wireless Attacks

Wireless attacks can be divided into two categories: technical and subscription attacks.

Technical attacks include cloning and hacking. Using scanning equipments, the mobile serial numbers and/or equipment numbers of one mobile handset can be stolen and programmed into another handset. SIM cloning involves making replicas of SIM cards, which hold user subscription information. Other types of attack involve hacking into the carrier's systems to access and manipulate subscription records. With better authentication and encryption techniques being employed in digital networks, technical frauds like cloning and hacking are becoming relatively difficult to commit. However, newer technical developments such as Local Number Portability (LNP) and advanced roaming capabilities in the next-generation networks will open up newer opportunities for committing technical attack.

Compared to technical attack, subscription attack is more prevalent and is growing. False or stolen identities are used to acquire subscriptions that can never be properly billed to the defrauder. Technical developments like roaming are making the task of fraud avoidance even more difficult. In many instances, a fraud is committed with an intention to use the phone while roaming in a different network[17]. In such instances, it is difficult to detect the improper activity in time to apprehend the offender.

4. Wireless Security Techniques

Authentication keys are assigned to the handset or the SIM card. Only the mobile network authentication center and the mobile know about the key. Authentication is performed during call setup by exchanging secret data generated randomly using these keys. These are deployed in user mobile wireless devices[4].

Authentication - A key aspect of security for activities such as mobile commerce and mission-critical corporate communications is the ability to authenticate a message sender's identity. There are several methods to accomplish this using variations of wireless public key infrastructure (PKI) mechanism, which provides a set of technologies that relies on encryption and digital certificates[9]. The certificates are message attachments, issued by a certificate authority, that authenticate a sender's identity and provide encryption keys. PKI works with public-key cryptography, in which a certificate authority uses a single algorithm to create a public and private key pair[8]. The public key encrypts the message, and the private key decrypts it. Senders of digital certificates keep their private key secure but make the public key available to people with whom they communicate. Anyone with access to the public key can send an encrypted message, but only the certificate sender can decrypt it.

Digital signatures can be used to ensure secure transaction over the wireless environment using wireless Public Key Infrastructure (PKI). The E-Sign act that was enacted in 2000 guarantees legal validity to digital signatures. Digital signatures can now be used to ensure non repudiation in a court of law. The challenge here is to design PKI to work on wireless devices that have very low

throughput and computational power and to develop wireless PKI systems that can interact with their wireline counterparts. The wireless PKI (WPKI) protocol offers a slimmed-down version of PKI optimized for wireless communications.

Smart Cards - One can store PKI-based authentication information in smart cards that he can insert into a device-mounted reader. Smart cards have been used as subscriber identity module (SIM) cards in global system for mobile communication (GSM) phones and wireless identity modules in WAP-enabled phones.

Firewalls - Organizations can run Neomar's Enterprise Server (NES), which provides authentication for wireless devices, behind their firewalls. A company configures its secure enterprise router proxy to permit only specified handheld devices to contact the NES. Devices communicate with the server via a dedicated connection that eliminates the need to penetrate and thereby creating vulnerabilities in firewalls. A device sends a message through an encrypted tunnel via the service provider to a recipient's NES, where decryption takes place, thereby providing security for a transmission. The process is reversed when the NES initiates a transmission.

A **WAP gateway** can serve as the single point of entry for an enterprise's wireless systems. Companies can secure and monitor the gateway as they do in a traditional firewall[10].

Virtual Private Networks (VPNs) - VPNs provide security by creating an encrypted tunnel through the public Internet. This tunnel shields data from unauthorized access. It reduces costs by eliminating the need for companies to build secure private networks. Basic wireline VPN mechanisms can be used for wireless networks [13], clients and servers. Once a handheld device's VPN client obtains an IP address by connecting to the Internet, it can authenticate itself to a company's VPN server. The client and server then set up the encrypted tunnel through which they communicate [11].

The other viable techniques being employed or developed to tackle the problem of wireless attack include the following:

RF Fingerprinting -This technique involves measuring the output of the handset and comparing it against the stored fingerprint of the same mobile, as each handset has a slightly different output frequency profile. Technical frauds like cloning can be prevented using this practice[14].

Profiling - This technique is based on profiling the call usage based on such indexes as number of calls made in a given time period, length of calls made, origination and destination of calls, etc. If a particular handset deviates from the expected profile, an administrator is notified to investigate[18].

Biometrics - Biometrics uses a person's unique physical characteristics such as fingerprints, thumbprint, facial geometry, or retinal images to identify authorized users[15]. Biometrics also includes measured physical aspects of a user such as voice authentication, which analyzes voice to allow or reject access to the service. It is expected that Biometrics technology could be accurate and inexpensive enough for vendors to embrace it in the future[6].

Real-time Billing by Prepaid Cards - Billing calls as they happen in real time can help the carrier prevent recurring losses from accumulating over the month. Also, prepaid cards, although not fraud-proof, can help limit the losses to a certain amount only.

5. Research Scenario on Wireless Security

There are several new wireless-security standards under research and development.

- There is a standard called Pre-IKE Credential (PIC). Internet Key Exchange (IKE) protocol provides flexibility and ease of configuration to the IPsec (IP Security standard)[17]. A PIC-based system's authentication server would authenticate devices that are authorized to communicate with the system. The server would provide credentials to these devices, which could then authenticate themselves via IKE to a system's secure IPsec gateway[16].

- Texas Instruments (TI) has developed the Open Multimedia Applications Protocol (OMAP), a library of software from various vendors that will permit secure transactions on wireless devices that use TI's digital signal processors[20]. OMAP software would do memory and firewall protection, public- and private-key encryption, virus screening, and fingerprint-based biometric security. Mobile smart phone vendors are set to use OMAP in their products[19].

- Leading mobile phone makers such as Ericsson, Motorola, Nokia, and Siemens have formed an alliance called Mobile electronic Transactions (MeT) to develop standards for secure mobile activities. This initiative will enhance

interoperability among wireless products and technologies facilitating access to mobile Internet services, including mobile commerce.

6. Conclusion

All in all, the challenges and solutions of wireless security especially on mobile systems platform was discussed. Interestingly, it is a new area of research that is evolving as most corporate organization and individuals are embracing the wireless communication because of its' latent qualities of ease of access, anytime, anywhere including not restricting the user to time. However, security in wireless systems still remains elusive. Nowadays users can get the complete wireless-security packages from vendors such as Cisco Systems and 3Com instead of piecing together various technologies to get the security they wanted. The impending release of Third Generation (3G) network technology, which would standardize TCP/IP on mobile systems, promises to permit strong, end-to-end SSL security, which functions only over IP networks. However, wireless security faces a number of hurdles, especially the challenge of adapting wireless technologies to work with the mobile world's more constrained resources. In spite of all the developments in fraud avoidance and detection, wireless fraud is expected to rise due to the rate at which wireless adoption in increasing. However, vendors and users alike hope that security will keep pace as other aspects of wireless technology continue to advance.

References

[1] P. Castro, P. Chiu, T. Kremenek, and R. Muntz, "A probabilistic room location service for wireless networked environments," in Proc. 3rd Int. Conf. Atlanta Ubiquitous Computing (Ubicomp), vol. 2201, Sep. 2001,pp. 18–34.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE Symp. Res. Security and Privacy, May 2003, p. 197.

[3] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 1187–1192.

[4] Y.-C. Hu and H. J. Wang, "Location privacy in wireless networks," in Proc. ACM SIGCOMM Asia Workshop, 2005.

[5] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki.Enhancing Wireless Location Privacy Using Silent Period. In Proceedings of the IEEE Wireless Communications and Networking Conference(WCNC), 2005.

[6] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2004.

[7] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks. In Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN), 2005.

[8] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. In Proceedings of WMASH, 2003.

[9] Kun Sun, Peng Ning, Cliff Wang, An Liu, and Yuzheng Zhou. Tinysersync: Secure and resilient time synchronization in wireless sensor networks. In Proceedings of the ACM Conference on Computer and Communications Security, 2006.

[10] Kun Sun, Peng Ning, and Cliff Wang;. Secure and resilient clock synchronization in wireless sensor networks. IEEE Journal on Selected Areas in Communications, 24(2):395–408, 2006.

[11] M. Cagalj, S. Capkun, RamKumar Rengaswamy,Ilias Tsigkogiannis, M. Srivastava, and Jean-Pierre Hubaux. Integrity (I) codes: message Integrity Protection and Authentication Over Insecure Channels. In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, 2006.

[12] S. ˇCapkun, L. Butty´an, and J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In Proceedings of the ACM workshop on Security of Ad Hoc and Sensor Networks (SASN), Washington, USA, October 2003.

[13] Y.C. Hu and H. J. Wang. Location Privacy in Wireless Networks. In Proceedings of the ACM SIGCOMM Asia Workshop, 2005.

[14] S. ˇCapkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In Proceedings of the IEEE Conference on Computer Communications (InfoCom), 2005.

[15] M. Sichitiu and C. Veerarittiphan. Simple, accurate time synchronization for wireless sensor networks. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), 2003.

[16] Y. Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu. Secure localization and authentication in ultra-wideband sensor networks. IEEE Journal on Selected Areas in Communications, 24(2), February 2006.

[17] G. Jiang and G. Cybenko, "Temporal and spatial distributed event correlation for network security", In American Control Conference, 2004.

[18] B. Harris and R. Hunt, "TCP/IP security threats and attack methods", In Computer Communications, 1999.

[19] T. Dimitriou, G. Karame and I. Christou, "SuperTrust: A Secure and Efficient Framework for Handling Trust in Super Peer Networks", In Proceedings of ACM PODC, 2007.

[20] G. Karame, I. Christou and T. Dimitriou, "A Secure Hybrid Reputation Management System for Super-Peer Networks", In Proceedings of IEEE CCNC, 2008.