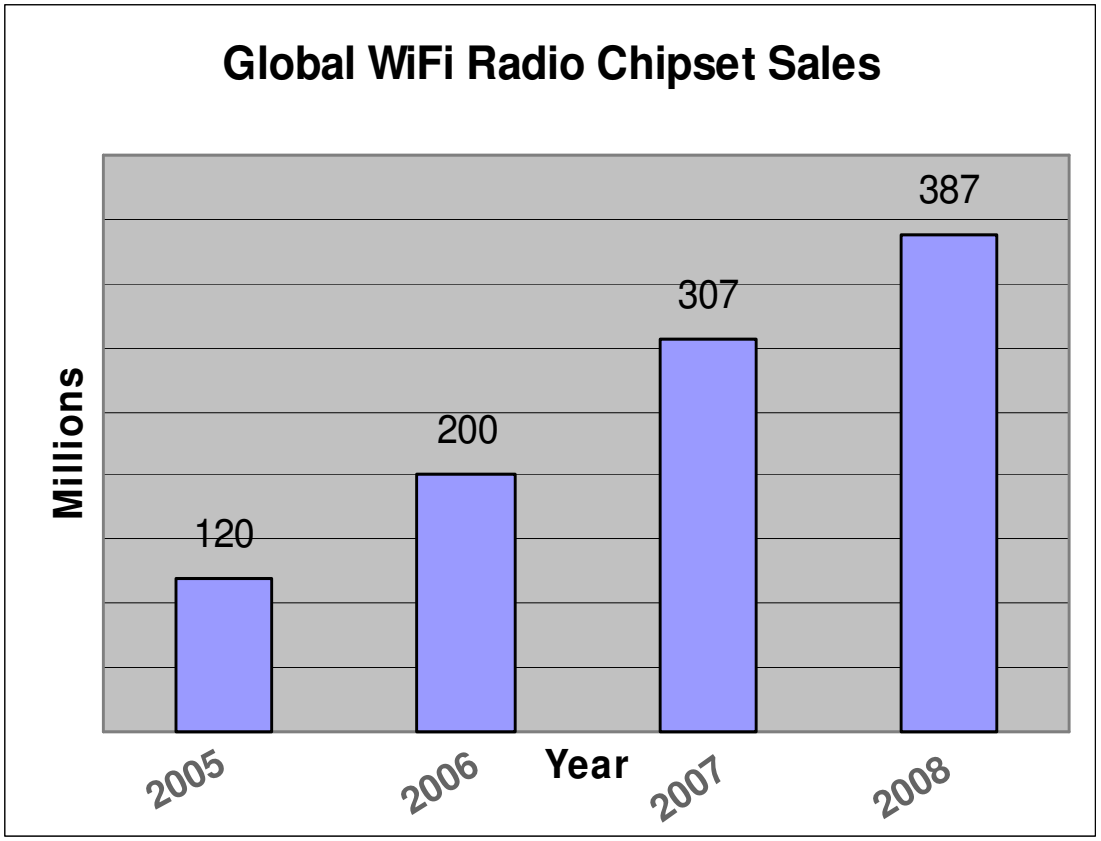
Understanding WiFi Security Vulnerabilities and Solutions

Dr. Hemant Chaskar
Director of Technology
AirTight Networks

WiFi Proliferation



Source: WiFi Alliance, www.wifialliance.org

AirTight® NETWORKS

Irony of Information Age

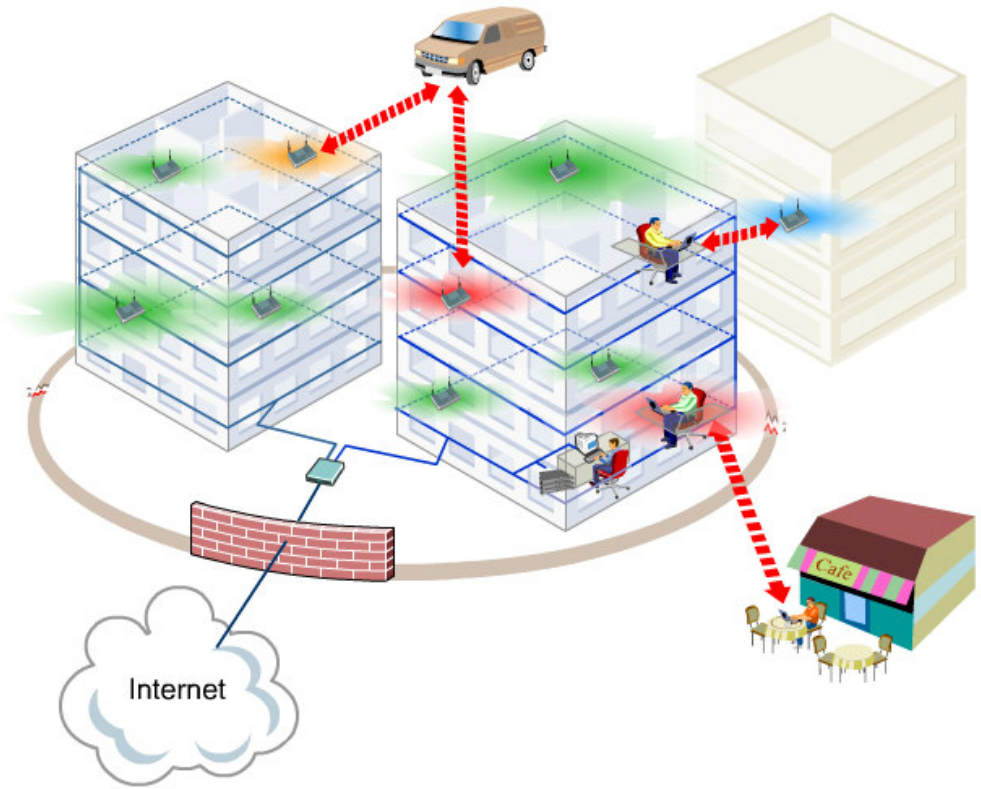
"It's the great irony of our Information Age -- the very technologies that empower us to create and to build also empower those who would disrupt and destroy."

- US President Obama on Cyber Security

AirTight® NETWORKS

WiFi Is No Exception

WiFi throws new pieces in the information security puzzle!



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

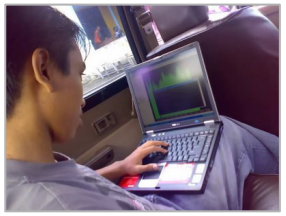
AirTight® NETWORKS

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

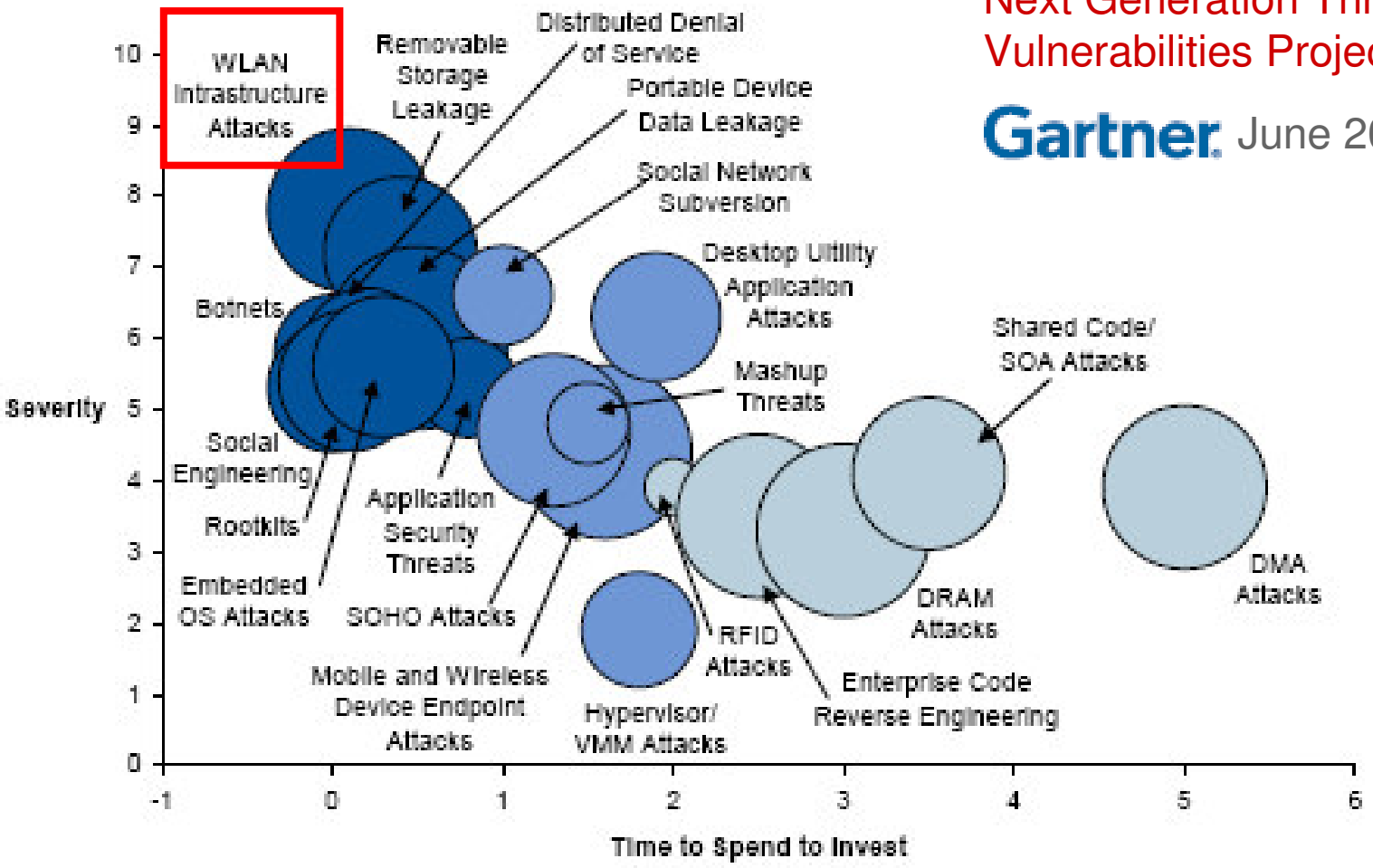


WiFi networks under attack from wardrivers, The Times of India, September 2008
http://timesofindia.indiatimes.com/India/WiFi_under_attack_from_wardrivers_/articleshow/3429169.cms

Security experts warn of dangers of rogue Wi-Fi hotspots, CNN Business Traveler, August 2009
http://edition.cnn.com/2009/TECH/science/08/11/wifi.security.hackers/index.html?iref=24hours

AirTight® NETWORKS

Some Say It Is Top Priority Today



Next Generation Threats and Vulnerabilities Projection

Gartner June 2009

AirTight® NETWORKS

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.

- 45.7 Million payment card accounts compromised at TJX stores in USA over WiFi
- 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*

AirTight® NETWORKS

Closer Look At WiFi Vulnerabilities

AirTight® NETWORKS

Incorrect Views of WiFi Security

No WiFi Enterprises

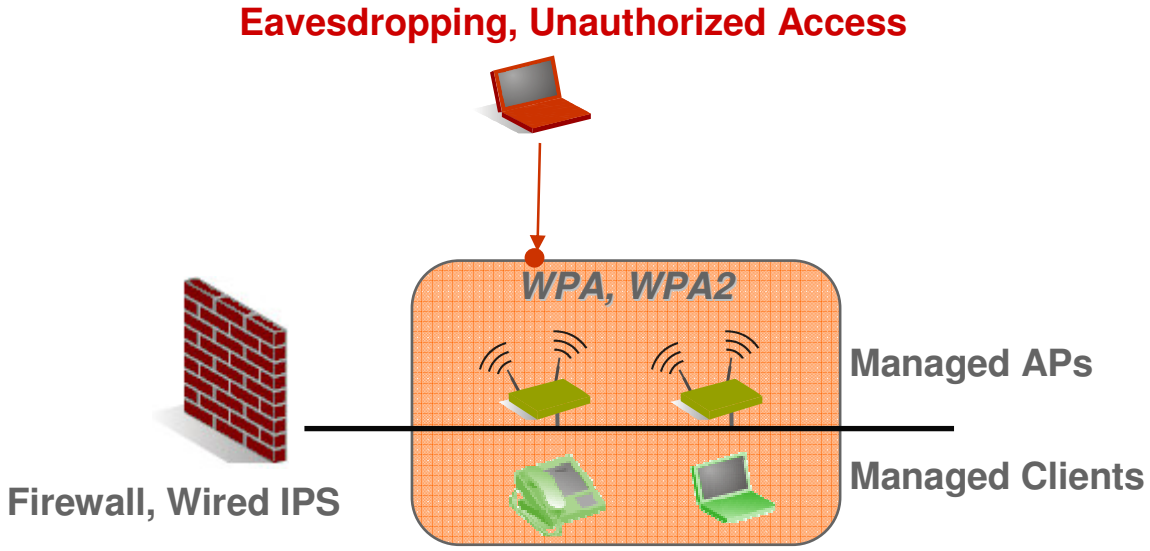
"I don't have any WiFi installed and hence I must be secure"

WiFi is officially deployed

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

AirTight® NETWORKS

Most Obvious WiFi Threat



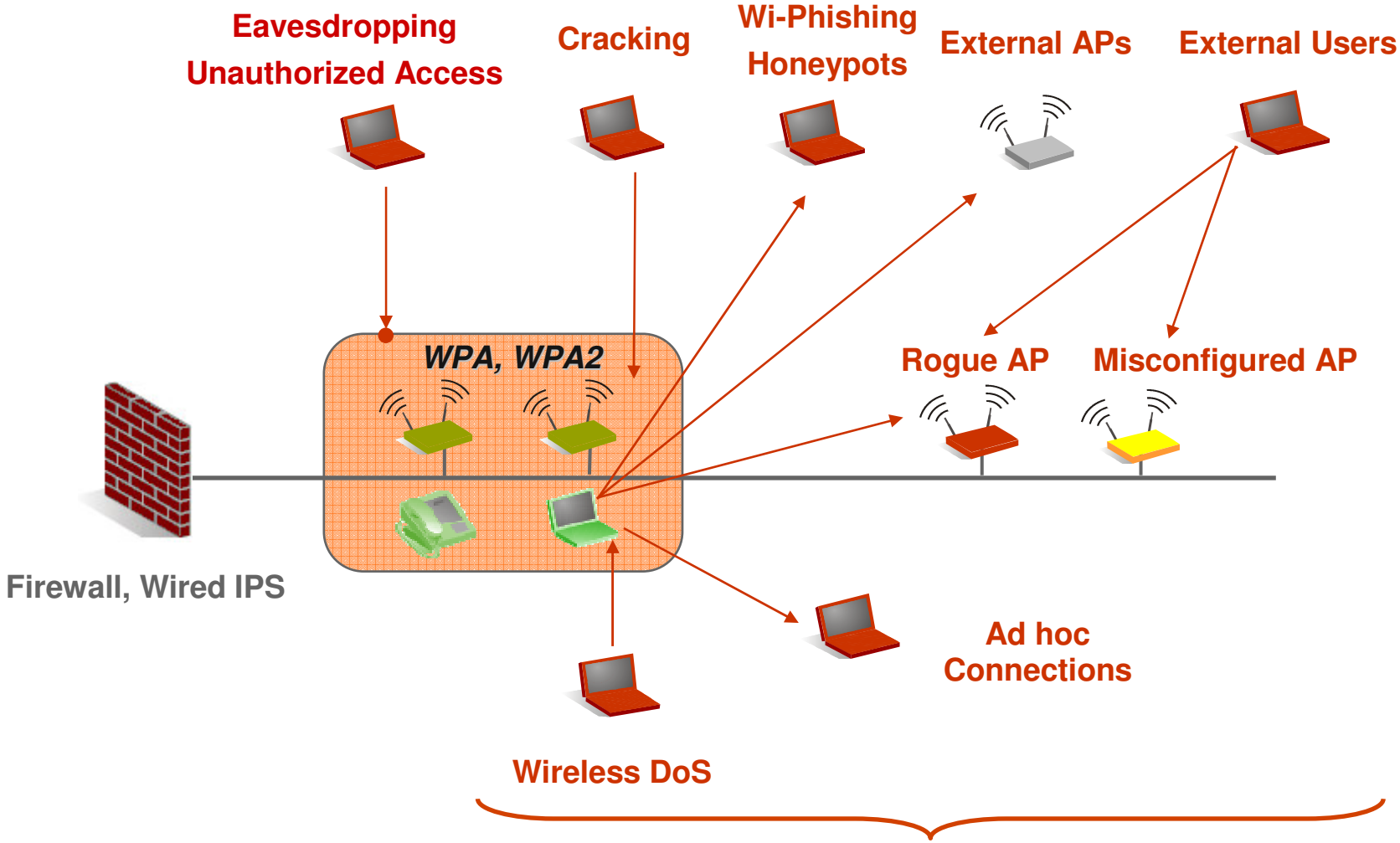
Solution: Use of strong wireless authentication & encryption in WiFi

- OPEN and WEP are big NO!
- WPA can be used, but not enterprise grade, use WPA2 which is enterprise grade
- SSID hiding and MAC access control lists can be evaded

Find tutorial on WPA/WPA2 at -
http://www.airtightnetworks.com/fileadmin/content_images/news/webinars/AuthEncryp_Primer.pdf

AirTight® NETWORKS

WPA2 or No-WiFi Cannot Address Unmanaged Devices



AirTight® NETWORKS

Rogue AP

= Unmanaged AP attached to network

= (Logically) LAN jack hanging out of window

Wall Jack AP

Pocket AP

Wireless Router

PCMCIA and USB APs

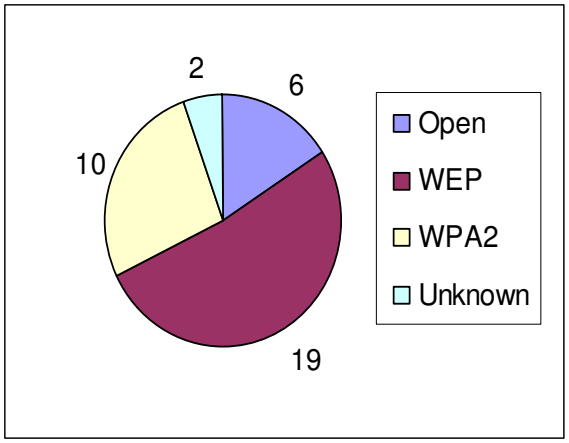
- Malicious intent or simply an unwitting, impatient employee
- Provides direct access to wired network from areas of spillage
  - Steal data on wire
  - Scan network for vulnerabilities
  - Firewall, anti-virus, WPA2 do not see this

AirTight® NETWORKS

Case Studies

Example: APs visible in airspace of client site

- 21 APs are unaccounted for (Open and WEP)
- Can one of the unaccounted for APs be on their wired network?
- How can they keep track of APs 24x7?



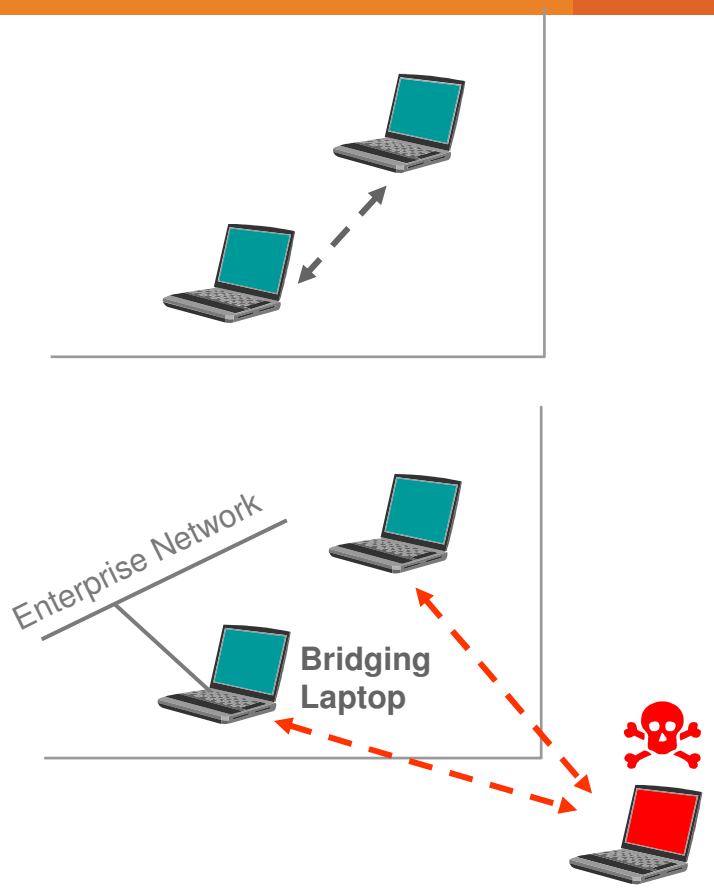
Unaccounted Insecure APs Are Present in All Wireless Neighborhoods.

- AirTight Networks Scan of Financial Districts in USA, May 2009
http://www.airtightnetworks.com/home/resources/knowledge-center/financial-districts-scanning-report.html
- RSA Wireless Security Survey, 2007 and 2008 scans of London, New York, Paris
http://www.rsa.com/node.aspx?id=3268
- Deloitte Scan of Indian Cities, December 2008
http://bcm-india.org/wifi_india.pdf
- AirTight Networks Scan of Indian Cities, November 2008

AirTight® NETWORKS

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

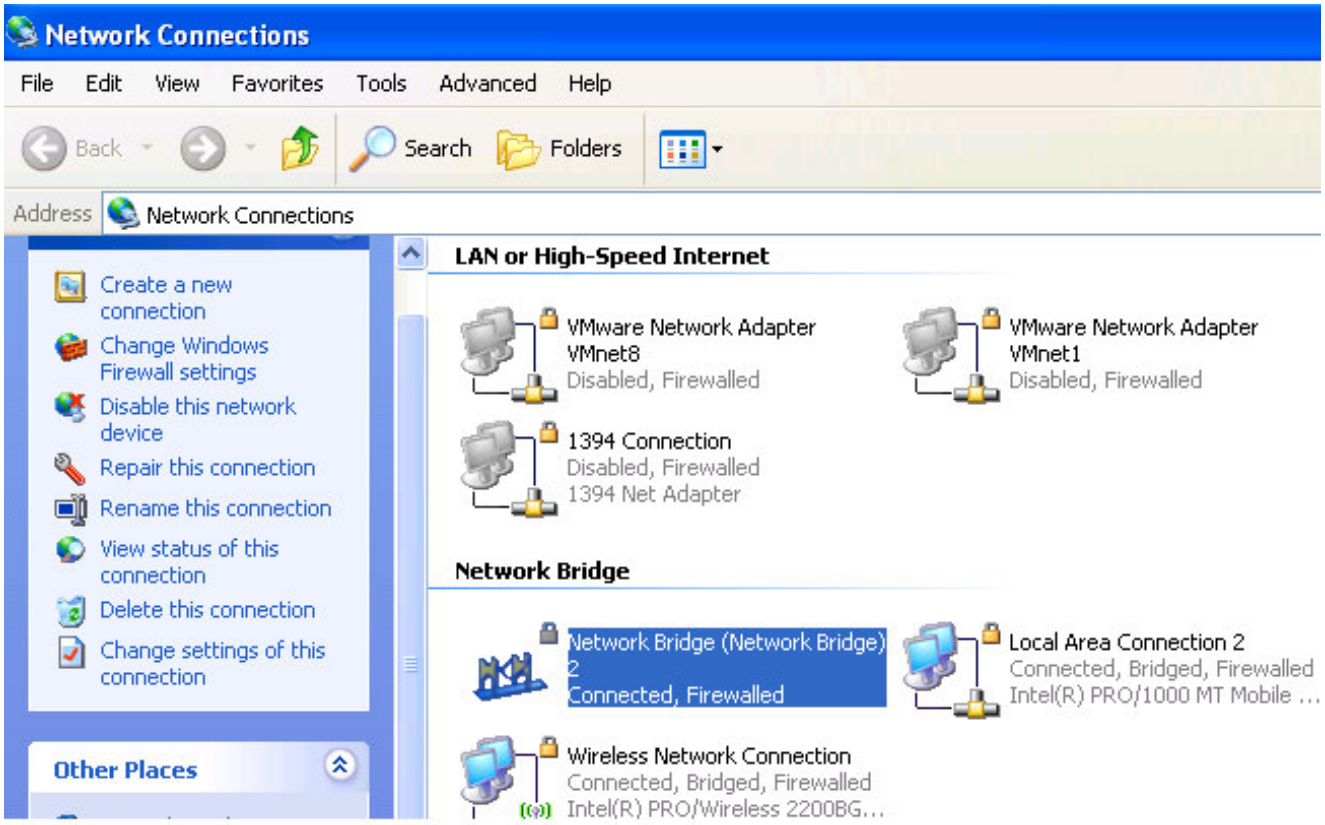


For some real world data on ad hoc vulnerability, see AirTight's scan study at worldwide airports:
http://www.airtightnetworks.com/home/resources/knowledge-center/airport-scan.html

AirTight® NETWORKS

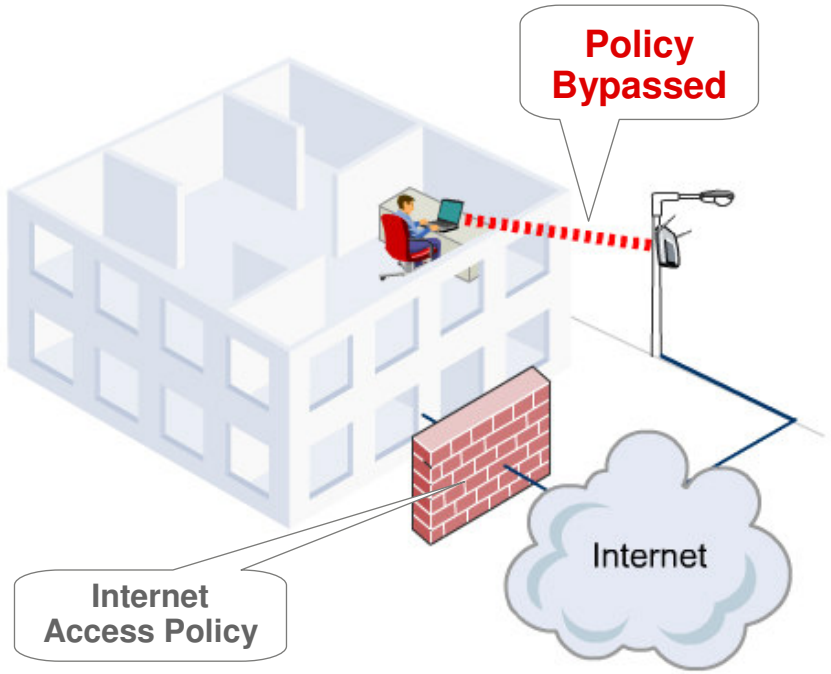
Ad hoc “Bridge” to Wired Network

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

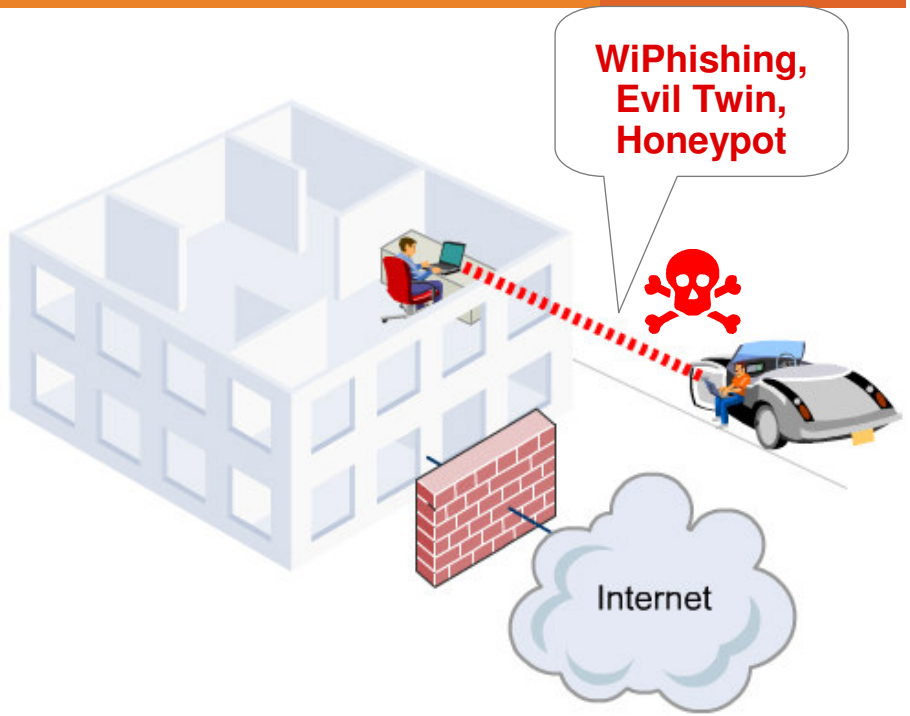


AirTight® NETWORKS

Misassociations



- **Policy violation**
  - Gmail, IM, banned websites, banned content



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

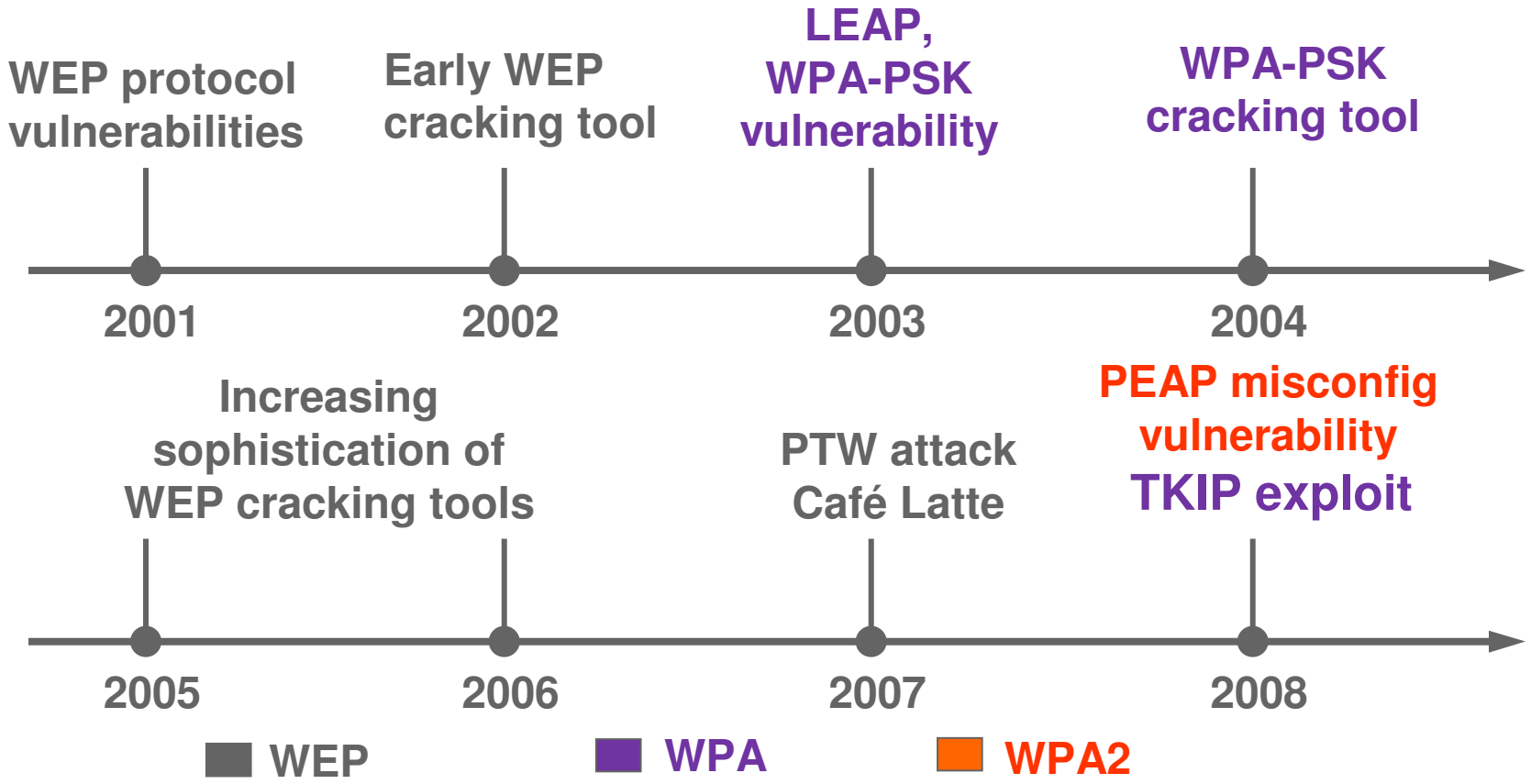
AirTight® NETWORKS

Honeypot/Evil Twin/WiPhishing

- KARMETASPLOIT:
  - http://trac.metasploit.com/wiki/Karmetasploit
    http://blog.trailofbits.com/karma/
    http://blog.airtightnetworks.com/karmetasploit-integrated-tool-lowers-bar-on-hacking-wireless-clients/
- SSLstrip:
  - http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf
    http://blog.airtightnetworks.com/sslstrip-even-the-scrupulous-users-can-be-trapped-by-wireless-honeypots/
- Airbase:
  - http://www.aircrack-ng.org/doku.php?id=airbase-ng#description
    YouTube - Fishing Windows Clients with airbase-ng and airchat
- WiFish Finder (free honeypot vulnerability assessment tool):
  - http://www.airtightnetworks.com/wifishfinder

AirTight® NETWORKS

Cracking Exploits



For more information on cracking exploits:
http://www.airtightnetworks.com/home/resources/knowledge-center/wep.html
http://www.shmoocon.org/2008/videos.html (Look for PEAP Pwned Extensible Authentication …)
http://www.airtightnetworks.com/home/resources/knowledge-center/wpawpa2-tkip-exploit.html

AirTight® NETWORKS

DoS Attacks

- Wireless DoS attacks are inevitable for WiFi
  - Spoofed disconnects
  - Spoofed connection floods
  - Hogging wireless medium

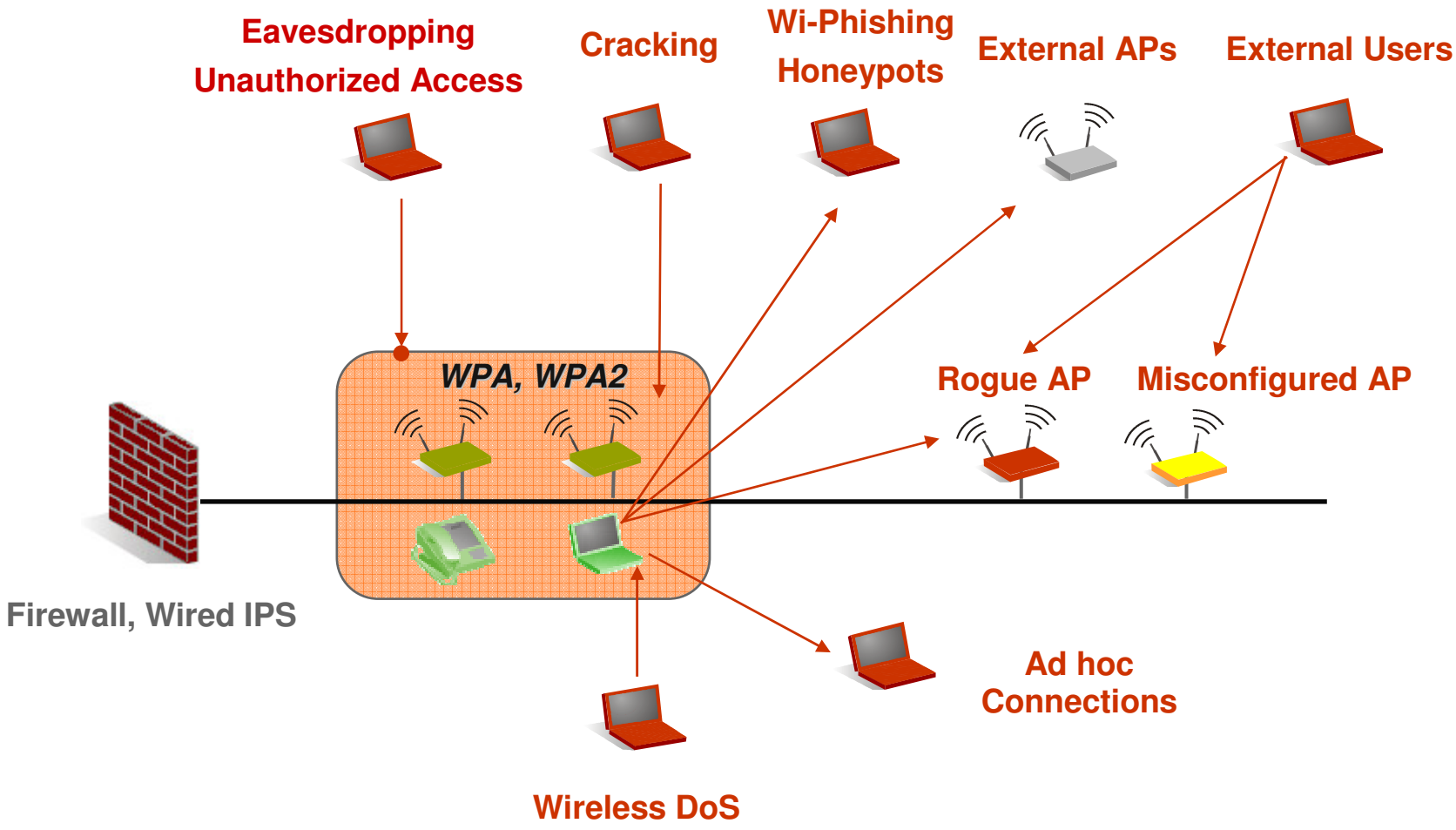
- Even Cisco MFP and 802.11w are vulnerable to DoS attacks
  - See “Autoimmunity disorder in Wireless LANs” http://www.airtightnetworks.com/home/resources/knowledge-center/wlan-self-dos.html

AirTight® NETWORKS

Comprehensive Protection From Wi-Fi Security Vulnerabilities

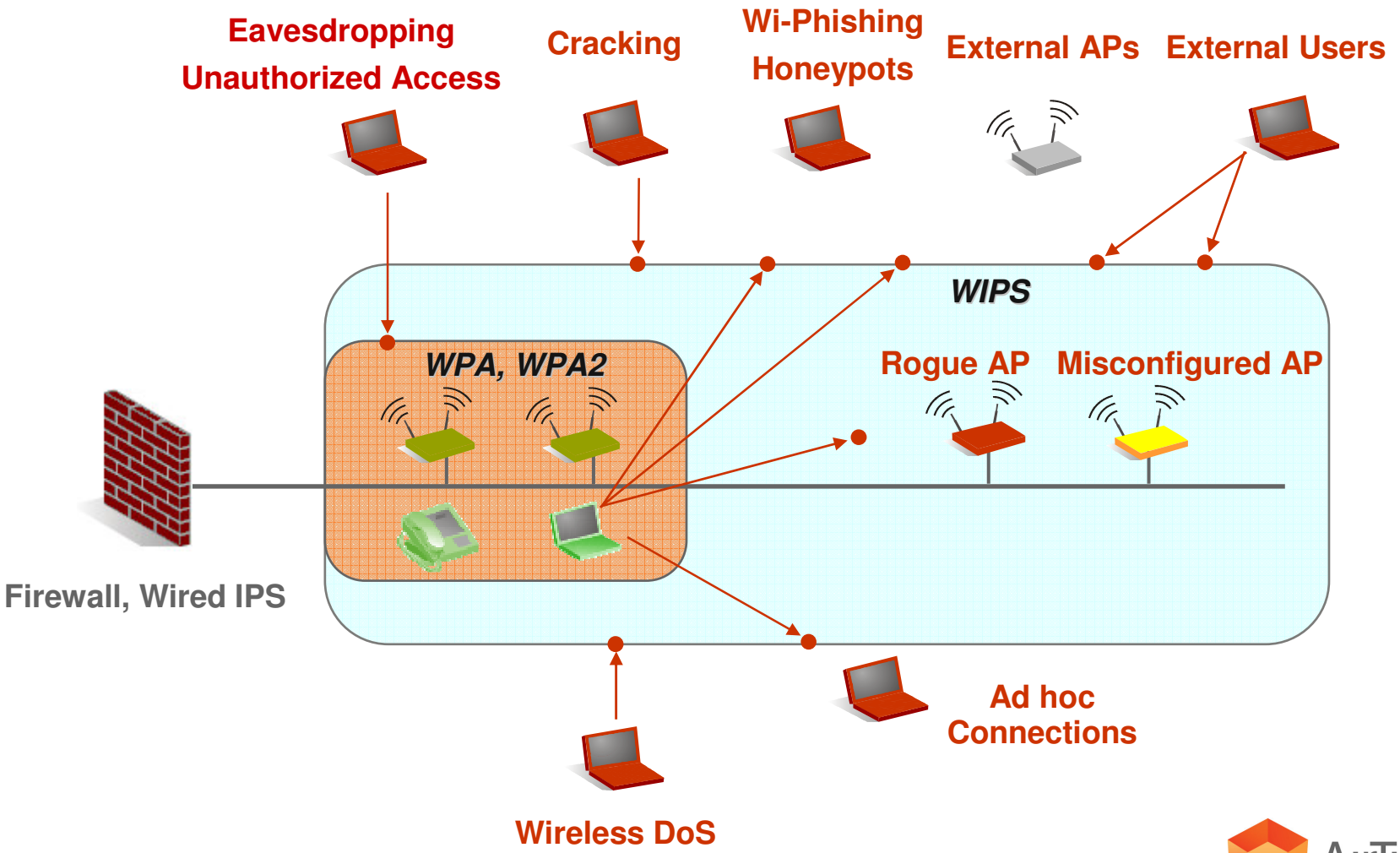
AirTight® NETWORKS

WPA2 is Essential, But Not Enough!
No-WiFi is Also Not Enough!



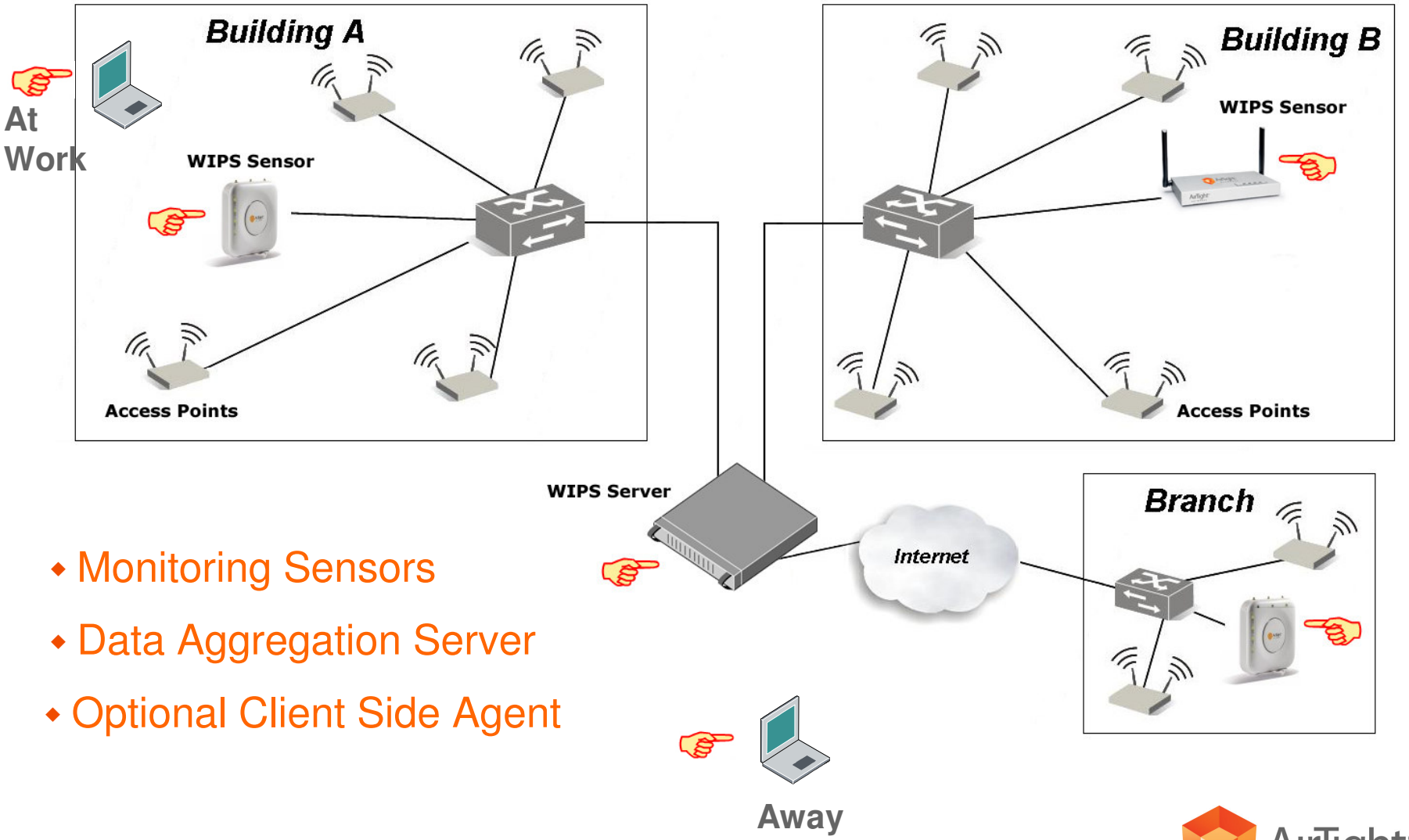
AirTight® NETWORKS

24x7 Comprehensive Protection with Wireless Intrusion Prevention System (WIPS)



AirTight® NETWORKS

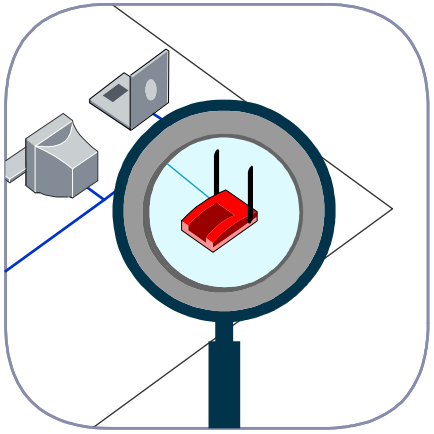
WIPS Components



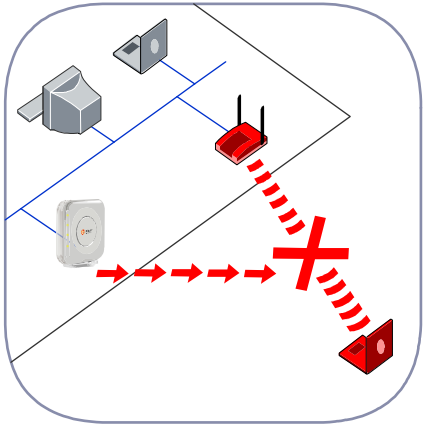
- Monitoring Sensors
- Data Aggregation Server
- Optional Client Side Agent

AirTight® NETWORKS

WIPS Benefits



Detect WiFi Threats and Vulnerabilities



Block WiFi Threats and Vulnerabilities

Locate Threat Posing Devices on Floor

Forensic Information

Compliance Monitoring

Performance Monitoring and Troubleshooting

AirTight® NETWORKS

WIPS Providers In The Market

	RATING		
	Caution	Promising	Positive
AirMagnet			X
AirTight Networks			X
Aruba Networks		X	
Cisco		X	
Motorola (AirDefense)			X

Source: Gartner July 2009

MarketScope for Wireless LAN Intrusion Prevention Systems

AirTight® NETWORKS

Conclusion

- **WiFi warrants new security controls in enterprise networks**
  - For both WiFi and no-WiFi networks
  - Perceived as high priority item today
  - Also a regulatory compliance requirement
- **Strong authentication and encryption (WPA2) is essential for authorized Wi-Fi**
  - Prevents eavesdropping and unauthorized access
- **Another layer of security in the form of WIPS (Wireless Intrusion Prevention System) is essential for comprehensive protection**
  - Prevents rogue APs, ad hoc connections, misassociations, cracking exploits, DoS attacks
  - Compliance monitoring
  - Performance monitoring and troubleshooting as added benefits

AirTight® NETWORKS

For More Information on WiFi Security

www.airtightnetworks.com

- WiFi security knowledge resource
- Real world scans and case studies
- Industry news
- Blog
- Videos
- Best practices
- Security solutions

AirTight® NETWORKS