Wireless Security:
A scalable solution for consumers, corporations, ISP and mobile operators

Giuseppe Paterno'

Wireless

There are different technologies for trasmitting data “over-the-air”, the most common are:

- GSM/GPRS
- UMTS
- Bluetooth
- Wireless LAN (o Wi-Fi)

Wireless LAN

- Based on IEEE 802.11
- Direct Sequence Spread Spectrum and Frequency Hopping Spread Spectrum
- Similar to Ethernet (CSMA/CA), through the extension IEEE 802.11b
- Easily integrable with the wired LAN

Wireless LAN

Data rate

- Up to 11 Mb/s (IEEE 802.11b) in the 2.4 Ghz
- Up to 56 Mb/s (IEEE 802.11a) in the 5 Ghz
- Up to 54 Mb/s (IEEE 802.11g) in the 2.4 Ghz (only three vendors announced it)

WEP

- Acronym for “Wired Equivalent Privacy”
- Developed to ensure data confidentiality
- Based on the RSA's RC4 encryption algorithm
- Key length is 40 or 104 bit long

WEP

- WEP is insecure and give a false security feeling
- Keys can be derived by observing IV collisions and with a probabilistic attack to the RC4 algorithm
- Data not encrypted at the presentation layer can be easily eavesdropped

MAC filtering

- Manufacturer introduced a security feature known as MAC filtering
- Access Points are able to “filter” the clients' MAC address, enabling the permitted ones
- First security response to WEP

MAC filtering

- Has issues on manageability: if the adapter is changed, a new MAC address must be configured
- MAC address can be easily guessed and changed by intruders

802.1X

- Provide authentication for both Wireline and Wireless LANs
- Based on EAPOL: EAP over LAN
- Needs a PKI infrastructure
- Different vendor proprietary implementations (e.g. Cisco's LEAP, Microsoft's EAP-TLS)

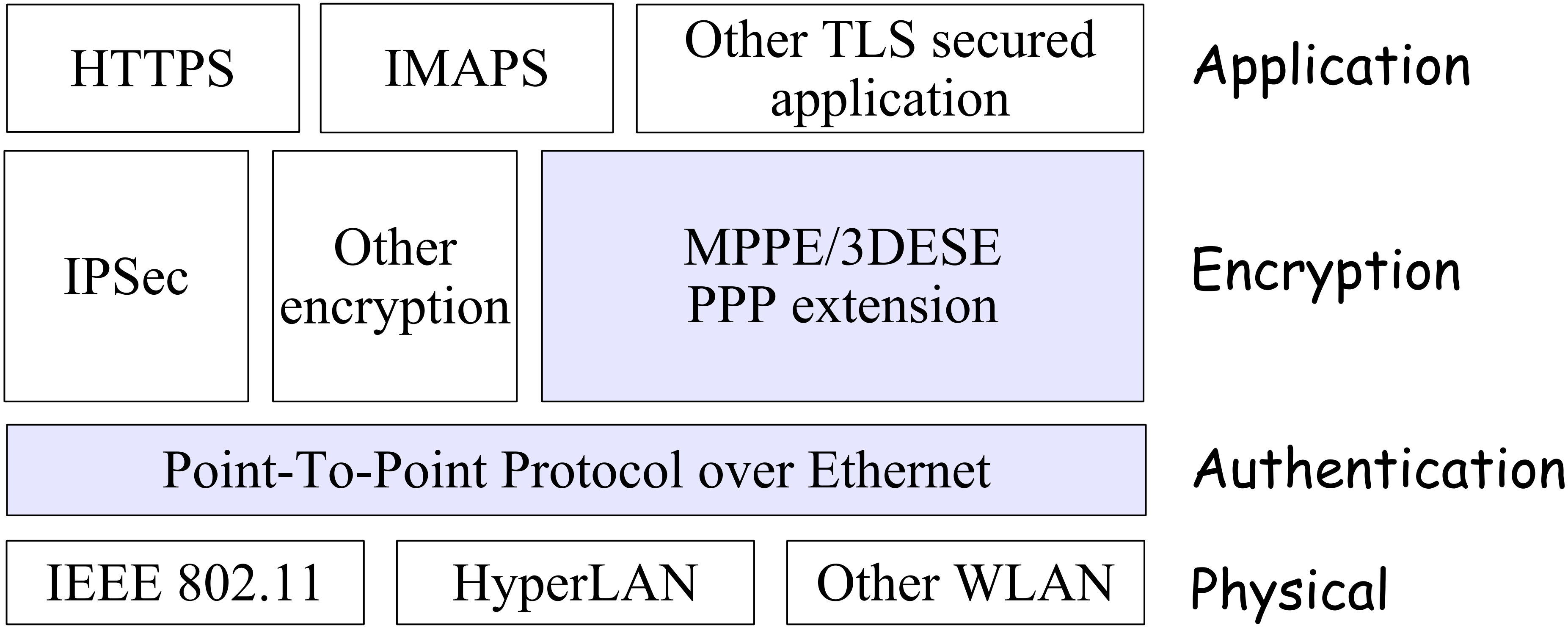
802.1X

- 802.1X compliant Access Points are still expensive
- Non compliant hardware must be repliaced
- More important: does not cover encryption

802.11i

- Based on the Temporal Key Integrity Protocol with AES-CCMP
- Should replace WEP
- Hardware must be replaced
- Vendor might not be willing to replace their proprietary fixes as it become available

Proposed solution: PPPoE



HTTPS

IMAPS

Other TLS secured application

Application

IPSec

Other encryption

MPPE/3DESE PPP extension

Encryption

Point-To-Point Protocol over Ethernet

Authentication

IEEE 802.11

HyperLAN

Other WLAN

Physical

PPPoE

- Acronym for Point-to-Point Protocol over Ethernet
- Used by the ISPs for ADSL and broadband world (e.g. cable modems)
- DHCP is not an advantage, no user identification is needed

PPPoE

- The idea is applying PPPoE to the Wireless LAN world
- It enables:
  - User authentication and authorization
  - Different networks protocol (e.g. IP, IPX, NetBIOS)
  - Encryption through MPPE and ECP (DESE/3DESE)

PPPoE: advantages

- Access control, billing, and several type of services can be performed on a per-user, rather than a per-site or cell basis
- Personalized services (e.g. Fixed IP, QoS)
- Scalable model for selling Virtual Dial-Up Networks (VPDNs) services

PPPoE: advantages

- PPP is another obstacle to hackers, that have to break both WEP and the PPP layer
- No network protocol (Layer 3) is bound to any interface
  - Network is protected from unauthorized access
  - Client is protected, no need for personal firewalls

PPPoE: advantages

- Can be easily embedded in existing Access Points, by upgrading the firmware
- No change on the existing infrastructure/hardware: only a PPPoE server is needed

PPPoE: disadvantages

- The disadvantage is the MTU/MSS size:
  - The PPP MTU must not be greater than 1492
  - Some misbehaved VPN packets adds overhead to the interface MTU, so that if VPNs are used MTU should be reduced to ~1460

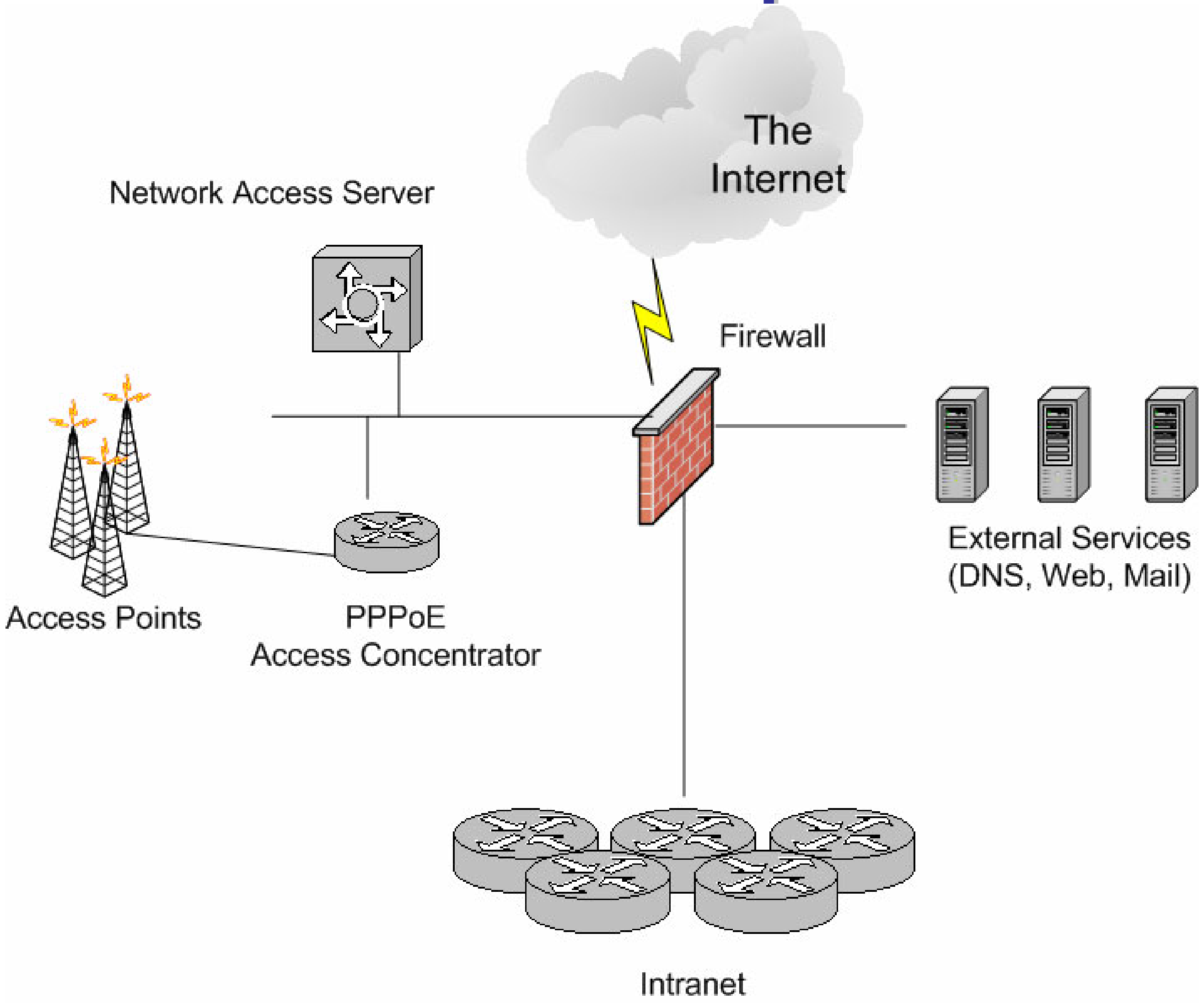
Roaming

- *Portability* is different than roaming
- Roaming is complex: physical layer and the logical layer must be synchronized
- IEEE 802.11 does not cover roaming
- Many manufacturers implements roaming in their AP at the MAC layer

Roaming

- Usually based on Mobile IP: hard to implement and to secure for Home Agent network positioning
- Portability is not an issue for PPPoE and for small coverage areas (buildings, small campus)
- Larger deployment is possible, but is not yet available

Architecture Example



Compatibility Matrix

Product/ Program	Server	Client	MPPE	3DESE	WiRAN
Cisco IOS	Yes	Yes	Yes	No	No
Windows	Yes	Yes	Yes	No	No
FreeBSD	Yes	Yes	Yes	No	No
Linux	Yes	Yes	Yes	No	No
MacOS X	No	Yes	No	No	No
FinePoint ServPoET	Yes	Yes	No	No	No

Thank You!

Giuseppe Paterno'
gpaterno@gpaterno.com