Entrust
Securing the Internet

How can you bring Trust and Security to Wireless LAN solutions?

November 2002

Entrust
Securing the Internet

Today's Topics

- Entrust Introduction
- Brief overview of the 802.11b technology/security
- Top vulnerabilities
- Analysis and attack tools
- Entrust & Cisco – delivering a Secure Wireless LAN
- Q & A

Relied on to Secure an Internet World

- First mover in Internet security:
  - PKI (1994)
  - PMI - Portal Access (1997)
  - Wireless (1999)
  - Enhanced Internet Security (2001)
- 90+ patents granted or pending
- #1 market share in PKI software globally*
- Top 3 in Authorization globally*

Broadest Portfolio in the Industry

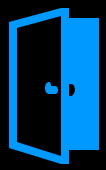
*Source: IDC, Gartner / Dataquest

Entrust
Securing the Internet

Trusted Transactions Require…

Enhanced Security Services

Identification → **Protecting** and **Authenticating** Identity used in Transactions



Entitlements → Providing **Personalized** Access and Authorization to Transactions

Privacy → Enforcing **Privacy** of Transaction Information

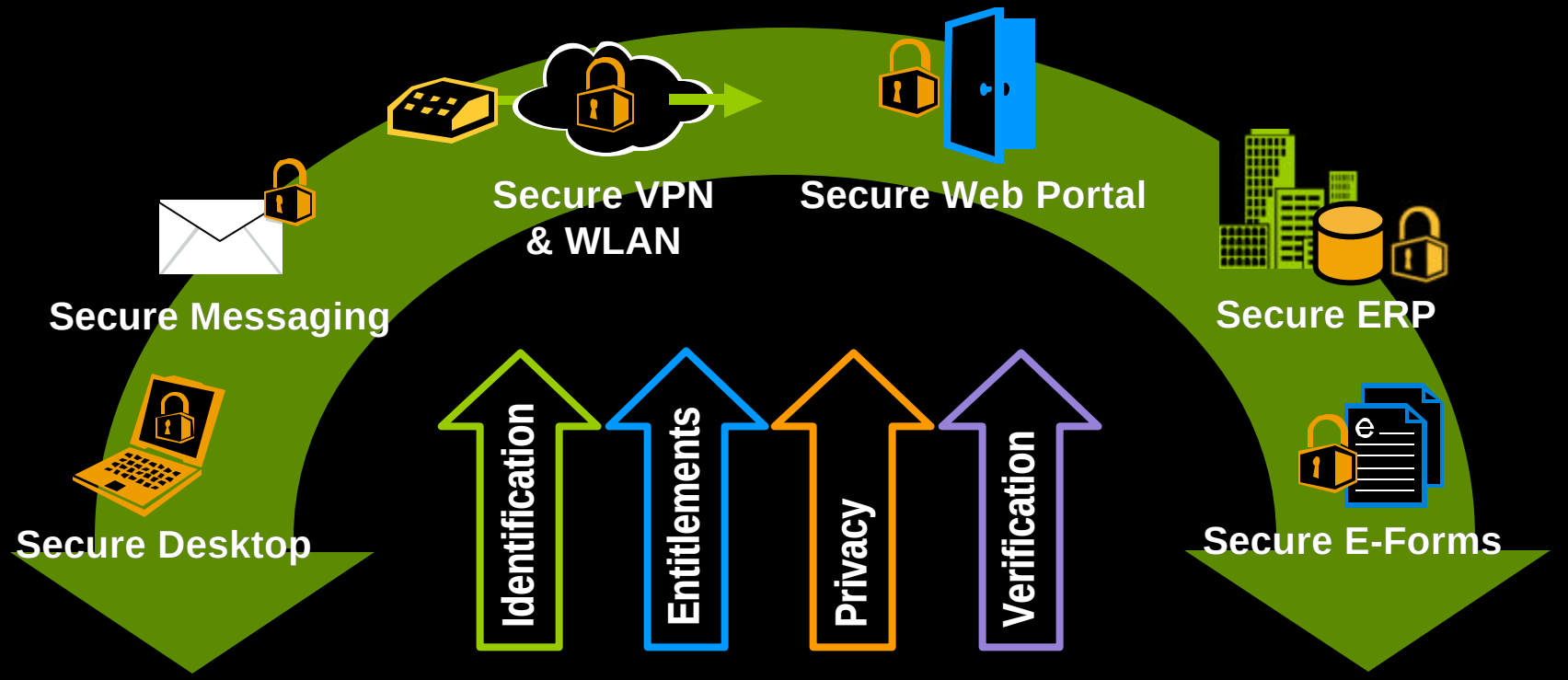
Verification → Ensuring Transactions are **Binding** and **Auditable**

… and

Security Management

Broad Range of Solutions

- Entrust has worked with industry leaders to integrate enhanced security services and deliver solutions that enable business return



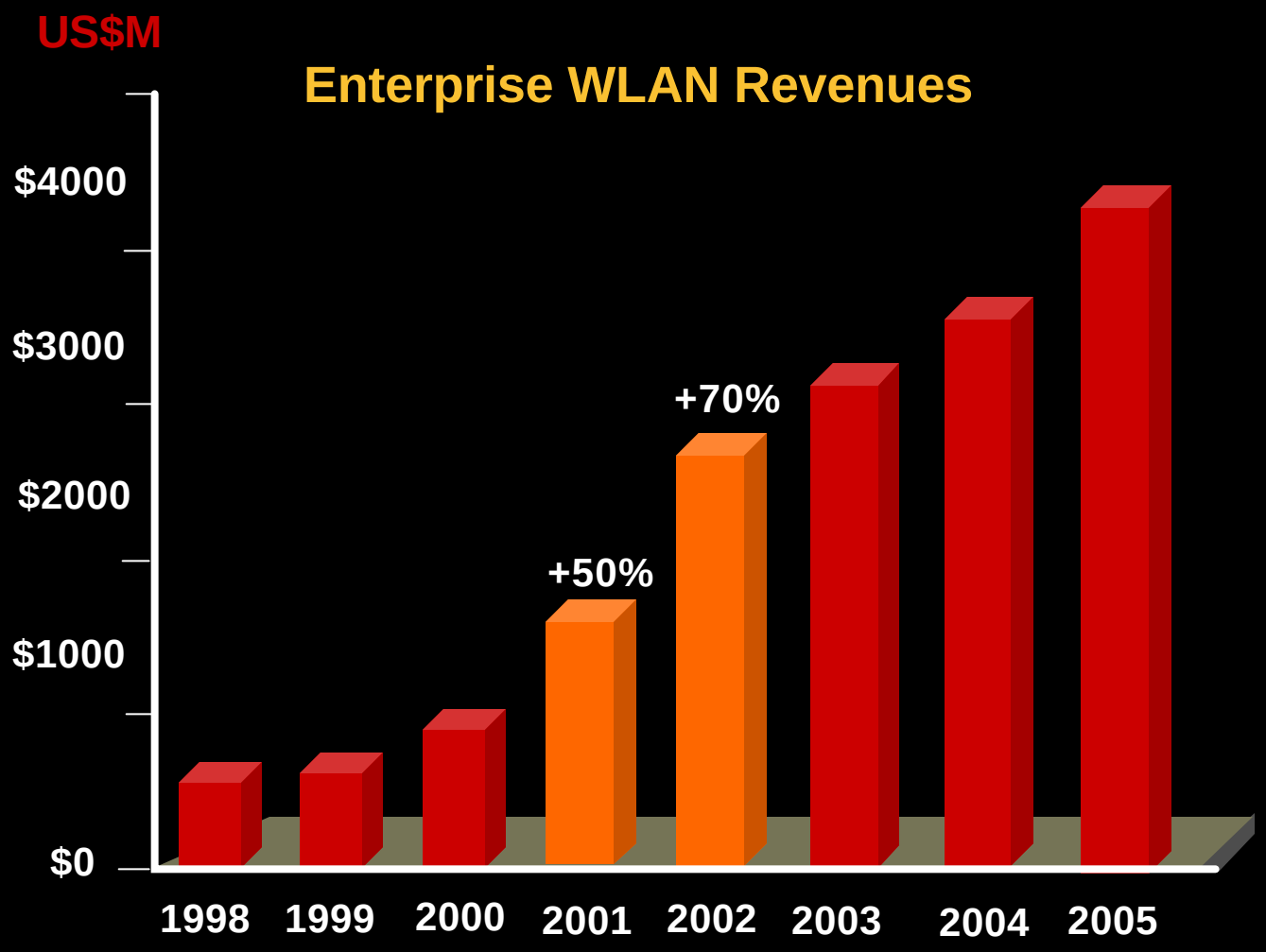
Entrust
Securing the Internet

Cisco & Entrust

- Partnered to deploy highly secure VPN and WLAN environments
- Combine enhanced security from Entrust w/ Cisco VPN/WLAN products
  - Use Entrust PKI & certificates for IPSec authentication
- Product integration:
  - Cisco provides VPN/WLAN software & hardware
  - Entrust provides PKI & certificate management software
- Product interoperability

Wireless LAN Revenue

Entrust
Securing the Internet



Source: Cahners In-Stat Group, 2001

Benefits of Wireless

Entrust
Securing the Internet

Productivity Gains

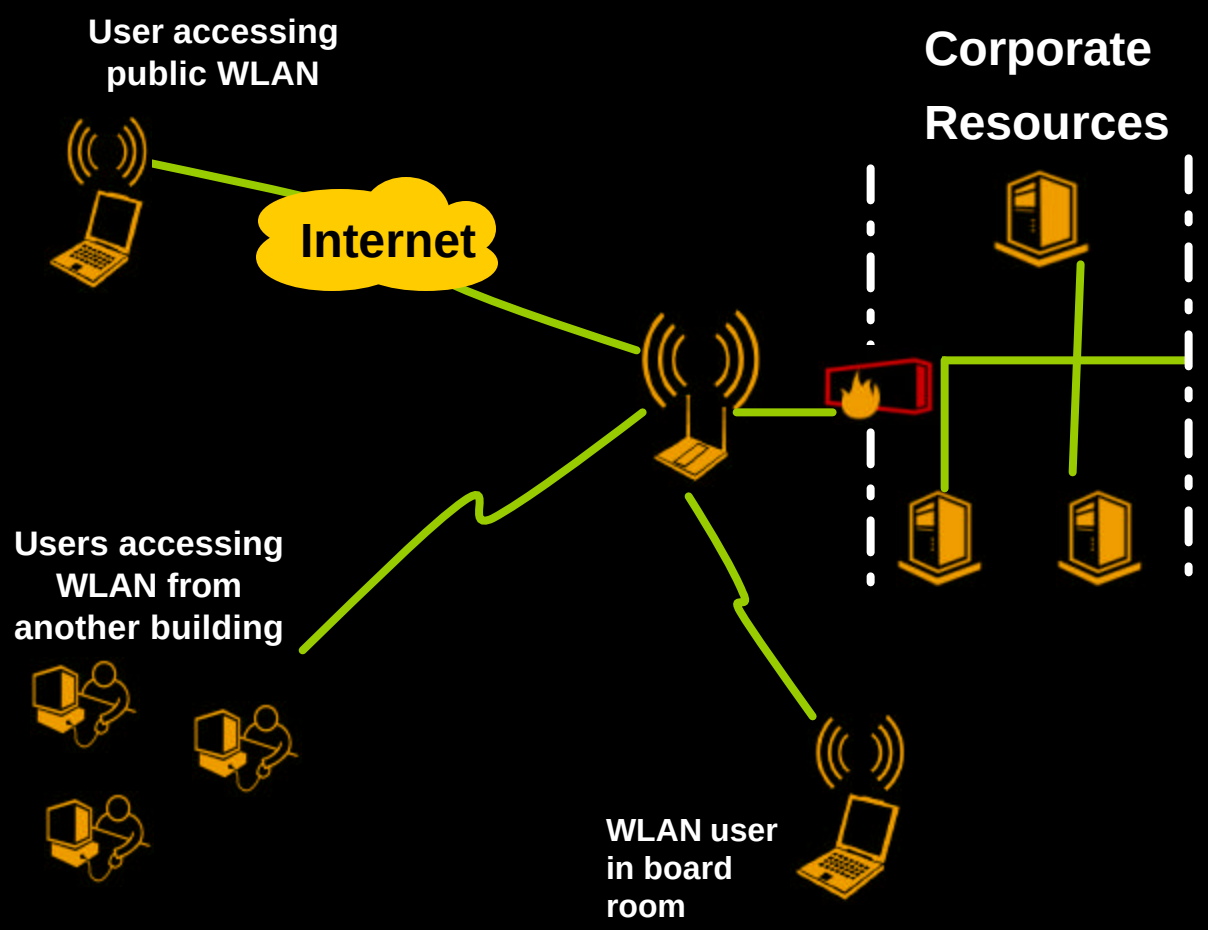
- access to real time information anywhere
- users stay connected longer

Increased Flexibility

- go where wire cannot
- access to all corporate resources anytime, anywhere

Cost Effective

- versus dedicated lines
- great ROI
- low TCO



NOP Study – Wireless LANs Increase Productivity

Entrust
Securing the Internet

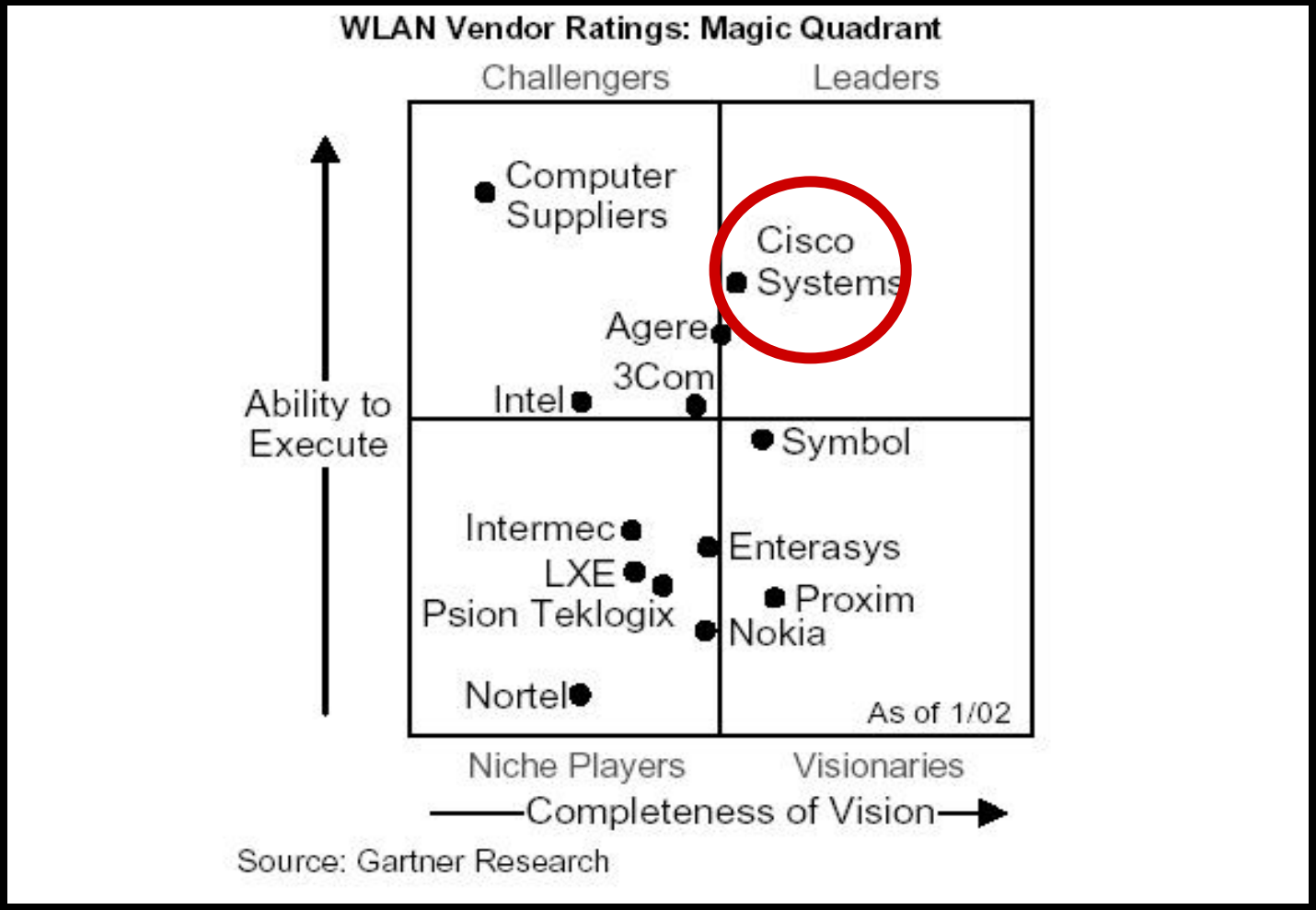
Based on a survey of 300+ U.S.-based organizations with more than 100 employees:

- End users stayed connected an average of 1¾ hours more per day to their corporate network
- Average daily time savings: 70 minutes
- Productivity: +22%

Source: NOP World-Technology, Sept. 2001

Entrust
Securing the Internet

WLAN Vendor Ratings



(From Gartner "Wireless LAN Vendor Evaluation and Magic Quadrant," 24 January 2002)

Entrust
Securing the Internet

The reality

"30% of enterprises will

suffer serious exposures from deploying WLANs

without implementing the proper security."

- Gartner 2002

"The greatest security threat
to businesses over the next 12 months will not
be from viruses, outside hackers
penetrating defenses, denial of service,
or inside jobs. It will be the

loss of trust and brand equity."

—Hurwitz Group

Entrust
Securing the Internet

Enhanced Security + 802.11b

John Pavelich
Senior Security Architect
Entrust

Entrust
Securing the Internet

Wireless LAN Technologies

	802.11b	802.11a	802.11g
Frequency Band	2.4 GHz	5 GHz	2.4 GHz
Availability	Worldwide	US/AP	Worldwide
Maximum Data Rate	11 Mbps	54 Mbps	54 Mbps

Source: Entrust & Cisco; Securing the Enterprise WLAN Webinar, July 2002

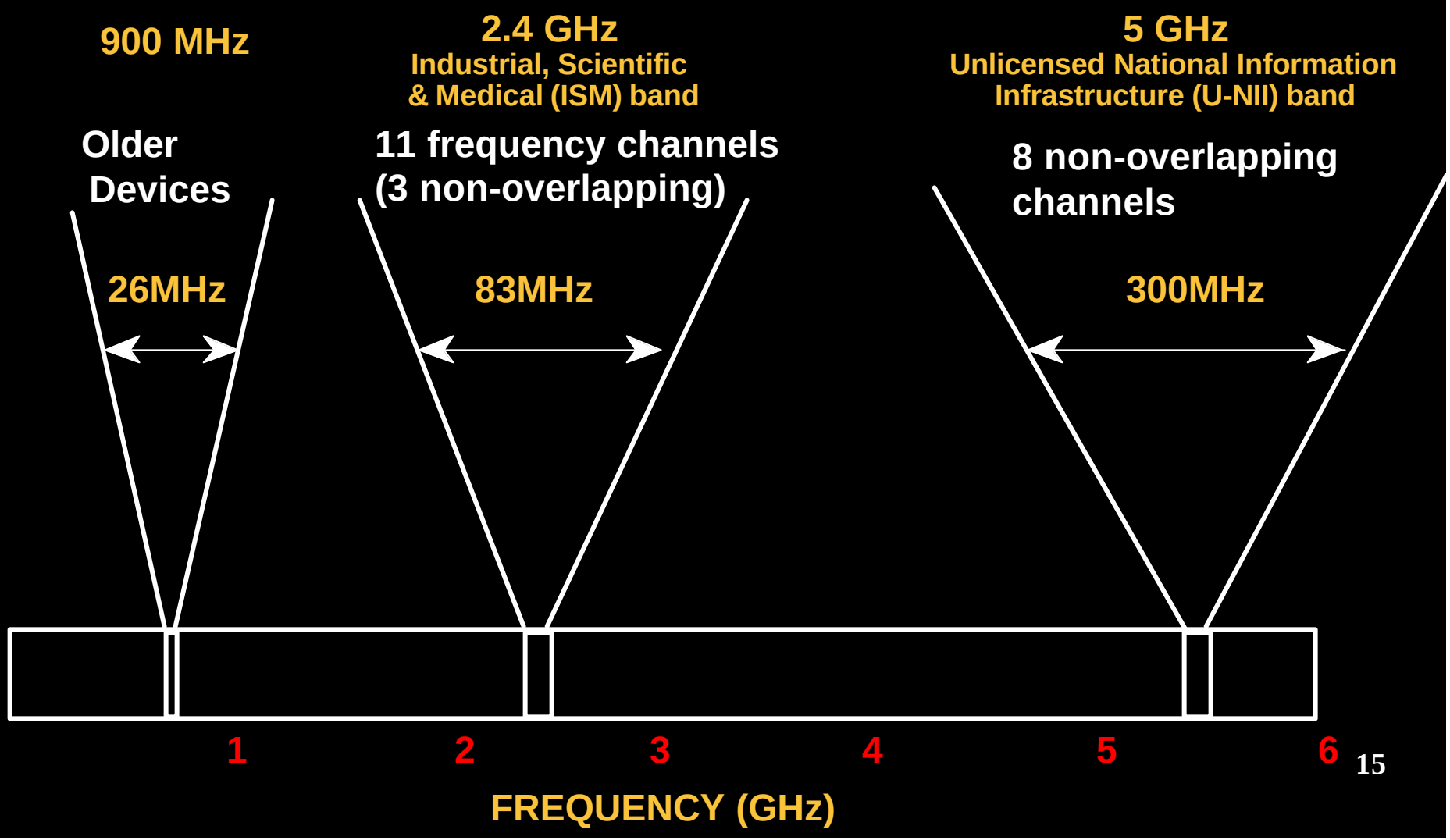
PHY Details: 802.11b, a and g

Entrust
Securing the Internet

	802.11b	802.11a	802.11g
Modulation Technique	DSSS	OFDM	OFDM
Operating Frequencies	2.4GHz	5GHz	2.4GHz
Maximum Throughput	11Mbps	54Mbps	22Mbps
Ratified Standard	Yes	Yes	No

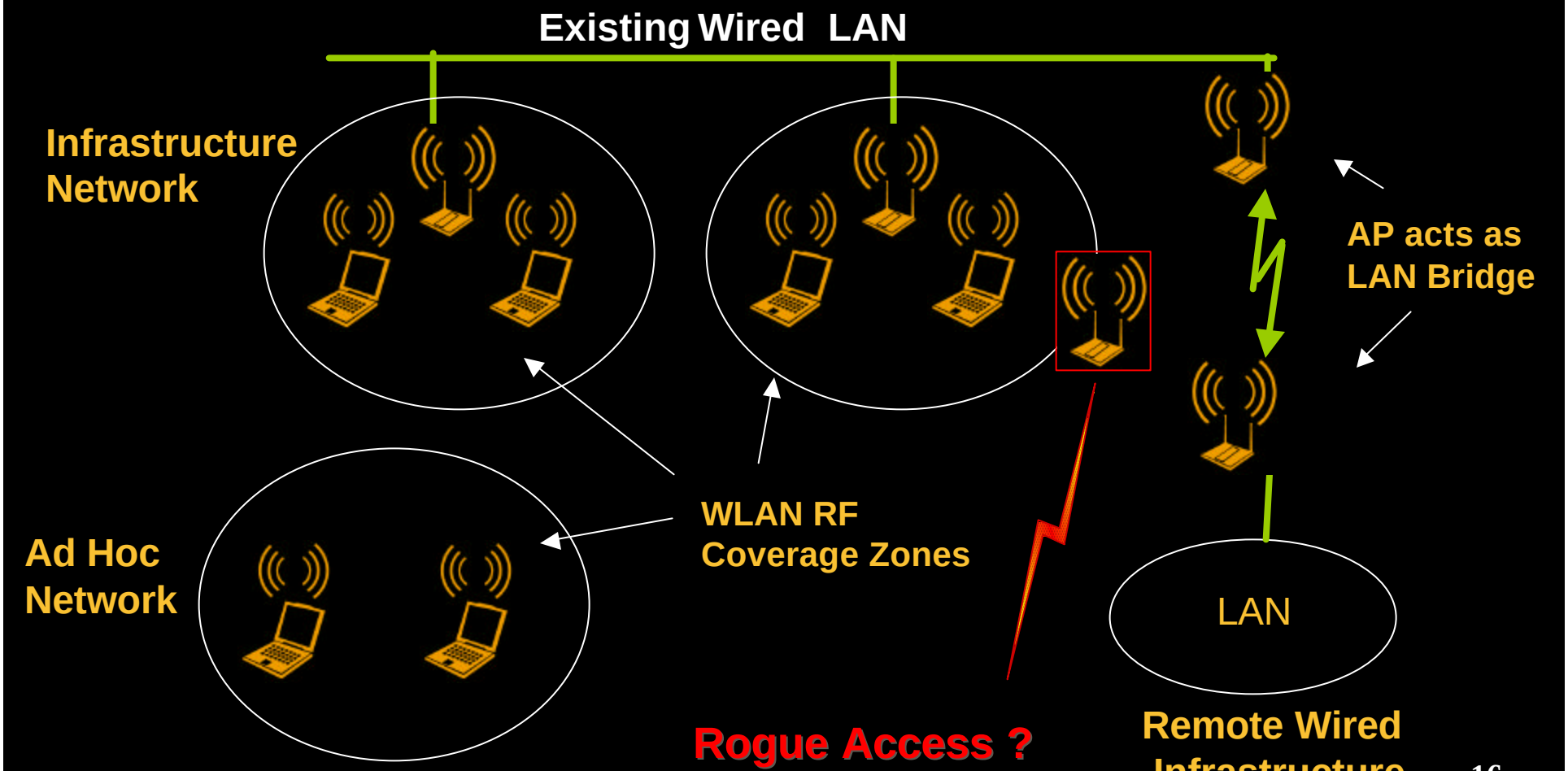
Entrust
Securing the Internet

Frequency Bands



Entrust
Securing the Internet

Basic WLAN Architecture



Entrust
Securing the Internet

WLAN Trends

- Cost of wireless technology decreasing
- Use is rapidly increasing ~ 73% expected growth this year
- Entering more 'sensitive' operational environments
- Training, certification and 'good' information is limited
- Information overload!

Entrust
Securing the Internet

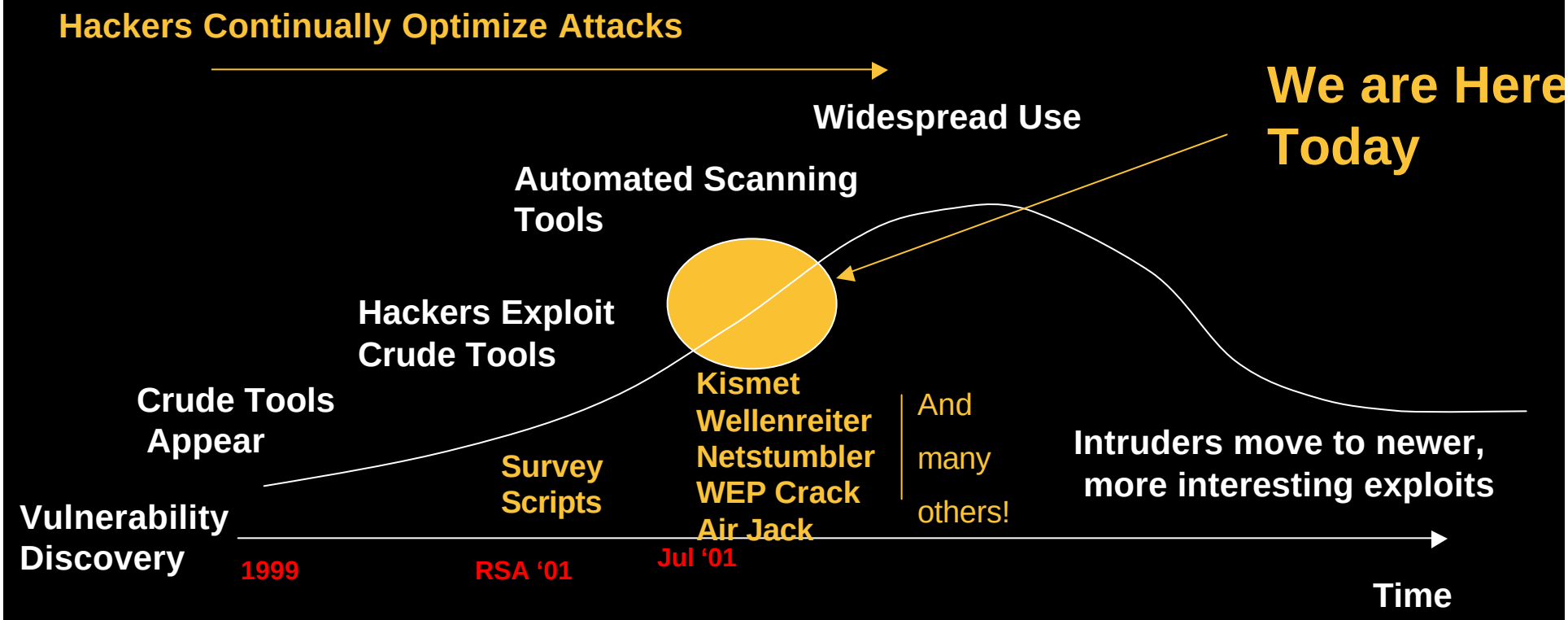
(Some) WLAN Security Issues

Default setups:	Work well, but are not secure
WEP:	Broken at any key length
AP Technology:	Many flawed implementations
Rogue APs:	Impact security of wired network
RF Propagation:	Extends network environment beyond the walls
New Attacks:	Radio protocol attacks are nasty (ECM)
Safeguards:	Poorly architected/implemented
Policy:	Monitoring, updating and enforcement
Newness:	Confusion, lots of attacks and variants

HOW DO WE ANALYZE WLAN SECURITY?

Entrust
Securing the Internet

Intruder/Safeguard Cycle



Basic Safeguards Inherent in Technology

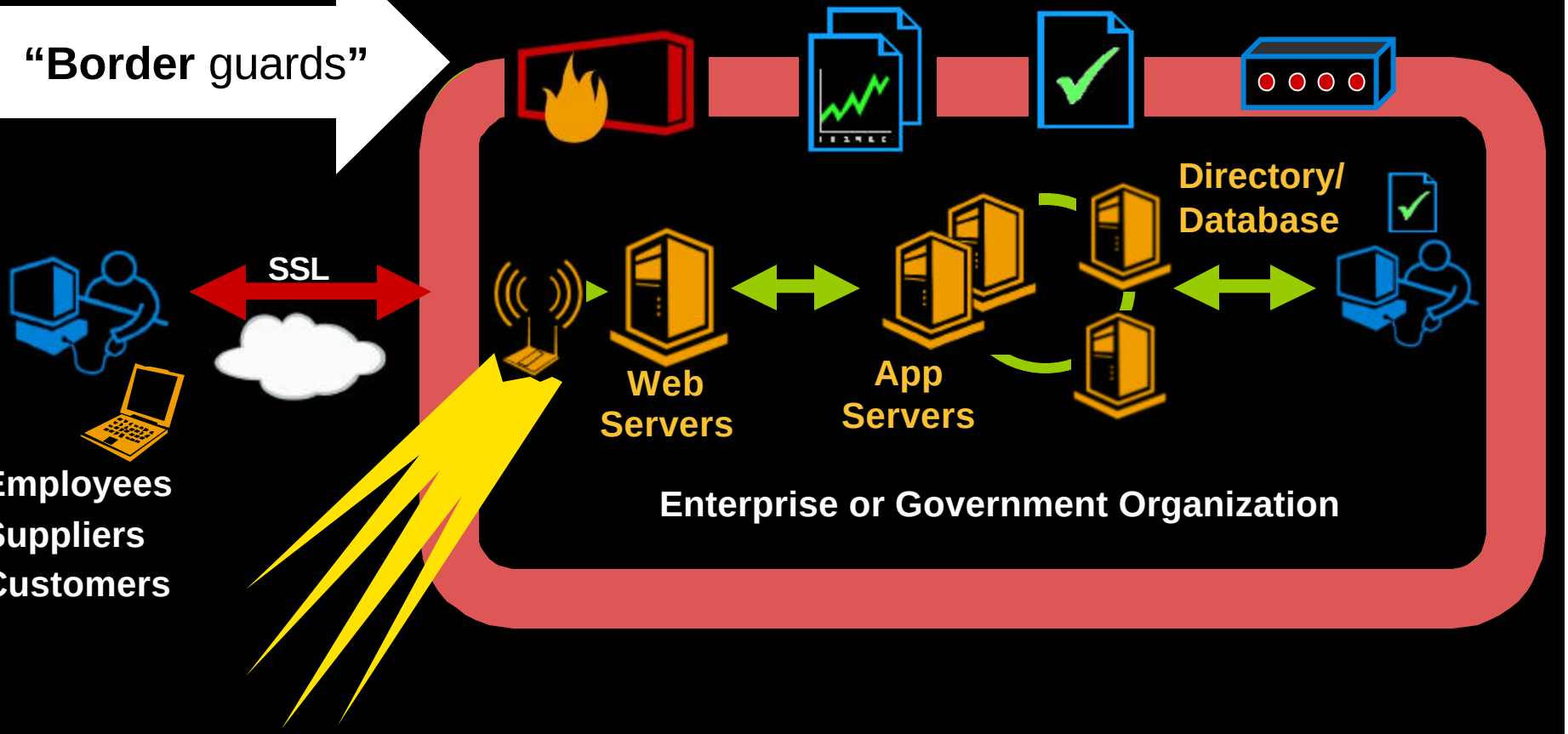
Better Safeguards Appear

Safeguards Mature, Attackers move on
Legacy Systems Still Vulnerable!

By Default, Wireless Breaches the Perimeter!

Entrust
Securing the Internet

"**Border** guards"



Entrust
Securing the Internet

Typical Attacks

NetStumbler + Utilities ~ War Driving 'Cultism'

Publicized vulnerabilities ~ War Chalking

WEP ~ Passive attacks (AirSnort) getting better

Passive network scans on wireless side ~ Kismet

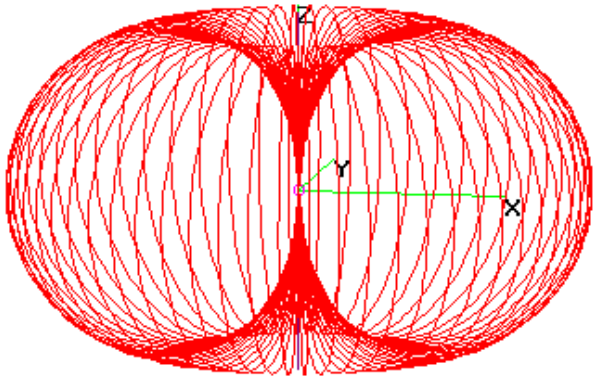
AP port and protocol scanning and probing

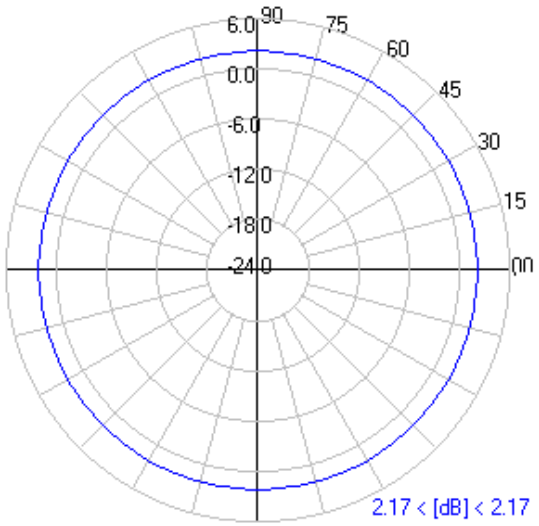
AirJack engine: Client, MITM and DoS attacks

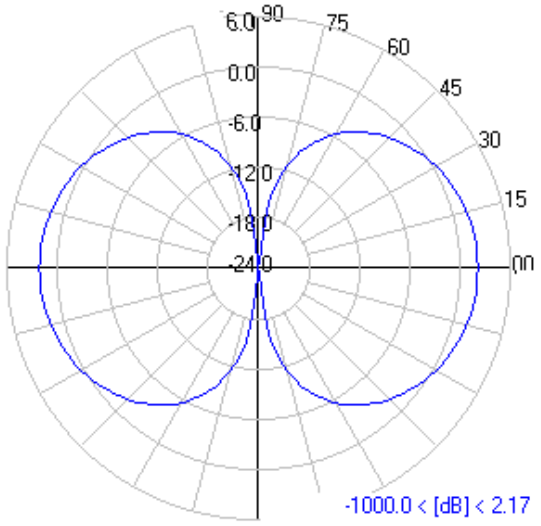
Honey Pot experience: Opportunity attacks and dedicated attacks

Entrust
Securing the Internet

Dispelling Misinformation





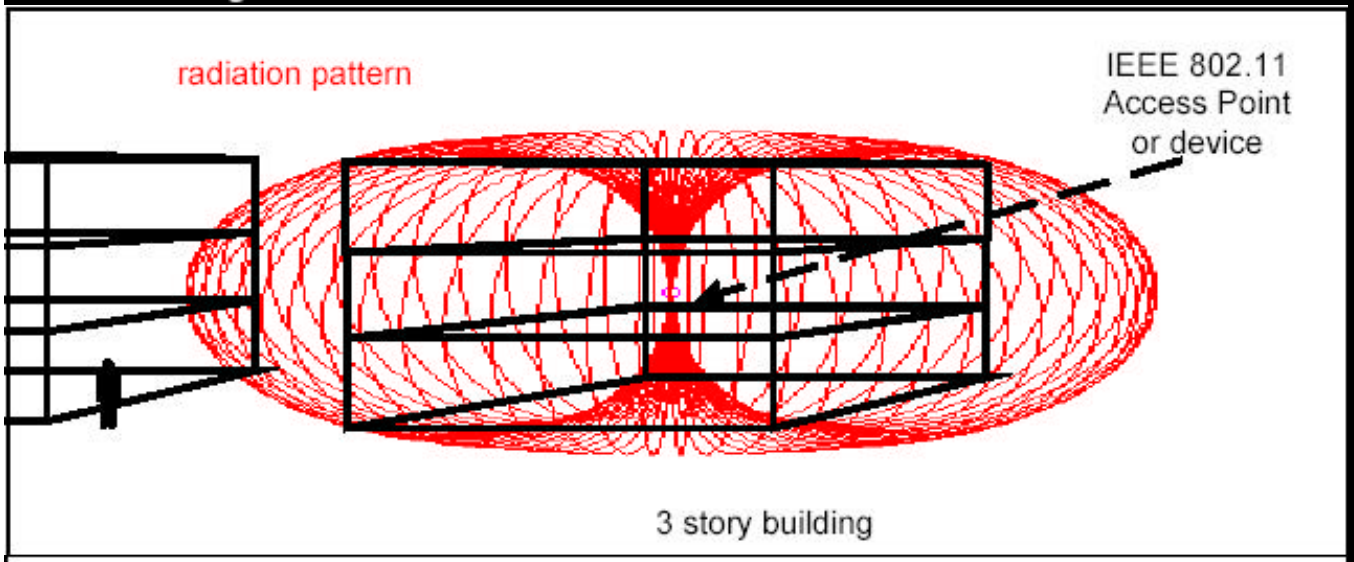


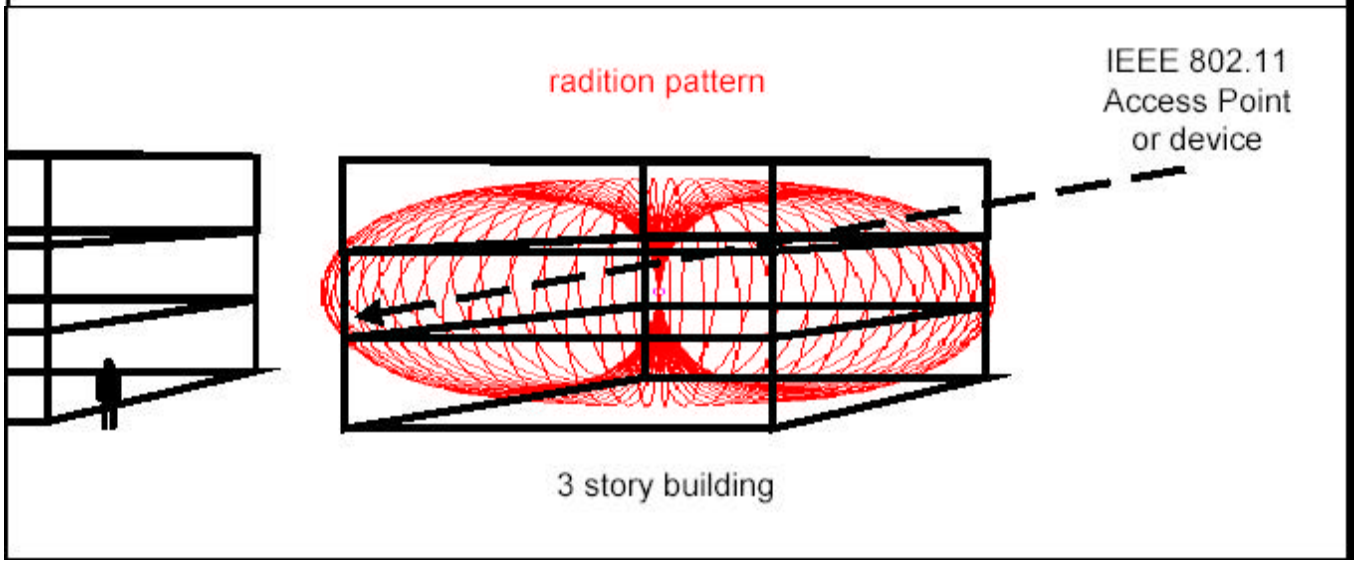
Security With Antennas?

Textbook radiation patterns of the AP isotropic monopole antenna

Entrust
Securing the Internet

Engineering Theory

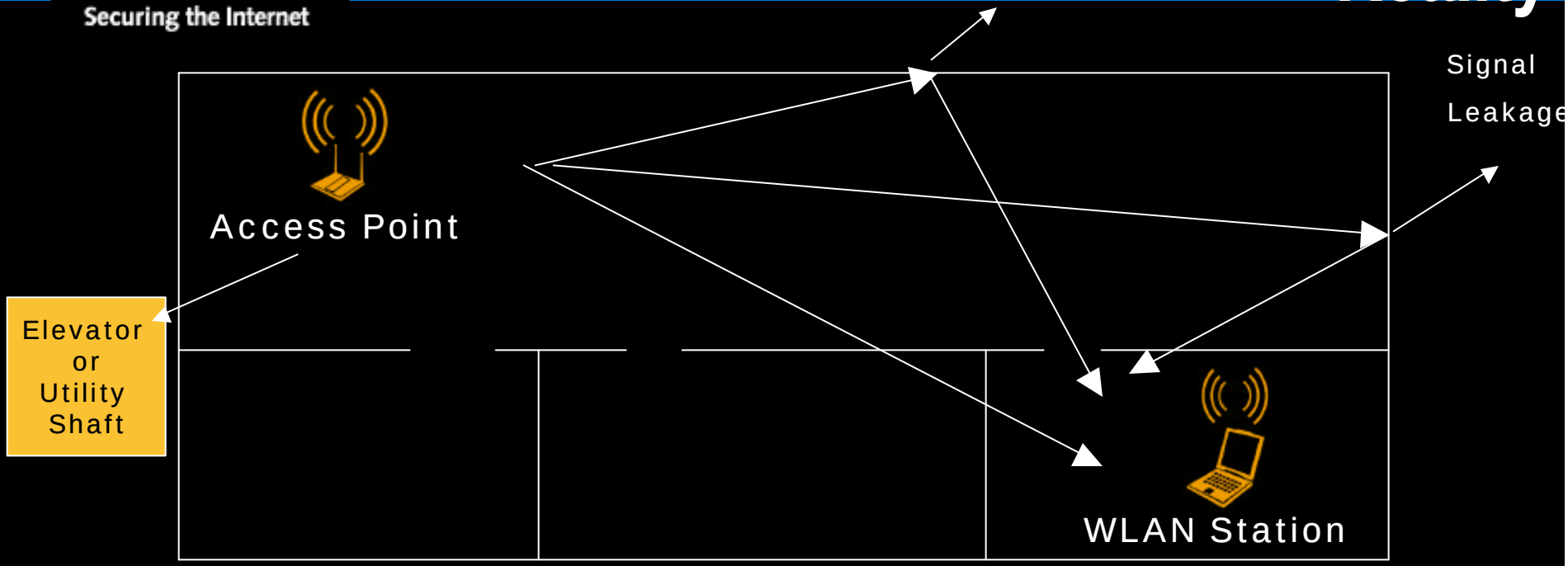




'Experts' say you can 'place the antenna' to get 'better security' and 'control the perimeter'

Entrust
Securing the Internet

Reality



Indoor Propagation in a Typical Crowded Office Building:

- **Reflections**
- **Re-Radiation**
- **Attenuation**
- **Un-intentional waveguide structures**
- **Not a 'perfect' environment**

Entrust
Securing the Internet

More Reality: The dB Factor!

Attenuation Factors in Office Buildings

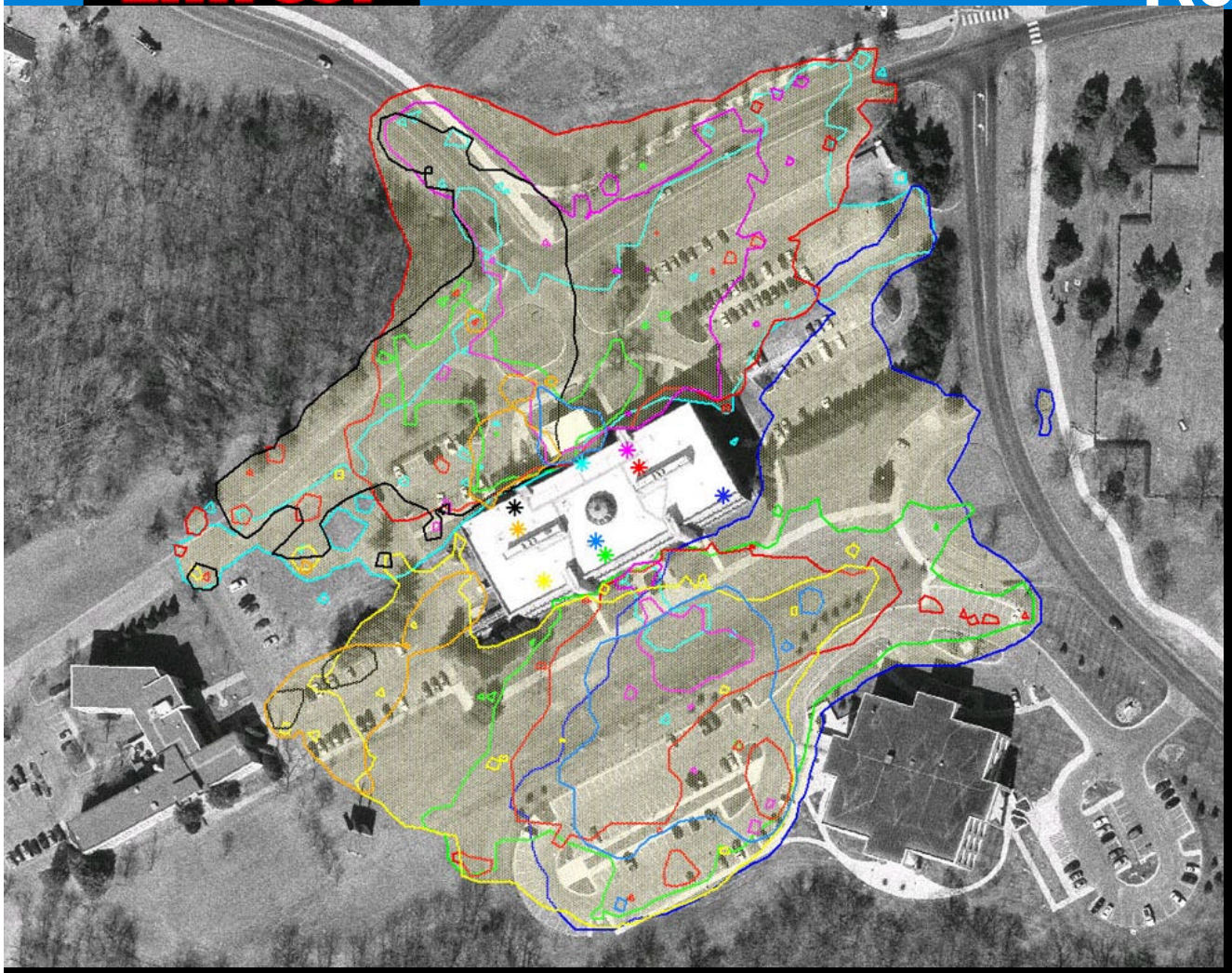
- **Window Non-Metallic Tint ~ 3dB**
- **Window Metallic Tint ~ 7dB**
- **Drywall ~ 7dB**
- **Wood Wall ~ 10dB**
- **Heavy Wall(6 inch) ~ 15dB**
- **Heavy Wall(12 inch) ~ 25dB**

Low Attenuation Permits Leakage!

Source: Fluke Networks

Entrust

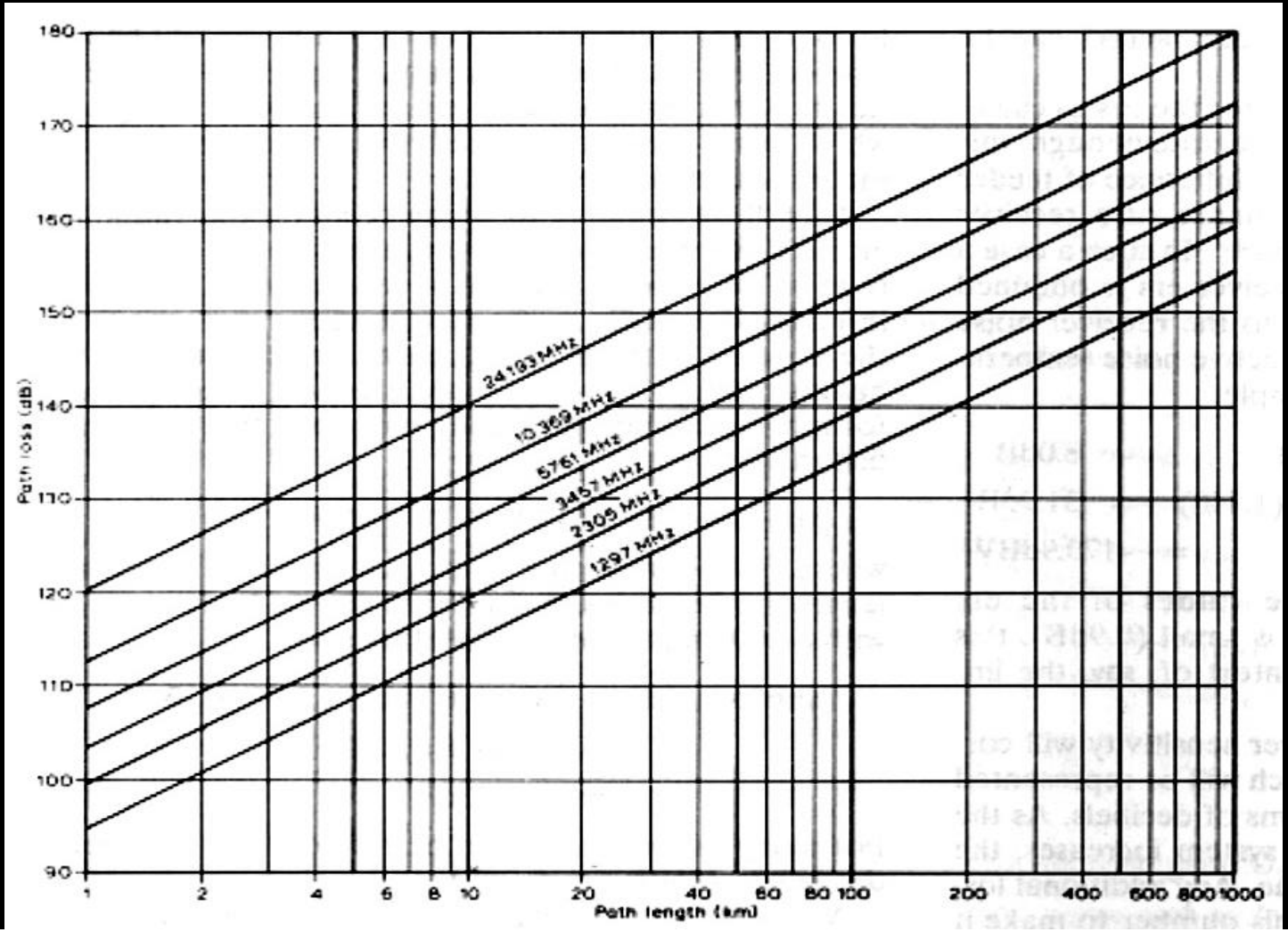
Reality in Practice



There are limits to what you can achieve with directional antennas, site surveys are needed if local physical environment requires it

Entrust
Securing the Internet

Why Reality is Important



Each ~6db improvement at 2.4 GHz doubles your intercept range

Entrust
Securing the Internet

Add Some Antenna Gain

Typical 2.4 GHz WLAN AP has mono-pole antennas with 0dBi gain.

A Low Profile patch antenna can provide 8 dBi gain at 2.4 GHz and costs about $65 US

Entrust
Securing the Internet

~12 dB gain,
+/- 2000
calorie
Yagi antenna
$3.29 + GST

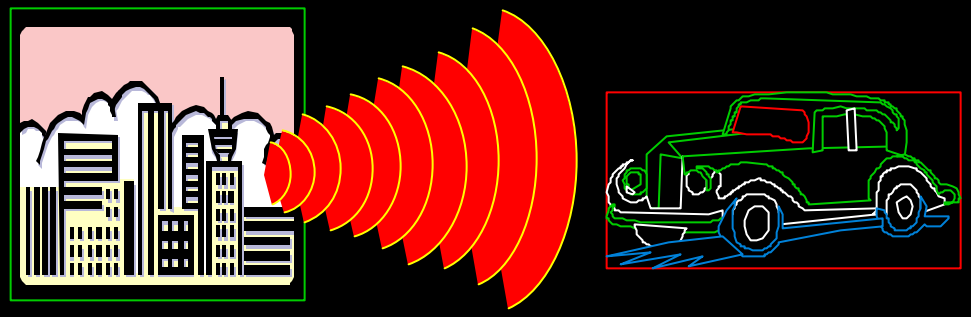
Entrust
Securing the Internet

The Result is Effective War Driving

Un-Protected WLANs are proliferating providing a 'target rich' environment for the attacker

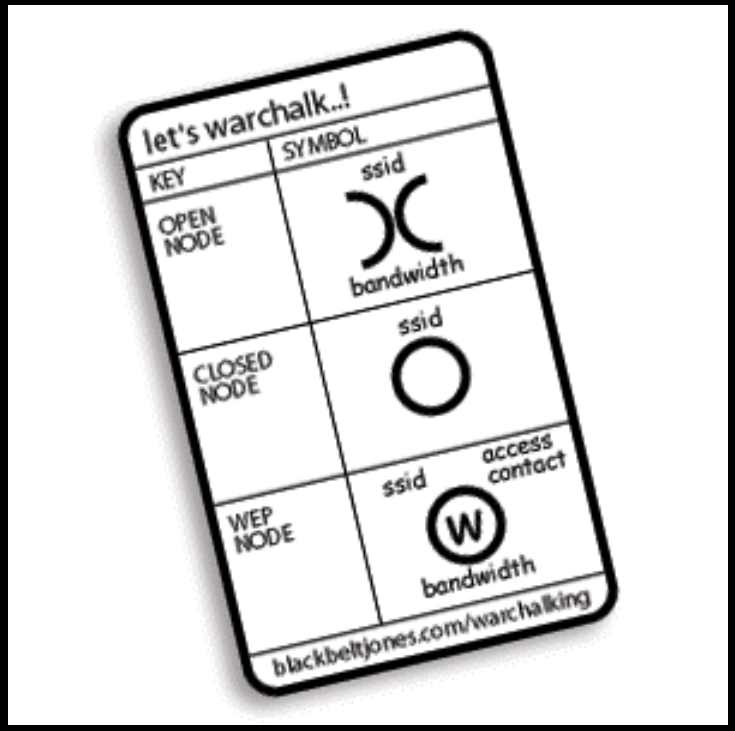
The War Driver is really doing a survey of AP's with default or poor security settings

Using network and wireless hacking tools he can get on the network from the wireless side and mount other attacks



Entrust
Securing the Internet

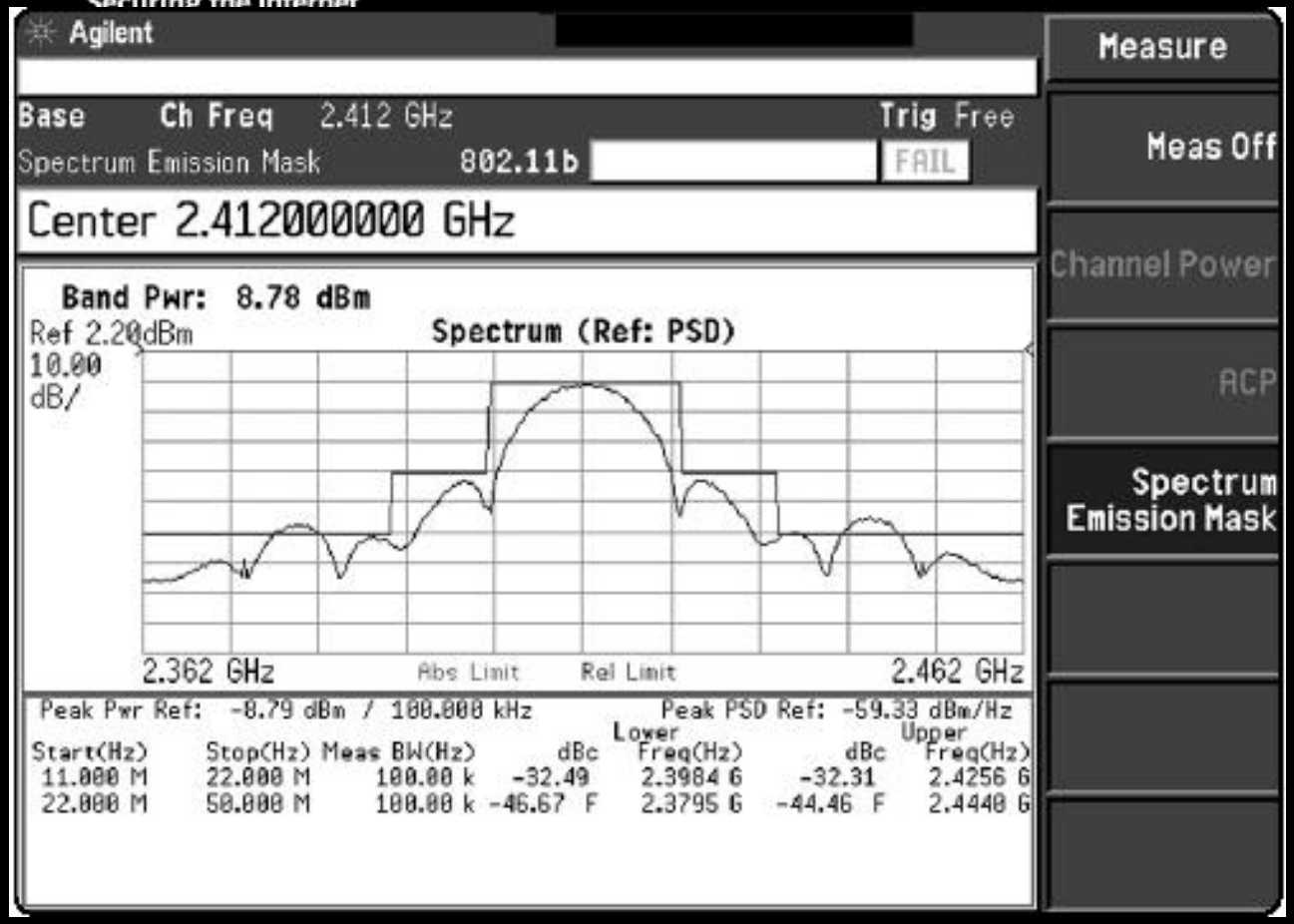
War Driver's Results



Has your building been chalked?

How to Assess Your Susceptibility to War Driving

Entrust
Securing the Internet

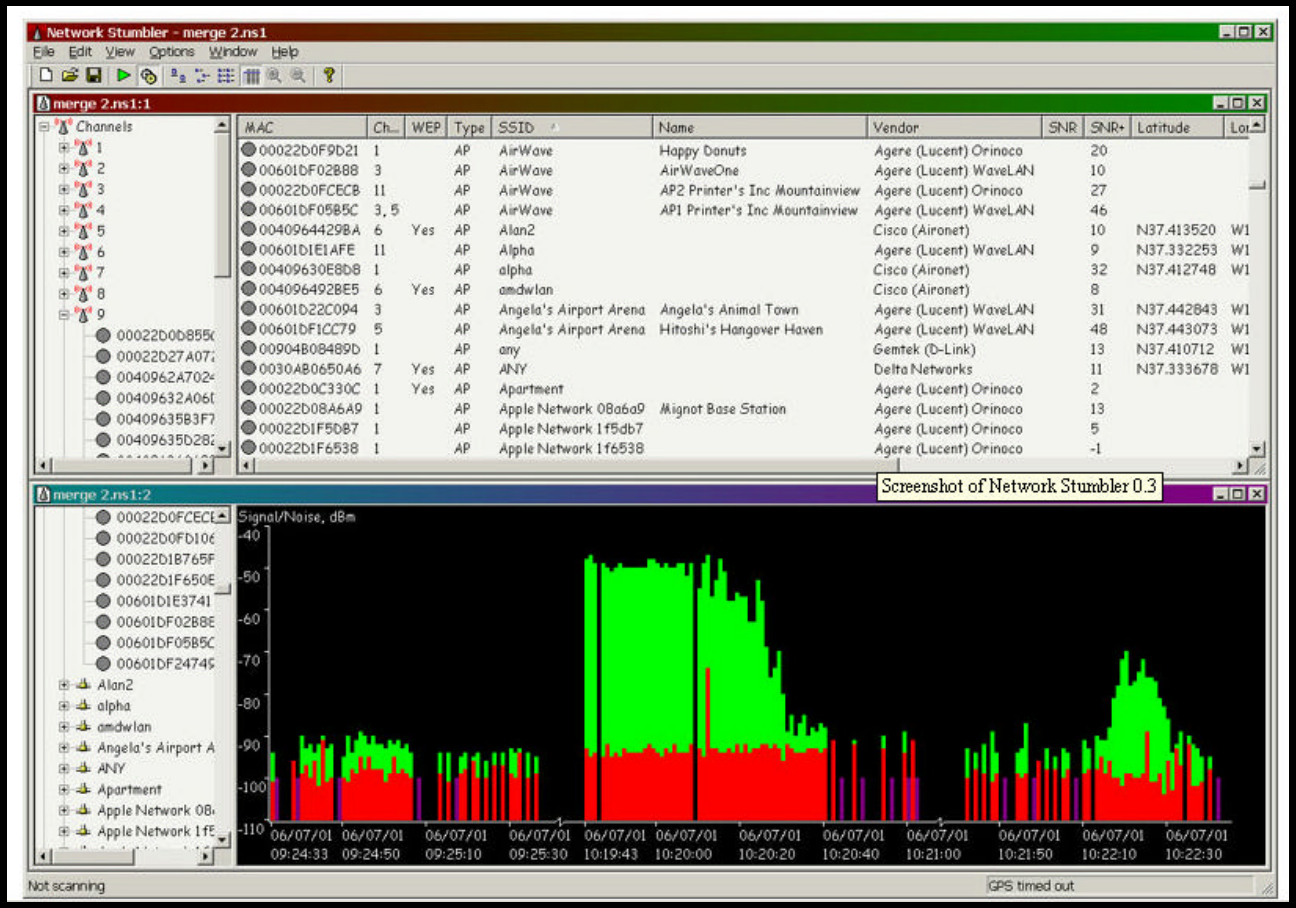


Some ‘Experts’ say you should use an Agilent Spectrum Analyzer
~ $50,000

While this is a good measurement instrument it is not a WLAN analysis tool

Entrust
Securing the Internet

Try Netstumbler

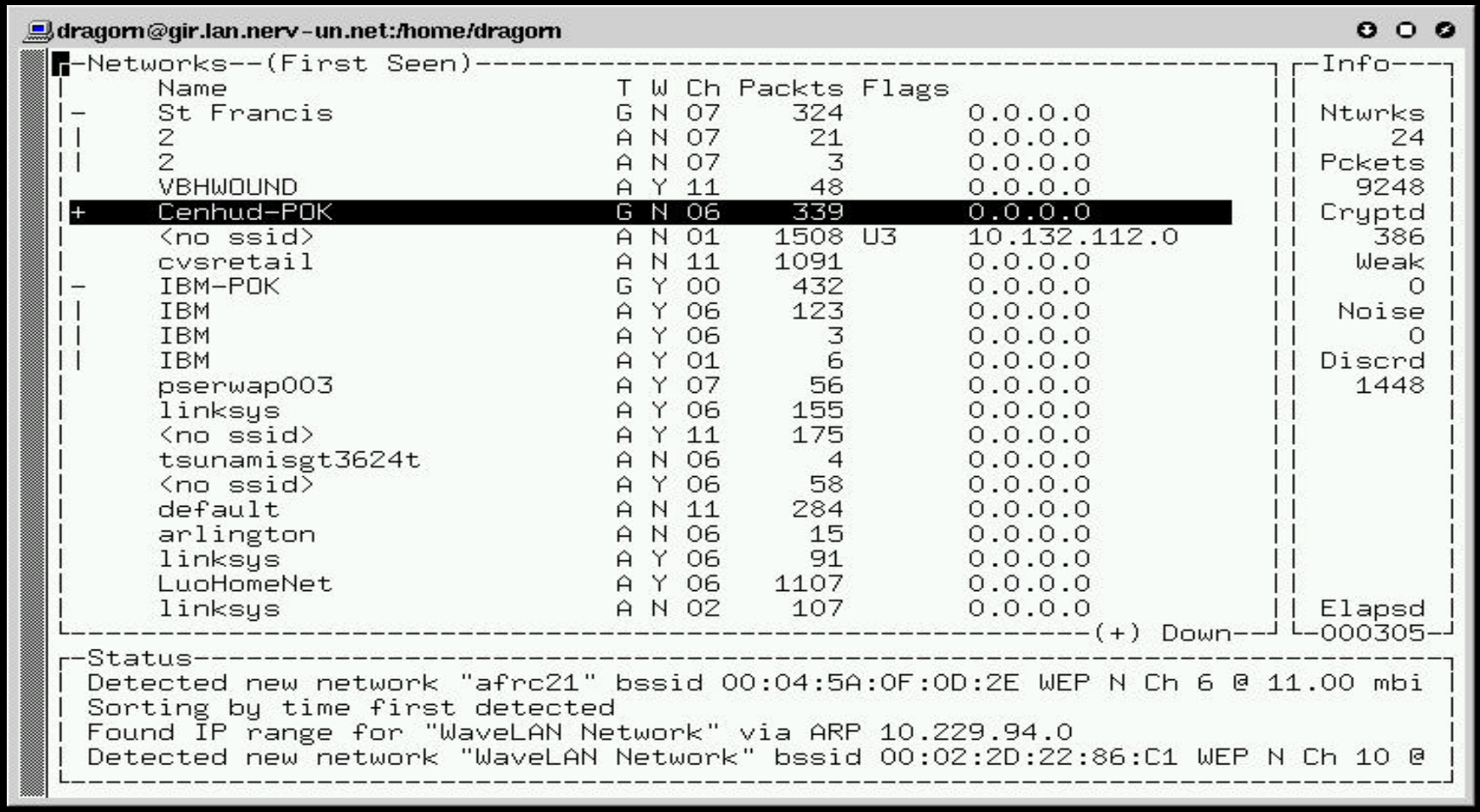


Free!

Also not a WLAN analysis tool but useful for ‘Script Kiddies’ and ‘Seeing’ Relative S/N Ratios

Entrust
Securing the Internet

Or Kismet (Also Free)



A good Linux freeware WLAN analysis tool

Professional Security Analysis Has More Refined Requirements

Entrust
Securing the Internet

Requires Commercial Tools:

1. Must be able to detect non-beaconing devices, noisy environments and 802.11b attacks
2. Must be able to detect *and* locate
3. Must be able to differentiate rogue from deployed
4. Must scan and analyze all channels, not just NA channels
5. Repeatable, accurate, intuitive results
6. Simple, low training overhead, field upgradeable, handheld tool with bulk analysis capability

Entrust
Securing the Internet

AirMagnet - www.airmagnet.com

Comprehensive WLAN Management In a Single Mobile Application

- Site Survey
- Security Assessment
- Performance Management
- Connection Troubleshooting
- Wireless Administration

AirMagnet is Available in Canada from Darkstart Consulting Inc

WLAN Security Assessment Tool: AirMagnet

Entrust
Securing the Internet

Security Assessment

Rogue AP Detection

- Detects All Traffic Including Non-Beaconing Devices
- Identify and Locate Rogue APs and Stations with Find Tool
- Highly Mobile Pocket PC
- Able to Scan All Channels

Security Alarms

- AP w/ WEP Disabled
- Un-configured AP
- Spoofed AP MAC
- DoS Attack (AirJack)
- Device Probing for AP

more…

- Adjustable Alarm Thresholds

Management Tools

- Detects Devices Unprotected by VPN
- Detects Devices Unprotected by 802.1x
- Provides Expert Analysis of Existing Security Threats and Suggests Solutions
- Quickly Drill Down to Detailed Info On Devices That Generate Alarms

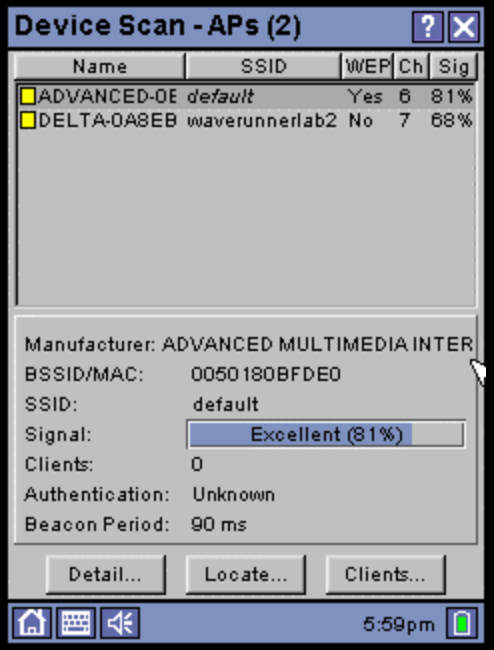
Entrust
Securing the Internet

Fluke Networks: Waverunner

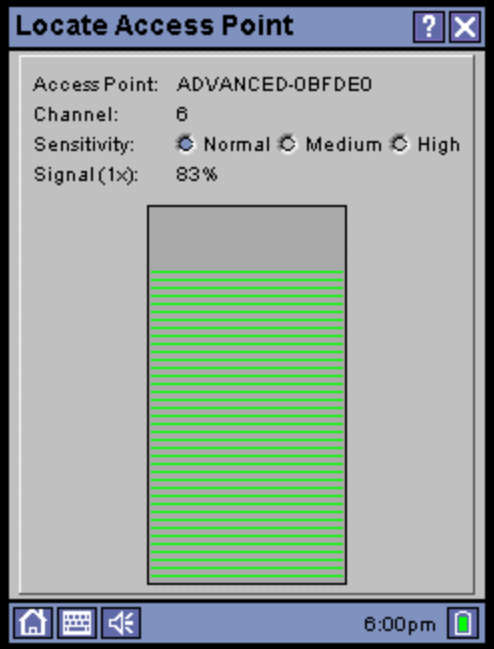
- Pocket Security Guard
- Support for:
  - Rogue AP Detection
  - Site Survey
  - Deployment Verification
  - Connectivity Troubleshooting
  - Latency and Capacity Monitoring

Entrust
Securing the Internet

Rogue AP Detection and Location



Where is the Access Point?



Where are the hidden APs?

How is the AP configured?

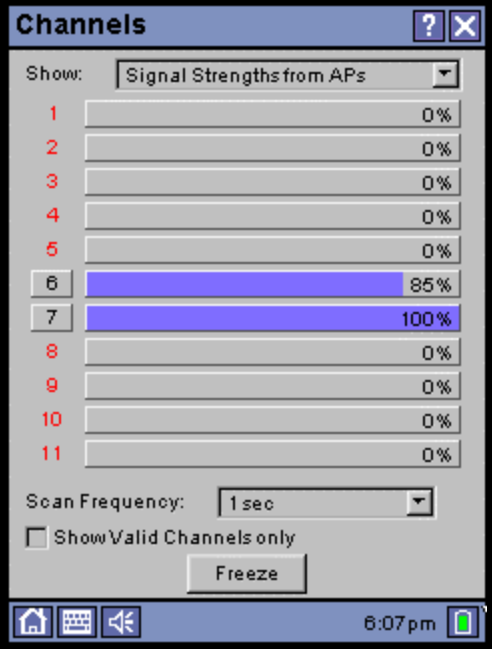
Entrust
Securing the Internet

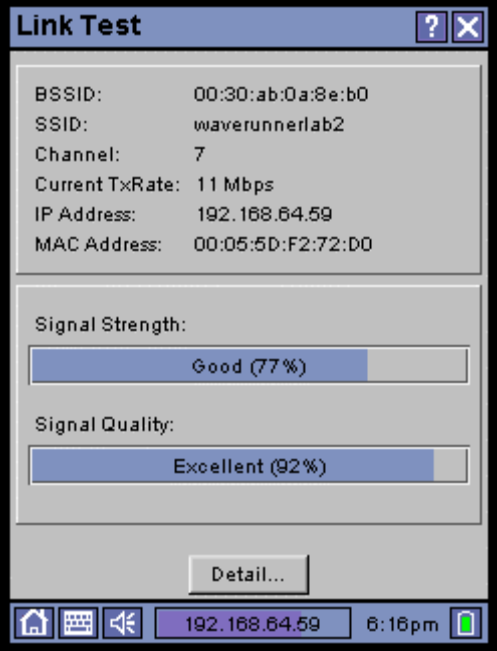
Site Survey

Where do the antennas go?

How should I assign channels?

Do I have rf interference?





Can I connect from everywhere?

What's the signal quality?

Safeguards Against War Drivers, Script Kiddies and Opportunists

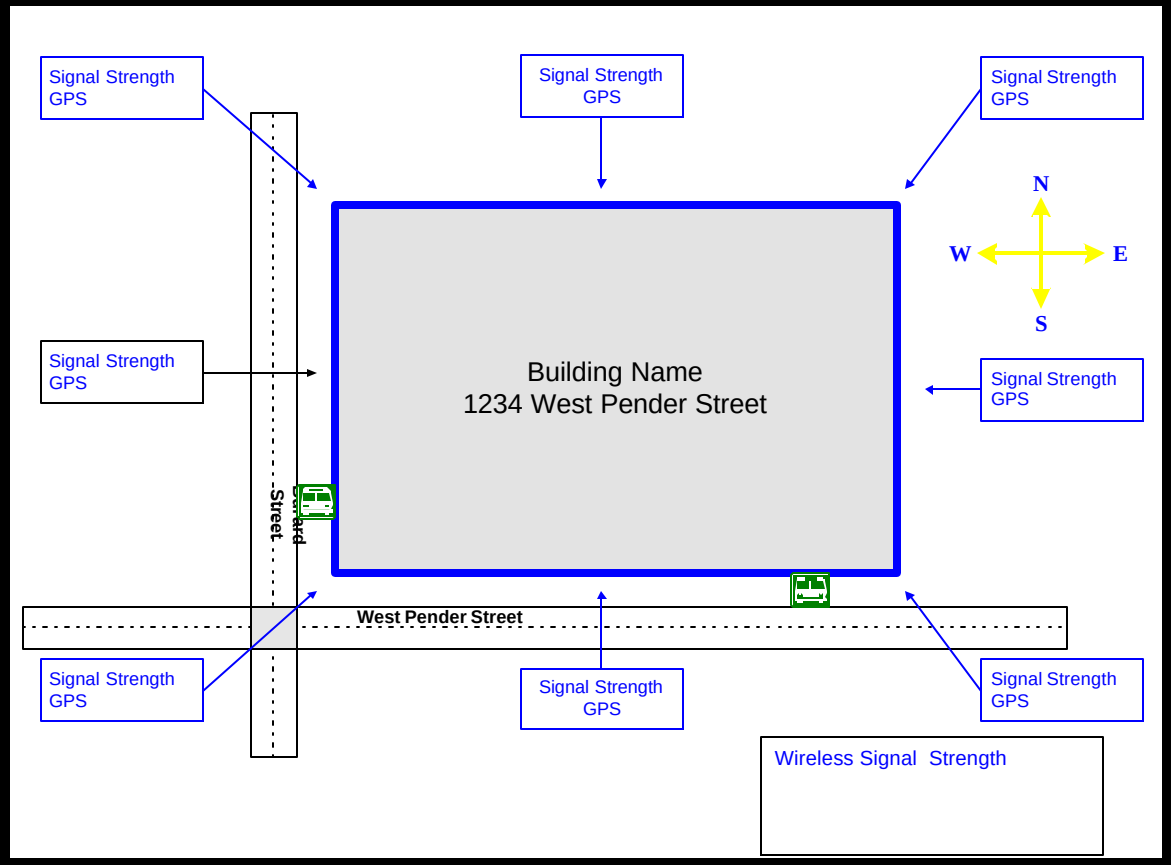
Entrust
Securing the Internet

Change the defaults!

- **Enable WEP**
- **Change the default SSID**
- **Disable “Broadcast SSID"**
- **Change the default password on the AP**
- **Control access based on the MAC address of the NIC**
- **Turn off DHCP, and change the default IP subnet**

But this is not all you need to do!

Conduct a Building Wireless Survey

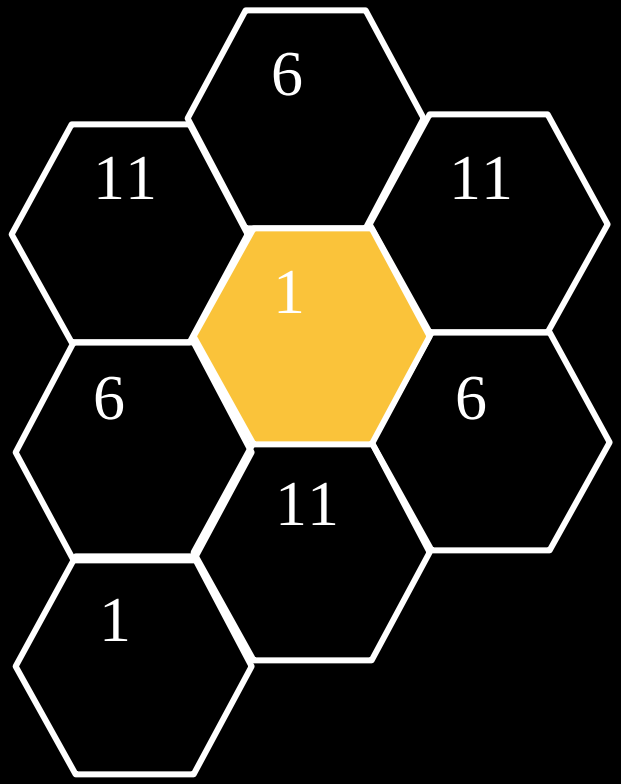


Link your coverage to your operational requirement

Entrust
Securing the Internet

802.11b Channels Overlap

If your neighbor is on Channel 11, pick 1 or 6 for your network



Even Good AP Settings are Not Good Enough

Entrust
Securing the Internet

For Example:

- Passive attacks against WEP are getting better and are slowly being merged with passive WLAN monitoring tools
- AP port and protocol scanning and probing derive WEP keys and AP management passwords
- AirJack Engine: Client, MITM and DoS attacks

Entrust
Securing the Internet

Improved Attacks on RC4 (WEP)

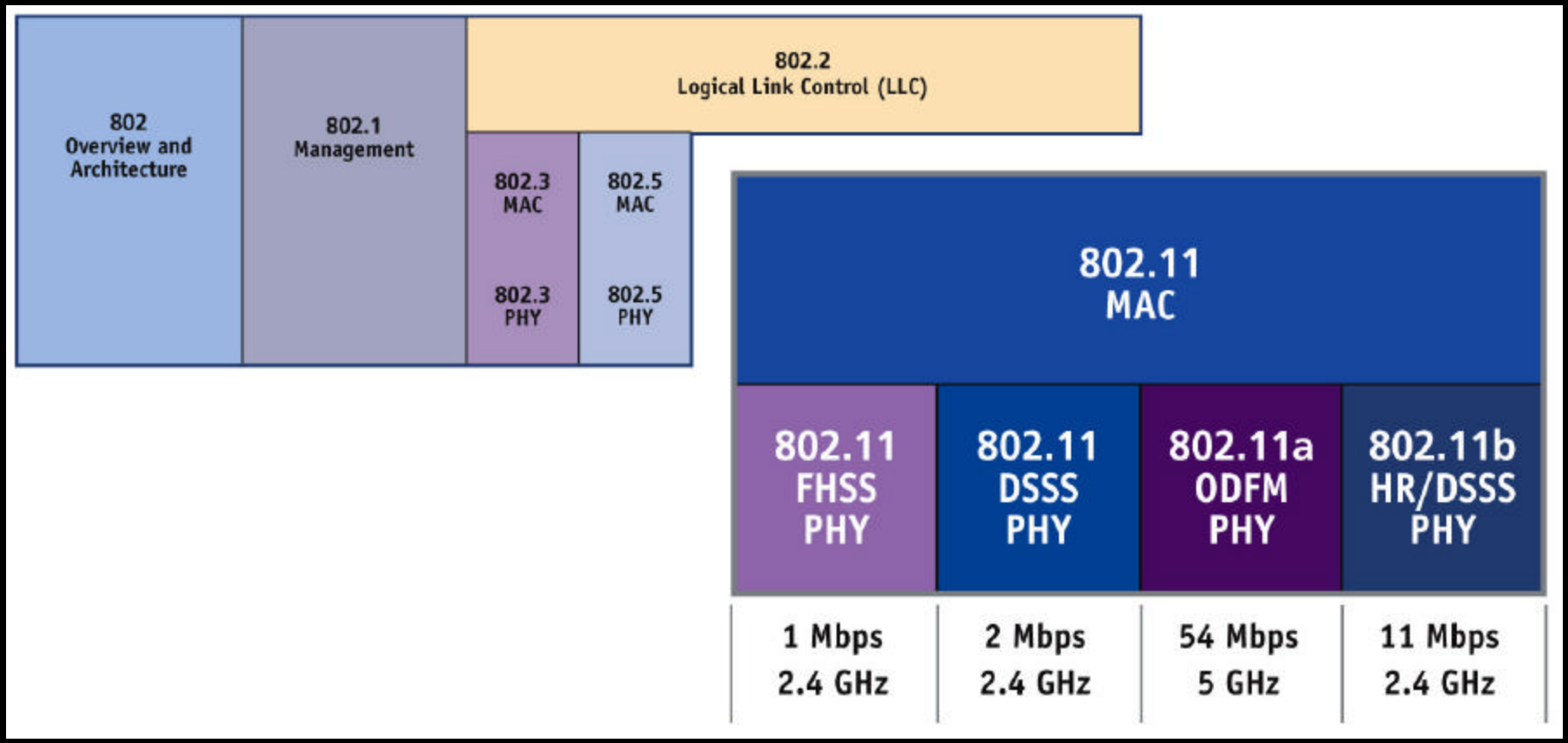
"In order to carry out the attack, the cryptanalyst needs the first output word of a large number RC4 streams along with the IV that was used to generate each one of them."

"Since in WEP, the IVs are transmitted in the clear, and the first message word in most packets is a known constant these requirements are satisfied. Optimizations of the attack have lead to deduction of a 128 bit RC4 key in 15 minutes from an actual network."

RSA Laboratories
Volume 5, No. 2, Summer / Fall 2002

Entrust
Securing the Internet

802 Layers



Source: Fluke Networks

Entrust
Securing the Internet

Management Frames

- Management frames control link characteristics and physical medium properties
- 802.11b management frames are **NOT** authenticated
- This allows radio protocol attacks
- All you need is some extra RF power and you can 'capture' the victim's radio receiver and feed it whatever protocol you want

Entrust
Securing the Internet

Attacks – AirJack

Denial of Service – De-Authentication

- Spoof MAC address of Access Point
- Send de-authenticate 802.11b management frames

  Send them continuously

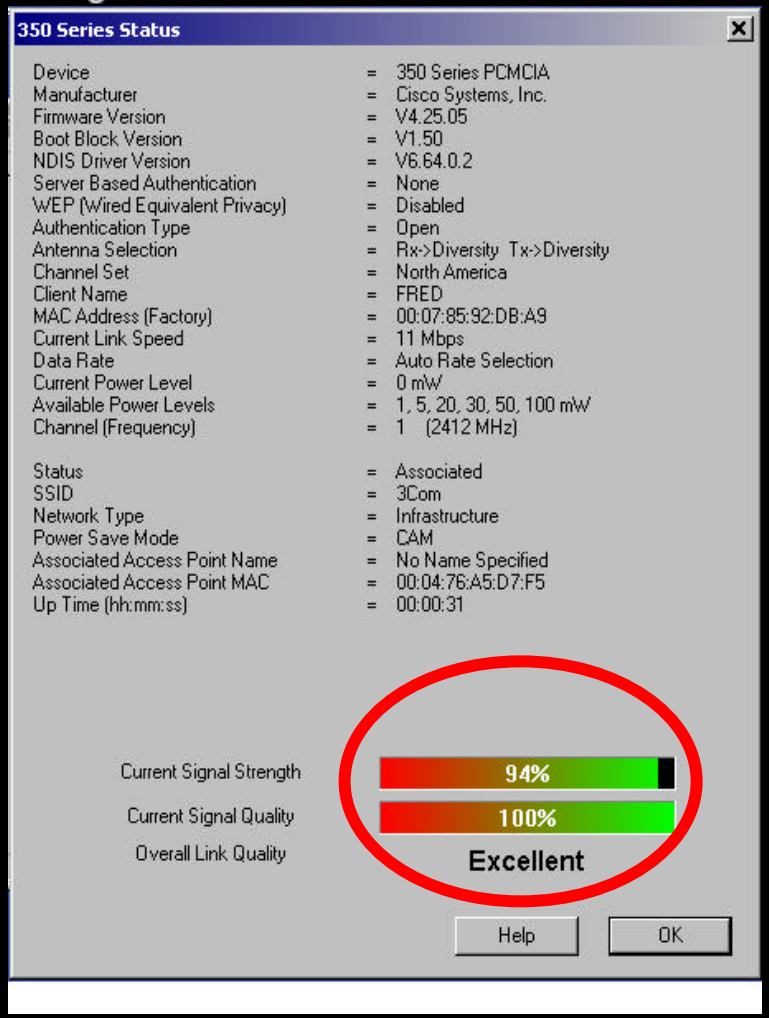
  Client is forced to re-associate and re-authenticate (longer process)

  Attacker uses lots of power, ‘pumps’ the victim’s receiver to slow it’s response time

Users are unable to re-associate with valid AP

Attacks – AirJack

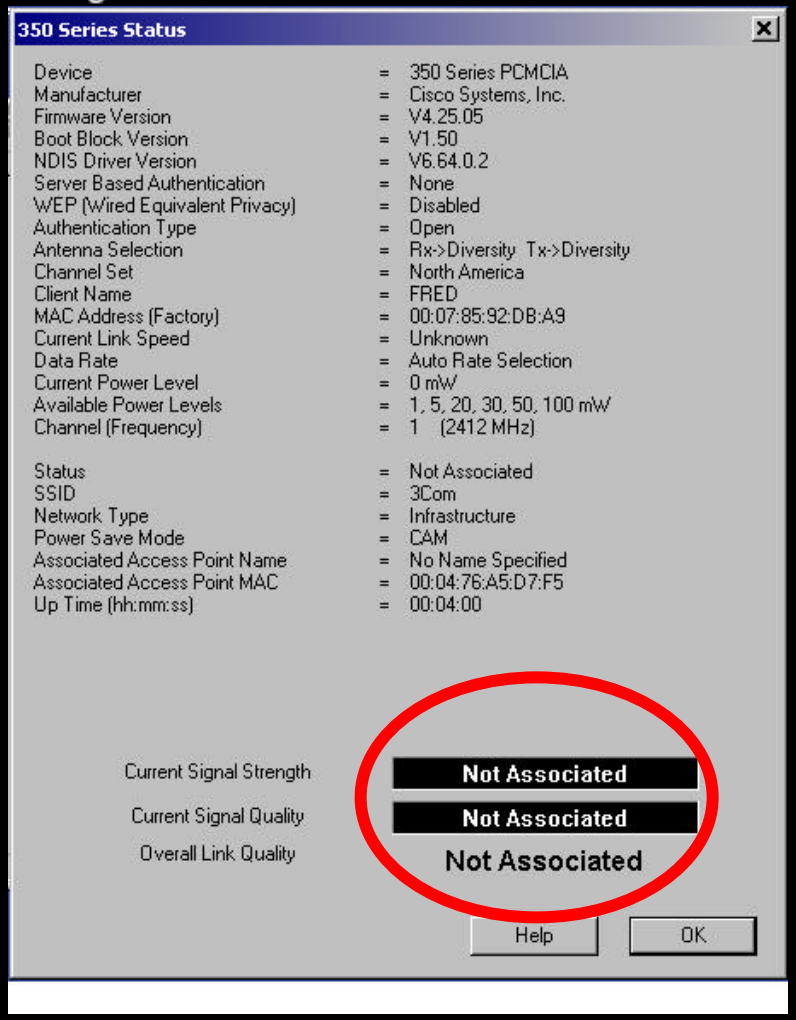
Entrust
Securing the Internet



This is your connection

Attacks – AirJack

Entrust
Securing the Internet



This is your connection during an AirJack-based attack

802.11b Frame Attacks

Entrust
Securing the Internet

Frame Type (bit 3, bit2)	Subfield (Bits 7,6,5,4)	Frame Function
Management Type 00	0000	Association Request
	0001	Association Response
	0010	Reassociation Request
	0011	Reassociation Response
	0100	Probe Request
	0101	Probe Response
	1000	Beacon
	1001	Announcement Traffic Indication (ATIM)
	1010	Dissassociation
	1011	Authentication
	1100	Deauthentication
Control Type 01	1010	Power-Save (PS) Poll
	1011	Request to Send (RTS)
	1100	Acknowledgement (ACK)
	1110	Contention Free (CF) End
	1111	CF End + CF ACK
Data Type 10	0000	Data
	0001	Data + CF ACK
	0010	Data + CF Poll
	0011	Data + CF ACK + CF Poll
	0100	Null (no data)
	0101	CF ACK
	0110	CF Poll
	0111	CF ACK + CF Poll
Reserved Type 11		

Management Frame Types

AirJack attacks these

Control Frames

What happens if they attack these?

Data Frames

Picture Source: Fluke Networks

Entrust
Securing the Internet

More AirJack Attacks

- MITM Attack
  - Take over connections
  - Insert attack machine between victim and AP (Power + Antenna)
  - Use it to attack the client or the network behind the AP
- Insert False Management Frames on the RF Channel (Power and antenna)
  - This forces de-authentication of the victim from the real AP
    - Send de-authenticate frames to the victim using the access point's MAC address as the source
  - Victim's 802.11 card scans channels to search for new AP

Entrust
Securing the Internet

Attacks

- Victim's 802.11 card associates with fake AP on the attack machine
  - Fake AP is on a different channel than the real one
  - Attack machine's fake AP is duplicating MAC address and ESSID of real AP
  - You can attack the victim, scan his hard drive, send him a Trojan horse, etc,
  - Attack machine may optionally associate with real AP
  - Attack machine duplicates MAC address of the victim's machine

Entrust
Securing the Internet

Some General Conclusions

802.11b wireless networks are more vulnerable to attacks than wired networks

802.11b security solutions are implemented with an assumption of secure radio management and control protocols

Inadequate authentication for protection against wireless MITM attacks

Weak management and security

Entrust
Securing the Internet

What do we do now?

How can you bring

Trust and **Security**

to WLAN?

Assess Your Security Requirements

Entrust
Securing the Internet

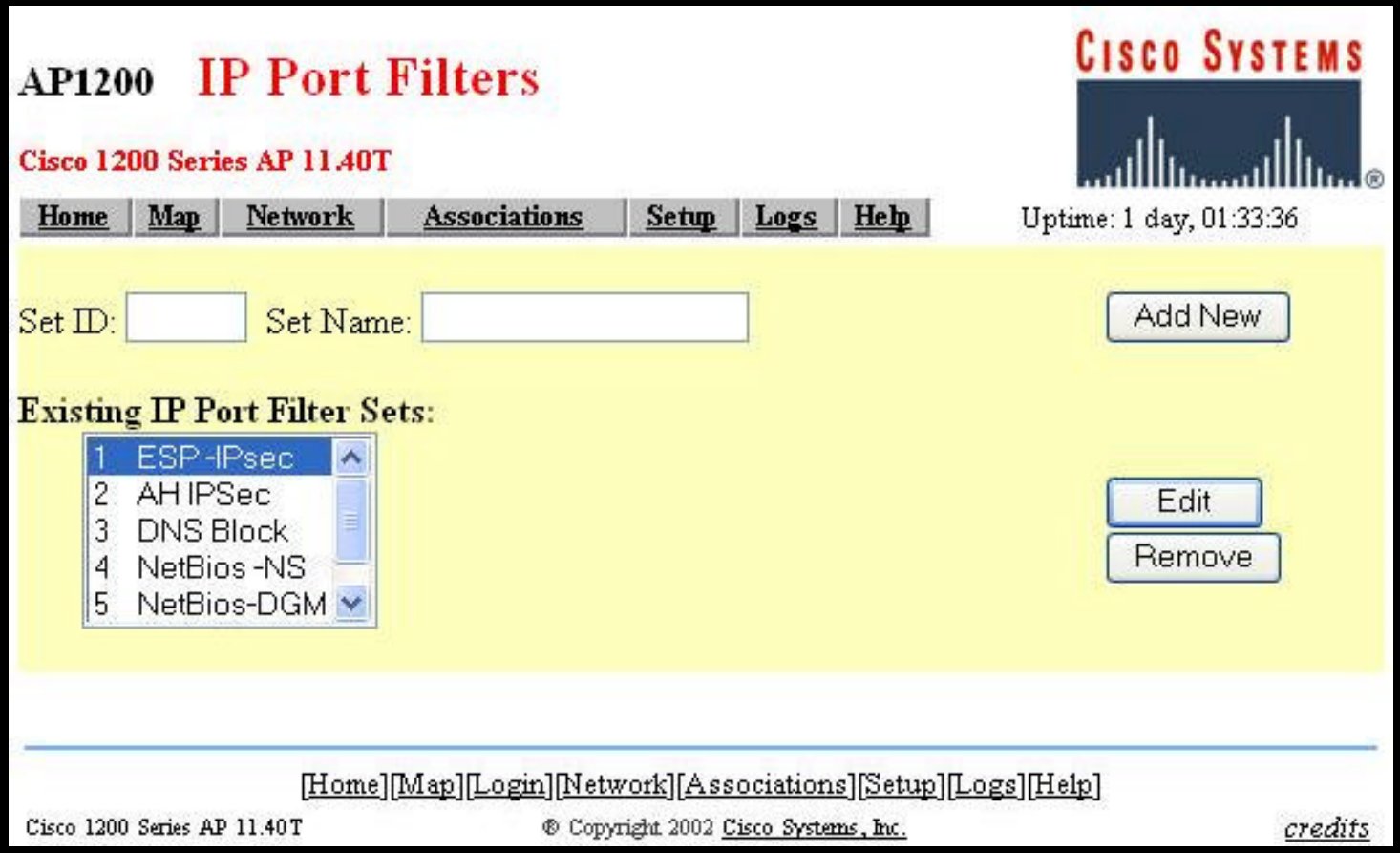
- ✓ Analyze your environment
- ✓ Perform your risk assessment
- ✓ Determine your wireless security profile ....

Security =

Knowledge + Strong Authentication + Encryption + Monitoring + the Other Layers of the Onion

Entrust
Securing the Internet

Cisco AP Allows for Filtering



This hardens the AP against attack!

Entrust
Securing the Internet

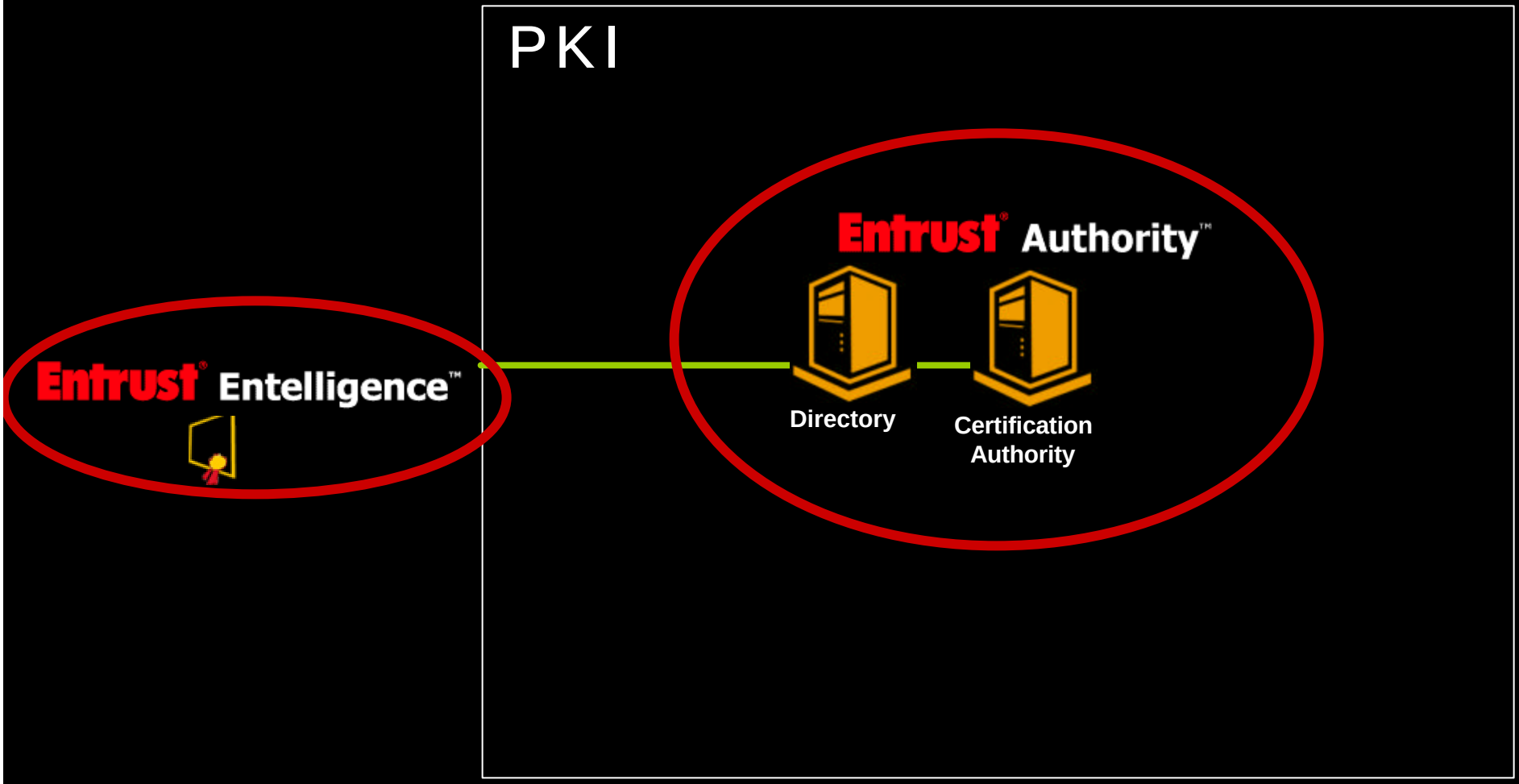
Cisco Advantages

Cisco VPN Client/Gateway technology is 'Best in Class' for WLAN Applications

- ✓ Strong encryption, True IPSec VPN
- ✓ Auto-initiate VPN tunnel for WLAN connections
- ✓ Force Security Policy e.g.: 'Disable Split Tunneling'
- ✓ Stateful Inspection Firewall Client AND Gateway
- ✓ Forced Virus scanning
- ✓ Strong, certificate based authentication using Entrust PKI certificates that are securely managed
- ✓ Security Hardware and Software from a 'Mature' vendor

Entrust Secure WLAN Solution Provides Security Infrastructure

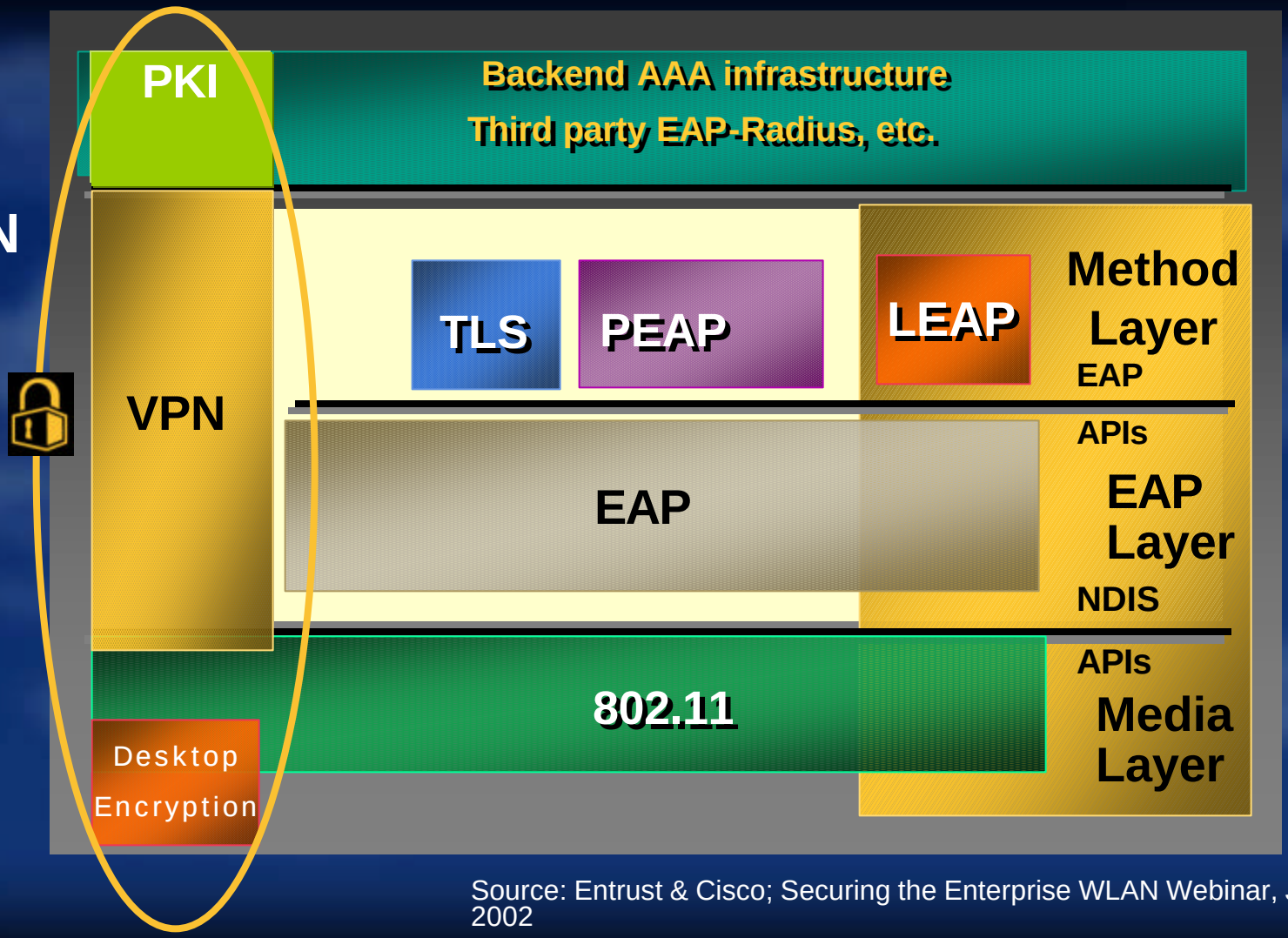
Entrust
Securing the Internet



Security Frameworks

Entrust
Securing the Internet

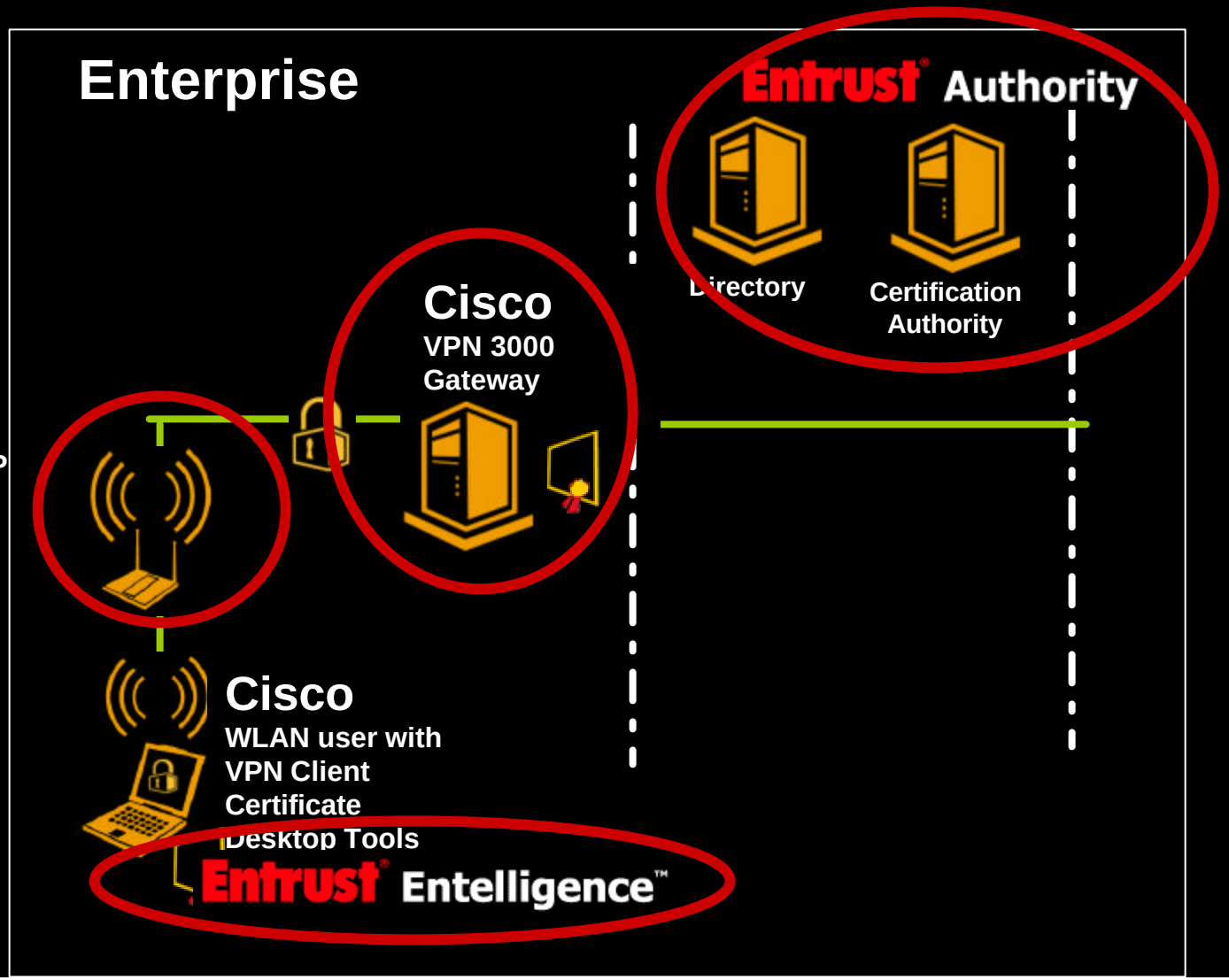
PKI
+ VPN



Source: Entrust & Cisco; Securing the Enterprise WLAN Webinar, July 2002

Securing WLAN: Cisco + Entrust

Entrust
Securing the Internet



Enhanced Security is Required When Using WLAN Technology!

Entrust
Securing the Internet

Enhanced Security is needed to Strongly Identify users and devices and to protect client data

Entrust
Securing the Internet

Summary

Achieving the benefits of WLAN requires confidence that the same level of privacy & trust is maintained in the wireless world as in the wired world!

Cisco WLAN +

Cisco VPN +

Entrust PKI =

Trusted WLAN transactions and protected networks and clients

Entrust
Securing the Internet

Questions & Answers

For more information

http://www.entrust.com/wlan

Thank You!

entrust@entrust.com