



HERVÉ SCHAUER CONSULTANTS
Network security consulting agency since 1989
Specialized in Unix, Windows, TCP/IP and Internet

Wireless LAN Security

ECMWF
11th Member State Security Representatives' meeting
May 15, 2003



Hervé Schauer
<Herve.Schauer@hsc.fr>

- Introduction
- Advantages and benefits of wireless LANs
- Threats with Wireless LANs
- WLAN security standards
- SSID
- 802.11 protocol

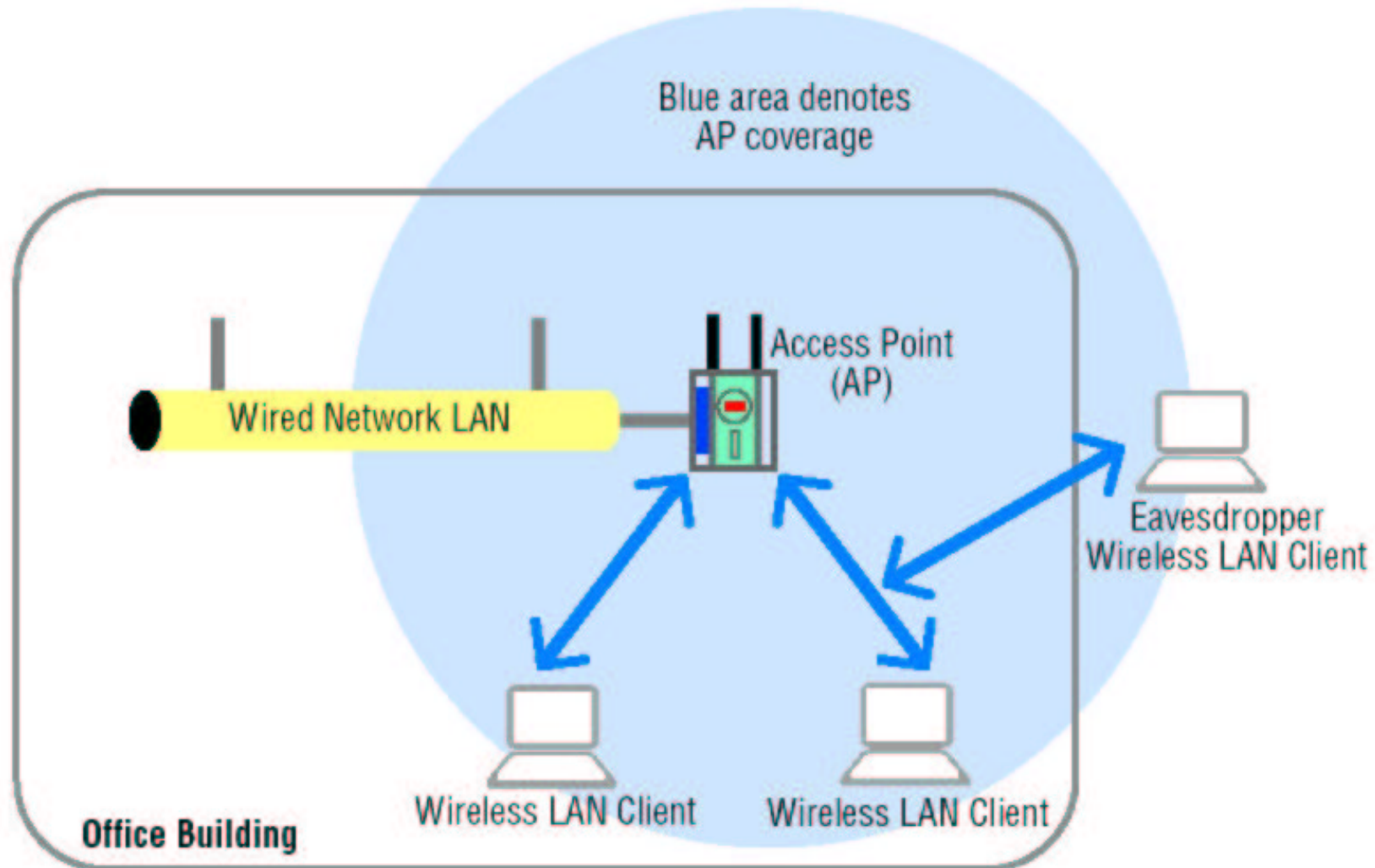
- Building Secure Wireless LANs
 - × Managment
 - × Segmentation
 - × 802.1X authentication
 - × Framework, Synoptic, Pre-requisites
 - × Integration Architecture
 - × Corporate networks
 - × Service Providers
 - × Audit Wireless LANs
 - × Example with WifiScanner
- Conclusion
- Ressources and thanks

- Network components
 - × Access Point : Bridges wireless client to the wired Ethernet network
 - × STP (spanning tree, IEEE 802.1d) dynamic topology
 - × Broadcast traffic like a hub
 - × Clients or Stations
- Two modes
 - × *Ad-hoc* : direct connection between two WLAN interfaces of stations
 - × *Infrastructure* : connection between AP and stations
- Technology characteristics
 - × Permanently send *beacons* (control frames) 10 times per second
 - × Identify networks with a SSID (*Service Set Identifier*)
 - × Encryption with WEP (*Wired Equivalent Privacy*)

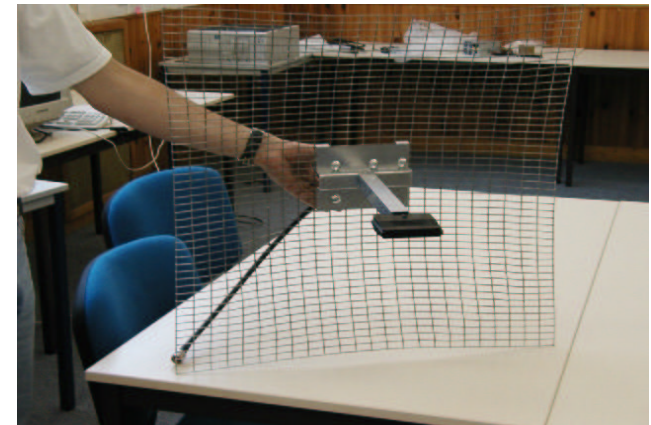
- Installation speed and simplicity
 - × No need to ask anyone
 - × No need to pull cable through walls or add hubs
- Reduced Cost of Ownership
 - × Initial hardware and set-up investment similar to wired LAN
- Scalability and flexibility
 - × Easy to grow and go everywhere
- Mobility and roaming
- Crossing obstacles
- Temporary networks

Threats with wireless LANs

- Attack from outside the organisation



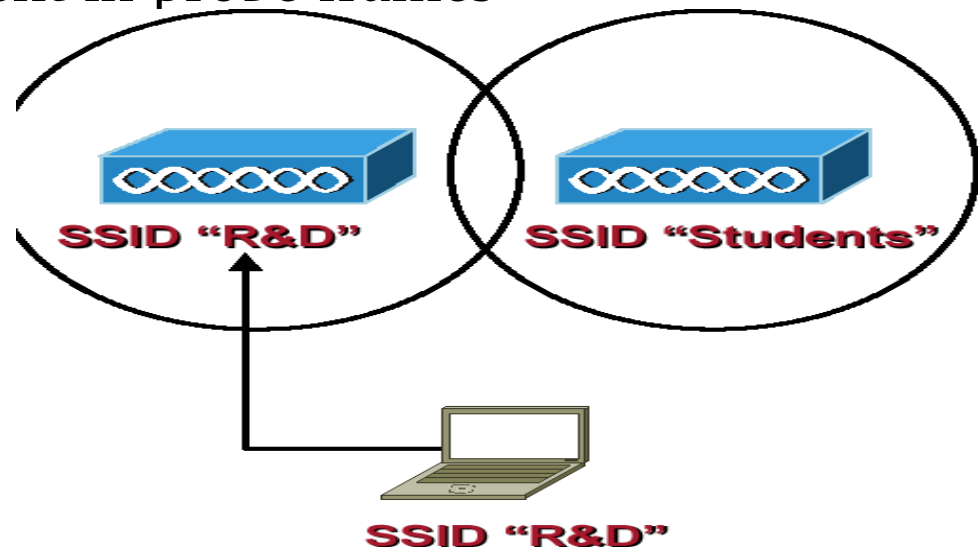
- Unwanted or automatic connection to the wrong network
- Theft of user authentication
 - × Man-in-the-middle attack with a fake AP
 - × Airjack
- Theft of information by illegal tapping of the network
 - × NetStumbler
- Intrusion via the Wireless LANs
- Scrambling of the WLAN
 - × Airjack
- Consumption of device batteries



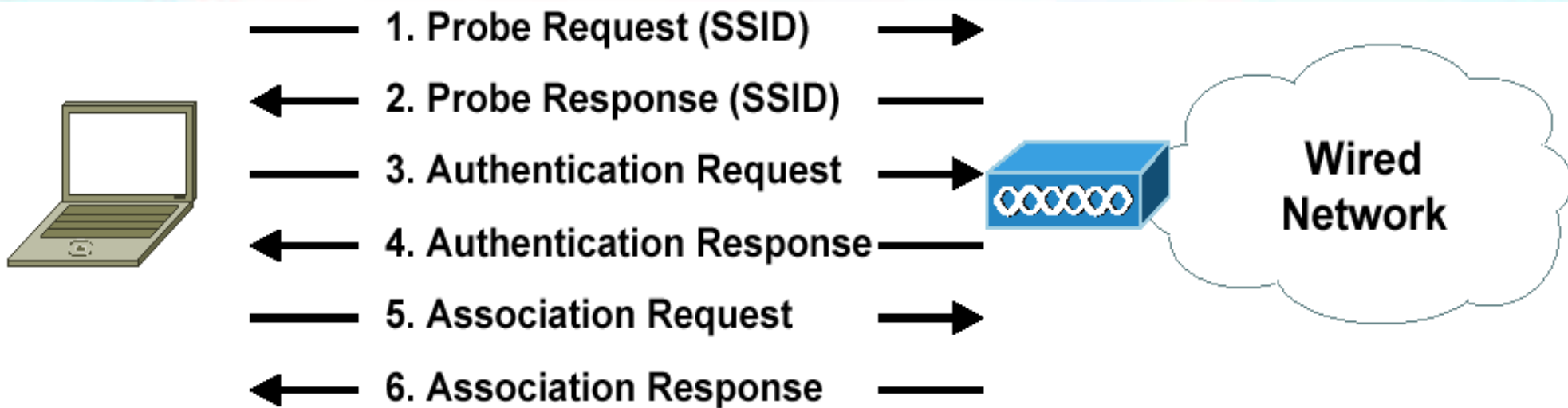
- IEEE 802.11g standard: 54 Mbits/s on 2.4 Ghz
 - × Approved by the working group in February 2003
- IEEE 802.11i standard: security in 802.11* networks
 - × Use IEEE 802.1X port access control (April 2001)
 - × CCMP (*Counter-Mode/CBC-MAC Protocol*)
 - × TKIP (*Temporal Key Integrity Protocol*)
 - × Dynamic key generation for WEP (*Wired Equivalent Privacy*)
 - × WRAP (*Wireless Robust Authenticated Protocol*)
 - × Key management specific to IEEE and replacement of RC4 by AES
 - × Rely on IETF EAP and Radius standards
 - × Synchronisation and coherence need time
- Security issues of 802.11b (Wi-Fi) are solved with this new generation
- Security remains a **voluntary choice** : it must be configured

HSC SSID

- Not a security feature : identification only
- 32 ASCII character string always sent in clear text
- Logically separate wireless LANs or wireless VLANs
- May be advertised by the AP in beacon frames
 - × Must be advertised by APs for public *Hot-Spots* with a clear name
- May be also advertised by the client in probe frames
 - × Save/Resume
 - × Windows XP
- Can be selected on the station



- 1) Manage WLANs
- 2) Segment WLANs from Corporate wired infrastructure
- 3) Authenticate users
 - × Will enable keys management for WEP encryption over the WLAN
- 4) Audit and own your airspace

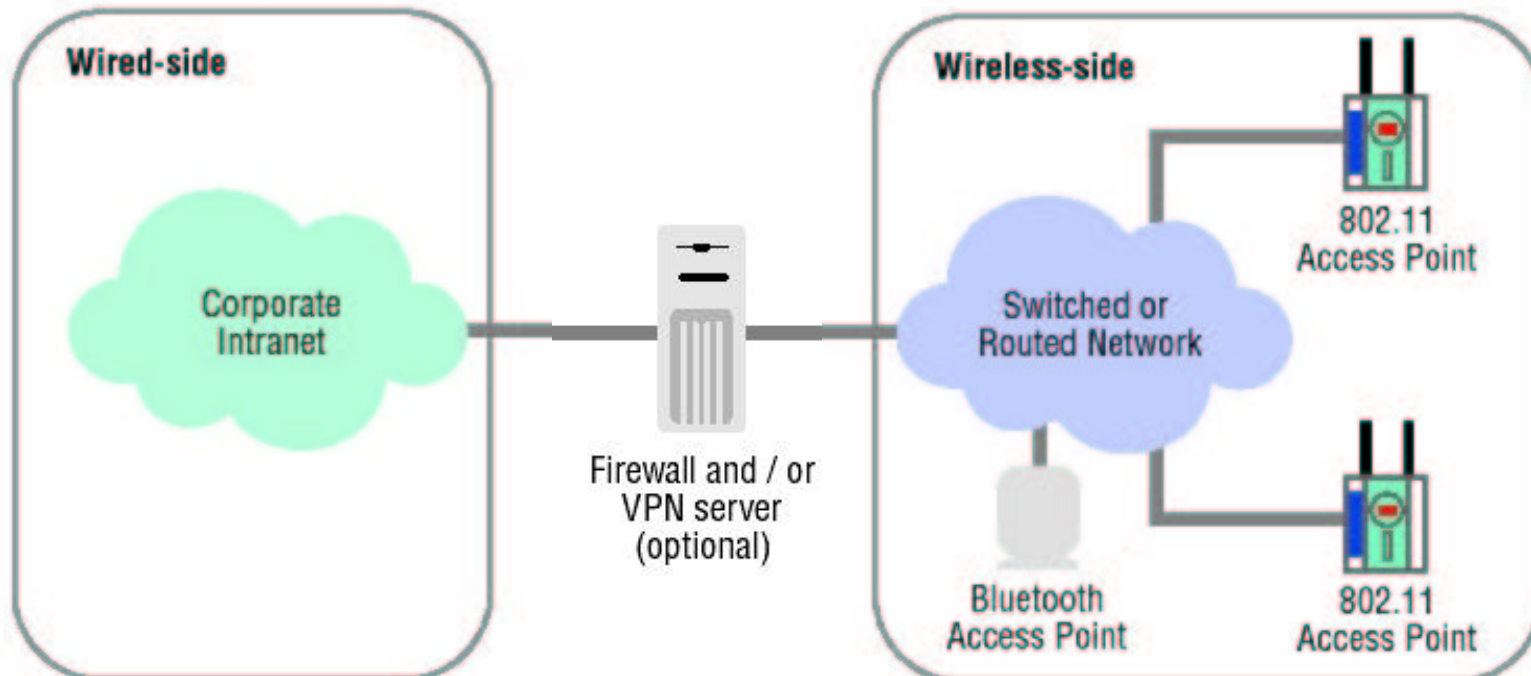


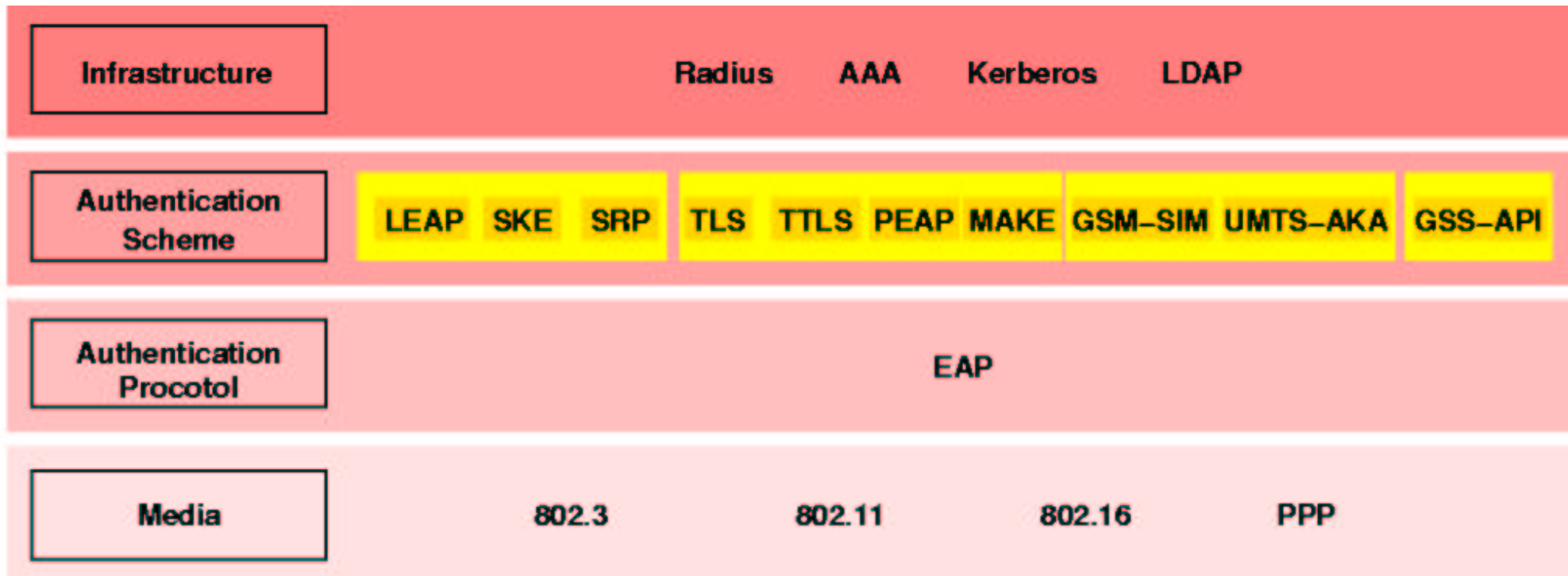
- Beacons include SSID, all network and AP characteristics (WEP, etc)
- 802.11 authentication is a formality
 - × Implies 4 exchanges, but network access always open (*null-authentication*)
 - × User's authentication to 802.11 network will be done with 802.1X
- After association, the client is connected to the WLAN

- Consider Access Points as part of your perimeter security
 - × Managed as you manage firewalls
 - × Skilled team, aware of security
- Explain to employees why WLAN security is a key issue
 - × Avoid rogue APs
 - × Get them warn you for any wireless connection without authentication
- Add WLAN security to your corporate Security Policy
 - × ISO17799 (12/2000) ignore wireless networks
- Look at your business needs and explore alternative solutions
- Use security features of APs
 - × MAC addresses filtering, 128 bits (104) encryption, VLANs

Segmentation of Wireless LANs

- Segment wireless network with a firewall from corporate network
- Enforce access control to the wireless network
- Authentication of hosts to access the wireless LAN is done by the network
 - × IEEE 802.1X standard: access control based on port authentication

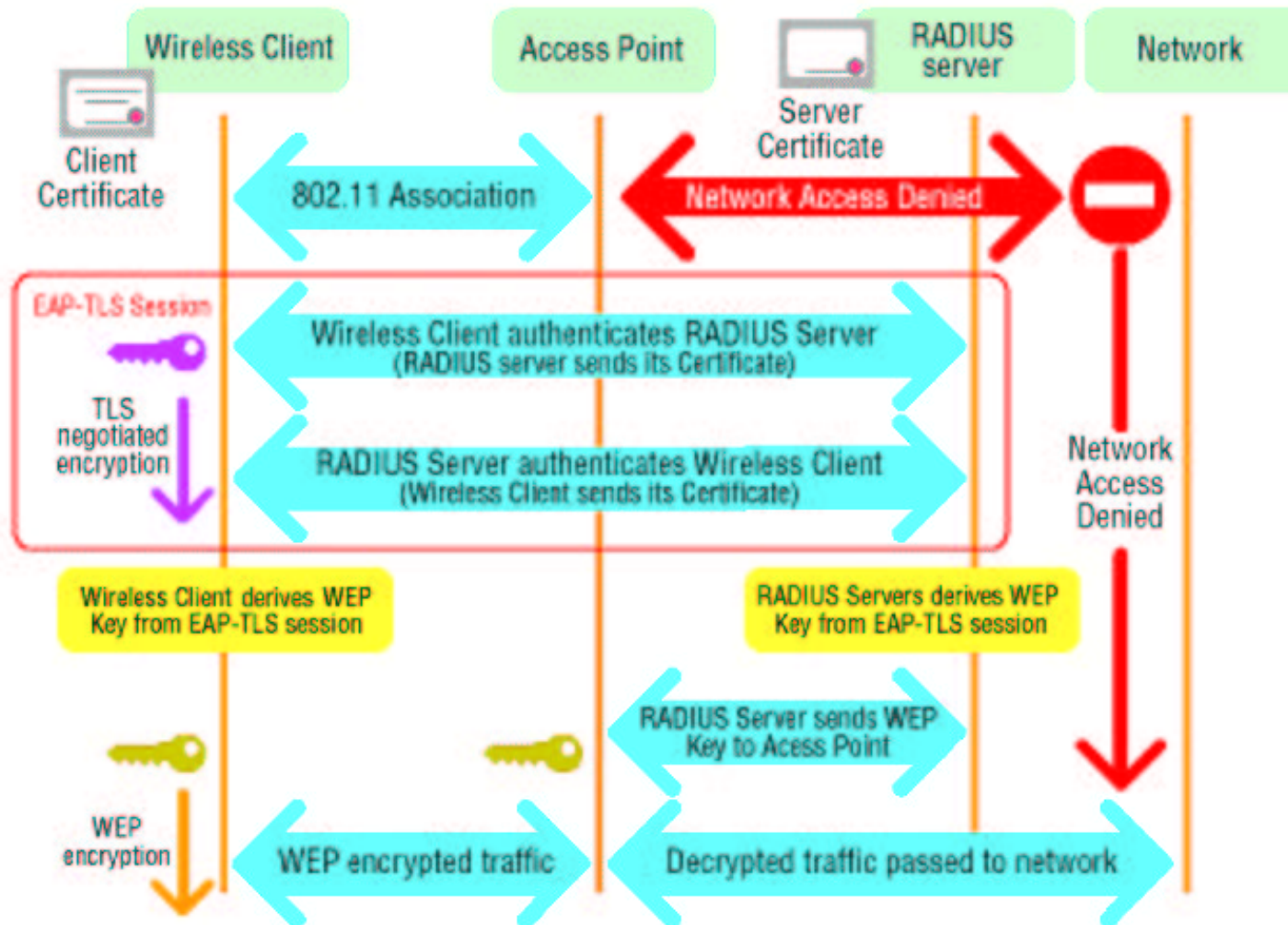




© Copyright Hervé Schauer Consultants 2002

- Authentication schemes for corporate networks
 - × Past : LEAP, Present : EAP-TLS, Future : PEAP
- × Authentication schemes for Wireless Internet Service Providers
 - × Present : password + HTTP/HTTPS highjacking, Future : EAP-SIM

802.1X synoptic with EAP-TLS



- AP opens port only for EAPOL traffic
- AP transforms EAPOL in EAP over Radius
- Client start TLS session to Radius server
- Successful authentication, AP receives WEP key and opens port to any traffic

- Already have or set-up a user service and help-desk department
- Deploy AP supporting 802.1X
- Have or deploy over all client hosts 802.1X authentication
 - × Even when 802.1X is available built-in, the authentication scheme you wish to use may not be
 - × Third-party software is available for all platforms and all authentication schemes
- Manage drawbacks
 - × Much longer connection time to the network for users
 - × 802.1X authentication schemes and roaming do not work together
 - × New work item for standardization

- Corporate networks
 - × Deploy your own IEEE 802.11b/g network architecture
 - × Best way to fight against fake AP and accidental connection to neighbours
 - × Always consider wireless networks as externals
 - × Segment the wireless LAN infrastructure with VLANs
 - × Separate WLAN for enterprise connectivity from WLAN for *HotSpot*
 - × Detect intruders using MAC addresses
 - × Test imperviousness of your wireless VLANs
 - × Work on physical security of waves over space
 - × Tune carefully APs power and appropriately locate antennae
 - × Secure APs and apply security patches
 - × Use switches' learning of MAC addresses to detect intruders
 - × Deploy authentication software over clients
 - × Consider alternative technologies to IEEE 802.11b/g (WiFi)
 - × Networks using electric cable, IEEE 802.15.3 (Bluetooth 2), IEEE 802.11a (WiFi5), IEEE 802.16a, IEEE 802.16b (metropolitan networks)



- *HotSpots* Service Providers
 - × Use authentication schemes based on SIM smartcards (EAP-SIM, EAP-AKA)
 - × In case of HTTP hijack authentication
 - × Use HTTPS
 - × Use one-time passwords
 - × Secure Radius authentication from APs when they cross over the Internet
 - × IPsec encrypted tunnel if AP or local device supports it
 - × Build an out-of-band network infrastructure for authentication and billing – if possible
 - × Segment, as any ISP which keeps its own infrastructure separated from the Internet infrastructure
 - × Do not forget that 802.11 is not designed for sharing several wireless infrastructures at the same place
 - × When you offer Wireless Internet Access : you are a HotSpot provider

- Objectives
 - × Detect unofficial 802.11 wireless LANs
 - × Detect client workstation badly configured or auto-configured
 - × Evaluate security of corporate wireless LANs
 - × Validate access control mechanisms deployed
- Methodology
 - × Walkthrough the audit perimeter with portable equipment
 - × Use of antennae to amplify signal reception
 - × Search of SSID, WEP keys, APs passwords
 - × Pursue with Intrusion Tests
- Auditing tools
 - × Kismet, WifiScanner





WifiScanner - 1

WifiScanner v0.7.0 (14) (c) 2002 Hervé Schauer Consultants (Jerome.Poggi@HSC.FR)

```

>AP 00:40:96:5B:15:9D " "
| STA 00:20:E0:89:08:50 " "
| AP 00:02:2D:36:5E:C8 "toto"
|====|_____ (9,11)
|_____ (0,14)
|_____ (0,22)
Summary
|| AP : 0
|| STA : 0
|| BEACON : 27
|| SSID : 0
|| Channel: 0
|| Invalid: 4
|| Packets: 45
|| Scan :

07/23/2002 09:02:29.426, " ",00,____,STA,007,6,FF:FF:FF:FF:FF:FF,00:20:E0:89:08:50,FF:FF:FF:FF:FF:FF,2Mb/s,Client,Radio only,PRBREQ
07/23/2002 09:02:29.497, " ",00,____,STA,008,5,FF:FF:FF:FF:FF:FF,00:20:E0:89:08:50,FF:FF:FF:FF:FF:FF,2Mb/s,Client,Radio only,PRBREQ
07/23/2002 09:02:29.498, " ",00,____,STA,013,11,FF:FF:FF:FF:FF:FF,00:20:E0:89:08:50,FF:FF:FF:FF:FF:FF,2Mb/s,Client,Radio only,PRBREQ
07/23/2002 09:02:29.573, " ",07,Wep,AP,010,3,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:02:30.577, " ",07,Wep,AP,010,3,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:02:30.717, " ",00,____,STA,009,5,FF:FF:FF:FF:FF:FF,00:20:E0:89:08:50,FF:FF:FF:FF:FF:FF,2Mb/s,Client,Radio only,PRBREQ
07/23/2002 09:02:37.471, " ",07,Wep,AP,010,5,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:02:42.608, "toto",10,____,STA,017,16,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,02:02:2D:36:5E:C8,2Mb/s,Ad-Hoc STA (beacon),Radio only, BEACON
07/23/2002 09:02:45.348, " ",07,Wep,AP,011,5,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:02:48.288, " ",07,Wep,AP,010,3,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:02:49.498, "toto",10,____,STA,014,16,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,02:02:2D:36:5E:C8,2Mb/s,Ad-Hoc STA (beacon),Radio only, BEACON
07/23/2002 09:02:50.502, "toto",10,____,STA,015,15,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,02:02:2D:36:5E:C8,2Mb/s,Ad-Hoc STA (beacon),Radio only, BEACON
07/23/2002 09:03:03.039, " ",07,Wep,AP,008,5,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:03:04.230, "toto",10,____,STA,015,15,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,02:02:2D:36:5E:C8,2Mb/s,Ad-Hoc STA (beacon),Radio only, BEACON
07/23/2002 09:03:08.500, "toto",00,____,AP,016,11,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,FF:FF:FF:FF:FF:FF,2Mb/s,Client,Radio only,PRBREQ

07/23/2002 09:03:13.050, "toto",10,____,STA,016,15,FF:FF:FF:FF:FF:FF,00:02:2D:36:5E:C8,02:02:2D:36:5E:C8,2Mb/s,Ad-Hoc STA (beacon),Radio only, BEACON
07/23/2002 09:06:07.295, " ",07,Wep,AP,008,3,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON
07/23/2002 09:06:12.195, " ",07,Wep,AP,009,3,FF:FF:FF:FF:FF:FF,00:40:96:5B:15:9D,00:40:96:5B:15:9D,1Mb/s,AP Base (dedicated),Radio only, BEACON

```



- Audit and analysis of 802.11b/g networks
- Passive sniffer
 - × No association with the WLAN
 - × Compliant with some laws
- Alternative listening over the 14 channels
- Saving of the captured traffic
 - × Ethereal-compatible file format
- Real-time display of all fields
 - × Display of SSID, client type
 - × Display of signal level for geolocalization
- Enable detection of Windows XP, fake APs, others' sniffers

- Wireless LANs are already deployed in your organization
- Wireless LANs are there forever
- You have to organize yourself to manage them and lower risks
 - × Segmentation and perimeter security
 - × Access control and authentication
 - × Logging and surveillance
- Wireless LANs second generation (802.11i & WPA) help you – no excuse
- Do not wait for hidden WLAN and intrusion : **own your air space by deploying your Secure Wireless LAN.**

Securing wireless LANs is possible

Questions ?

www.hsc.fr

Herve.Schauer@hsc.fr

- <http://www.hsc.fr/ressources/themes.html#wireless>
 - × All HSC resources about wireless networks security
- <http://www.hsc.fr/ressources/outils/wifiscanner/>
 - × Freeware for Wireless LAN audit

- Christophe Serda for Madge figures
 - × *Reproduced with permission*
- Eric Vyncke for Cisco figures
 - × *Reproduced with permission*
- Jérôme Poggi & Thomas Seyrat for their pictures
- Pam Prior for her corrections