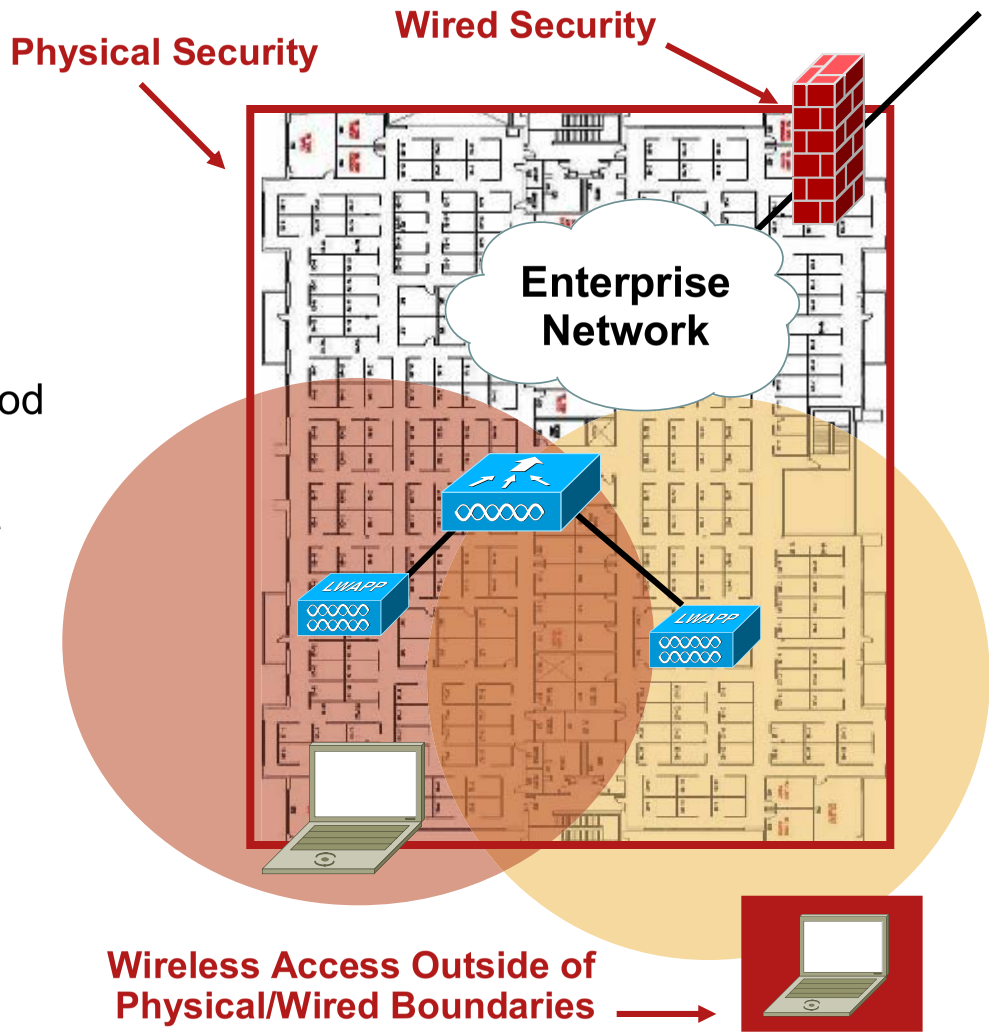
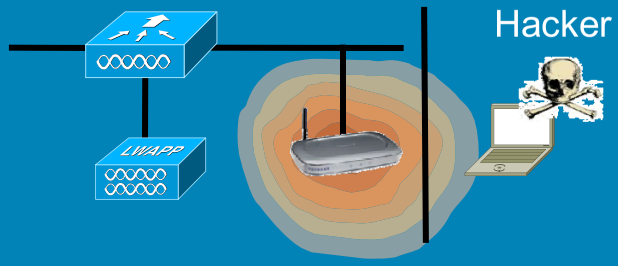
Why Are Wireless LANs Prone to Attack?

- "Open air"
  - No physical barriers to intrusion
  - Silent attacks
- Standard 802.11 protocol
  - Well-documented and understood
  - Most common attacks against WLAN networks are targeted at management frames
- Unlicensed
  - Easy access to inexpensive technology



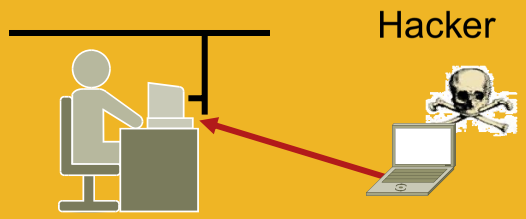
Radio Frequency Based Threats

Rogue Access Points



Employees Unknowingly Create Opening to Enterprise Network

Ad-hoc Wireless Networks

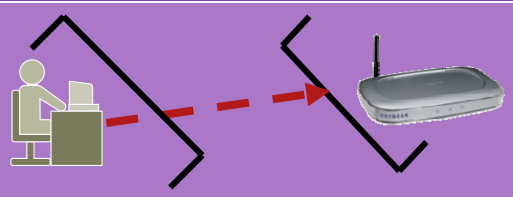


Client-to-Client Connections Bypass Infrastructure Security Checkpoints

Denial of Service Attacks

Malicious Hackers Disrupt Critical Business Services

Client Mis-Association



Employees Connect to an External WLAN, Creating Portal to Enterprise Wired Network

WLAN Security Vulnerabilities and Threats Summary

- Wireless LAN's have become easy targets for both "traditional" network exploits, as well as criminal elements
- Passive SSID probe sniffing and WEP key attacks are just the first stage in WLAN exploits
- More sophisticated WLAN exploits are likely to employ management frames, as most management packets are not encrypted
- If an attacker can gain access to a WLAN, it is possible to launch a variety of higher-layer exploits over this media

The Business Agenda

- Business and security compliance is top-of-mind for executives
- Protecting sensitive business and customer data is the key focus of regulatory compliance requirements

Sarbanes-Oxley	Publicly Traded Companies Must: • Maintain an adequate internal control structure and procedures for financial reporting • Assess the effectiveness of internal control structures
HIPAA	For Patient Information, Firms Must: • Maintain administrative, technical and physical safeguards to ensure integrity and confidentiality • Protect against threats or hazards; unauthorized uses or disclosures
PCI	All Merchants Using Payment Cards, Must: • Build and maintain a secure network • Protect and encrypt cardholder data • Regularly monitor and test networks, including wireless

Business Impact of Lack of Compliance

- Direct financial ramifications
  - FTC fines
  - Compensation payout to customers
  - Cost of external security audits
  - Lost customer confidence
- Research shows substantial indirect costs associated with brand damage
- "The fall in share price attributed to a security incident is estimated at 2.7% over one day, increasing to 4.7% over three days"*

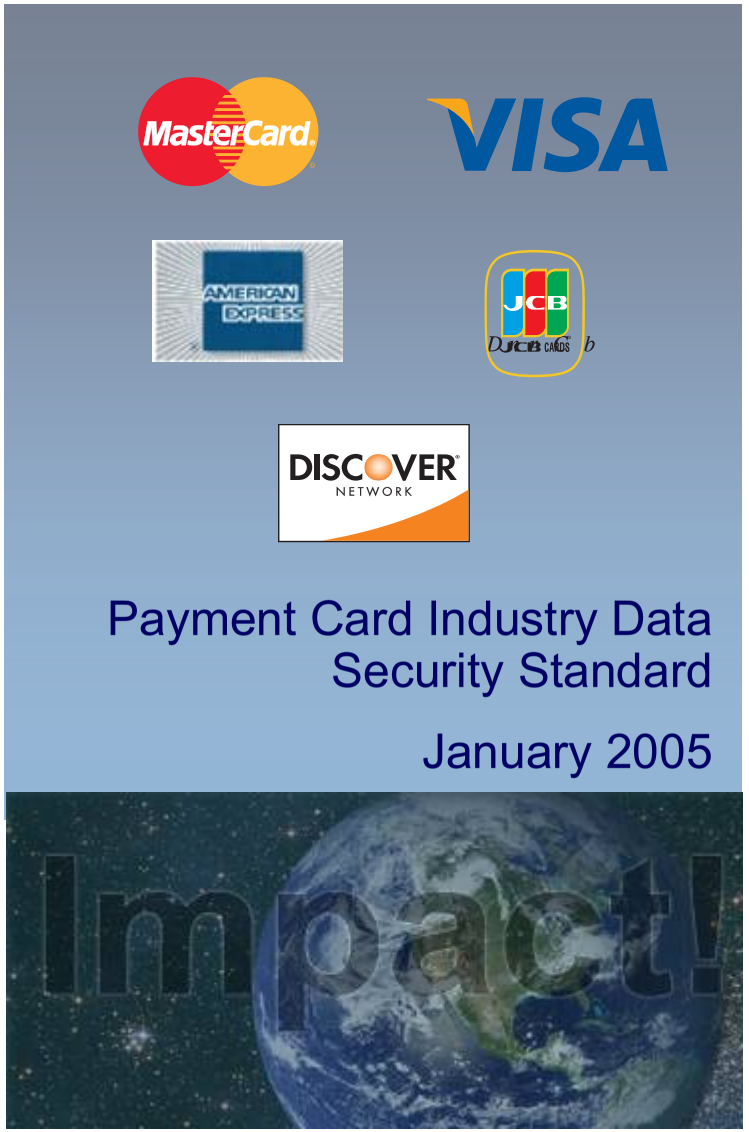
*Source: "The Financial Impact of IT Security Breaches: What Do Investors Think?" Information Systems Security, 2003

Case Study

- Company: Large retailer
- Issue: Data breach due to poor wireless security
- Ramifications:
  - 20 years of third-party security audits mandated by FTC
  - Compromise of 1.4 million credit cards and 96,000 checking accounts
  - Company losses related to security breach ranged from $6.5m to $9.5m

The PCI Data Security Standard

- Published January 2005, ver. 1.1 released Sept 7, 2006
- Impacts **all** who
  - Process
  - Transmit
  - Store: cardholder data
- Developed by MasterCard and Visa, endorsed by other brands
- Global reach (AIS* regulation outside of US)

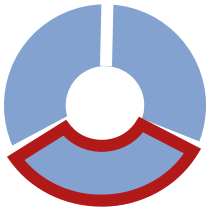


*Account Information Security
http://www.cisco.com/go/compliance

Mapping Wireless Security to PCI

Wireless Security Tools for PCI Compliance	
Build and Maintain a Secure Network	• Change default settings Best Practice: No default SSIDs, disable broadcast No default login passwords for wireless management
Protect Cardholder Data	• Encrypt wireless data in transit Best Practice: WPA or WPA2 (uses TKIP and AES) VPNs for remote access, host intrusion prevention
Maintain a Vulnerability Management Program	• Deploy wireless Network Admission Control for client posture • Use CSA for host based intrusion detection • Integrate wired and wireless IPS/IDS
Implement Strong Access Control Measures	• Authenticate wireless users and devices—802.1X • Deploy wireless NAC for client posture assessment Best Practice: NAC with 802.1X for Single Sign On
Regularly Monitor and Test Networks	• Deploy monitoring to secure and control the wireless domain Best Practice: Integrated 24/7 RF monitoring
Maintain an Information Security Policy	• Ensure wireless LANs are included in security policy • Enforce consistent information security policy using NAC

Client Validation and Posture Assessment



Business Challenge

Identify Who Is on the Network and Enforce Granular Policies to Prevent Exposure to Viruses and "Malware"

- Ensures wireless client is 'up-to-date' with latest security policies
- Quarantines and fixes any wireless client that is non-compliant
- Enforces differentiated policies and network services based on user role
- Products:
  - NAC Appliance
  - WLAN Controller

Authenticate and Authorize

- Enforces authorization policies and privileges

Scan and Evaluate

- Agent and network scan for required versions and infections

Quarantine and Enforce

- Isolate non-compliant devices from rest of network

Update and Remediate

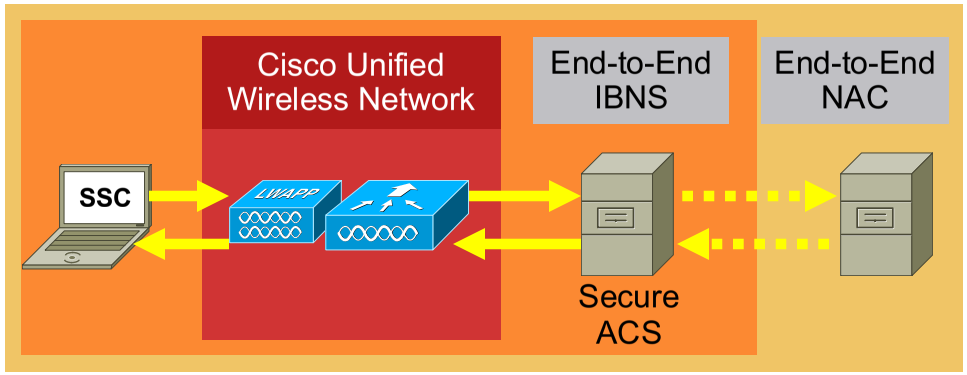
- Network-based tools for remediation of threats and vulnerabilities

Simple, Secure Client Connectivity

Business Challenge

Deploying and Managing a Common Security Profile Across an Increasingly Diverse Array of Wireless Clients

- A single 802.1X authentication supplicant for wired and wireless devices
  - Simplified management
  - Improved security
  - Lower total cost of ownership (TCO)
- Encryption of management frames
- Products:
  - Cisco Secure Services Client
  - Cisco Secure ACS
  - Cisco Compatible Extensions



- ✓ Management Frame Protection
- ✓ Fast Secure Roaming
- ✓ LEAP and EAP-FAST

Wireless Security Management

Business Challenge

Supporting and Maintaining a Diverse Range of Security Products, Correlating Events and Delivering Concise Reporting

- WCS offers central, one-touch configuration and management of wireless security profiles
- Security alerts are located and viewed graphically
- CS-MARS allows quick response with incident capture and event correlation for security alarms
- Products:
  - CS-MARS
  - WCS