REGIONAL DEPARTMENT
OF DEFENSE RESOURCES MANAGEMENT STUDIES

THE 6th EXPLORATORY WORKHOP "INFORMATION SECURITY MANAGEMENT IN THE 21ST CENTURY"

5 948490 380293 13012

ISSN: 2286 - 2765
ISSN-L: 2286 - 2765

COORDINATOR: Advanced Instructor PhD eng. **DANIEL SORA**

National Defense University "Carol I" Publishing House
Bucharest 2013

THE 6th EXPLORATORY WORKHOP
"INFORMATION SECURITY MANAGEMENT -
IN THE 21ST CENTURY"

WORKSHOP COMMITTEE

COL.eng. Daniel SORA, Advanced Instructor PhD.
COL.eng. Cezar VASILESCU, Senior Lecturer PhD.
COL. Florin-Eduard GROSARU, Lecturer PhD.
Maria CONSTANTINESU, Lecturer PhD.
Aura CODREANU, Lecturer PhD.
Brînduşa POPA, Junior Lecturer PhD.
LTC. Cătălin ANTON
CAPT.eng. Florin OGÎGĂU-NEAMŢIU

SESSION CHAIRMEN

COL.eng. Daniel SORA, Advanced Instructor PhD.

CAPT.eng. Florin OGÎGĂU-NEAMŢIU

THE 6th EXPLORATORY WORKHOP "INFORMATION SECURITY MANAGEMENT - IN THE 21ST CENTURY"

December 16th 2013

Proceedings of the workshop unfolded as a result
of the scientific research project:

PROCEDURE FOR TESTING AND EVALUATION OF THE WIRELESS NETWORKS SECURITY

contained in the Research and Development Sectorial Plan
of the Ministry of National Defense for 2013, position 13

conducted by the Regional Department
of Defense Resources Management Studies
2013
Braşov
ROMÂNIA

This page is intentionally left blank

CONTENTS

WIRELESS LOCAL AREA NETWORKS

Introduction

In today's technological market, there are many types of networks. These networks include wireless personal area networks (WPANs), wireless local area networks (WLANs), wireless metropolitan area networks (WMANs), and cellular networks. In general, the range coverage of WPANs is smaller than that of WLANs, and that of WLANs is smaller than that of cellular networks. Between WMANs and cellular, their range coverage depends on the frequency band in which they are operating. In each type of network, there are also different categories of networks. For example, there are ZigBee, Bluetooth, WiMedia, and IEEE 8022.15.3c networks in WPANs. IEEE 802.11 WLANs can be further classified as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n. These WLANs differ in the data rates that they can deliver. Worldwide interoperability for microwave access (WiMax) is an example of WMAN.

A wireless local area network (WLAN) is a wireless network that allows two or more users to communicate with each other at relatively high speed compared to that offered by a cellular network. It is similar to Ethernet except that Ethernet is wired, whereas WLAN is wireless and supports user mobility. It is very commonly used in the office and home environments. The most prominent WLAN under deployment today is the IEEE 802.11 WLAN. The IEEE 802.11 standard has been evolved further into the following five types: IEEE 802.11b, 802.11a, 802.11g, 802.11n, and 802.11s.

The Internet today is a widespread information infrastructure, but it is inherently an insecure channel for sending messages. When a message (or packet) is sent from one web site to another, the data contained in the message are routed through a number of intermediate sites before reaching their destination. The Internet was designed to accommodate heterogeneous platforms so that people who are using different computers and operating systems can communicate. The history of the Internet is complex and involves many aspects – technological, organizational, and community.

802.11 Wireless LANs

Wireless LANs are specified by the IEEE 802.11 series standard, which describes various technologies and protocols for wireless LANs to achieve different targets, allowing the maximum bit rate from 2 Mbits per second to 248 Mbits per second. Wireless LANs can work in either access point (AP) mode or ad hoc mode. When a wireless LAN is working in AP mode, all communication passes through a base station, called an access point. The access point then passes the communication data to the destination node, if it is connected to the access point, or forwards the communication data to a router for further routing and relaying. When working in ad hoc mode, wireless LANs work in the absence of base stations.

Nodes directly communicate with other nodes within their transmission range, without depending on a base station. One of the complications that 802.11 wireless LANs incur is medium access control in the data link layer.

Medium access control in 802.11 wireless LANs can be either distributed or centralized control by a base station. The ***distributed*** medium access control relies on the Carrier Sense Multiple Access (CSMA) with Collision Avoidance (CSMA/CA) protocol. CSMA/CA allows network nodes to compete to transmit data when a channel is idle and uses the Ethernet binary exponential backoff algorithm to decide a waiting time before retransmission when a collision occurs. CSMA/CA can also operate based on MACAW (Multiple Access with Collision Avoidance for Wireless) using virtual channel sensing. Request packets and clear-to-send (CTS) packets, are broadcast before data transmission by the sender and the receiver, respectively. All stations within the range of the sender or the receiver will keep silent in the course of data transmission to avoid interference on the transmission.

The ***centralized*** medium access control is implemented by having the base station broadcast a beacon frame periodically and poll nodes to check whether they have data to send. The base station serves as a central control over the allocation of the bandwidth. It allocates bandwidth according to the polling results. All nodes connected to the base station must behave in accordance with the allocation decision made by the base station. With the centralized medium access control, it is possible to provide quality-of-service guarantees because the base station can control on the allocation of bandwidth to a specific node to meet the quality requirements.

Security Protocols

WEP

Wired Equivalent Privacy (WEP) was defined by the IEEE 802.11 standard. WEP is designed to protect linkage-level data for wireless transmission by providing confidentiality, access control, and data integrity, to provide secure communication between a mobile device and an access point in a 802.11 wireless LAN.

Implemented based on shared key secrets and the RC4 stream cipher, WEP's encryption of a frame includes two operations. It first produces a checksum of the data, and then it encrypts the plaintext and the checksum using RC4.

WPA and WPA2

Wi-Fi Protected Access (WPA) is specified by the IEEE 802.11i standard. The standard is aimed at providing a stronger security compared to WEP and is expected to tackle most of the weakness found in WEP.

WPA

WPA has been designed to target both enterprise and consumers. Enterprise deployment of WPA is required to be used with IEEE 802.1x authentication, which is responsible for distributing different keys to each user. Personal deployment of WPA adopts a simpler mechanism, which allows all stations to use the same key. This mechanism is called the Pre-Shared Key (PSK) mode.

The WPA protocol works in a similar way to WEP. WPA mandates the use of the RC 4 stream cipher with a 128 _ bit key and a 48 _ bit initialization vector (IV), compared with the 40 _ bit key and the 24 _ bit IV in WEP. WPA also has a few other improvements over WEP, including the Temporal Key Integrity Protocol (TKIP) and the Message Integrity Code (MIC). With TKIP, WPA will dynamically change keys used by the system periodically. With the much larger IV and the dynamically changing key, the stream cipher RC4 is able to produce a much longer keystream. The longer keystream improved WPA's protection against the well-known key recovery attacks on WEP, since finding two packets encrypted using the same key sequences is literally impossible due to the extremely long keystream.

With MIC, WPA uses an algorithm named Michael to produce an authentication code for each message, which is termed the message integrity code. The message integrity code also contains a frame counter to provide protection over replay attacks.

WPA uses the Extensible Authentication Protocol (EAP) framework to conduct authentication. When a user (supplicant) tries to connect to a network, an authenticator will send a request to the user asking the user to authenticate herself using a specific type of authentication mechanism. The user will respond with corresponding authentication information. The authenticator relies on an authentication server to make the decision regarding the user's authentication.

WPA2

WPA2 is not much different from WPA. Though TKIP is required in WPA, Advanced Encryption Standard (AES) is optional. This is aimed to provide backward compatibility for WPA over hardware designed for WEP, as TKIP can be implemented on the same hardware as those for WEP, but AES cannot be implemented on this hardware.

TKIP and AES are both mandatory in WPA2 to provide a higher level of protection over wireless connections. AES is a block cipher, which can only be applied to a fixed length of data block. AES accepts key sizes of 128 bits, 196 bits, and 256 bits. Besides the mandatory requirement of supporting AES, WPA2 also introduces supports for fast roaming of wireless clients migrating between wireless access points.

First, WPA2 allows the caching of a Pair-wise Master Key (PMK), which is the key used for a session between an access point and a wireless client; thus a wireless client can reconnect a recently connected access point without having to re-authenticate. Second, WPA2 enables a wireless client to authenticate itself to a wireless access point that it is moving to while the wireless client maintains its connection to the existing access point. This reduces the time needed for roaming clients to move from one access point to another, and it is especially useful for timing-sensitive applications.

Key Establishment

Because wireless communication is open and the signals are accessible by anyone within the vicinity, it is important for wireless networks to establish trust to guard the access to the networks. Key establishment builds relations between nodes using keys; thus security services, such as authentication, confidentiality, and integrity can be achieved for the communication between these nodes with the help of the established keys.

The dynamically changing topology of wireless networks, the lack of fixed infrastructure of wireless ad hoc and sensor networks, and the limited computation and energy resources of sensor networks, has all added complication to the key establishment process in wireless networks.

Bootstrapping

Bootstrapping is the process by which nodes in a wireless network are made aware of the presence of others in the network. On bootstrapping, a node gets its identifying credentials that can be used in the network the node is trying to join. Upon completion of the bootstrapping, the wireless network should be ready to accept the node as a valid node to join the network.

To enter a network, a node needs to present its identifying credential to show its eligibility to access the network. This process is called pre-authentication. Once the credentials are accepted, network security associations are established with other nodes. These network security associations will serve as further proof of authorization in the network. Security associations can be of various forms, including symmetric keys, public key pairs, hash key chains, and so on. The security associations can be used to authenticate nodes.

Security associations may expire after a certain period of time and can be revoked if necessary. For example, if a node is suspected of being compromised, its security association will be revoked to prevent the node accessing the network. The actual way of revocation depends on the form of the security associations.

Management Countermeasures

Management countermeasures ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that wireless networks and devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack.

The items below are possible actions that organizations should consider; some of the items may not apply to all organizations. A wireless network security policy should be able to do the following (check all tasks completed):

1. *Identify who may use WLAN technology in an organization.*
2. *Identify whether Internet access is required.*
3. *Describe who can install access points and other wireless equipment.*
4. *Provide limitations on the location of and physical security for access points.*
5. *Describe the type of information that may be sent over wireless links.*
6. *Describe conditions under which wireless devices are allowed.*
7. *Define standard security settings for access points.*
8. *Describe limitations on how the wireless device may be used, such as location.*
9. *Describe the hardware and software configuration of any access device.*
10. *Provide guidelines on reporting losses of wireless devices and security incidents.*
11. *Provide guidelines on the use of encryption and other security software.*
12. *Define the frequency and scope of security assessments.*

Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy and compliance therewith, is the foundation on which other countermeasures (the operational and technical) are rationalized and implemented. Finally, the most important countermeasures are trained and aware users.

Organizations should understand that maintaining a secure wireless network is an ongoing process that requires greater effort than for other networks and systems. Moreover, it is important that organizations more frequently assess risks and test and evaluate system security controls when wireless technologies are deployed.

Maintaining a secure wireless network (and associated devices) requires significant effort, resources and vigilance and involves the following steps:

- Maintaining a full understanding of the topology of the wireless network.
- Labeling and keeping inventories of the fielded wireless and handheld devices.
- Creating frequent backups of data.
- Performing periodic security testing and assessment of the wireless network.
- Performing ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
- Applying patches and security enhancements.
- Monitoring the wireless industry for changes to standards to enhance to security features and for the release of new products.
- Vigilantly monitoring wireless technology for new threats and vulnerabilities.

Organizations should not undertake wireless deployment for essential operations until they understand and can acceptably manage and mitigate the risks to their information, system operations, and risk to the continuity of essential operations. As described in this chapter, the risks provided by wireless technologies are considerable.

Many current communications protocols and commercial products provide inadequate protection and thus present unacceptable risks to organizational operations. Agencies must proactively address such risks to protect their ability to support essential operations, before deployment. Furthermore, many organizations poorly administer their wireless technologies. Some examples include deploying equipment with factory default settings; failing to control or inventory their access points; not implementing the security capabilities provided; and, not developing or employing a security architecture suitable to the wireless environment (firewalls between wired and wireless systems, blocking unneeded services/ports, using strong cryptography, etc.). To a large extent, most of the risks can be mitigated. However, mitigating these risks requires considerable tradeoffs between technical solutions and costs. Today, the vendor and standards community is aggressively working towards more robust, open, and secure solutions for the near future.

Threats to (WiFi) Networks

Network Security Threats

Worm

A computer worm is a stand-alone malware program which replicates itself and spreads to other devices via network by utilizing vulnerabilities on the target devices. Unlike a computer virus, it does not need to attach itself to an existing program. Worms are usually made to harm the network by consuming bandwidth, whereas viruses usually corrupt or modify files on a targeted device.

Virus

A computer virus is a program that can replicate itself and spread from one computer to another. Viruses increase their chances of spreading to other computers by infecting files on an NFS or a file system that is accessed by other computers. Recently, viruses are distributed mainly to exploit personal computers for distributed denial-of-service (DDoS) attacks.

DDoS

A denial-of-service attack or DDoS attack is an attempt to make a computer or network resource unavailable to its users. Attackers typically target web sites or services such as search engines, banks, credit card payment gateways, and even servers in national security agencies. DDoS attack overloads and saturates the target machine with external communication requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

Internet and Mobile Security Threats

Phishing

Phishing is to acquire confidential information such as usernames, passwords, and credit card numbers by masquerading a trustworthy entity in an electronic communication such as e-mail and Web. An example of e-mail phishing is an e-mail which is disguised as an official e-mail from a well-known bank. The sender is trying to trick the recipient by keying in confidential information in order for putting a link in the e-mail leading to his own fake phishing site.

Not all phishing attacks require a fake website. Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialed, prompts told users to enter their account numbers and PIN.

Vishing

Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

SMishing

SMishing (SMS phishing) is a form of criminal activity using social engineering techniques. SMS phishing uses cell phone text messages to deliver the *bait* to induce people to divulge their personal information. The *hook* (the method used to actually capture people's information) in the text message may be a website URL, but it has become more common to see a telephone number that connects to an automated voice response system.

SNS Security Threats

Privacy Infringement

With the advancement of data mining technology, personal information on Social Network Services (SNS) such as Facebook and Twitter are easily obtained by an ordinary person, even a child. The revealed personal information is exploited to embarrass, to blackmail, or even to damage the image of its owner.

Spamming

Malicious SNS users can easily create unsolicited messages and produce overloaded traffic in the social networks, called Social Network Spam. The Spam not only overloads SNS servers so as to make it difficult in using the SNS, but also phishes the SNS users and directs them to malicious commercial sites like pornographic Web pages.

Identity Theft

A malicious SNS user can create a fake profile and ID impersonating a famous person or commercial brand. Such a squatting profile usually damages the reputation of the original person or brand, leading to financial and social loss.

Computer Security Threats

Exploit

An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or electronic devices. This often refers to things like gaining control of a computer system or allowing privilege escalation or a denial-of-service attack.

Buffer Overflow

Buffer overflow is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. Buffer overflows can be triggered by inputs that are designed to execute code, or alter the way the program operates. This may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security. Thus, they are the basis of many software vulnerabilities and can be maliciously exploited.

Cross-Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users. An XXS vulnerability may be used by attackers to bypass access controls such as the same origin policy.

Cross-Site Request Forgery

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a web site whereby unauthorized commands are transmitted from a user that the web site trusts. Unlike XSS, which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

Password Cracking

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Another common approach is to say that you have "forgotten" the password and then changing it. The purpose of password cracking might be to help a user recover a forgotten password, to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords.

Rootkit

A rootkit is a malicious software designed to hide the existence of certain processes or programs from normal methods of detection and enables continued privileged access to a computer. Rootkit installation may be either automated or when an attacker installs it once they have obtained root or administrator access. Obtaining this access is a result of direct attack on a system. Once installed it becomes possible to hide the intrusion as well as to maintain privileged access. Like any software they can have a good purpose or a malicious purpose. Rootkit detection is difficult because a rootkit may be able to subvert the software that is intended to find it.

Trojan Horse

A Trojan horse is a stand-alone malicious program that does not attempt to infect other computers in a completely automatic manner without help from outside forces like other programs and human intervention. The term is derived from the Trojan Horse story in Greek mythology. Others rely on drive-by downloads in order to reach target computers.

Trojan may allow a hacker remote access to a target computer system. Once a Trojan has been installed on a target computer system, a hacker may have access to the computer remotely and perform various operations, limited by user privileges on the target computer system and the design of the Trojan. Popular Trojan Horses include Netbus, Back Orifice, Schoolbus, Executor, Silencer, and Striker.

Keylogging

Keylogging is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. There are numerous keylogging methods, ranging from hardware- and software-based approaches to electromagnetic and acoustic analysis.

Spoofing Attack

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

ARP Spoofing

ARP spoofing is a computer hacking technique whereby an attacker sends fake ARP messages onto a LAN. ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether.

IP Spoofing

IP spoofing refers to the creation of IP packets with a forged-source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

E-mail Spoofing

E-mail spoofing is e-mail activity in which the senders address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. Because core SMTP does not provide any authentication, it is easy to impersonate and forge e-mails.

Web Site Spoofing

Web site spoofing is the act of creating a web site, as a hoax, with the intention of misleading readers that the web site has been created by a different person or organization. Normally, the spoof web site will adopt the design of the target web site and sometimes has a similar URL. Another technique is to use a “cloaked” URL. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual web site.

Packet Sniffer

A packet sniffer is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet’s raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

Session Hijacking

Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to Web developers, as the HTTP cookies used to maintain a session on many Web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

Wireless DoS attacks

The idea of a wireless network introduces multiple opportunities for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. During the past few years, wireless LAN security threats have increased rapidly which has affected users, vendors as well as manufacturers. The level of attacks has become more and more complex as more and more sophisticated and highly automated applications were made available. One of the most destructive attacks of a network and especially of a wireless network is a DoS (Denial of Service) attack.

In a DoS attack an attacker tries to stop the provision of services of a protocol/application or a particular machine within the network. Although the reasons for this kind of attacks are varied and do not necessarily lead into compromising data they obstruct access to networking resources of the organization and cause considerable damage. In a wireless environment such attacks generally target the access points because, given their role of nodes of interconnection, their operational status affects a lot of other users. An analysis of this type of attack revealed that in the first 3 months of 2013 the number of DoS attacks increased by approximately 27% compared to the same period of the last year. [3] In the next lines we are going to introduce the main DoS attack modes, present their mode of operation and provide some protection measures.

DoS by de-association / de-authentication

The 802.11i standard defines the conditions which must be satisfied by the client in order to be allowed to associate to the network. As depicted in Figure 1, before a station is granted the right to transmit it has to pass the authentication and then the association process. Consequently, when a station or AP wants to interrupt communication they will send a de-authentication request. Unfortunately, those messages are not secured so it is very easy to spoof the mac addresses of the station or AP and forge the de-authentication requests.

In a DoS by a deautentication attack one will try to take advantage of this behavior and send false data packets to the client or AP in order to make him believe that the other party wants to interrupt the connection (to de-authenticate).

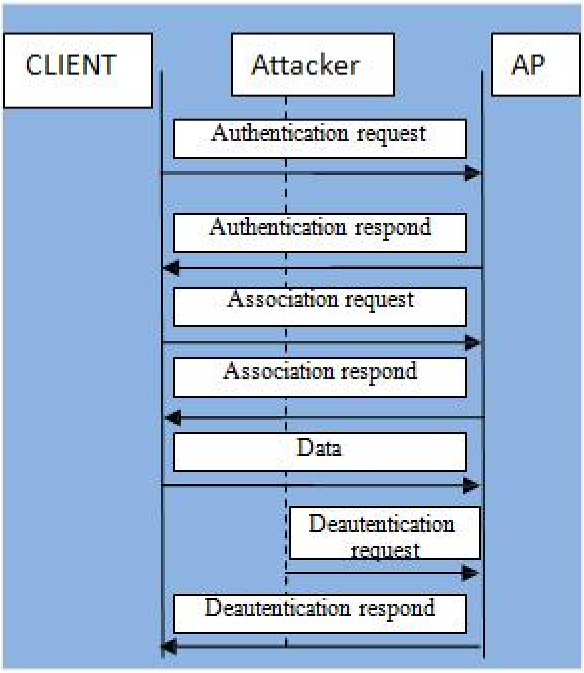
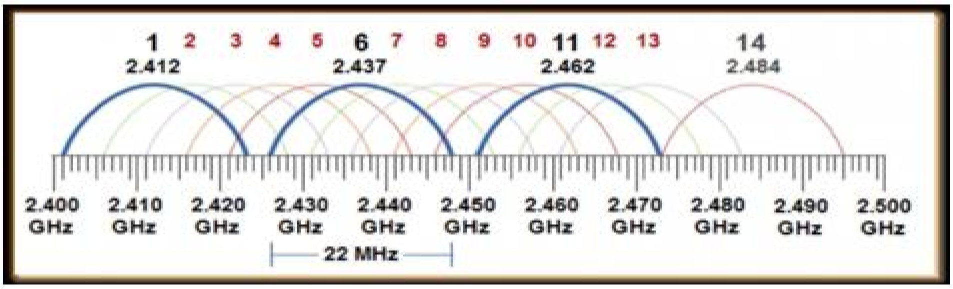


Figure 1 - 802.11i Authentication and association process

Because the client is involved in a communication it will immediately start the reconnection procedure. However, if the attacker will repeatedlysend deautentication packets the client station will enter a connection-disconnection cycle and interrupt the transfer of useful data. This kind of attack offers great flexibility to the attacker and he can choose which station to attack or by capturing the AP's MAC address and using the broadcast MAC address he can target all stations connected to the network.

Jamming AP

Another method which can be used to achieve a DoS attack on a wireless network is by jamming frequencies that are used for communication. Currently 802.11 refer to the use of 2.4 GHz, 3.6 GHz, 4.9GHz and 5 GHz spectrum for wireless networking [11]. Each spectrum is divided into several partially overlapping channels. For example, the range of 2.4 GHz is divided into 14 channels of which 11 are used in the United States and 13 in Europe.



Pict. 2 - The 2.4GHz channels

With the help of adequate hardware and software equipment an attacker can identify the frequency used for communication and by using a high-power noise emission he can block the signal from the AP and consequently the stations are unable to connect or pass traffic.

Quensland DoS

The previous attack required specialized equipment to create a high power radio signal, equipment that costs a lot and is not always available. The Queensland method eliminates this drawback. This type of attack speculates the behavior of CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) protocol used is wireless networking to initiate data transmission. The protocol specifies that before sending a signal the station has to listen if some communication occurs on the selected channel. The station will initiate transmission only if the channel is free. By putting a NIC into continuous transmit mode no other communication can be initiated.

Association DoS attack

An association DoS attack consists of two phases. The first phase of this attack is to capture the MAC address for one or more stations. Then, using these addresses, the attacker floods the target AP with association packages causing equipment to create a huge number of entries in the association table. During this process the equipment's memory fills up and customer services are limited or stopped.

How to protect

An effective protection against DoS attacks is very hard to obtain because even if 802.11i has increased security measures it does not provide protection against this kind of attack. It is very important for an administrator to quickly identify such an attack and take appropriate measures. The most useful tool is a wireless intrusion prevention system (WIPS). It can help organizations establish a performance baseline for the network, detecting the DoS signatures, identify emerging attacks (a DOS de-authentication attack usually is followed by a “Evil twin” attack), identify emerging access points within network, provide detailed logs of the activities within the network, and even detect the source of the attack.

Because the DoS attack uses the unprotected association/disassociation authentication/ deauthentication packets IEEE developed the 802.11 w amendment in order to increase the security of management frames. So using equipment supporting this amendment could improve wireless security.

To defend against physical attacks strategic placement of access points is crucial. The equipment layout has to be made based on good area coverage, minimization of the signal spread outside of the desired space and interference avoidance. Because the frequencies are unlicensed and everybody can use them a lot of interferences can appear from other wireless equipment (wireless cameras, bluetooth devices, cordless phones, etc) or even other access points.

Wi-Fi PROTECTED SETUP – SECURITY ENHANCEMENT OR THREAT?

“Wi-Fi Protected Setup” (WPS; originally Wi-Fi Simple Config) is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on wireless local area networks. Introduced by the Wi-Fi Alliance in early 2007, the program provides an industry-wide set of network setup solutions for homes and small office (SOHO) environments. The goal of the WPS protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Prior to the standard, several competing solutions were developed by different vendors to address the same need.

The Wi-Fi Simple Configuration Specification (WSC) is the underlying technology for the Wi-Fi Protected Setup certification. Almost all major vendors (including Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL and Technicolor) have WPS- certified devices, other vendors (eg. TP-Link) sell devices with WPS-support which are not WPS-certified.

Although WPS is marketed as being a secure way of configuring a wireless device, there are design and implementation flaws which enable an attacker to gain access to an otherwise sufficiently secured wireless network. WPS has been shown to easily fall to brute-force attacks. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours and, with it, the network's WPA/WPA2 pre-shared key. Users have been urged to turn off the WPS feature, although this may not be possible on some router models.

Terminology:

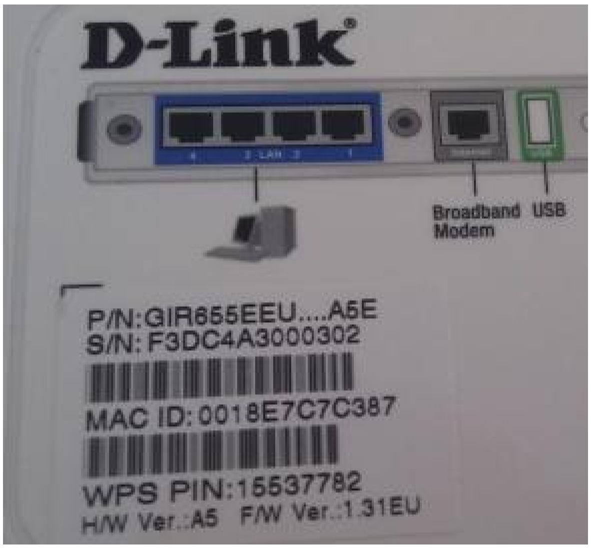
- The enrollee is a new device that does not have the settings for the wireless network.
- The registrar provides wireless settings to the enrollee.
- The access point (AP) provides normal wireless network hosting and also proxies messages between the enrollee and the registrar.

The Wi-Fi Protected Setup Security Hole

Wireless vendors have a few ways to implement WPS, but the PIN method is the only one required, and is the source of the security hole. The way the PIN information is exchanged between the router and clients makes it much easier to brute-force the PIN, repeatedly sending guesses to the router from a client using a tool like Reaver or WPScrack. After a few hours, these tools will likely reveal the target router’s WPS PIN and the WPA or WPA2 passphrase, both of which can be used to connect to the network.

The standard emphasizes usability and security, and allows up to four usage modes aimed at a home network user adding a new device to the network:

1. PIN Method, in which a personal identification number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be entered at the "representant" of the network, usually the access point of the network. Alternately, a PIN on the Access Point may be entered into the new device. The PIN Method is the mandatory baseline mode; every Wi-Fi Protected Setup certified product must support it.



Label with WPS PIN on the back of a D-Link router

2. Push-Button-Method, in which the user simply has to push a button, either an actual or virtual one, on both the access point and the new wireless client device. Support of this mode is mandatory for access points and optional for connecting devices.

3. Near-Field-Communication Method, in which the user simply has to bring the new client close to the access point to allow a near field communication between the devices. NFC Forum compliant RFID tags can also be used. Support of this mode is optional.

4. USB Method, in which the user uses a USB flash drive to transfer data between the new client device and the access point of the network. Support of this mode is optional, but deprecated.

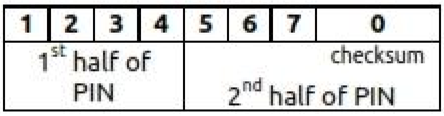
The WPS push button (center, blue) on a wireless router

The last two modes are usually referred as out-of-band methods as there is a transfer of information by a channel other than the Wi-Fi channel itself. Only the first two modes are currently covered by the Wi-Fi Protected Setup certification. The USB method has been deprecated and is not part of the Alliance's certification testing.

In December 2011, researcher Stefan Viehböck1 reported a design and implementation flaw that makes brute-force attacks against PIN-based WPS feasible to perform on WPS-enabled Wi-Fi networks. A successful attack on WPS allows unauthorized parties to gain access to the network. The only effective workaround is to disable WPS.

The vulnerability centers around the acknowledgement messages sent between the registrar and enrollee when attempting to validate a PIN. The PIN is an eight digit number used to add new WPA enrollees to the network. Since the last digit is a checksum of the previous digits, there are seven unknown digits in each PIN, yielding 107 = 10,000,000 possible combinations.

When an enrollee attempts to gain access using a PIN, the registrar reports the validity of the first and second halves of the PIN separately. Since the first half of the pin consists of four digits (10,000 possibilities) and the second half has only three active digits (1000 possibilities), at most 11,000 guesses are needed before the PIN is recovered. This is a reduction by three orders of magnitude from the number of PINs that would have to be tested.



1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

An attacker can derive information about the correctness of parts the PIN from the

AP´s responses.

- If the attacker receives an EAP-NACK message after sending M4, he knows that the 1st half of the PIN was incorrect.
- If the attacker receives an EAP-NACK message after sending M6, he knows that the 2nd half of the PIN was incorrect.

This form of authentication dramatically decreases the maximum possible authentication attempts needed from 108 (=100.000.000) to 104+ 104 (=20.000).

As the 8th digit of the PIN is always a checksum of digit one to digit seven, there are at most 104 + 103 (=11.000) attempts needed to find the correct PIN.

As a result, an attack can be completed in less than four hours. The ease or difficulty of exploiting this flaw is implementation dependent, as Wi-Fi router manufacturers could defend against such attacks by slowing or disabling the WPS feature after several failed PIN validation attempts.

In some devices, disabling WPS in the user interface does not result in the feature actually being disabled. The device remains vulnerable to attack. Firmware updates have been released for some of these devices so that WPS can be disabled completely.

Protecting your network from the WPS security hole

Since the vulnerability lies in the implementation of WPS, your network should be safe if you can simply turn off WPS (or, even better, if your router doesn't support it in the first place). Unfortunately, even with WPS manually turned off through his router's settings, Reaver was still able to crack his password. The inability to shut this vulnerability down is widespread. We have found it to occur with every Linksys and Cisco Valet wireless access point. On all of the Linksys routers, you cannot manually disable WPS. While the Web interface has a radio button that allegedly turns off WPS configuration, it's still on and still vulnerable.

Wireless vendors and/or the Wi-Fi Alliance may help patch this security hole by implementing additional security measures, such as limiting the amount and frequency of PIN guesses. They could possibly fix the issue in new models and in existing models by releasing firmware updates that you may even be able to use with your current router. If they don't make any enhancements, the only way to patch the security hole is to turn WPS off, but even then some routers still might be vulnerable as they may still response to PIN queries.

To see if your router supports WPS—whether or not you should be worried about this security hole—first check if there's an 8-digit PIN number printed on the bottom of your router. Also see if there are any WPS logos on it or on the box it came in. But even if you don't see any evidence, you should still double-check your router's settings for any mention of WPS.

To check or change your router's settings, log on to the web-based interface by typing the router's IP address into a web browser on a computer that's connected to your network. If you don't remember the password to log on, try the default, which can be found in the router's documentation or online. Once logged on, look for WPS settings, perhaps in the wireless or advanced settings.

If you find you have WPS, you can usually disable via the router settings. But again, it may not actually stop people from taking advantage of the security hole.

Before giving up on your router, check the wireless vendor's website and look for any firmware updates for your particular router that were released in January 2012 or after. Then look at the release notes for any mention of a WPS fix or update. If you see one, then you can simply download the firmware file and upload it to your router via the settings interface in your web browser. Otherwise, you might consider checking to see if your router is supported by after-market firmware, like DD-WRT or Tomato, which don't support or include WPS.

As a last resort for full peace of mind, if your router doesn't have firmware updates and can't go the after-market route, you may consider buying a different router model that doesn't come with WPS.

DD-WRT is a Linux based alternative OpenSource firmware suitable for a great variety of WLAN routers and embedded systems. The main emphasis lies on providing the easiest possible handling while at the same time supporting a great number of functionalities within the framework of the respective hardware platform used.

DD-WRT does not support WPS, so there's yet another reason to love the free firmware.

If the router is for business use, consider using the Enterprise (802.1X) mode of WPA2 instead of the personal or PSK mode. When using the enterprise mode, the WPS vulnerability doesn't apply even if you have WPS on your router. This is because WPS only works with the personal mode, and if you don't have it enabled there isn't anything to worry about.

The Enterprise mode, however, is much more complex to set up. It uses 802.1X authentication, which requires a RADIUS server. If you have a domain network, you can use the Internet Authenticate Service (IAS) feature of Windows Server 2000 or 2003 or the Network Policy Server (NPS) feature of Windows Server 2008 or later. If you don't have a Windows Server, consider the free open source FreeRADIUS server. But if you don't want to run your own server, consider APs with built-in RADIUS servers or cloud services that can host the server for you.

As nearly all major router/AP vendors have WPS-certified devices and WPS – PIN (External Registrar) is mandatory for certification, it is expected that a lot of devices are vulnerable to this kind of attack.

Having a sufficiently long lock-down period is most likely not a requirement for certification. However it might be a requirement in the WSC Specification Version 2.

Collaboration with vendors will be necessary for identifying all vulnerable devices. It is up to the vendors to implement mitigations and release new firmware.

Affected end-users will have to be informed about this vulnerability and advised to disable WPS or update their firmware to a more secure version (if available).

Wireless Intrusion Detection System (WIDS)

A wireless intrusion detection system (WIDS) monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity. The typical components in a WIDS are the same as an NIDS: consoles, database servers (optional), management servers, and sensors. However, unlike an NIDS sensor, which can see all packets on the networks it monitors, a WIDS sensor works by sampling traffic because it can only monitor a single channel at a time. The longer a single channel is monitored, the more likely it is that the sensor will miss malicious activity occurring on other channels. To avoid this, sensors typically change channels frequently, so that they can monitor each channel a few times per second.

Wireless sensors are available in multiple forms. A dedicated sensor is a fixed or mobile device that performs WIDS functions but does not pass network traffic from source to destination. The other wireless sensor forms are bundled with access points (AP) or wireless switches. Because dedicated sensors can focus on detection and do not need to carry wireless traffic, they typically offer stronger detection capabilities than wireless sensors bundled with AP or wireless switches. However, dedicated sensors are often more expensive to acquire, install, and maintain than bundled sensors because bundled sensors can be installed on existing hardware, whereas dedicated sensors involve additional hardware and software. Organizations should consider both security and cost when selecting WIDS sensors.

WIDS components are typically connected to each other through a wired network. Because there should already be a strictly controlled separation between the wireless and wired networks, using either a management network or a standard network should be acceptable for WIDS components. Choosing sensor locations for a WIDS deployment is a fundamentally different problem than choosing locations for any other type of IDS sensor.

If the organization uses wireless local area networks (WLAN), wireless sensors should be deployed so that they monitor the range of the WLANs. Many organizations also want to deploy sensors to monitor parts of their facilities where there should be no WLAN activity, as well as channels and bands that the organization’s WLANs should not use. Other considerations for selecting sensor locations include physical security, sensor range, wired network connection availability, cost, and AP and wireless switch locations.

WIDSs provide several types of security capabilities. Most can collect information on observed wireless devices and WLANs and perform extensive logging of event data. WIDSs can detect attacks, misconfigurations, and policy violations at the WLAN protocol level. Organizations should use WIDS products that use a combination of detection techniques to achieve broader and more accurate detection. Examples of events detected by WIDSs are unauthorized WLANs and WLAN devices, poorly secured WLAN devices, unusual usage patterns, the use of active wireless network scanners, denial of service attacks, and impersonation and man-in-the-middle attacks. Most WIDS sensors can also identify the physical location of a detected threat by using triangulation.

Compared to other forms of IDS, WIDS is generally more accurate; this is largely due to its limited scope (analyzing wireless networking protocols). WIDSs usually require some tuning and customization to improve their detection accuracy. The main effort is in specifying which WLANs, APs, and STAs are authorized and in entering the policy characteristics into the WIDS software. Besides reviewing tuning and customizations periodically to ensure that they are still accurate, administrators should also ensure that changes to building plans are incorporated occasionally. This is needed for accurate identification of the physical location of threats and accurate planning of sensor deployments.

Although WIDSs offer robust detection capabilities, they do have some significant limitations. WIDSs cannot detect certain types of attacks against wireless networks, such as attacks involving passive monitoring and off-line processing of wireless traffic. WIDSs are also susceptible to evasion techniques, especially those involving knowledge of a product’s channel scanning scheme. Channel scanning can also impact network forensics because each sensor sees only a fraction of the activity on each channel. WIDS sensors are also susceptible to denial of service attacks and physical attacks.

WIDS sensors can offer intrusion prevention capabilities. Some sensors can instruct end points to terminate a session and prevent a new session from being established. Some sensors can instruct a switch on the wired network to block network activity for a particular wireless end point; however, this method can only block wired network communications and will not stop an end point from continuing to perform malicious actions through wireless protocols.

Most IDS sensors allow administrators to specify the prevention capability configuration for each type of alert. Prevention actions can affect sensor monitoring; for example, if a sensor is transmitting signals to terminate connections, it may not be able to perform channel scanning to monitor other communications until it has completed the prevention action. To mitigate this, some sensors have two radios – one for monitoring and detection and the other for performing prevention actions. When selecting sensors, organizations should consider what prevention actions may need to be performed and how the sensor's detection capabilities could be affected by performing prevention actions.

Configuring Wireless Internet Security Remote Access

This chapter describes how to configure and add wireless remote access points (APs) as RADIUS clients of the Microsoft 2003 and Vista Internet Authentication Service (IAS) servers.

Adding the Access Points as Radius Clients to IAS

You must add wireless remote APs as RADIUS clients to IAS before they are allowed to use RADIUS authentication and accounting services. The wireless remote APs at a given location will typically be configured to use an IAS server at the same location for their primary RADIUS server and another IAS server at the same or a different location as the secondary RADIUS server. The terms "primary" and "secondary" here do not refer to any hierarchical relationship, or difference in configuration, between the IAS servers themselves. The terms are relevant only to the wireless remote APs, each of which has a designated primary and secondary (or backup) RADIUS server. Before you configure your wireless remote APs, you must decide which IAS server will be the primary and which will be the secondary RADIUS server for each wireless remote AP.

The following procedures describe adding RADIUS clients to two IAS servers. During the first procedure, a RADIUS secret is generated for the wireless remote AP; this secret, or key, will be used by IAS and the AP to authenticate each other. The details of this client along with its secret are logged to a file. This file is used in the second procedure to import the client into the second IAS

You must not use this first procedure to add the same client to two IAS servers. If you do this, the client entries on each server will have a different RADIUS secret configured and the wireless remote AP will not be able to authenticate to both servers.

Adding Access Points to the First IAS Server

This part describes the adding of wireless remote APs to the first IAS server. A script is supplied to automate the generation of a strong, random RADIUS secret (password) and add the client to IAS. The script also creates a file (defaults to Clients.txt) that logs the details of each wireless remote AP added. This file records the name, IP address, and RADIUS secret generated for each wireless remote AP. These will be required when configuring the second IAS server and wireless remote APs.

The RADIUS clients are added to IAS as “RADIUS Standard” clients. Although this is appropriate for most wireless remote APs, some APs may require that you configure vendor specific attributes (VSA) on the IAS server. You can configure VSAs either by selecting a specific vendor device in the properties of the RADIUS clients in the Internet Authentication Service MMC or (if the device is not listed) by specifying the VSAs in the IAS remote access policy.

Scripting the Addition of Access Points to IAS Server (Alternative Procedure)

If you do not want to add the wireless remote APs to the IAS server interactively using the previous procedure, you can just generate the RADIUS client entries output files for each wireless remote AP without adding them to IAS. You can then import the RADIUS client entries into both the first IAS server and the second IAS server.

Because you can script this whole operation, you may prefer to add your RADIUS clients this way if you have to add a large number of wireless remote APs.

This procedure is an alternative method for adding RADIUS clients in a scripted rather than an interactive fashion.

Configuring the Wireless Access Points

Having added RADIUS clients entries for the wireless remote APs to IAS, you now need to configure the wireless remote APs themselves. You must add the IP addresses of the IAS servers and the RADIUS client secrets that each AP will use to communicate securely with the IAS servers. Every wireless remote AP will be configured with a primary and secondary (or backup) IAS server. You should perform the procedures for the wireless remote APs at every site in your enterprise.

The procedure for configuring wireless remote APs varies depending on the make and model of the device. However, wireless remote AP vendors normally provide detailed instructions for configuring their devices. Depending on the vendor, these instructions may also be available online.

Prior to configuring the security settings for your wireless remote APs, you must configure the basic wireless network settings. These will include but are not limited to:

- IP Address and subnet mask of the wireless remote AP
- Default gateway
- Friendly name of the wireless remote AP
- Wireless Network Name (SSID)

The preceding list will include a number of other parameters that affect the deployment of multiple wireless remote APs: settings that control the correct radio coverage across your site, for example, 802.11 Radio Channel, Transmission Rate, and Transmission Power, and so forth. Use the vendor documentation as a reference when configuring these settings or consult a wireless network services supplier.

This guidance assumes that you have set these items correctly and are able to connect to the wireless remote AP from a WLAN client using an unauthenticated connection. You should test this before configuring the authentication and security parameters.

Enabling Secure WLAN Authentication on Access Points

You must configure each wireless remote AP with a primary and a secondary RADIUS server. The wireless remote AP will normally use the primary server for all authentication requests, and switch over to the secondary server if the primary server is unavailable. It is important that you plan the allocation of wireless remote APs and carefully decide which server should be made primary and which should be made secondary. To summarize:

In a site with two (or more) IAS servers, balance your wireless remote APs across the available servers so that approximately half of the wireless remote APs use server 1 as primary and server 2 as secondary, and the remaining use server 2 as primary and server 1 as secondary.

In sites where you have only one IAS server, this should always be the primary server. You should configure a remote server (in the site with most reliable connectivity to this site) as the secondary server.

In sites where there is no IAS server, balance the wireless remote APs between remote servers using the server with most resilient and lowest latency connectivity.

Ideally, these servers should be at different sites unless you have resilient wide area network (WAN) connectivity.

Table 1 lists the settings that you need to configure on your wireless remote APs. Although the names and descriptions of these settings may vary from one vendor to another, your wireless remote AP documentation helps you determine those that correspond to the items in table 1.

The Key Refresh Time-out is set to 60 minutes for use with dynamic WEP. The Session Timeout value set in the IAS remote access policy is the same or shorter than this. Whichever of these has the lower setting will take precedence, so you only need to modify the setting in IAS. If you are using WPA, you should increase this setting in the AP to eight hours. Consult your vendor’s documentation for more information.

Use the same RADIUS secrets procedure to add wireless remote APs to IAS. Although you may have not yet configured a secondary IAS server as a backup to the primary server, you can still add the server’s IP address to the wireless remote AP now (to avoid having to reconfigure it later).

Depending on the wireless remote AP hardware model, you may not have separate configurable entries for Authentication and Accounting RADIUS servers. If you have separate configurable entries, set them both to the same server unless you have a specific reason for doing otherwise. The RADIUS retry limit and timeout values given in table 1 are common defaults but these values are not mandatory.

Additional Settings to Secure Wireless Access Points

In addition to enabling 802.1X parameters, you should also configure the wireless remote APs for highest security. Most wireless network hardware is supplied with insecure management protocols enabled and administrator passwords set to well-known defaults, which poses a security risk. You should configure the settings listed in table 2; however, this is not an exhaustive list. You should consult your vendor's documentation for authoritative guidance on this topic. When choosing passwords and community names for Simple Network Management Protocol (SNMP), use complex values that include upper and lowercase letters, numbers, and punctuation characters.

Avoid choosing anything that can be guessed easily from information such as your domain name, company name, and site address.

You should not disable SSID (WLAN network name) broadcast since this can interfere with the ability of Windows XP to connect to the right network. Although disabling the SSID broadcast is often recommended as a security measure, it gives little practical security benefit if a secure 802.1X authentication method is being used.

Even with SSID broadcast from the AP disabled, it is relatively easy for an attacker to determine the SSID by capturing client connection packets. If you are concerned about broadcasting the existence of your WLAN, you can use a generic name for your SSID, which will not be attributable to your enterprise.

Replicating Radius Client Configuration to Other IAS Servers

Typically, the wireless remote APs in a given site are serviced by an IAS server at that site. For example, the site A IAS server services wireless remote APs in site A, while the site B server services wireless remote APs in site B and so on. However, other server settings such as the remote access policies will often be common to many IAS servers. For this reason the export and import of RADIUS client information is handled separately by the procedures described here. Although you will find relatively few scenarios where replicating RADIUS client information is relevant, it is useful in certain circumstances (for example, where you have two IAS servers on the same site acting as primary and secondary RADIUS servers for all wireless remote APs on that site).

TABLE 1 Wireless Access Point Configuration

Item	**Setting**
Authentication Parameters	
Authentication Mode	802.1 X Authentication
Re-authentication	Enable
Rapid/Dynamic	Re-keying Enable
Key Refresh Time-out	60 minutes
Encryption Parameters (these settings usually relate to static WEP encryption)	(Encryption parameters may be disabled or be overridden when rapid re-keying is enabled)
Enable Encryption	Enable
Deny Unencrypted	Enable
RADIUS Authentication	
Enable RADIUS Authentication	Enable
Primary RADIUS Authentication Server	Primary IAS IP Address
Primary RADIUS Server Port	1812 (default)
Secondary RADIUS Authentication Server	Secondary IAS IP Address
Secondary RADIUS Server Port	1812 (default)
RADIUS Authentication Shared Secret	XXXXXX (replace with generated secret)
Retry Limit	5
Retry Timeout	5 seconds
RADIUS Accounting	
Enable RADIUS Accounting	Enable
Primary RADIUS Accounting Server	Primary IAS IP Address
Primary RADIUS Server Port	1813 (default)
Secondary RADIUS Accounting Server	Secondary IAS IP Address
Secondary RADIUS Server Port	1813 (default)
RADIUS Accounting Shared Secret	XXXXXX (replace with generated secret)
Retry Limit	5
Retry Timeout	5 seconds

TABLE 2 Wireless Access Point Security Configuration

Item	Recommended Setting	Notes
General		
Administrator Password	xxxxxx	Set to complex password.
Other Management Passwords	xxxxxx	Some devices use multiple management passwords to help protect access using different management protocols; ensure that all are changed from the defaults to secure values.
Management Protocols		
Serial Console	Enable	If no encrypted protocols are available, this is the most secure method of configuring wireless remote APs although this requires physical serial cable connections between the wireless remote APs and terminal and hence cannot be used remotely.
Telnet	Disable	All Telnet transmissions are in plaintext, so passwords and RADIUS client secrets will be visible on the network. If the Telnet traffic can be secured using Internet Protocol security (IPsec) or SSH, you can safely enable and use it.
HTTP	Disable	HTTP management is usually in plaintext and suffers from the same weaknesses as unencrypted telnet. HTTPS, if available, is recommended.
HTTPS (SSL or TLS)	Enable	Follow the vendor's instructions for configuring keys/certificates for this.
SNMP Communities		SNMP is the default protocol for network management. Use SNMP v3 with password protection for highest security. It is often the protocol used by GUI configuration tools and network management systems. However, you can disable it if you do not use it.
Community 1 Name	XXXXXX	The default is usually "public." Change this to a complex value.
Community 2 Name	Disabled	Any unnecessary community names should be disabled or set to complex values.

References:

[1] http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup

[2] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

[3] http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[4] WPS Flaw Vulnerable Devices list at https://docs.google.com/spreadsheet/ccc?key=0Ags-JmeLMFP2dFp2dkhJZGIxTTFkdFpEUDNSSHZEN3c#gid=0

[5] Default Password List at http://www.phenoelit.org/dpl/dpl.html

[6] http://arstechnica.com/business/2011/12/researchers-publish-open-source-tool-for-hacking-wifi-protected-setup/

[7] http://dd-wrt.com/site/index

[8] https://rstforums.com/forum/75480-how-crack-wi-fi-networks-wpa-password- reaver.rst

[9] https://rstforums.com/forum/73951-wifi-hacking-wpa-2-psk-traffic-decryption.rst

[10] https://rstforums.com/forum/74283-video-hacking-wpa-2-key-evil-twin-method- no-bruteforce.rst

[11] http://www.scribd.com/doc/126108319/Vulnerabilitati-WLAN-WEP-WPA-WPA2

[12] http://www.us-cert.gov/ncas/alerts/ta12-006a

[13] http://www.kb.cert.org/vuls/id/723755

[14] http://www.ciscopress.com/articles/article.asp?p=1847302

[15] Ken Masica, “Securing WLANs using 802.11i”, Lawrence Livermore National Laboratory, 2007;

[16] http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf, last retrieved 07.09.2013;

[17] http://www.pcworld.com/article/2035407/ddos-attacks-have-increased-în-number- and-size-this-year-report-says.html last retrieved 07.09.2013;

[18] http://en.wikipedia.org/wiki/List_of_WLAN_channels, last retrieved 02.10.2013;

[19] http://en.wikipedia.org/wiki/Beacon_frame, last retrieved 15.10.2013; last retrieved 11.10.2013.