



Module Objectives

- Wireless Networking Basics
- Attacks on Wireless Networks
- Why Wireless?
- Radio Wave Technologies
- IEEE 802.11 Radio Wave Networking
 - Wireless Components
 - Wireless Networking Access Methods
 - Handling Data Errors
 - Transmission Speeds
 - Infrared Wireless Networking
 - Using Authentication to Disconnect
 - 802.11 Network Topologies
 - Multiple-Cell Wireless LANs
- Bluetooth Radio Wave Networking
- Anatomy of Attacks on Wireless Networking
 - Rogue Access Points
 - Attacks through Long-Range Antennas
 - Man-in-the-Middle Attacks
 - Pitfalls of Wireless Communications
- Wireless Security Measures
 - Open System Authentication
 - Shared Key Authentication
 - Wired Equivalent Privacy (WEP)
 - Service Set Identifier
 - 802.1x Security
 - 802.1i Security
 - Wi-Fi Protected Access
- Wireless Policy
- Next Module...

Systems Security Management

Eller / MIS 

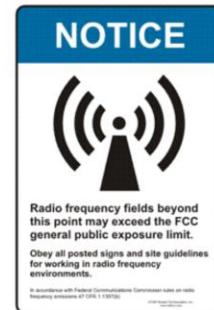
Copyright © 2015, Arizona Board of Regents

At the end of the module, you should be able to:

- Understand the basics regarding wireless networking.
- Understand what kind of attacks are possible on wireless networks.
- Describe why wireless is used in organizations.
- Describe the different radio wave technologies in use today.
- Understand the various IEEE 802.11 radio wave networking technologies and how they work.
- Understand the Bluetooth radio wave technology and what it is used for.
- Describe the different methods for attacking wireless networks.
- Describe the different security options available for wireless networks.
- Understand the need for a wireless policy.

Wireless Networking Basics

- Radio Spectrum Licensed by FCC
- Hertz (Hz)
 - Main Unit of Measurement for Radio Frequencies
- Radio Frequencies (RF)
 - Range of Frequencies Above 10 Kilohertz
 - Electromagnetic Signal Radiated into Space
- Needs for Wireless Networking
 - Enabling Communications where Wired Network is Difficult to Install
 - Reducing Installation Costs
 - Providing “Anywhere” Access to Users
 - Enabling Easier Small and Home Office Networking
 - Enabling Data Access to Fit the Application



Systems Security Management

Eller / MIS 

Copyright © 2015, Arizona Board of Regents

Wireless Networking Basics

In the United States, wireless networks make use of a radio wave spectrum that is licensed by the Federal Communications Commission, or FCC. Radio wave spectrums are measured in hertz (Hz), with radio frequencies, or RF, using the range of frequencies above 10 Kilohertz. Radio frequencies are electromagnetic signals that are radiated throughout a given area and even out into space.

In general there are several reasons why a wireless network might be necessary. These needs include:

- Enabling Communications where Wired Network is Difficult to Install
- Reducing Installation Costs
- Providing “Anywhere” Access to Users
- Enabling Easier Small and Home Office Networking
- Enabling Data Access to Fit the Application

Attacks on Wireless Networks

- Widespread Use of Wireless Networks Interests Attackers
 - Reasons for Attacker Interest Mimic Advantages for Wireless Use
 - Hard-to-Wire Locations of Interest to Attackers since Wireless Easier to Tap w/o Attracting Attention
 - Relatively Inexpensive for Attackers to Obtain Gear to Tap into a Wireless Network
 - “Anywhere” Access Provided by Wireless Networks Gives Attackers Similar Options for “Anywhere” Attacks
 - Common Use of Wireless in Home Offices Creates More Potential Target Sites
 - Wireless Networks Appeal to Attackers Preferring to Work with Wireless Communications

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Attacks on Wireless Networks

The widespread deployment and use of wireless networks is a great interest to attackers, and the reasons these networks interest attackers directly mimic the advantages a wireless network provides for those who need them. Some of these reasons include:

- Hard-to-Wire Locations of Interest to Attackers since Wireless Easier to Tap w/o Attracting Attention.
- Relatively Inexpensive for Attackers to Obtain Gear to Tap into a Wireless Network.
- “Anywhere” Access Provided by Wireless Networks Gives Attackers Similar Options for “Anywhere” Attacks.
- Common Use of Wireless in Home Offices Creates More Potential Target Sites.
- Wireless Networks Appeal to Attackers Preferring to Work with Wireless Communications.

Why Wireless?

- Wired Networks Can be Difficult or Impossible to Install in some Situations
- Consider This Scenario
 - Two Buildings Separated by a Highway Must be Networked
 - Solution #1
 - Dig a Trench Under Concrete Highway
 - » Results in Great Expense & Traffic Delays While Trench is Dug, Cable Laid, Trench Filled In, & Road Restored
 - Solution #2
 - Create a Metropolitan Area Network (MAN)
 - » Both Buildings Connected to a Fiber Optic MAN via Public Network Carrier. Less Cost, but Ongoing Fees

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Why Wireless?

So why install a wireless network? One reason is in some instances it may be too difficult or impossible to install a wired network. Consider the following scenario: an organization is housed in two buildings, and both buildings are separated by a highway that runs between them. Both buildings must have a computer network, and both buildings must be on the same network. How might you accomplish this?

Solution #1

One solution might be to dig a trench under the concrete highway in order to lay fiber optic cable connecting the two buildings. This solution would result in great expense and traffic delays while the trench is dug, cable laid, trench filled in, and finally restoring the roadway.

Solution #2

A second solution might be to create a Metropolitan Area Network, or MAN. This would be accomplished by contracting with an Internet Service Provider, or ISP, for service to each building separately. This solution would allow both buildings to be connected to a fiber optic MAN via the ISP, which would incur less initial cost than solution #1; however, it would have ongoing fees to the ISP for the duration of the contract.

Why Wireless?

- Solution #3
 - Install a Wireless Network
 - » Involves One-Time Cost for Equipment & Ongoing Network Management Costs
 - Solution #3 is Likely the Most Cost-Effective Over Long Term
- Many Organizations Use Integrated Networks
 - Combines Wired & Wireless Networks
 - Allows Network Augmentation
 - Depending on When Cable Originally Laid, Wireless May be Faster
 - Lower General Cost
 - Less Health Risks (Many Buildings have Asbestos)

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Why Wireless? (continued)

Solution #3

A third solution would be to install a wireless network in both buildings. This solution would involve a one-time cost for equipment and ongoing network management costs. Over the long-term, it is likely this solution would be the most cost-effective.

Many organizations make use of integrated networks, or a network that combines both wired and wireless networks. This allows network augmentation, and depending on when a building's cable was originally laid, wireless networks may be faster. In general, wireless networks provide a lower overall cost to the organization for deployment, and there are less health risks associated with deploying wireless networks since many buildings still have asbestos in the walls.

Radio Wave Technologies

- Network Signals Transmitted over Radio Waves
 - Similar Fashion to Local Radio Station Broadcasts
- In the United States
 - Network Signals Transmitted Over Higher Radio Frequencies
 - 902-928 MHz – AKA 900 MHz Band
 - 2.4-2.4835 GHz – AKA 2.4 GHz Band
 - 5.0-5.825 GHz – AKA 5 GHz Band
- Radio Signals Transmitted in One or Multiple Directions
 - Depends on Type of Antenna Used



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Radio Wave Technologies

Radio wave technologies transmit network signals over radio waves in a fashion similar to local radio station broadcasts. In the United States, network signals are transmitted over higher radio frequencies. The common radio frequency bands include:

- 902-928 MHz (900 MHz Band)
- 2.4-2.4835 GHz (2.4 GHz Band)
- 5.0-5.825 GHz (5 GHz Band)

Also, radio signals can be transmitted either in a single direction or multiple directions at the same time, depending on the type of antenna used.

Radio Wave Technologies

- Line-of-Sight Transmission
 - Signal goes Point-to-Point, Following Surface of Earth
 - Limited by Tall Land Masses (Hills, Mountains)
- Spread Spectrum Technology
 - Used by Most Wireless Radio Network Equipment
 - Uses One or More Adjoining Frequencies
 - Transmits Signal Across Greater Bandwidth
 - Frequency Ranges Very High
 - 902-928 MHz
 - Data Rates Between 1-54 Mbps

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Radio Wave Technologies (continued)

Line-of-sight transmission involves a radio signal being transmitted in a point-to-point manner over the surface of the Earth. This type of transmission is limited by tall land masses, such as hills or mountains.

Spread spectrum technology is used by most wireless radio network equipment. Spread spectrum uses one or more adjoining frequencies in order to transmit a signal across a greater bandwidth. The frequency ranges are typically very high, usually operating in the 900 MHz band, from 902-928 MHz, providing data rates between 1-54 megabits per second.

IEEE 802.11 Radio Wave Networking

- Offers Significant Advantages
 - Compatibility & Reliability
 - Devices do not Rely on Proprietary Communications
 - 802.11 Devices from Different Vendors can be Intermixed
 - Different Manufacturer's Devices More Likely to Interoperate
 - Upgrades to Newer Wireless Features Easier to Implement
- IEEE 802.11 Standard
 - AKA IEEE Standard for Wireless LAN Medium Access (MAC) & Physical Layer (PHY) Specifications
 - Standard Encompasses Wireless Stations Fixed or Mobile

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

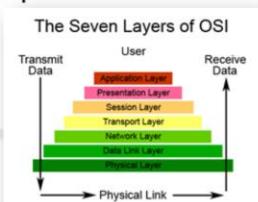
IEEE 802.11 Radio Wave Networking

The IEEE 802.11 radio wave networking standards offer significant advantages with compatibility and reliability. These devices do not rely on proprietary communications, making it possible for 802.11 devices from different vendors to be intermixed. This standard allows for different manufacturer's devices to be able to interoperate, and any upgrades to newer wireless features will be easier to implement.

The IEEE 802.11 standard is also referred to as the IEEE standard for wireless LAN medium access and physical layer specifications. The standard encompasses both fixed or mobile wireless stations.

IEEE 802.11 Radio Wave Networking

- OSI Model Implications for 802.11
 - Standard Focuses on Use of Physical & Data-Link
 - Layers 1 & 2
 - Defines Data Transmission Rates Over Specified Frequencies
 - Physical Layer
 - Provides for Transmitting the Signal
 - Operating at Specified Frequency
 - Data-Link Layer
 - Media Access Control (MAC) & Logical Link Control (LLC)
 - Standards for Gaining Access to Wireless Medium, Determine if Other Stations Exist, Providing Authentication, Addressing, & Data Validation through CRC



Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

IEEE 802.11 Radio Wave Networking (continued)

There are some OSI Model implications where it relates to 802.11 radio wave networking. The standard focuses on the use of the Physical and Data-Link layers, or layers one and two, defining data transmission rates over specified frequencies. The physical layer provides for transmitting signals, operating at a specified frequency. The data-link layer uses Media Access Control, or MAC, and Logical Link Control, or LLC, which are standards for gaining access to wireless mediums, to determine if other stations exist, and to provide authentication, addressing, and data validation through cyclic redundancy checks, or CRCs.

IEEE 802.11 Radio Wave Networking

- Standard Involves Two Kinds of Communication
 - Asynchronous Communication
 - Occurs in Discrete Units
 - Start of Unit Signaled by Start bit at the Front & Stop bit at the Back End
 - Communication Governed by Time Restrictions
 - Signal Must Reach Destination in Given Amount of Time
 - Otherwise Considered Lost or Corrupted
 - Element of Time Restrictions
 - Makes 802.11 Standard Similar to 802.3 Ethernet Standard
 - Includes Support for Network Management Services
 - » SNMP
 - Includes Support for Network Authentication

Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

IEEE 802.11 Radio Wave Networking (continued)

The IEEE 802.11 standard involves two kinds of communication: asynchronous communication and communication governed by time restrictions. Asynchronous communication occurs in discrete units, where the start of a unit is signaled by a start bit at the front and a stop bit at the back end.

Communications that are governed by time restrictions means a signal must reach its destination in a given amount of time, otherwise it is considered lost or corrupted. The element of time restrictions makes the 802.11 standard similar to the 802.3 Ethernet standard. Time restrictions also include support for network management services, such as SNMP, and support for network authentication.

IEEE 802.11 Radio Wave Networking

- Standard Recognizes Indoor & Outdoor
 - Indoor
 - Office Building
 - Manufacturing Floor
 - Retail Store
 - Private Home
 - Where Communications Occur Inside a Single Building
 - Outdoor
 - University Campus
 - Sports Field
 - Parking Areas
 - Where Communications Required Between Buildings



The Standard for
Wireless Fidelity.

Systems Security Management

Eller / MIS 

Copyright © 2015, Arizona Board of Regents

IEEE 802.11 Radio Wave Networking (continued)

IEEE 802.11 standard recognizes both indoor and outdoor uses. Indoor environments the standard supports include:

- Office Buildings
- Manufacturing Floors
- Retail Stores
- Private Homes
- Where Communications Occur Inside a Single Building

Outdoor environments the standard supports include:

- University Campuses
- Sports Fields
- Parking Areas
- Where Communications are Required Between Buildings

IEEE 802.11 Radio Wave Networking

- IEEE 802.11 Wireless Network Function Specifics
 - Wireless Components used in IEEE 802.11
 - Wireless Networking Access Methods
 - How Data Errors are Handled
 - Transmission Speeds Used in IEEE 802.11
 - Infrared Wireless Networking
 - How Authentication is Used to Disconnect
 - Wireless Network Topologies
 - How to Use Multiple-Cell Wireless LANs

Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

IEEE 802.11 Radio Wave Networking (continued)

Finally, the IEEE 802.11 standard defines several wireless network function specifics, including:

- Wireless Components used in IEEE 802.11
- Wireless Networking Access Methods
- How Data Errors are Handled
- Transmission Speeds Used in IEEE 802.11
- Infrared Wireless Networking
- How Authentication is Used to Disconnect
- Wireless Network Topologies
- How to Use Multiple-Cell Wireless LANs

Wireless Components

- Involves 3 Main Components

- Wireless Network Interface Card (WNIC)
 - Transceiver Card Functions on both Physical & Data-Link
 - Most WNICs Compatible w/ Microsoft's Network Driver Interface Specification (NDIS) & Novell's Open Data-Link Interface (ODI) Specification
 - Enable Multiple Protocols to be Carried over a Network
 - Also Allows Computer & OS to Interface w/ WNIC
- Access Point
 - Device Attached to Cable Network Servicing Wireless Communication between WNICs & Wired Network
- Antenna
 - Device Sends Out & Picks Up Radio Waves & Used on both WNICs & Access Points
 - Either Directional or Omnidirectional

Systems Security Management



Eller / MIS

Copyright © 2015, Arizona Board of Regents

Wireless Components

Deploying a wireless network involves three main components: wireless network interface cards, access points, and antennas.

Wireless network interface cards, or WNICs, are a transceiver card that plugs into your computer (or is provided on the chipset in laptops) and operates on both the Physical and Data-Link layers of the OSI model. Most WNICs are compatible with Microsoft's network driver interface specification, or NDIS, and Novell's open data-link interface, or ODI, specification. Both of these specifications enable multiple protocols to be carried over a network, and allow the computer and operating system to interface with the WNIC.

Access points are devices which are physically attached to a wired network via cable and are designed to service wireless communication between WNICs and the wired network.

Antennas are devices which send out and pick up radio waves. Antennas are used on both WNICs and access points for communication, and they can be either directional or omnidirectional.

Wireless Components

- Directional Antenna
 - Sends Radio Waves in One Main Direction
 - Can Amplify Radiated Signal
 - Gain
 - Offers Longer Range than Omnidirectional
- Omnidirectional Antenna
 - Radiates Radio Waves in All Directions
 - Signal More Diffused, Likely has Less Gain
 - Often Used in Indoor Networks
 - Where Users are Mobile
 - Gain does not Need to be as High as Outdoor Networks



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Wireless Components (continued)

Directional Antennas

Directional antennas are designed to send radio waves in one main direction. This allows the antenna to amplify the radiated signal, or gain, in order to offer a longer range than omnidirectional antennas.

Omnidirectional Antennas

Omnidirectional antennas, on the other hand, radiate radio waves in all directions. This means the signal is more diffused; however, it will generally have a lower gain.

Omnidirectional antennas are often used in indoor networks where users are mobile. Using them in indoor spaces means the gain does not need to be as high as is necessary for outdoor networks.

Wireless Components

- Attackers

- Both Antenna Types Offer Unique Advantages
 - Directional Antenna Radiates in One Direction
 - Longer Distance Means Attacker does not Need to be Close to the Source to Pick up the Signal
 - Attacker does have to Locate the Signal Path
 - » Harder, Since Path is Narrow
 - Omnidirectional Antenna Radiates in All Directions
 - Easier to Find Signal
 - Attacker does not have to Determine Path
 - Attacker Must be in Close Proximity to the Signal
 - » Few Feet up to 300 Feet
 - » May be Easier to Detect

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Wireless Components (continued)

When it comes to wireless networks, both types of antennas offer unique advantages with regard to protecting the network against attackers.

Directional antennas radiate in a single direction. For longer distances, this means the attacker does not need to be close to the source in order to pick up the signal; however, the attacker will need to locate the signal path, which is much more difficult since the radio signal path is narrow.

Omnidirectional antennas radiate in all directions, making it much easier for an attacker to find the radio signal since the attacker will not need to determine the signal path. Despite this, the attacker will need to be in close proximity to the signal in order to breach it. This range can be a few feet up to 300 feet, which makes the attacker much easier to detect.

Wireless Networking

Access Methods

- Two Access Methods in 802.11 Standard
 - Priority-Based Access
 - Carrier Sense Multiple Access w/ Collision Avoidance
 - CSMA/CA
 - Both Methods are OSI Data-Link Layer Functions
- Priority-Based Access
 - Functions as Point Coordinator
 - Establishes Contention-Free Period
 - Stations cannot Transmit Unless Contacted by Coordinator
 - Intended for Time-Sensitive Communication
 - Includes Voice, Video, & Videoconferencing



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Wireless Networking Access Methods

There are two primary access methods for connecting to 802.11 standard networks: priority-based access and carrier sense multiple access with collision avoidance, or CSMA/CA. Both of these methods are OSI Data-Link layer functions.

Priority-based Access

Priority-based access functions as a point coordinator in order to establish a contention-free period. In other words, when using this access method, stations cannot transmit data unless they are first contacted by a coordinator. This type of access is intended for time-sensitive communications, such as voice, video, and videoconferencing.

Wireless Networking Access Methods

- Carrier Sense Multiple Access w/ Collision Avoidance (CSMA/CA)
 - Commonly Used Access Method
 - AKA Distributed Coordination Function
 - Station Waiting to Transmit
 - Listens to Determine if Frequency Idle
 - Uses Received Signal Strength Indicator (RSSI) Level
 - When Frequency Idle, Most Risk of Data Collisions
 - When Frequency Idle, Uses Predefined Mandatory Delay
 - Each Station Calculates Different Delay Period
 - » Backoff Time
 - Avoids Collisions



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Wireless Networking Access Methods (continued)

Carrier Sense Multiple Access w/ Collision Avoidance

CSMA with collision avoidance is the most commonly used access method for wireless networking. Also known as a distributed coordination function, this access method involves communicating with stations that are waiting to transmit. The station will listen to determine if the radio frequency is idle, using a Received Signal Strength Indicator, or RSSI. This is used because the greatest risk for data collisions over a wireless network occurs when the radio frequency is idle.

When idle, the station will then use a predefined, mandatory delay before attempting to transmit data in an effort to avoid collisions. Each station will calculate a different delay period, and a backoff timer, used to provide an additional random length of time to wait before transmitting. All of this combined allows CSMA/CA to successfully avoid data collisions.

Handling Data Errors

- Wireless Vulnerable to Signal Interference
 - Weather, Solar Flares, Competing Wireless Networks, Physical Obstacles, etc.
 - Can Corrupt Successful Reception of Data
 - Automatic Repeat Request (ARQ)
 - Part of 802.11 Standard
 - Helps Take these Possibilities into Account
 - Station Sending Packet(s) does not Receive ACK
 - Automatically Retransmits Packet(s)
 - After 10 Unacknowledged Attempts
 - Station Stops Retransmitting Packet(s)

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

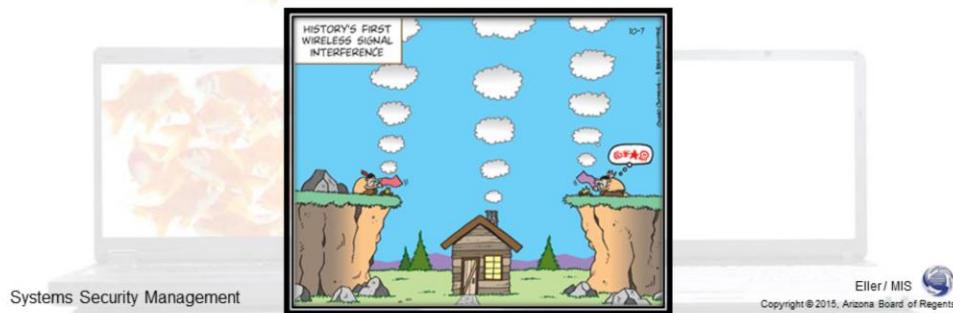
Handling Data Errors

Data errors on wireless networks can wreak all sorts of havok on the network. Wireless networks, by their very nature, are vulnerable to signal interference by the weather, solar flares, competing wireless networks, physical obstacles, and even microwave ovens, among others. This interference can easily corrupt successful reception of data. In order to help handle data errors, 802.11 wireless networking standards include the automatic repeat request, or ARQ. For example, if a station that is sending packets over wireless does not receive an ACK from the access point, the station will automatically retransmit the packets. After 10 unacknowledged attempts at transmitting packets, the station will stop transmitting.

Handling Data Errors

- Attackers

- Can Cause Havoc with Reception
 - Purchasing or Building Transmitter Operating on Same Bands as Wireless Networks
 - Ample Watts in Transmission & Appropriate Antenna
 - Attacker can Effectively Create Interference



Handling Data Errors (continued)

Attackers can also cause problems with wireless reception. For example, an attacker can purchase or build a radio wave transmitter that operates on the same radio signal bands as those used by wireless networks. By ensuring the transmitter has ample wattage and an appropriate antenna, the attacker can easily create effective interference.

Transmission Rates

- Transmission Speeds & Radio Frequencies

- Defined through Five (5) Standards
 - 802.11a
 - 802.11b
 - 802.11g
 - 802.11n
 - 802.11ac



- 802.11a

- 5 GHz Frequency Band
- 6, 9, 12, 18, 24, 36, 48, & 54 Mbps
- All 802.11a Devices MUST Transmit
 - At 6, 12, & 24 Mbps Minimum



Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

Transmission Rates

With 802.11 wireless networks, transmission speeds and radio frequencies are defined through five (5) different standards: 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac.

802.11a

The 802.11a wireless network standard operates on the 5 gigahertz frequency band. This allows communications to operate at a variety of data rates, ranging from 6 megabits per second up to a maximum of 54 megabits per second. At a bare minimum, all 802.11a devices are required to transmit at 6, 12, and 24 megabits per second.

Transmission Rates

- 802.11b
 - 2.4 GHz Frequency Band
 - 1, 2, 10, 11 Mbps
 - Uses Direct Sequence Spread Spectrum Modulation
 - DSSS
 - First Spreads Data Across up to 14 Channels
 - Each 22 MHz in Width
 - Exact Number Depends on Country Transmission Occurs
 - Canada & U.S, 11 Channels
 - Europe, 13 Channels
 - France, 4 Channels
 - Data Signal Sequenced & Amplified to have High Gain
 - Combats Interference



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Transmission Rates (continued)

802.11b

The 802.11b wireless networking standard operates on the 2.4 gigahertz frequency band and guarantees data transmission rates between 1 and 11 megabits per second. 802.11b uses direct sequence spread spectrum modulation, or DSSS, in order to spread data across up to fourteen (14) different channels, each channel is 22 megahertz in width. The exact number of channels in this standard will vary depending on the country in which data transmission occurs. For example, in Canada and the U.S, 11 channels are used. In Europe up to 13 channels are used, and in France only 4 channels are used. By using different channels, this allows data signals to be sequenced and amplified in order to have a high gain, which helps to combat interference.

Transmission Rates

- 802.11g
 - 2.4 GHz Frequency Band
 - Extension & Successor to 802.11b
 - 6, 9, 12, 18, 24, 36, 48, 54 Mbps
 - WNICs can Communicate w/ 802.11b or 802.11g AP
 - 802.11g Required to have Backwards Compatibility
 - 802.11a & 802.11g
 - Advantage of Higher Data Speeds
 - Disadvantage in Shorter Transmission Ranges
 - 802.11a = ~ 60 feet / 18 meters
 - 802.11b = ~ 300 feet / 91 meters
 - 802.11g = ~ 100 feet / 30 meters



Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

Transmission Rates (continued)

802.11g

Similar to 802.11b, the 802.11g standard also uses the 2.4 gigahertz frequency band for data transmissions. 802.11g is the official successor and extension to 802.11b. This is why you will often see wireless access points and wireless routers for sale that support both the 802.11b and 802.11g standards. This standard defines data rates between 6 and 54 megabits per second, so it operates at the same speeds as 802.11a, albeit at a much lower radio frequency. Wireless NICs that are designed for 802.11g are able to communicate with both 802.11b and 802.11g access points, since 802.11g is required to maintain backwards compatibility.

Both the 802.11a and 802.11g standards have the advantage of higher data speeds; however, the higher the data speed, the shorter the transmission range. With 802.11a, the transmission range is approximately 60 feet, with 802.11b, the range is approximately 300 feet, and with 802.11g, the range is approximately 100 feet.

Transmission Rates

- 802.11n
 - 2.4 GHz and/or 5 GHz Frequency Band
 - 100 to 600 Mbps
 - Can Operate on both Frequencies
 - Separately or at the Same Time
 - Channel Width of 40 MHz
 - Width Increases Potential Speed
 - Multiple Input, Multiple Output (MIMO)
 - Uses Multiple Antennas to Resolve More Information
 - Increased Range – 70+ Mbps @ 300 feet
 - Backwards Compatible with 802.11a, b, g



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Transmission Rates (continued)

802.11n

The newest wireless networking standard, 802.11n, was designed to operate at both the 2.4 gigahertz and 5 gigahertz frequency bands, achieving transmission rates between 100 and 600 megabits per second. 802.11n can operate on both frequencies either separately or at the same time. In addition, each channel has a width of 40 megahertz, which increases the potential speed for transmission. 802.11n uses multiple antennas in order to resolve more information through the use of multiple input, multiple output, or MIMO. This standard also increases the radio transmission range, allowing for 70 megabits per second at a distance of 300 feet. Finally, since this standard uses both frequency bands, it is backwards compatible with 802.11a, b, and g standard equipment.

Transmission Rates

- **802.11ac**

- Newest Standard

- Channel Width of 80 MHz
 - More speed compared to 802.11n
 - Multiple User – Multiple Input, Multiple Output (MU-MIMO)
 - Support for up to eight spatial streams (vs. four in 802.11n)
 - Multiple Stations, with one or more antennas, transmit or receive independent streams simultaneously

- 5GHz Frequency Band

- Up to 1,300 Mbps (1.3Gbps)

- Backwards compatible ONLY with 802.11n, a



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Transmission Rates (continued)

802.11ac

The newest wireless networking standard, 802.11ac, was designed with increased wireless needs in mind. With the typical corporate user in possession of, on average, 2.7 devices, the need for greater throughput and speed is getting more apparent. The new technologies provided by 802.11ac include: extended channel binding (80MHz instead of 802.11n's 40MHz channels), more MIMO spatial streams (up to eight, compared to the four offered in 802.11n), downlink Multi-user MIMO that allows up to four simultaneous downlink MU-MIMO clients, and speeds of up to 1.3Gbps. Because it only transmits in the 5GHz range, it is only backwards compatible with 802.11n and 802.11a devices. Older devices with 802.11g or b WNICs will not even be able to connect to access points offering 802.11ac streams. In practice, however, most newer access points will contain two radios to ensure backwards compatibility with older technology.

Infrared Wireless Networking

- Alternative to Radio Waves
 - 802.11R
 - Standard for Infrared Transmission
 - Can be Broadcast in Single or All Direction(s)
 - Using Light Emitting Diode (LED) to Transmit
 - Photodiode to Receive
 - Transmits at 100 GHz to 1000 THz Frequency
 - Security Factors
 - Not as Predominant as 802.11a, b, g, n
 - Very Difficult to Intercept Infrared w/o Detection
 - Infrared not Susceptible to RFI and EMI

Systems Security Management



Eller / MIS Copyright © 2015, Arizona Board of Regents

Infrared Wireless Networking

Another form of wireless networking uses infrared light technology. Infrared is an alternative to radios waves, and the standard for infrared transmission is 802.11R. One benefit to infrared is it can be broadcast in either a single direction or all directions using light emitting diodes, or LEDs. Photodiodes are used by infrared equipment for receiving data transmissions. Infrared technology transmits data between the 100 gigahertz and 1000 terahertz frequencies.

Security Factors

Some security factors for infrared networking include the fact it is not nearly as predominant as 802.11a, b, g, and n for data transmissions. It is also very difficult to intercept infrared transmissions without detection, and infrared is not susceptible to either radio frequency or electromagnetic interference, making this a more secure, albeit limited, wireless networking standard.

Infrared Wireless Networking

- Disadvantages
 - Transmission Rates up to 16 Mbps
 - For Directional
 - Transmission Rates up to 1 Mbps
 - For Omnidirectional
 - Cannot Travel through Walls
- Disadvantages Make Infrared More Secure
- Diffused Infrared
 - Transmits by Reflecting Infrared Light from Ceiling
 - Transmission Range Between 30 & 60 Feet
 - Provides 1 to 2 Mbps Speed with Peak Power of 2 Watts



Systems Security Management

Eller / MIS 

Copyright © 2015, Arizona Board of Regents

Infrared Wireless Networking (continued)

With infrared wireless networks, there are some disadvantages, specifically related to data transmission rates. When using directional infrared, transmission rates can be up to 16 megabits per second; however, when using omnidirectional infrared, transmission rates can only be as high as one megabit per second. Infrared also cannot travel through walls, making it more difficult to use in a multi-room scenario. The interesting thing about these disadvantages is they actually work to make infrared wireless networking more secure.

Another method for using infrared involves adopting diffused infrared, which works by transmitting infrared light by reflecting it off a ceiling. This helps to increase the transmission range to between 30 and 60 feet, providing 1 to 2 megabits per second speed with a peak power requirement of 2 watts.

Using Authentication to Disconnect

- One Function of the Authentication Process is Disconnecting when Communication Session is Complete
 - This is **VERY** Important!
 - Prevents Two Communicating Stations from Being Inadvertently Disconnected by Non-authenticated Station
 - De-authentication Notice Sent to Disconnect
 - Results in Instant Termination of Connection



Using Authentication to Disconnect

When using wireless networks, one major security function of the authentication process involves disconnecting securely when the communications session is complete. This is very important as it prevents two communicating stations from being inadvertently disconnected by a station that has not been authenticated. This process occurs after communications when a de-authentication notice is sent to the client system, which results in instant termination of the wireless connection.

802.11 Wireless Topologies

- Two General Topologies Used
 - Independent Basic Service Set (IBSS) Topology
 - Simplest Topology, Consists of Two or More Wireless Stations
 - Relatively Unplanned, Impromptu, Ad Hoc Peer-to-Peer Network
 - Extended Service Set (ESS) Topology
 - Deploys a More Extensive Area of Service
 - Uses One or More Access Points
 - Small, Medium, or Large Network
 - Significantly Extend the Range of Wireless Communications
 - Stay w/ 802.11-Compliant Devices, Easy to Expand
 - Avoid Combining IBSS & ESS Topologies
 - ESS Topology is More Secure
 - Security Configured through Access Points



Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

802.11 Wireless Topologies

With 802.11 wireless network standards, there are two general topologies used: the independent basic service set (IBSS) topology and the extended service set (ESS) topology.

IBSS is the simplest topology for wireless networks, consisting of two or more wireless stations. This topology is used by wireless networks that are relatively unplanned, impromptu, and used by ad hoc peer-to-peer networks.

ESS topologies are used when deploying a more extensive area of service, using one or more access points. This is your typical wireless network that you will access in small, medium, or large organizations, or even just your local coffee shop. This topology allows network operators to significantly extend the range of wireless communications. It will be important for a network administrator to use 802.11-compliant devices, so the network will be easy to expand. It is also important to note that one should avoid combining both IBSS and ESS topologies as this can cause radio frequency interference on the network. ESS is also a more secure topology, as all security is configured and achieved through the use of access points.

Multiple-Cell Wireless LANs

- ESS Topology Employing Two or More APs
 - Broadcast Area Around Single AP is a Cell
 - 5 Access Points = 5 Cells
 - If All 5 APs Configured the Same Way
 - Devices with WNICs can Move from Cell to Cell
 - » This is Roaming
 - 802.11 does not Specifically Define a Standard for a Roaming Protocol
 - Inter-Access Point Protocol (IAPP)
 - Developed by 802.11 Vendors
 - Encapsulates both UDP & IP for Roaming Communications
 - Enables Existing APs to be Notified when a new AP is Added
 - » Shares Configuration Information
 - Automatically Transfers Connection Info to Next Cell when Roaming

Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

Multiple Cell Wireless LANs

Deploying the ESS topology typically involves employing two or more access points. The radio broadcast area that surrounds each access point is referred to as a “cell.” So, if you deploy an ESS network using five access points, your network will have five cells. Assuming all of the access points are configured in the same manner, any devices with wireless NICs can move from one cell to another without disconnecting from the network. This is known as roaming.

The 802.11 standards do not specifically define any standard for a roaming protocol; however, the Inter-Access Point Protocol, or IAPP, was developed by 802.11 hardware vendors to achieve this goal. This protocol encapsulates both UDP and IP for roaming communications, enabling existing access points to be notified when a new access point is added to the network. The protocol then shares the access point configuration from existing APs to the new AP. The access points then automatically transfer connection information from one cell to the next when a user is roaming.

Bluetooth Radio Wave Networking

- Wireless Technology Defined through the Bluetooth Special Interest Group
 - Uses Frequency Hopping in 2.4 GHz Band
 - Transmissions Hop Among 79 Frequencies for Each Packet Sent
 - Reduces Likelihood of Interference when Multiple Devices in Use
 - High-Wattage Transmissions
 - Transmits up to 330 Feet
 - In Practice, Transmits up to 30 Feet
 - Time-Division Duplexing (TDD)
 - Packets Sent in Alternating Directions, Using Time Slots
 - Can Use up to 5 Slots to Mimic Full-Duplex Communication
 - Up to 7 Devices Connected at One Time
 - One Device Automatically Selected as Master Device



Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Bluetooth Radio Wave Networking

Bluetooth radio wave networking is a wireless technology defined through the Bluetooth Special Interest Group and is used in a wide variety of devices, from wireless keyboards to wireless earpieces for hands-free cell phone communication. Bluetooth technologies use frequency hopping in the 2.4 gigahertz band, allowing transmissions to hop among 79 different frequencies for every packet sent. This reduces the likelihood of interference when multiple Bluetooth devices are in use. The Bluetooth standard allows for high-wattage transmissions, enabling devices to transmit data up to 330 feet; however, in practice, Bluetooth devices typically transmit up to 30 feet. In addition, Bluetooth uses time-division duplexing, or TDD, allowing data packets to be sent in alternating directions using pre-determined time slots. Devices can use up to 5 slots, allowing Bluetooth data transmission to mimic full-duplex communication. Finally, Bluetooth allows up to 7 devices to be connected at any one time, which is only possible because one of the devices will automatically be selected as the master device.

Anatomy of Attacks on Wireless Networks

• First Step: Locate a Wireless Network Target

- Four Main Elements Used by an Attacker
 - An Antenna
 - A Wireless Network Interface Card
 - A GPS
 - War-Driving Software
- Attacker May Use Several Kinds of Antennas
 - Depends on Omnidirectional vs. Directional
 - Some May be High Gain while Others Low Gain
- Global Positioning System (GPS)
 - Determine Location of Target Wireless Network
- War-Driving Software
 - Some Use Broadcast Probe Requests, can be Thwarted



image:bigstock.com

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

Anatomy of Attacks on Wireless Networks

When an attacker is looking to find a wireless network to breach, this requires the attacker to first locate the wireless network target. Four main elements are used by an attacker: an antenna, a wireless network interface card, a GPS, and war-driving software.

The attacker may choose to use different antennas in an attempt to breach the network. Depending on whether or not the antenna is directional or omnidirectional will determine the type of network, and some antennas may be high gain while others are low, determining the distance at which the attacker can operate. Using a global positioning system, the attacker can identify the location of the target wireless network within a few yards, and by using war-driving software, the attacker can also locate networks while on the move. It is important to note that some war-driving software uses broadcast probe requests, which can be easily thwarted.

Rogue Access Points

- Compromise from Inside
 - AP Installed w/o Knowledge of the Network Admin
 - Likely Not Configured with Security
 - Might be Installed by Dissatisfied Employee
 - Or Simply a User Wanting Wireless Access (Convenience)
 - However Innocent
 - Provides Attacker with Unsecured Entryway to the Packet Communications in a Portion of the Network
 - Create & Publish Organizational Policy Prohibiting Users from Installing their Own Wireless Devices
 - Specifically Access Points & WNICS

Systems Security Management



Eller / MIS
Copyright © 2015, Arizona Board of Regents

Rogue Access Points

A rogue access point is an access point that is installed on a wireless network without the knowledge of the network administrator, so in effect, it is a compromise from within the organization. These rogue access points are not likely to have any security configured so it is much easier to breach a network. Rogues can be installed by a dissatisfied employee, or just simply a user wanting wireless access for their own convenience. However innocent the reason for installing a rogue access point, they provide attackers with an unsecured entryway to packet communications in a portion of the network.

To combat rogue access points, organizations need to create and publish organizational policy that prohibits users from installing their own wireless devices, specifically access points and wireless NICs.

Attacks through Long-Range Antennas

- Attacker Inside the Network
 - Can Accompany a Rogue Access Point with a Long-Range Antenna
 - Increases the Reach of the Signal
 - Makes it Possible to Monitor Network from a Greater Distance w/o being Observed
 - Transmission Wattage can be Increased
 - Furthers Advantage of Long-Range Antenna
 - Gains Distance in the Transmission
 - Same Approach can be Used with WNICs
 - Client Communications Broadcast Far Enough Away to be Picked up by Attacker

Systems Security Management



Eller / MIS Copyright © 2015, Arizona Board of Regents

Attacks through Long-Range Antennas

In some cases, if the attacker is actually inside the network, they can attach a long-range antenna to a rogue access point in order to extend the reach of the signal, making it possible to monitor the network from a greater distance without being observed. In addition, the attacker can increase the transmission wattage, which furthers the advantage of using a long range antenna in order to gain even more distance in the transmission. The same approach can be used with wireless NICs because client communications will be broadcast far enough away to be picked up by the attacker.

Man-in-the-Middle Attacks

- Some Networks Particularly Susceptible
 - Occurs when Attacker Able to Intercept a Message Meant for a Different Computer
 - Attacker Literally Operating Between Two Communicating Computers & has Opportunity to
 - Listen in on Communications
 - Modify Communications
 - Some Wireless Networks
 - Communicating Devices May be Set to Wait up to 30 Minutes Between Initiation & Synchronization
 - From a Few Minutes to 30 Minutes, Provides Ideal Opportunity for Attacker to Synchronize with Initiator & Pretend to be Computer Initiator is Waiting For

Systems Security Management



Eller / MIS Copyright © 2015, Arizona Board of Regents

Man-in-the-Middle Attacks

Some networks are particularly susceptible to a man-in-the-middle attack, where an attacker is able to intercept a message meant for a different computer. The attacker is literally operating between two communicating computers and has the opportunity to both listen in and modify the communication session.

On some wireless networks, communicating devices may be configured to wait up to 30 minutes between initiation of the connection and synchronization. Any timeframe from a few minutes to 30 minutes will provide an ideal opportunity for an attacker to synchronize with the initiator and pretend to be the computer the initiator is waiting to communicate with.

Pitfalls of Wireless Communications

- There are Many Ways to Intercept Wireless Communication if Desired
 - Main Point
 - Wireless Communications Inherently Insecure
 - When You Plan a Wireless Network
 - Avoid Using Wireless Communications on a Network Transporting Sensitive Information
 - Financial Information
 - Company Strategies
 - Organizational Secrets
 - If no Alternative, Consider Using Infrared
 - Configure the Tightest Security Available on **ALL** Devices

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents



Pitfalls of Wireless Communications

There are many ways to intercept wireless communication if an attacker desires. The main point with this is that wireless communications are inherently insecure. When you are planning a wireless network, avoid using wireless communications on a network where it is common to transport sensitive information, such as financial information, company strategies, or organizational secrets. If there is no alternative, and wireless access is required, consider using infrared technologies. Also, make certain you configure the wireless network to use the tightest possible security on ALL devices.

Wireless Security Measures

- Many Wireless Security Measures Can be Taken
 - Open System Authentication
 - Shared Key Authentication
 - Wired Equivalency Privacy (WEP)
 - Service Set Identifier (SSID)
 - 802.1x Security
 - 802.1i Security
 - Wi-Fi Protected Access (WPA/WPA2)

Systems Security Management

What, Me Worry?



Eller / MIS
Copyright © 2015, Arizona Board of Regents

Wireless Security Measures

Having stated that wireless networking is inherently insecure, what security measure can be taken? The primary security measures for wireless networks include:

- Open System Authentication
- Shared Key Authentication
- Wired Equivalency Privacy (WEP)
- Service Set Identifier (SSID)
- 802.1x Security
- 802.1i Security
- Wi-Fi Protected Access (WPA/WPA2)

Open System Authentication

- Any Two Stations can Authenticate Each Other
 - Sending Station Requests to be Authenticated by Destination Station or AP
 - Destination Verifies Request
 - Authentication is Completed
- In this Method, Any Station Requesting Authentication is Granted Access
- OSA Provides Very Little Security
 - Used by Default on Many Wireless Products

Systems Security Management



Eller / MIS

Copyright © 2015, Arizona Board of Regents

Open System Authentication

Open system authentication, or OSA, allows any two wireless stations to authenticate each other on the network. The sending station will request to be authenticated by the destination station or access point. The destination will then verify the request and authentication is completed. Using this method, any station requesting authentication is granted access, making OSA very insecure. Despite this, OSA is the default security setting used on many wireless products.

Shared Key Authentication

- Uses Symmetrical Encryption
 - Same Key Used for Both Encryption & Decryption
 - Authentication Type is Challenge/Response
 - Computer Being Accessed Requests “Shared Secret”
 - Such as Encryption Key Both will Use to Encrypt/Decrypt
 - Following Steps Used:
 - Initiator Sends Authentication Management Request Frame
 - Target Sends Authentication Management Request Frame Asking for Shared Secret
 - Initiator Sends Shared Secret Along with CRC Value to Verify Accuracy of Shared Secret
 - If Target Determines Shared Secret is Correct, Sends Back Message Authentication Successful, Communication Started

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Shared Key Authentication

Shared key authentication uses symmetrical encryption, so the same key is used for both encryption and decryption. When authenticating to a wireless network using the shared key, the user is presented with a challenge/response authentication. The computer being accessed will request the “shared secret,” which is the encryption key both will use to encrypt and decrypt. By selecting shared key authentication, the following steps will be used by systems on the network:

- Initiator Sends Authentication Management Request Frame
- Target Sends Authentication Management Request Frame Asking for Shared Secret
- Initiator Sends Shared Secret Along with CRC Value to Verify Accuracy of Shared Secret
- If Target Determines Shared Secret is Correct, Sends Back Message Authentication Successful, Communication Started

Wired Equivalent Privacy

- In 802.11 Communication, Shared Secret is WEP Key
 - Used for Encryption & Decryption
 - Key Itself is Encrypted
 - WEP Developed by IEEE
- Two Stations Used Same Encryption Key Generated by WEP Services
 - Encryption Key is 40 bits or 104 bits Long
 - Includes Checksum & Initialization Information
 - Total Actual Encryption Length of 64 or 128 bits Long
- WEP not Intended to Provide Fully Hardened Security
 - Only Intended as a Basic Step
 - Sniffers can Intercept & Decode WEP Key
 - Also Vulnerable to Brute Force

Systems Security Management



Eller / MIS Copyright © 2015, Arizona Board of Regents

Wired Equivalent Privacy

In 802.11 wireless network communication, the wired equivalent privacy, or WEP, uses a shared secret as a WEP encryption key. This key is then used to encrypt and decrypt data during transmission, and the key itself will be encrypted to better protect it during transmission. WEP was developed by the IEEE standards organization for securing 802.11 wireless networks.

When using WEP, two stations will use the same encryption key that is generated by WEP services. The encryption key is either 40-bits or 104-bits long, and when the key includes a checksum and initialization information, the total actual encryption length will be 64-bit or 128-bits long. WEP was not designed to provide fully hardened security for wireless communications, it was intended to be a basic step into wireless security. Modern sniffers can intercept and decode WEP keys easily, and the standard is also vulnerable to brute force attacks.

Service Set Identifier

- Ensure All Purchased Devices Support SSID
 - SSID is Identification Value Typically up to 32 Characters in Length
 - **NOT** a Password
 - A Value Defines a Logical Network for All Devices
 - Might be a String Value Describing Network Purpose
 - E.g. UA Public
 - Not Likely to Thwart Attacker, but Wise to Use One
 - Used in ESS Topology Networks
 - As a First Step, Configure Wireless Network Devices to Use SSIDs
 - Provide a New Value to Replace Default

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

Service Set Identifier

Network Administrators need to ensure that all purchased wireless devices support the Service Set Identifier, or SSID. An SSID is an identification value, typically up to 32 characters in length, that defines a logical network for all connected devices. Remember, this is NOT a password! The SSID may be a string value that describes the network's purpose, for example: UA Public provides a wireless network with no security for public use. The SSID is not likely to thwart an attacker, but it is wise to use one. In fact, it is also recommended that wireless devices are configured to not broadcast the SSID, making it more difficult to detect the wireless network.

SSIDs are used specifically in wireless networks using the ESS topology. As a first step, network admins should configure wireless devices to use SSIDs, providing a new value to replace the default.

802.1x Security

- Wireless & Wired Authentication Approach
 - Offered by IEEE, Supported by Some OS's
 - Port-Based Form of Authentication
 - Communications Defined Over a Port (Wireless or LAN)
 - Port can Act in Two Roles (One at a Time)
 - Uncontrolled Port
 - » Allows Communication Regardless if Authentication has Actually Occurred
 - Controlled Port
 - » Allows Only Authenticated Communications
 - For Best Security
 - Authentication Server Should be a Different Computer than Authenticator
 - Remote Authentication Dial-In User Service (RADIUS) For Example

Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents

802.1x Security

802.1x security is both a wireless and a wired authentication approach offered by the IEEE and supported by some operating systems. 802.1x security is a port-based form of authentication. Communications are defined over a specific port, either wireless or wired and the port can act in two different roles, although only one at a time. Uncontrolled ports will allow communication regardless of whether or not authentication has actually occurred. Controlled ports allow for only that communication which has been authenticated. For the best security, the authentication server should be a different system than the authenticator, for example: using the Remote Authentication Dial-In User Service, or RADIUS.

802.1x Security

- 802.1x does not Include Encryption
 - Can be Setup to Work with Extensible Authentication Protocol (EAP)
 - EAP can Employ Many Encryption Methods
 - Smart Cards, DES/3DES, Certificates
 - Evolving Versions of EAP
 - EAP-TTLS (EAP-Tunneled Transport Layer Security)
 - Designed to Provide More Secure Connection or Controlled Port for Entire Authentication Process
 - Protecting All Steps in Authentication Process Opens Way to Use Additional Authentication/Encryption Methods
 - EAP-TTLS Requires Use of Certificates
 - Protected EAP (PEAP)
 - Developed as Alternative to Reduce Complexity
 - Does not Require the Use of Certificates

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents

802.1x Security (continued)

Another important item to note is 802.1x security does not include encryption; however, it can be configured to work with the Extensible Authentication Protocol, or EAP. EAP can employ many encryption methods, such as smart cards, DES/3DES, and certificates. Evolving versions of EAP, such as EAP with Tunneled Transport Layer Security, or EAP-TTLS, is designed to provide more secure connections or controlled ports for the entire authentication process. By protecting all steps in the authentication process will open ways to use additional authentication and encryption methods. EAP-TTLS requires the use of digital certificates. Another EAP variant: Protected EAP, or PEAP was developed as an alternative to reduce the complexity of EAP and does not require the use of digital certificates.

802.1i Security

- Relatively New Standard for 802.11
- Compatible with 802.1x
 - Also Used Temporal Key Integrity Protocol (TKIP)
 - Creating Random Encryption Keys from Master Key
 - TKIP Similar to Block Cipher Method of Encryption
 - Packet is Equivalent to Block
 - Creates Unique Encryption Key for Each Packet
 - Some Encryption Experts Believe this Technique Means it would Take an Attacker Over 100 Years to Decrypt
 - Further Encrypts Data in Wireless Packet Using AES
 - Combines Private Key & Block Cipher Technique

Systems Security Management

Eller / MIS

Copyright © 2015, Arizona Board of Regents

802.1i Security

802.1i security is a relatively new standard for 802.11 networks. It is compatible with 802.1x security; however, it also adopts the use of the temporal key integrity protocol, or TKIP, allowing for the creation of random encryption keys from a master key. TKIP is similar to the block cipher method of encryption. Each data packet is the equivalent of a block of data. TKIP will then create a unique encryption key for each packet. Because of this encryption method, some experts believe this technique means it would take an attacker over 100 years to decrypt a communications session. In addition, 802.1i security further encrypts the data in wireless packets using the Advanced Encryption Standard, or AES, combining a private key encryption with a block cipher technique for increased security.

Wi-Fi Protected Access

- WPA – Created by Wi-Fi Alliance
 - Effort to Overcome Weaknesses of WEP
 - Uses Temporal Key Integrity Protocol
 - Standards Based Wireless Security
 - Can Use RADIUS or LDAP for Authentication
- WPA2 – Created For Additional Security
 - Uses TKIP or AES for Encryption
 - 802.11i Security Standard
 - Backwards Compatible with WPA
 - Can Use RADIUS or LDAP for Authentication

Systems Security Management

Eller / MIS 

Copyright © 2015, Arizona Board of Regents

Wi-Fi Protected Access

Wi-Fi Protected Access, or WPA, was created by the Wi-Fi Alliance in an effort to overcome the weaknesses of WEP. WPA uses TKIP for encryption and is a standards-based wireless security method. In addition, WPA can use a RADIUS or LDAP server for authentication purposes.

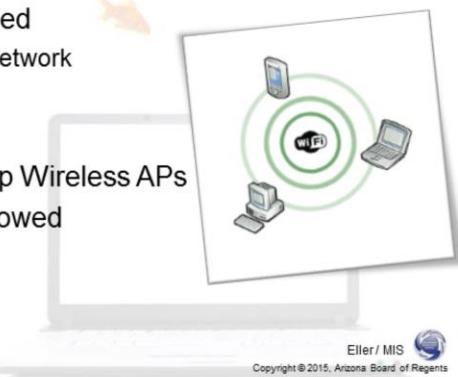
In order to improve the security of WPA, the Wi-Fi Alliance created its successor: WPA2. WPA2 uses either TKIP or AES for encryption and is considered to be an 802.1i security standard. WPA2 remains backwards compatible with WPA and can use RADIUS or LDAP for authentication.

Wireless Policy

- Based on the Inherent Insecurity of Wireless Technology
 - Organizations Must Address Wireless Networking in Organizational IT Policies
 - Define if Wireless to be Used
 - What Type of Wireless Network
 - Who can Use it
 - Security Method(s) Used
 - Users Not Allowed to Setup Wireless APs
 - What Kind of Access is Allowed
 - Topology Used
 - Perform Cell-Site Survey

Systems Security Management

Eller / MIS Copyright © 2015, Arizona Board of Regents



Wireless Policy

Based on the inherent insecurity of wireless network technology, organizations must address wireless networking in organizational IT policy. Policies should include the following information:

- Define if Wireless to be Used, and What Type of Wireless Network to Adopt
- Who can Use it
- Security Method(s) Used
- Users Not Allowed to Setup Wireless APs
- What Kind of Access is Allowed
- Topology Used
- Perform Cell-Site Survey

Next Module...

- Internet Security
- Hypertext Transport Protocol (HTTP)
- S-HTTP & HTTPS
- File Transfer Protocol
- Network File System
- Samba & Server Message Block
- Configuring Web Browsers for Security
- Configuring Remote Access Services for Security
- Microsoft Remote Access Service
- Understanding Remote Access Protocols
- Configuring RAS Policy
- Virtual Private Networks
- Security on a Virtual Private Network

Systems Security Management

Eller / MIS 
Copyright © 2015, Arizona Board of Regents

In the next module we will discuss Web, Remote Access, and VPN Security, including:

- Internet Security
- Hypertext Transport Protocol (HTTP)
- S-HTTP & HTTPS
- File Transfer Protocol
- Network File System
- Samba & Server Message Block
- Configuring Web Browsers for Security
- Configuring Remote Access Services for Security
- Microsoft Remote Access Service
- Understanding Remote Access Protocols
- Configuring RAS Policy
- Virtual Private Networks
- Security on a Virtual Private Network

References

- Geier, J. (2003, March 30). WPA Security Enhancements. *Wi-Fi Planet*. Retrieved from <http://www.wi-fiplanet.com/tutorials/article.php/2148721>.
- Haskin, D. (2007, May 16). FAQ: 802.11n Wireless Networking. *ComputerWorld*. Retrieved from http://www.computerworld.com/s/article/9019472/FAQ_802.11n_wireless_networking.
- IEEE 802.11n-2009. (2010, January 30). *Wikipedia: The Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/IEEE_802.11n-2009.
- Palmer, M. (2004). Guide to Operating System Security, 1st Edition. *Thomson Course Technology*. Canada.
- Wi-Fi Alliance: Articles. (2010). *Wi-Fi Alliance*. Retrieved from http://www.wi-fi.org/knowledge_center_overview.php?type=7.

Systems Security Management

Eller / MIS
Copyright © 2015, Arizona Board of Regents