

Cyber Security Technologies

Session 15 – Wireless Network Security & Attacks

Shawn Davis
ITMS 448 – Spring 2016

Slides contain original content from Davis, S. and may contain content from Ch.24 of Stallings, W. and Brown, B, Computer Security 2ed; Pearson Education, Inc. 2012

Homework and Projects

- I have now graded all homework except for Homework13 which was due last night
- I will review the project slides and video submissions this week and will email each student with any suggestions that should be made before the class presentations next week

IIT Instructor/Course Evaluations

- I will now give everyone 10 minutes to complete an evaluation. If you have already done so, feel free to review your slides or recent homework feedback
 - Certificate students might not have evaluations
- Your feedback is anonymous and Dr. Carlson and Prof. Trygstad read each and every review for all courses
- I also review all feedback for this course and appreciate your effort in providing it!

Overview

Part I – Wireless Introduction

Part II – Common Wireless Security Threats

Part III – Wireless Attack Demo

Part I

Wireless Introduction

Wireless Network Components

- Wireless Client
 - Computer with internal or external wifi card
 - Cell phone
 - RF scanner
 - Wireless sensor
- Wireless Access
 - Wireless Router
 - Wireless Access Point

Typical Wireless Router

- Public interface connects to modem
- Serves as network gateway
- Single, dual, or triple band wireless radio(s)
- 4-port wired switch
- DHCP server & NAT
 - Hands out private IP addresses to connected clients

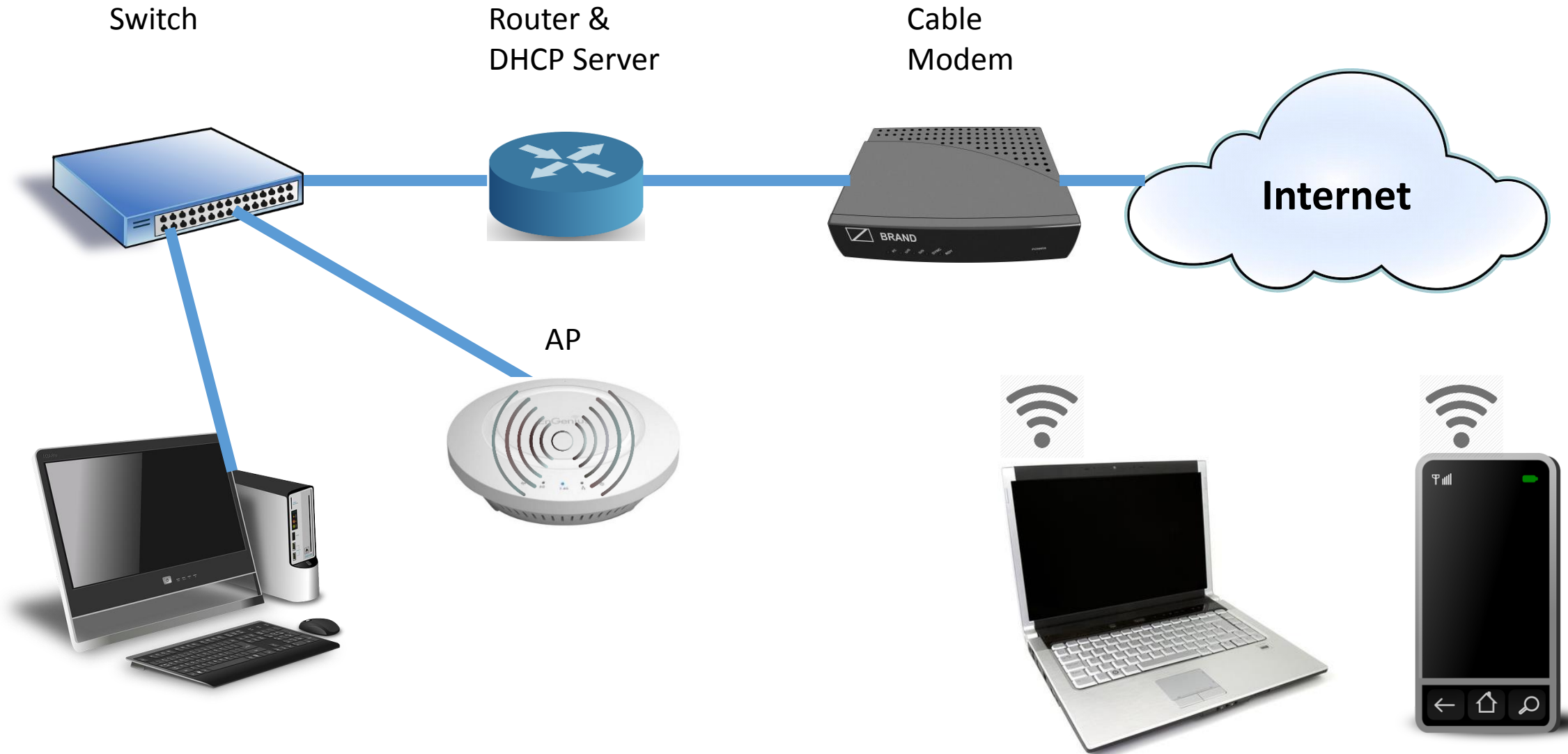
Basic Wireless Router Network Topography



Typical Wireless Access Point

- AP's switch interface connects to network switch
- Does not serve as network gateway
- No DHCP server or NAT
- Single, dual, or triple band wireless radio(s)
- AP Receives its IP address from network DHCP server
- Wireless clients connected to the AP receive their IP addresses from network DHCP server

Basic Wireless Access Point Network Topography



How Wireless Fits in the OSI Model

Application

Presentation

Session

Transport

Network

Data Link

Physical Link

802.2 Logical Link Control (LLC): Flow/Error Control
802.11 Media Access Control (MAC): Addressing, CSMA/CA

Radio Frequency (RF) Waves, Channel Selection, etc.

CSMA/CD vs. CSMA/CA

- Carrier Sense Multiple Access / Collision Detection (CSMA/CD)
 - Wired LAN (Ethernet)
 - Steps:
 1. Wait for cable to be free of traffic
 2. Transmit the frame
 3. If a collision occurs, stop the transmission
 4. Retransmit after a random time

CSMA/CD vs. CSMA/CA

- Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)
 - Wireless LAN
 - Steps:
 1. Listen for wireless signals to determine if another client is transmitting or not
 2. If client is transmitting, wait a random time
 3. Listen again and if clear, transmit the frame
 4. Client waits for acknowledgement packet
 5. If acknowledgement packet does not arrive quickly, a collision is assumed and process starts over at step 3.

802.11

- IEEE wireless standard that defines the specs for the Physical and MAC layers
- Popular standards are:
 - 802.11b: 2.4 GHz, up to 11Mbps, Longer range
 - 802.11a: 5 GHz, up to 54 Mbps, Shorter range
 - 802.11g: 2.4 GHz, up to 54 Mbps, Longer range
 - 802.11n: 2.4/5 GHz, up to 300 Mbps, Longer range
 - 802.11ac: 5 GHz, up to 1300 Mbps, Beamforming
 - Theoretical speed could reach 7 Gbps

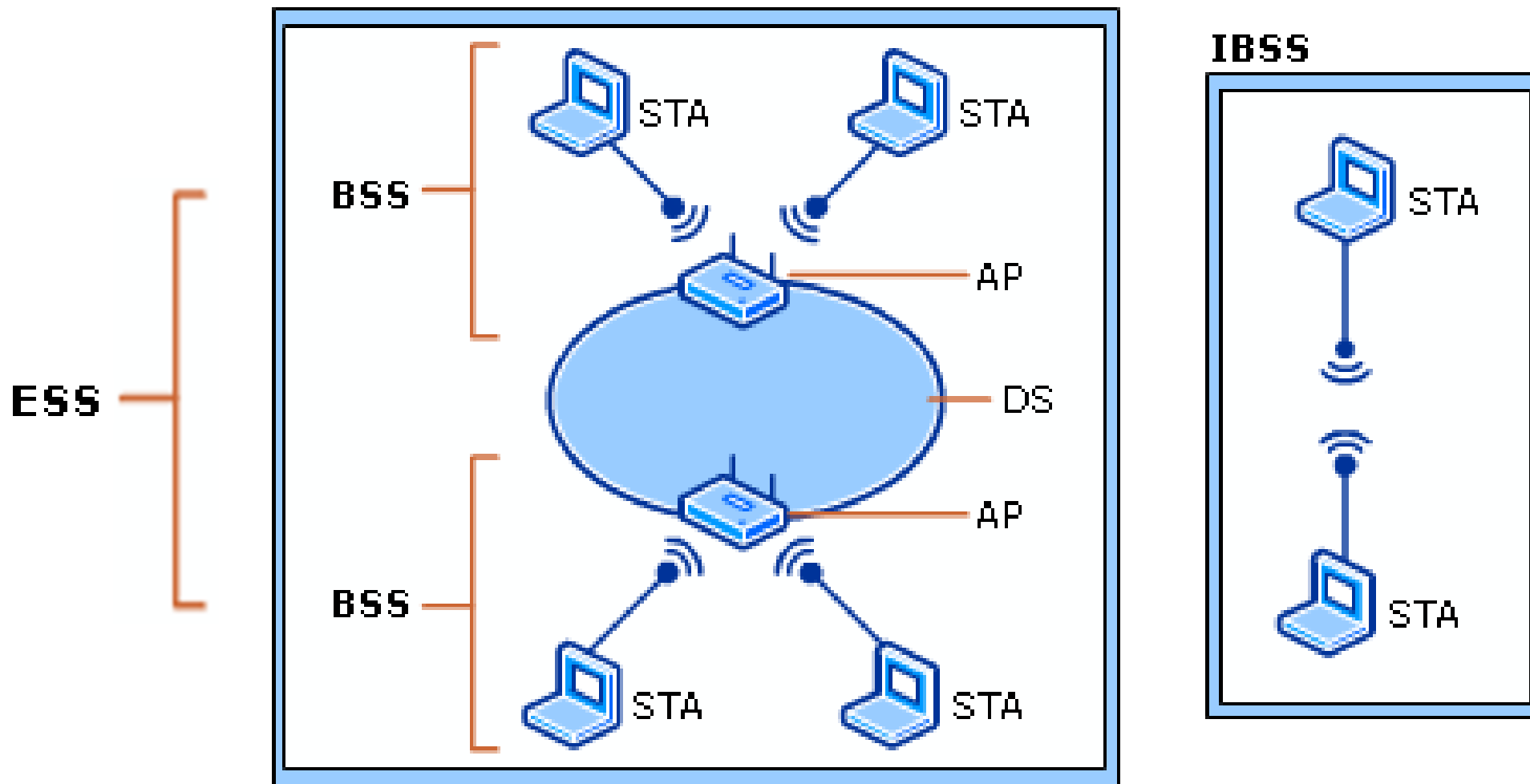
IEEE 802.11 Architecture Terms

- Station (STA)
 - The wireless client (laptop, phone, etc.)
- Basic Service Set (BSS)
 - Wireless network of one AP supporting one or many clients
- Extended Service Set (ESS)
 - Two or more BSSs that are connected via a wired network

IEEE 802.11 Architecture Terms (Cont.)

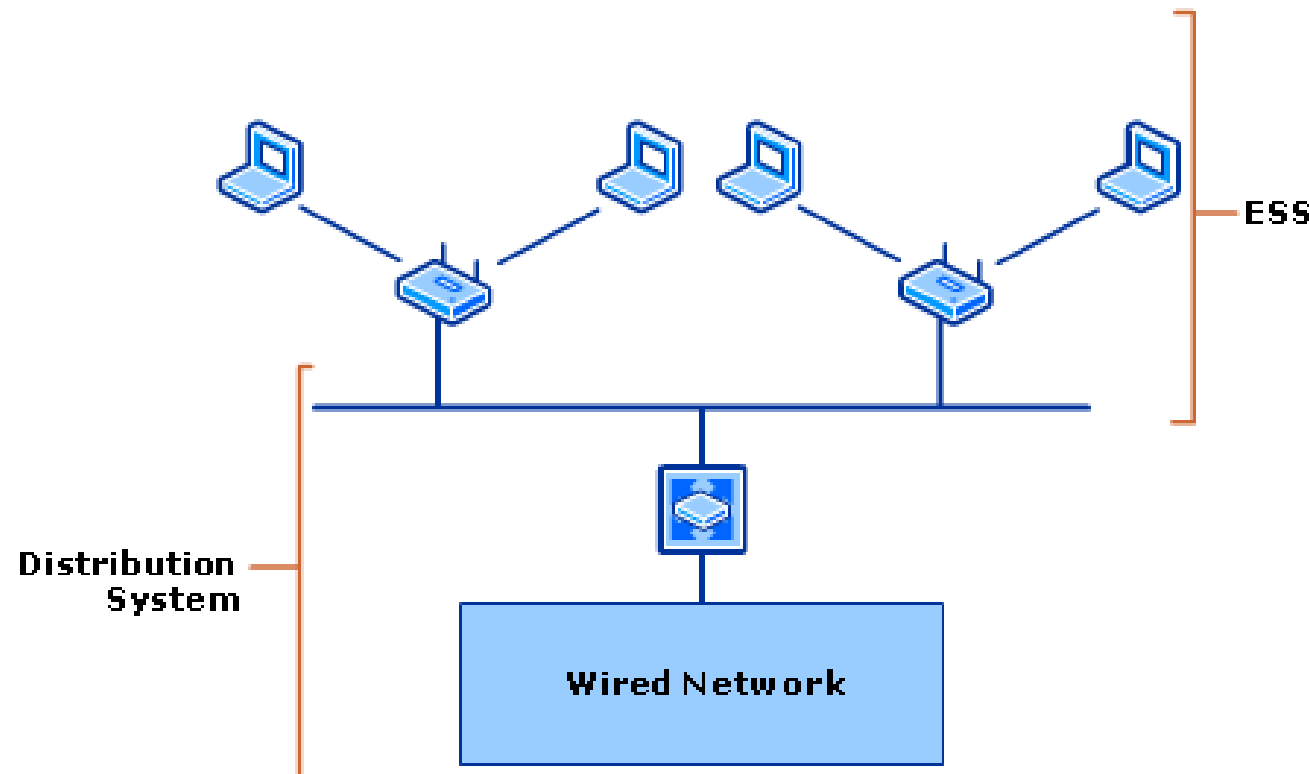
- Distribution System (DS)
 - In an ESS, multiple BSSs are connected by the DS
 - Allows a client to move or roam from one BSS to another BSS
- Independent Basic Service Set (IBSS)
 - Ad hoc wireless network where clients connect directly to each other (No APs involved)

802.11 Architecture Diagram



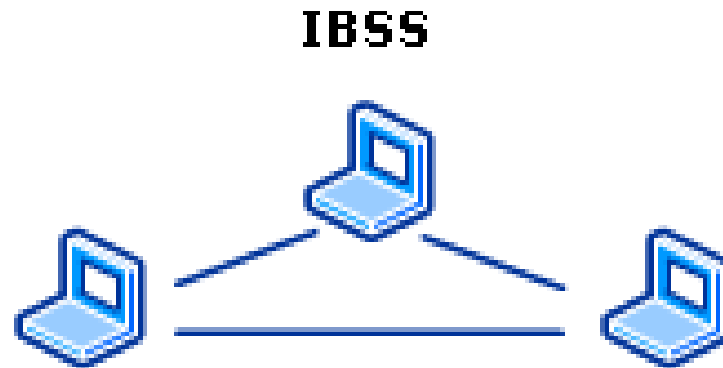
802.11 Operating Modes

- Infrastructure Mode
 - One or more BSS use AP to access traditional wired network



802.11 Operating Modes

- Ad Hoc Mode
 - One or more clients form an Independent Basic Service Set (IBSS) AKA: peer-to-peer mode



Message Delivery within a DS

- Association
 - Initial association between client and AP
- Reassociation
 - Allows established association to be transferred from one AP to another / one BSS to another
- Disassociation
 - Notification from a client or an AP that an existing association is terminated

Wireless Client Association

- APs announce their presence by sending out periodic management frames called Beacons
- Beacons contain:
 - Service Set Identifier (SSID)
 - Name of the wireless network
 - Supported data rates
 - Capability information of device/network
- Client selects AP after listening for beacons

Wireless Authentication vs. Association Note

- Authentication occurs when a station (client) proves its identity to another station or AP
- Station can be authenticated with several APs at once but only associated with one at a time

Wireless Security Protocols

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access v2 (WPA2)
 - Also known as 802.11i

Wired Equivalent Privacy (WEP)

- Original security protocol for wireless
- Highly insecure due to vulnerabilities
- Encrypts data sent between a client and an AP
- Uses RC4 symmetric stream cipher with 40-bit and 104-bit encryption key options
- Uses Initialization Vector (IV) to randomize keys

Wired Equivalent Privacy (WEP) (Cont.)

- User may enter Passphrase of secure345# for example
- WEP combines secure345# with the IV to create the encryption key
- WEP encrypts packet with key and sends IV to other side in plain text
- Unfortunately, WEP uses small IV and keys are reused

Wired Equivalent Privacy (WEP) (Cont.)

- Attacker generates large amount of traffic to collect ciphertext and plaintext IVs
 - Attacker can spoof MAC of a connected client, associate to the AP and generate various traffic
- Attacker can take packet capture of traffic and use cryptanalysis to determine WEP key in a short time
- I will demonstrate this at the end

Wi-Fi Protected Access (WPA)

- Temporary quick replacement for WEP until WPA2 could be finished
- Clients didn't need to upgrade hardware
- Uses RC4 cipher with Temporal Key Integrity Protocol (TKIP)
- TKIP was a little better than WEP but was eventually cracked as well
- Later, strong AES cipher introduced as replacement for TKIP
 - Required software updates

Wi-Fi Protected Access (WPA)

- If you have to use WPA, try to use it with AES only
 - Again, you may have to upgrade software in older clients
- WPA has since been replaced with WPA2
- Client can use Pre-Shared Keys (PSK) or Enterprise Mode to generate master key

Pre-Shared Keys (PSK) vs. Enterprise Mode

- PSK
 - Also known as Personal mode
 - Simple to configure
 - User enters passphrase to generate keys
 - Encryption but no individualized authentication
- Enterprise Mode
 - 802.11X server (RADIUS) that handles central authentication for individual wireless clients before key distribution

802.11X

- IEEE standard for network port authentication
- Can be used for wired or wireless LANs
- For a wireless LAN, 802.11X:
 - Provides key management and can use any cipher
 - Uses Extensible Authentication Protocol (EAP) as framework for authentication
 - Certificate-based
 - One-time passwords
 - Smart cards
 - Etc.

802.11X

- Authentication occurs with back-end server
 - Requests and responses are just passed through APs

802.11X Port Authentication Steps

1. Client associates with an AP
2. AP blocks access to LAN by default
3. Client provides login credentials (login/password, digital certificate, etc.)
4. Client and authentication server perform mutual authentication through the AP
5. When authentication is complete, server and client determine encryption session key (WEP, WPA, WPA2, etc.) that is unique to client

802.11X Port Authentication Steps

6. Server sends session key over wired LAN to the AP
7. AP encrypts its broadcast key with the session key and sends encrypted broadcast key to client
8. Client decrypts broadcast key with session key
9. Client and AP activate encryption (WEP, WPA, WPA2, etc.) to secure data transmissions that may now occur securely

Wired vs. Wireless Security Needs

- Wired LAN clients must be physically connected to transmit and receive which offers some built in protection
- Wireless LAN clients in radio range can simply transmit and receive at will
- Therefore, Wireless LANs suggest increased need for robust security
- WEP and WPA v1 attempted this but failed

Wi-Fi Protected Access v2 (WPA2)

- Also known as IEEE 802.11i as well as Robust Security Network (RSN)
- Replaced WEP and WPA
- Most secure option available currently
- Uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on AES
- Can use 802.1X

Part II

Common Wireless Security Threats

Default Passwords

- Ex: WRT54GL
 - Login: [none]
 - Password: admin
- Defense:
 - Change them!

The screenshot shows the SHODAN search interface with the keyword 'WRT54GL' entered in the search bar. The results are categorized into 'Services' and 'Top Countries'. The 'Services' section lists various protocols and their counts: HTTP Alternate (10,027), HTTPS (2,395), HTTP (1,300), Telnet (112), and HTTP (36). The 'Top Countries' section lists: United States (2,277), Germany (1,053), Romania (1,005), Canada (976), and Hungary (846). The main results area displays two '401 Unauthorized' entries. The first entry is for IP 79.126.139.228, identified as 'ONE Telecommunications Services DOOEL Skopje', with a date of 11.03.2014. The second entry is for IP 64.250.55.163, identified as 'Nex-Tech', also dated 11.03.2014. Both entries show HTTP/1.0 401 Unauthorized status, server: httpd, and a WWW-Authenticate header with the realm 'WRT54GL'. A third entry for IP 213.215.68.141 is partially visible, identified as 'GTS Slovakia, a.s.'. At the bottom right, the text 'DD-WRT v24-sp2 mini (c) 2009 NewMedia-NET GmbH' and 'Release: 10/10/09 (SVN revision: 13064)' are visible, along with the text 'WRT54GL login:'.

SHODAN WRT54GL Search

Services

HTTP Alternate	10,027
HTTPS	2,395
HTTP	1,300
Telnet	112
HTTP	36

Top Countries

United States	2,277
Germany	1,053
Romania	1,005
Canada	976
Hungary	846

401 Unauthorized
79.126.139.228
ONE Telecommunications Services
DOOEL Skopje
Added on 11.03.2014
Skopje

HTTP/1.0 401 Unauthorized
Server: httpd
Date: Mon, 10 Mar 2014 22:14:45 GMT
WWW-Authenticate: Basic realm="WRT54GL"
Content-Type: text/html
Connection: close

401 Unauthorized
64.250.55.163
Nex-Tech
Added on 11.03.2014
Russell

HTTP/1.0 401 Unauthorized
Server: httpd
Date: Tue, 11 Mar 2014 01:08:04 GMT
WWW-Authenticate: Basic realm="WRT54GL"
Content-Type: text/html
Connection: close

213.215.68.141
GTS Slovakia, a.s.
Added on 11.03.2014

DD-WRT v24-sp2 mini (c) 2009 NewMedia-NET GmbH
Release: 10/10/09 (SVN revision: 13064)

WRT54GL login:

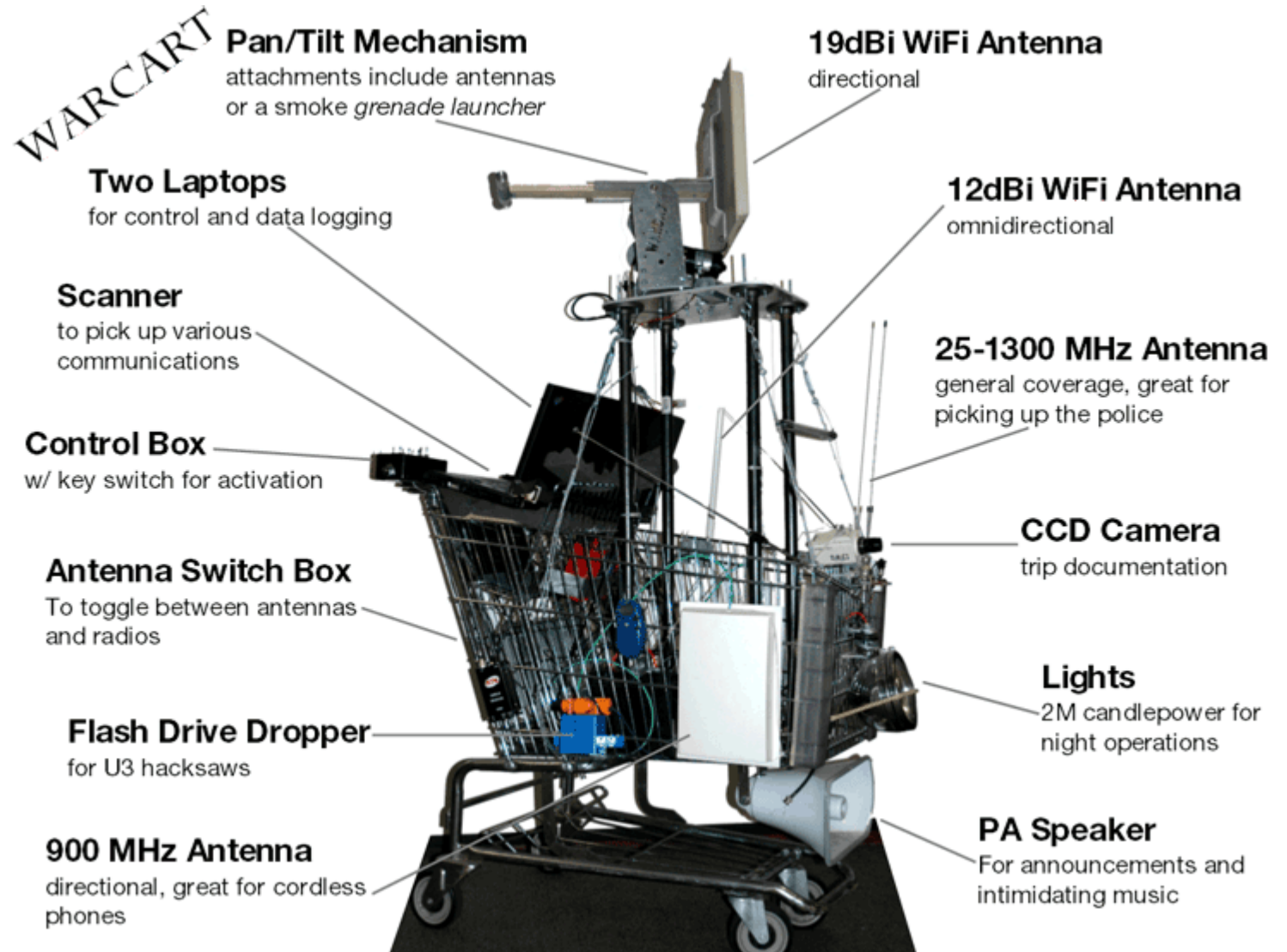
Wardriving

- I will demo cracking WEP at the end

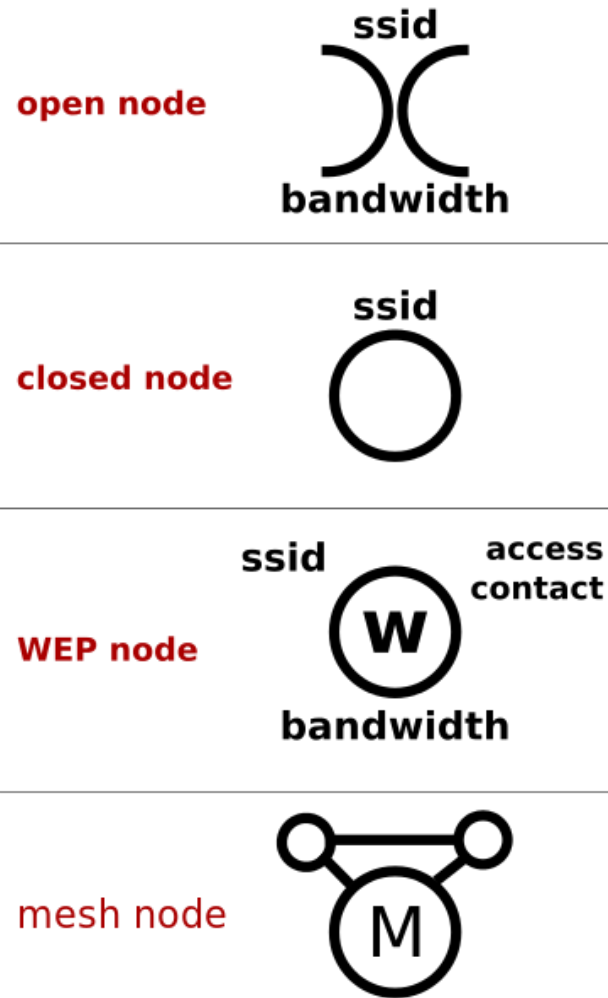


Or Warcarting...

- MIT Student Project:



Warchalking



MAC Spoofing

- Ex: Attacker eavesdrops on network traffic of AP secured by WEP
- Sends disassociation message but is blocked by MAC filtering
- Spoofs own computer with MAC of a client connected to the AP
- Attacker successfully sends disassociation message with spoofed MAC

MAC Spoofing

- Attacker generates other traffic with spoofed MAC and eventually cracks WEP key
- Attacker connects to network using spoofed MAC and WEP key, effectively evading MAC address filtering

Rogue Access Points

- AP placed on a LAN by insider or attacker
- Sometimes hidden in wiring closets or near a window with an open network port
- SSID broadcast often disabled
- Attacker captures traffic in parking lot

Evil Twins

- An AP with the same SSID as a legitimate AP
- Often placed in public free hotspots
 - Coffee Shops
 - Airports
 - Hotels
- Attacker may serve up “logon” web page to capture credentials
- ...or just capture all of the traffic

Ad-Hoc Privileges

- No authentication usually
 - Anyone nearby can connect
- Ex: Two clients connected directly to each other's wireless cards
 - If client A is logged in as an administrator, client B may have administrative rights to client A's system
- Connect as a limited privilege user if using Ad-Hoc wireless

MiTM Attacks

- Wireless clients are more susceptible since APs broadcast all traffic
- Can skip flooding a switch, arp spoofing, etc. to be able to see all traffic

DoS

- Attacker continually bombards an AP with traffic
- Attacker can also spoof MAC of AP and send deauthentication and disassociation frames
- Power Save Exploits
 - Mobile wireless clients can enter sleep state to conserve battery life
 - AP caches traffic until client wakes up
 - Attacker can send spoofed power save poll message to make the AP transmit and discard the traffic destined for the sleeping client before the client wakes up

DoS (Cont.)

- Attacker can circumvent MAC backoff wait time to gain access to a wireless channel before a legitimate device does
- Unintentional DoS can occur if too many neighboring APs are on the same channel

DoS Countermeasures

- Motorola has a Wireless Intrusion Prevention System (WIPS) that can help pick optimum channels and use triangulation to try to find the malicious attacker
- Preventing DoS is difficult on a WLAN
 - A determined attacker can always disrupt a wireless network

Vulnerable Wireless Drivers

- Can attack client even if not connected to a network!

```
< metasploit >
.....
      \  (oo)_____)
       (  (_____) \
        ||..|| *

      =[ msf v3.0-beta-dev
+ -- --=[ 178 exploits - 104 payloads
+ -- --=[ 17 encoders - 5 nops
      =[ 30 aux

msf > use windows/driver/broadcom_wifi_ssld
msf exploit(broadcom_wifi_ssld) > set PAYLOAD windows/adduser
PAYLOAD => windows/adduser
msf exploit(broadcom_wifi_ssld) > set INTERFACE wifi0
INTERFACE => wifi0
msf exploit(broadcom_wifi_ssld) > set DRIVER madwifing
DRIVER => madwifing
msf exploit(broadcom_wifi_ssld) > set PASS moo
PASS => moo
msf exploit(broadcom_wifi_ssld) > exploit
[*] Sending beacons and responses for 60 seconds...
```

RADIUS Server Impersonation Attack

- Attacker impersonates AP and RADIUS Server
- Attacker issues rogue certificate to authenticating client
- Client proceeds to authenticate
- Attacker captures authentication traffic and attempts to crack it offline

Anonymity Attacks

- Attack involving an attacker attempting to locate a specific target's Wi-Fi network
- Wireless cards search for preferred networks by name periodically
- Attacker can use a sniffer to capture management frames containing the SSID names

Anonymity Attacks

- Additionally, attacker can use Wigle to determine the location of a specific SSID if you know the general location
- Ex: I have seen an SSID named PrettyFly4aWifi downtown a few times

Wigle

Network Search

[General Search](#)[Network Detail](#)










Query for networks

Latitude: to: Longitude: to: Search Radius Tolerance(+/- degrees): ▼BSSID/MAC: SSID or Network Name: Last Observed: ☐ Must Be a FreeNet ☐ Must Be a Commercial Pay Net ☐ Only Networks I Was the First to Discover

Addresses are for the U.S. only (2002 Census data)

Street Address: State: Zip: [Query](#)[Reset](#)

Wigle

Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel	Bcn Int.	QoS
map	00:11:95:37:2E:89	PrettyFly4aWiFi		infra	1969-12-31 18:00:00	2012-03-18 21:26:34		41.80376053	-87.58541107	6		0
map	00:12:17:32:BB:98	PrettyFly4Awifi		infra	2013-11-02 16:26:18	2013-11-08 13:20:31		40.10986710	-88.21926117	6		0
map	00:1C:10:4D:5B:B2	PrettyFly4aWifi		infra	2011-10-18 08:13:57	2011-12-14 18:14:15		41.94240570	-87.65366364	6		6
map	00:1c:df:e2:2f:99	PrettyFly4aWiFi		infra	0000-00-00 00:00:00	2013-02-01 17:24:08		42.13222885	-88.46495819	6	100	7
map	00:1F:B3:B9:F5:69	PrettyFly4aWiFi		infra	2012-09-14 11:42:40	2014-06-08 14:49:31		42.13239670	-88.46585083	11		2
map	00:8E:F2:71:DF:2E	prettyfly4awifi		infra	2013-10-01 17:52:49	2013-10-08 16:10:09		40.81161499	-91.10579681	10		1
map	08:86:3B:19:C8:4C	PrettyFly4aWIFI		infra	2011-09-30 18:12:59	2011-10-03 20:24:43		38.78588104	-90.51069641	6		1
map	14:D6:4D:24:13:06	prettyfly4awifi		infra	2012-03-18 14:55:34	2012-03-18 19:51:37		41.90641403	-87.67357635	6		0
map	20:10:7A:7A:27:0E	PrettyFly4aWiFi		infra	2014-01-31 08:32:57	2014-02-03 08:46:16		38.80654144	-90.54557800	8		0

Wigle



Car Attacks

- Two main methods:
 1. Interception and replay of code (if static)
 - Defense is to use rolling codes
 2. Amplification of remote keyless entry signal from car searching for nearby keys
 - Defense is to put remote in freezer

Notable WLAN Attacks

- Lowe's (2003)
 - Attackers accessed an unencrypted AP that didn't require authentication
 - Planted Credit Card sniffing software and ended up crashing POS system

Notable WLAN Attacks (Cont.)

- Marshalls (2007)
 - Attackers hacked WEP WLAN at a store
 - Stole 45-200 million CC numbers
 - Stole 450k driver's licenses and many SS#s
 - Cost of breach could surpass 1 billion dollars in 5 years

Notable WLAN Attacks (Cont.)

- Pentagon FCU, Citibank (2007)
 - Attacker used high-powered antenna to intercept wireless traffic
 - Used information to gain access to Pentagon FCU, Citibank, and a government employee's computer

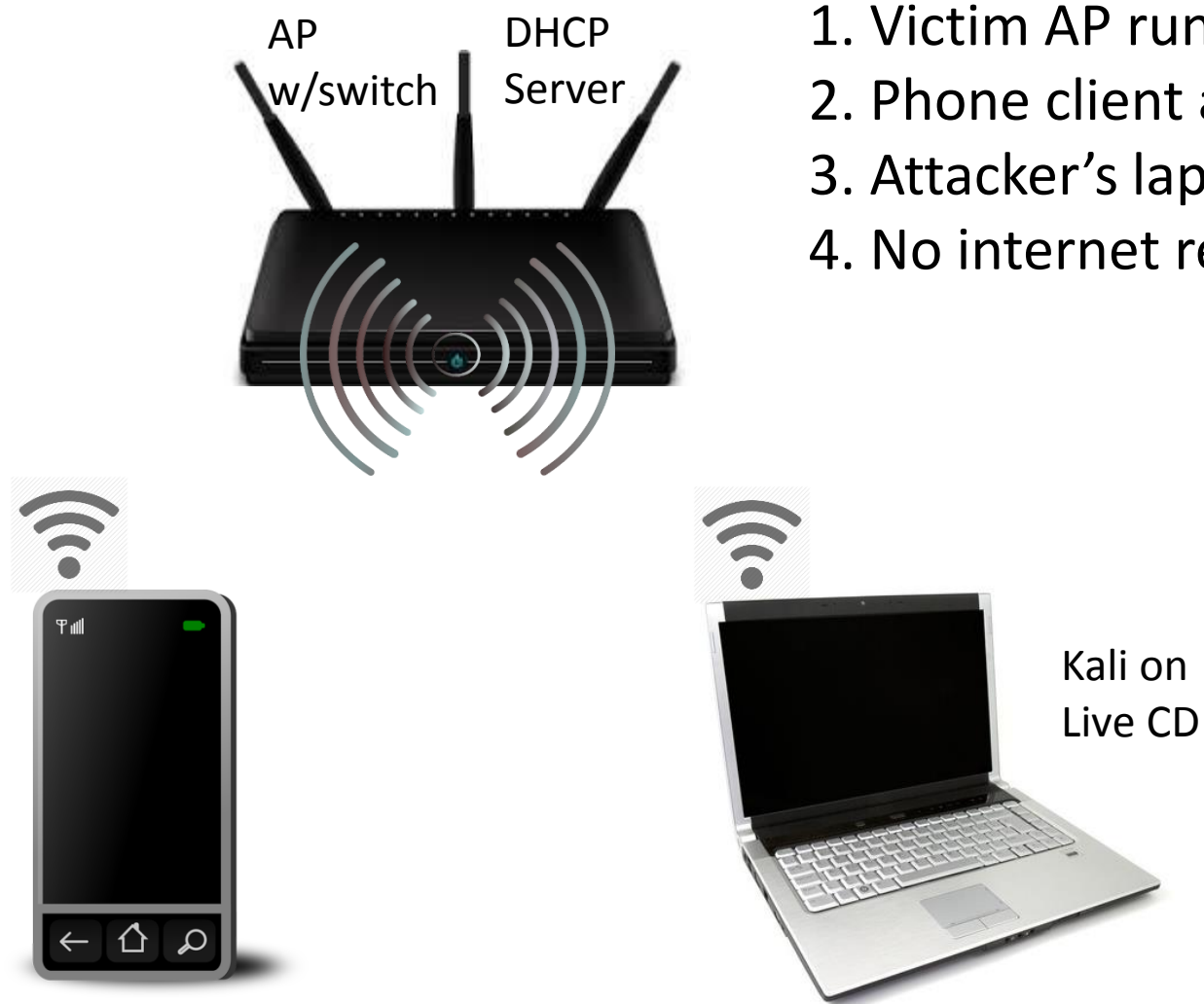
Part III

Wireless Attack Demo

Wireless Attack Demo

- Since your systems don't have wireless cards in them, I will just demo the following:
 - Finding the MAC addresses of an AP and its attached clients
 - Capturing traffic of an AP
 - Evading MAC address filtering
 - Cracking WEP using the IV vulnerability
 - General settings on a wireless router
 - Revealing the SSID of a wireless router that has the SSID broadcast feature turned off

Wireless Hacking Environment



1. Victim AP running WEP
2. Phone client attached to Victim AP
3. Attacker's laptop
4. No internet required

Future Items

- We will have a few early presentations today and the rest next week
- Next Monday (4/25) you will present your individual project slides and video
 - Attendance is mandatory
- Final Exam is in two weeks (5/2) in this lab from 5pm-7pm
 - Note the exam is at **5pm** and not 5:30pm.
- Next, we will cover the Final Review and then a few presentations