Modelling Wireless Local Area Networks (LANs) Security

Sarumi J.A. (PhD) & Danso, J.
Dept of Computer Science, Lagos State University of Science & Technology, Ikorodu, Lagos State, Nigeria
Faculty of Compoutational Sciences & Informatics, Academic City University College, Accra, Ghana
E-mails: sarumi.j@mylasustech.edu.ng & joseph.danso@acity.edu.gh

ABSTRACT

Emergency of the wireless networking standard (e.g. IEEE 802.11) has contributed to the popularity of wireless local area network (LAN) deployment in many organizations. While wireless LAN provides greater mobility and flexibility, it also poses security risks to the organization. As many organizations have implemented wireless networks and as the numbers continues to grow, it becomes crucial for them to learn and understand the types of threats in wireless LANs. The objective of 'Wireless Local Area Network (LAN) Security Guideline' is to guide organizations in securing their wireless LANs. The Guideline provides recommendations on three security controls that organizations should implement. Security policies and procedures related to wireless LANs should be developed, documented, approved and maintained based on security requirements, best practices and agreed fundamental guidelines set forth by organizations. A policy is typically a document that outlines overall intention and direction as formally expressed by management Security is not a task; it is a continuous process that every employee in organizations should understand and undertake in their job functions. To ensure adequate security in wireless LANs, senior management should play significant roles in network security especially related to wireless networks. Like most advances, wireless LANs pose both opportunities and risks. The technology can represent a powerful complement to an organization's networking capabilities, enabling increased employee productivity and reducing IT costs. This article x-rays wireless LAN Security and associated Issues

Keywords: ICT, LAN, Modelling, Organization, Sensors, Guidelines, Technology

CISDI Journal Reference Format
Sarumi, J.A. & Danso, J. (2022): Modeling Wireless Local Area Network (LAN) Security. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 1, Pp 9-16.. DOI: 10.22624/AIMS/CISDI/V13N1P2.
Available online at www.isteams.net/cisdijournal

1. INTRODUCTION

The emergence of the wireless networking standard (e.g. IEEE 802.11) has contributed to the popularity of wireless local area network (LAN) deployment in many organizations. While wireless LAN provides greater mobility and flexibility, it also poses security risks to the organizations. The 'Wireless Local Area Network (LAN) Security Guideline' focuses on information security issues in wireless LAN, and recommends a set of security controls to help organizations secure their wireless LANs.

There are 3 aspects of security controls described in this Guideline:

1. **Management, Technical and Operational controls. Management controls:** For securing wireless LAN involve senior management's support i.e. defining roles and responsibilities, producing a comprehensive set of security policies and procedures, and conducting risk assessments and wireless network assessments.

2. **Technical controls:** Involves the use of hardware and software solutions in securing the wireless LAN environment. Wireless client protection, access points protection, wireless encryption, radio frequency interface monitoring, wireless equipment inventory, and wireless connectivity management are included in technical controls.
3. **Operational controls:** include physical and environmental protection, human resource security, training and awareness programs, patch management, and an incident handling and response management. Organizations are recommended to combine management controls with operational and technical controls.

These three security controls, when adequately implemented and configured, can be effective in reducing information security risks in organizational wireless LANs. A wireless LAN is a flexible data communications system implemented as an extension to, or as an alternative for, a wired network. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility. Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for many organizations and home users. Wireless LAN users can access shared information without looking for a place to plug in, and network administrators can set up networks without installing physical cables. However, organizations should be aware of threats in wireless LANs, and learn how to manage or reduce information security risks in wireless LANs effectively

1.1 Objective

The objective of 'Wireless Local Area Network (LAN) Security Guideline' is to guide organizations in securing their wireless LANs. The Guideline provides recommendations on three security controls that organizations should implement. The recommendations are in line with relevant standards and findings from vulnerability assessments. This Guideline provides advice and guidance only; as such no penalties are imposed for organizations that do not follow them. It is also not intended to replace any existing information on security standards and/or guidelines produced by standards organizations or regulators.

1.2 Scope of Studies

The scope of this Guideline is three security controls: Management, Technical, and Operational control, which organizations should implement in securing their wireless LAN. The three security controls discussed in this Guideline are directly related to information security aspects in wireless LAN only. The wireless LAN referred to in this guideline is the IEEE 802.11 which denotes a set of wireless LAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802) [1]. However, certain organizations may have additional or specific requirements (which are derived from international, local, organizational, and/or government regulations) that are applicable to them. These additional requirements are not within the scope of this guideline.

1.3 Target Audience

This Guideline is recommended for the following:

- ✓ Organizations that plan, develop, implement or assess their wireless LAN.
- ✓ Individuals who are system and network administrators, who design, deploy, administer and maintain organisational wireless LANs.
- ✓ Individuals who are information security or network security personnel with information system and monitoring responsibilities on organisational wireless LANs.
- ✓ Individuals who are internal and external auditors, information security officers or security consultants who perform security assessments on organisational wireless LANs.

1.4 Terms and Definitions

Access Point
A device that logically connects wireless clients operating in an infrastructure to one another, and provides access to the distribution system, if connected, which is typically an organization's enterprise wired network.

Ad-Hoc Network
A wireless network that dynamically connects wireless clients to each other without the use of an infrastructure mode's device, such as an access point.

Attacker
Someone who breaks into someone else's computer system, often a network, bypasses passwords or licenses in computer programs, or in other ways intentionally breaches computer security. Attackers can do this for profit, maliciously, for an altruistic purpose or cause, or because the challenge is there. Also known as cracker.

Computing Related Equipment
Computer, network, telecommunications and peripheral equipment that support the information processing activities of an organization. Examples of computing related equipment are computers, personal digital assistants (PDAs), thumb drives, printers, video cameras, game consoles and multimedia devices.

Firewall
A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. The term also implies the security policy that is used with the programs.

Information and Communication Technologies (ICT) System
A set up consisting of hardware, software and firmware of computing related equipment, and the people who use them. An ICT system includes any computing related equipment or other electronic information handling systems and associated equipment, or interconnected systems that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information. ISO/IEC 27001:2005 Information Security Management Systems 7 NIST SP 800-48r1 Guide to Securing Legacy IEEE 802.11 Wireless Networks 8 NIST SP 800-83 Guide to Malware Incident Prevention and Handling 9 ISO/IEC 27001:2005 Information Security Management Systems 10 ISO/IEC 27001:2005 Information Security Management Systems 11 ISO/IEC 27001:2005 Information Security Management Systems

Information Security
Preservation of confidentiality, integrity and availability of information; other properties such as authenticity, accountability, non-repudiation and reliability may be included [6].

Infrastructure Network
A wireless network that requires the use of an infrastructure device such as an access point, to facilitate communication between wireless clients [7].

Malicious Code
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or intentionally annoying or disrupting the victim [8].

Media Access Control
A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer [9].

Organisations
Public or private registered entities.

Patch
A piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics, and improving the usability or performance.

Range
The maximum possible distance for communicating with a wireless network infrastructure or wireless client.

Risk Assessment
An initial and periodical step in the risk management process, risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat .

Rogue Access Point
An unauthorized Access Point that do not meet the documented or implied organizational requirements for wireless networks .

Service Set Identifier (SSID)
A name assigned to a wireless local area network that allows wireless clients to distinguish one wireless local area network from another.

Threat A
Probable impending danger or warning of impending danger where vulnerability may be exploited to cause harm to wireless LANs.

Virtual Private Network
A means by which certain authorised individuals (such as remote employees) can gain secure access to an organisation's intranet by an extranet (a part of the internal network that is accessible via the Internet).

Vulnerability
A weakness in an ICT system that allows an attacker to violate the integrity of the ICT system in a wireless network.

Wireless Client
A computing related equipment in a wireless local area network.

Wireless Local Area Network (LAN)
A group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. Wireless LANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility.

Wired Equivalent Privacy
A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a wireless local area network with a level of security and privacy comparable to what is usually expected of a wired local area network. WEP is no longer considered a viable encryption mechanism due to known weaknesses [16].

IEEE 802.11i
An IEEE standard specifying security mechanisms for 802.11 networks. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher. The standard also includes improvements in key management, user authentication through 802.1X and data integrity of headers. (802.1X, AES, WPA2) Wi-Fi Alliance is a governing body that introduce WPA/WPA2 security standards.

WPA/WPA2
Wi-Fi Protected Access, a specification adopted from the 802.11i specification by the Wi-Fi Alliance to promote an improved interoperable security mechanism for wireless network .

Abbreviation of Terms

ACL	-	Access Control List)
AES	-	Advanced Encryption Standard
AP	-	Access Point)
CISO	-	Chief Information Security Officer
CCMP	-	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DES	-	Data Encryption Standard
DoS	-	Denial of Service
EAP	-	Extensible Authentication Protocol
GPS	-	Global Positioning System
IDS	-	Intrusion Detection System
IPS	-	Intrusion Prevention System
IEC	-	International Electrotechnical Commission
IEEE	-	Institute of Electrical and Electronics Engineers
IP	-	Internet Protocol
IPSec	-	Internet Protocol Security
ISO	-	International Organisation for Standardisation
IT	-	Information Technology
LAN	-	Local Area Network
MAC	-	Medium Access Control
NIC	-	Network Interface Card
PC	-	Personal Computer
PCI	-	Peripheral Component Interconnect
PCMCIA	-	Personal Computer Memory Card International Association
RADIUS	-	Remote Authentication Dial-in User Service
RF	-	Radio Frequency
SNMP	-	Simple Network Management Protocol
SSH	-	Secure Shell
SSID	-	Service Set Identifier
SSL	-	Secure Socket Layer
TLS	-	Transport Layer Security
TKIP	-	Temporal Key Integrity Protocol

USB	-	Universal Serial Bus
VPN	-	Virtual Private Network
WAP	-	Wireless Application Protocol
WEP	-	Wired Equivalent Privacy
Wi-Fi	-	Wireless Fidelity
WLAN	-	Wireless Local Area Network
WNIC	-	Wireless Network Interface Card
WPA	-	Wi-Fi Protected Access
WPA2	-	Wi-Fi Protected Access 2

2. OVERVIEW OF WIRELESS LOCAL AREA NETWORK

Wireless local area networks (LAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication . Wireless LANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility and network access. This enables organisations to offer its employees the mobility to move around within a broad coverage area and still be connected to the network. The most widely implemented wireless LAN technologies are based on the IEEE 802.11 standard and its amendments. The original 802.11 standard was published in June 1997 as IEEE Std. 802.11-1997, and it is often referred to as 802.11 Prime because it was the first WLAN standard. The standard was revised in 1999, reaffirmed in 2003, and published as IEEE Std. 802.11-1999 (R2003). Please refer to Appendix A for the summaries of various IEEE802.11 standards. Wireless LAN offers a quick and effective extension of a wired network or standard LAN. Installing a wireless LAN is easy and eliminates the need to pull wired cables through walls and ceilings.

2.1 Wireless Lan Components

The two fundamental components in wireless LAN are access points and wireless clients.

Access Points (APs) – These are base stations for the wireless network. They transmit and receive radio frequencies for wireless clients to communicate with.

Wireless Clients: Wireless clients can be any computing related equipment device such as laptops, personal digital assistants, and IP phones, or fixed devices such as desktops and workstations that are equipped with a Wireless Network Interface Card (WNIC).

Wireless Lan Operating Mode: A wireless LAN can be configured in either ad-hoc mode or infrastructure mode.

Wireless Networks Ad-Hoc Mode – Ad-hoc Mode 4 PC, PCI Notebook , Notebook PCMCIA Wireless LAN Notebook USB. USB 18 NIST SP800-48r1 Guide to Securing Legacy IEEE 802.11

2.2 Wireless Networks Infrastructure Mode

Wireless LAN Ethernet LAN PC, PCI USB Notebook. Access Point Switch Workstation Router Internet Server PC Card Notebook An ad-hoc wireless LAN mode allows wireless clients to connect directly to one another to share files or resources. This mode does not require a wireless access point; hence the wireless clients connect and communicate directly to each other (within a certain range) via a wireless client device (e.g. wireless USB, PCI, PCMCIA, PC card adapters, and built-in wireless chips). This mode is established by several wireless clients, which have the same SSID and radio channel for a peer-to-peer communication mode.

Infrastructure Mode must contain at least one wireless access point that connects wireless clients to wireless LANs or other networks such as the Internet or intranet. The wireless access point establishes an infrastructure mode for networking between all wireless clients and wired network resources (i.e. servers, printers).

2.3 Roles And Responsibilities

Security is not a task; it is a continuous process that every employee in organisations should understand and undertake in their job functions. To ensure adequate security in wireless LANs, senior management should play significant roles in network security especially related to wireless networks. The following tasks should be used as guidance in identifying the roles and responsibilities in ensuring wireless LAN security: 1. Senior management should provide support for planning and implementing security for wireless LANs through clear direction and demonstrated commitment. 2. Senior management should ensure risk assessment is performed before implementing wireless LANs

2.4 Benefits of Wireless LAN To Organisations

Wireless LAN offers organisations the following benefits:

i. **Mobility** – Organisations provide employees with convenience to access online resources and the Internet without a network cable.
ii. **Rapid Deployment** – Organisations reduce time involved in implementing wireless LANs due to reduction in need to lay out or pull physical cables through walls and ceilings.
iii. **Flexibility** – Organisations enjoy flexibility of setting up and removing wireless LANs in many locations, i.e. temporary locations for conferences and seminars.
iv. **Scalability** – Organisations easily increase the network coverage from small ad-hoc networks to very large infrastructure networks by putting an access point.

3. WIRELESS LAN THREATS

As many organisations have implemented wireless networks and as the numbers continues to grow, it becomes crucial for them to learn and understand the types of threats in wireless LANs. Organisations, therefore, need to understand security threats before implementing wireless LANs by carrying out further studies in understanding threats associated with wireless LANs. The threats described here are relevant to wireless LANs in general :

i. **Denial of Service** – Attacker prevents or limits the normal use or management of wireless networks or network devices.
ii. **Eavesdropping** – Attacker passively monitors wireless networks for data, including authentication credentials.
iii. **Man-in-the-Middle** – Attacker actively intercepts communications between wireless clients and APs, thereby obtaining authentication credentials and data.
iv. **Masquerading** – Attacker impersonates an authorised user and gains certain unauthorised privileges to wireless networks.
v. **Message Modification** – Attacker alters a legitimate message sent via wireless networks by deleting, adding to, changing, or reordering it.
vi. **Message Replay** – Attacker passively monitors transmissions via wireless networks and retransmits messages, acting as if the attacker was a legitimate user.
vii. **Traffic Analysis** – Attacker passively monitors transmissions via wireless networks to identify communication patterns and participants.
viii. **Physically Tampered** – Passwords can be retrieved from the hardware due to changes to the AP's antenna or when the AP is moved to another location. This increases the signal strength in favour of the attacker). With the identified threats in a wireless network, and others that may prevail, there is a need for organisations to apply the

following recommended security controls in protecting computers and securing wireless LANs in their organisations. Without implementing appropriate security controls, many opportunities will abound for attackers to impose threats to an organisation's wireless network.

4. SECURITY CONTROLS IN WIRELESS LANS

Security controls is a suite of security safeguards or countermeasures to be established by organisations to protect the confidentiality, integrity and availability of their information system and information. Security controls provide a means of managing risks that include, but are not limited to, policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature. Therefore, security controls for wireless LANs can be selected from a variety of areas (including risk management, personnel security, media protection, physical and environmental protection, contingency planning, incident response management, etc.) to ensure a holistic approach to securing wireless LANs in organisations. For this Guideline, security controls are grouped into three categories: Management, Technical, and Operational controls. Management controls are security controls that focus on management of risk and information system security . The management needs to understand the objectives, benefits, threats and vulnerabilities, as well as risks, before deciding on the deployment of a wireless LAN in an organisation. Once the decision is made, the management shall identify strategies and security controls to prevent any compromise to the wireless LAN.

However, the management controls cannot work independently; it should and usually is complemented by two other aspects: technical and operational. Technical controls are security controls which are primarily implemented and executed through mechanisms contained in computing related equipments (hardware, software, or firmware components of the system). They involve the use of countermeasures or safeguards which are already incorporated into computing related equipments or wireless devices. They involve providing security awareness and training to employees, and securing the physical premise which houses the wireless LAN facilities and/or devices. These controls need to be implemented by organisations continuously throughout the year to ensure wireless network risks can be identified and mitigated effectively to reduce their impact to organisations. These three security controls, Management, Technical, and Operational are to be used together not just to mitigate security risks in wireless LANs, but also to ensure the preservation of confidentiality, availability and integrity of transactions, and data transmitted via wireless LANs.

4.1 Management Controls

Management controls are very much required to ensure that a secure wireless LAN is implemented in organisations. To ensure this, roles and responsibilities for wireless LAN planning and implementation are to be clearly defined. Security policies and procedures related to wireless LANs need to be developed and endorsed. Senior management has to ensure that risk assessment on wireless LANs and wireless network assessments are conducted periodically and in accordance to organisational policies and procedures, as well as other security requirements.

5. CONCLUSION

Like most advances, wireless LANs pose both opportunities and risks. The technology can represent a powerful complement to an organization's networking capabilities, enabling increased employee productivity and reducing IT costs. To minimize the attendant risks, IT administrators can implement a range of measures, including establishment of wireless security policies and practices, as well as implementation of various LAN design and implementation measures. Achieving this balance of opportunity and risk allows enterprises to confidently implement wireless LANs and realize the benefits this increasingly viable technology offers.

REFERENCES

1. Security controls for Operational Risk Management. http://www.occ.treas.gov/ftp/release/2013-53c.pdf, 05/05/2018.
2. Kipper, Grogery. Wireless Crime and Forensic Investigation. Auerbach Publications, Taylor & Francis Group. 2017.
3. Mell, Kent, Nusbaum, Joseph", November 20015. NIST Special Publication 800-83, "Guide to Malware Incident Prevention and Handling.
4. http://csrc.nist.gov/publications/nistpubs/ 800-83/SP800-83.pdf
5. Ross, Katzke, Johnson et all December 2016. NIST Special Publication 800-53 Revision 1, "Recommended Security Controls for Federal Information Systems".
6. http://csrc.nist.gov/publications/nistpubs/ 800-53-Rev1/800-53-rev1-final-clean-sz.pdf
7. NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, June 2010. http://csrc.nist.gov/publications/PubsSPs.html#800-53a [SP800-70]
8. NIST Special Publication 800-70 Revision 2, National Checklist Program for IT Products—Guidelines for Checklist Users and Developers, February 2011. http://csrc.nist.gov/publications/PubsSPs.html#800
9. GAO-11-43, Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk, November 2010. http://www.gao.gov/new.items/d1143.pdf [NCP] National Checklist Program Repository. http://checklists.nist.gov/ [SP800-37]
10. NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010. http://csrc.nist.gov/publications/PubsSPs.html#800-37