Wireless Security: Critical Issues and Solutions

Craig J. Mathias

Principal, Farpoint Group

COMNET 2003

29 January 2003

Our Speakers Today…

- Yangmin Shen, Director of Technical Marketing, The Americas, Wireless Networking Group, Wireless Systems Division, Symbol Technologies, Inc.
- Fred Tanzella, Chief Security Officer, AirDefense
- Stephen C Swartz, Technical Application Manager, Federal Government, Sprint

Farpoint Group

7 Whippoorwill Lane
Ashland MA 01721

508-881-6467
508-881-8058 (fax)

info@farpointgroup.com

WLAN Security

Maintaining Perspective

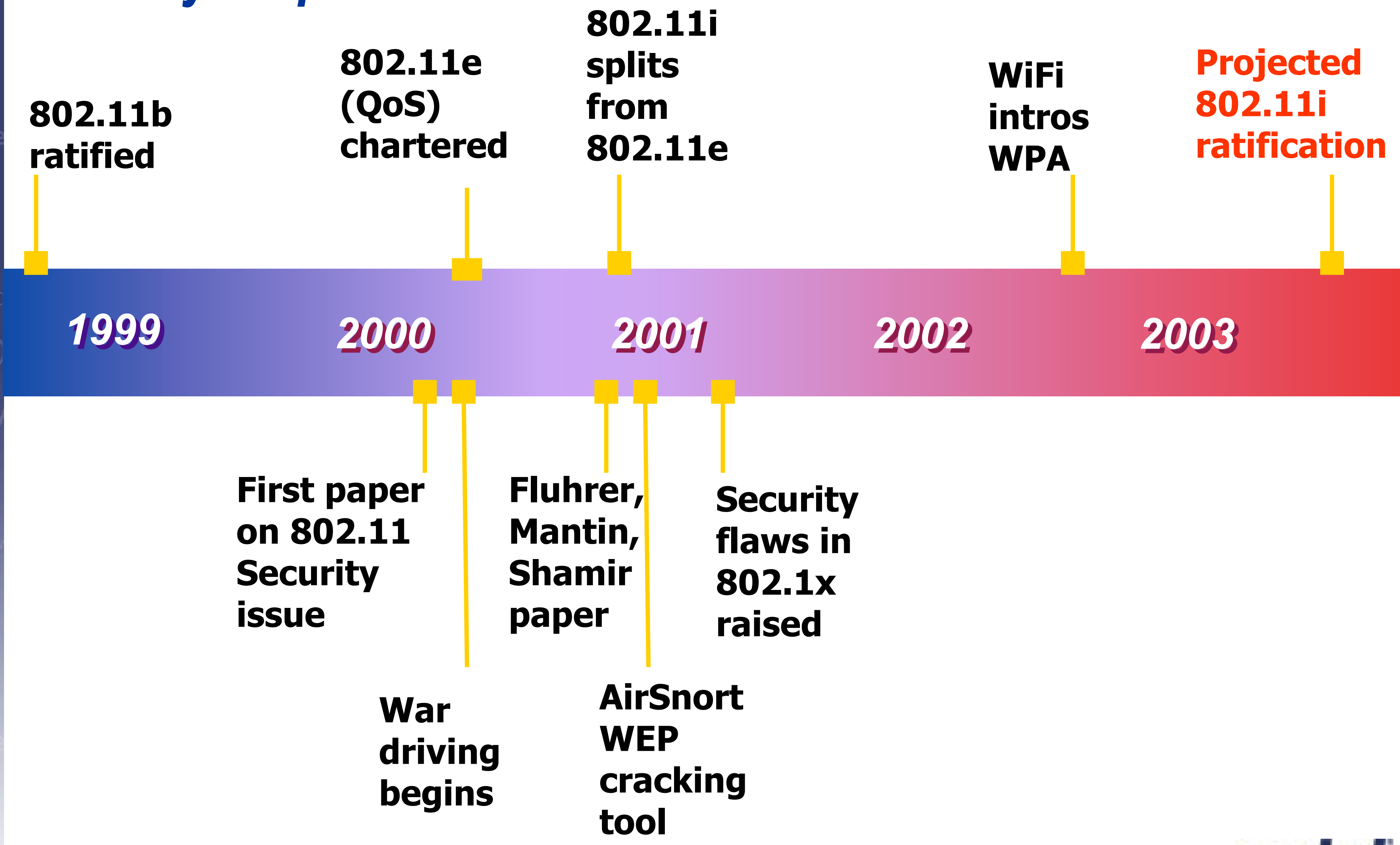
Yangmin Shen

Director, Technical Marketing

Wireless Systems Division

WLAN Security Timeline

Multi-year process



802.11b ratified

802.11e (QoS) chartered

802.11i splits from 802.11e

WiFi intros WPA

Projected 802.11i ratification

First paper on 802.11 Security issue

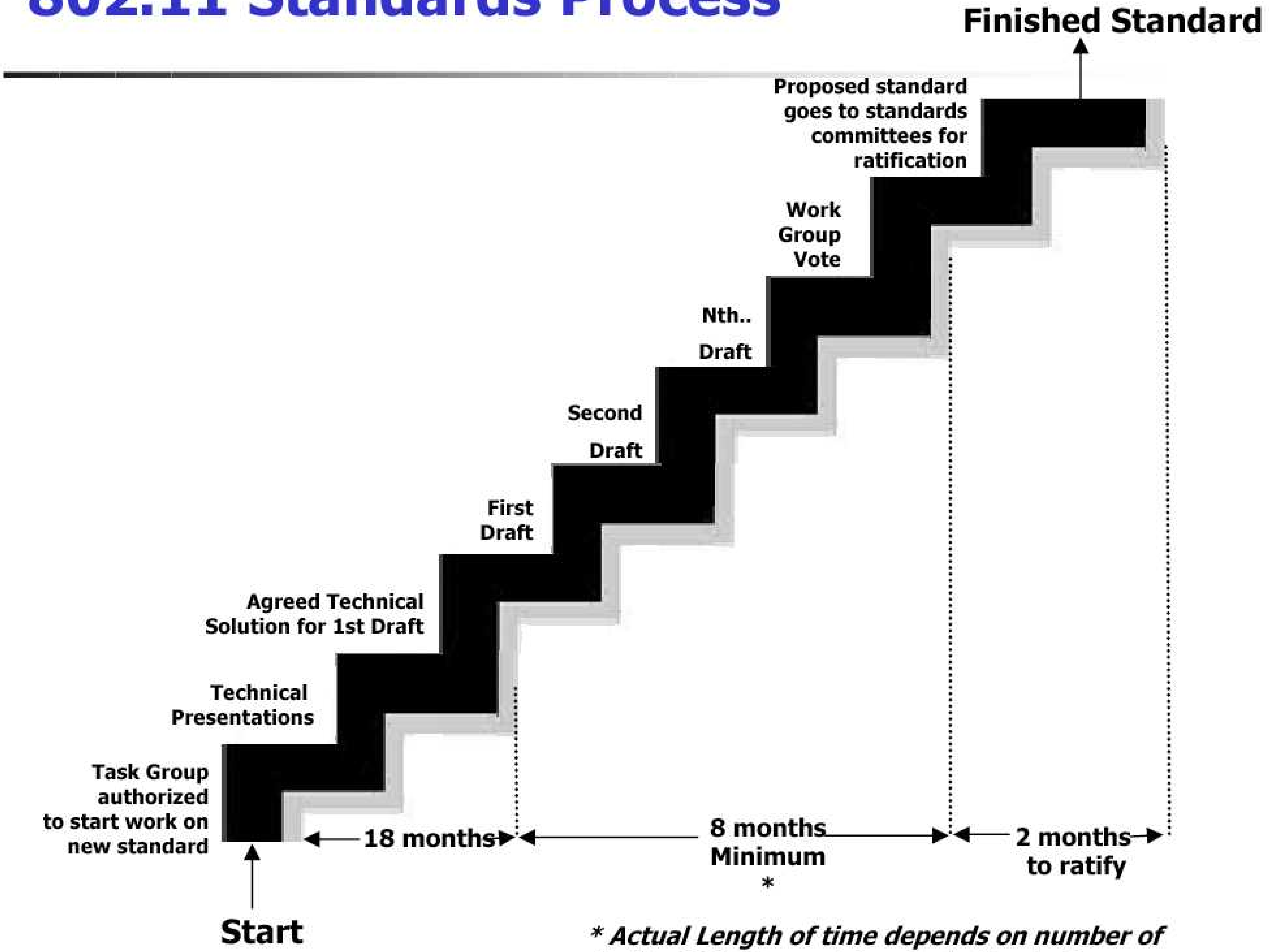
War driving begins

Fluhrer, Mantin, Shamir paper

AirSnort WEP cracking tool

Security flaws in 802.1x raised

802.11 Standards Process



Finished Standard

Proposed standard goes to standards committees for ratification

Work Group Vote

Nth.. Draft

Second Draft

First Draft

Agreed Technical Solution for 1st Draft

Technical Presentations

Task Group authorized to start work on new standard

18 months

8 months Minimum *

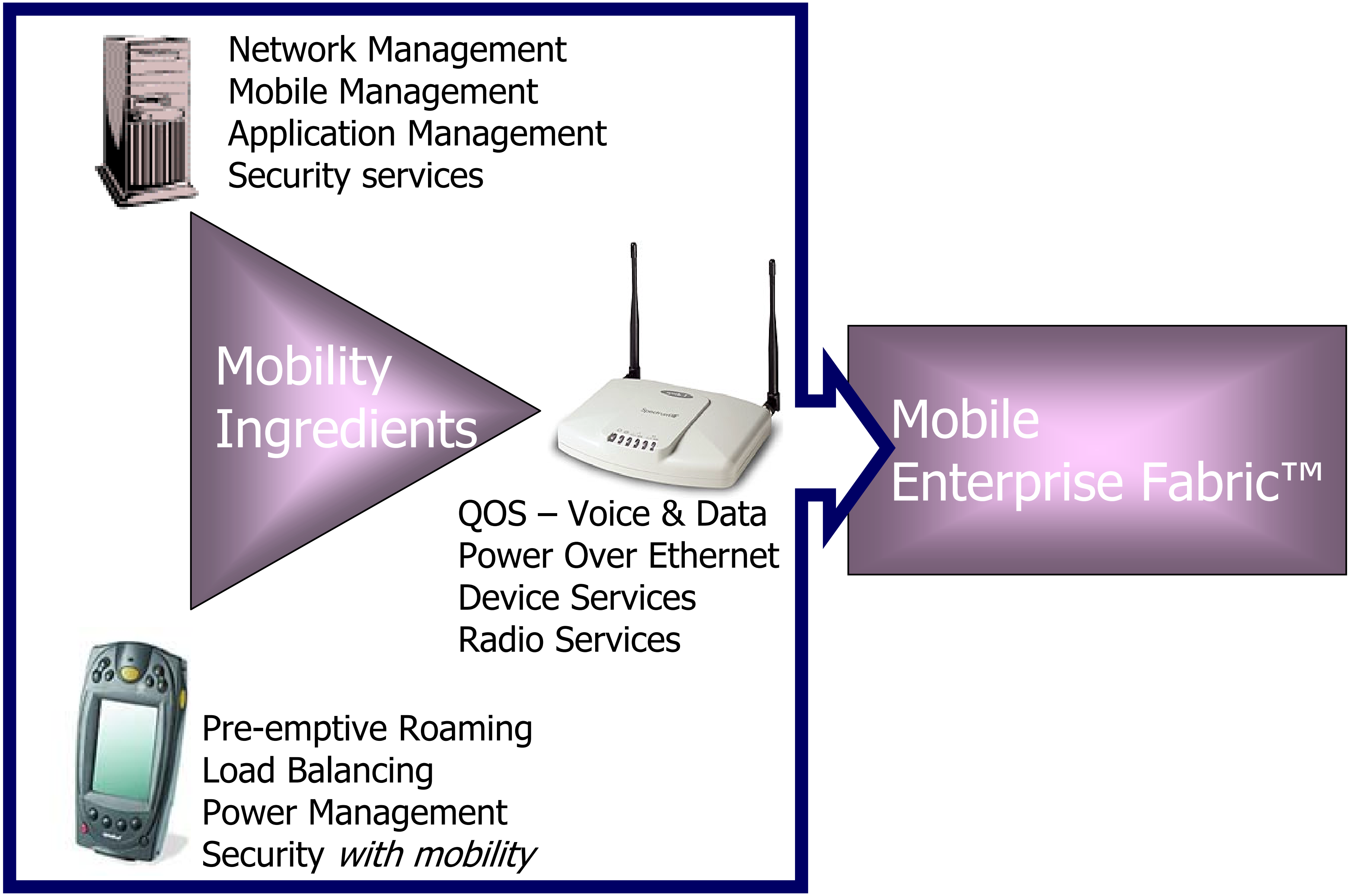
2 months to ratify

Start

** Actual Length of time depends on number of drafts. 802.11 spent 4 years in the draft process*

symbol

You Are Building a System



Network Management
Mobile Management
Application Management
Security services

Mobility
Ingredients

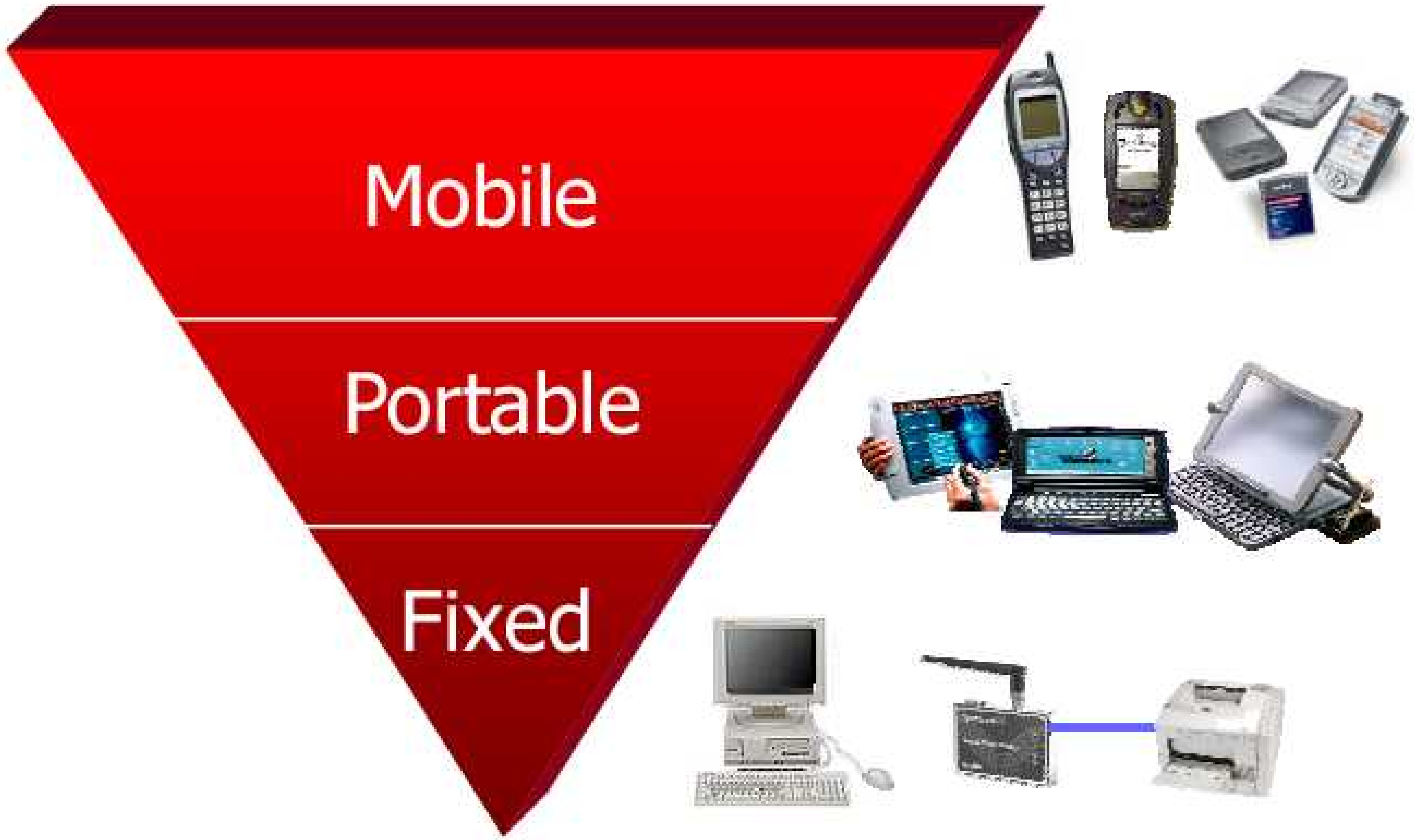
QOS – Voice & Data
Power Over Ethernet
Device Services
Radio Services

Pre-emptive Roaming
Load Balancing
Power Management
Security *with mobility*

Mobile
Enterprise Fabric™

Mobile Applications Demand More

- WLANs naturally allow Portability, *but must be designed for Mobility*
- Requirements for Mobility are a superset of requirements for Portability



VoIP Phones
Vehicle Mounted Devices
Hand Held Devices

Notebooks, Laptops
With WLAN PC Cards

Desktops with
WLAN PCI Cards

Serial Client
Bridge with Printer

Understand Device Security Implications

The Least Common Denominator (LCD) problem

- There may be critical devices that cannot be upgraded to 802.11i or other future security protocols
  - CPU, memory, cost constraints (printers, client bridges, embedded devices)
  - Some are legacy devices
  - Many are future devices
- Single ESSID networks are forced to use the LCD for security
  - Usually WEP, but WEP is unacceptable
- Eliminating lightweight security devices not practical
- Single vendor policy won’t solve this problem
- Multiple security solutions will be a way of life for several years to come.

New Feature Awareness

- Multi-ESSID & VLAN Support
  - Multiple ESSIDs allows for multiple security classes on same AP
  - Lowest security class can be isolated and restricted
    - IP Re-direct
    - VLANs
  - Security by function is practical
    - Lightweight CPU devices can’t do 802.11i
      - naturally less traffic, naturally less vulnerable
    - High-end devices can do more sophisticated security
      - Naturally more traffic, naturally more vulnerable
- Rogue AP Detection
  - Detects unauthorized APs
  - Rogue APs are biggest industry problem

Maintaining Perspective

- Security standards are still a moving target
- System Design: Security affects system performance
- Be wise & design for mobile users, not portable
- Understand your WLAN clients & plan for the Least Common Denominator problem
- Evaluate significance of new features

Don't feel your way when you can navigate

AirDefense™
Enterprise Wireless LAN Security

Wireless LAN Security

Fred Tanzella
Chief Security Officer
AirDefense

October 2002

Topics

I. Wireless LAN Overview

II. Wireless LAN Security Overview

III. War Driving

III. Vulnerability Examples

IV. Securing Your Wireless LAN

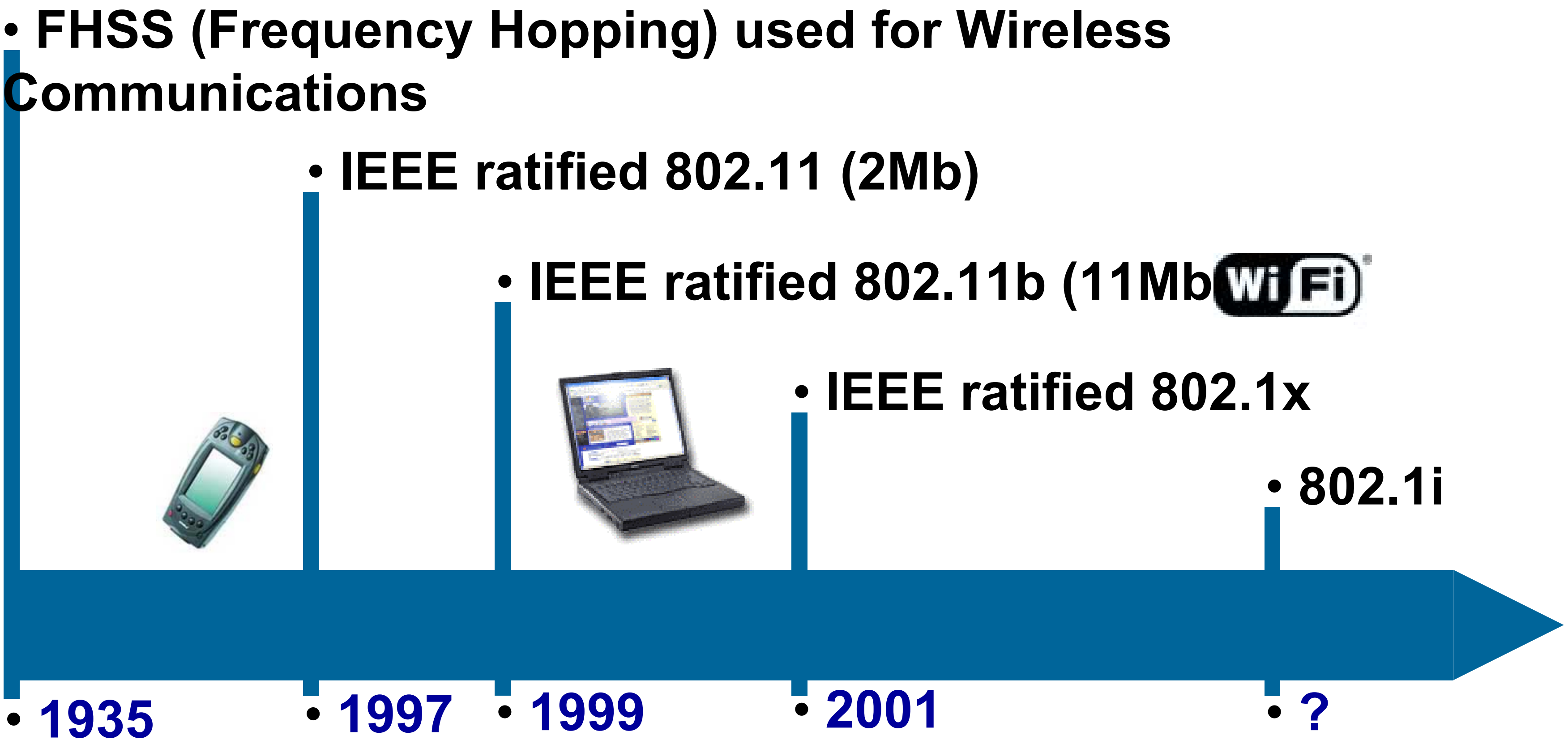
V. Q & A

AirDefense

AirDefense™
Enterprise Wireless LAN Security

Wireless LAN Overview

Wireless Technology Standards Timeline



- FHSS (Frequency Hopping) used for Wireless Communications
- IEEE ratified 802.11 (2Mb)
- IEEE ratified 802.11b (11Mb
- IEEE ratified 802.1x
- 802.1i

- 1935
- 1997
- 1999
- 2001
- ?

Why are Wireless LANs Taking Off?

- Cheap to Deploy
- Good Performance
- Allow mobility for workforce
- Saves Ports in Switches

AirDefense

Wireless LAN Example Deployments

- Utility Company Trucks

  Meter Reading

- Government Agency

  Office Applications

- Railroad

  Rail Yard Applications

- Hospitals

  Mobile Point of Care

AirDefense

AirDefense™

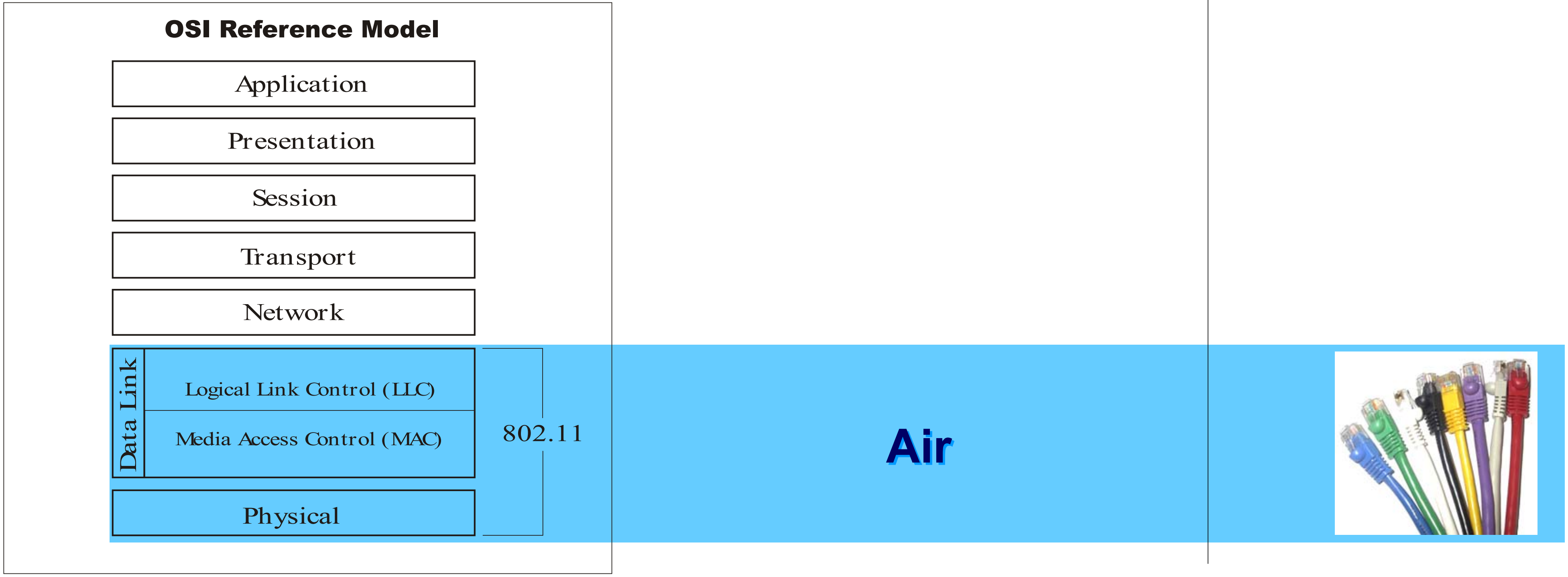
Enterprise Wireless LAN Security

Wireless LAN Security Overview

Why is Wireless LAN Security Different?

Wireless LAN

Wired LAN



OSI Reference Model

Application

Presentation

Session

Transport

Network

Data Link

Logical Link Control (LLC)

Media Access Control (MAC)

Physical

802.11

Air

MAC Address: 00:09:B7:13:A9:B2
SSID: TSUNAMI

Wireless LAN Security Flaws

- WEP Disabled / WEP Cracking
- Rogue Access Points
- Internal Abuse
- Ad Hoc Networks
- Identity Theft
- Denial of Service
- Man-in-Middle Attack

AirDefense

Wireless LANs - What's at Risk

- Corporate Networks
- Corporate Data
- Financial Systems
- Intellectual Property
- Executive's Local Data

AirDefense

AirDefense™
Enterprise Wireless LAN Security

Protecting your WLAN airwaves

War Driving

War Driving Tools

1. NetStumbler and MiniStumbler
2. Kismet
3. WEPCrack
4. AirSnort
5. Fake AP
6. Wireless Security Auditor
7. THC-WarDrive
8. THC-RUT
9. MacStumbler
10. BSD-AirTools
11. PrismStumbler
12. Mognet
13. WarLinux
14. Wellenreiter
15. WaveStumbler
16. AiroPeek
17. Stumbverter
18. AP Scanner
19. SSID Sniff
20. Wavemon
21. AirTraf
22. AirJack

NETSTUMBLER.COM

Kismet

WildPackets AiroPeek™

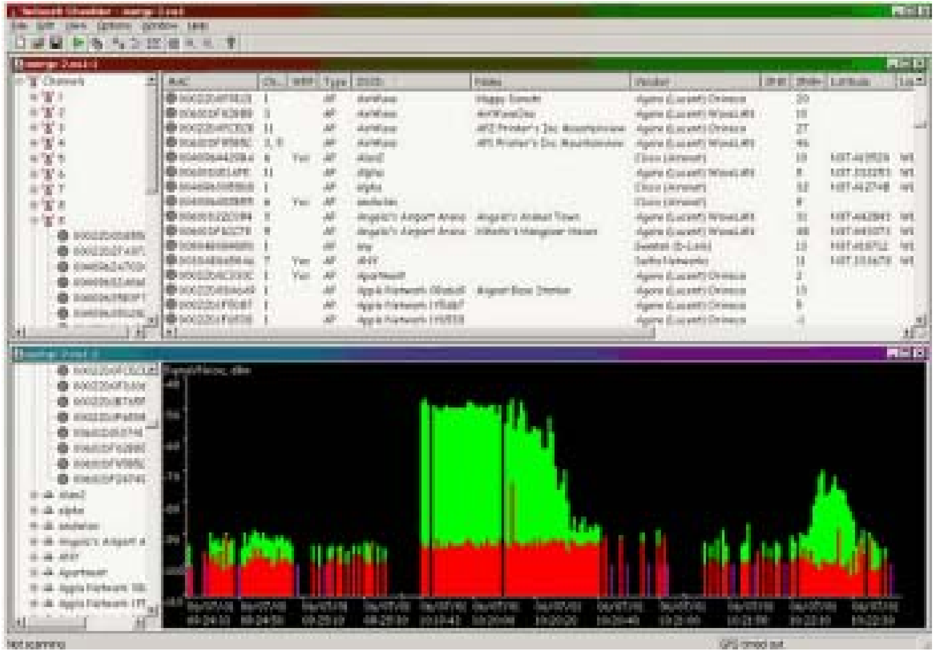
AIR SNORT

wellenreiter

Using NetStumbler

NETSTUMBLER.COM

- What is it?
  - Freeware Network sniffer
- What it does.
  - Sniffs wireless packets
- How it works.
  - Actively probes

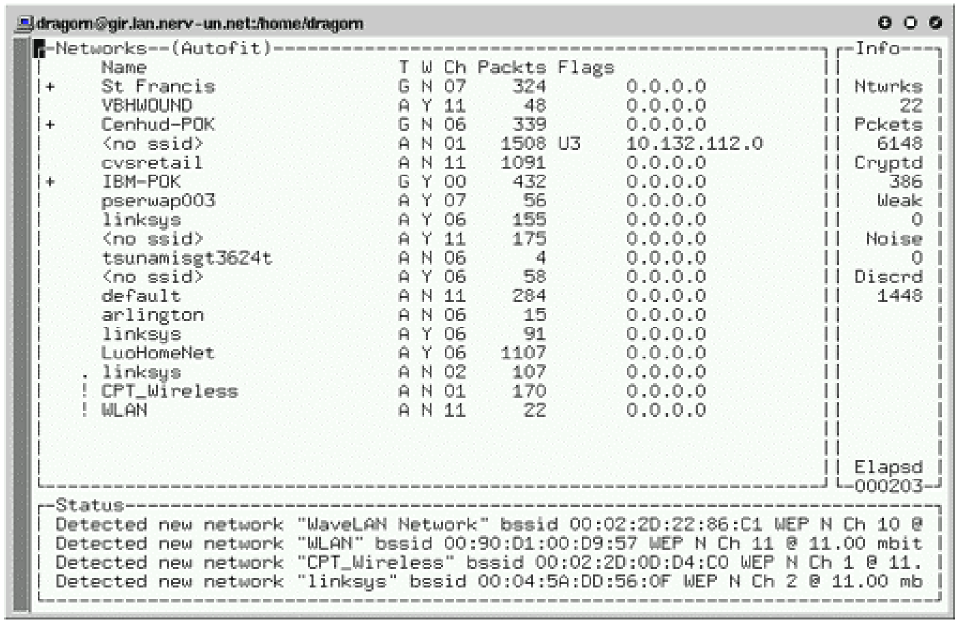


Runs on:
Windows Laptops
PocketPC PDAs

AirDefense

Using Kismet to find APs

- **What is it?**
  - **- Freeware Network sniffer**
- **What it does.**
  - **- Sniffs wireless packets**
- **How it works.**
  - **- Passively monitors**

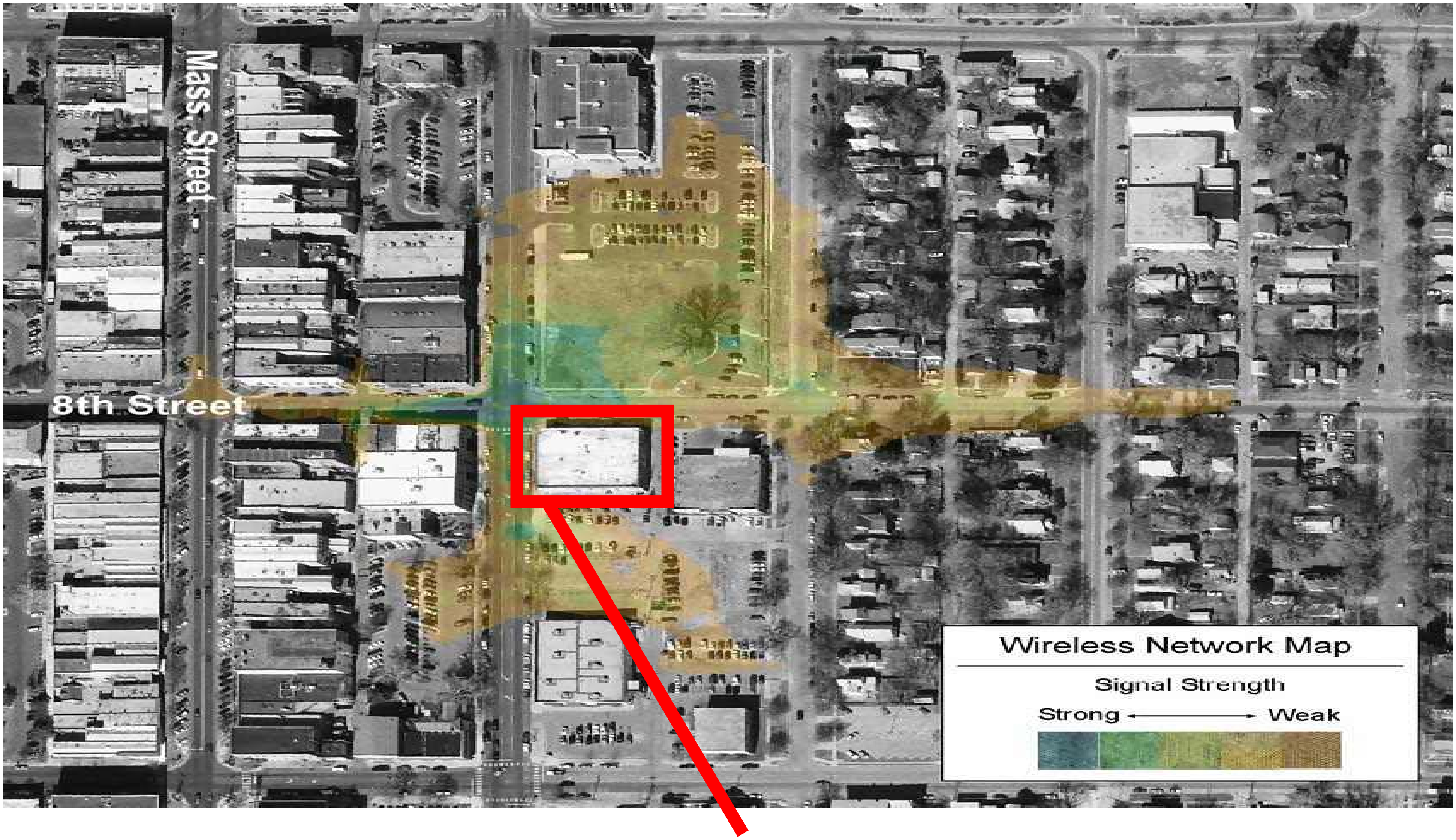


```
dragorn@gir.lan.nerv-un.net:/home/dragorn
-Networks--(Autofit)--------------------------------------------  -Info---
|      Name                         T W Ch Packts Flags          || |        |
|+     St Francis                   G N 07    324       0.0.0.0  || | Ntwrks |
|      VBHWOUND                     A Y 11     48       0.0.0.0  || |     22 |
|+     Cenhud-POK                   G N 06    339       0.0.0.0  || | Pckets |
|      <no ssid>                    A N 01   1508 U3    10.132.112.0 || |   6148 |
|      cvsretail                    A N 11   1091       0.0.0.0  || | Cryptd |
|+     IBM-POK                      G Y 00    432       0.0.0.0  || |    386 |
|      pserwap003                   A Y 07     56       0.0.0.0  || |   Weak |
|      linksys                      A Y 06    155       0.0.0.0  || |      0 |
|      <no ssid>                    A Y 11    175       0.0.0.0  || |  Noise |
|      tsunamisgt3624t              A N 06      4       0.0.0.0  || |      0 |
|      <no ssid>                    A Y 06     58       0.0.0.0  || | Discrd |
|      default                      A N 11    284       0.0.0.0  || |   1448 |
|      arlington                    A N 06     15       0.0.0.0  || |        |
|      linksys                      A Y 06     91       0.0.0.0  || |        |
|      LuoHomeNet                   A Y 06   1107       0.0.0.0  || |        |
|    . linksys                      A N 02    107       0.0.0.0  || |        |
|    ! CPT_Wireless                 A N 01    170       0.0.0.0  || |        |
|    ! WLAN                         A N 11     22       0.0.0.0  || |        |
|                                                               || |        |
|                                                               || | Elapsd |
----------------------------------------------------------------  -000203-
-Status-----------------------------------------------------------------------
| Detected new network "WaveLAN Network" bssid 00:02:2D:22:86:C1 WEP N Ch 10 @ |
| Detected new network "WLAN" bssid 00:90:D1:00:D9:57 WEP N Ch 11 @ 11.00 mbit |
| Detected new network "CPT_Wireless" bssid 00:02:2D:0D:D4:C0 WEP N Ch 1 @ 11. |
| Detected new network "linksys" bssid 00:04:5A:DD:56:0F WEP N Ch 2 @ 11.00 mb |
------------------------------------------------------------------------------
```

Runs on:
Linux Laptops
& PDAs

WLAN Signal Strength

RF signal propagates far outside buildings housing APs



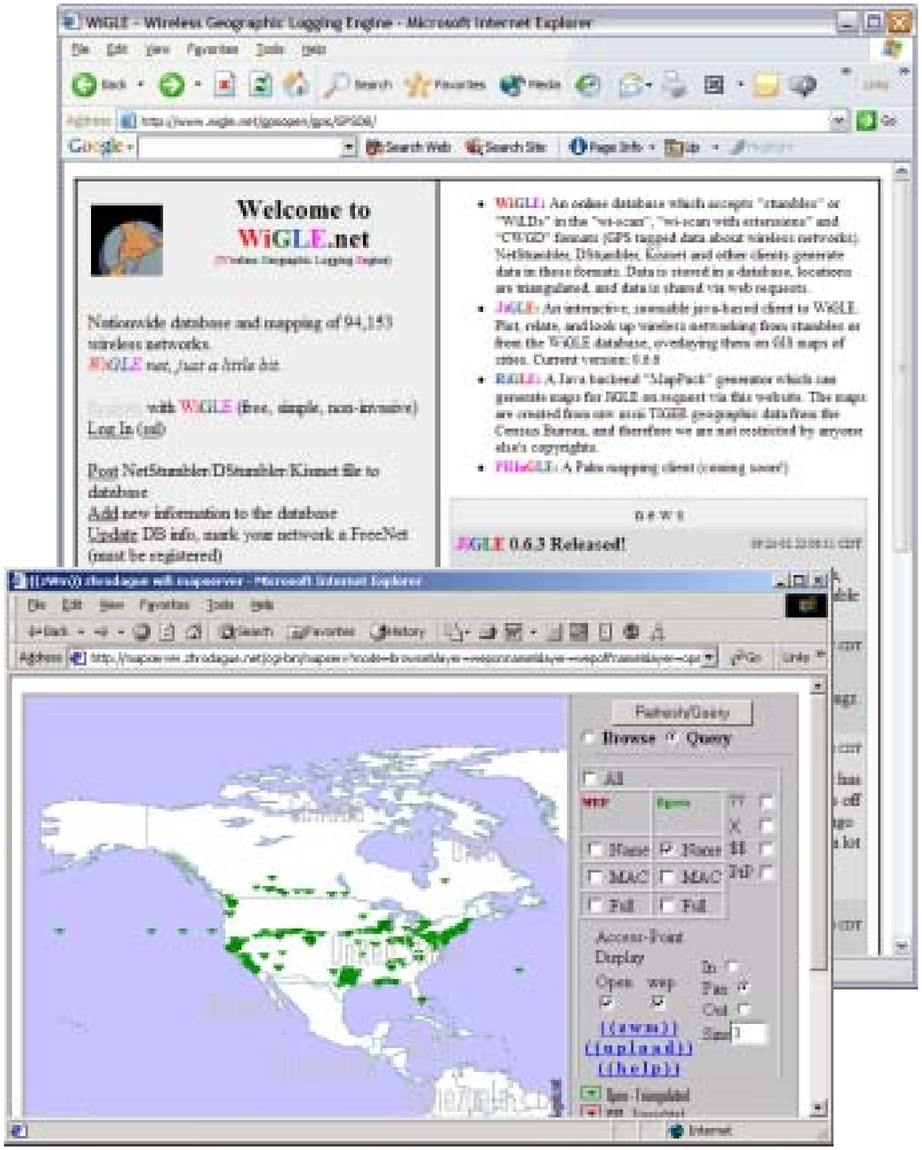
Building housing AP

AirDefense

Is Your Organization a Hot Spot?

- It could be your network!

http://www.wigle.net
http://www.netstumbler.org
http://mapserver.zhrodague.net/
http://www.freenetworks.org/
http://www.nodedb.com/unitedstates/?
http://www.hotspot.nl
http://www.airshare.org
http://www.amsterdamwireless.net
http://www.itee.uq.edu.au/~mesh/db2/
http://www.shmoo.com/gawd/
http://www.wifinder.com/



WiGLE - Wireless Geographic Logging Engine - Microsoft Internet Explorer

Welcome to WiGLE.net
(Wireless Geographic Logging Engine)

Nationwide database and mapping of 94,153 wireless networks.
WiGLE net, *just a little bit.*

Register with WiGLE (free, simple, non-invasive)
Log In (nil)

Post NetStumbler/DStumbler/Kismet file to database
Add new information to the database
Update DB info, mark your network a FreeNet (must be registered)

- WiGLE: An online database which accepts "stumbles" or "WiLDs" in the "wi-scan", "wi-scan with extensions" and "CWGD" formats (GPS tagged data about wireless networks). NetStumbler, DStumbler, Kismet and other clients generate data in these formats. Data is stored in a database, locations are triangulated, and data is shared via web requests.
- JiGLE: An interactive, zoomable java-based client to WiGLE. Plot, relate, and look up wireless networking from stumbles or from the WiGLE database, overlaying them on GIS maps of cities. Current version: 0.6.3
- RiGLE: A Java backend "MapPack" generator which can generate maps for JiGLE on request via this website. The maps are created from raw .e00 TIGER geographic data from the Census Bureau, and therefore we are not restricted by anyone else's copyrights.
- PiGLE: A Palm mapping client (coming soon!)

news

JiGLE 0.6.3 Released!

zhrodague wifi mapserver - Microsoft Internet Explorer

802.11 Devices Beacon You…

Hardware is friendly

- Laptops
- PDAs
- Any Wireless device

Microsoft XP - Most WiFi friendly OS

AirDefense

Converting a Laptop into Malicious AP

Host AP

- Intersil firmware supports Host AP mode
- Freeware
- Hacker Laptop becomes an AP

Blocking Intruders with MAC Filtering

What is it?

List of Valid MAC addresses for an AP

- ## Why is it used?

  Limits associations to AP to ones in list

- ## Limitations

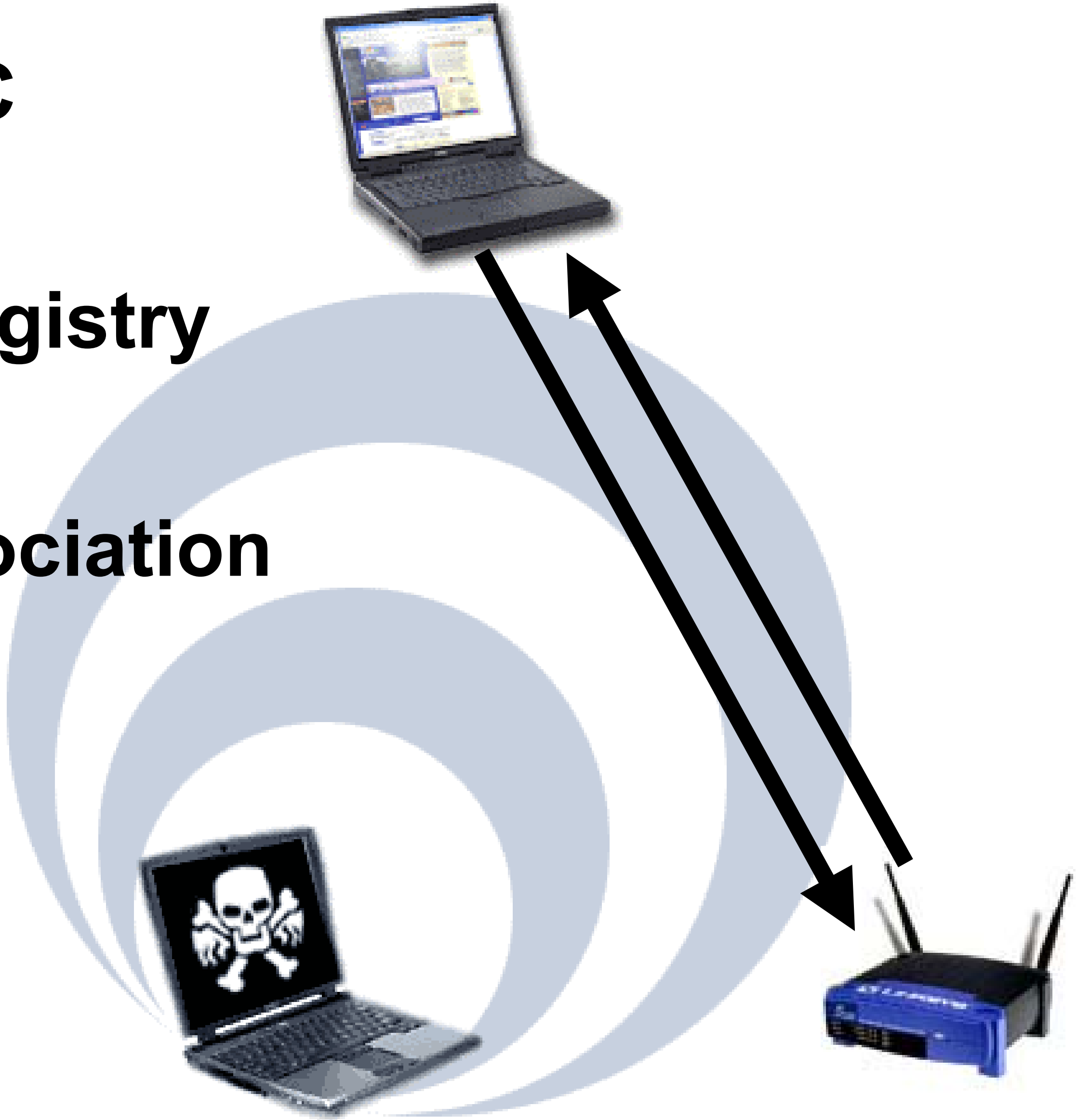
  MAC addresses can be spoofed easily

MAC Address Spoofing - Stations

- Finding the MAC

- Updating the Registry

- Making the Association



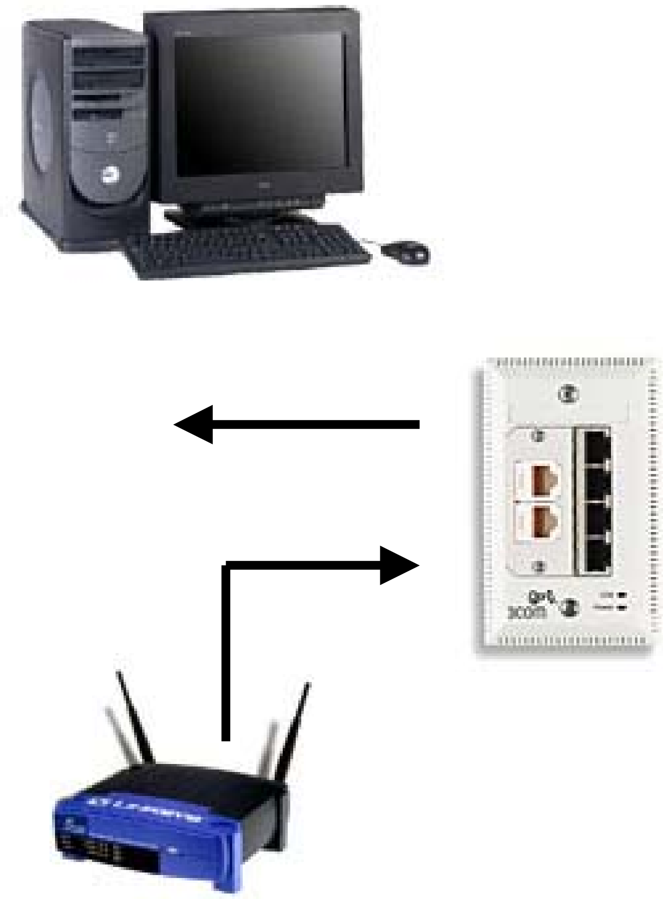
AirDefense

MAC Address Spoofing - APs

1. Unplug Workstation

2. Copy / Clone MAC to AP

3. Insert AP into Network



AirDefense

RADIUS Authentication for the Enterprise

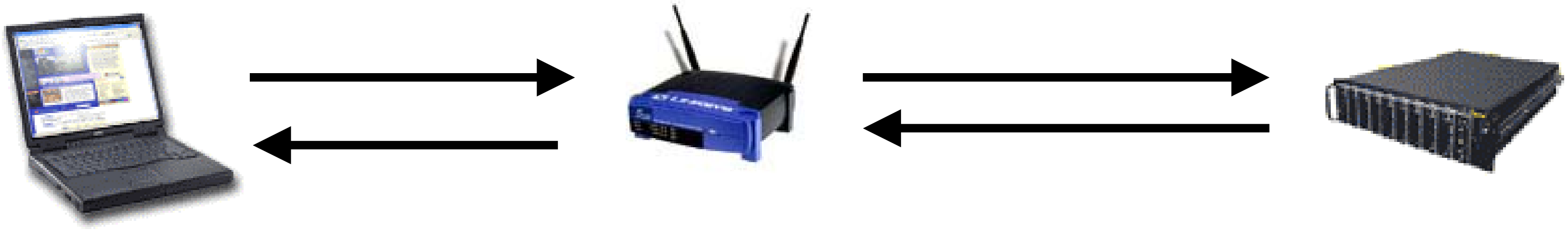
- **What is it?**

  Protocol and Server for remote user authentication

- **Why use it?**

  Central management of authentication

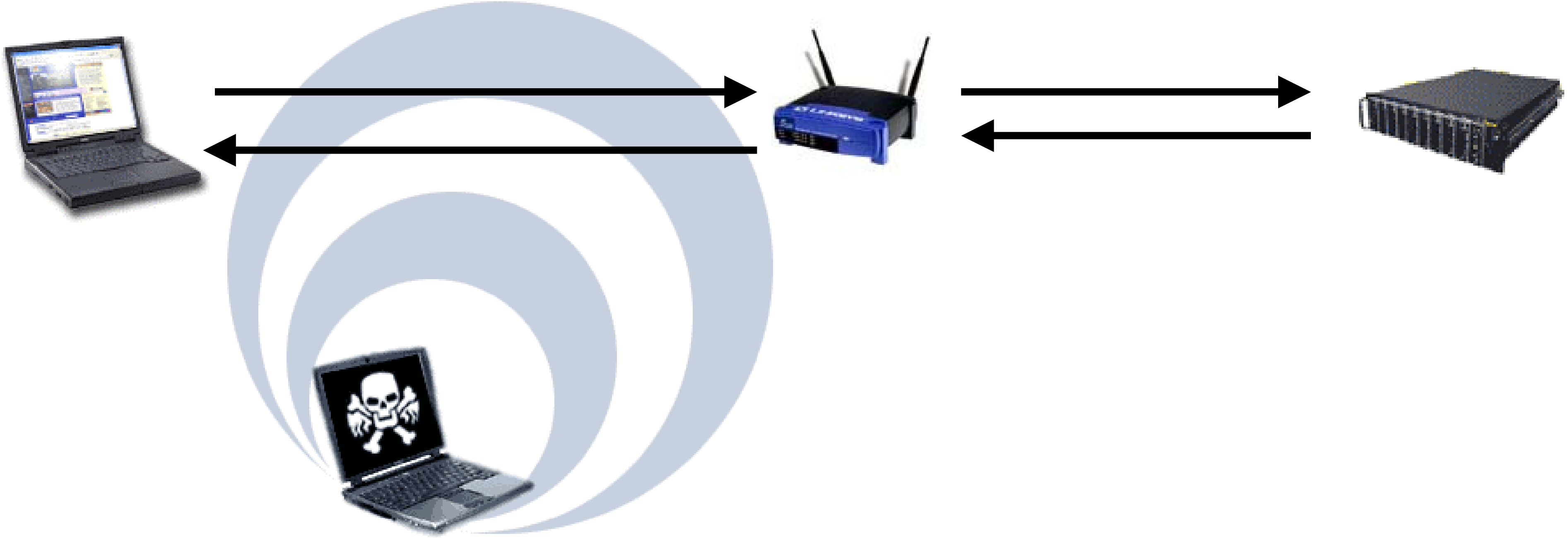
- **How does it work?**



AirDefense

RADIUS Authentication: How Secure is it?

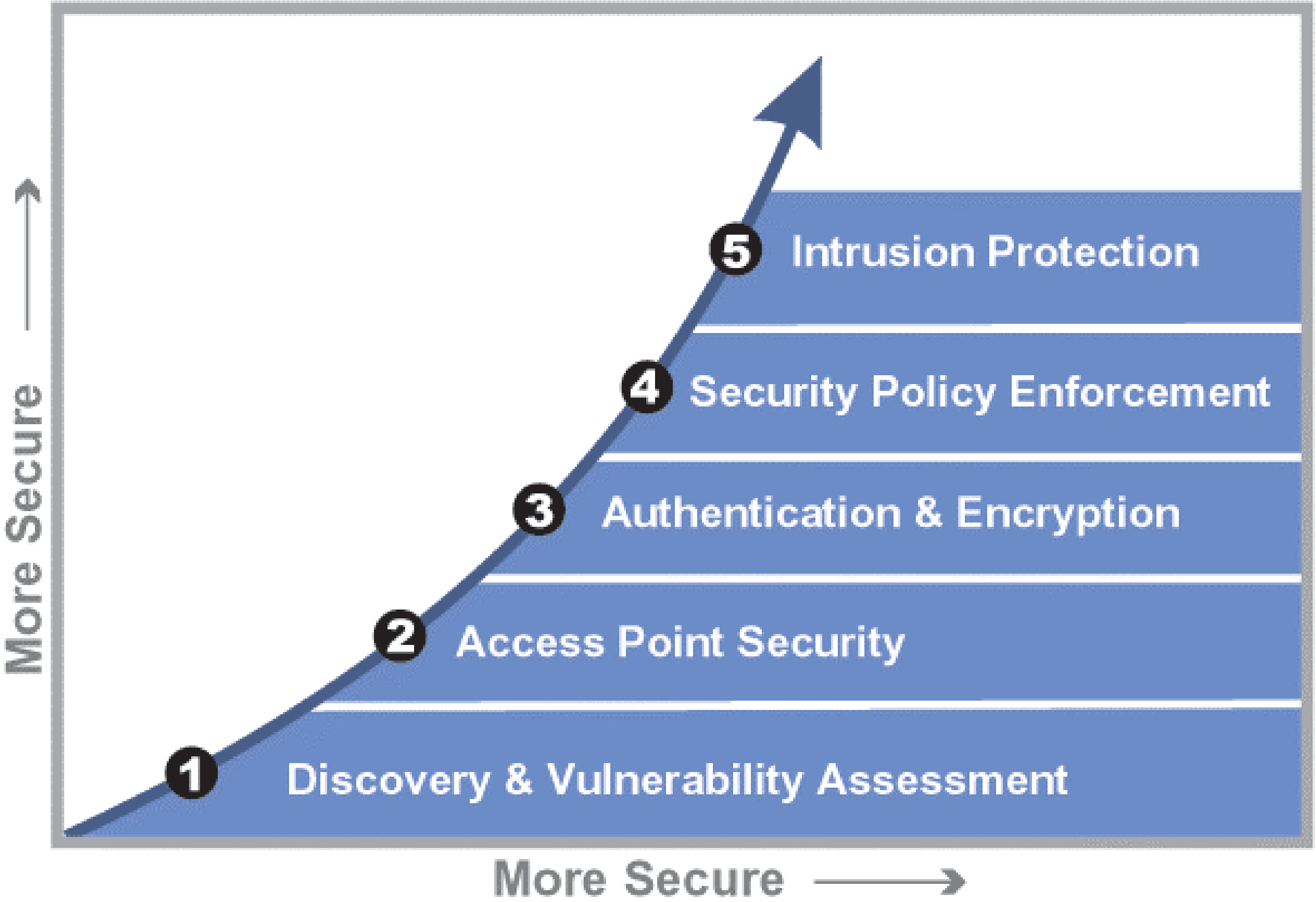
- **Man-in-the-Middle (MIM) Attack**



AirDefense

Securing Your Wireless LAN - Implementing a Layered Approach

Five Practical Steps to Secure Your WLAN


5 Intrusion Protection
4 Security Policy Enforcement
3 Authentication & Encryption
2 Access Point Security
1 Discovery & Vulnerability Assessment
More Secure
More Secure

AirDefense

AirDefense™
Enterprise Wireless LAN Security

Wireless LAN Security

Fred Tanzella
Chief Security Officer
AirDefense

ftanzella@airdefense.NET

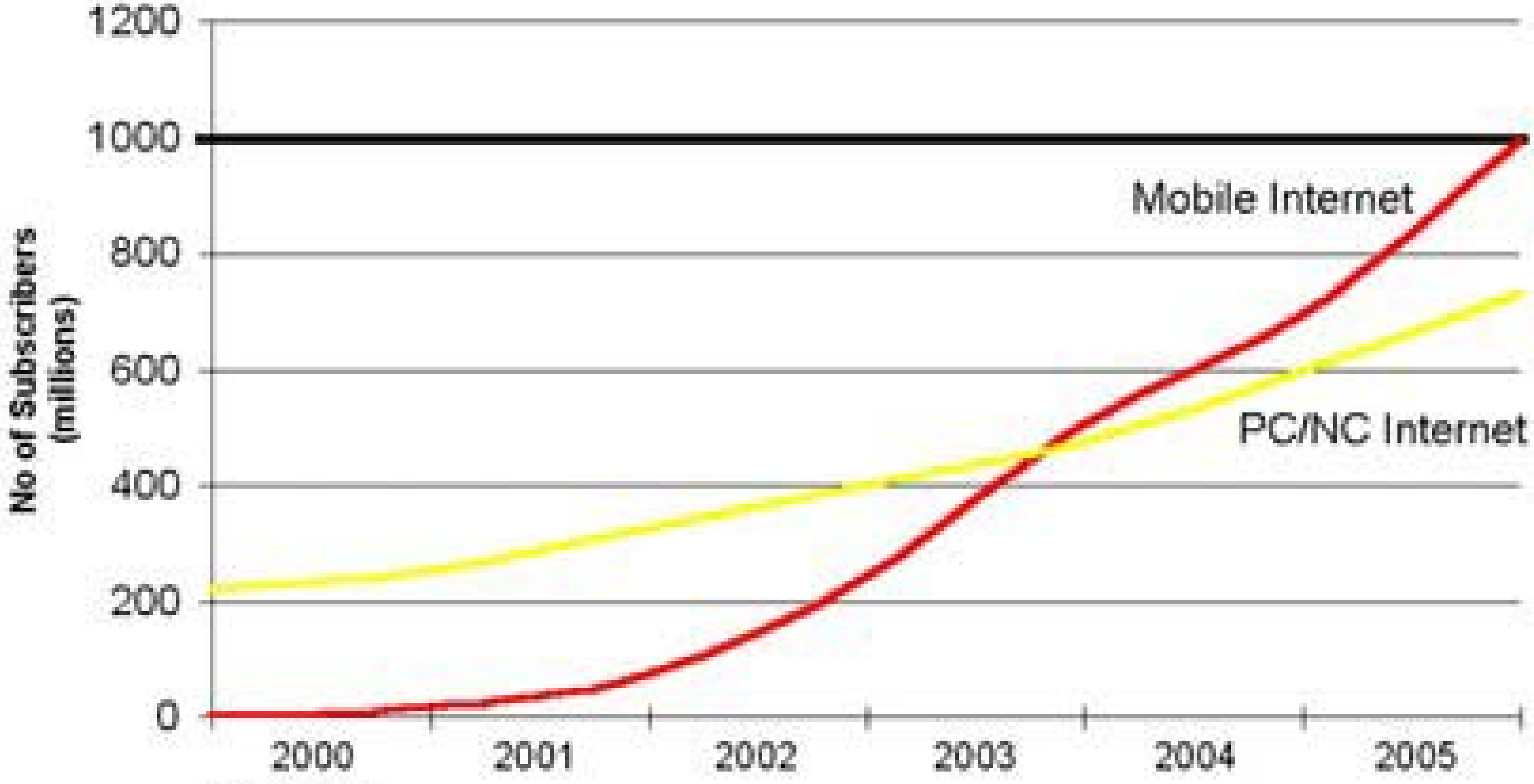
October 2002

WAN Wireless Security - PCS Model

Presentation to Comnet 2003

Stephen C. Swartz
Technical Application Manager
FedGov
Sprint - PCS Division
SSwart03@sprintspectrum.com

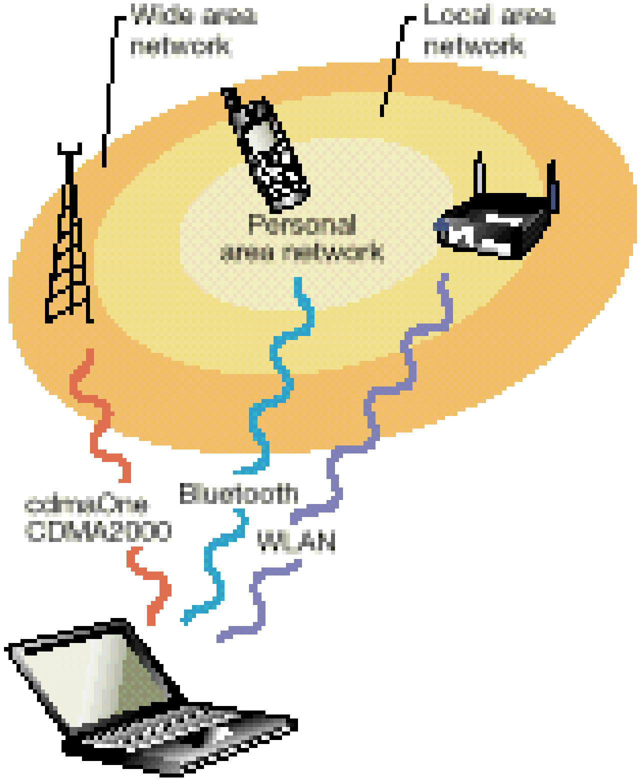
Worldwide Internet Users



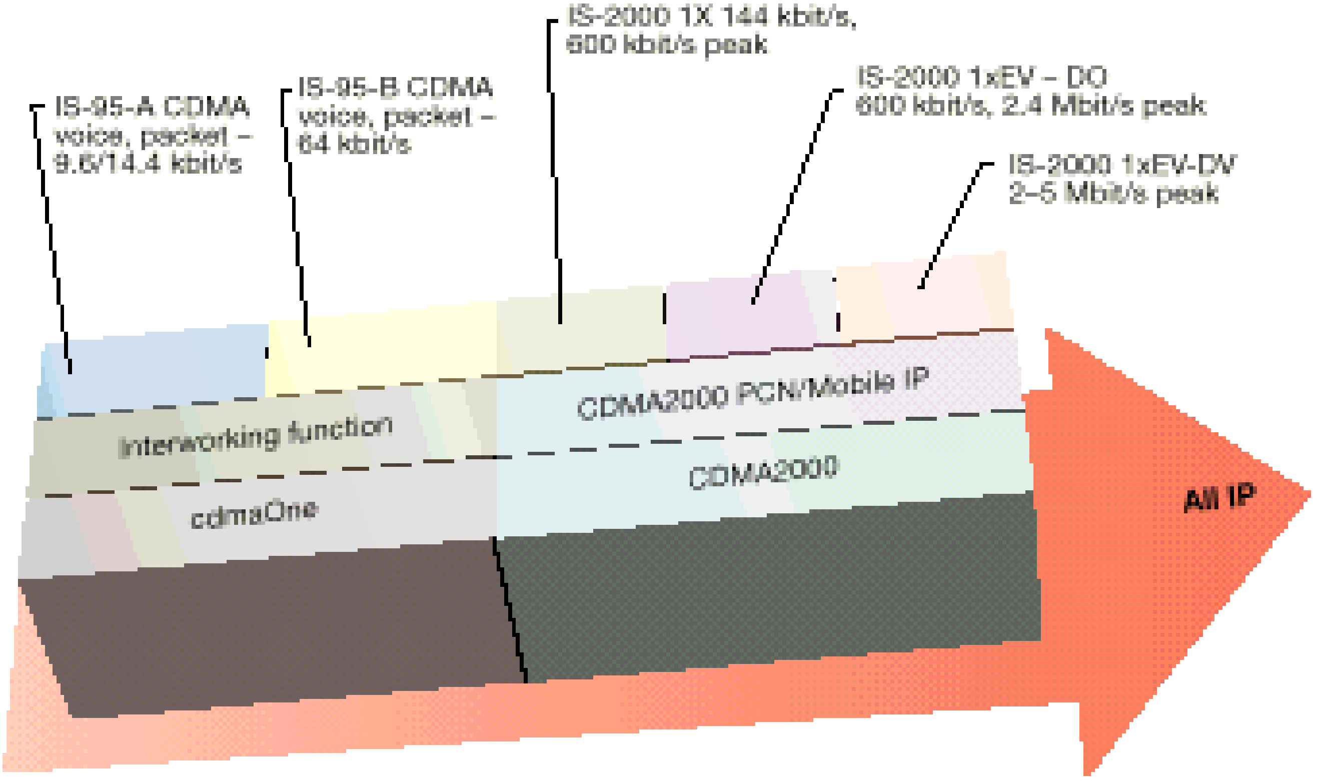
Source: Ericsson

Wireless Realms

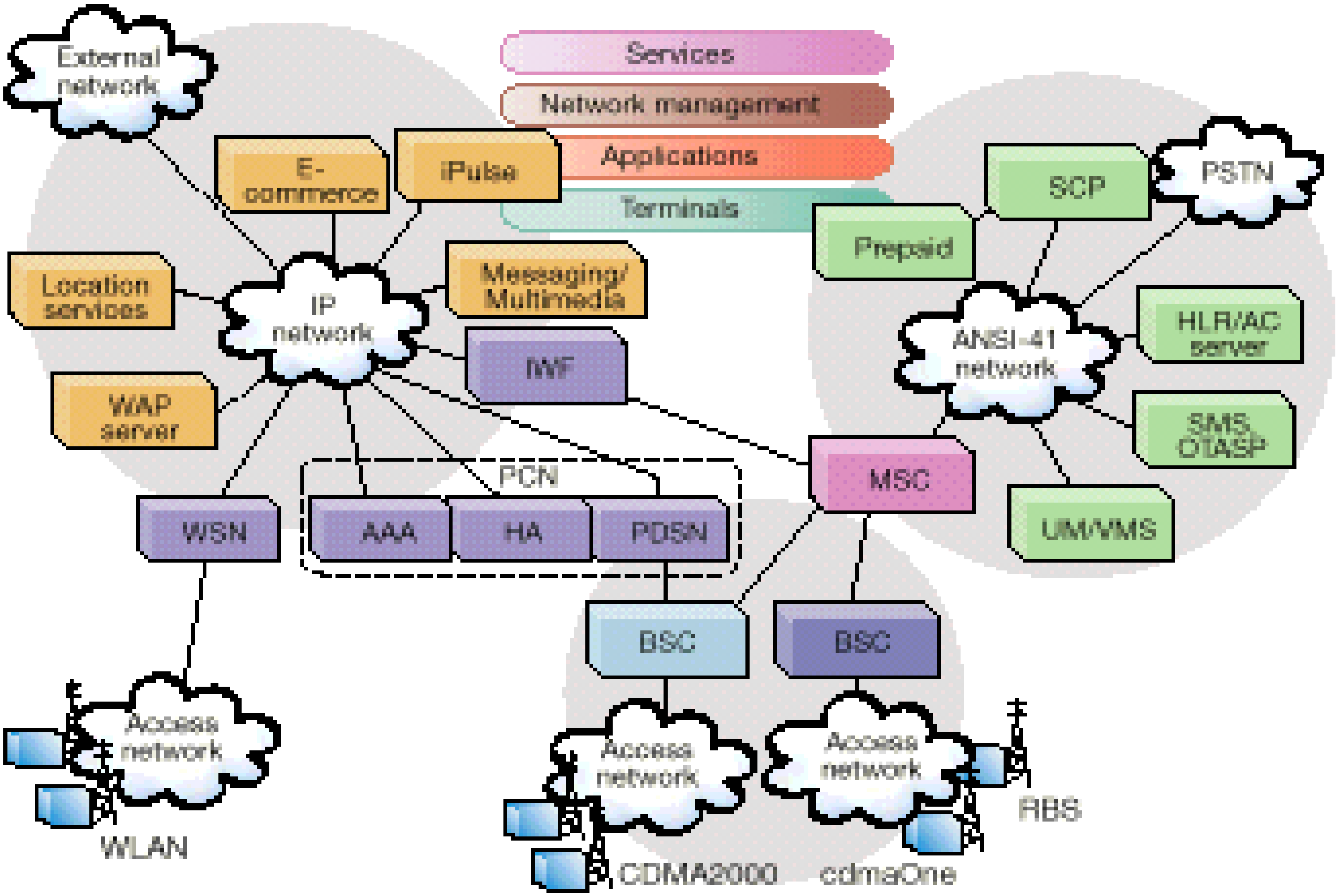
- PAN - Bluetooth - “arms reach”
- LAN - 802.11x - building/campus
- MAN - Sonet - ~20 miles radius
- WAN - PCS/CDMA- national/global



Global Evolution of CDMA Platform


IS-95-A CDMA voice, packet – 9.6/14.4 kbit/s
IS-95-B CDMA voice, packet – 64 kbit/s
IS-2000 1X 144 kbit/s, 600 kbit/s peak
IS-2000 1xEV – DO 600 kbit/s, 2.4 Mbit/s peak
IS-2000 1xEV-DV 2–5 Mbit/s peak
Interworking function
CDMA2000 PCN/Mobile IP
cdmaOne
CDMA2000
All IP

Combined Network Model



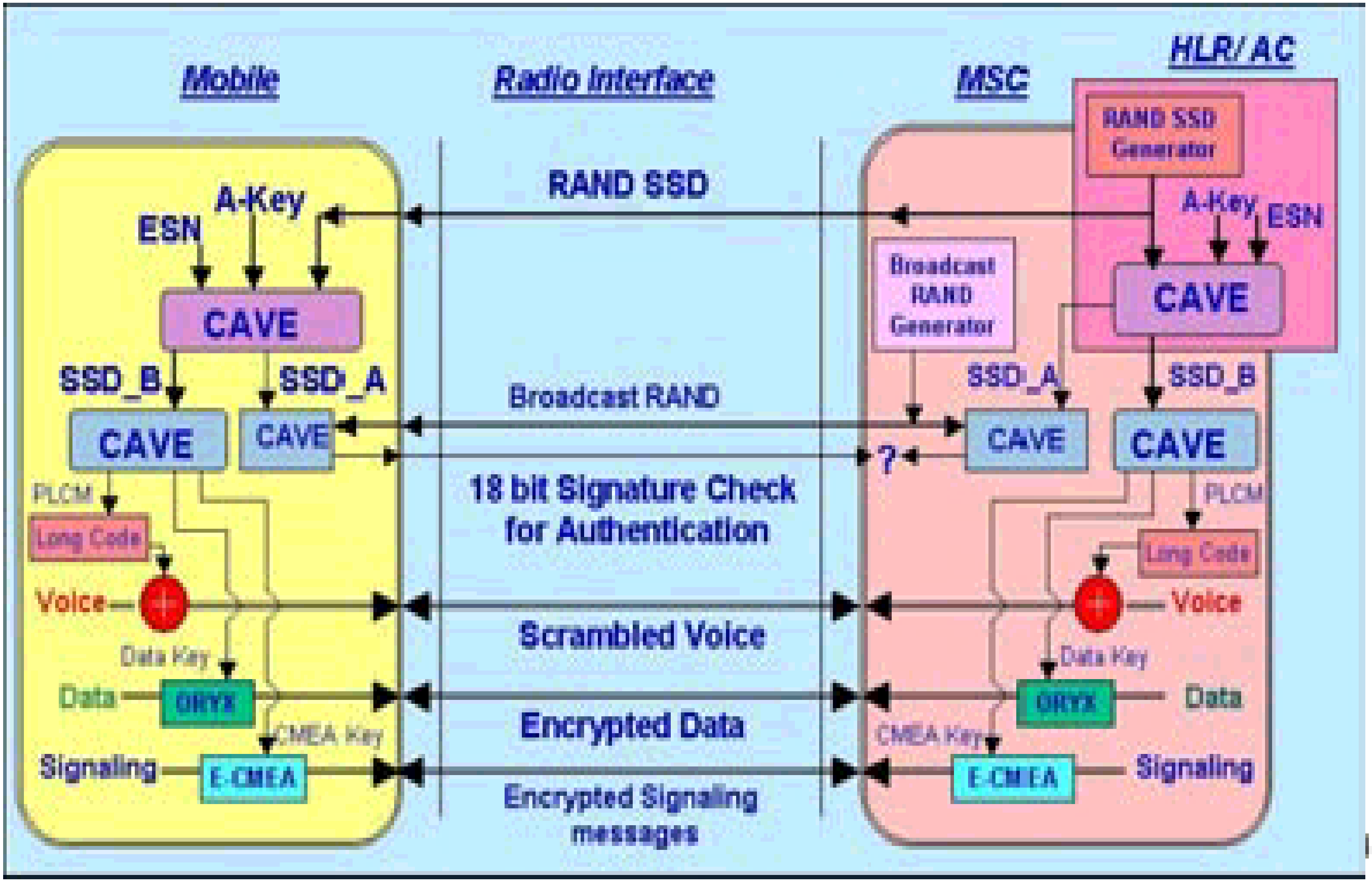
Required Features for Mobile Telecommunications (per Tr45.2)

- User authentication & cipher - both cckt & packet mode
- Terminal Identity including stolen or non-approved detect
- User - Network mutual authentication
- Service dependent authentication & ciphering
- Control over net misuse by unauthorized users
- Ciphering of radio interface
- Lawful Interception
- Privacy of user data, billing data and user messages
- Authentication negotiation of user - serving, and home networks

3G Attacks & Required Equipment

- **Evesdropping - modified MS (mobile station)**
- **Impersonation of a User - modified MS**
  - Identity catching passive or active
- **Impersonation of the Network - modified BS (base station)**
  - suppressing encryption (go into non cypher mode)
  - Compromised cypher key
- **Man-in-the-middle - modified MS & BS**
- **Compromising authentication vectors in the network :**
  - challenge/response pairs, cipher keys and integrity keys
- **Denial of Service:**
  - User deregistration request spoofing - mod MS
  - Location Update request spoofing - mod MS
  - Camping on false BS - mod BS

3G authentication and security



Source: Qualcomm

OTA interface security features of 3G CDMA 1x

- **operates at OSI layer 2 (Media Access Component)**
- **Path Diversity- soft handoff & multiple access via Rake rcvr**
- **Signal levels often below “noise” level (neg 95)**
- **Spread spectrum transmission**
  - 42 bit “pseudorandom” noise - the Long Code - scrambles voice and data transmission

OTA interface security features of 3G CDMA 1x -cont

- User authentication
  - "A" key loaded at 1) factory, 2) dealer, 3)OATSP [utilizing 512 bit Diffie - Hellman key]
  - 64 bit "A key" + ESN +RANDSSD (random number from HLR) used to generate SSD (Shared secret data - 128 bit) two part code
    - SSD_A for authentication signatures
    - SSD_B for key generation

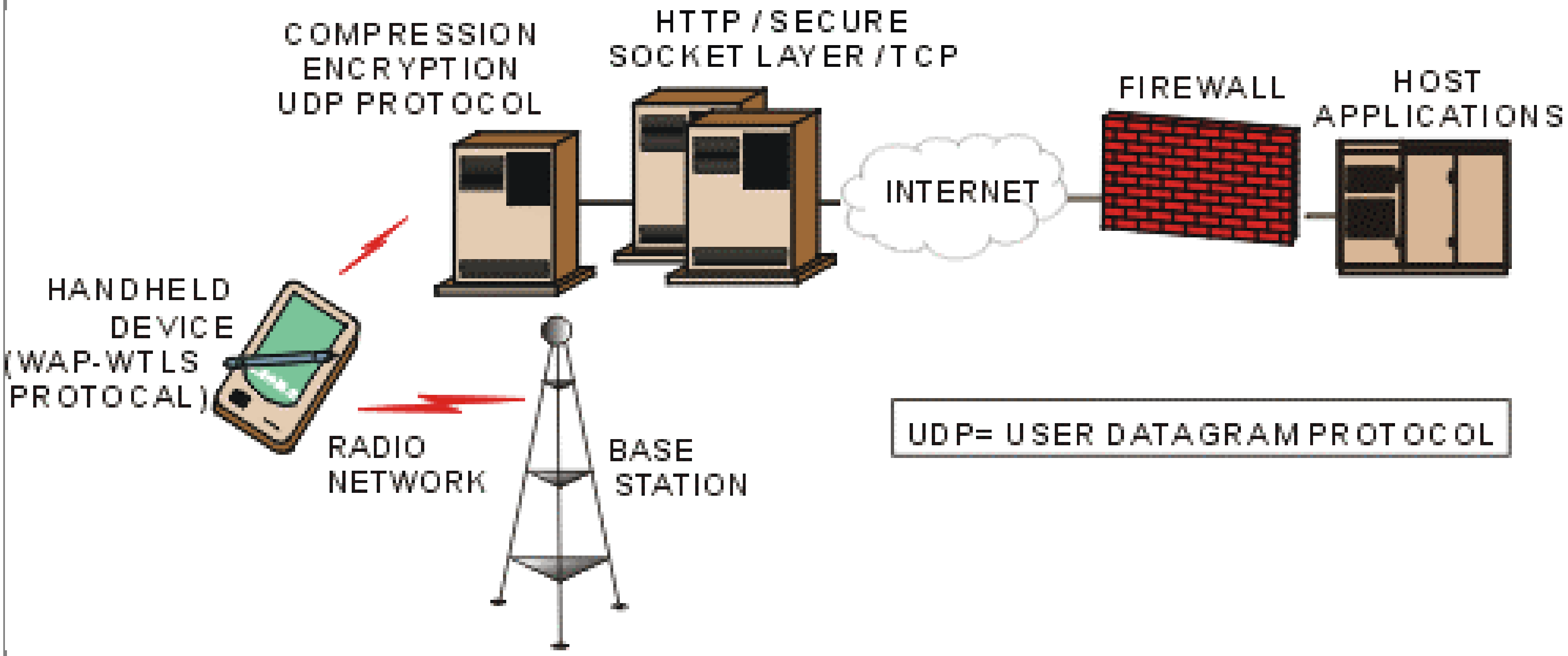
Voice & Data Privacy

- Private Long Code Mask modifies long code - unique to individual mobile - network connection
- CMEA key (64 bit) encrypts signaling
- Data key (32 bit) + ORYX encryption algorithm for data

New Releases of CDMA2000 (after release C) feature:

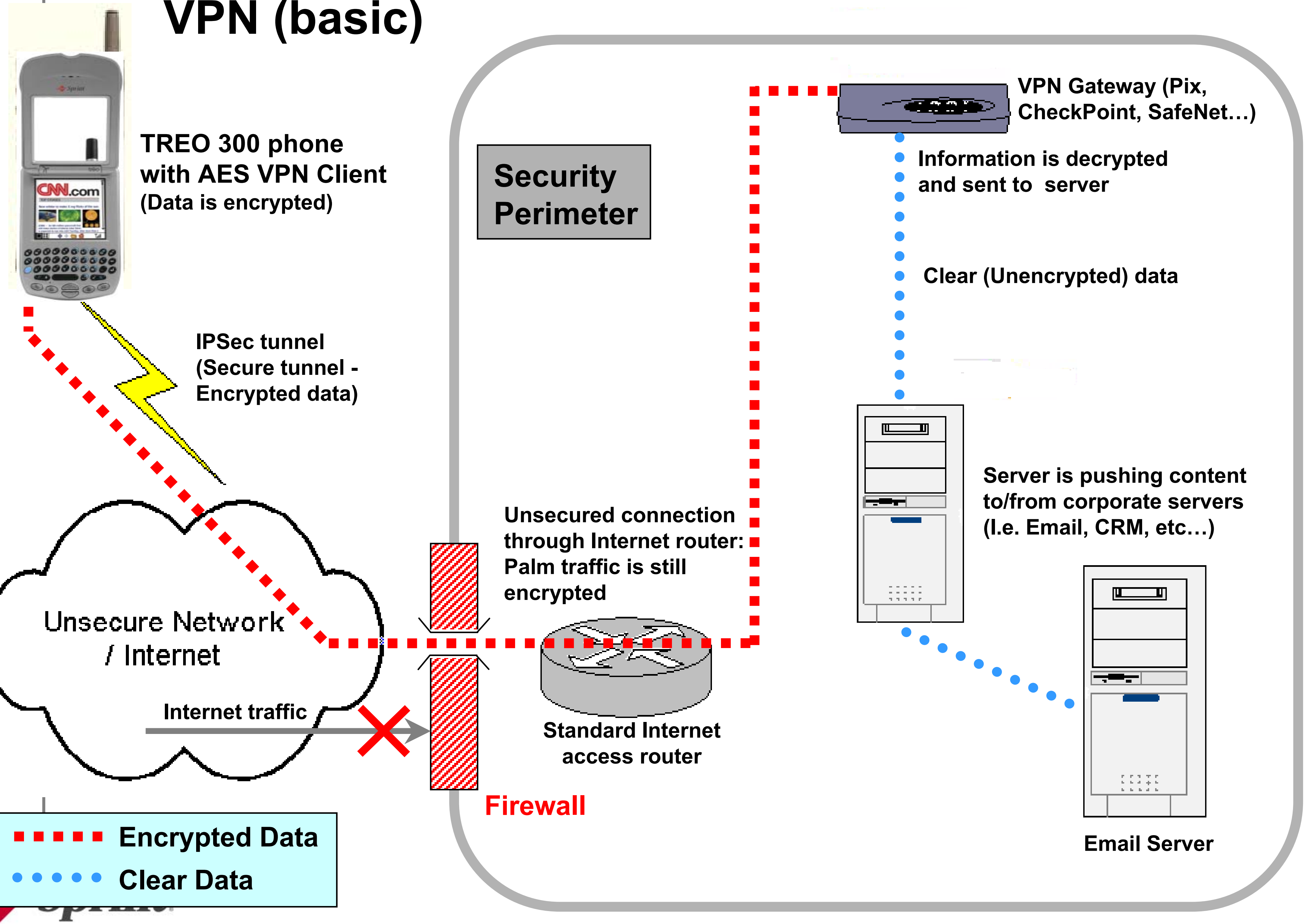
- SHA-1 secure hashing algorithm
- AES (Rijndael) for message encryption
- AKA authentication & Key Agreement
- 128 privacy and authentication keys

WAP / WTLS Non-Critical “Security”



UDP= USER DATAGRAM PROTOCOL

VPN (basic)



TREO 300 phone
with AES VPN Client
(Data is encrypted)

IPSec tunnel
(Secure tunnel -
Encrypted data)

Unsecure Network
/ Internet

Internet traffic

Firewall

Security
Perimeter

Unsecured connection
through Internet router:
Palm traffic is still
encrypted

Standard Internet
access router

VPN Gateway (Pix,
CheckPoint, SafeNet…)

Information is decrypted
and sent to server

Clear (Unencrypted) data

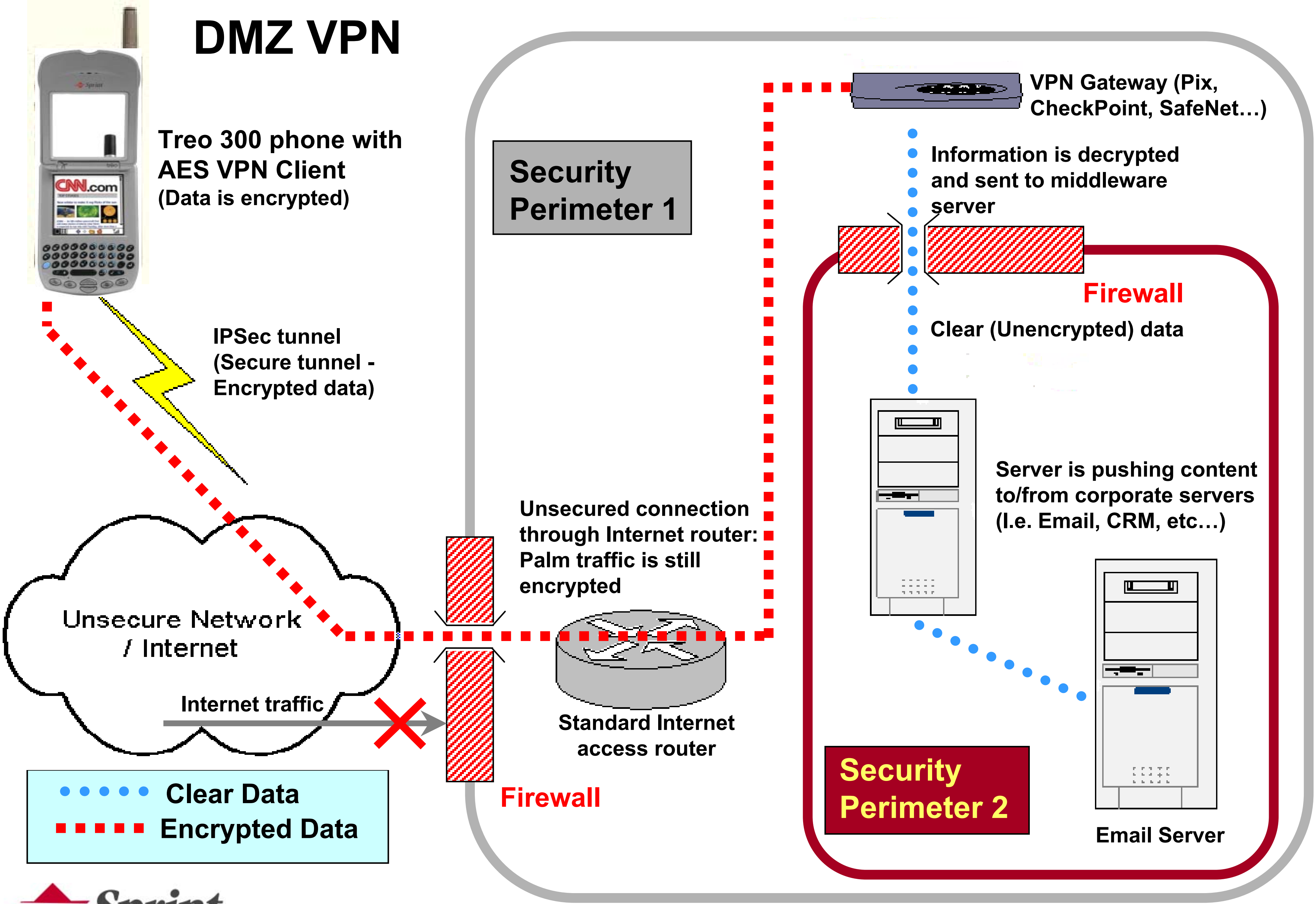
Server is pushing content
to/from corporate servers
(I.e. Email, CRM, etc…)

Email Server

■ ■ ■ ■ ■ Encrypted Data

● ● ● ● ● Clear Data

DMZ VPN



Treo 300 phone with AES VPN Client (Data is encrypted)

IPSec tunnel (Secure tunnel - Encrypted data)

Unsecure Network / Internet

Internet traffic

Unsecured connection through Internet router: Palm traffic is still encrypted

Standard Internet access router

Firewall

Security Perimeter 1

VPN Gateway (Pix, CheckPoint, SafeNet…)

Information is decrypted and sent to middleware server

Firewall

Clear (Unencrypted) data

Server is pushing content to/from corporate servers (I.e. Email, CRM, etc…)

Security Perimeter 2

Email Server

● ● ● ● ● Clear Data

■ ■ ■ ■ ■ Encrypted Data

Questions?