WLAN (Wireless LAN)
IEEE 802.11

© Marco Cremonini 1

WLAN 802.11 :

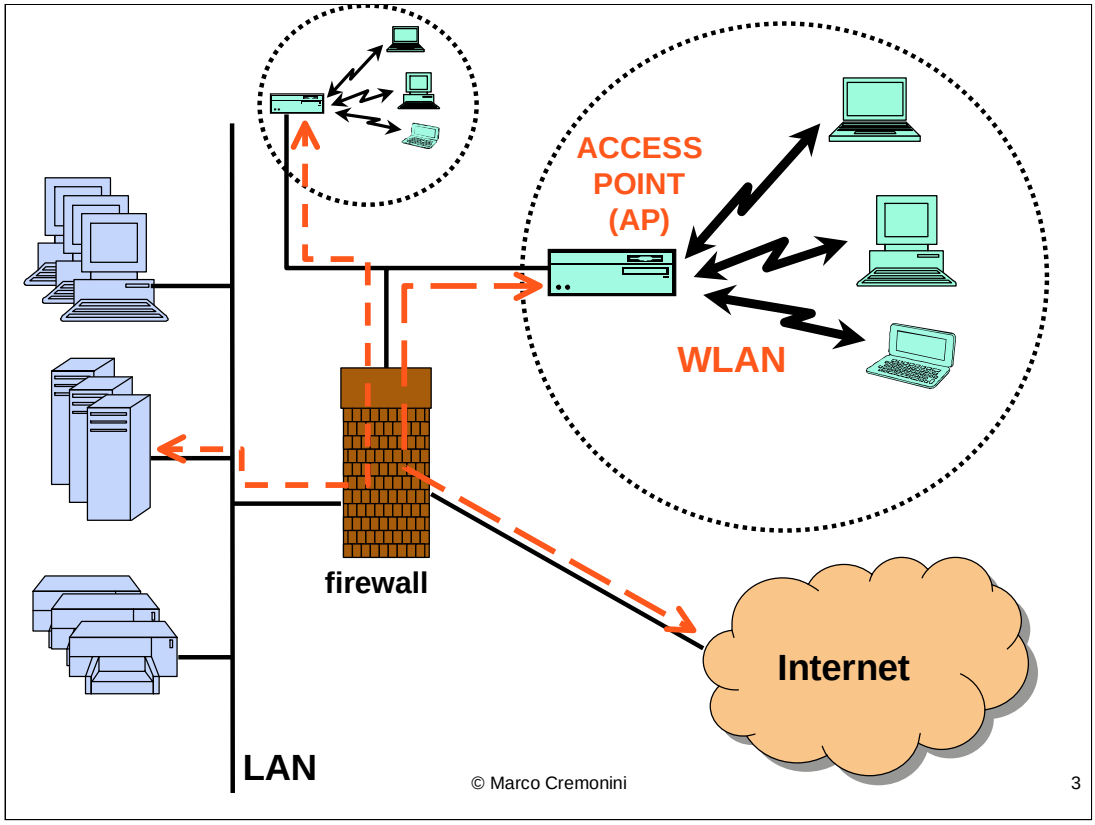
- Estensione di una LAN Ethernet e dei protocolli relativi (IEEE 802.3) al mondo wireless;
- Protocolli definiti dalla IEEE (ente di standardizzazione) a partire dal 1999.

Ampia scelta di prodotti commerciali disponibili a prezzi molto contenuti.

Componenti necessari:

- **Schede di rete (NIC) wireless** per i pc (es. laptop) o dispositivi palmari (es. pocket computer);
- **ACCESS POINT** per connessione alla LAN su ed alle risorse di rete.

© Marco Cremonini 2


ACCESS
POINT
(AP)
WLAN
firewall
Internet
LAN
© Marco Cremonini
3

WLAN 802.11 : **Portata**

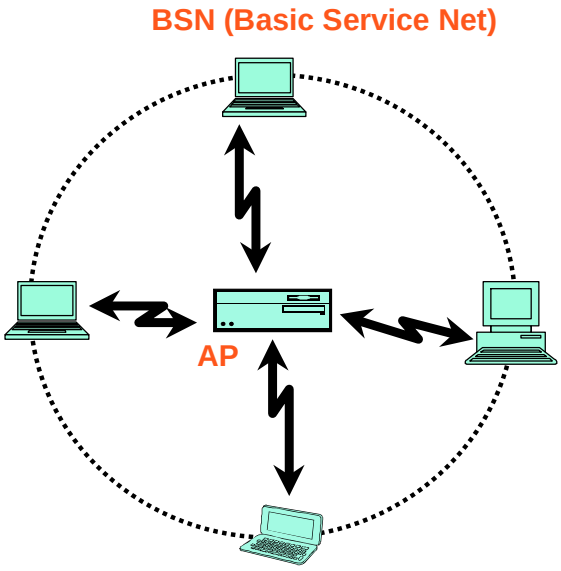
- Interni : 15 -150 m.
- Esterni : ~300 m.

WLAN 802.11 : **Frequenza**

- 802.11a : 5 GHz
- 802.11b : 2.4 GHz
- 802.11g : 2.4 GHz

WLAN 802.11 : **Throughput**

- 802.11a : 24 - 54 Mbs
- 802.11b : 5.5 - 11 Mbs
- 802.11g : 24 - 54 Mbs



© Marco Cremonini 4

Una differente tecnologia per connessioni wireless, BLUETOOTH, ha un range di trasmissione molto piu' ridotto (10 metri, circa) e non viene usata per realizzare WLAN ma connessioni locali tra dispositivi (es. PC con modem, pocket pc con workstation, etc.).

Gli standard 802.11 sono definiti per il livello FISICO dello stack OSI (primo livello). Esistono tre principali versioni degli standard:

802.11a : poco diffuso, frequenza di 5 GHz e Banda Trasmissiva tra i 24 e i 54 Mbs.

802.11b : il piu' diffuso tra i prodotti commerciali, frequenza di 2.4 GHz e Banda Trasmissiva tra i 5.5 e gli 11 Mbs. (802.11a e 802.11b non sono interoperabili).

802.11g : standard previsto per il prossimo futuro. Compatibile con i dispositivi che supportano lo standard 802.11b. Incrementa la banda trasmissiva al livello dell'802.11a (24-54 Mbs) mantenendo pero' la stessa frequenza dell'802.11b (2.4 GHz).

Connessione a una WLAN :

ACCESS POINT: invia ad intervalli regolari frame contenenti:

SSID (Service Set IDentifier) - stringa alfanumerica che identifica un AP da altri operanti sullo stesso canale;

CANALE - numero tra 1 e 11 (USA) o tra 1 e 13 (Europa) che identifica la frequenza alla quale la WLAN sta operando.

CLIENT Wireless:

configurati per accedere direttamente ad un AP (specifici SSID e canale).

invio di segnali broadcast per rilevare la presenza di un Access Point.

© Marco Cremonini 5

Sicurezza di una WLAN :

- **ACCESS CONTROL TABLE**: tabella contenente i MAC address delle unita' autorizzate a connettersi all'AP.
- **WEP (Wired Equivalency Privacy)**

MAC address: identificatore fisico univoco cablato all'interno di ogni scheda di rete (sia essa rete cablata che wireless) dal produttore della scheda stessa.

© Marco Cremonini 6

WEP (Wired Equivalency Privacy) :

- Algoritmo facente parte degli standard 802.11 (indipendentemente dalla versione);
- Algoritmo crittografico (chiavi simmetriche a 40 o 128 bit) per la confidenzialita' dei dati trasmessi su di una WLAN;
- Crittazione dei dati a livello di data link layer;
- Marzo 2001: pubblicata prima vulnerabilita' del WEP e conseguente tecnica per violare la confidenzialita' dei dati. Ne seguiranno altre.
- Gravi problemi di sicurezza relativi alle WLAN;
- Molti tool per compiere intrusioni su WLAN.

© Marco Cremonini 7

WLAN Scanner

- Usati per identificare la presenza di un AP;
- Eseguono dei broadcast di pacchetti su tutti i canali, monitorando le risposte dagli AP;
- Talvolta integrati con GPS per localizzare geograficamente gli AP individuati.

© Marco Cremonini 8

I WLAN scanner sono i corrispettivi nel mondo wireless degli scanner per reti cablate.

Disponibili gratuitamente sia per ambiente Windows (es, Netstumbler) che Linux (es. Kismet).

WLAN Sniffer

- Usati per loggare ed analizzare il traffico su di una WLAN;
- Simili agli sniffer per reti Ethernet (software di sniffing + scheda di rete wireless in modalita' promiscua);
- Diversamente dalle reti cablate, tutto il traffico di una WLAN puo' essere acceduto semplicemente posizionandosi all'interno del raggio di trasmissione di un AP;
- Unica contromisura: WEP, ovvero crittare il traffico.

© Marco Cremonini 9

I WLAN Sniffer sono anch'essi del tutto analoghi agli sniffer per reti Ethernet.

Kismet e AirSnort sono esempi di tool disponibili.

WEP Cracker

- Tool usati per violare l'algoritmo crittografico WEP sfruttandone le vulnerabilita' note;
- Sia chiavi di 40 che di 128 bit vengono violate;
- Il successo dipende dal numero di pacchetti collezionati dallo sniffer, quindi, in generale, tentativi ripetuti portano ad un attacco efficace.

© Marco Cremonini 10

WEPcrack e AirSnort sono esempi di tool disponibili.

WAR DRIVING

Intrusori che semplicemente muovendosi per strada, in citta', in zone universitarie o in zone industriali, dotati di laptop, scheda di rete wireless (eventualmente dotati di antenna particolarmente sensibile) e i tool appena descritti (WLAN scanner, WLAN sniffer e WEP cracker) possono facilmente compromettere la sicurezza aziendale di molte organizzazioni.

© Marco Cremonini 11

La presenza delle WLAN e le vulnerabilita' ad esse connesse, permette questo fenomeno detto di "war driving".

Cio' ha un impatto significativo sulle misure di sicurezza FISICA adottate dalle societa'. Nel caso delle WLAN le misure di sicurezza fisica a protezione dell'infrastruttura tecnologica (ingressi controllati, autorizzazioni personali, dispositivi isolati fisicamente, etc.) diventano sostanzialmente inutili.

Test di war driving effettuato:

fine 2001 (Manhattan, New York)

Tempo: 15 minuti di viaggio in taxi;

Equipaggiamento: Win 2000 laptop, scheda wireless, WLAN scanner;

Risultato:

AP identificati: 106

AP non utilizzanti WEP: 77 (75%)

© Marco Cremonini 12

I dati sono riportati in:

Michael Sutton, “Hacking the Invisible Network - Insecurities in 802.11x”, iDEFENSE Inc., Luglio 2002. Http://www.idefense.com

Per l’accesso ad una WLAN priva di crittografia e’ necessario:

- WLAN scanner per individuarla;
- indirizzo IP valido
  - se l’organizzazione usa DHCP, questo viene fornito automaticamente al momento della tentata connessione;
  - se l’organizzazione usa indirizzi IP statici, e’ comunque semplice individuare quale sia il range di indirizzi utilizzato.

Dati raccolti da `http://www.worldwidewardrive.org/`

CATEGORIA	TOTALE	PERCENT.	VARIAZIONE
Numero di AP Individuati	24958	100%	
WEP Abilitato	6970	27,92%	-2,21%
WEP Non Abilitato	17988	72,07%	+2,21%
SSID di Default	8802	35,27%	+5,74%
SSID di Default e WEP Non Abilitato	7847	31,44%	+4.8%

I risultati si riferiscono a dati raccolti tra il 26 Ottobre e il 2 Novembre 2002.

Le variazioni sono relative ad un'analoga raccolta di dati condotta tra il 31 Agosto e il 7 Settembre 2002.

© Marco Cremonini 13

Dati raccolti da WiGLE.net (`http://www.wigle.net`)

CATEGORIA	TOTALE	PERCENT.
Numero di AP Registrati	171201	100%
WEP Abilitato	45583	26,63%
WEP Non Abilitato	119349	69,71%
WEP Non Determinato	6259	3,66%

Dati raccolti da Portel (`http://www.portel.it`)

Con una attivita' di scanning nel centro di Milano della durata di circa un'ora, sono state individuate 18 reti, di cui 12 senza il Wep (66,67%) e solo 6 con il protocollo di sicurezza attivato (33,33%).

© Marco Cremonini 14

Dell'indagine pubblicata da Portel rileviamo alcuni elementi interessanti:

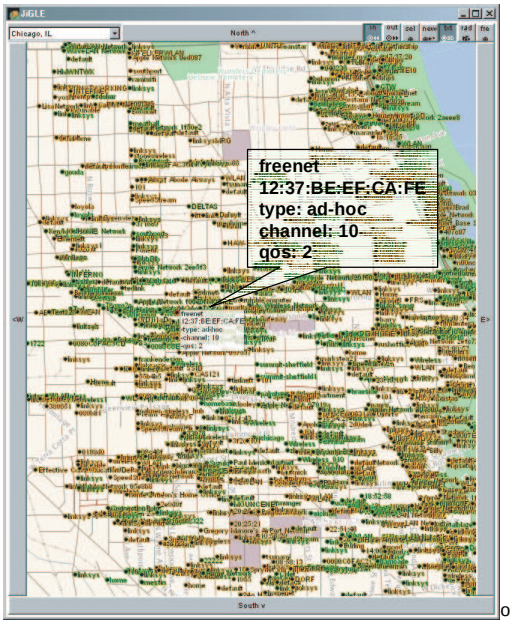
- il numero di WLAN estremamente ridotto, indizio della scarsa adozione della tecnologia 802.11 in Italia;

- i risultati, anche se poco significativi dal punto di vista statistico, risultano in linea con i dati presentati nelle diapositive precedenti e riferiti in gran parte a casi statunitensi e dimostrano in maniera evidente il deficit di competenze (competenze di base, va sottolineato) in tema di sicurezza da parte di esperti applicativi e di reti.

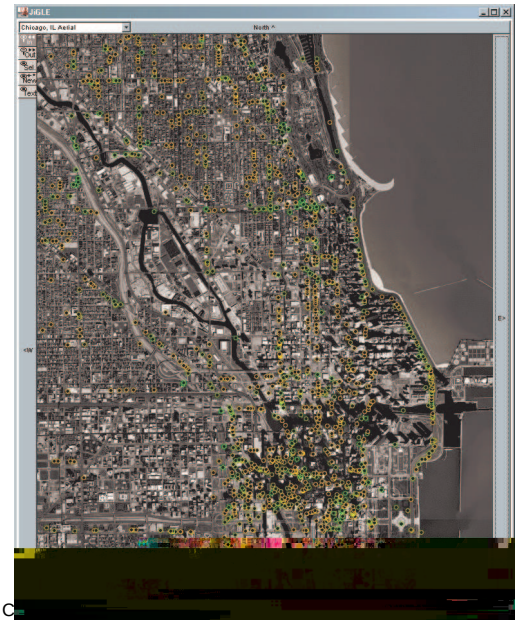
Informazioni geografiche da WiGLE.net (`http://www.wigle.net`)

Chicago (USA)

Mappa con dettagli delle WLAN individuate



Locazione degli Access Point da vista aerea



WLAN : Rischi per la Sicurezza Aziendale

- WLAN posizionate dietro i firewall e considerate quindi alla stregua della LAN interna possono fornire facili possibilita' di intrusioni;
- Possibile attivita' di sniffing e conseguente accesso a dati trasmessi su WLAN senza lasciare alcuna traccia di tale attivita';
- Host accedibili da WLAN non protette possono costituire teste di ponte per successivi attacchi. Molto difficile risalire al responsabile;
- WLAN non adeguatamente protette possono consentire il logon a utenti non autorizzati e il conseguente uso illecito di risorse (es. navigazione su Web, spamming di posta elettronica).

© Marco Cremonini 16

Contromisure: Linee Guida

- Usare sempre WEP: anche se vulnerabile, la mancanza di misure protezione rende una WLAN totalmente accessibile da chiunque;
- Non affidarsi al solo WEP per la confidenzialita' dei dati: ai dati trasmessi dovrebbero applicarsi misure di sicurezza applicative (es. PGP, VPN);
- Isolare le WLAN: non permettere alcun traffico tra una WLAN e una LAN aziendale in modo incontrollato. Deve sempre esistere un firewall che isoli la WLAN dalla rete aziendale. Richiedere sempre autenticazione;

© Marco Cremonini 17

Nonostante l'intrinseca vulnerabilita' di una WLAN e le vulnerabilita' del protocollo WEP, esistono comunque linee guida per una gestione corretta.

Occorre notare che le linee guida non risolvono le problematiche evidenziate ma ne permettono una gestione dei rischi connessi .

Contromisure: Linee Guida (cont.)

- Utilizzare ogni volta sia possibile la Access Control Table con i MAC address delle unita' autorizzate a connettersi;
- Cambiare periodicamente le chiavi crittografiche del WEP.
- Disabilitare l'invio periodico dei pacchetti da parte dagli Access Point che ne facilitano l'individuazione;
- Assicurarsi che la copertura degli AP non sia eccessiva (strada, parcheggi, etc.)

© Marco Cremonini 18

Contromisure: Linee Guida (cont.)

- Cambiare le Password di Default per l'accesso al tool di amministrazione degli Access Point cosi' come l'indirizzo IP e la configurazione di default per l'autenticazione dell'AP stesso;
- Usare chiavi a 128 bit per WEP.
- Monitorare periodicamente l'eventuale presenza di AP illeciti: all'interno dell'organizzazione potrebbero venire installati AP non autorizzati (cosi' come accade per i modem) e compromettere gravemente la sicurezza aziendale. Usare WLAN Scanner per verificarne la presenza.

© Marco Cremonini 19

Evoluzione attuale: Standard IEEE 802.1X

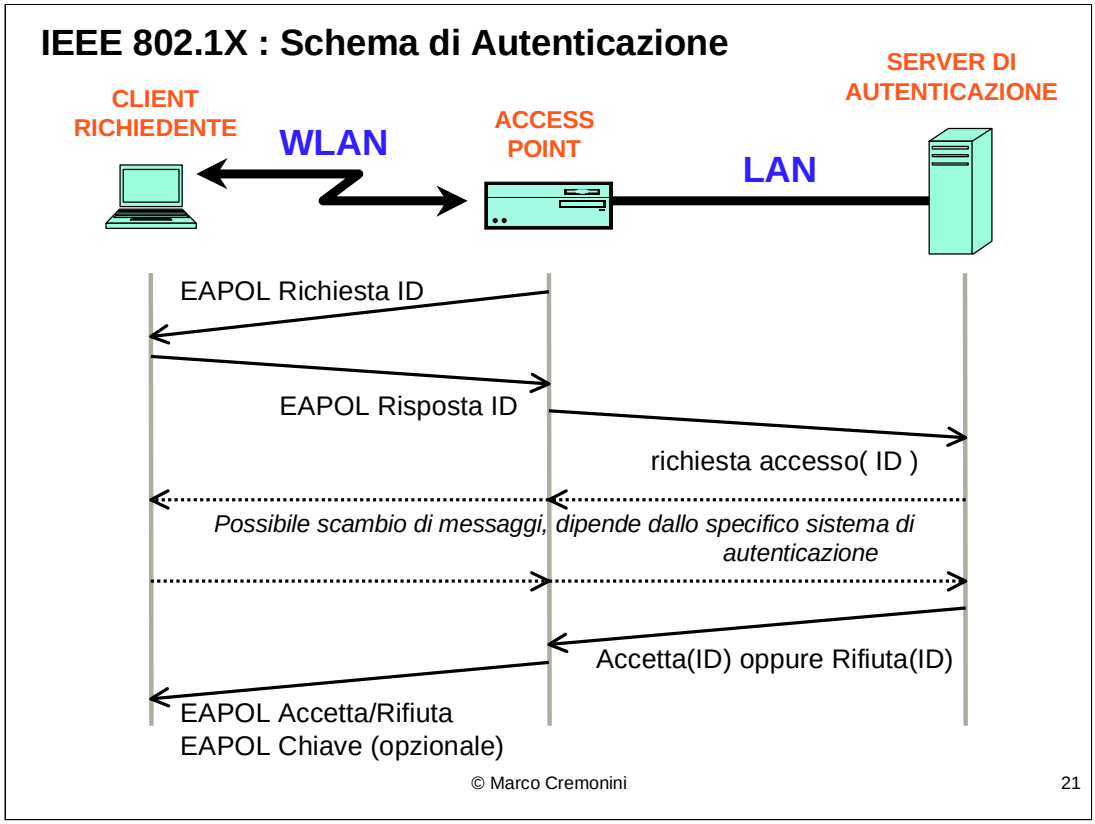
- Standard **proposto** per controllo degli accessi, autenticazione e gestione di chiavi crittografiche;
- Non sostituisce o risolve i problemi relativi all'algoritmo WEP di cifratura del traffico su di una WLAN ma e' usato in combinazione con gli standard 802.11;
- IEEE 802.1X definisce una modalita' di uso in reti wireless del protocollo EAP (Extensible Authentication Protocol) che viene comunemente utilizzato per accessi Internet telefonici (PPP - Point-to-Point Protocol)
  --> **EAPOL** (EAP Over LAN).

© Marco Cremonini 20

IEEE 802.1□ e' uno standard proposto che sta avendo una certa diffusione per reti wireless perche' supporta alcune delle funzionalita' di sicurezza indispensabili e non comprese dalle specifiche di IEEE 802.11.

Specifica modalita' di AUTENTICA□IONE, CONT□OLLO DEGLI ACCESSI e GESTIONE DI CHIA□I C□ITTOG□AFICHE per reti locali sia cablate (LAN) che wireless (WLAN).

Impiega, come modalita' di autenticazione, il protocollo EAP gia' noto e diffuso per le connessioni Internet telefoniche PPP.



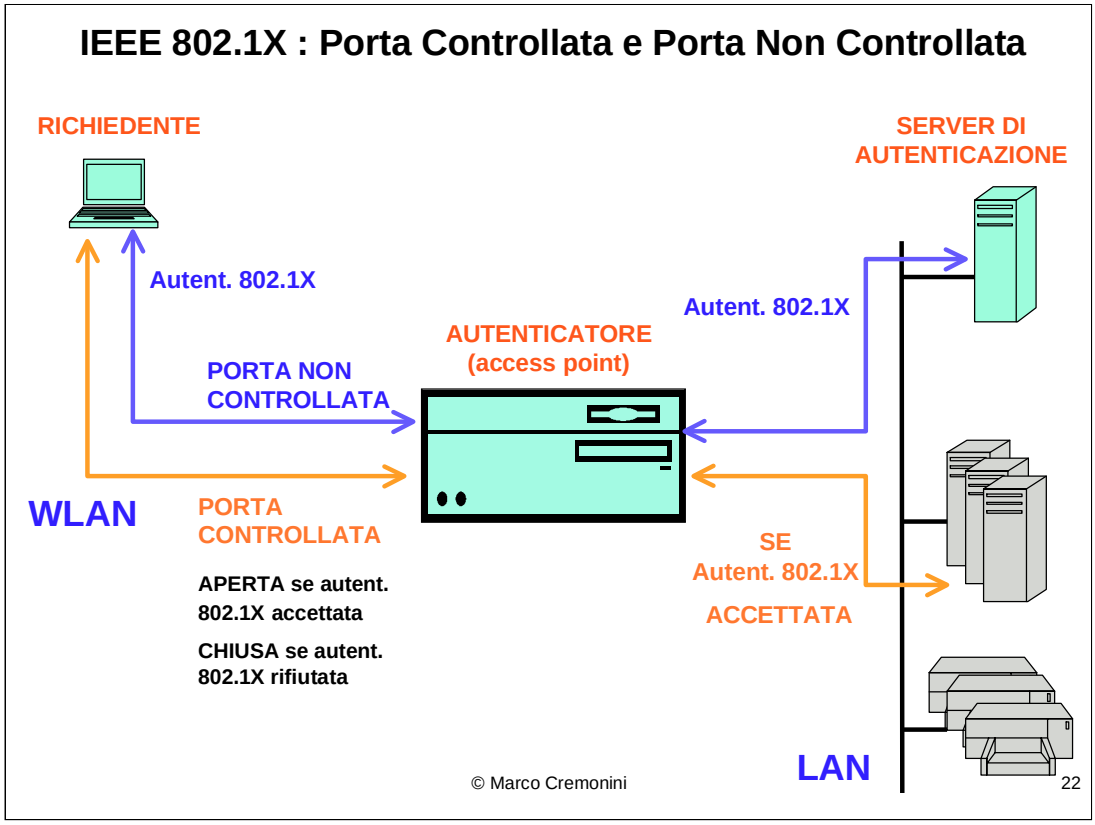
L'access point (AUTENTICATO□E) durante la fase di autenticazione agisce come semplice proxy tra il □ICHIEDENTE e il SE□□E□ DI AUTENTICA□IONE.

Messaggi secondo il protocollo EAP vengono scambiati tra richiedente e autenticatore (access point) e sono di 4 tipi:

- EAP □ichiesta ID/ EAP □isposta ID;

- EAP AccettaID/ EAP □ifiuta ID.

Messaggi tra l'autenticatore (access point) e il server di autenticazione sono dipendenti dalla particolare tecnologia di autenticazione impiegata (es. □ADIUS e' tipica per accessi remoti).



L'AUTENTICATO□E (access point) che implementa le specifiche 802.1□, deve attivare due porte applicative:

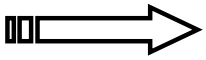
- PO□TA NON CONT□OLLATA : sempre abilitata e dedicata a scambiare i messaggi secondo il protocollo EAP con il richiedente;

- PO□TA CONT□OLLATA : sempre chiusa tranne quando il richiedente non sia stato positivamente autenticato dal Server di Autenticazione. Usata per le connessioni tra il richiedente e i server applicativi (es. web server, mail server, etc.) della LAN.

IEEE 802.1X : Conclusione

Criticita'

- Crittografia dei dati sulla WLAN dipendente da WEP o da estensioni proprietarie dell'EAP;
- Autenticazione del solo richiedente?
  Possibile Man-In-The-Middle (attaccante si sostituisce all'access point legittimo)



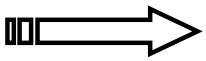
Proposte estensioni ad EAP (EAP-TLS) con impiego di algoritmi per crittare i dati in transito ed autenticare le due parti (TLS, simile ad SSL comunemente usato in applicazione web)

© Marco Cremonini

IEEE 802.1X : Conclusione (cont.)

Criticita'

- Meccanismo di autenticazione del richiedente (password/IP address/MAC address)? Possibile Predizione di password, Spoofing, Session Hijacking



Proposto uso di certificati elettronici su smartcard, token di autenticazione scambiati tra richiedente ed access point e rinnovati ad intervalli di tempo brevi (es. Kerberos), etc.

- Possibili attacchi di tipo Denial-of-Service

© Marco Cremonini

IEEE 802.1X : Conclusione (cont.)

Benefici

- Integrazione con 802.11 di meccanismi di sicurezza noti ed efficaci;

⇒ maggiore robustezza e maturita' della tecnologia

Contromisure?

GESTIONALI, OPERATIVE e TECNOLOGICHE

- **analisi dei rischi;**
- **riduzione dei rischi;**
- **monitoraggio.**

© Marco Cremonini 25