

The Global Leader in Wireless Security and Compliance

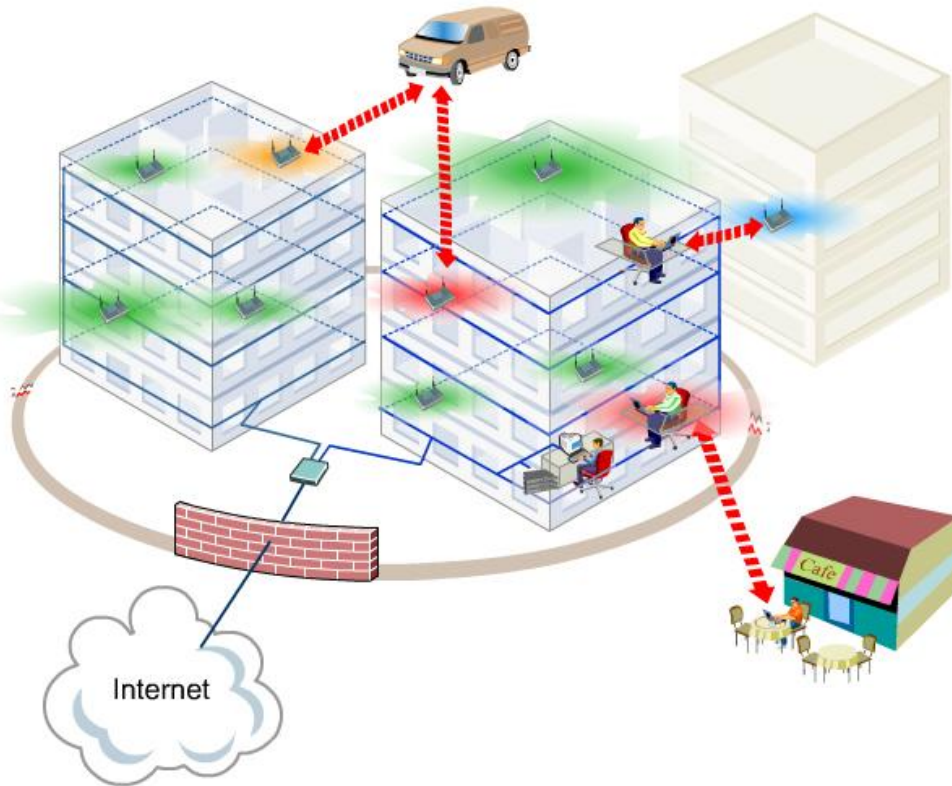


Wireless: The Invisible Threat to Your Network

Rick Farina
Senior Wireless Security Researcher

Wireless: The Invisible Threat to your Network

WiFi throws new pieces in the information security puzzle!



- ◆ Wired firewalls, IDS/IPS, anti-virus ineffective against WiFi threats
- ◆ Threats operate below Layer 3
- ◆ Operation in unlicensed band, open technology
- ◆ Signal spillover outside buildings

Everyone Is Talking About WiFi Security



Financial Districts Airspace Reveals Wi-Fi Security Risks,
Sarbanes-Oxley Compliance Journal, May 2009

http://www.s-ox.com/dsp_getNewsDetails.cfm?CID=2614



Citing safety, Govt bans WiFi in key offices, missions,
Indian Express, August 2009

<http://www.indianexpress.com/news/citing-safety-govt-bans-wifi-in-key-offices-missions/497766/>



PCI (Payment Card Industry) DSS Wireless Guidelines, June 2009

https://www.pcisecuritystandards.org/education/info_sup.shtml



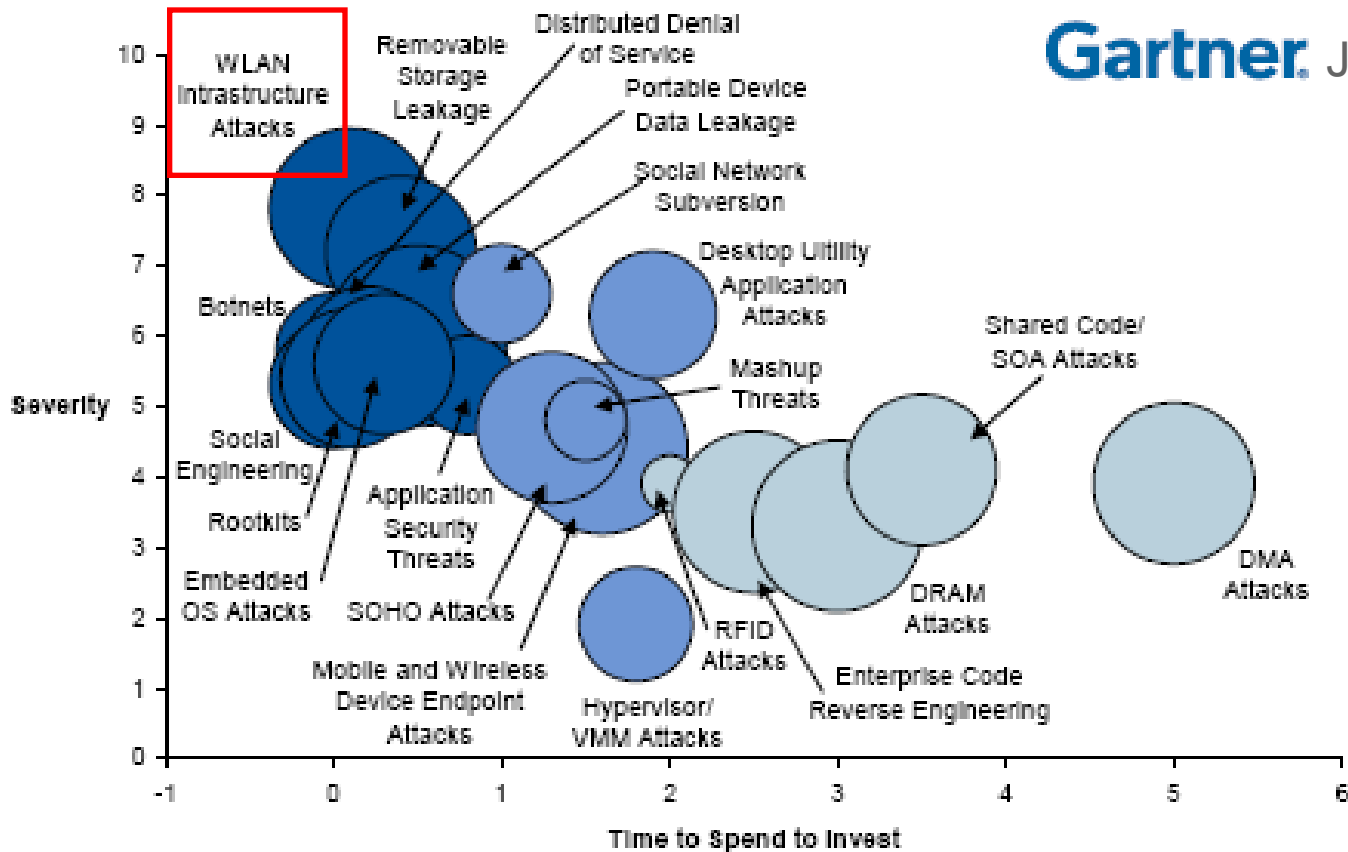
Security experts warn of dangers of rogue Wi-Fi hotspots,
CNN Business Traveler

<http://edition.cnn.com/2009/TECH/science/08/11/wifi.security.hackers/index.html?iref=24hours>

Some Even Say It Is A Top Priority

Next Generation Threats and Vulnerabilities Projection

Gartner June 2009



Sometimes We Learn The Hard Way



WSJ.com THE WALL STREET JOURNAL ONLINE

As of Friday, May 4, 2007

PAGE ONE

BREAKING THE CODE

How Credit-Card Data Went Out Wireless Door

Biggest Known Theft Came from Retailer With Old, Weak Security

By JOSEPH PEREIRA
May 4, 2007; Page A1

The biggest known theft of credit-card numbers in history began two summers ago outside a Marshalls discount clothing store near St. Paul, Minn.

- ◆ 94 Million payment card accounts compromised at TJX stores in USA over Wi-Fi
- ◆ Estimated liabilities more than \$4.5 Billion



expressindia.com

Latest terror email sent from WiFi at Khalsa College

Express News Service Posted: Aug 25, 2008 at 2344 hrs
Mumbai, August 24 ATS officials say email bears photographs of cars stolen from Navi Mumbai for terror activities; senders deleted log entries after using WiFi facility

Incorrect Views of WiFi Security



No WiFi
Enterprises

It doesn't apply to me.

“I don't have any WiFi installed and hence
I must be secure”



WiFi is officially
deployed

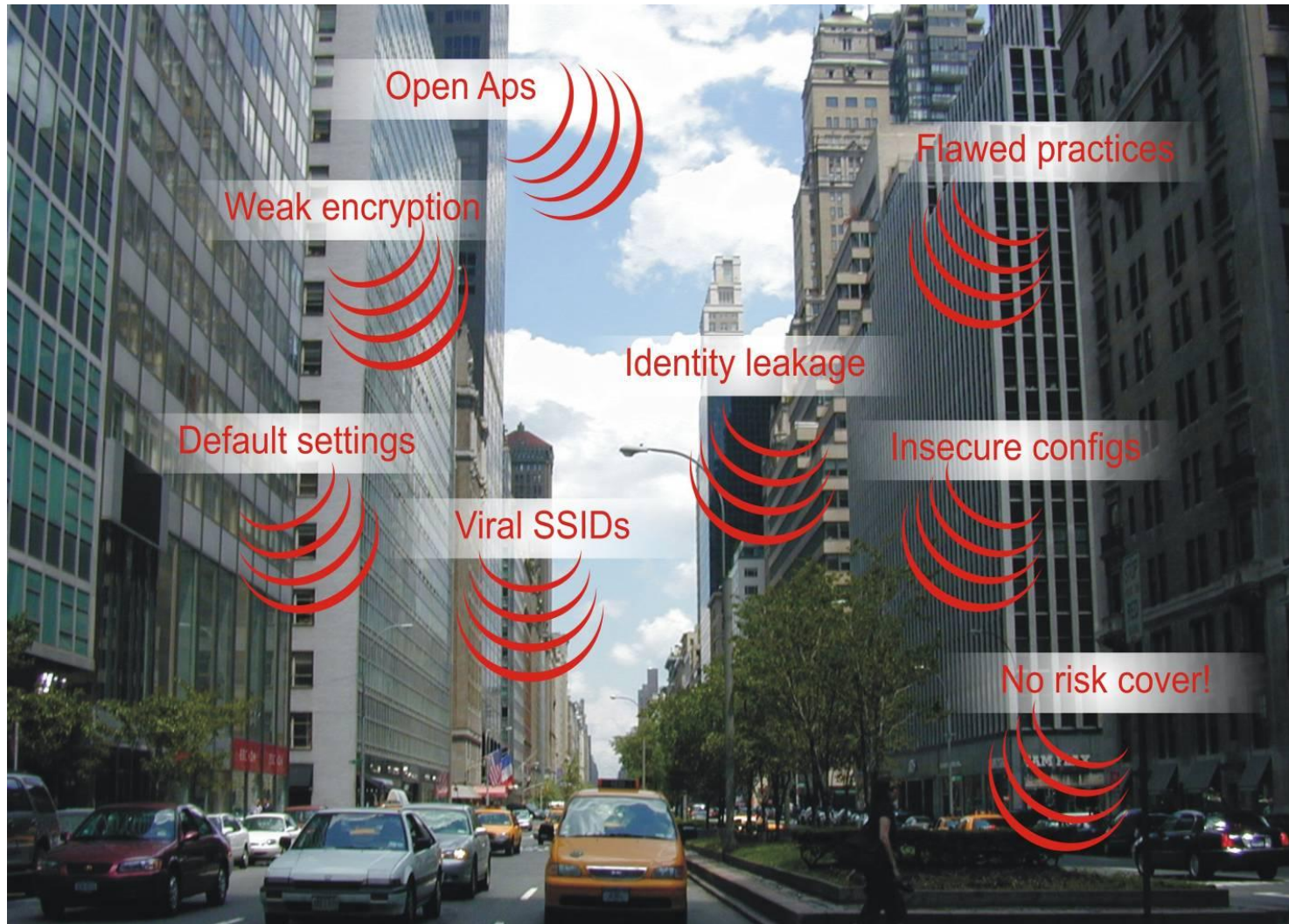
What I have is good enough

“I have Firewalls, IDS, Anti-virus installed and
hence I am already protected”

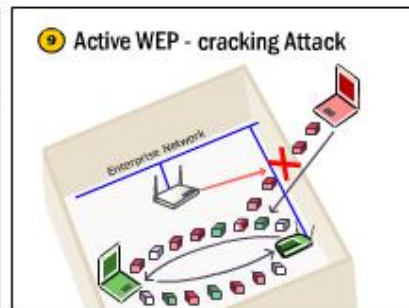
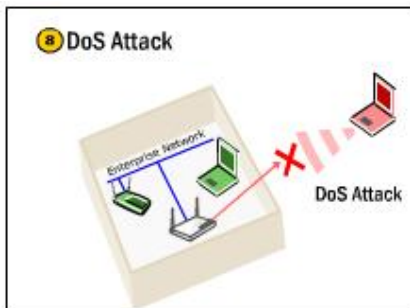
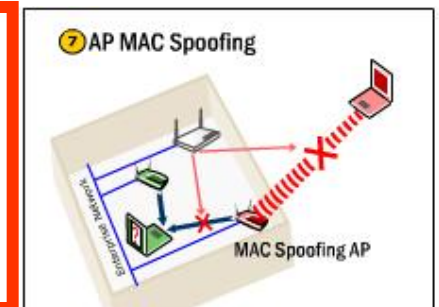
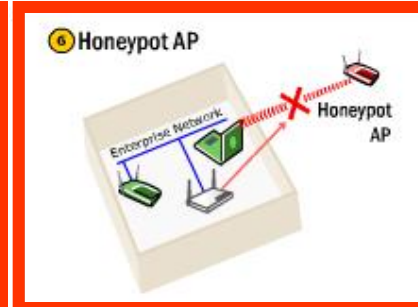
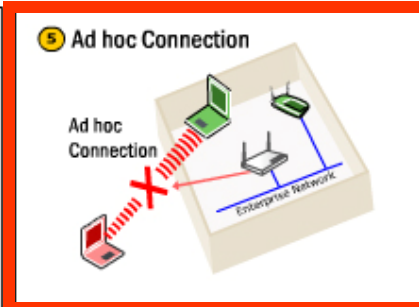
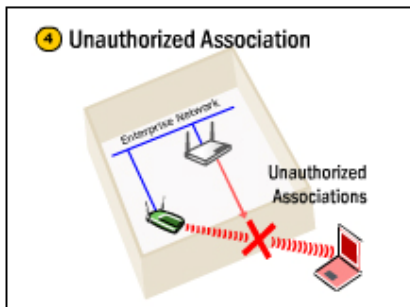
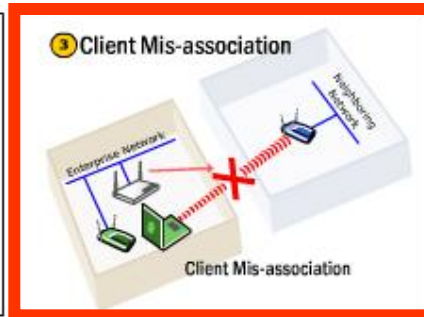
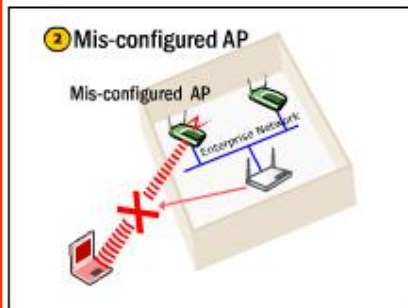
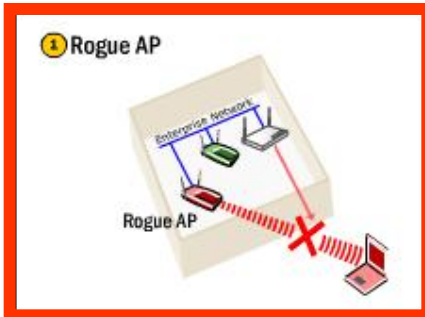
Today's Presentation

- ◆ 10 common wireless threats
- ◆ Challenges facing IT to detect and defend these threats
- ◆ The impact of 802.11n
- ◆ Different approaches for wireless threat detection, classification and prevention
- ◆ Client vulnerabilities
- ◆ Best practices

View from Hacker's Windshield



10 Common Wireless Threats



These threats also apply to “no WiFi” environments

Rogue AP

Unauthorized AP connected to monitored wired network

- ◆ Malicious intent or simply an unwitting, impatient employee looking to “light up” his office
- ◆ Provides direct access to enterprise network from areas of spillage
- ◆ Bypasses wireless encryption and wired firewall



Pocket AP



Wireless Router



Wall Jack AP

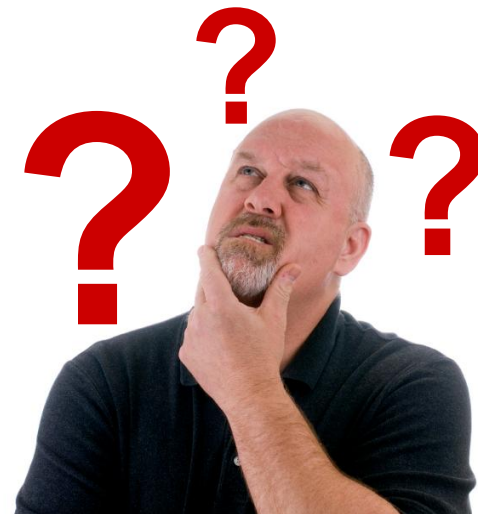


WiFi USB Drives

The Challenge – Which threats are genuine?

MAC	SSID	Enc...
000FCC5AE59C	BPMVR	WEP
001C106C6928	zguest	
0019A9A7C131	gear6-guest	
0030AB1EF491	nothere	WEP
001C106C63D8	zguest	
000D9714A632	GoogleWiFiSecure	WEP
000D9704A632	GoogleWiFi	
0018F8A2595C	meeting	WEP
001D7E9ADB88	earth	WEP
000D97140B89	GoogleWiFiSecure	WEP
000D97040B89	GoogleWiFi	
000F66E8242D	Corp	WEP
000D9704845E	GoogleWiFi	
00119334BE90	Netgear102	WEP
000D9714845E	GoogleWiFiSecure	WEP
00237521D0C0	1037 1665	WEP
000FCCFEE1C0	7756 7014	WEP
001195E0F2D8	matisse.netg	WEP
001E5823BF27	matisse.guest	WEP
00121762B57D	linksys-g	
000D0B2B0C1B	spectra	WEP
0040058ECC17	dlink614	WEP
0014BFF480E8	Alice	WEP
001EE5F30E03	SIT Network	WEP
0020A6534D1C	anw	WEP

- ◆ Large number of APs visible in air
- ◆ New APs come up often
- ◆ Old APs change configurations
- ◆ Most of them are not Rogue APs
 - Neighborhood, municipal, hotspot

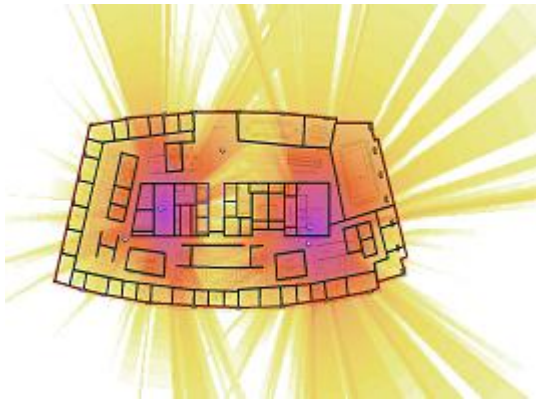


802.11n Amplifies Existing Security Threats



Rogue threats evade legacy WiFi security

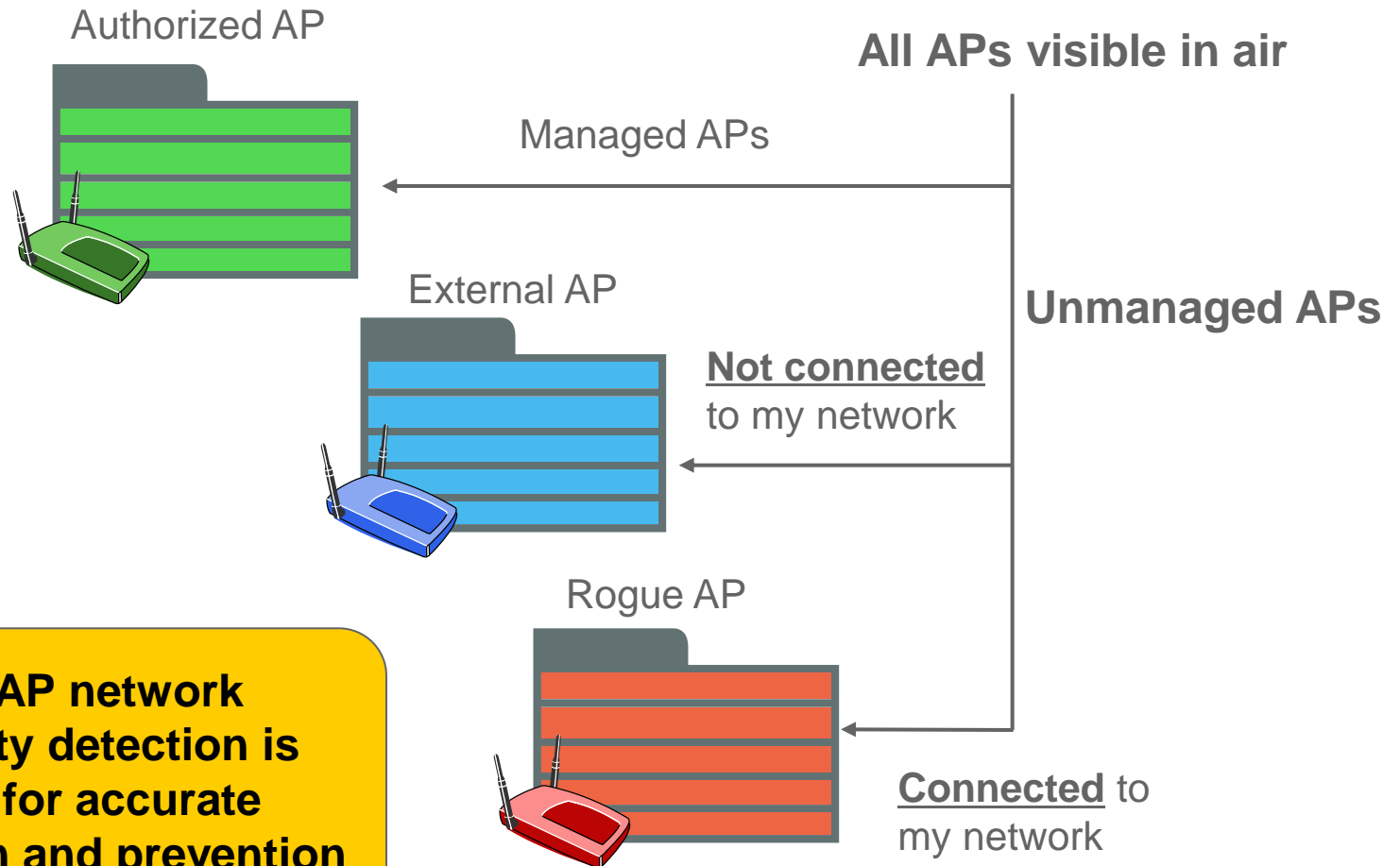
- ◆ 802.11n is already accepted by consumers & SMBs
- ◆ Majority of rogue APs are consumer APs
- ◆ Legacy WiFi security tools often miss new 11n devices
- ◆ 802.11n devices allow hackers to evade existing monitoring systems



Increased RF exposure

- ◆ 11n devices increase the range
- ◆ Networks more vulnerable to eavesdropping
- ◆ APs visible to more unauthorized users
- ◆ More external APs visible

Solution: On wire/off wire detection



Robust AP network connectivity detection is required for accurate classification and prevention

Two Basic Approaches to AP Classification

Active Techniques (Packet Injection)

- **Confirm network connectivity**
- Inject small signature packets in the wired and wireless network
- Detect which devices forward signature packets between wired and wireless interfaces

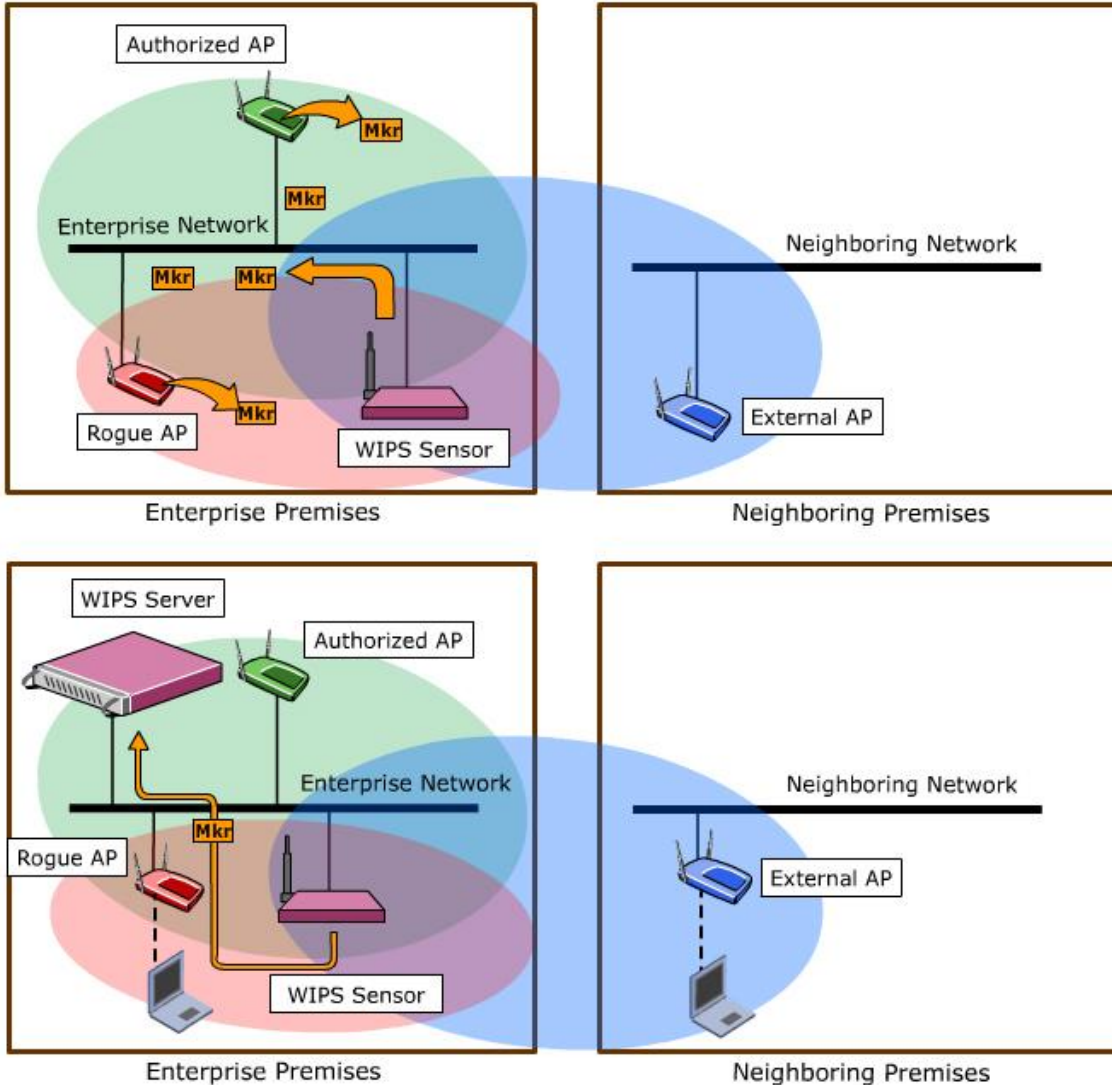
HP, Enterays/Siemens,
Trapeze, AeroHive, 3COM,
AirTight

Passive Techniques (MAC Correlation)

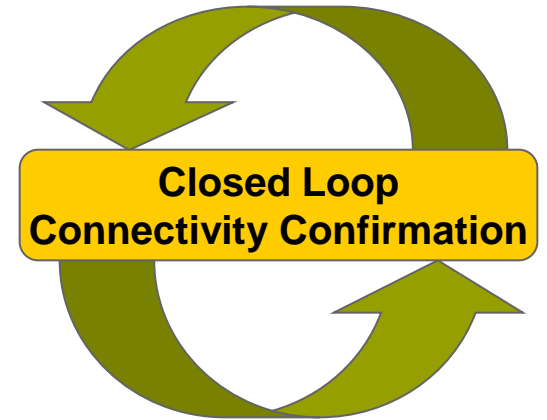
- **Presume network connectivity**
- Lookup all MAC addresses seen on **wired** network
- Detect all MAC addresses seen on **wireless** network
- **Try to match wired and wireless** MAC addresses

Cisco, Motorola/AirDefense,
Aruba, Fluke/AirMagnet

Active Techniques (Packet Injection)



Wired to Wireless Test



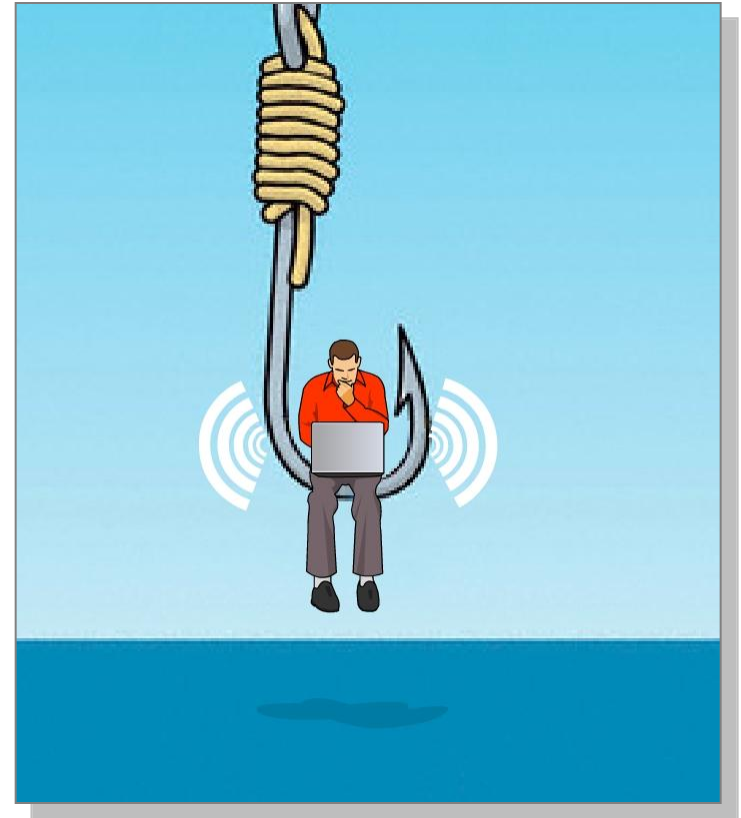
Wireless to Wired Test

Active vs. Passive Techniques

Criteria	Active Techniques	Passive Techniques
AP types covered for connectivity detection (bridge, NAT/Router etc.)	All	Many NAT/Router APs not covered
Latency of detection	Low (few minutes)	High (45 minutes or longer)
Misclassification (external APs appear connected to wired network)	Never	Routine
Manual inspection required	Rarely	Often
Automates threat prevention	Yes	Beware of shutting down neighbors
Scalability to large wired networks	Excellent	Poor

Users Unaware They Are Vulnerable to Wi-Phishing

- ◆ 56 % Clients were found to be probing for one or more SSIDs
- ◆ 34 % of them were willing to connect to “HIGHLY INSECURE” Wi-Fi networks
- ◆ 13 % Clients were found probing for OPEN ad hoc networks



Trusted Network Information Leakage By Wi-Fi Users

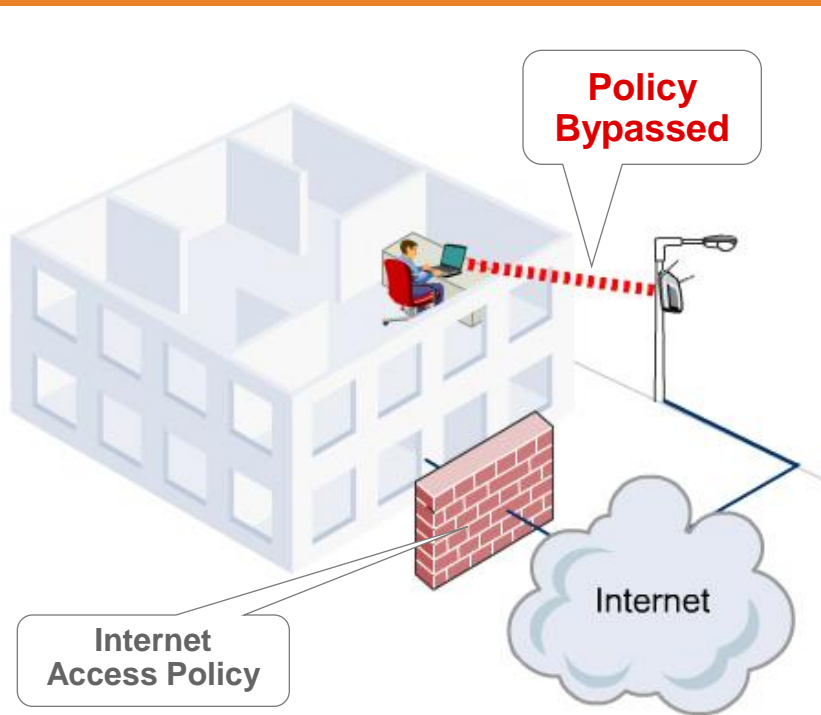


```
0:ld:e0:90:1[redacted] | 15827258f644cc7e635a8bc, Booyakasha, Mikes[redacted], mobile  
point, 5d52f14f3d5c0954f4fe6d39, tmobile, stayonline, deloro  
0:ld:e0:c[redacted] | concourse, Guimond, ramada  
0:le:4c:67:[redacted] | IMCCENTRAL  
0:le:4c:67:[redacted] | RRDWIR1  
0:le:4c:b3:[redacted] | kendog4, MBTA_WiFi_Coach0708_Box-062  
0:le:8c:2b:[redacted] | Skywriter, BUCKINGHAM, 10SConf, Conference, CudziloC-Wirele  
ss, martinipark  
0:le:8c:4c:[redacted] | AMF, loganwifi, Cammocks Network, SRHSWiFi, ihs, M1M1 Wirele  
ss, eircom6526 6330, eircom6542 6404, Hoffmanns  
0:le:8c:df:[redacted] | focr  
0:lf:29:f4:[redacted] | linksys  
0:lf:3a:12:[redacted] | TradIT  
0:lf:3a:4:[redacted] | MBP  
0:lf:3a:4c:[redacted] | Str8CashHomey, edoren  
0:lf:3a:4d:[redacted] | Vendor  
0:lf:3a:e:[redacted] | 2WIRE831, 2wire  
0:lf:3b:1f:[redacted] | Enernoc-BG  
0:lf:3b:39:[redacted] | testwire, Customer ID  
0:lf:3b:3f:[redacted] | RJ_HOTSPOT, Berthold Network, linksys, Baymont 3, PacificInn  
Crest, admiralsclub, tmobile
```

Laptop's probing for SSIDs from preferred network list (cached)
are vulnerable to "Honeypot" attacks

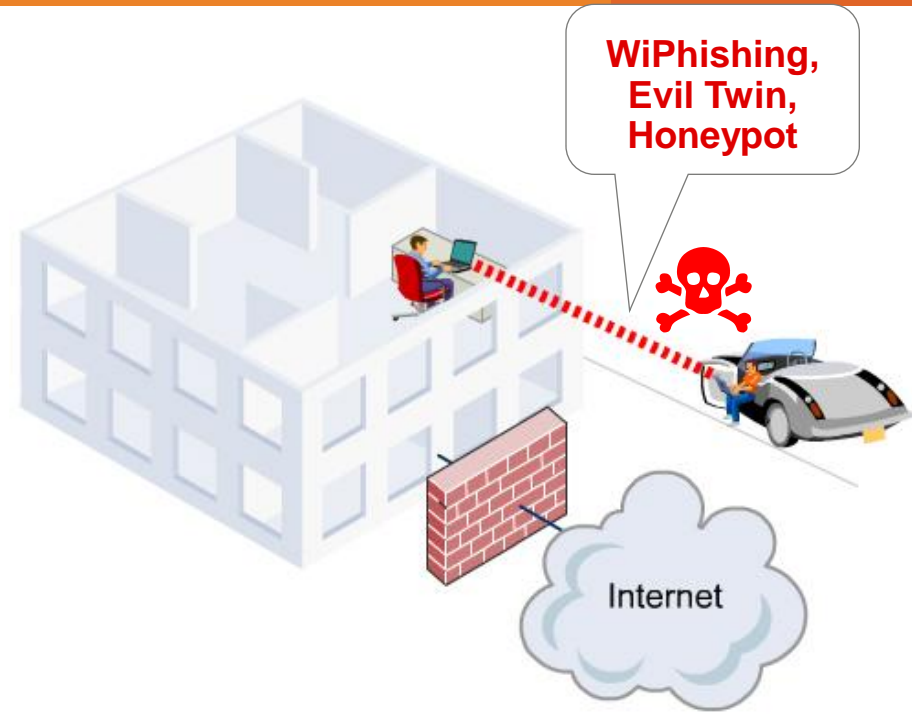
Client Vulnerability Demo

Client Mis-associations



◆ Policy violation

- Gmail, IM, banned websites, banned content

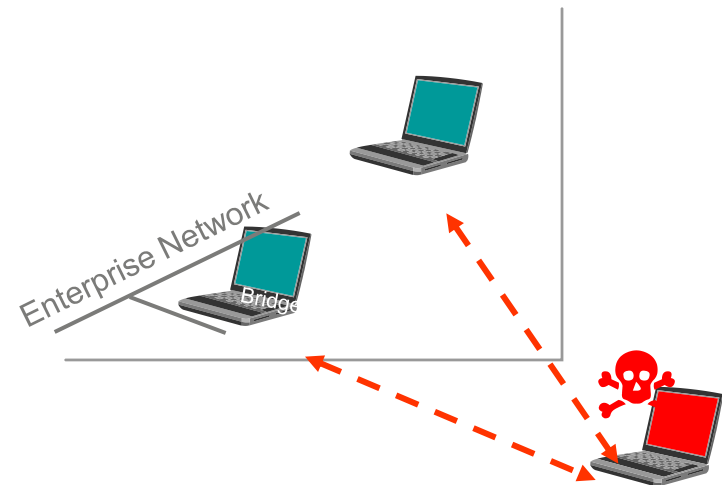
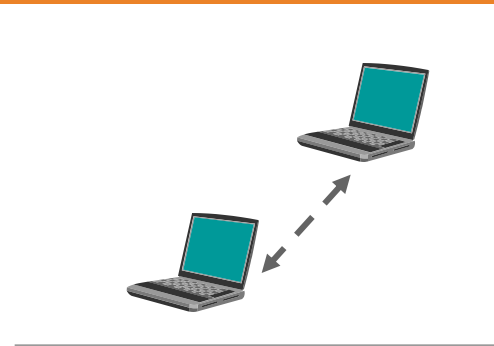


◆ MITM attack

- Password stealing, data interception
- Growing number of hack tools: KARMETASPLOIT, SSLstrip, Airbase

Ad hoc Connections

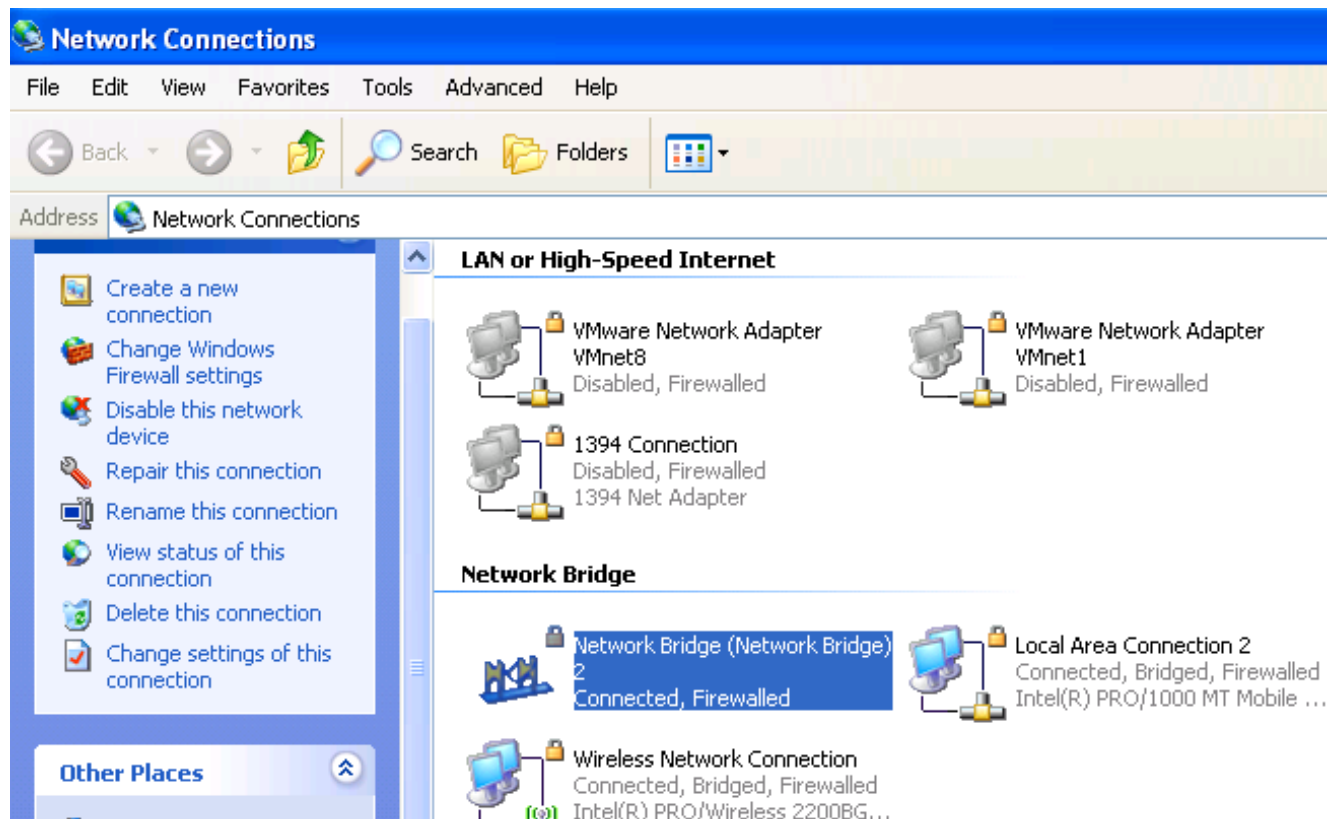
- ◆ Employees may use ad hoc connections to share content
 - Reduce productivity
 - Leak sensitive data
- ◆ Inadvertent ad hoc connections
 - Compromise laptop
 - Bridge to enterprise network



For some real world data on ad hoc vulnerability, see AirTight's scan study at worldwide airports: <http://www.airtightnetworks.com/home/resources/knowledge-center/airport-scan.html>

“Bridge” to Wired Network

- ◆ Users may “bridge” wired and WiFi interfaces on their laptops



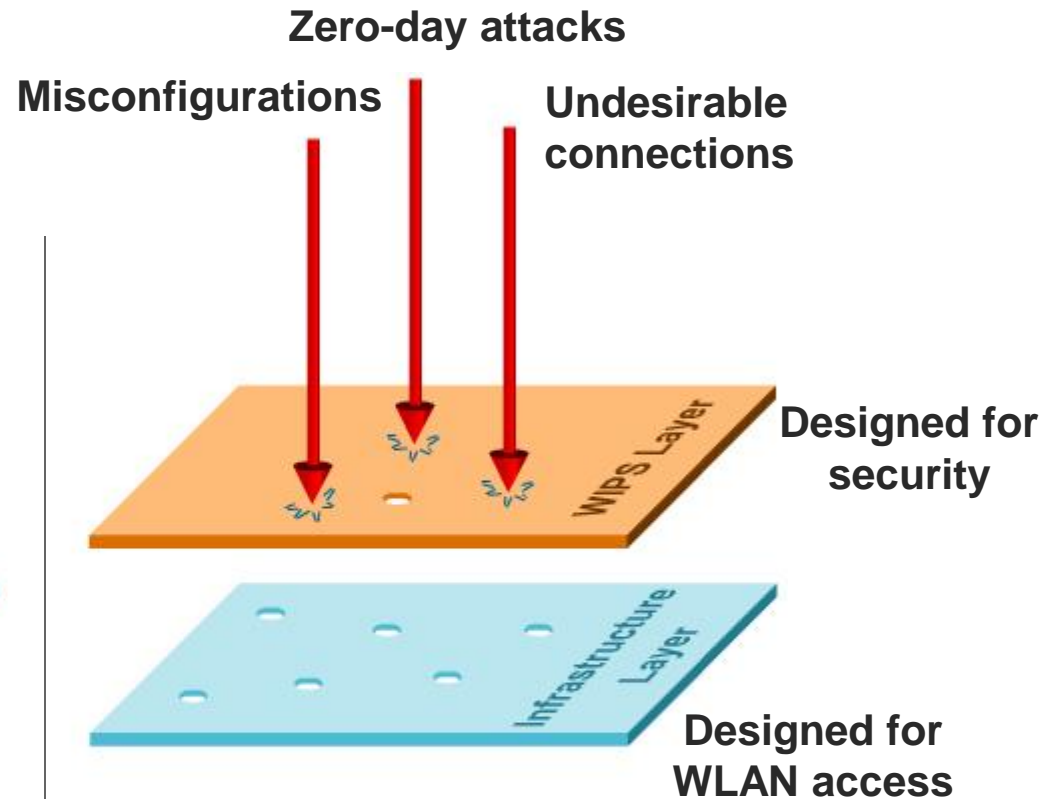
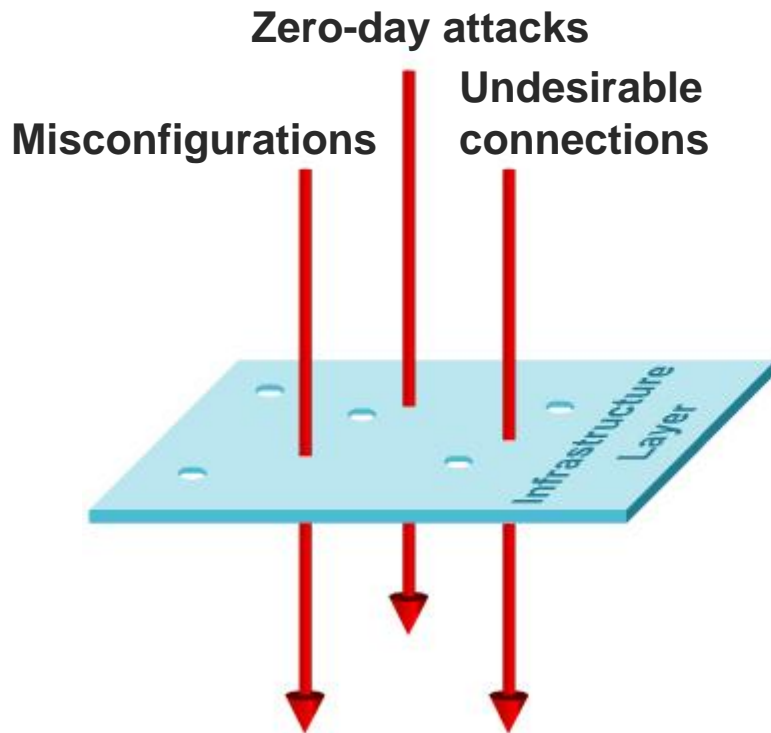
Background Scanning is Insufficient for WLAN Security

- ◆ Use an independent layer of security, separate from the WLAN infrastructure

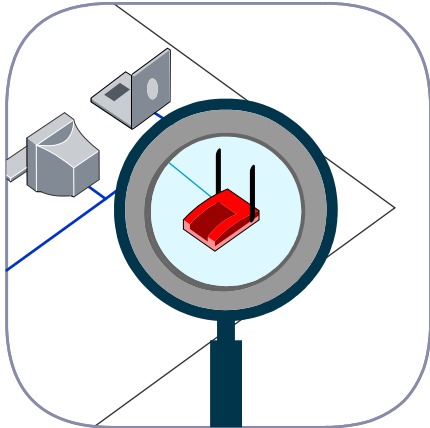
Gartner.

“...overlay systems provide the most flexible approach for rapidly incorporating wireless monitoring and intrusion prevention.”

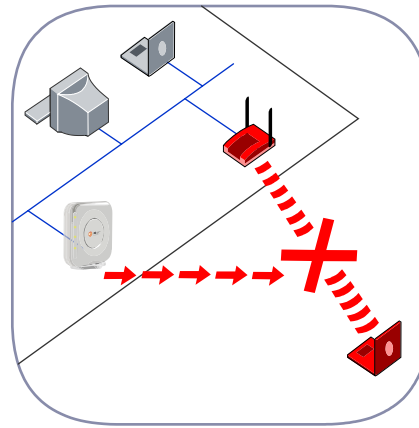
WIPS: An Independent Layer of Protection



WIPS Capabilities



Detect WiFi Threats and Vulnerabilities



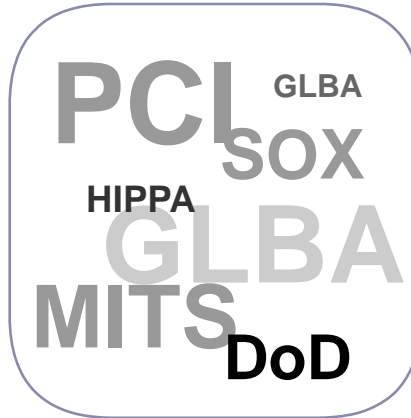
Block WiFi Threats and Vulnerabilities



Locate Threat Posing Devices on Floor



Forensic Information











Compliance Monitoring



Performance Monitoring and Troubleshooting

Five Steps to Protect Against WiFi Security Breaches

Recommended Best Practice	WiFi deployed	WiFi not deployed
<p><u>Use strong authentication and encryption</u> Use the best standards for authentication and encryption (e.g., WPA/WPA2) when deploying WiFi networks</p>		
<p><u>Monitor guest WiFi access</u> Authenticate guest users and monitor unauthorized access when providing guest access over WiFi networks</p>		
<p><u>Conduct wireless security audits and scans</u> Periodically conduct wireless scans to detect presence of unauthorized WiFi devices and activity in your premises.</p>		
<p><u>Follow endpoint wireless security best practices</u> Promote WiFi security best practices among laptop users. Using wireless security endpoint security agent, enforce your enterprise policies seamlessly across all laptops and secure them even when they are away.</p>		
<p><u>Use a Wireless Intrusion Prevention System (WIPS)</u> Prevent leakage of sensitive data and protect your network from wireless security threats with 24/7 wireless monitoring</p>		

AirTight Background

The global leader in wireless security solutions

Customers

AirTight protects leading enterprise companies in a broad range of industries

- ♦ Financial Services
- ♦ Retail
- ♦ Healthcare
- ♦ Government
- ♦ Education
- ♦ Manufacturing
- ♦ Transportation/Logistics
- ♦ Telecom/Technology

Technology Leadership

AirTight patents cover the key elements of wireless intrusion prevention (WIPS)

- ♦ 15 patents granted
- ♦ 25+ patents pending
- ♦ Industry's first 802.11n WIPS
- ♦ World's first wireless security subscription service (SaaS)

Industry Recognition

AirTight is widely recognized as an innovator and leader in wireless security

Gartner



F R O S T & S U L L I V A N