

Multipot: A More Potent Variant of Evil Twin

K. N. Gopinath

Senior Wireless Security Researcher and
Senior Engineering Manager

AirTight Networks

<http://www.airtightnetworks.net>

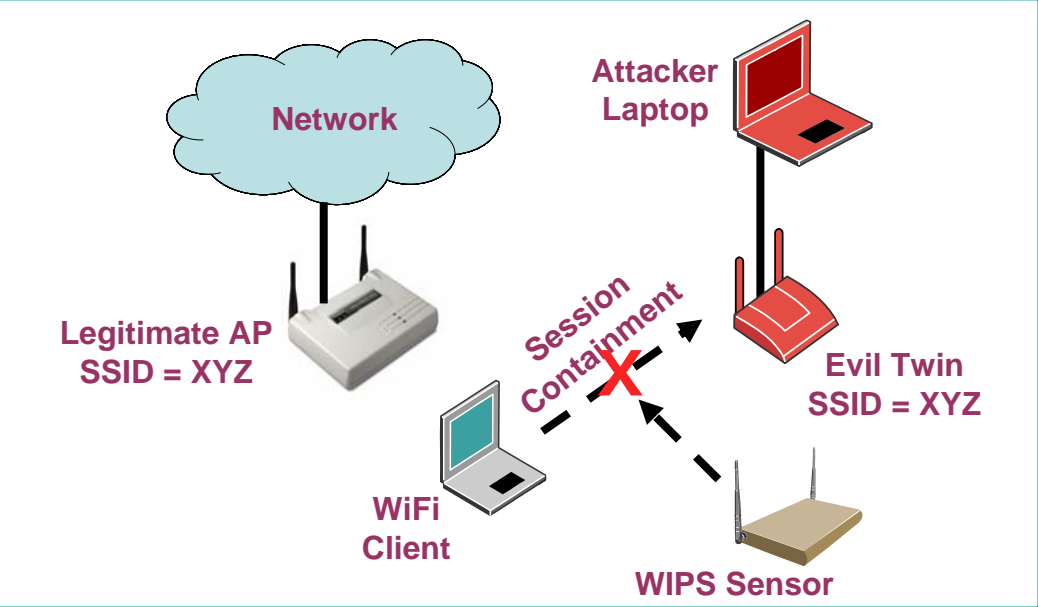
Email: gopinath.kn@airtightnetworks.net

What is this presentation about?

It is about discovery of a more potent variant of Evil Twin.
We call it 'Multipot'.

- Evil Twin recapitulation
- Fundamentals of Multipot
- Technical details about Multipot threat
 - ◆ Why traditional defenses against Evil Twin threat are ineffective against Multipot.
- Threat scenarios that arise due to Multipot
- A demonstration of Multipot threat

Evil Twin - Recap



- ◆ Attacker sets up AP with a spoofed SSID
- ◆ Client lured into connecting to attacker's AP
- ◆ Attacker becomes man-in-the-middle
- ◆ Threat is rampant in hotspots, also present in homes and campuses

Established Attack Tools: KARMA, delegated, hotspotter, Monkey Jack and more...

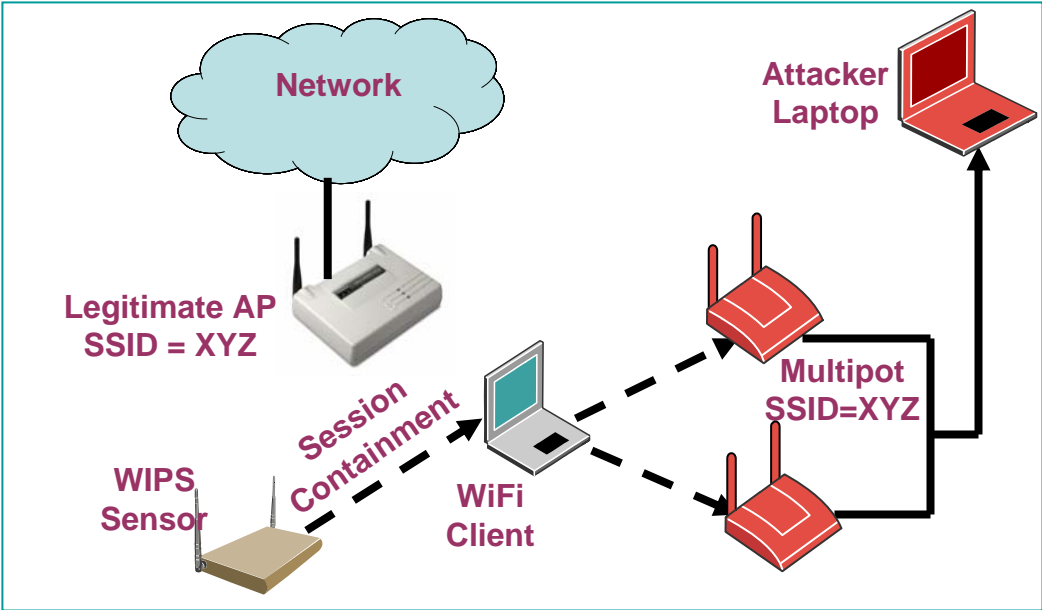
Known Countermeasures

- Level 1 Defense: Don't let client to be lured
 - E.g., watchful user, layer 2 mutual authentication, pre-programmed list of legitimate AP MACs etc.
- Level 2 Defense
 - Use Wireless Intrusion Prevention System (WIPS) to contain wireless session to Evil Twin.
 - Session containment via spoofed death from sensor is prevalent

Not foolproof and not always practical

MultiPot

Multiple APs Acting as Evil Twin



- ◆ Multiple APs with identical SSID feeding data into common endpoint
- ◆ If traditional WIPS session containment is used on one AP, client "hops" to another AP in the Multipot and continues its communication

MultiPot can be combined with: KARMA, delegated, hotspotter, Monkey Jack and more...

Known Countermeasures

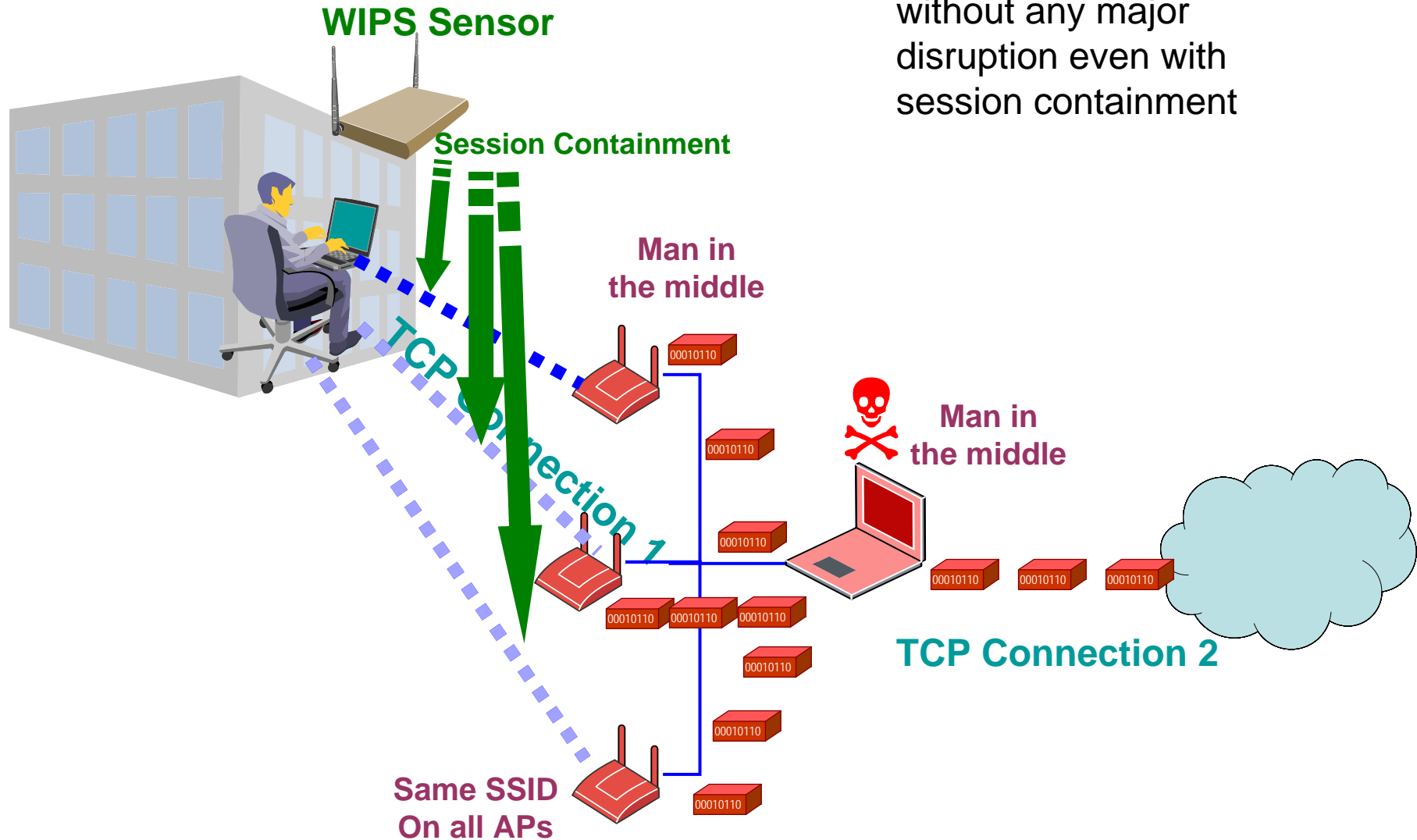
- Level 1 Defense: Don't let client to be lured
 - E.g., watchful user, layer 2 mutual authentication, pre-programmed list of legitimate AP MACs etc.

- Level 2 Defense
 - Use Wireless Intrusion Prevention System (WIPS) to break wireless connection to Evil Twin.

Not foolproof and not always practical

Death based session containment becomes ineffective

Multipot Threat in Action!



Multipot:

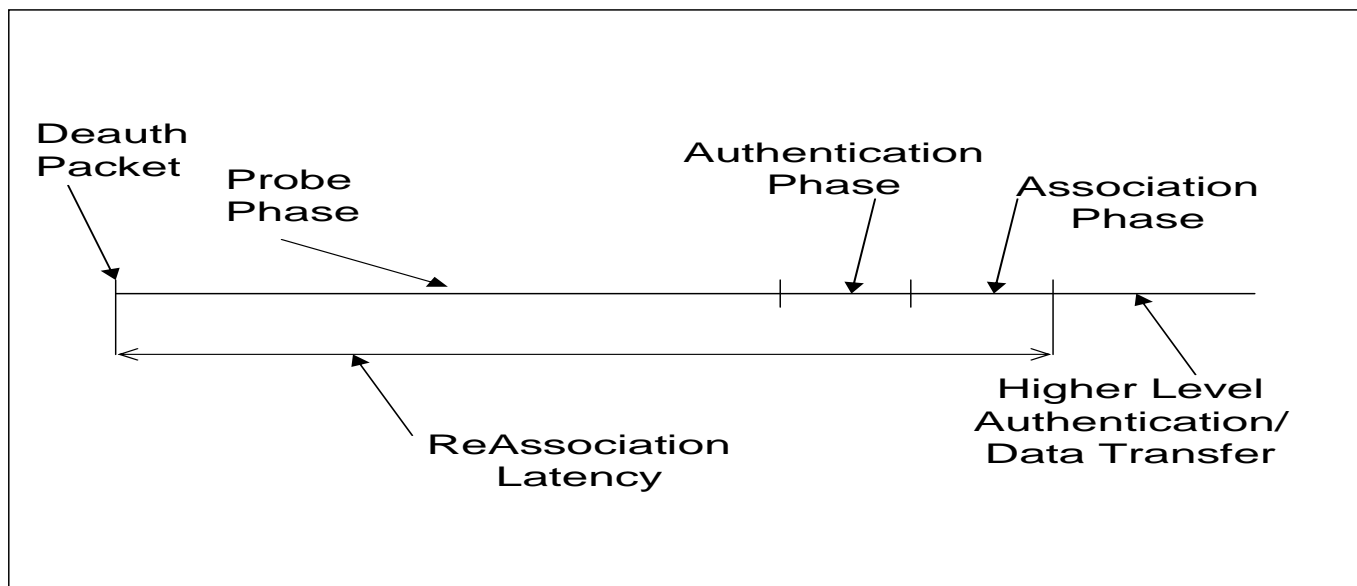
Client communicates without any major disruption even with session containment

Multipot Threat Analysis: Sensor Behavior

- ◆ WIPS sensor detects and deauths client's connection to any AP after finite delay
 - Sensor needs to operate on several 802.11 channels to detect unauthorized communication
 - ◆ 802.11 G consists of 14 channels in 2.4 GHz band
 - ◆ 802.11 A consists of about 25 channels in 5.0 GHz band
 - ◆ Sensors may also need to scan proprietary modes such as Atheros Turbo
 - Today's sensors built using commodity hardware cannot receive or transmit on all channels simultaneously
 - ◆ Sensor needs to dwell on each channel for a certain time (e.g., 100 ms) in a certain order (e.g., round robin)
 - ◆ Hence, channel scanning and processing delay in a WIPS sensor is unavoidable
- ◆ Our observation indicates that channel scanning delay can be typically around a second, even up to 10 seconds in some systems

Multipot Threat Analysis: Client Behavior

- 802.11 client reconnection 101
 - After receiving a 802.11 deauthentication packet
 - An 802.11 client performs a 802.11 MAC connection handshake with an AP
 - Handshake involves probe, authentication and association phases

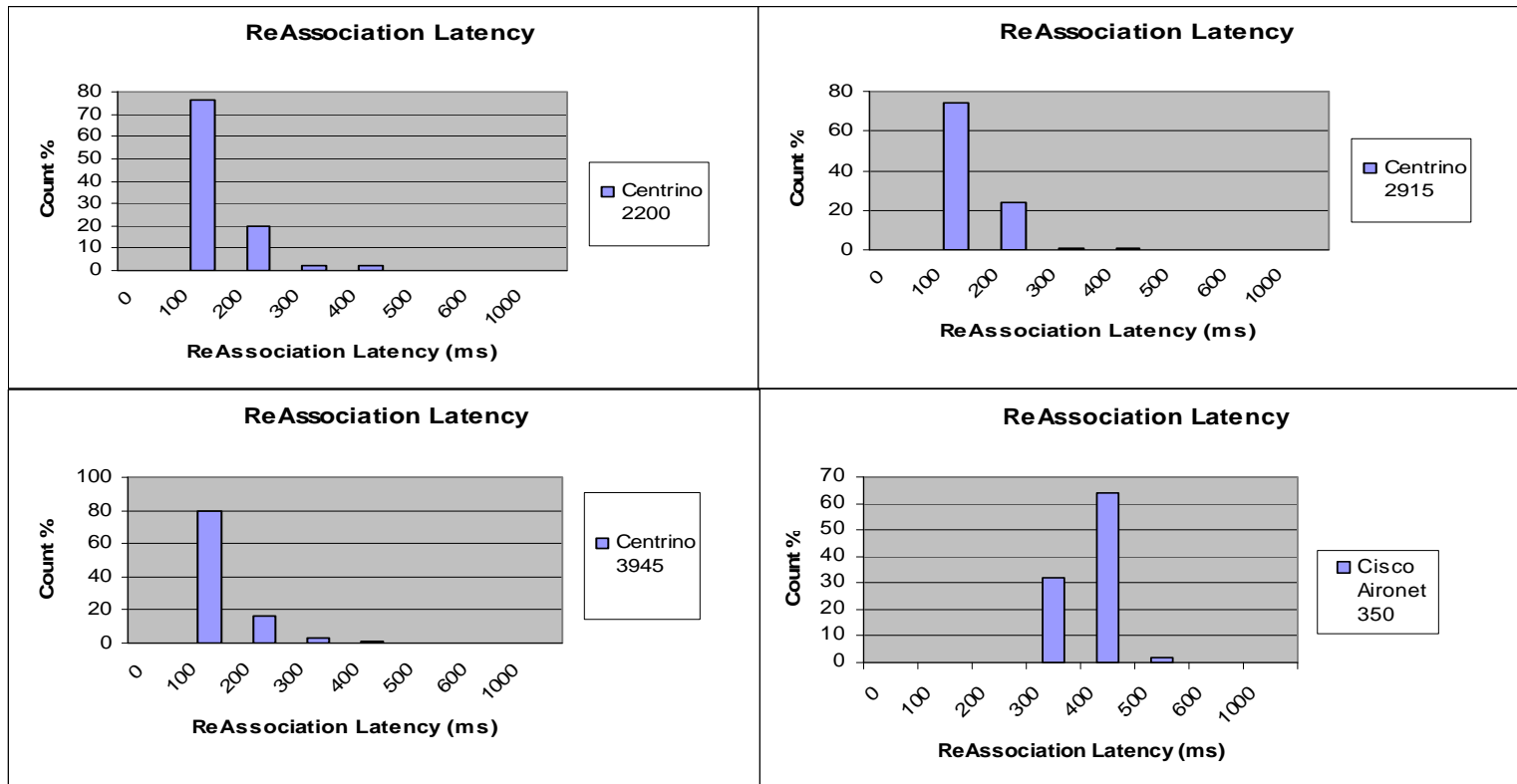


- MAC connection handshake scheme is not specified in 802.11 standard
 - Vendors implement different heuristics
 - Some vendors use aggressive reconnection scheme

Multipot Threat Analysis: Client Behavior (Contd.)

◆ ReAssociation latency measurements

- 3 popular models of Centrino & Cisco 350 used as clients
- AP used: Dlink DWL-G730AP
- Raw packet death injection and simple scripts for timing analysis



◆ Centrino & Cisco 350 reassociate to an AP aggressively

- We have frequently observed Centrinos reassociate in 30 ms!
- Optimizations such as periodic scanning, scanning selected channels seem to be implemented

Multipot Threat Analysis - Summary

- ◆ WIPS sensor detects and deauths client's connection to any AP after finite delay (order of **seconds**)
- ◆ Clients such as Centrino and Cisco Aironet 350 cards swiftly connect to new APs after being disconnected (order of **milliseconds**)
- ◆ WIPS sensor gets trapped into a cat and mouse game due to the above inherent time disparities involved
- ◆ Client's wireless application does not see disruption while sensor loses the cat and mouse game

Multipot

Prevalent Countermeasure Analysis

- ◆ As noted earlier
 - deauth based session containment is NOT effective for Multipots due to association hopping
 - Client side software is NOT enough
- ◆ Wire-side prevention (e.g., switch port disabling) will NOT work for Multipots
 - Multipots may not have a controllable switch port associated with them as we talking of clients connecting to external APs (and NOT rogue APs connected to a wired network)

Multipot

Prevalent Countermeasure Analysis (Contd.)

- ◆ Starting session containment concurrently (e.g., round robin) on all APs in a Multipot will NOT be sufficient
 - Reliable containment requires deauth packets to be sent at a certain frequency
 - A sensor cannot send packets with required frequency on multiple (typically more than 2) channels
- ◆ Using N Sensors for session containment will NOT work
 - Not scaleable
 - An attacker can use $N+1$ APs
 - ◆ It is relatively easier for an attacker to set up a Multipot with $N+1$ APs
 - ◆ Setting up of a Multipot with many APs is possible (e.g., using Virtual APs, soft APs)

Additional Technical Details

Multipot Packet Trace for Ping Traffic

No. -	Time	Source	Destination	Protocol	Info
3431	33.171937	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3461	33.415792	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3463	33.416636	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3477	33.655878	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3479	33.656739	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3638	35.295100	192.168.5.10	192.168.5.1	ICMP	Echo (ping) request
3640	35.296563	192.168.5.1	192.168.5.10	ICMP	Echo (ping) reply
3682	35.886947	192.168.5.1	192.168.5.10	ICMP	Echo (ping) request
3683	35.887274	192.168.5.10	192.168.5.1	ICMP	Echo (ping) request
3688	35.893157	192.168.5.1	192.168.5.10	ICMP	Echo (ping) reply
3742	36.771596	192.168.5.1	192.168.5.10	ICMP	Echo (ping) request
3752	36.872628	192.168.5.10	192.168.5.1	ICMP	Echo (ping) request
3754	36.874101	192.168.5.1	192.168.5.10	ICMP	Echo (ping) reply
3842	37.126799	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3844	37.127660	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3881	37.371027	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3883	37.371870	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3904	37.611019	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3906	37.611821	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
3921	37.851055	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication
3923	37.851896	AlphaNet_05:2f:ff	192.168.5.10	IEEE 8	Deauthentication
2026	28.001018	192.168.5.10	AlphaNet_05:2f:ff	IEEE 8	Deauthentication

File: Trace1.cap 2655 KB | P: 10717 D: 524 M: 0

Containment for AP on ch. 6 prompts the client to hop to another AP on ch. 11. Traffic flows on ch. 11 (not seen)

Containment for AP on ch. 11 prompts the client to return to AP on ch. 6. Traffic flows on ch. 6 (seen)

Containment for AP on ch. 6 prompts the client to hop to another AP on ch. 11 (not seen)

Additional Technical Details

Multipot Packet Trace for HTTP Traffic

No. -	Time	Source	Destination	Protocol	Info
21653	120.20403	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
21655	120.20500	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication
21664	120.22248	192.168.2.29	202.138.113.146	HTTP	GET /RealMedia/ads/adstream
21686	120.35991	202.138.113.146	192.168.2.29	HTTP	HTTP/1.1 200 OK (application,
21689	120.36217	202.138.113.146	192.168.2.29	HTTP	HTTP/1.1 200 OK (application,
21692	120.37180	202.138.113.146	192.168.2.29	HTTP	Continuation
21693	120.37280	202.138.113.146	192.168.2.29	HTTP	Continuation
21695	120.37408	202.138.113.146	192.168.2.29	HTTP	Continuation
21700	120.38574	202.138.113.146	192.168.2.29	HTTP	Continuation
21701	120.38613	202.138.113.146	192.168.2.29	HTTP	Continuation
21705	120.39157	202.138.113.146	192.168.2.29	HTTP	Continuation
21823	120.89452	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
21828	120.90053	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication
21830	120.90223	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
21833	120.90554	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication
21846	120.93255	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
21854	120.94464	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
21855	120.94544	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication
22697	125.06497	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
22698	125.06577	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication
22716	125.10764	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Deauthentication
22717	125.10806	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Deauthentication

File: Trace2.cap 6813 KB C:\P: 23454 D: 1413 M: 0

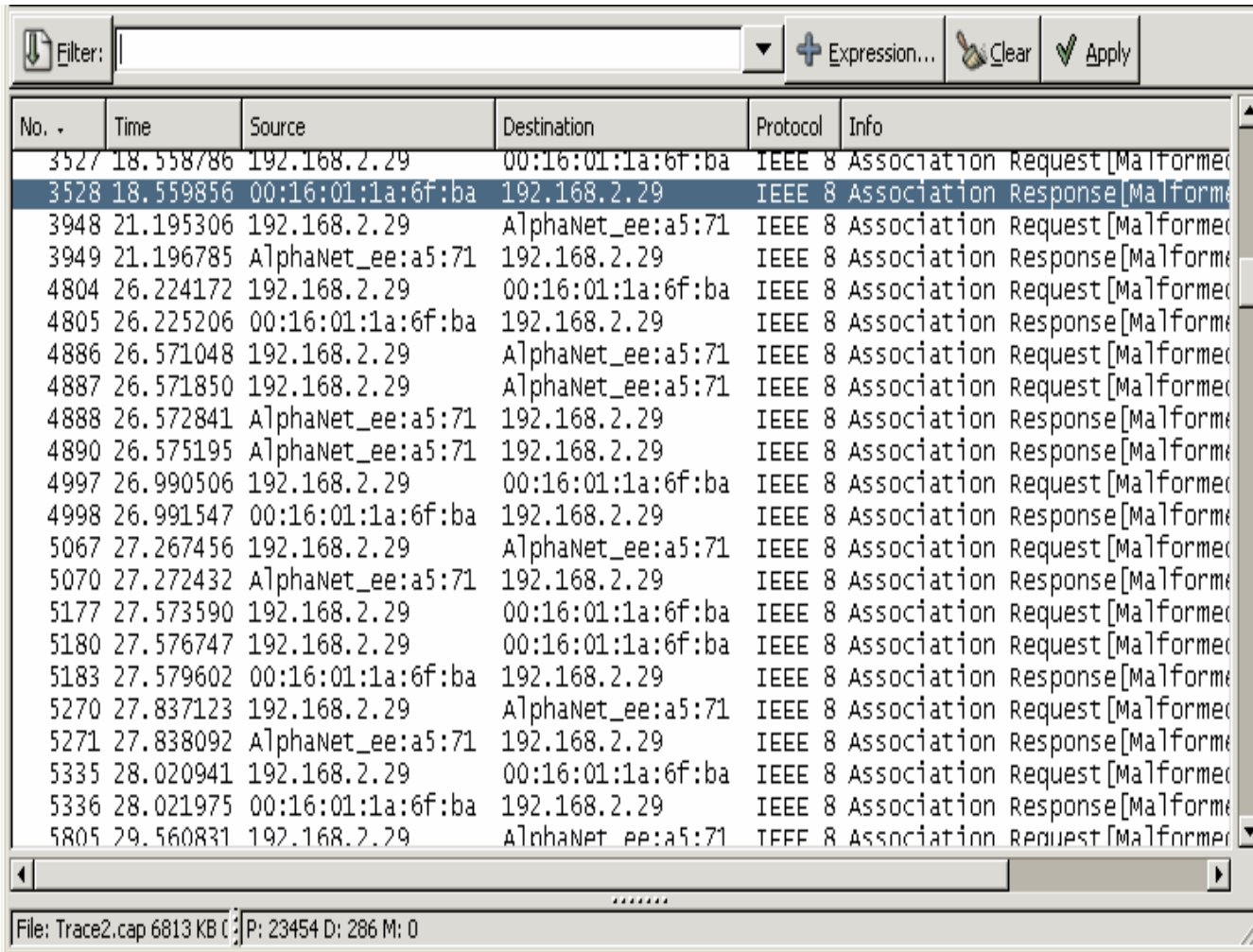
Containment for AP on ch. 6 prompts the client to hop to another AP on ch. 11. Traffic flows on ch. 11 (not seen)

Containment for AP on ch. 11 prompts the client to return to AP on ch. 6. Traffic flows on ch. 6 (seen)

Containment for AP on ch. 6 prompts the client to hop to another AP on ch. 11 (not seen)

Additional Technical Details

Multipot Packet Trace Showing Association Hopping



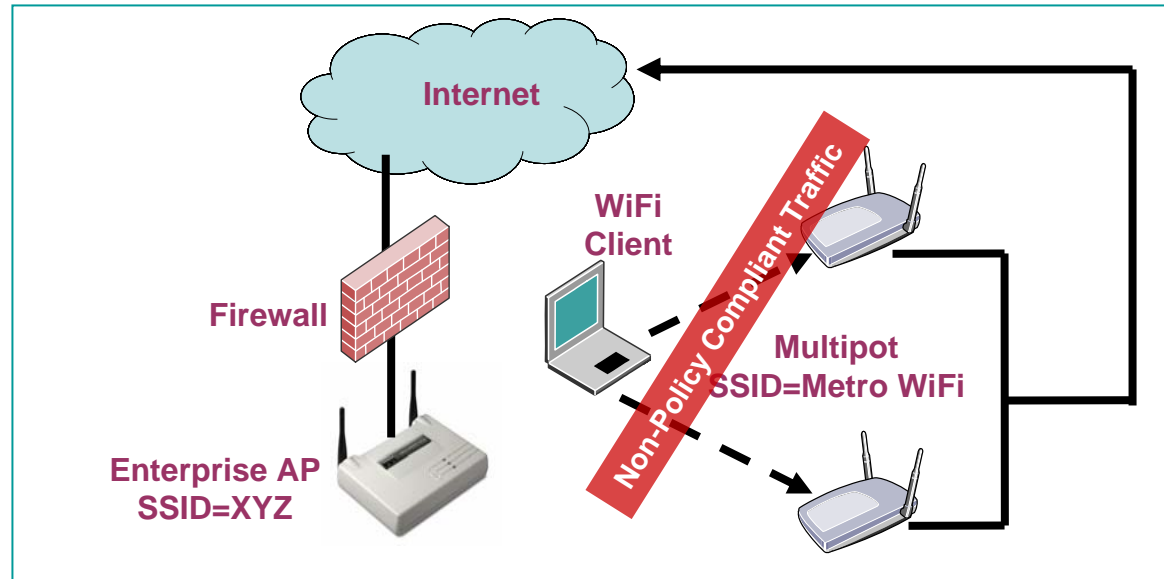
The image shows a Wireshark packet capture window with a filter set to empty. The packet list pane displays a series of IEEE 802.11 Association Request and Response packets. The packets alternate between the source IP 192.168.2.29 and the MAC address AlphaNet_ee:a5:71. The status for all packets is 'Malformed', likely due to the 'Association Hopping' mentioned in the title. The status bar at the bottom indicates the file is 'Trace2.cap' (6813 KB) and the packet size is 23454 bytes (286 M).

No. -	Time	Source	Destination	Protocol	Info
3527	18.558786	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
3528	18.559856	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Association Response [Malformed]
3948	21.195306	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]
3949	21.196785	AlphaNet_ee:a5:71	192.168.2.29	IEEE 8	Association Response [Malformed]
4804	26.224172	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
4805	26.225206	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Association Response [Malformed]
4886	26.571048	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]
4887	26.571850	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]
4888	26.572841	AlphaNet_ee:a5:71	192.168.2.29	IEEE 8	Association Response [Malformed]
4890	26.575195	AlphaNet_ee:a5:71	192.168.2.29	IEEE 8	Association Response [Malformed]
4997	26.990506	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
4998	26.991547	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Association Response [Malformed]
5067	27.267456	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]
5070	27.272432	AlphaNet_ee:a5:71	192.168.2.29	IEEE 8	Association Response [Malformed]
5177	27.573590	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
5180	27.576747	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
5183	27.579602	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Association Response [Malformed]
5270	27.837123	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]
5271	27.838092	AlphaNet_ee:a5:71	192.168.2.29	IEEE 8	Association Response [Malformed]
5335	28.020941	192.168.2.29	00:16:01:1a:6f:ba	IEEE 8	Association Request [Malformed]
5336	28.021975	00:16:01:1a:6f:ba	192.168.2.29	IEEE 8	Association Response [Malformed]
5805	29.560831	192.168.2.29	AlphaNet_ee:a5:71	IEEE 8	Association Request [Malformed]

File: Trace2.cap 6813 KB (P: 23454 D: 286 M: 0

Multipot Threat Scenarios

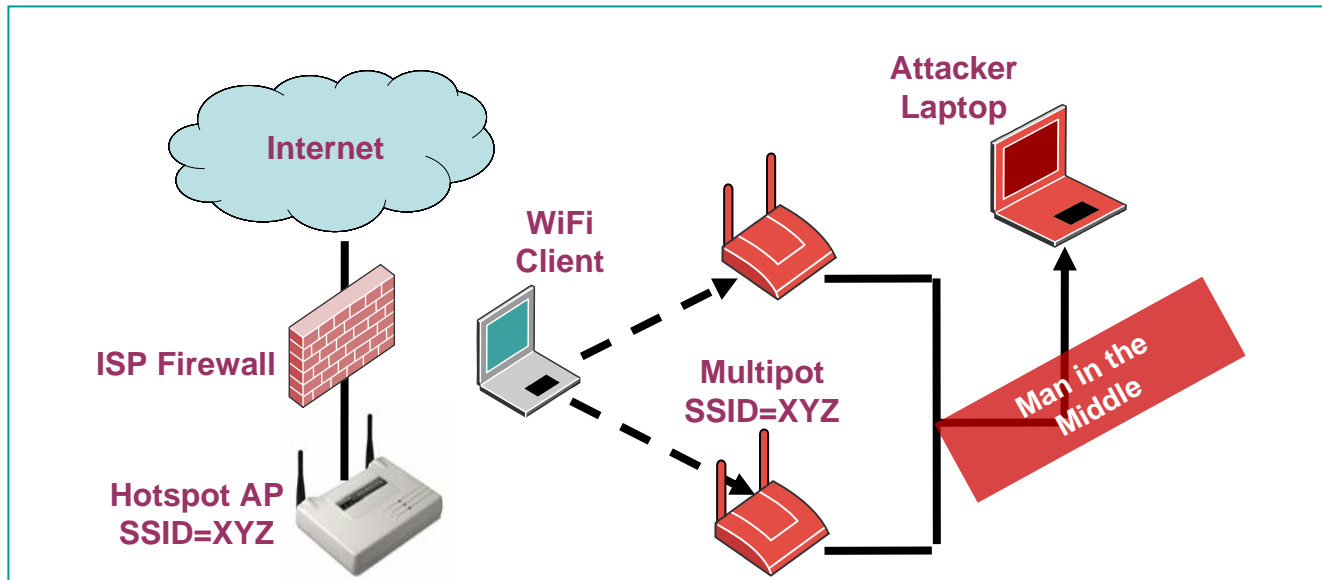
Scenario 1: Naturally Occurring Habitat



- ◆ Enterprise/Campus network scenario
 - Enterprises/campuses have policies against their clients connecting to public APs (e.g., Metro WiFi) or open neighbor APs
 - Multiple APs with identical SSIDs are naturally present in such scenarios creating a Multipot
 - Traditional WIPS session containment fails to stop non-policy compliant connections to such Multipots!

Multipot Threat Scenarios

Scenario 2: Handcrafted Variants



◆ Public Hotspot scenario

- Multipots can be handcrafted with malicious intentions
- Attacker can setup a Multipot to lure clients at public hotspots
- Once a client connection to Multipot is established, the attacker can perform various man-in-the-middle attacks using popular tools (KARMA, hotspotter etc.)
- Traditional WIPS countermeasure fails to defend against such attacker

Related Works of Other Researchers

Conjectures on Evading WIPS (Traditional Session Containment)

- ◆ In his May 2005 paper titled “Weaknesses in Wireless LAN Session Containment”, Joshua Wright concluded that:
 - “[S]ession containment can be a valuable mechanism to augment a secure wireless network deployment. The use of session containment does not come without risks however, including WLAN IDS fingerprinting and possible evasion.”
- ◆ No specific evasion scenario is mentioned
- ◆ In this presentation we presented a real life scenario which can be naturally occurring or deliberately deployed to evade traditional deauth based session containment.

Related Works of Other Researchers

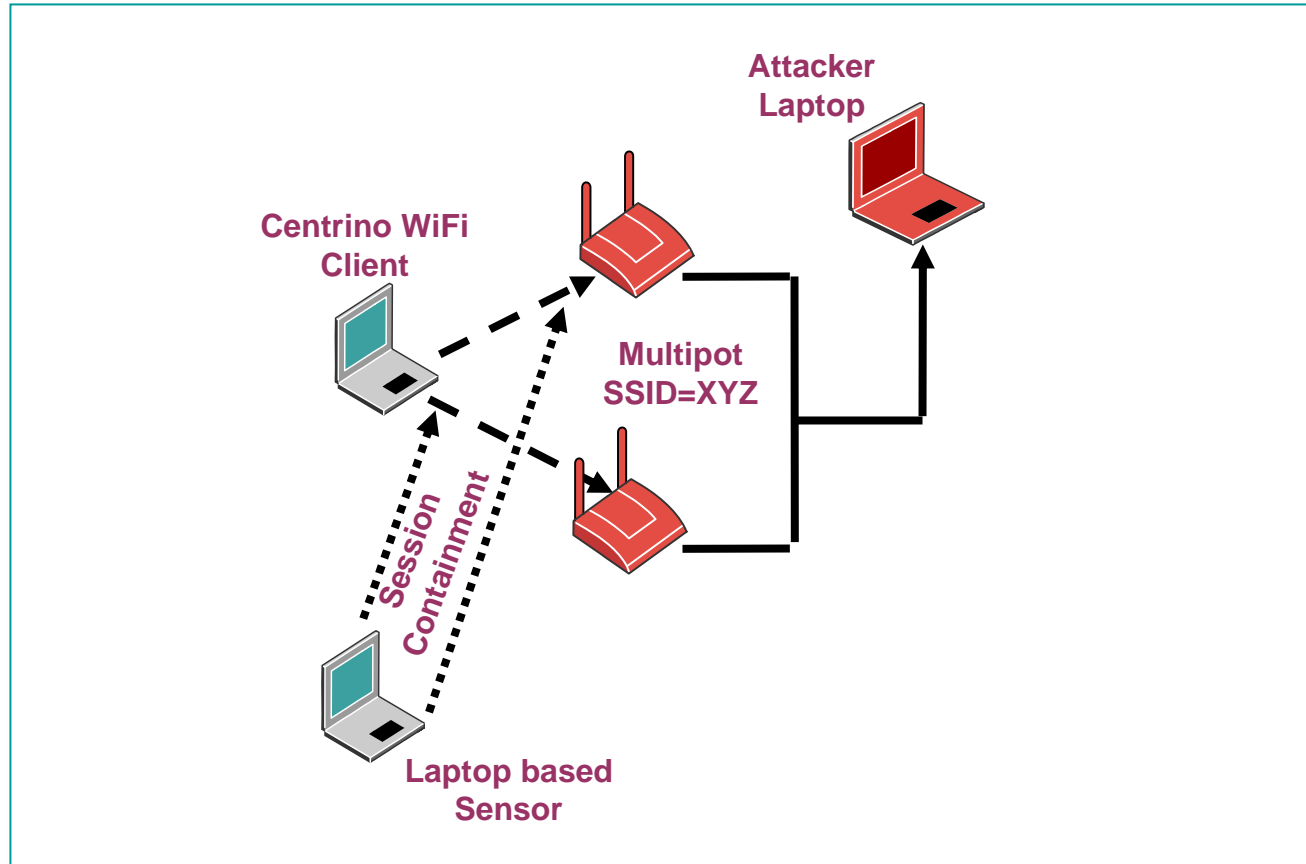
Recognition that Wireless Threats in the Future can be Evasive

- ◆ DARPA and Department of Homeland Security funded project MAP (Measure, Analyze and Protect), which is aimed at developing defenses against wireless based attacks
- ◆ One of the motivations for MAP is the fact that wireless attackers may use evasive techniques in the future to bypass WIPS defense

Demonstration

ACKNOWLEDGEMENTS: Sohail, Amit

Demo Setup Testbed



Demo Setup

What will be Seen?

- Centrino victim client swiftly hopping between APs in the Multipot in response to deauth session containment
- Ping progress well when both APs in the Multipot are on and sensor is chasing the wireless connection to deauth

ACKNOWLEDGEMENTS

AirTight Team

Hemant, Pravin (Presentation review)

Debu (Presentation graphics)

References

1. Joshua Wright, Weaknesses in Wireless LAN Session Containment, 5/19/2005,
http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf
2. Jon Cox, Researchers crafting intelligent scaleable WLAN defense, Networkworld, Dec 2006,
<http://www.networkworld.com/news/2006/120706-intelligent-scaleable-wlan-defense-darpa.html>
3. Christopher Null, Beware the "Evil Twin" Wi-Fi Hotspot,
<http://tech.yahoo.com/blogs/null/23163/beware-the-evil-twin-wi-fi-hotspot>
4. CNN, 'Evil twin' threat to Wi-Fi users,
<http://www.cnn.com/2005/TECH/internet/01/20/evil.twins/index.html>
5. KARMA, <http://www.theta44.org/karma/>
6. Delegated, <http://www.delegate.org/delegate/mitm/>
7. Airsnarf, <http://airsnarf.shmoo.com/>
8. Hotspotter, http://www.remote-exploit.org/codes_hotspotter.html
9. Monkey jack, <http://sourceforge.net/projects/airjack/>

Thank You

gopinath.kn@airtightnetworks.net