All You Wanted to Know About WiFi Rogue Access Points

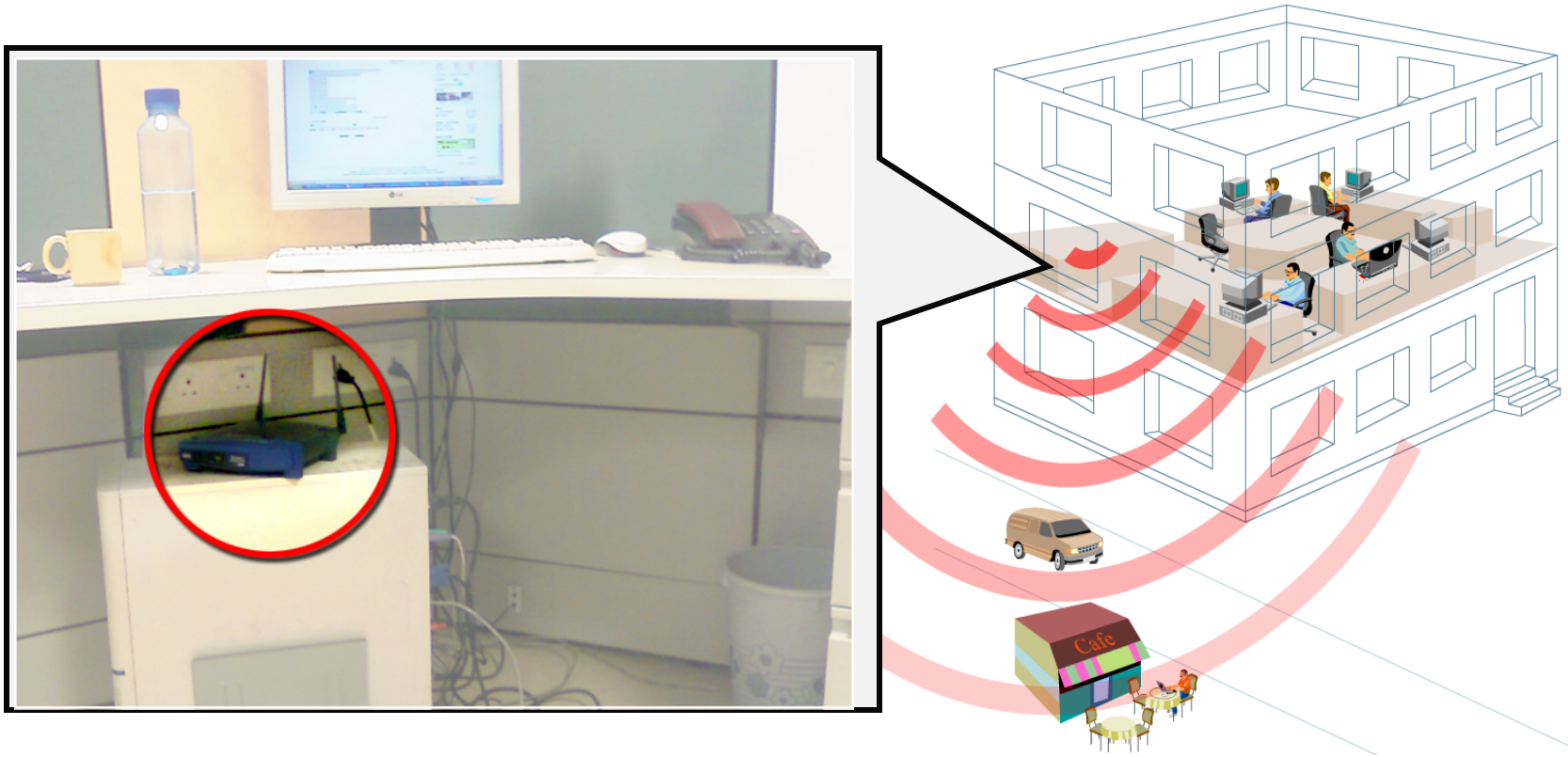
A quick reference to Rogue AP security threat, Rogue AP detection and mitigation

Gopinath K. N. Hemant Chaskar

AirTight Networks
www.AirTightNetworks.com

What is Rogue AP

- Unmanaged (unauthorized) AP attached to enterprise wired network



AirTight NETWORKS

How does Rogue AP pop up on enterprise network

- Malicious intent or simply unwitting, impatient employee
- Commoditization of WiFi APs raises the risk of someone putting up personal AP on the enterprise network

Wall Jack AP

Pocket AP

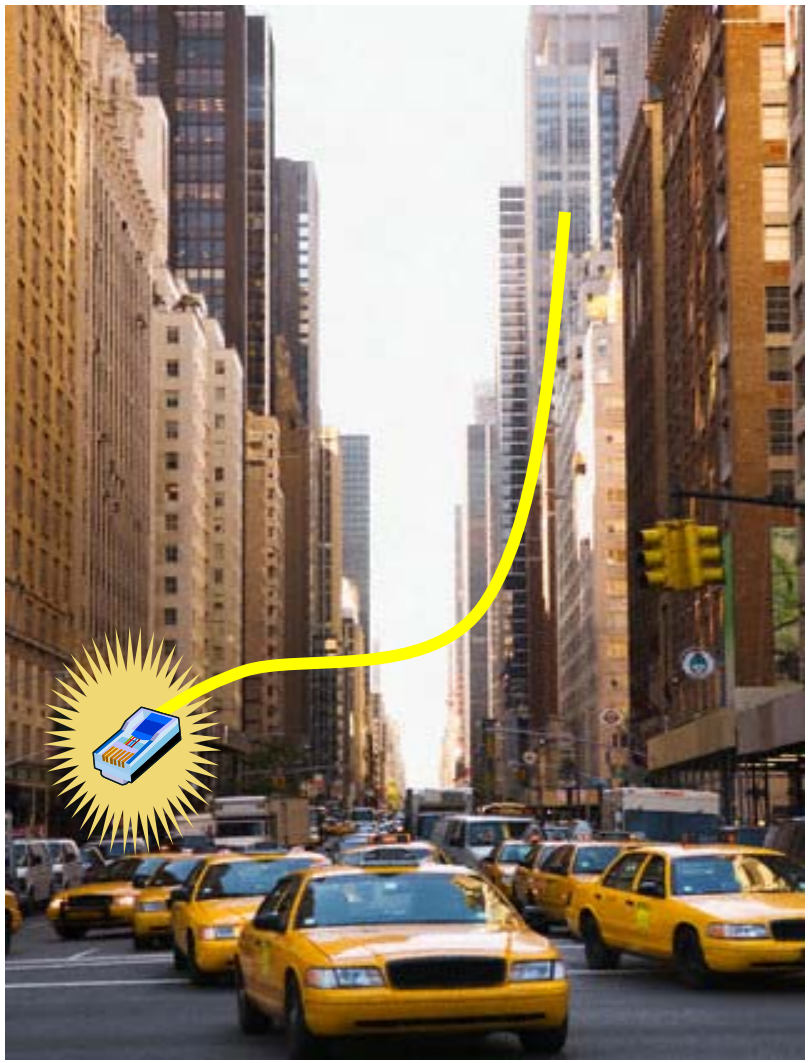
Wireless Router

PCMCIA and USB APs

- It has been estimated that almost 20% of corporations have Rogue APs in their networks at some time

AirTight® NETWORKS

Why is Rogue AP such a bad thing



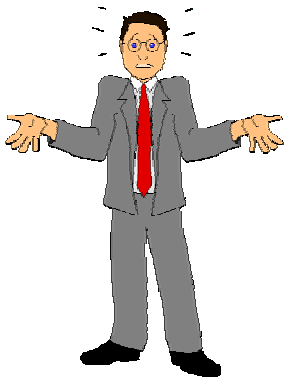
- Rogue AP on network = (logically) LAN jack of your network hanging out of the premises

- RF signal spillage of Rogue AP provides access to wired enterprise network from outside of the premises

AirTight NETWORKS

What are some specific attacks which can be launched through Rogue AP

- Attacks on wired network infrastructure
  - ARP poisoning, DHCP attacks, STP attacks, DoS attacks etc.
- Mapping the network for targeted attacks
- Scanning hosts on network for targeted attacks
- MIM (Man-In-Middle) and data sniffing on wired network
- See this blog article for details on attacks through Rogue AP http://blog.airtightnetworks.com/wifi-rogue-ap-5-ways-to-%e2%80%9cuse%e2%80%9d-it/

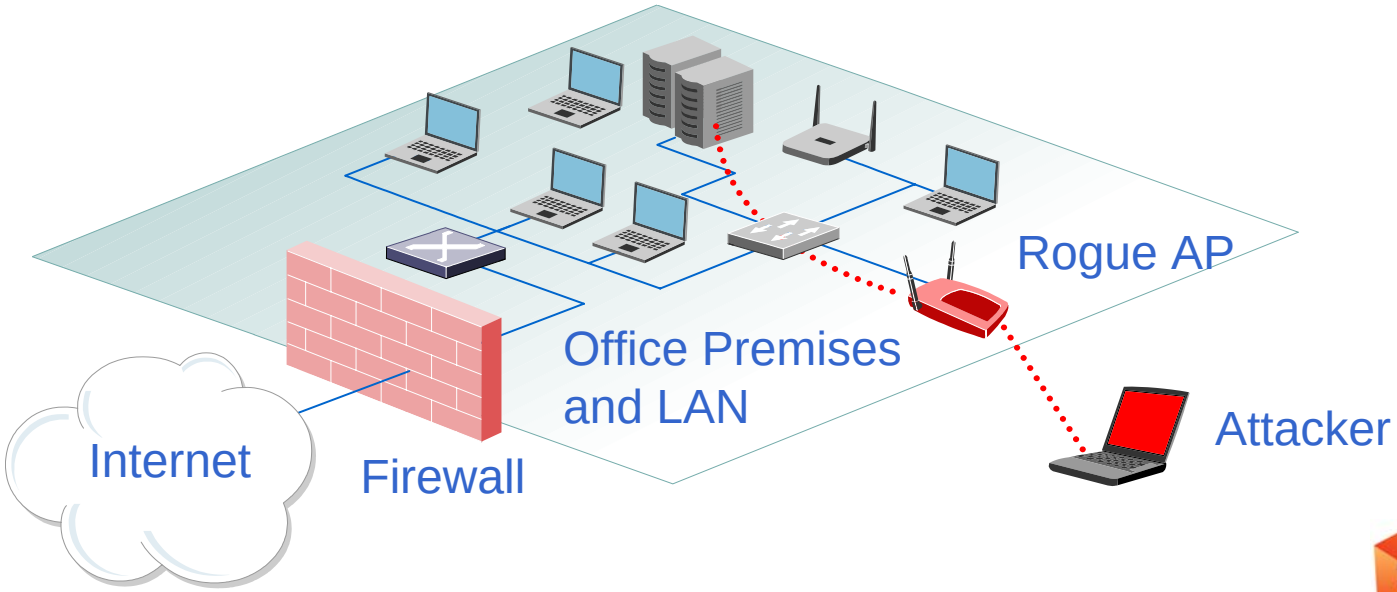


So, how can you protect enterprise network from Rogue APs?

AirTight NETWORKS

Can the firewall protect from Rogue AP

- No!
- Firewall works at traffic transfer point between LAN & Internet
- Firewall does not detect Rogue AP
- Firewall does not see traffic through Rogue AP



AirTight NETWORKS

Can WPA2 protect from Rogue APs

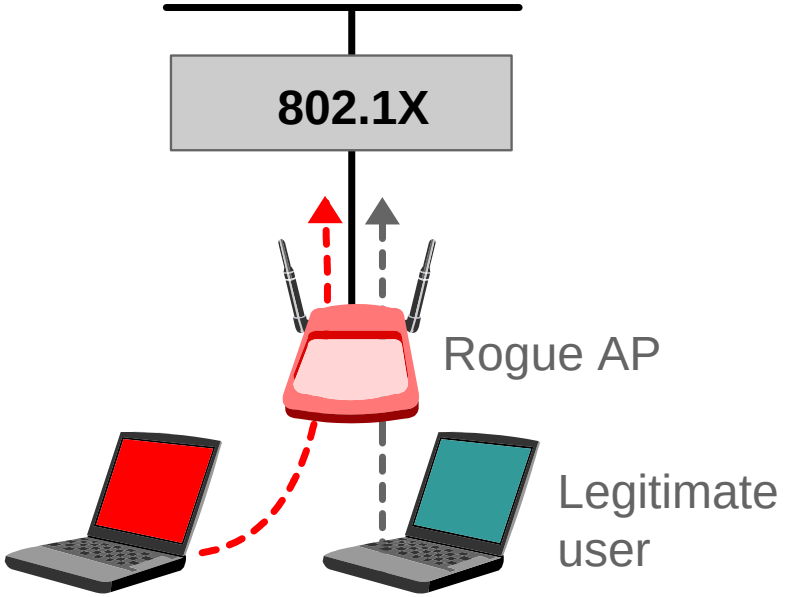
- No!
- You can enforce security controls such as WPA2 only on APs which you manage, i.e., your Authorized APs
- Rogue AP is not your managed AP
- In fact, most Rogue APs found in the field installed by naïve users either have
  - OPEN wireless link (out of box default) or
  - WEP wireless link (deterministically crackable)

AirTight® NETWORKS

Is 802.1X port control sufficient to protect from Rogue AP

- As a matter of fact, most networks do not have 802.1x port control today
- If even if 802.1x is deployed, it cannot protect from all Rogue AP configurations, some examples below:

Rogue APs over bridging laptops



MAC spoofer

AirTight NETWORKS

Can antivirus, wired IDS protect from Rogue AP

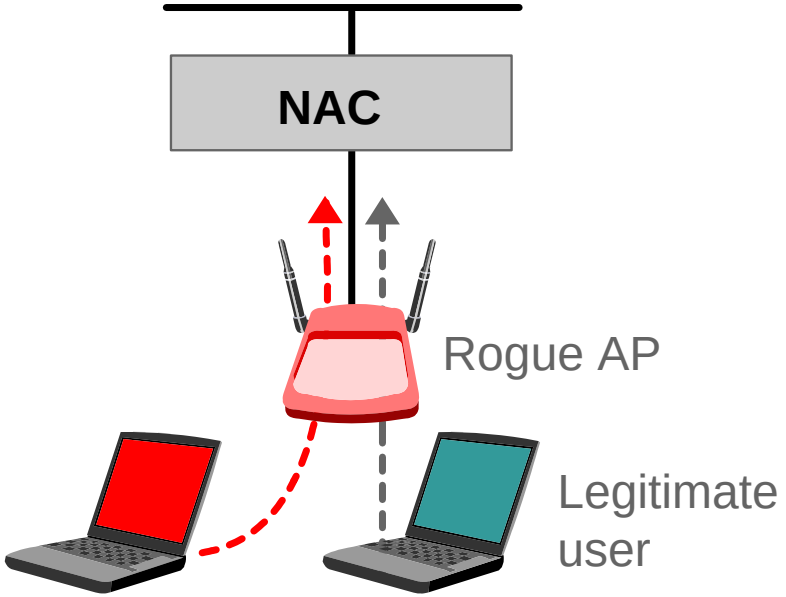
- No!
- Rogue AP threats operates at a layer below antivirus and wired IDS protection

AirTight NETWORKS

Is NAC sufficient to protect from Rogue AP

- As a matter of fact, most networks do not have NAC deployed today
- If even if NAC is deployed, it cannot protect from all Rogue AP configurations, some examples below:

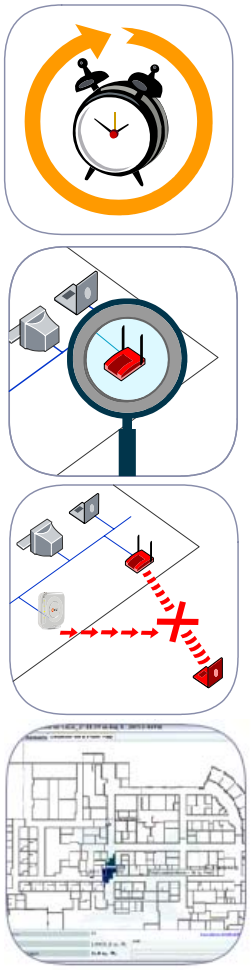
Rogue APs over bridging laptops



AirTight NETWORKS

So what protects network from Rogue APs

- Sensor based wireless intrusion prevention system (WIPS) which
  - Watches for Rogue APs 24x7
  - Performs wired/wireless correlation for AP network connectivity testing to detect Rogue AP
  - Provides for automatic blocking of Rogue AP
  - Locates Rogue AP for easy searching and removal from the network



AirTight® NETWORKS

WIPS in action - Rogue AP protection

- See demonstration video at

  http://www.airtightnetworks.com/fileadmin/content_images/demos/RogueAP-Demo/RogueAP-Demo.html

AirTight® NETWORKS

What are different types of Rogue APs

- Various permutations and combinations of
  - Bridging APs (on subnets coinciding with or different from wired interface address)
  - Router (NAT) APs (with and without MAC cloning)
  - APs with encrypted wireless links
  - APs with open wireless links
  - Soft APs (natively configured on wireless client or which use external devices such as USB sticks)
  - APs on different VLANs in the LAN including no-WiFi subnets

AirTight® NETWORKS

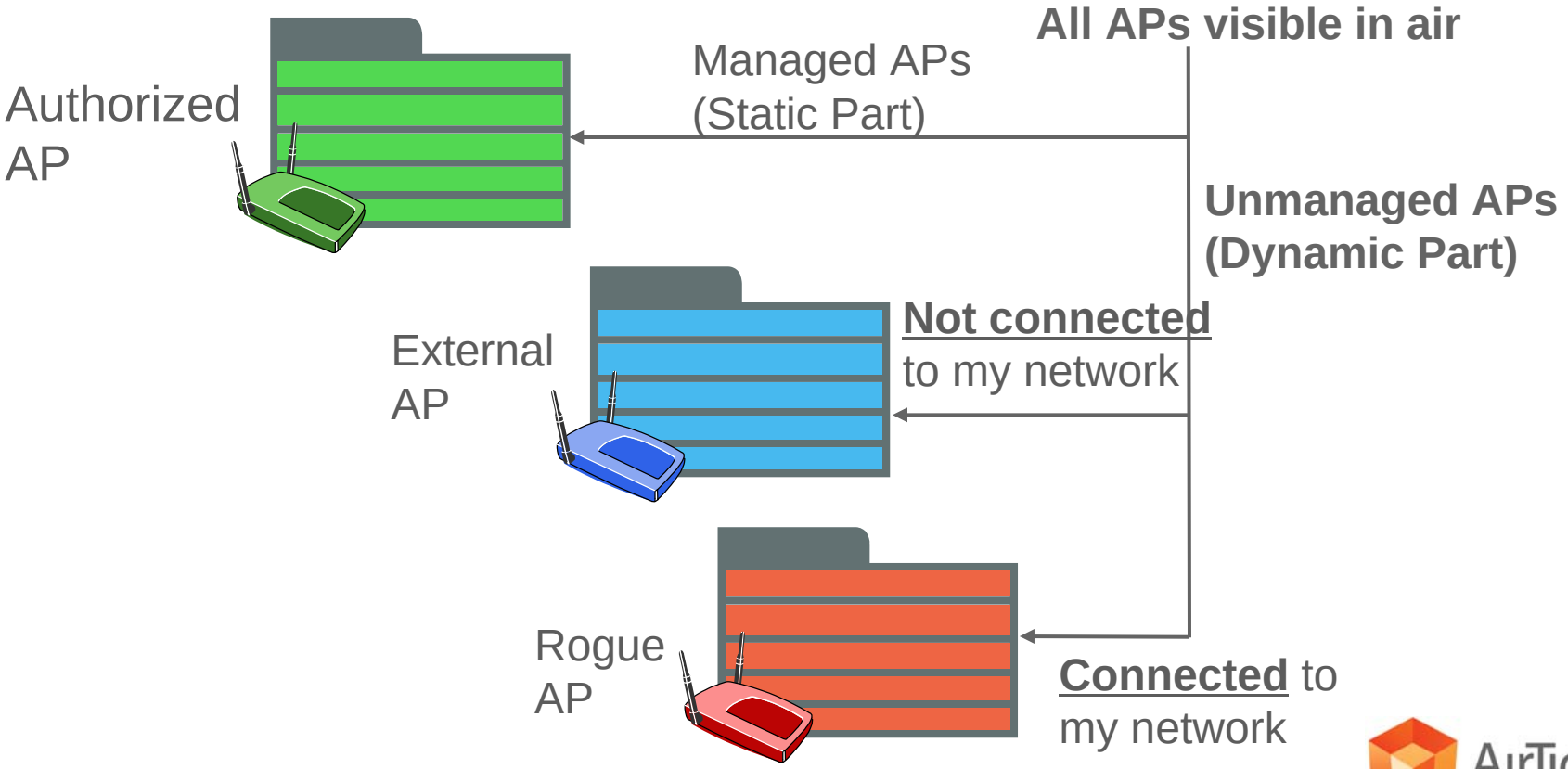
Can wire side only scanning protect from all Rogue AP

- No!
- Several Rogue AP types are undetectable by wire side only scanning, examples:
  - Bridging APs on a subnet inconsistent with their wired IP address (default configuration)
  - Soft APs
  - Router (NAT) APs with cloned wire side MAC address
- See http://blog.airtightnetworks.com/rogue-ap-detection-pci-compliance/ for more details

AirTight NETWORKS

What does AP auto-classification mean in the context of Rogue AP

- Automatically classifying APs visible in airspace into three categories: Authorized, External and Rogue



AirTight NETWORKS

What is key technology enabler for accurate auto-classification

- Robust testing of AP's connectivity to monitored enterprise network is the key technology enabler
- If AP is not detected as connected, when it is indeed connected to the monitored enterprise network, it results in security hole (false negative)
- If AP is detected as connected, when it is indeed not connected to the monitored enterprise network, it results in false alarm (false positive)

AirTight® NETWORKS

What are prevalent AP connectivity testing methods

MAC Correlation (CAM table lookup)

- Collect all MAC addresses seen on wired network (CAM table lookup)
- Detect all MAC addresses seen on wireless network
- Presume network connectivity of APs based on match between wired and wireless MAC addresses

Signature Packet Injection

- Inject signatures packets in the wired and wireless network
- Detect which APs forward signature packets between wired and wireless interfaces
- Confirm network connectivity of APs based on signature packet forwarding

AirTight® NETWORKS

How do these connectivity testing methods compare

- Packet injection method is superior to CAM table lookup as it is fast, accurate, gracefully scalable to large networks and capable of detecting all types of Rogue APs
- For more details on this comparison and auto-classification methods used in various WIPS in the market, see

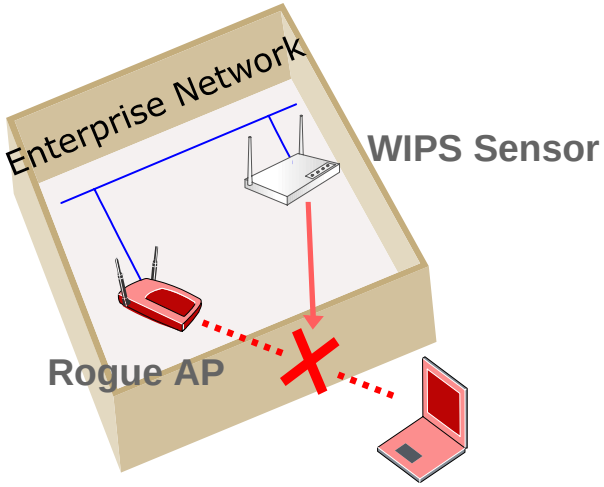
  http://blog.airtightnetworks.com/ugly-bad-and-good-of-wireless-rogue-access-point-detection/

  http://blog.airtightnetworks.com/making-the-right-choice-for-rogue-access-point-detection-technology/

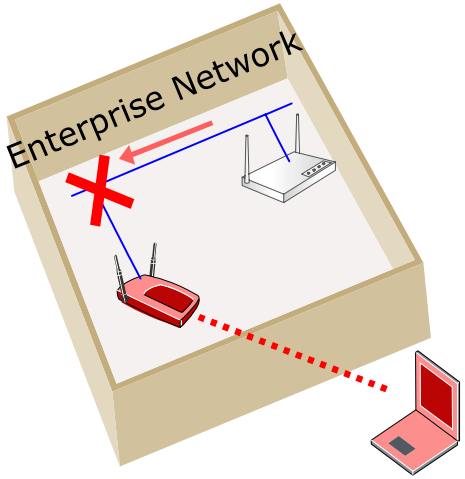
AirTight® NETWORKS

How does WIPS block Rogue AP

- Over the air quarantine
  - WIPS sensor blocks client's connection to Rogue AP by transmitting spoofed disconnection frames
  - Deauthentication is popularly used disconnection frame



- Switch port disable
  - WIPS attempts to locate switch port into which Rogue AP is connected
  - If found, disables the switch port using SNMP



AirTight NETWORKS

How do the two Rogue AP blocking methods compare

- Over the air quarantine
  - Works independent of correlation between wired and wireless addresses of Rogue AP
  - Non-intrusive with network infrastructure
  - No interoperability problems with different switch vendors
  - Deauthentication based over the air quarantine will not work with .11w Rogue APs
- Switch port disable
  - Only works for those Rogue APs which have correlation between wired and wireless addresses
  - Highly intrusive. WIPS needs need to know “set” password on switches. Error in tracing leaf switch may turn off entire switch branch
  - Suffers from switch vendor interoperability problems

AirTight® NETWORKS

Conclusion

- Rogue AP is unmanaged AP plugged into wired enterprise network by unwilling or malicious employees or visitors
- Rogue AP can expose wired enterprise network to outsiders over its RF signal spillage
- Rogue AP threat is not mitigated by firewalls, WPA2, 802.1x, NAC, anti-virus or wire side scanners
- Sensor based wireless intrusion prevention system (WIPS) detects, blocks and locates Rogue APs
- Testing of AP's connectivity to monitored enterprise network is key technology enabler for reliable protection from Rogue APs

AirTight® NETWORKS