Wireless Networks Auditing

FLOAREA NASTASE
PAVEL NASTASE
Department: Management Information Systems
University: Academy of Economic Studies
Address: Bucuresti, Piata Romana, nr. 6, Sector 1, 010374, OP 22
COUNTRY: ROMANIA

Abstract: Wireless networking increases the flexibility in the home, work place and community to connect to the Internet without being tied to a single location. Home users have embraced wireless technology and businesses see it as having a great impact on their operational efficiency. However undeniable the benefits of wireless networking are, there are additional risks that do not exist in wired networks. It is imperative that adequate assessment and management of risk is undertaken by businesses and home users. In this paper we have discussed some of the key concerns surrounding the security of wireless networks. We tray to analyse some aspects concerning the audit process in order to increase the reliability, availability and security when using wireless networks.

Keywords: security, WEP, WLAN, WPA, risk assessment, risk management, threat analysis.

1 Introduction

The wireless computing refers to the ability of computing devices to communicate in a form to establish a local area network without cabling infrastructure (wireless), and involves those technologies converging around IEEE 802.11x and other wireless standards and radio band services used by mobile devices.

The mobile computing extends this concept to devices that enable new kinds of applications and expand an enterprise network to reach places in circumstances that could never have been done by other means. It is comprised of PDAs (personal digital assistants), cellular phones, laptops and other mobile and mobile-enabled technologies [1] .

Wireless nerworks including the wireless computing and the mobile computing offer (organizations) business and users many benefits, such as portability, flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs.

2 Advantages of Wireless Nerworks

Wireless nerworks offer users and organizations a number of advantages, including:

User Mobility. Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN and network resources;

Rapid Installation. The time required for installation is reduced because network connections can be made without moving or adding wires or pulling them through walls or ceilings, or making modifications to the infrastructure cable plan. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules;

Flexibility and increased productivity - Enterprises can also enjoy the flexibility of installing and removing WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, meeting, or Continuity of Operations (COOP) activities. Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location;

Scalability. WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area;

Convenience - The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant;

Deployment - Initial setup of an infrastructure-based wireless network requires little more than a single access point. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building);

Expandability - Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring;

Cost - Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables. Wi-Fi chipset pricing continues to come down, making Wi-Fi a very economical networking option and driving inclusion of Wi-Fi in an ever-widening array of devices.

The disadvantages of wireless nerworks include: no physical control over network connections, weak built-in security measures, security complacency, unmonitored, untrusted connection to network core.

Using this advantages wireless nerworks are now becoming a viable alternative to traditional wired solutions in some cases. For example, hospitals, universities, airports, hotels, and retail shops are using wireless technologies to conduct daily business operations. In the same time for a given networking situation, wireless nerworks may not be desirable for a number of reasons.

2 Wireless Netorks Architecture

Although there are a number of wireless technologies and devices available on the market, the wireless networks include two fundamental components:
- *Station (STA)* is a wireless endpoint device (client devices or base station); typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with wireless capabilities.
- *Access Point (AP)* connects STAs with a distribution system (DS), which is typically an organization's wired infrastructure. APs can also logically connect wireless STAs with each other without accessing a distribution system.

In practice, a STA is authenticated to an AP simply by providing the following information:
- *Service Set Identifier* (SSID) for the AP. The SSID is a name assigned to a WLAN; it allows STAs to distinguish one WLAN from another. SSIDs are broadcast in plaintext in wireless communications, so an eavesdropper can easily learn the SSID for a WLAN. However, the SSID is not an access control feature, and was never intended to be used for that purpose.
- *Media Access Control* (MAC) *address for the STA*. A MAC address is a unique 48-bit value that is assigned to a particular wireless network interface by the network card's vendor. Many implementations of IEEE 802.11 allow administrators to specify a list of authorized MAC addresses; the AP will permit devices with those MAC addresses only to use the WLAN. This is known as MAC address filtering. However, since the MAC address is not encrypted, it is simple to intercept traffic and identify MAC addresses that are allowed past the MAC filter. Unfortunately, almost all WLAN adapters allow applications to set the MAC address, so it is relatively trivial to spoof a MAC address, meaning attackers can gain unauthorized access easily.

There are many types of wireless networking [3]:
- *A Wireless personal area network* (WPAN) is a small-scale wireless network that require little or no infrastructure and typically used by a few devices in a single room instead of connecting the devices with cables. The common WPAN technologies are: IEEE 802.15.1 (Bluetooth), IEEE 802.15.3 (High-Rate Ultrawideband; WiMedia, Wireless USB) and IEEE 802.15.4 (Low-Rate Ultrawideband; ZigBee).
- *The Wireless local area networks* (WLAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility and network access. The common WLAN standards are IEEE 802.11, also known as Wireless Fidelity (Wi-Fi) and High Performance Radio Local Area Network (HIPERLAN).

ISBN: 978-960-6766-76-3 ISSN 1790-5109

- *The Wireless metropolitan area networks* (WMAN) can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas. The most commonly used standard for WMANs is IEEE 802.16, better known as World Interoperability for Microwave Access (WiMAX).
- *The Wireless wide area networks* (WWAN) connect individuals and devices over large geographic areas. WWANs are typically used for cellular voice and data communications, as well as satellite communications.

There are two types of general wireless network topologies, *infrastructure* and *ad hoc*. Infrastructure based networks encompass WLANs, cellular networks, and other network types. These types of networks require the use of an infrastructure device, an AP for example, to facilitate communication between client devices. Ad hoc networks are designed to dynamically connect devices such as cell phones, laptops, and PDAs to each other without the use of any infrastructure devices (fig. 1). These networks are termed ad hoc or peer-to-peer (P2P) because of the network's dynamic topology. Whereas infrastructure networks use a fixed network infrastructure, ad hoc networks maintain dynamic network configurations, relying on peer devices to manage network communication; no infrastructure-based devices are involved in the network.

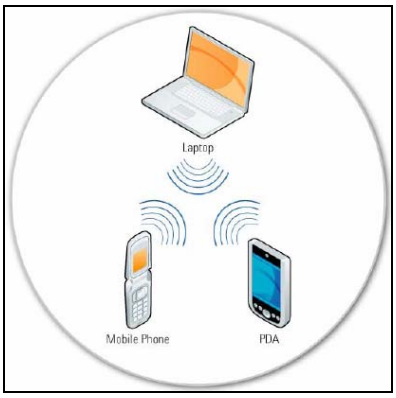

Fig. 1 Wireless network ad hoc topology (source:[3])

In infrastructure topology, an IEEE 802.11 WLAN comprises one or more Basic Service Sets (BSS), the basic building blocks of a WLAN (fig. 2). A BSS includes an AP and one or more STAs. The AP in a BSS connects the STAs to the DS. The DS is the means by which STAs can communicate with an organization's wired LANs and external networks, such as the Internet.

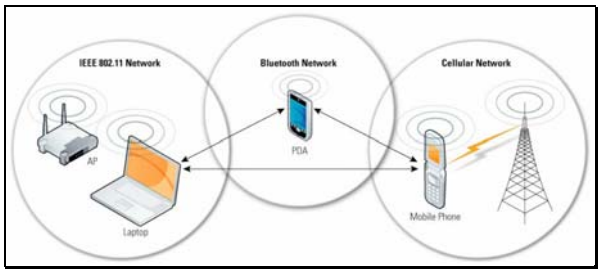

Fig. 2 Wireless network infrastructure topology (source:[3])

3 Risks Analysis in Wireless Netorks

The increasing use of wireless technology and the proliferation of new portable devices with Internet browsing capabilities expand the physical frontiers of organisations and requires the IS auditor to understand this technology to identify the associated risks.

Specific threats and vulnerabilities to wireless networks include the following:
- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.
- Malicious entities may gain unauthorized access to an organization's computer network through wireless connections, bypassing any firewall protections.
- Sensitive information that is transmitted without being encrypted (or that is encrypted with weak cryptographic techniques) may be intercepted and disclosed.
- DoS attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Malware may corrupt data on a wireless device and subsequently be introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other organizations for the purposes of launching attacks and concealing their activities.

ISBN: 978-960-6766-76-3

ISSN 1790-5109

- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use rogue wireless networks deployed within an organization to gain access to the organization's network resources.
- Internal and client device-based attacks may be possible via ad hoc transmissions.

The major vulnerabilities result from the users of wireless technologies not addressing the following:
- Reliance on WEP(Wired Equivalent Privacy) for encryption;
- Wireless networks not being segregated from other networks;
- Descriptive SSID or AP names being used;
- Hard-coded MAC addresses;
- Weak or nonexistent key management;
- Beacon packets that have not been disabled or are "enabled";
- Distributed APs;
- Default passwords/IP addresses;
- WEP weak key avoidance;
- DHCP being used on WLANs;
- Unprotected rogue access points;

Wireless technologies typically need to support the most common security objectives: confidentiality, integrity, availability and access control. Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security. Once the risk assessment is complete, the organization can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The organization should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing.

The risk analysis include:
- *Privacy* - An important component when sensitive information (such as, credit card numbers, financial details and patient records) is transmitted. Privacy protocols and related procedures are very important as wireless transmissions cannot be protected from hacker access by other means (such as physical access controls).
- *Authentication* - Can be ensured by using a token or certificate that can be verified by a recognised certification authority (CA)
- *Two-factor authentication* - Used to verify both the device and the identity of the end user during a secure transaction (i.e., confirms that both the device and the user are authorised agents). Two-factor authentication is used to deny network access from stolen or lost devices.
- *Data integrity* - Involves the detection of any change to the content of a message during the transmission or while stored on the mobile device
- *Nonrepudiation* - A system to prevent users from denying they processed a transaction. Nonrepudiation requires a successful user authentication, and establishes a credible and legally enforceable record of the user that originated a transaction.
- *Confidentiality and encryption* - Involves transformation of data using algorithms to avoid unauthorised users or devices that could eventually read and understand it. Encryption technologies rely on keys to encode and decipher pieces of data during transmission. Procedures for key distribution and safekeeping should also be considered.
- *Unauthorised use* of equipment and communications, including the risk of using unauthorised access to the Internet to break into a third-party's networks (subjecting the entity to potential legal liability)

4 Auditing Process

Auditing are an essential for checking the security of a wireless network using wireless network analyzers and other tools and for determining corrective action. According to the objectives and scope of the audit, prezented in ISACA IS Standards, Guidelines and Procedures for Auditing and Control Professionals, the IS auditor should include in the review security areas, such as:
- Communications (covering risks such as sniffing and denial-of-service, and protocols such as encryption technologies and fault tolerance);
- Network architecture;
- Virtual private networks;
- Application delivery;
- Security architecture and security awareness;
- User and session administration (covering risk such as spoofing, loss of integrity of data);
- Physical security;
- Public key infrastructure;
- Backup and recovery procedures;
- Operations (such as incident response and back-office processing);
- Security software (such as IDS, firewall and antivirus);
- Business contingency planning.

ISBN: 978-960-6766-76-3

ISSN 1790-5109

Commonly used types of *security controls* for wireless networks are as follows:
- *Encryption of communications*. Using cryptography to encrypt wireless communications prevents exposure of data through eavesdropping.
- *Cryptographic hashes for communications*. Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit, either intentionally or unintentionally. This prevents masquerading and message modification attacks.
- *Device authentication and data origin authentication*. Authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading.
- *Replay protection*. There are several options to implement the detection of message replay, including adding incrementing counters, timestamps, and other temporal data to communications.
- *Physical security*. Limiting physical access within the range of the wireless network prevents some jamming and flooding attacks.
- *Wireless intrusion detection and prevention systems* (IDPS). Wireless IDPSs have the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Wireless IDPSs are most commonly used for IEEE 802.11a/b/g WLANs, but they are also available for Bluetooth networks, and they can also detect rogue networks that use uncommon frequencies, such as those used in other countries, in an attempt to avoid detection.

An assessment procedure in the audit process consists in a set of assessment objectives, each with an associated set of assessment methods and assessment objects [4]. An assessment objective includes a set of determination statements related to the particular security control under assessment.

For example, the organization scans for vulnerabilities in the information system or when significant new vulnerabilities potentially affecting the system are identified and reported. Vulnerability scanning is conducted using appropriate scanning tools and techniques. Vulnerability scans are scheduled in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 provides guidance on patch and vulnerability management.

In addition to these controls, organizations need to create a wireless network security policy that addresses each type of wireless network technology of interest. The policy should identify such things as who may or may not use the technology, who may install equipment, where the technology may be used, what the physical security requirements are for the technology, what types of information may or may not be sent and received through the technology, how security incidents should be reported, how wireless devices should be protected, how transmissions should be protected (e.g., encryption requirements), and how often the security of the implementation should be assessed. Organizations also need to ensure that all critical personnel are properly trained on the use of the wireless technology. Network administrators need to be fully aware of the security risks that the networks and associated devices pose, and they need to know what steps to take in the event of an incident. Users also need to be aware of their responsibilities.

5 Tools for Auditing

BlueAuditor is a private area network auditor and easy-to-use program for detecting and monitoring Bluetooth devices in a wireless network. It can discover and track any Bluetooth device within a distance between 1 and 100 meters and display key information about each device being detected as well as the services device provided. With the growing popularity of the Bluetooth technology, BlueAuditor will enable network administrators to effectively audit their wireless networks against security vulnerabilities associated with the use of Bluetooth devices. BlueAuditor enables the user to save the data of the detected Bluetooth devices in an .xml file and supports the most Microsoft Bluetooth drivers available on the market. All the mentioned features are provided with a user friendly graphical interface.

NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 98 on up to Windows Vista (under compatibility mode). A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating

system. The program is commonly used for: wardriving, verifying network configurations, finding locations with poor coverage in a WLAN, detecting causes of wireless interference, detecting unauthorized ("rogue") access points, aiming directional antennas for long-haul WLAN links.

6 Conclusion

The audit review process provides the closed-loop cycle of continuous improvement that is necessary in today's wireless applications. Auditors must understand that the solution is not a quick fix and will build over time with the awareness of all employees and the unfettered support of management. One should not forget that auditors provide assurance to various stakeholders, and client management is one significant stakeholder.
While wireless networks provide a great number of advantages such as: mobility, rapid installation, flexibility and increased productivity, scalability, expandability, they also are a source of additional risk exposures.

Strong authentication, wireless intrusion detection and prevention systems procedures are likely to keep intruders out of a system. In the event that unauthorized users enter the network, compromising confidential data would be a serious concern for the organization. The best protection against this exposure can be obtained using encryption technology. Several affordable tools are available to the auditor to verify accessibility of wireless networks and whether encryption is used in data transmission.

In looking for assurances in wireless network security, the auditor should take a defense-in-depth approach. For example, to the extent possible, the wireless network should be isolated from other networks, and the resources (including data) available to it should be restricted to what is absolutely required.

References:

[1] http://www.isaca.org, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, ISACA, 2008

[2] Pauline Bowen, Joan Hash, Mark Wilson, Nadya Bartol, Gina Jamaldinian, *Information Security Handbook: A Guide for Managers*, NIST, 2006

[3] Karen Scarfone, Derrick Dicoi, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth* (DRAFT), NIST Special Publication 800-48r1, 2007

[4] Ron Ross, Arnold Johnson, Stu Katzke, Patricia Toth, Gary Stoneburner, George Rogers, *Guide for Assessing the Security Controls in Federal Information Systems*, NIST Special Publication 800-53A, 2007

[5] Năstase Floarea, Năstase Pavel, Risk Management for e-Business, Informatics in Knowledge Society, *The Eigth International Conference on Informatics in Economy*, ASE Publishing House, Bucharest, pp. 222-227, 2007, ISBN 978-973-594-921-1

[6] Năstase Floarea, Năstase Pavel, Security Controls to Protect Information Systems, *Proceedings of the 3rd International Conference - Economy and Transformation Management*, Editura Universităţii de Vest, Timişoara, pp. 826-834, 2006, ISBN 1842-4880

[7] Năstase Pavel, Năstase Floarea, Şova Robert, IT Audit Trends within Framework of Balkan Countries, *The Balkan Countries' 1st International Conference on Accounting and Auditing (BCAA)*, 8-9 March 2007, Edirne - Turkey, pp. 41-51, ISBN 978-975-0960-0-2