Managing Wireless Security in an Organization

Muhammad Jahanzaib Khan

Abstract:- The adoption of wireless mobile computing solutions has been of benefit to government institutions, commerce and learning institutions among others. This is because of the higher customer satisfaction and higher productivity that have been made possible. A wireless network is a computer network, which is not connected by cables. This assists business enterprises and organizations by facilitating a flexible environment and avoids the capital cost of installing cabling in a building. The network is implemented by use of radio waves for transmission. This paper will discuss how to handle wireless security in an organization.

Keywords:- Wireless Networks, Wireless Security

INTRODUCTION

Currently, about 150 million organizations worldwide use wireless technologies. The technology is implemented to gain flexibility of infrastructure, reduce capital expenditure gain advantages over competitors and to solve business problems. In academic institutions such as universities, wireless technology is widely used. Lecturers and students use wireless network to access information over the internet. Business people use the potential to increase production, generate more sales, as well as to interact with the customers better. Wireless networks allow for more adaptable in office environment configurations (Negrino and Smith 26). Wireless networks have a number of components. One of the components is access points which are the equivalent of a hub in a wired network. The access point is connected to a wired backbone through an Ethernet cable and communicates with the attached devices through an antenna. The unit uses the 802.11 standard modulated techniques (Potter and Fleck 9). In a normal configuration, the access point shows its presence to the wireless uses. The second component is NIC (Network Interface Cards) of the device. The unit scans the frequency spectrum availability for connectivity. After connectivity, it then associates with the wireless client or access point. The card allows users to connect automatically to a wireless network and allow internet access. These components are connected in different configurations. These configurations include infrastructure, micro cells, and independent networks (Ross 32). Controls of access to a wireless network is difficult to control and as a result are more prone to malicious attacks than the wired equivalent. Hackers execute wireless attacks utilizing free software, off the shelf hardware, to create simple man in the middle and denial of service attacks. Organizations are motivated to implement effective security in a wireless network, by the need to protect their information and services and also by regulatory compliance. Examples of the types of regulations used by organizations include SOX (Sarbanes-Oxley), HIPAA (Health Insurance Portability and Accountability Act), data security standard, and PCI (Payment Card Industry). Many organizations instigate policies to ban installation of unauthorized Aps in an attempt to control access to the networks. However, some organizations do not have the necessary resource to enforce these policies. Some organizations use manual security scans to resolve network threats. The disadvantages of this method include the limited returns to the organization and time that is taken by these processes. Additionally, organizations use Airwave RAPIDS detection to manage compliance and enforce security policy. RAPIDS are Airwave wireless features from Aruba networks. The feature is used to manage service quality for mobile users by delivering the core capabilities. RAPIDS automatically detect unauthorized access points using existing authorized APs to scan the RF spectrum environment. RAPIDS provide a wireless intrusion prevention module in their routers. This offers the customers a protection solution referred to as WIPS. To scan for any authorized access and air spaces for IDS events, RAPIDS uses existing authorized access points within the range. These devices take care of wired traffic and correlating wireless. The information corrected is reported to RAPIDS for confirmation. Likewise, RAPIDS uses HTTP and SNMP fingerprint scans which allows the system to scan the IP addresses within a specific range. RAPIDS interrogates a suspicious device, determine its OS and other available information to determine rouge devices. This helps organizations to identify potential threats, risk mitigation and reduces false-positives. Frameworks are used to determine if the device is rogue (Goldsmith 12). When managing, implementing, designing and planning network communications, security is a vital concern. Poor security in an organization exposes company information to threats. Wireless network represent an entry point for attacks, which can cause the entire network to collapse. Wireless radio signals may extend beyond the physical boundaries in a building. These transmissions can extend to public places such as other buildings, parks, and roads. This exposes the network to hackers who can then access company information. The capability of the hacker is enhanced by use of free software's and hardware's which overcome the WEP encryption capabilities. Wireless networks are exposed to the unapproved deployment of access points. Students and lecturers may not wait for the IT department to carry out network repairs or the installation of additional access points. This leads to a number of challenges to the corporate network such as equipment incompatibility. Likewise, it may also lead to the interruption of the wireless network. Currently, the majority of the laptops purchased have WIFI capabilities. This has an added advantage to hackers in accessing organization data even if the device has never been used to receive wireless transmissions (Tse et al 69). There are three different threats that affect wireless network in different organizations. They include Eavesdropping, spoofing and denial of service. Eavesdropping is the attack that affects the confidentiality of the data being transmitted over the network by a third party.. Spoofing is where the attacker gains access to resources and privileged data within an organization network. Most organization networks use 802.11, which do not authenticate the MAC (Media Access

Control) of the network frames. Hackers hijack sessions and the MAC address since they do not require Authentication for the users. Denial of service is the attack where the intruders flood the network with invalid messages, which consumes resources and affects the availability of network resources. Wireless networks are more venerable to denial of service attacks than a wired network. In addition to the above problems, this is also due to the low-bit rates within the network. Use of powerful transceiver may also make the wireless network unable to communicate (Rhoton 37). According to the IBM Corporation in 2002, there are different ways to manage wireless networks in a learning institution. One of the ways is the use of WEP (Wired Equivalent Privacy). WEP is a standard encryption process for wireless networks. WEP is a system from the IEEE 802.11 standard, which is a data encryption system and user authentication to overcome threats. To provide security, data over the air is encrypted such that only receivers with the correct encryption key can decrypt the information. WEP uses a cyclic redundancy code (CRC-32), encryption algorithm and a shared secret key. WEP supports three different secret keys with key IDS 0 to 3. The keys are shared among individuals in the wireless network. To achieve network security WEP operates on MPDUs (MAC Protocol Data Units) packet fragments. To protect information, an ICV (integrity check value) is performed over MPDU data. ICV allows the receiver to detect forgery. WEP selects a 24-bit an initialization vector and a base key (Abrams et al pp.98-99). However, despite WEP giving protection from attacks, it is venerable to attacks by hackers. First, WEP has no forgery protection (Gast 60). Secondly, WEP does not offer protection against replays. Forgeries can be created without changing the existing data by recording the packets and then retransmitting them later. Replays are used to derive information about data and encryption key used. Thirdly, WEP allows attackers to decrypt information by using initialization vectors. In addition, data collection from the environment allows attackers to attack information passed through the network (Rappaport 7). WPA2 (**W**i-Fi **P***rotected* **A***ccess* **2)**, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1 x-based authentications. *[Adapted from* Wi-Fi.org*]* There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA. The second way to manage wireless networks is by changing the SSID default. Service Set Identifier is uniquely attached to the header of the packets over a wireless network. An SSID acts as a searchable wireless network (Geier). This mechanism provides a security mechanism in the absence of activating the security options. During network configuration, the administrator is required to change the SSID password for maintain security. The third way is utilizing a VPN (Whitson 57). A VPN authenticates users from entrusted places and encrypts their communication. Wireless authentication is run in a common switch to provide security for wireless network on the same VPN server. The fourth way is the use of Dynamic Host Configuration Protocol. DHCP assigns an IP addresses automatically to user devices. However, DHCP does not recognize a hacker from a legitimate user. To overcome this, static IP addresses are assigned and DHCP is disabled hence preventing hackers from obtaining genuine IP addresses. The fifth way is that wireless networks should be placed near firewalls to protect against attackers accessing corporate information (Molisch pp 2-4). The Firewall is configured with the IP and MAC addresses. In addition, the IP addresses are spoofed hence making it difficult for hackers. The sixth way is to minimize radio waves in non-users' areas. Antennas are oriented to prevent them from covering areas outside the boundaries. This will enhance the security of the network in the organization (Borisov Pp.23-25). According to Knowledge Systems (UK) Ltd 2002, there are a number of tools that can be used to minimize security threats on a WLAN. One of the tools is AirDefence (AirDefense 10). This is a system that detects attacks and protects the network from hackers and intruders. Likewise, the system assists wireless management in an organization. The system provides robust wireless management, which allows users to enforce, monitor, and understand the network. The second tool used is Isomair wireless Sentry. The tools monitor the air space using sophisticated technology to identify insecure access points. The tools also inform network managers when threats occur in the network. The third tool is WSA (Wireless Security Auditor). The tools assists network administrators in automatically auditing a wireless network from a proper security configuration. These tools run on the Linux operating system (Weeks et al 20).

CONCLUSION

Wireless networks provide an alternative, flexible network infrastructure in an organization as compared to wired networks. WLAN is beneficial to many organizations worldwide since it provides for reduced capital investment and convenience in access to company information. Wireless networks components include access points and NIC (Network Interface Cards). Threats that affect wireless network in organizations include Eavesdropping, spoofing and denial of service. Different ways to manage wireless networks in a learning institution include use of WEP (Wired Equivalent Privacy), changing the SSID default, utilizing a VPN, use of Dynamic Host Configuration Protocol, placing wireless networks near firewalls and minimizing radio waves in nonuser's areas. Tools that minimize security threats of WLAN include AirDefence, Isomair wireless Sentry and Wireless Security Auditor. WEP is venerable to attacks since it has no forgery protection, it does not offer protection against replays, and it allows attackers to decrypt information by using initialization vectors.

REFERENCES

[1] Abrams, Marshall D., Jajodia, Sushil G., and Podell Harold J. Information Security: An Integrated Collection of Essays, in IEEE Computer Society Press, Los Alamitos, CA: USA. 1995.

[2] AirDefense, Inc. Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise. 2002: Pp.9-10.

[3] Borisov, Nikita, Goldberg, Ian and Wagner, David. Security of the WEP Algorithm.

[4] Computer Security Research Centre, National Institute of Standards and Technology. Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publications. 2002. 23-25.

[5] Geier, Jim. 802.11 Security Beyond WEP. 28 Oct. 2002. August 30, 2011 http://www.80211planet.com/tutorials/article.php/1377171

[6] Gast, Matthew. 802.11 Wireless Networks: The Definitive Guide, Second Edition. Sebastapol, CA: O'Reilly & Associates, Inc., 2005: pp.50-60.

[7] IBM Corporation. Wireless Security Auditor (WSA) 30 Oct. 2002. August 30, 2011 http://researchweb.watson.ibm.com/gsal/wsa/Isomair.com.

[8] Goldsmith, Andrea. Wireless Communications. Cambridge University Press. 2005. Pp.12-15.

[9] Knowledge Systems (UK) Ltd. Wireless LAN Security Issues. (28 Oct. 2002). August 30, 2011 http://www.ksys.info/wlan_security_issues.html

[10] Isomair Security for Wireless World. (30 Oct. 2002). August 30, 2011 http://www.isomair.com/products.html

[11] Molisch, Andreas. Wireless Communications. Wiley-IEEE Press. 2005: Pp2-4.

[12] Negrino, Tom and Smith, Dori. Mac OS X Unwired. Sebastopol, CA: O'Reilly & Associates, Inc., 2003. pp.24-26.

[13] Rappaport, Theodore. Wireless Communications: Principles and Practice. Prentice Hall. 2002. Pp.5-7.

[14] Rhoton, John. The Wireless Internet Explained. Digital Press. 2001. Pp.33-37.

[15] Tse, David; Viswanath, Pramod. Fundamentals of Wireless Communication. Cambridge press, 2005. pp.65-69.

[16] Potter, Bruce and Fleck, Bob. 802.11 Security. Sebastopol, CA: O'Reilly & Associates, Inc.2002. Pp.5-9. Ross, John.

[17] The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless, Second Edition. San Francisco, CA: No Starch Press. 2008. Pp.28-32.

[18] Trèek, Denis. An integral framework for information systems security management.

[19] Computers & Security. Vol.22. New York: Macmillan, 2003. pp.337-360.

[20] Weeks, Roger et al. Linux Unwired. Sebastopol, CA: O'Reilly & Associates, Inc., 2002. pp.18-20.

[21] Whitson, G. Computer security: theory, process and management, J. Comput. Small Coll, 18. (2003): 57-66.