



Client-Side Wireless Attacks and Defenses

Matthew Neely
SecureState



- Matt Neely CISSP, CTGA, GCIH, GCWN -
Manager of the Profiling team at SecureState
 - Areas of expertise: wireless security, penetration testing, physical security, security convergence and incident response
 - 10 years of security experience
- Previously
 - Security analyst at a top 10 bank
 - Security subject matter expert on the Financial Service Technology Consortium (FSTC) mobile banking working group
 - Formed and ran the TSCM team at a Fortune 200 company
- Outside of work:
 - Co-host on the Security Justice podcast
 - Board member for the North Eastern Ohio Information Security Forum



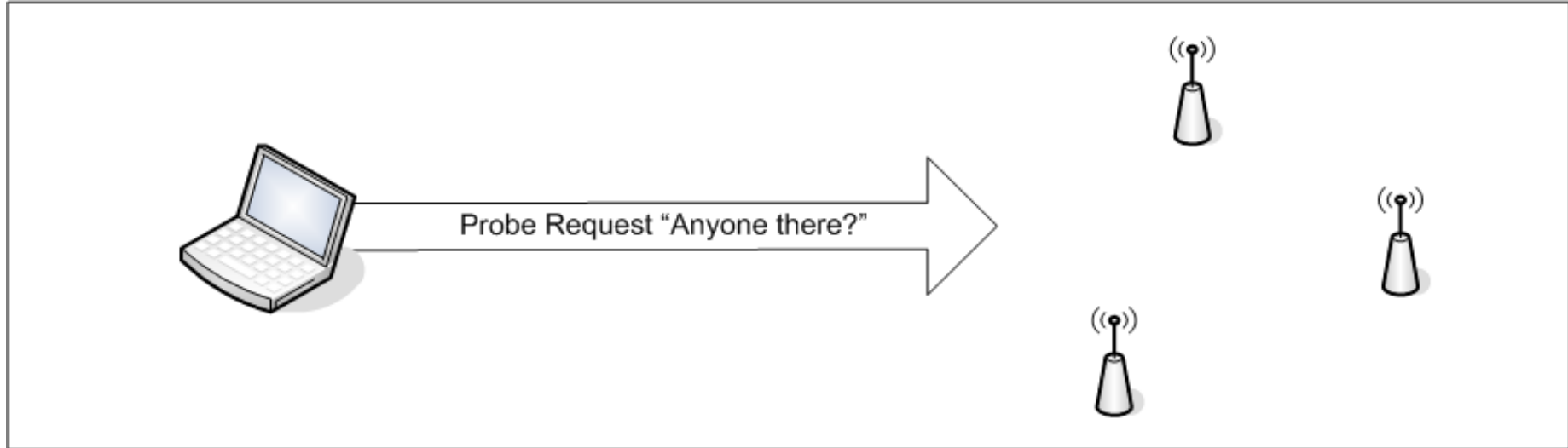
- Introduction to WZC Service
- Attacking wireless clients
 - Demos of tools and attacks
- Defending wireless clients
- Conclusion
- Questions/Open Discussion



- Windows Zero Configuration Service: A service used to make sure the NIC gets the “right” SSID, authentication mode, encryption keys and encryption mode
 - Does not select the AP
 - Does not take into account signal strength
- Alternate name: Windows XP Wireless Auto Configuration (WZCSVC)
- Different from third party configuration utilities shipped with some cards

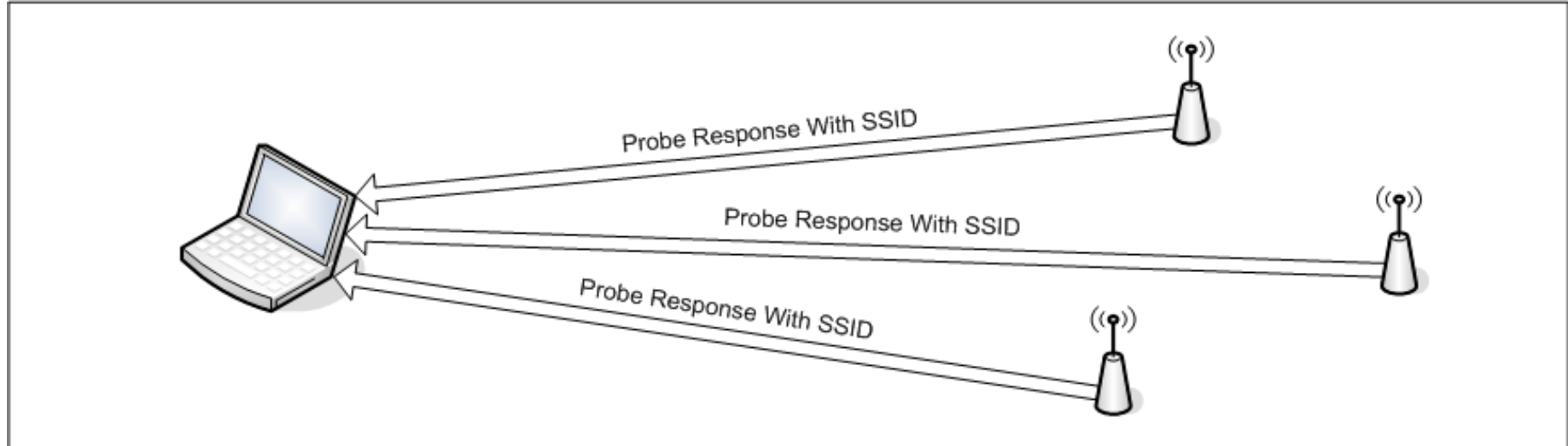
WZC Process: Step 1

- Client sends a broadcast Probe Request on each channel and creates a list of available networks



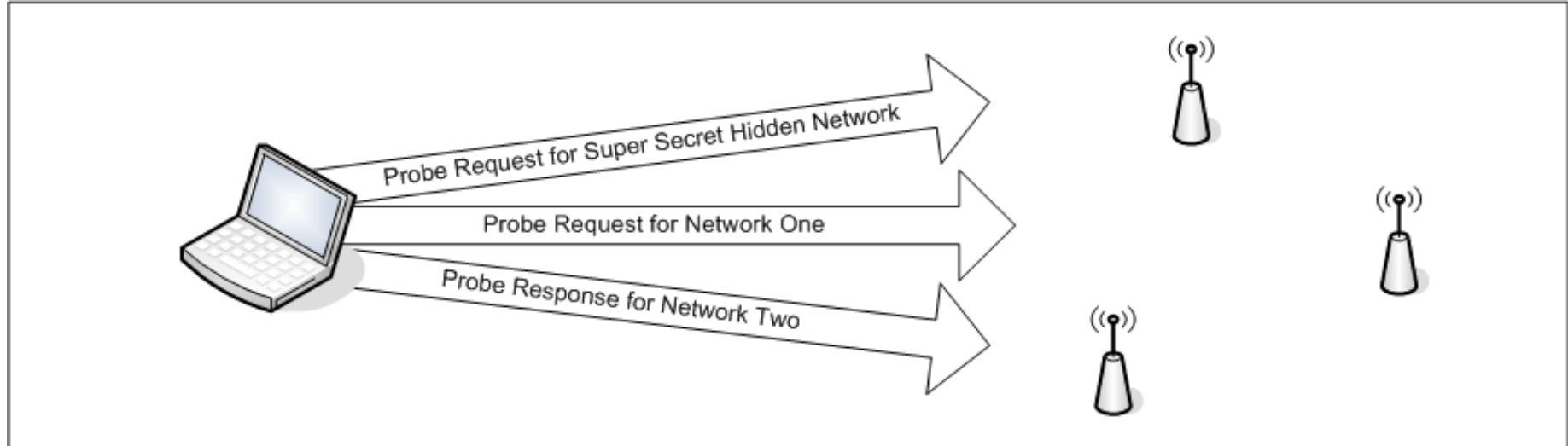
WZC Process: Step 2

- Access points within range respond with Probe Response packets
- If Probe Responses are received from networks on the Preferred Network List (PNL) the client connects to them in PNL order



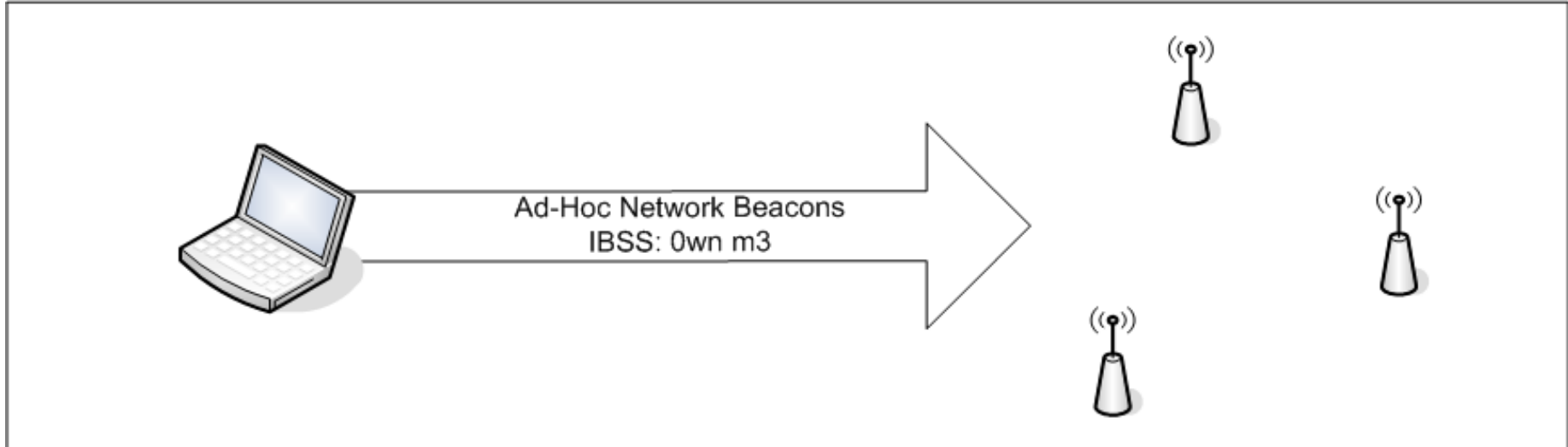
WZC Process: Step 3

- If no available networks on the PNL respond, specific Probe Requests are sent for each preferred network in case they are “hidden”



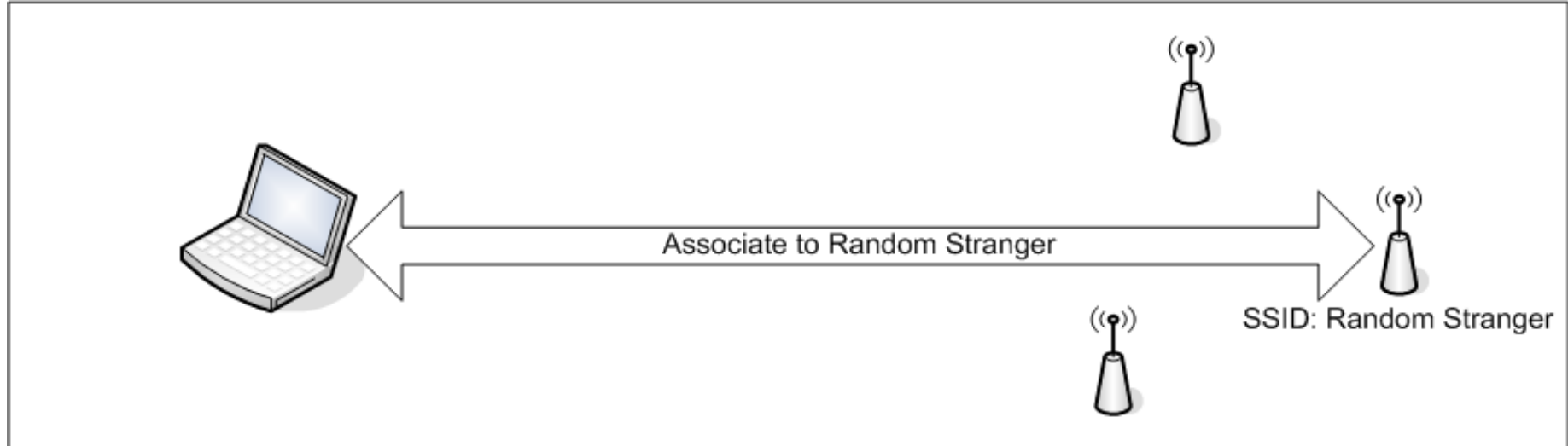
WZC Process: Step 4

- If client is not associated and there is an ad-hoc network on the PNL
 - Establishes the ad-hoc network
 - Becomes the first node
 - Begins sending beacon packets
- Self-assigns an IP address in the Windows Automatic Private Address range of 192.168.0.0/16



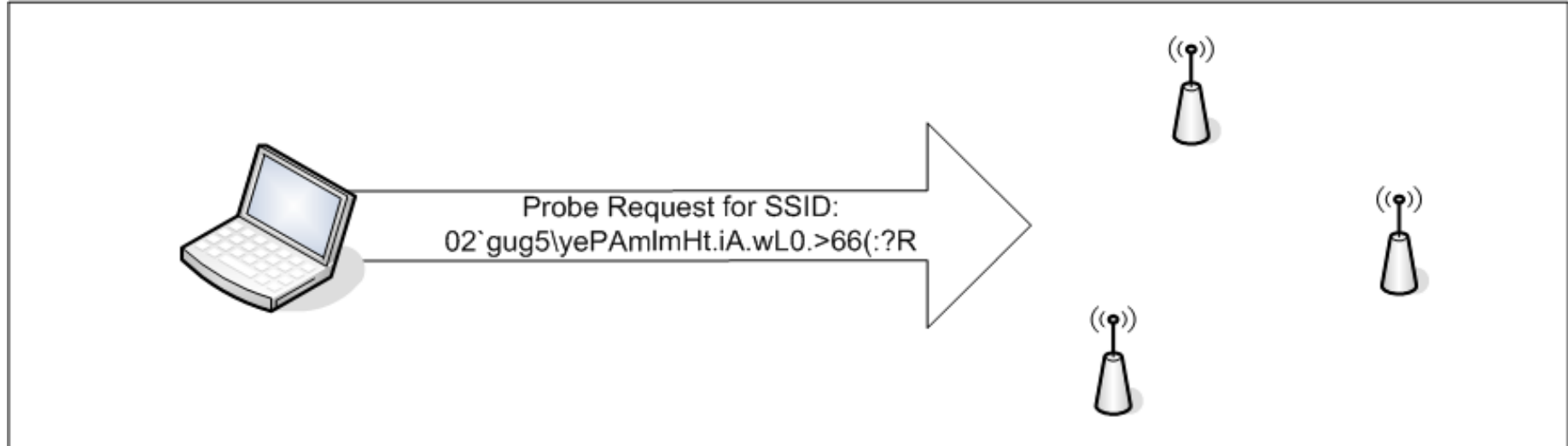
WZC Process: Step 5

- If “Automatically connect to a non-preferred networks” is enabled (disabled by default) it connects to any network in the order in which they are detected



WZC Process: Step 6

- If not in ad-hoc mode or associated to a network, Windows sets the NIC to Infrastructure mode and assigns a random 32 character SSID



WZC Process: Step 7

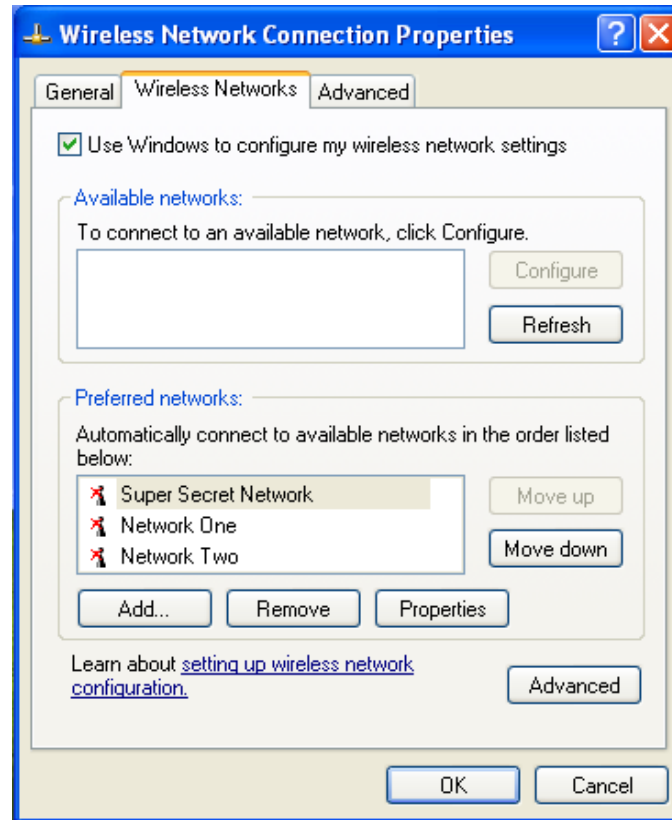
- WZC sleeps for 60 seconds
- Algorithm restarts





- SSID is sent to the NIC
- NIC decides which AP with select SSID to connect to
- Algorithm used to pick the AP is dependant on drivers and firmware
 - Usually determined by signal strength, speed and stability

WZC - Example



WZC - Example



Source	Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Protocol	Summary
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	78%	2.0	46	802.11 Probe Req	FC=.....,SN= 8,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	81%	2.0	46	802.11 Probe Req	FC=.....,SN= 9,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	70%	2.0	46	802.11 Probe Req	FC=.....,SN= 11,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	81%	2.0	46	802.11 Probe Req	FC=.....,SN= 27,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	77%	2.0	73	802.11 Probe Req	FC=.....,SN= 32,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	84%	2.0	73	802.11 Probe Req	FC=.....,SN= 33,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	80%	2.0	57	802.11 Probe Req	FC=.....,SN= 52,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	82%	2.0	57	802.11 Probe Req	FC=.....,SN= 53,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	84%	2.0	57	802.11 Probe Req	FC=.....,SN= 73,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	80%	2.0	57	802.11 Probe Req	FC=.....,SN= 74,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	71%	2.0	78	802.11 Probe Req	FC=.....,SN= 95,FN= 0,SSID=1C340>#bZ)6<UrFLJUJJe69b2b.kP>
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	70%	2.0	73	802.11 Probe Req	FC=.....,SN= 101,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	60%	2.0	73	802.11 Probe Req	FC=.....,SN= 102,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	81%	2.0	57	802.11 Probe Req	FC=.....,SN= 119,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	81%	2.0	57	802.11 Probe Req	FC=.....,SN= 120,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	80%	2.0	57	802.11 Probe Req	FC=.....,SN= 137,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	82%	2.0	57	802.11 Probe Req	FC=.....,SN= 138,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	80%	2.0	78	802.11 Probe Req	FC=.....,SN= 155,FN= 0,SSID=VjC,S*4.kB& j!_l[N5F\p#dg7Pxeasel
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	84%	2.0	78	802.11 Probe Req	FC=.....,SN= 156,FN= 0,SSID=VjC,S*4.kB& j!_l[N5F\p#dg7Pxeasel
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	82%	2.0	73	802.11 Probe Req	FC=.....,SN= 162,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	84%	2.0	73	802.11 Probe Req	FC=.....,SN= 163,FN= 0,SSID=Super Secret Hidden Network
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	74%	2.0	57	802.11 Probe Req	FC=.....,SN= 180,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	80%	2.0	57	802.11 Probe Req	FC=.....,SN= 181,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	67%	2.0	57	802.11 Probe Req	FC=.....,SN= 201,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	78%	2.0	57	802.11 Probe Req	FC=.....,SN= 202,FN= 0,SSID=Network Two
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	67%	2.0	46	802.11 Probe Req	FC=.....,SN= 212,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	82%	2.0	46	802.11 Probe Req	FC=.....,SN= 213,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	74%	2.0	46	802.11 Probe Req	FC=.....,SN= 226,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	82%	2.0	46	802.11 Probe Req	FC=.....,SN= 227,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	85%	2.0	57	802.11 Probe Req	FC=.....,SN= 243,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	67%	2.0	46	802.11 Probe Req	FC=.....,SN= 254,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	77%	2.0	46	802.11 Probe Req	FC=.....,SN= 255,FN= 0
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	70%	2.0	57	802.11 Probe Req	FC=.....,SN= 262,FN= 0,SSID=Network One
00:13:46:94:EB:EB	Ethernet Broadcast	FF:FF:FF:FF:FF:FF	*	6	74%	2.0	57	802.11 Probe Req	FC=.....,SN= 263,FN= 0,SSID=Network One



ATTACKING WIRELESS CLIENTS



- Wireless is a broadcast medium
- Attackers can passively monitor unencrypted traffic to see:
 - Username and passwords
 - Web traffic
 - Instant messages
 - Email
- Tools:
 - Wireshark
 - Dsniff
 - Driftnet



- System automatically creates an ad-hoc network if one is in the PNL and other networks in the PNL are not present
 - Self assigns an IP address in the Windows Automatic Private Address range of 192.168.0.0/16
 - Starts broadcasting the IBSS in beacon packets
- If encryption is not enabled anyone in range can attach to this network
- Compromised systems can be use as stepping stones onto any wired networks attached to the system



- MITM: [man|monkey]-in-the-middle
- Attacker intercepts and relays the communications between two systems
- Allows an attacker to view and manipulate data
- During a MITM attack an attacker can:
 - Control and modify traffic sent to and from the client
 - Break SSL connections to view the encrypted contents
 - Hi-jack sessions
 - Inject malicious content

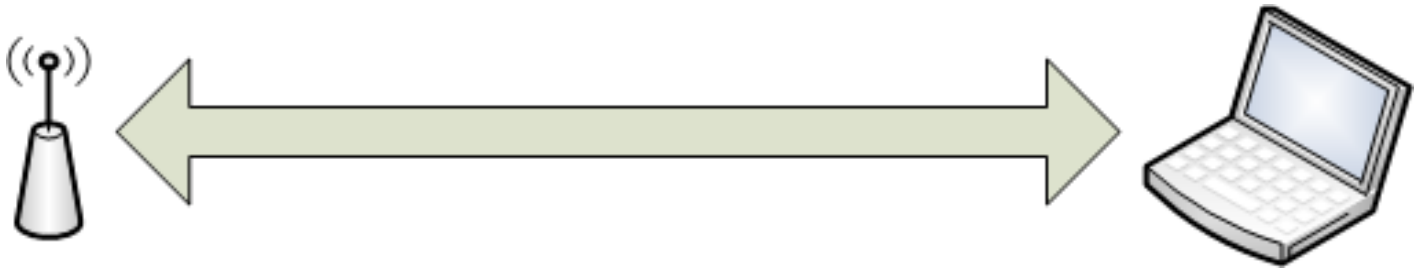
ARP Poisoning MITM



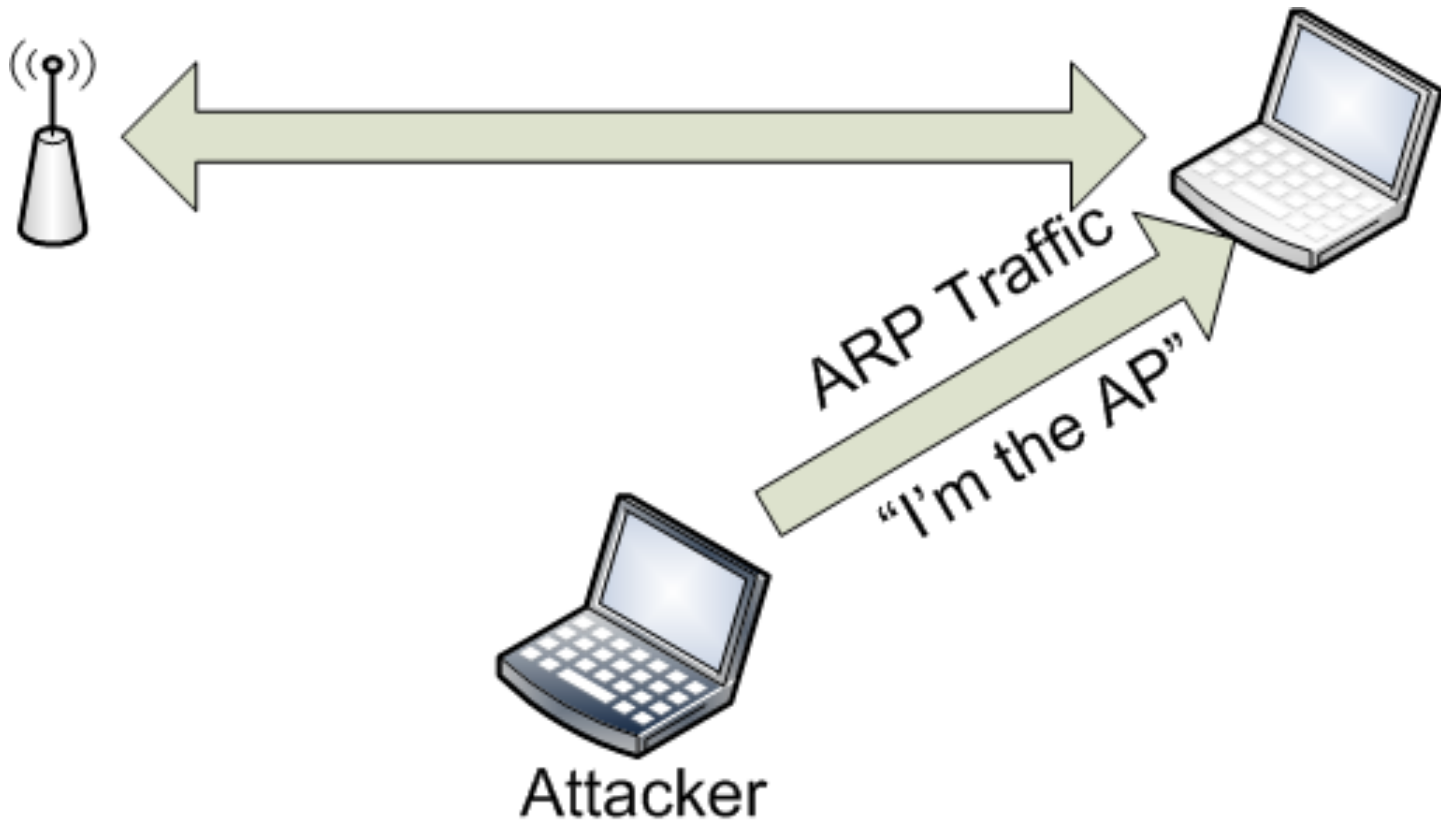
O-ISC '09
Ohio Information Security Conference

- Attacker sends fake ARP packets to trick a target system into thinking the attacker's system is the default gateway
- Once the attacker's system is the default gateway it can view and manipulate any traffic sent by the target
- Useful when the client is attached to a unencrypted network or an encrypted network the attacker has cracked
- Tools:
 - Cain
 - Ettercap

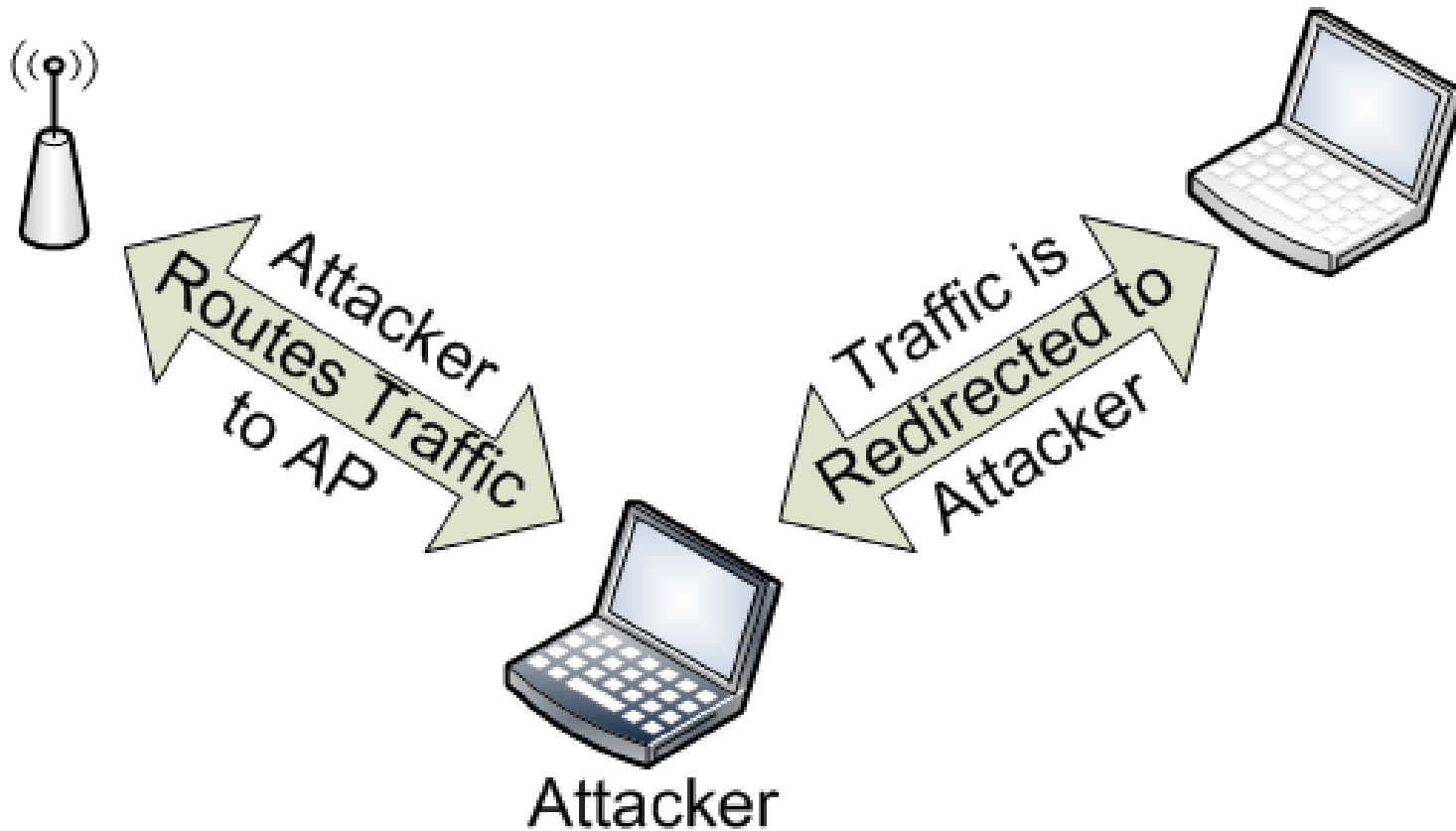
MITM Example



ARP Poison



MITM Complete





- Useful when the target has wireless enabled but is not associated to an AP or if the target is attached to an encrypted network
- Create a fake AP with a common SSID or create an AP that will reply to any SSID probe
 - If the client is looking for SSID “default” the AP will appear to have an SSID of “default” to that client
 - Simplifies the random SSID attack
 - Any un-encrypted network in the PNL will connect to the AP
- Tools:
 - Karma
 - Jasage – Karma for embedded devices
 - Airbase-ng



KARMA DEMO





- Collection of tools designed to launch client-side attacks against wireless users
- Commonly used to exploit vulnerabilities in Internet Explorer
- Performed by combining the following tools:
 - Karma or Airbase-ng
 - DHCP server
 - Metasploit



DEMO





- Session hijacking
 - The Middler
 - Hampster
 - WifiZoo

- Attacking wireless drivers
 - Metasploit
 - Scapy

- Attacking automatic update services
 - Evilgrade



DEFENDING WIRELESS CLIENTS





- Apply all patches quickly
- Run Anti-Virus software and keep definitions up to date
- Run a spyware protection package and update regularly
- Have users login with a non-administrative level account
- Encrypt sensitive data on the drive
- Disable filesharing
- Prevent network bridging



- User education
- Wireless Network Group Policy Settings
 - Disable Ad-hoc networks
 - Never “enable connect to non-preferred networks”
- Deploy a 802.11 aware personal firewall or security aware connection manager
- Only keep secure networks on the PNL



■ Teach users:

- To turn off wireless when not in use
- Not to form or connect to ad-hoc networks
- To remove networks from the PNL when the session is complete
- Use a VPN when accessing sensitive data
- If a VPN is not available
 - Use HTTPS when logging in or sending sensitive information
 - “Look for the lock”
 - Select a secure login connection
- Not to accept invalid certificates



- Configure wireless network settings
 - Global network settings
 - Preferred network list
 - 802.11X settings
- A computer Group Policy
- Available by default in Windows 2003 Domains
 - Can be added to Windows 2000 Domains
- Applies to Windows 2003, Windows XP SP1 and SP2
- Configure in the "Computer Configuration/Windows Settings/Security Settings/Wireless Network (IEEE 802.11) Policies" node in the Group Policy snap-in
- Policy not defined in default configuration

Wireless Group Policies

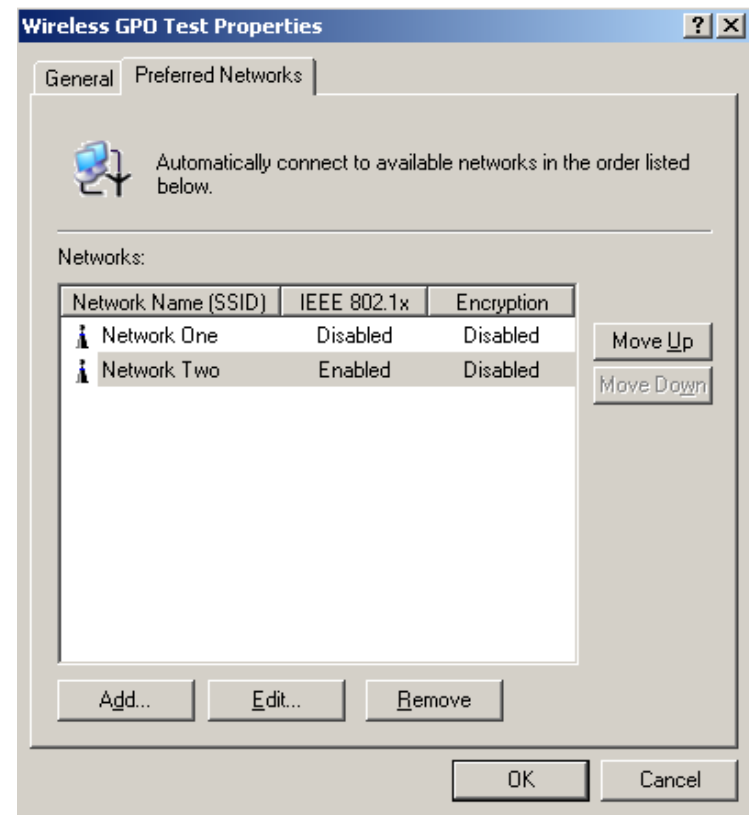


O-ISC '09
Ohio Information Security Conference

- “Network to access:” specifies the type of network a client is allowed to connect to
 - Set to “Access point (Infrastructure) networks only”
- Enable “Use Windows to configure wireless network settings for client” to have policies apply
- Do not enable “Automatically connect to non-preferred networks”
 - Enables automatic connections to wireless networks not defined in the preferred network list

A screenshot of the Windows Group Policy Object (GPO) configuration window titled "Wireless GPO Test Properties". The window has two tabs: "General" and "Preferred Networks", with "Preferred Networks" selected. The "Name" field contains "Wireless GPO Test". The "Description" field is empty. Below that, there is a "Check for policy changes every:" section with a text box containing "180" and the label "minutes". The "Networks to access:" dropdown menu is set to "Access point (infrastructure) networks only" and is circled in red. Below this, there are two checkboxes: "Use Windows to configure wireless network settings for clients" (checked) and "Automatically connect to non-preferred networks" (unchecked), both of which are also circled in red. At the bottom right, there are "OK" and "Cancel" buttons.

- Adds networks to the Preferred Network List
- When a network is added, authentication, encryption and 802.11x values can be defined





- GPO takes precedence over user-defined settings
 - Exception: Preferred Network List
 - Merges with client's list
 - Networks added through policy are at the top of the list
 - Client can add additional networks
 - Client cannot remove preferred networks added through policy
- If multiple policies are present, settings are not merged
- The policy closest to the computer within the domain structure is applied



- If possible, select a personal firewall with integrated connection manager
- If not, enable a separate firewall and connection manager
 - Test for interoperability
- Features to look for:
 - Prevents ad-hoc network
 - Limits what SSIDs a user can connect to
 - Only allows connections to authorized SSIDs of encrypted networks
 - Disables wireless network card when on a wired network
 - Prevents network bridging
 - Only allows “secure” networks in the Preferred Network List
 - Ability to block client-to-client connections
 - Only allows traffic to and from the AP
 - Ability to block inbound and outbound traffic
 - Easy central management
- Example:
 - * Example does not imply endorsement
 - Personal or Enterprise versions of “AirDefense”
 - ZoneAlarm’s Wireless PC Protection



- Startup script to turn off wireless
- Script to remove insecure networks from the PNL on shutdown or startup
- Script to remove all networks from the PNL so only GPO networks are listed
- Insert a long SSID into the PNL and monitor for an AP with this SSID
- Working on getting example scripts available to the public



- A variety attacks are possible against wireless clients
- Attacks can result in sensitive information being disclosed
- User education and technical controls can help to mitigate these risks
- Group Policies and custom scripts can be used to manage wireless settings



QUESTIONS?

More Information:

www.SecureState.com

www.matthewneely.com

mneely@securestate.com





- What are you doing to protect your mobile users?
- Has anyone experienced these attacks in the wild?
- What is the largest challenge you see with a mobile workforce?