Wireless Network Esercitazioni

Alessandro Villani
avillani@science.unitn.it

Security e Reti Wireless

Sicurezza: Overview

- Open network
- Open network+ MAC-authentication
- Open network+ web based gateway
- WEP (wireless)
- IEEE 802.1X

Sicurezza: Overview

- **Open network**
  - Non è una reale soluzione
  - Al più gli indirizzi IP vengono assegnati da un DHCP Server (Soluzione di livello 2/3)
  - Molto semplice da implementare: non è necessaria l'installazione di software speciale (i client DHCP sono utilizzati ovunque)
  - Praticamente impossibile il controllo d'accesso
  - La rete è aperta (Ogni client e server della LAN è raggiungibile)

Sicurezza: Overview

- **Open network + MAC authentication**
  - Come nel caso precedente, ma il MAC-address della scheda dell'utente è verificato dalla rete
  - È comunque complicato dal punto di vista amministrativo gestire i MAC addresses
  - I MAC addresses possono essere spooffati
  - Non è possibile gestire un utente guest

Sicurezza: Overview

- **Open network + web based gateway**
  - Si utilizza un gateway di Livello 3 (router IP) tra la WLAN e la rete cablata intercetta inizialmente tutto il traffico e presenta una pagina web all'utente attraverso cui l'utente dovrà immettere le proprie 'credenziali'.
  - Se l'utente è autenticato, il suo traffico (tutto o solo quello di un certo tipo) è autorizzato a passare
  - È possibile gestire l'utente guest facilmente
  - Un browser deve essere installato, e deve rimanere attivo durante l'intera sessione (anche se stiamo usando una stampante)

Sicurezza: Overview

- **Open network + web based gateway**
  - Implementazioni free (NoCat, anche su AP: WRT54G + Portless Network)
  - Implementazioni proprietarie (Anche su AP: Orinoco AP 2500)
  - Sviluppato anche dal progetto WILMA

Sicurezza: Overview

- **WEP**
  - Crittografia a livello 2 tra Client ed Access Point
  - Il client deve conoscere una stringa (lunga) per poter accedere alla rete Wireless
  - WEP si è dimostrato molto facile da violare
  - È complessa la gestione del cambiamento delle chiavi WEP (le chiavi devono essere cambiate regolarmente per far si che un hacker non possa raccogliere traffico sufficiente per crackare la chiave WEP

Sicurezza: Overview

- **IEEE 802.1X**
  - È una soluzione di livello 2 per gestire l'accesso alla rete wireless
  - Sono stati sviluppato vari meccanismi di autenticazionwe (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP)
  - È una soluzione standard
  - Cripta tutti i dati, utilizzando chiavi dinamiche
  - Utilizza RADIUS come server
  - Richiede un software opportuno installato su ciascun client

802.1X

- 802.1X è divenuto standard nel giugno del 2001
- Può essere scaricato all'indirizzo: http://standards.ieee.org/getieee802/portfolio.html
- 802.1X sostanzialmente definisce un framework per l'autenticazione che utilizza protocolli esistenti (quali EAP e Radius)
- L'autenticazione avviene attravero il protocollo EAP al di sopra dell'802.1X

802.1X: EAP

- Il protocollo EAP (Extensible Authentication Protocol) è definito nella RFC 2284
- Fornisce una architettura nella quale più meccanismi di autenticazione possono essere usati

802.1X: EAP

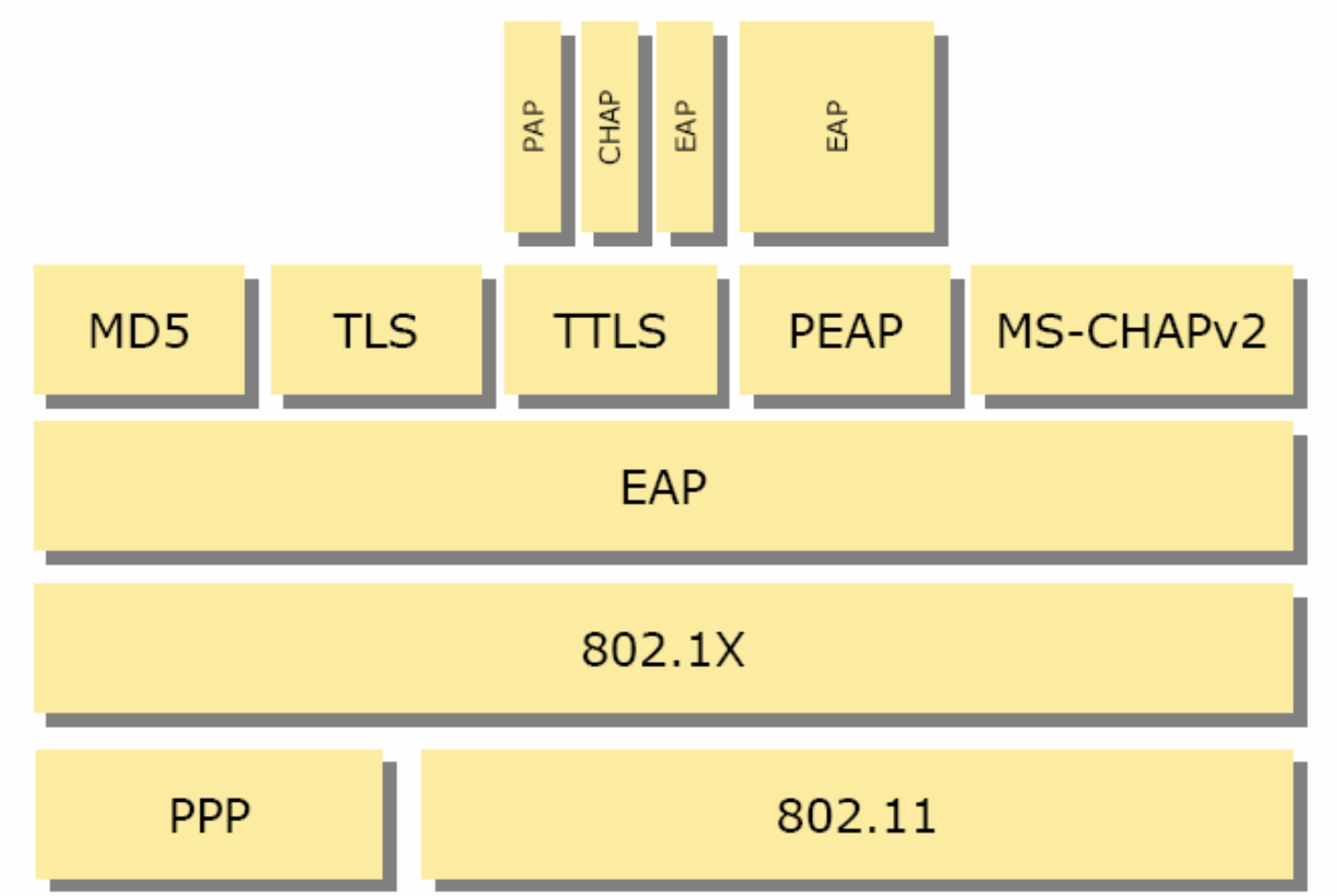
- Metodi di autenticazioni per EAP:
  - EAP-MD5 Username/Password (insiscuro)
  - EAP-TLS Certificati, autenticazione forte
  - EAP-TTLS Username/Password (sicuro)
  - MS-CHAPv2 Username/Password Microsoft (insicuro)
  - PEAP Modulo tunnel Microsoft/Cisco per il trasporto sicuro di MS-CHAPv2

802.1X: EAP

- **EAP/MD5:** L'autenticazione è fatta sulla base di uno shared secret che può corrispondere ad un username e password per il client. Metodo semplice anche da gestire ma non sicuro
- **EAP/TLS:** In EAP/TLS la mutua autenticazione è implementata utilizzando TLS, eliminando così i problemi di attacchi *man-in-the-middle* visto che sono utilizzati dei certificati
- **EAP/TTLS:** EAP/TTLS implementa una mutua autenticazione senza richiedere al client wireless un proprio certificato
- **EAP/PEAP:** L'autenticazione è fatta mediante un tunnel TLS direttamente tra il client ed il server di autenticazione che fornisce il certificato

802.1X

- Lo schema del protocollo è il seguente:



802.1X: EAP

- Poiché il canale fisico è facilmente accessibile da un attaccante, la mutua autenticazione attraverso un tunnel è uno dei metodi preferiti per evitare attacchi di tipo *man-in-the-middle*.
- La mutua autenticazione evita che i clients si connettano a “finti” AP nella wireless network

802.1X: EAP

- Se 802.1x, con un metodo di autenticazione su TLS, è usato in congiunzione con WEP, allora è possibile definire un meccanismo di chiavi per utente e per sessione
- Quando l'autenticazione è realizzata, il server ed il supplicant determinano una chiave di sessione, che è inviata all'AP dall'authentication server.
- L'authenticator genera un insieme di chiavi WEP e le transmette al supplicant

802.1X

- 802.1x definisce 3 componenti per completare una sequenza di autenticazione:
  - **Supplicant:** Colui che desidera accedere ai servizi (ad esempio una stazione mobile) fornendo le corrette credenziali all'authenticator
  - **Authenticator:** Colui che si occupa di applicare le security policies (ad esempio l'Access Point), prima di lasciar accedere ai servizi ad un supplicant
  - **Authentication Server:** Colui che verifica se il supplicant è autorizzato ad accedere al servizio attraverso l'authenticator (ad esempio un server RADIUS)

802.1X

- Il processo di autenticazione si basa sullo scambio di informazioni tra il supplicant e l'authentication server
  - L'utente fornisce le sue credenziali, che possono essere anche certificati digitiali, login e password, ...
  - EAP può supportare la mutua autenticazione, nel qual caso il server manda le sue credenziali al supplicant

802.1X

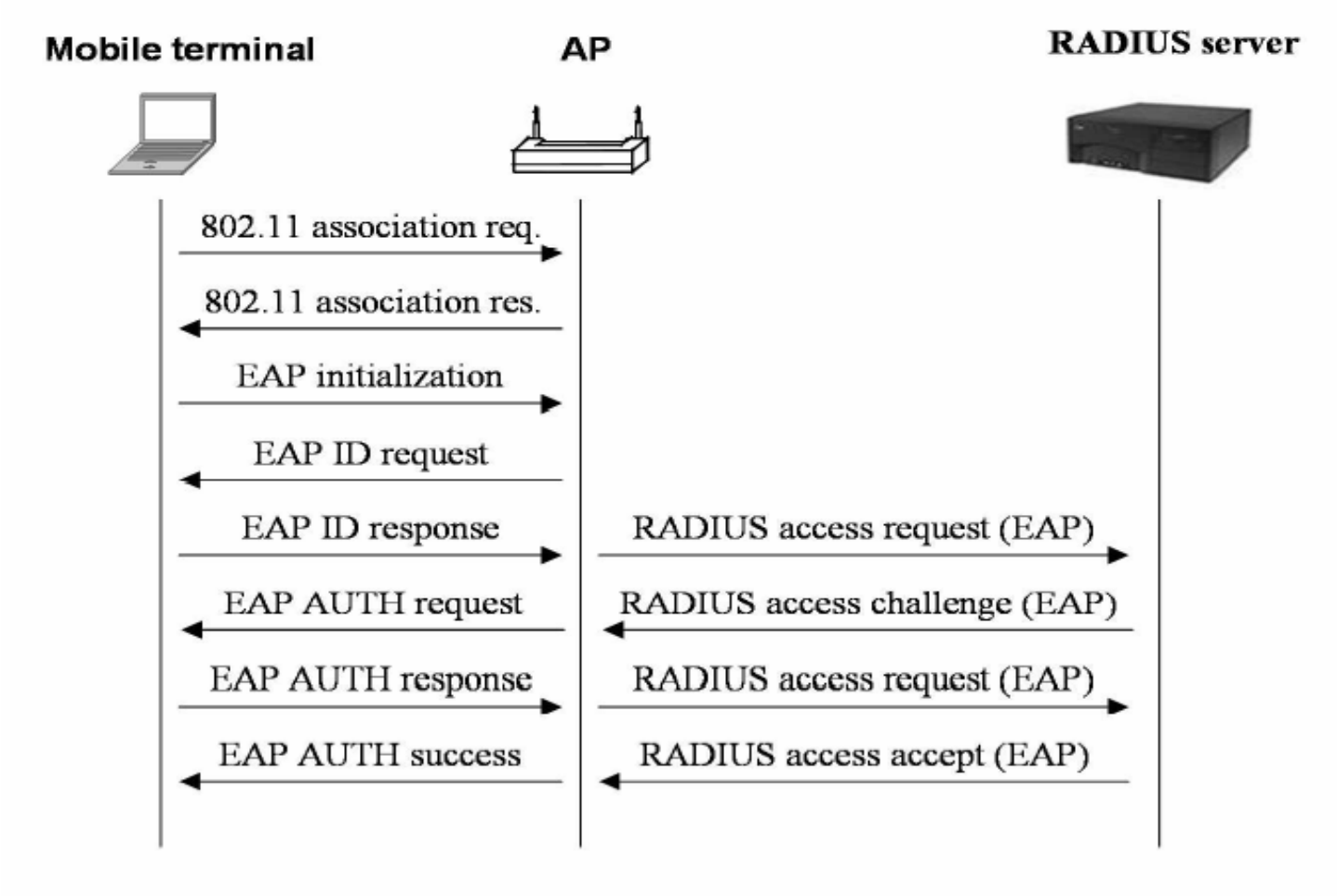
- 802.1x definisce due punti di attacco per un client di una rete wireless:
  - Una porta **“Controlled”** ed una porta **“uncontrolled”**
- Il supplicant prima dell’autenticazione comunica con l’authentication server attraverso la porta "uncontrolled".
- L’autenticazione tra il supplicant e l’authenticator è realizzata mediante EAP su LAN (EAPOL), una forma incapsulata di EAP
- A sua volta l’authenticator inoltra le credenziali del client all’authentication server utilizzando RADIUS

802.1X

- Il client rimane collegato alla porta “uncontrolled” finché l’autenticazione è conclusa.
- Dopo una avvenuta autenticazione, l’authentication server comunica all’authenticator di spostare il client sulla porta “controllata”
- Una porta “controlled” accetta solo pacchetti da clienti autorizzati.

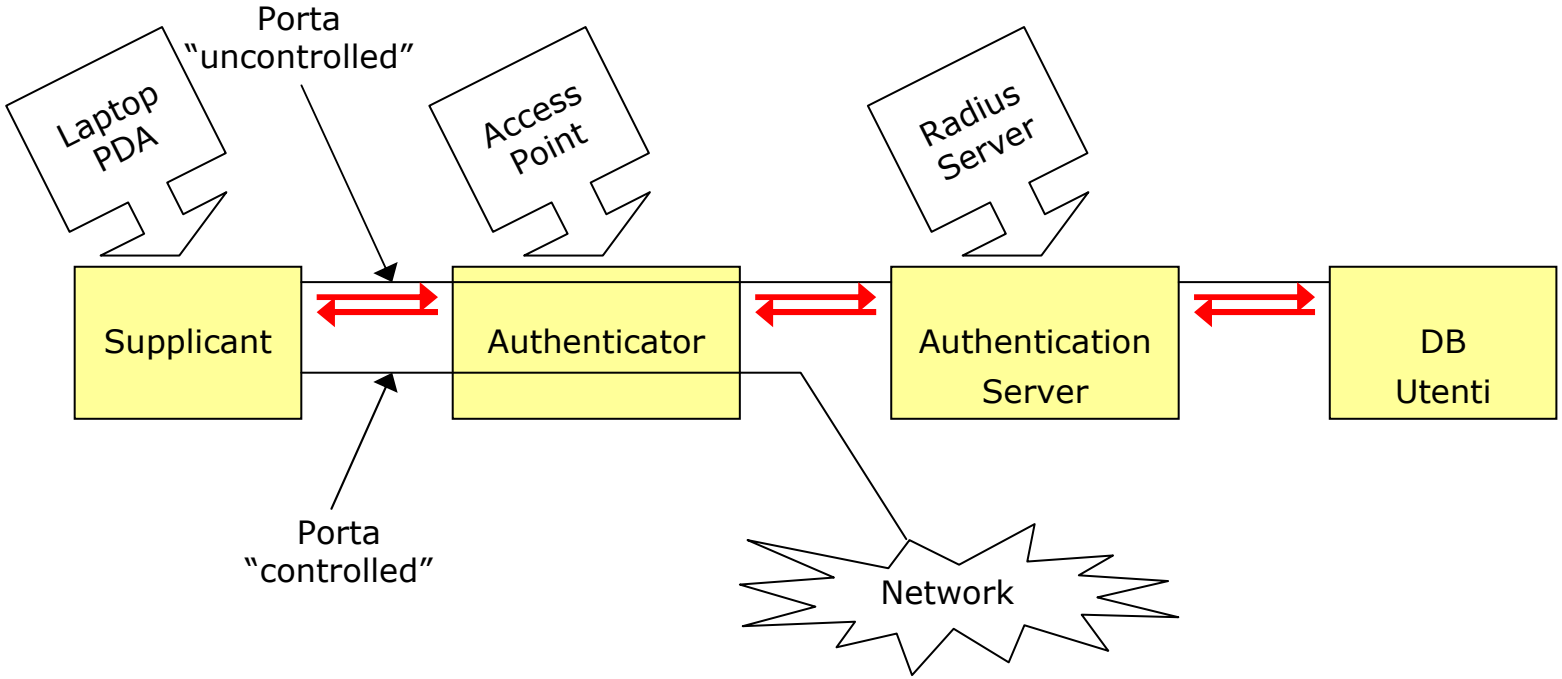
802.1X

- Lo schema di una autenticazione è:



802.1X

- Lo schema di una autenticazione è:



802.1X

- Nello standard lo schema è rappresentato come segue:

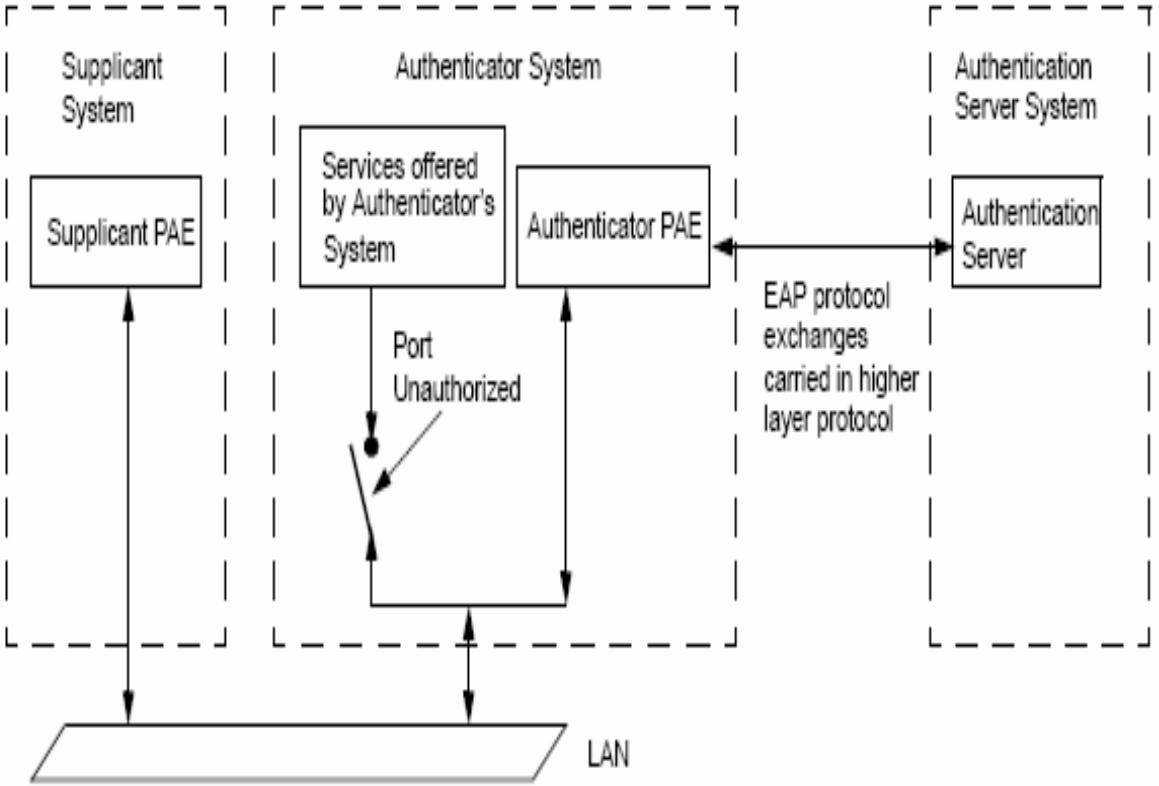


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

802.1X: EAP tunnellizzati

- Nel caso di EAP-TTL, EAP-TTLS, EAP-PEAP lo schema si complica un po' con due fasi distinte:
  - Inizializzazione del tunnel sicuro
  - Scambio di informazioni per l'autenticazione all'interno del tunnel

802.1X: EAP tunnellizzati

- Tunnel Sicuro:
  - L'Authenticator manda un "EAP-Request/Identity" al Supplicant appena stabilito il link (il Supplicant si è associato all'AP)
  - Il Supplicant invia un "EAP-Response/Identity" con la sua identità all'Authenticator che la riformatta come paccheto Radius e la invia all'Authentication Server
  - L'Authenticator invia un "EAP-Request/EAP-XXX" (con XXX corrispondente al protocollo di crittazione supportato per avviare l'opportuno scambio di chiavi
  - L'Authentication Server ed il Supplicant stabiliscono il tunnel

802.1X: EAP tunnellizzati

- Scambio Informazioni:
  - L'Authentication Server invia una challenge all'Authenticator. L'Authenticator la converte da RADIUS in EAPOL e la manda al Supplicant
  - Il Supplicant risponde alla challenge attraverso l'Authenticator, che la gira all'Authentication Server
  - Se il Supplicant ha fornito le credenziali corrette, l'Authentication Server risponde con un messaggio di successo che è passatoal Supplicant. L'Authenticator autorizza all'accesso alla rete

802.1X: EAP tunnellizzati

- Tutte le informazioni rilevanti (username, password) rimangono crittate tra il Supplicant e l'Authentication Server
- L'Authenticator ha il ruolo di supporto nella costruzione del tunnel visto che il Supplicant non può ancora accedere direttamente alla LAN.

802.1X: Linux & Windows

- Molte cose sono cambiate nel 2003:
- Windows XP supportava 802.1x con EAP-MD5, rimosso nei service pack
- Linux ha finalmente un supplicant free, scaricabile all'indirizzo:

http://www.open1x.org/

802.1X: Linux & Windows

- Vari server radius supportano le modalità avanzate di autenticazione
- FreeRadius è uno dei pochi radius server free che implementa il supporto per il protocollo EAP.
- FreeRadius può essere scaricato all'indirizzo:

  http://www.freeradius.org/