Wireless (in)security:
(in)sicurezza dell'802.11

Fabio (naif) Pietrosanti - Yvette (vodka) Agostini

fabio@pietrosanti.it – yvette@yvetteagostini.it

CNR 4 Novembre 2003

Missione impossibile

Volete imparare tutto quello che c'e' da sapere su 802.11, WEP,802.1x,TKIP, EAP, 802.11i in 60 minuti?

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

01 - Wireless: perchè?

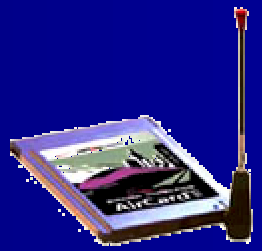
- è comodo da utilizzare
- consente di accedere alle risorse di rete senza essere vincolati a cavi, presenza di prese di rete, ecc.
- si declina in differenti modi per venire incontro a esigenze di scala differente (wwan, wlan, wpan, wman)
- è relativamente poco dispendioso

01 - Wireless: perchè preoccuparsi?

- Il media e' condiviso, chiunque puo' accedervi
- Il media condiviso e' FRAGILE
- Tanti standard nati male dal punto di vista della sicurezza(GSM, 802.11)
- La mancanza di cultura della sicurezza e la diffusione di punti di accesso alla rete "anonimi"
- L'impiego delle tecnologie wireless non e' sempre un'esigenza

01 - Tecnologie wireless più utilizzate

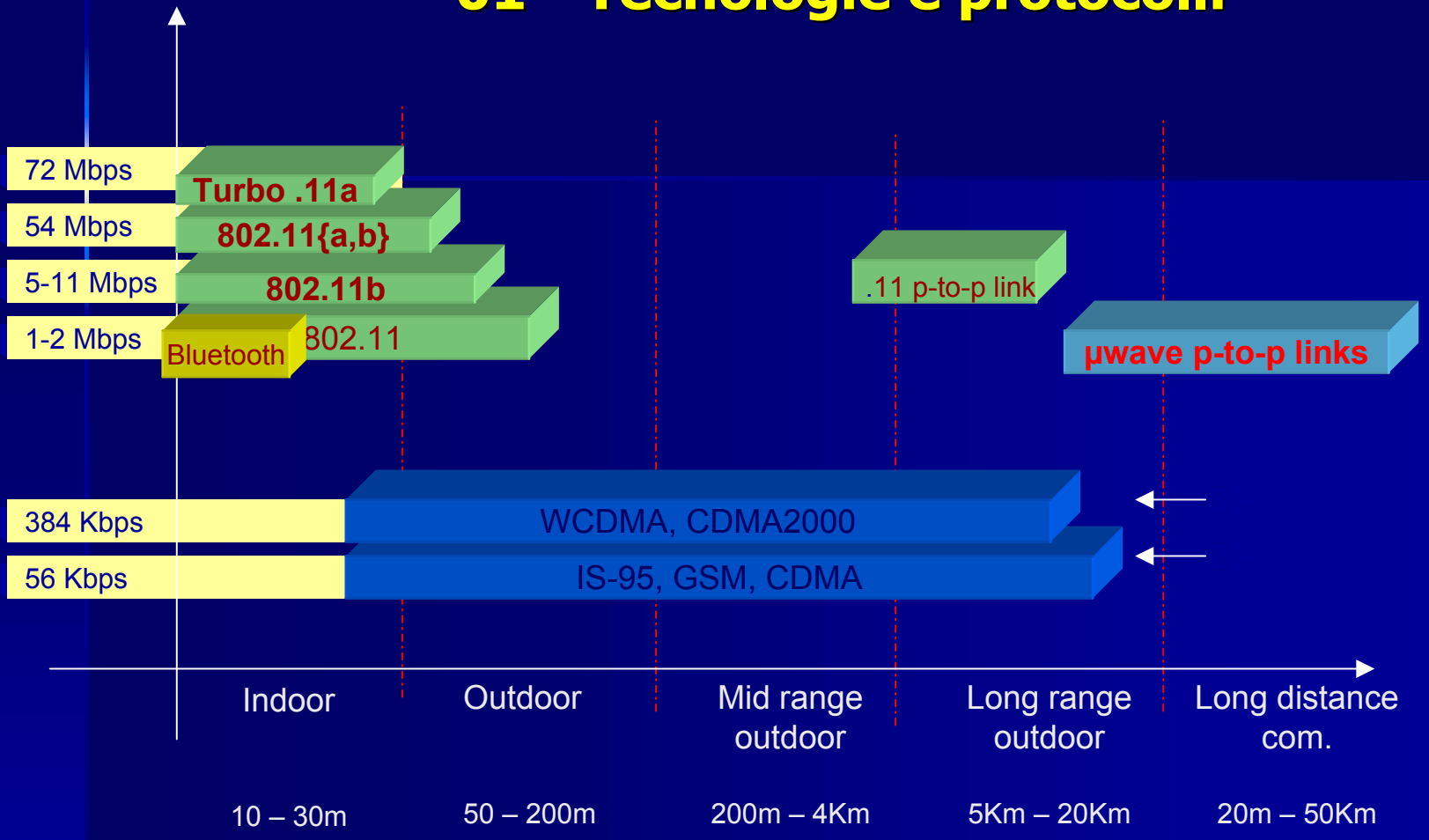
- Wireless Wide Area Network
  - GPRS, GSM, WCDMA



- Wireless Metropolitan Area Network (802.16)
- Wireless Personal Area Network
  - bluetooth

- Wireless Local Area Network
  - Wi-Fi 802.11

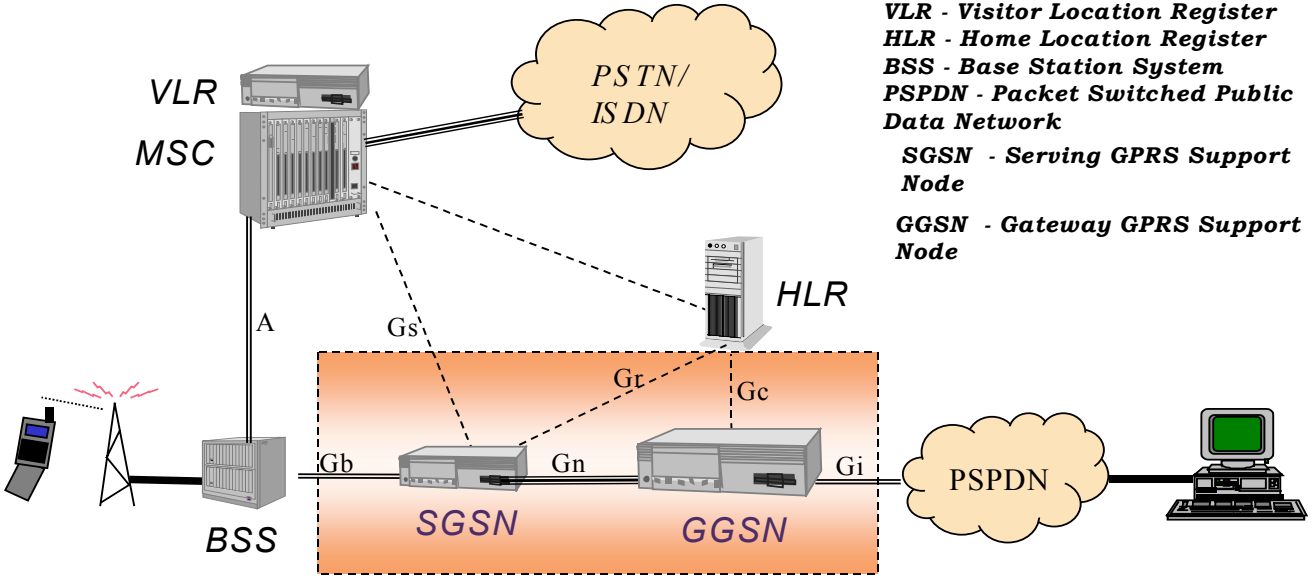
01 - Tecnologie e protocolli



01 - Reti cellulari (GPRS)

- Le prime reti dati cellulari si hanno con il GPRS che sfrutta piu' canali GSM in un unico canale logico
- L'autenticazione su rete GPRS e' paragonabile a quella con certificati digitali.
- L'infrastruttura prevede network logici sul network fisico cui si accede tramite APN
- La sicurezza del GPRS e' interamente gestita dall'operatore (security trough obscurity spesso e volentieri!)

01 - Reti cellulari (GPRS)



MSC - Mobile Switching Centre
VLR - Visitor Location Register
HLR - Home Location Register
BSS - Base Station System
PSPDN - Packet Switched Public Data Network
SGSN - Serving GPRS Support Node
GGSN - Gateway GPRS Support Node

N.B. Gc & Gs interfaces are optional

01 - Reti satellitari

- Le reti dati satellitari piu' usate sono:
  - DVB (Digital Video Broadcat)
  - VSAT (Very Small Aperture Terminal)
- Entrambe sono tecnologie broadcast
- Tirare giu' un satellite: facilissimo!
- Tecnologie instabili (pioggia, grandine)
- La crittografia e' "mandatory"

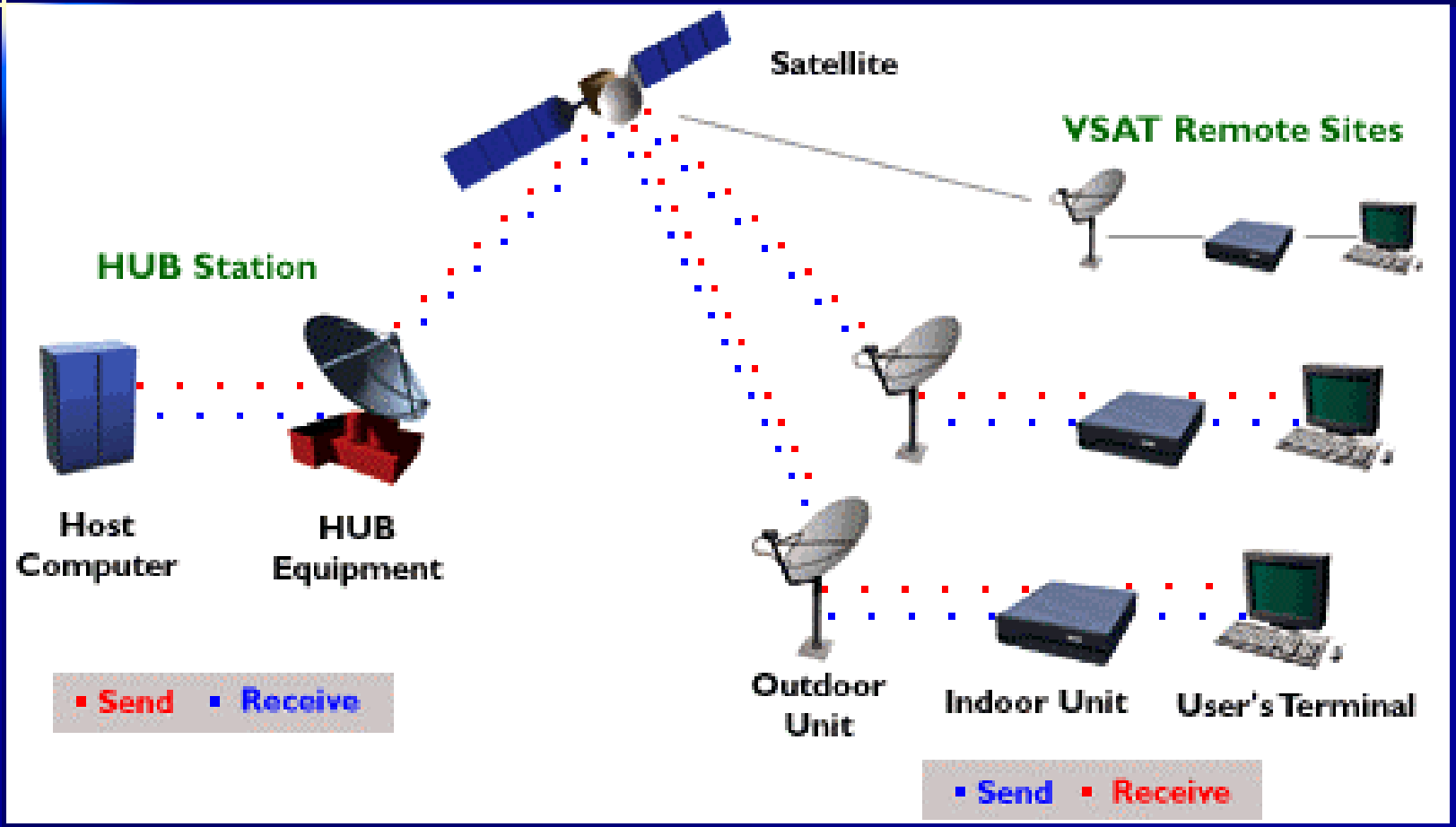
01 - Reti satellitari (DVB)

- Il DVB e' stato creato per le trasmissioni televisive digitali
- E' standard ETSI 302 192
- Per la trasmissione di IP si usa IP in DVB
- La crittografia usata per le trasmissioni televisive non centra nulla con quella per ip
- Viene impiegato impiegato spesso tramite routing asimmetrico con linee analogiche
- Spesso usato per push di contenuti multicast .

01 - Reti satellitari (VSAT)

- Il vsat e' ampiamente utilizzato dove vi e' carenza di infrastrutture
- VSAT richiede una attenta configurazione e puntamento degli apparati
- VSAT non raggiunge il grande pubblico per i suoi costi (2k euro per installazione)

01 - Reti satellitari (VSAT)



01 - Wireless local loop

- Utilizzate per l'ultimo miglio
- Gli apparati sono molto costosi, gli addetti al settore relativamente pochi e piu' esperti di radiofrequenze che di informatica
- Frequenze utilizzate molto alte (18ghz)
- La maggior parte delle volte non sono cifrati (secondo voi i link p-to-p degli operatori gsm sono cifrati???)
- La famiglia 802.11 sta' provvedendo con 802.11f (WMAN)

01 - Bluetooth

- Ideato nel 1994 da Ericsson
- Nel 1998 nasce lo Special Interest Group formato da IBM, Intel, Nokia, Toshiba and Ericsson
- Le specifiche tecniche complete sono disponibili solo per i membri del SIG
- Rientra nella categoria delle PAN, personal area network
- Supporta sia connessioni point-to-point che ad-hoc
- La sicurezza si basa su autenticazione non mutua con chiavi a 128bit

01 - Bluetooth

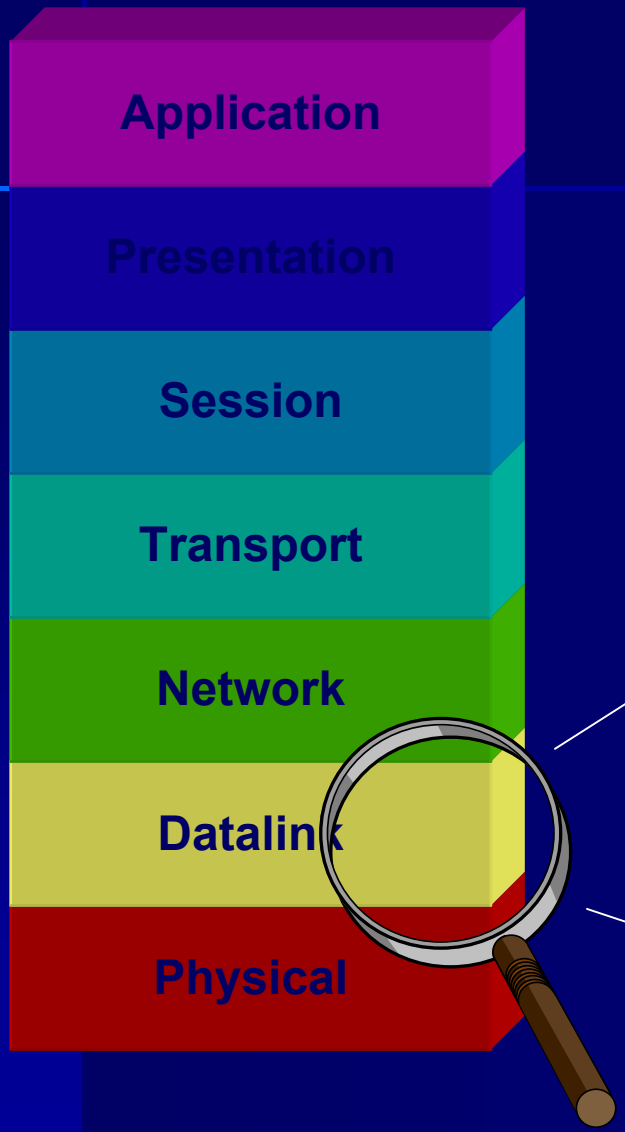
- rimpiazzare i cavi di connessione tra cellulari-palmari-pc
- Trova applicazioni di ogni tipo, pubblicita', informative, pagamento, identificazione
- Utilizza la stessa banda di frequenza dell'802.11 (2,4GHz)
- Dispositivi di bassa potenza
  - Classe 3 (1mW)
  - Classe 1(100mW)
- Utilizza uno schema Frequency Hopping Spread Spectrum predefinito poco sensibile alle interferenze
- Su uno spazio di 1MHz, l'hopping avviene ogni 625 microsecondi

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

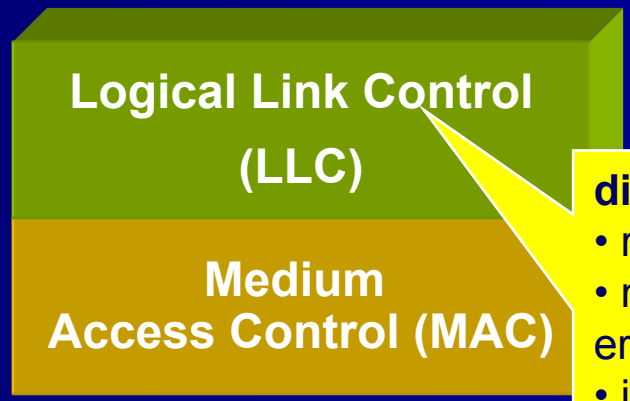
802.11:il Wi-Fi

02 - 802.11: cosa definisce



LLC fornisce un tipo di protocollo HDLC

MAC controlla l'accesso al canale fisico nel rispetto di un insieme di regole predeterminate



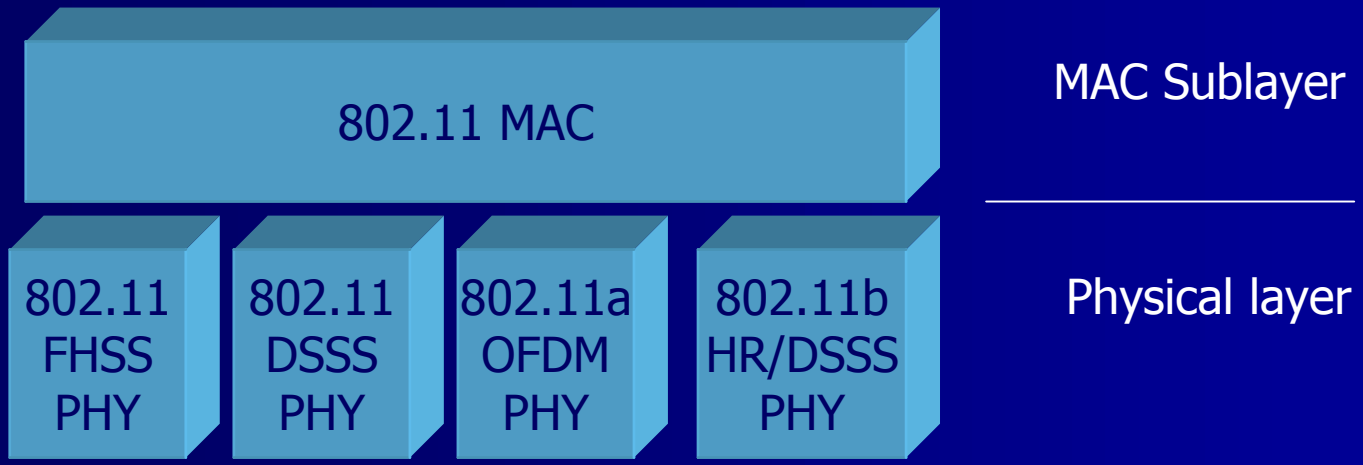
differenze:
- radio poco affidabile
- maggior tasso di errore
- intercettazione
- tutto il traffico passa per l'ap

02 - 802.11: cosa definisce

E' parte della famiglia di standard 802, relativa alle Local Area Network (LAN)

Lo standard 802 si concentra sui due layer più bassi della pila OSI:

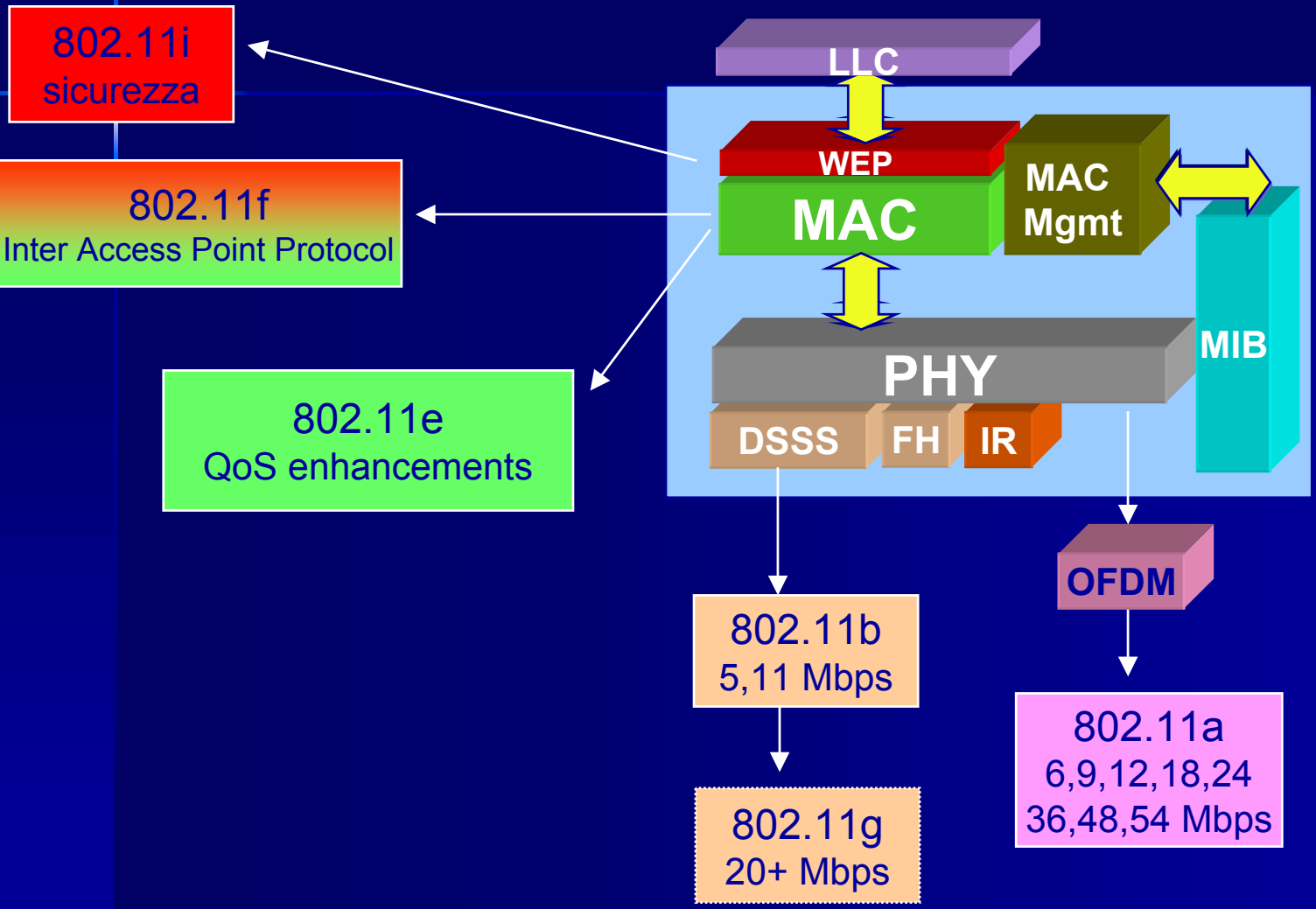
- Physical layer
- Datalink layer



02 - La famiglia 802.11 (1)

- 802.11 wireless lan 2.4ghz 1-2mb/s
- 801.11b wireless lan 2.4ghz 11mb/s
- 802.11a wireless lan 5.0ghz 54mb/s (problema in europa)
- 802.11g wireless lan 2.4ghz 54mb/s
- 802.1x funzionalita' di autenticazione per le reti wired
- EAP framework di autenticazione modulare
- TLS protocollo derivato da SSL utilizzato dai metodi EAP moderni
- PAP, CHAP, MSCHAPv1, MSCHAPv2 protocolli di "autenticazione" usati sul framework EAP

02 - La famiglia 802.11 (2)



02 – Modulazione DSSS e FHSS

- DSSS invia molti pacchetti differenti su alcune frequenze diverse nello stesso momento
  - Veloce
  - Costoso
  - Soggetto a interferenze

802.11b

- FHSS invia pochi pacchetti, poi cambia la frequenza (frequency hopping) e invia altri pacchetti
  - Poco costoso
  - Non molto soggetto a interferenze
  - Lento rispetto a DSSS

02 - Tipi di frame

CONTROLLO

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

DATI

- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

GESTIONE

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

02 - Frame di controllo

Servono a controllare l'accesso al mezzo trasmissivo wireless

Request To Send (RTS) – serve a avere accesso almezzo per la trasmissione di grossi frames (la dimensione e' definita dal soglia RTS della scheda wireless)

Clear To Send (CTS) – e' la risposta a un RTS

Acknowledgement (ACK) – sono usati in ogni trasmissione (dati, frame frammentati, ecc)

PowerSave Poll (PS-Poll) – inviati dal client all'AP quando il client si "risveglia" dalla modalità di power saving

02 - Frame di gestione (1)

Beacon – vengono trasmessi a intervalli regolari e annunciano l'esistenza di una rete

Probe Request – trasmesso dal client che cerca una rete, contiene due soli campi: SSID e velocità di trasmissione

Probe Response – Se il probe request incontra una rete con parametri che soddisfano le richieste, l'AP invia un probe response

Disassociation – sono usati per terminare una relazione di associazione

Deauthentication – sono usati per terminare una relazione di autenticazione

02 - Frame di gestione (2)

Association Request – una volta identificata una rete con parametri compatibili, il client invia questo frame per unirsi alla rete

Reassociation Request – in tutto simile al precedente tranne che contiene l'indirizzo dell'AP cui il client e' associato nel momento dell'invio. Questo consente al nuovo AP di contattare l'altro per farsi passare i dati di associazione

Association Response

- da AP in risposta a uno dei frame precedenti

Reassociation Response

Authentication – inviati dal client per autenticarsi con l'AP

02 - Frame dati

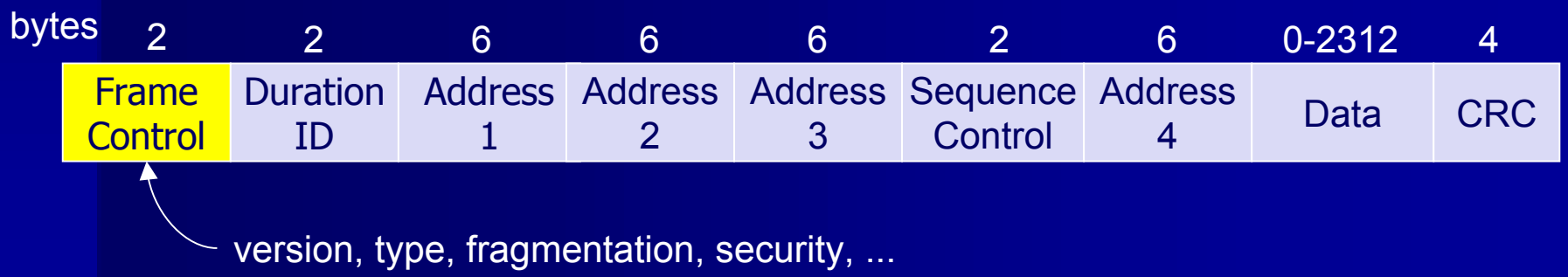
Trasportano i dati dei livelli di protocollo superiori

Possono trasportare dati oppure assolvere funzioni di gestione

Tipo di frame	trasporta dati	non trasporta dati
data	x	
data+CF-ACK	x	
data+CF-Poll	x	
data+CF-ACK+CF-Poll	x	
Null		x
CF-ACK		x
CF-Poll		x
CF-ACK+CF-Poll		x

02 - Formato dei frames 802.11

- Tipi
  - Frame di controllo, frame di management, frame di dati
- Numeri di sequenza
  - Importanto contro i frame dplicati per ACK perduti
- Indirizzi
  - ricevente, trasmittente (fisico), identificativo del BSS, mittente (logico)
- Vari
  - Tempo di invio, checksum, frame di controllo, dati



Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

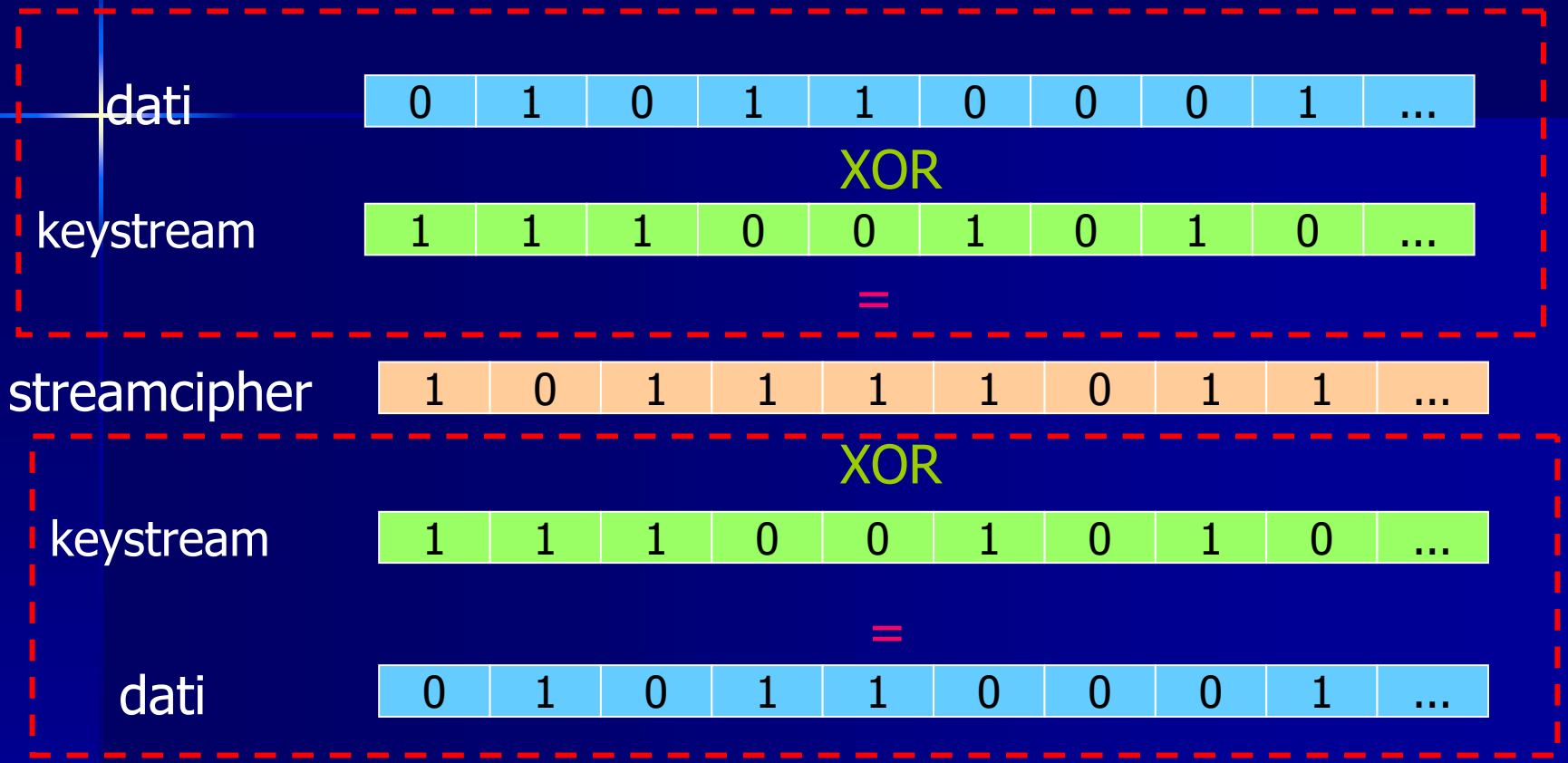
03 – Il WEP (1)

- E’ una “chiave condivisa” (shared key): deve essere conosciuta dall’Access Point e dal client.
- “segreto di pulcinella” e difficile scalabilita’
- Si basa su RC4 (cipher stream) e operazioni di XOR con lo stream dei dati in transito
- L’Initialization Vector (IV) del WEP che serve a inizializzare il cipher stream viene trasmesso in chiaro
- analizzando sufficiente traffico e’ possibile individuare lo stream chiave e decifrare.

03 – Il WEP (2)

- WEP esiste con chiave da 40bit o 128bit
- la versione a 128bit non era stata standardizzata (104bit o 128bit o 152bit ? Interoperabilità?) a causa delle leggi sulla crittografia degli USA.
- lo standard 802.11b definisce un CRC a Mac layer che porta ad accettare come validi pacchetti non cifrati, purche' il loro checksum sia corretto. (integrità dei dati non garantita)

03 - Meccanismo del WEP



03 - Caratteristiche dello streamcipher

- Per tenere corta la secret key si usa il PRNG (pseudo random number generator)

  Secret key -> PRNG -> keystream

- Mittente e ricevente dovranno quindi usare la stessa chiave segreta e lo stesso algoritmo PRNG per poter essere interoperabili

- RC4 (di RSA) usa l'operazione di or esclusivo (XOR) per ottenere lo streamcipher a partire dal keystream e i dati

03 - Wep e C I A

• confidenzialità – nel transito tra client wireless e access point, tramite la cifratura per cui viaggia lo streamcipher e non il dato in chiaro

• Integrità – un controllo di integrità sui dati trasmessi garantisce che non siano modificati nel transito

• autenticazione – attraverso l'utilizzo della chiave si ottiene l'autenticazione del dispositivo wireless client nei confronti dell'AP

03 - Wep: una coperta troppo corta

Il wep non riesce a essere efficace nel garantire i requisiti di sicurezza C I A:

- Confidenzialità – e' stata dimostrata la vulnerabilita' dell'RC4 nel 2001. Riutilizzo del keystrem, Initialization Vector trasmesso in chiaro

- Integrità – e' stato dimostrato che e' possibile far passare come integri anche pacchetti che non lo sono. Non usa hashing, ma Cyclic Redundancy Check a 32 bit

- autenticazione – l'autenticazione non e' bidirezionale e non riguarda l'utente ma il solo dispositivo

- Problemi di distribuzione della chiave (shared secret) su molti utenti

03 - L'attacco crittografico al wep

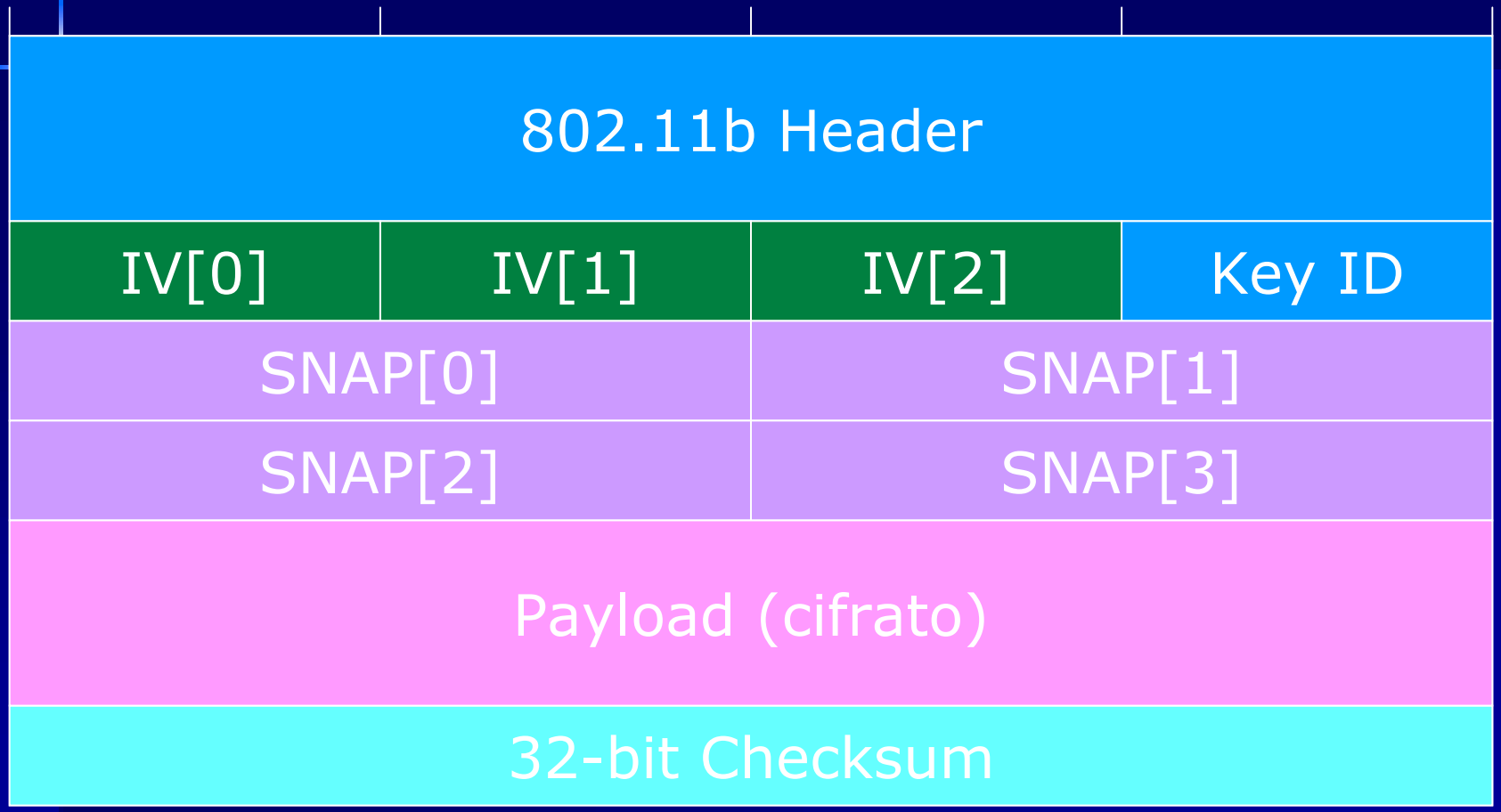
Abbiamo visto le debolezze intrinseche al protocollo. Vediamo l'attacco.

Viene sfruttata una debolezza nel modo in cui viene generato il keystream.

Assumendo di poter recuperare il primo byte del payload cifrato Poiche' 802.11 utilizza il Link Layer Control, il cui primo byte e' 0xAA (SNAP header), tramite uno xor con il primo byte cifrato del payload, e' possibile ricavare il primo byte del keystream

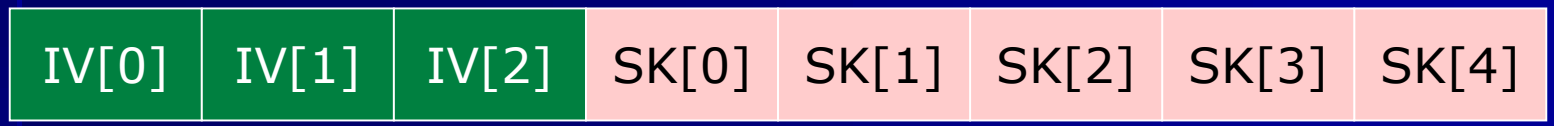
Questo attacco e' lineare. Al crescere dei byte del keystream decifrati, cresce la velocita' di decifratura dei rimanenti.

03 - Il frame con wep



03 - WEP Data Transmission

Keystream = InitializationVector . StaticKey



03 - WEP Data Transmission

Node

Node

K = IV . SK

IV viene generato o con un contatore o randomicamente

03 - WEP Data Transmission

03 - WEP Data Transmission

Il ricevente usa l'IV ricevuto e la chiave statica SK in suo possesso per decifrare

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

04 – Autenticazione

- L'autenticazione e' uno degli elementi piu' critici nella sicurezza.
- Una buona infrastruttura di autenticazione protegge dalla maggior parte degli attacchi
- Le fasi del processo di autenticazione:
  - Autenticazione
  - Autorizzazione
  - Accounting

04 - Identificazione e Autenticazione (1)

- Consente a un entita' (una persona o un sistema) di dichiarare la sua identita' a un'altra entita' .
- Di solito l'entita' che vuole identificarsi deve dimostrare la conoscenza di un segreto all'altra.
- Strong authentication: L'entita' rivela la conoscenza del segreto all'altra senza rivelare S a quest'ultimo

- Autenticarsi significa disporre di credenziali

04 - Identificazione e Autenticazione (2)

- Le credenziali possono essere di alcuni tipi:
- **Quello che sai**
  - Password, pin, compleanno di tua madre.
- **Quello che hai**
  - Token, badge, smartcard
- **Quello che sei**
  - Fingerprint, voice recognition, analisi della retina
- **Combinazioni:**
  - Quello che hai + quello che sai . Token con pass dinamiche
  - Quello che sei + quello che sai . Fingerprint+pin .

04 - Autorizzazione

- Dopo avere verificato l'identita' del soggetto il sistema informatico deve determinare i suoi diritti e privilegi: questo e' il processo di autorizzazione.

- Consentire all'utente piero del marketing di potere accedere alle sole risorse (reti, fileserver, web interno, etc) del marketing e non a quelle dell'amministrazine

04 - Accounting

- La registrazione di eventi relativi alle autenticazioni e autorizzazioni
- Es:
  - User pippo logged in on 7 Mar 2002 on port 12
  - Failed password for user mario on 8 Mar 2002

04 - Protocolli di autenticazione: (1)

Lo scambio delle credenziali deve essere immune allo sniffing e al replaying dei dati.

Per questo sono e' fondamentale avere dei solidi meccanismi per gestire l'autenticazione.

Questi meccanismi sono definiti come protocolli di autenticazione ma non tutti sono sicuri

La combinazione di questi protocolli assieme ad altre tecnologie di autenticazione sono il fondamento della sicurezza del Wi-Fi

04 - Protocolli di autenticazione: (2)

- I protocolli di autenticazione definiscono delle metodologie per lo scambio di crede ziali fra due peer.
- Creati inizialmente per le necessita' del ppp i principali protolli sono:
  - PAP (Password authentication protocol)
  - CHAP (ChallengeReponse Handshake authentication protocol)
  - MS-CHAP v1/v2 (Variante Micrsoft del CHAP)
  - EAP (Extendable authentication protocol)

04 - Protocollo PAP (1)

PAP (Password Authentication Protocol): Il modulo base di autorizzazione - nome utente e password - viene trasferito sulla rete e confrontato con una tabella delle coppie nome-password che risiede nel server.

E' definito dall' RFC 1334 .

04 - Protocollo PAP (2)

- **La password attraversa la rete in chiaro**
- PAP non puo' essere riutilizzato piu' volte .
- PAP non offre grandi garanzie di sicurezza.
- Non e' un metodo EAP ed e' implementato solo nel tunnelled protocol EAP-TTSL

04 - Protocollo CHAP (1)

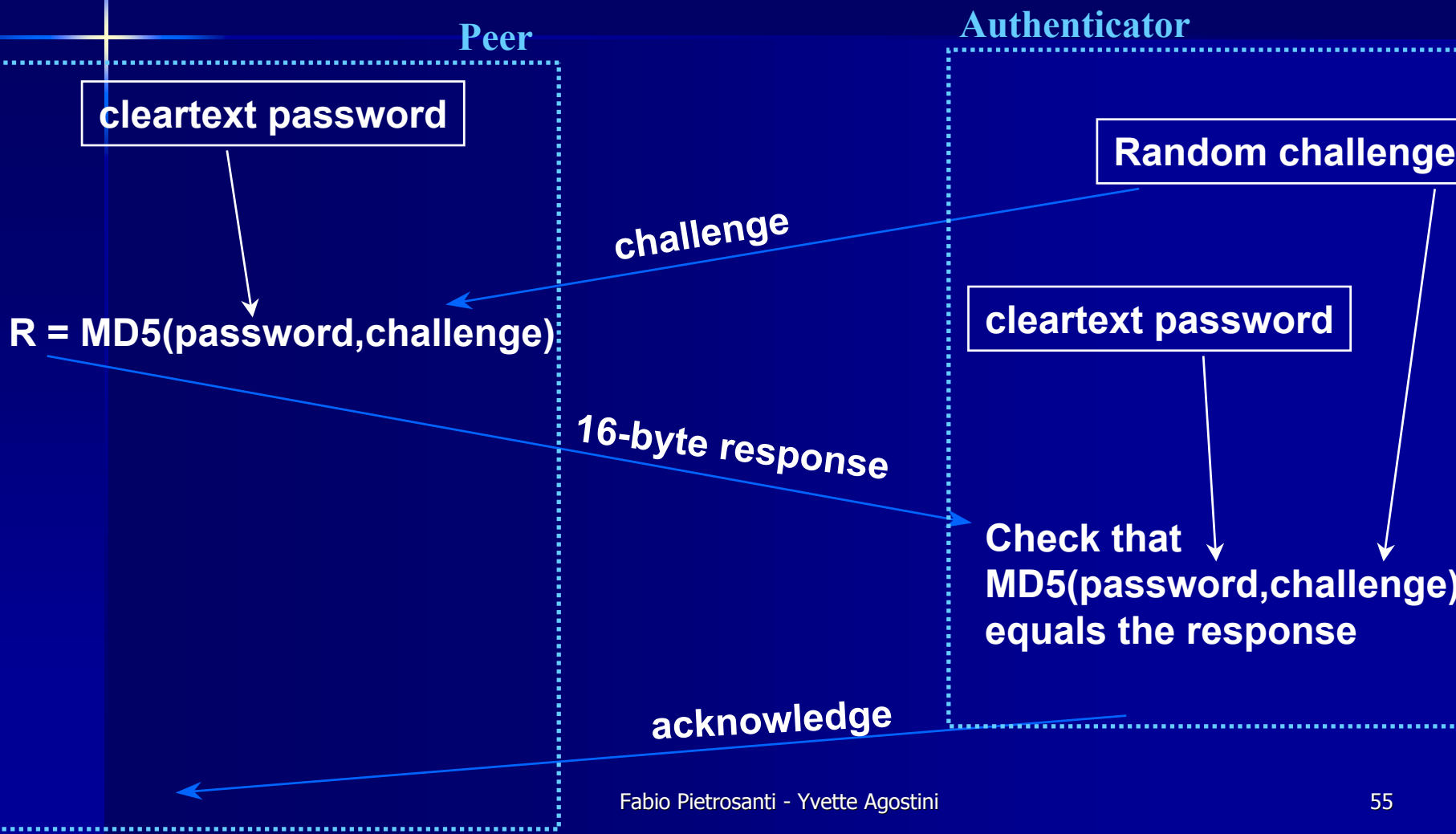
CHAP(Challenge Authentication Password Protocol):

- l'autenticatore invia, dopo aver stabilito la connessione, un challenge al client che chiede di essere autenticato.
- Il client prova di essere in possesso dello shared secret rispondendo al suo challenge .

04 - Protocollo CHAP (2)

- Puo' essere utilizzato piu' volte all'interno di una sessione per verificare se questa e' stata hijackata .
- E' definito secondo RFC 1994
- Non supporta la mutua autenticazione.
- Richiede la disponibilita' dello shared secret in chiaro
- Non e' un metodo EAP ed e' implementato solo nel tunnelled protocol EAP-TTSL .

04 - Protocollo CHAP (3)



04 - Protocollo MS-CHAP v1

- **MS-CHAP v1** e' un protocollo proprietario creato da Microsoft che poi lo ha documentato nell'RFC 2433 ed e' molto simile al CHAP .
- Risolve il problema del dovere mantenere la password in chiaro su entrambi i peer
- Si basa sul concetto che il client, conoscendo l'algoritmo di cifratura (hashing) e la password, puo' generare l'hash di questa senza farla transitare in chiaro sulla rete.
- E' particolarmente utilizzata in ambienti microsoft vista la sua compatibilita' con i meccanismi di challenge response dell'NTLM .
- Non e' un metodo EAP ed e' implementato solo nel tunnelled protocol EAP-TTSL.

04 - Protocollo MS-CHAP v2

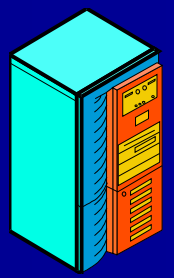
- **MS-CHAP v2** e' un protocollo proprietario creato da Microsoft come alternativa ad alcune vulnerabilita' intrinseche della MS-CHAP v1 .
- E' documentato dall' **RFC 2759**
- Ha un migliore supporto per la generazione delle chiavi
- Supporta la mutua autenticazione
- Ha eliminato il supporto verso vecchi client (w95)
- E' sia un metodo PPP che un metodo EAP
- Puo' essere utilizzato cosi' come e' con **EAP-TTSL**
- E' descritto come metodo EAP come **EAP-MS-CHAP-V2** e puo' essere usato nei tunneled protocol **EAP-TTSL** e **PEAP**

04 - Protocollo EAP (1)

- EAP (Extensible Authentication Protocol) e' stato sviluppato per il PPP in risposta alla crescente richiesta di un sistema di autenticazione di utenti che accedono da un sistema remoto che consentisse di utilizzare altri dispositivi di protezione
- Fornisce un meccanismo standard per il supporto di metodi di autenticazione aggiuntivi nell'ambito delle connessioni PPP
- **E' LA BASE DELL'AUTENTICAZIONE NEL Wi-Fi**

EAP

La negoziazione a dopo



04 Protocollo EAP (2)

- È possibile aggiungere il supporto per altri schemi di autenticazione tra cui:
  - Token card
  - Password temporanee
  - Autenticazione di chiavi pubbliche tramite smart card
  - Certificati
- La tecnologia EAP, insieme ai metodi di autenticazione EAP, è un componente essenziale per garantire connessioni protette su reti private virtuali che offre un elevato livello di protezione da
  - Tentativi di accesso non autorizzato
  - Individuazione delle password superiore a qualsiasi altro metodo di autenticazione (compreso CHAP)

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

05 - 802.1X port security

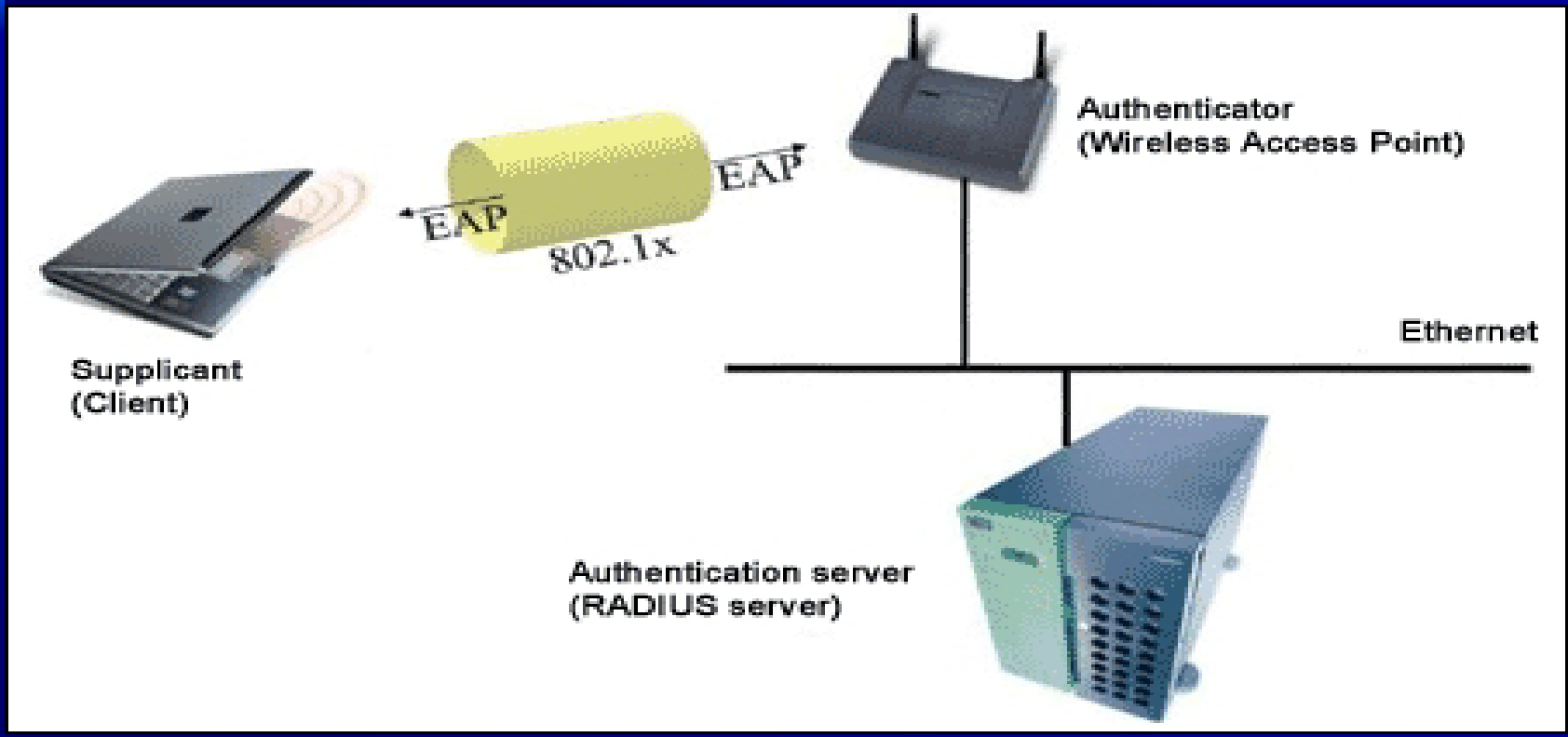
- Vista la necessita' di fornire un framework di controllo accessi per le reti ethernet e' stato creato lo standard 802.1X .
- "sfornato" nel 1999, ratificata la versione 1 jun2001
- E' stato da poco migliorato dall'802.1aa
- Senza 802.1x non sarebbe possibile authenticare dal layer2 gli utenti per l'accesso alla rete ethernet
- Pochi apparati e OS lo supportano
- Si occupa di autenticare, non cifrare
- Si autentica un soggetto e non un oggetto
- URL: http://www.ieee802.org/1/pages/802.1x.html

05 - 802.1X port security

- Requisiti che si vogliono raggiungere per il wifi con l'802.1x
  - Mutua autenticazione fra utente e network
  - Cifratura delle credenziali inviate
  - Generare dinamica chiavi crittografiche (WEP, TKIP, etc)
- I requisiti di una rete wired sono MOLTO diversi da una rete wireless

05 - 802.1X port security, EAP

- 802.1x utilizza per l'autenticazione il framework EAP

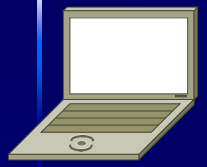


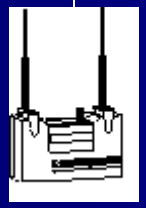
05 - 802.1X port security, protocolli

- Esistono due protocolli per i messaggi
  - EAPOL (EAP over LAN) usato per l'autenticazione
  - EAPOW (EAP over WirelessLAN) usato per il delivery della chiave WEP e per l'inizio della sessione
  - EAPOL ha un ethertype dedicato 0x888e
- Ci sono tre elementi:
  - Supplicant
  - Authenticator
  - Authentication server (RADIUS)

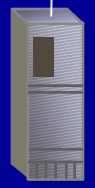
05 - Terminologia IEEE 802.1x

semi-public network





EAP over RADIUS



RADIUS server

Supplicant

Operates on client

Authenticator

Operates on devices at network edge, like APs and switches

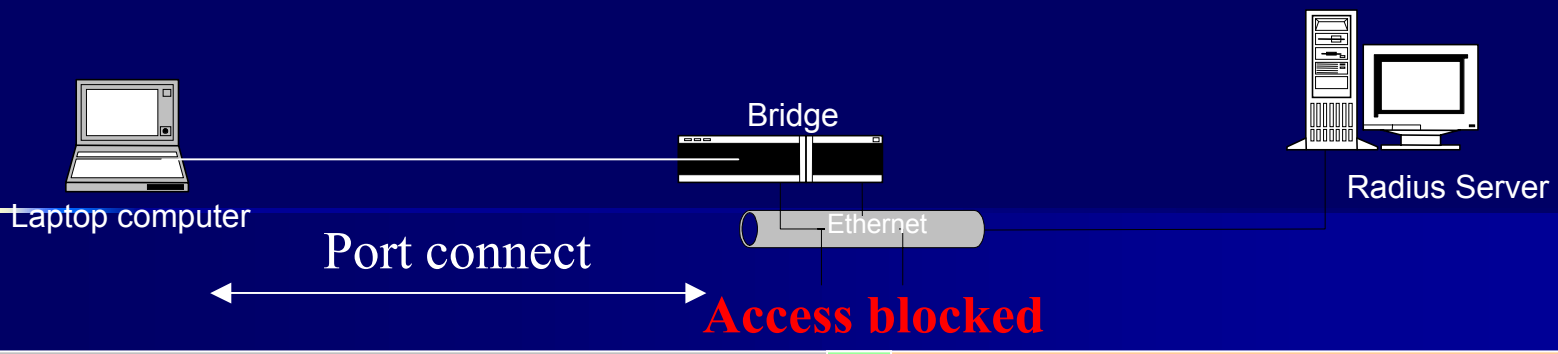
Authentication Server

EAP plug-in goes in RADIUS server

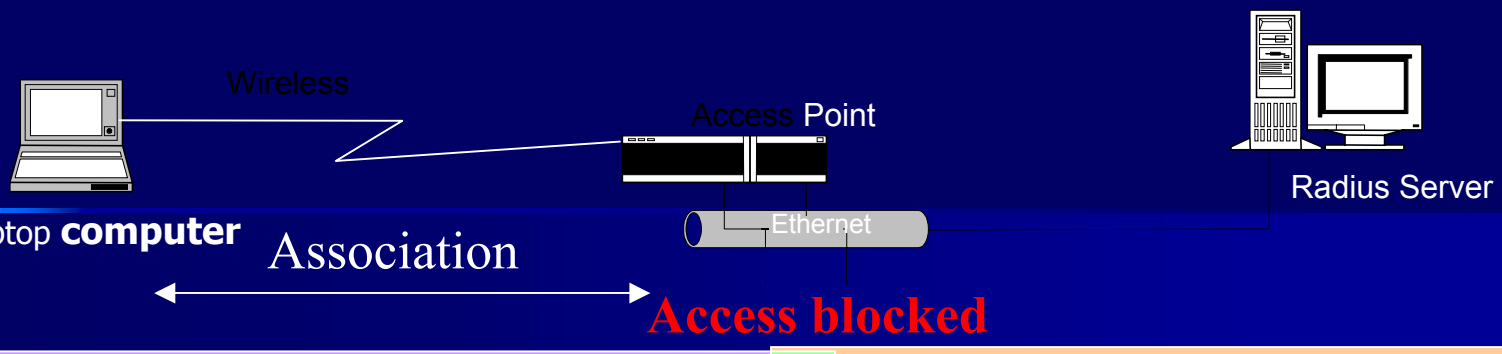
Open port:
Authentication traffic

Controlled port:
Data traffic

05 - 802.1x over 802.3



05 - 802.1X over 802.11



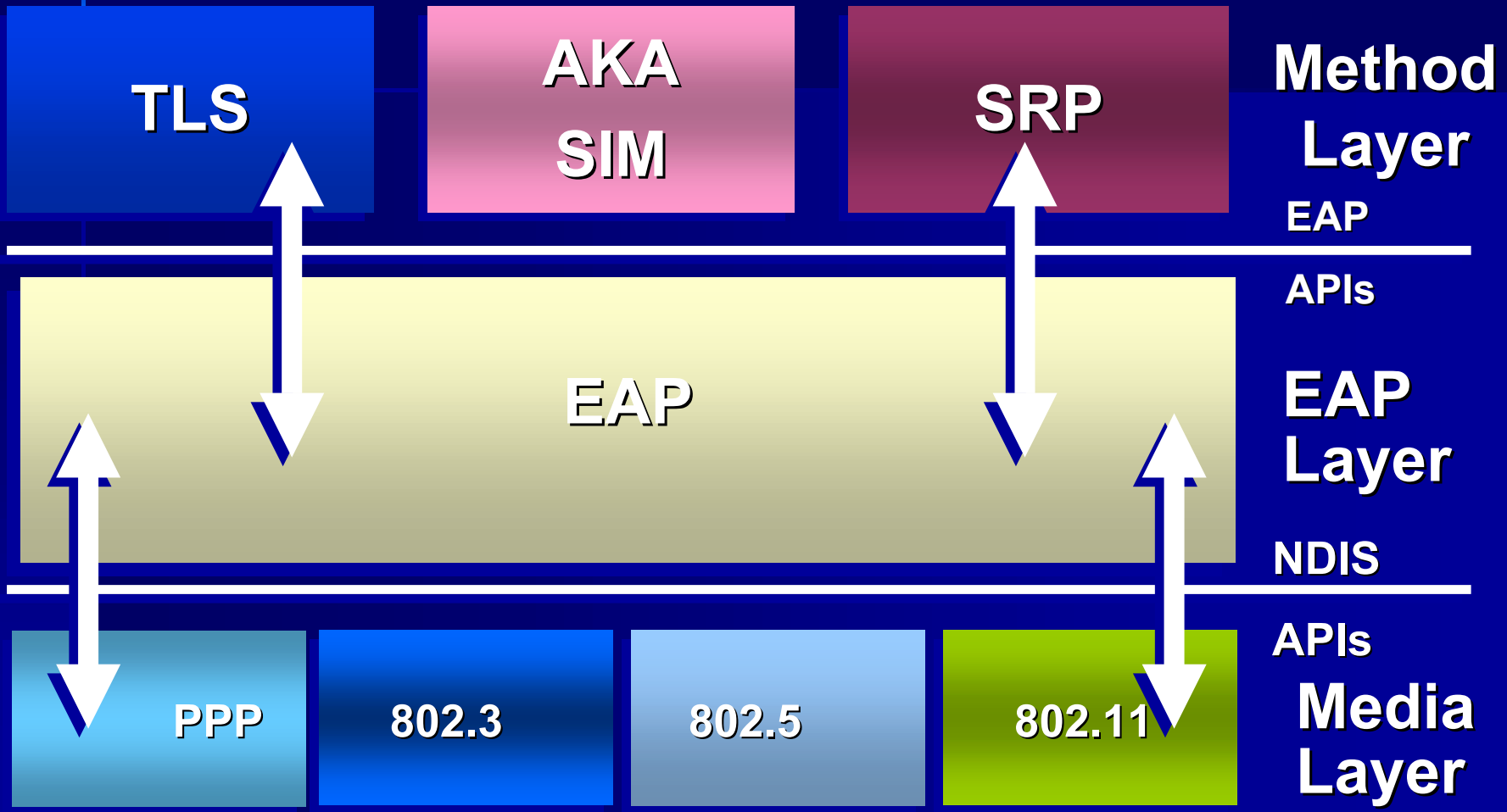
Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

06 – Extensible authentication protocol

- Extensible Authentication Protocol e' un framework di autenticazion defintio secondo RFC 2284
- Consiste di diversi schemi di autenticazione detti metodi EAP
- Originalmente definito per il PPP con pochi metodi standard
  - –plain password hash (MD5) (non mutua)
  - –GSS-API (Kerberos)
  - –OTP Tokens (non mutua)
  - –TLS (based on X.509 certificates)
- Le implementazioni proprietarie sono molteplici e le strategi per favorirne la diffusione ancora di piu'

06 - Architettura EAP secondo standard



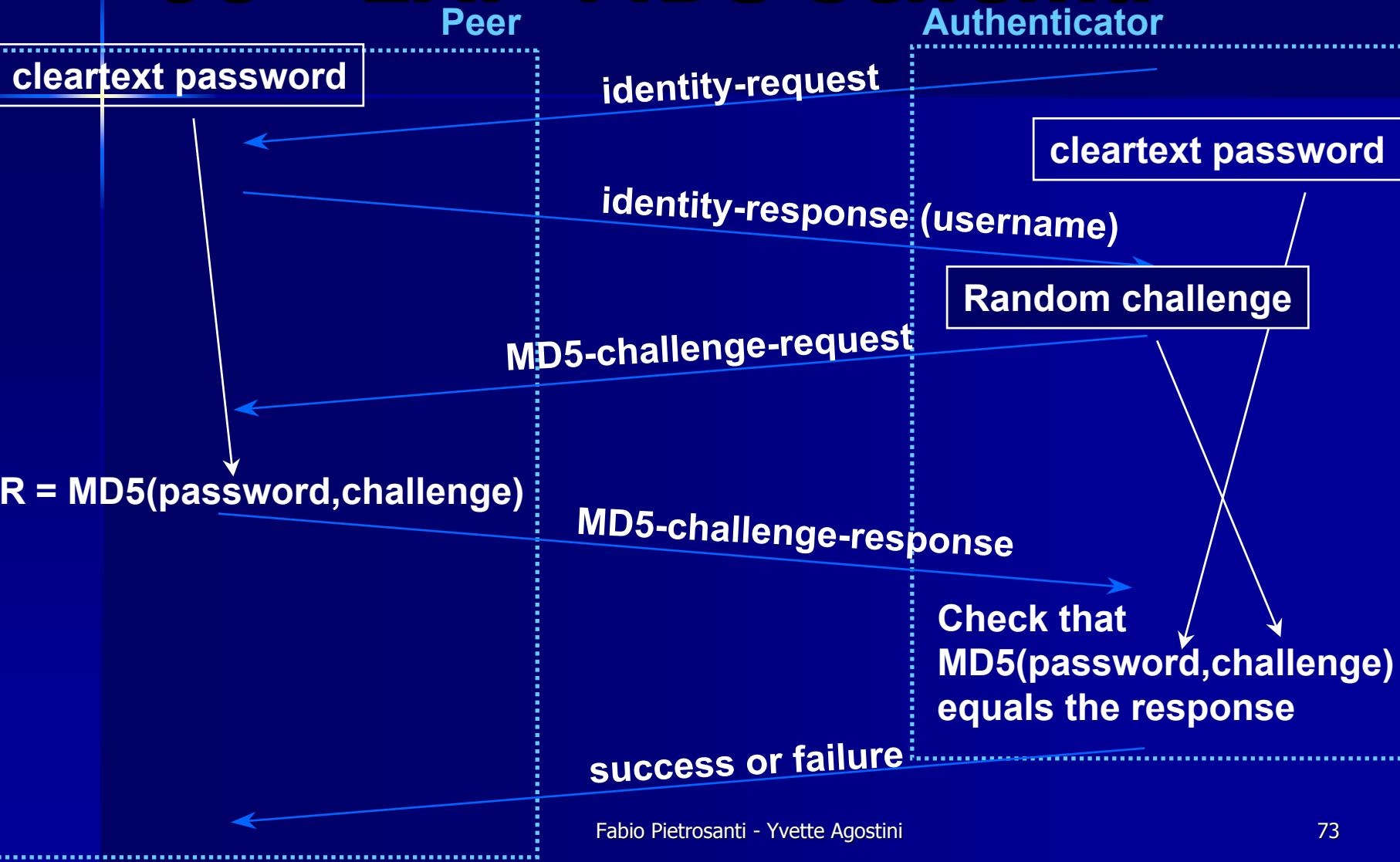
06 - I metodi EAP

- EAP-MD5 (type 4)
- EAP-SIM / EAP-AKA
- EAP-LEAP
- EAP-TLS Transport Layer Security (type 13)
- EAP-TTLS Tunnelled TLS (type 21)
- EAP-PEAP Protected EAP (type 25)
- Lista completa: http://www.iana.org/assignments/ppp-numbers

06 - EAP-MD5

- E’ simile al chap
- Viene calcolato l’hash md5 e inviato in chiaro
- E’ intercettabile l’hash e attaccabile a bruteforce e man in the middle
- Non supporta la mutua autenticazione
- Non supporta la derivazione della chiave wep dinamica
- NON VA’ USATO!!!

06 - EAP-MD5 schema



06 - EAP-SIM / EAP-AKA

- Destinato all'utilizzo nelle PWLAN
- Rilasciate pochi giorni fa' WLAN-SIM 1.0 http://wlansmartcard.org che include 802.1x, EAP su tls e WPA
- Concettualmente simile a EAP-TLS per il funzionamento delle SIM e USIM
- Entrato a far parte degli standard 3GPP
- Supporta il fast reconnect
- Sara' utilizzatissimo secondo alcune strategie

06 - EAP-LEAP

- Protocollo proprietario Cisco basato su username e password per le credenziali.
- Utilizzato da cisco per introdurre TKIP e MIC proprietari
- Attaccabile tramite brute force (cisco cerca di fare migrare verso PEAP)
- Disclosure della vulnerabilita' LEAP
- Statistiche dicono che nel mondo enterprise rappresenta il 46% degli schemi di autenticazione

06 - EAP-LEAP

client

AP

RADIUS server

Start

AP blocks all requests until authentication completes

Request identity

identity

identity

RADIUS server authenticates client

Client authenticates RADIUS server

Derive key

Derive key

broadcast key

key length

AP sends client broadcast key, encrypted with session key

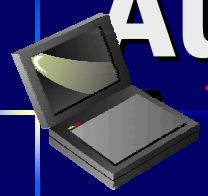
06 - EAP-TLS (1)

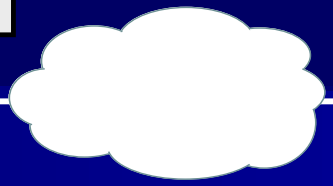
- E' il protocollo EAP che usa solo TLS
- Definito secondo (RFC 2716)
- TLS gestisce la negoziazione di:
  - crittografia
  - mutua autenticazione
  - key management.
- EAP-TLS definisce lo scambio di messaggi EAP fra client e server
  - Identity Request/Response, TLS Start, TLS client_hello, TLS server_hello, etc.

06 - EAP-TLS (2)

- E’ il piu’ sicuro dei protocolli basati su TLS
- Supporta il delivery della chiave WEP dinamica
- L’entropia e le funzioni crittografiche del TLS sono utili per la generazione delle chiavi WEP/TKIP/CCMP
- Richiede l’esistenza o l’implementazione di una PKI
- La gestione dei certificati digitali client side e’ estremamente onerosa

06 - EAP-TLS Authentication





RADIUS server

Supplicant

AP

EAPOL Start

Start EAP Authentication

EAP-Request/Identity

Ask client for identity

EAP -Response/Identity (UserID)

RADIUS Access request

Access Request with UserID

Server-side TLS

....

Perform sequence defined by EAP-TLS

Client-side TLS

key

RADIUS Access success (Pass session key to AP)

key

EAP success

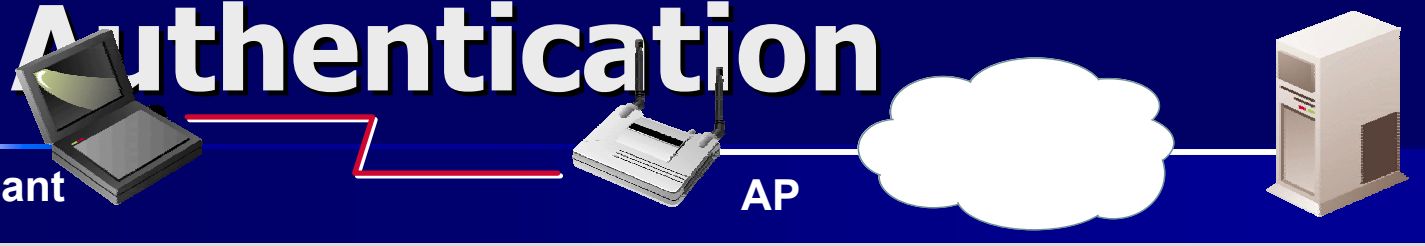
Client derives session key

EAPOL-Key (multicast)

EAPOL-Key (session parameters)

Deliver broadcast key encrypted with session key && session

06 - EAP-TLS Authentication



EAP-TLS Start

[EAP-Type=EAP-TLS, Start bit set, no data]

[EAP-Type=EAP-TLS (TLS client_hello)]

EAP-Response

[EAP-Type=EAP-TLS (TLS server_hello, TLS certificate, TLS server_key_exchange, TLS certificate_request, TLS server_hello_done)]

EAP-Request

[EAP-Type=EAP-TLS (TLS certificate, TLS client_key_exchange, TLS certificate_verify, TLS change_cipher_spec, TLS finished)]

EAP-Response

EAP-Request

[EAP-Type=EAP-TLS (TLSchange_cipher_spec, TLS finished)]

[EAP-Type=EAP-TLS]

EAP-Response

EAP-Success

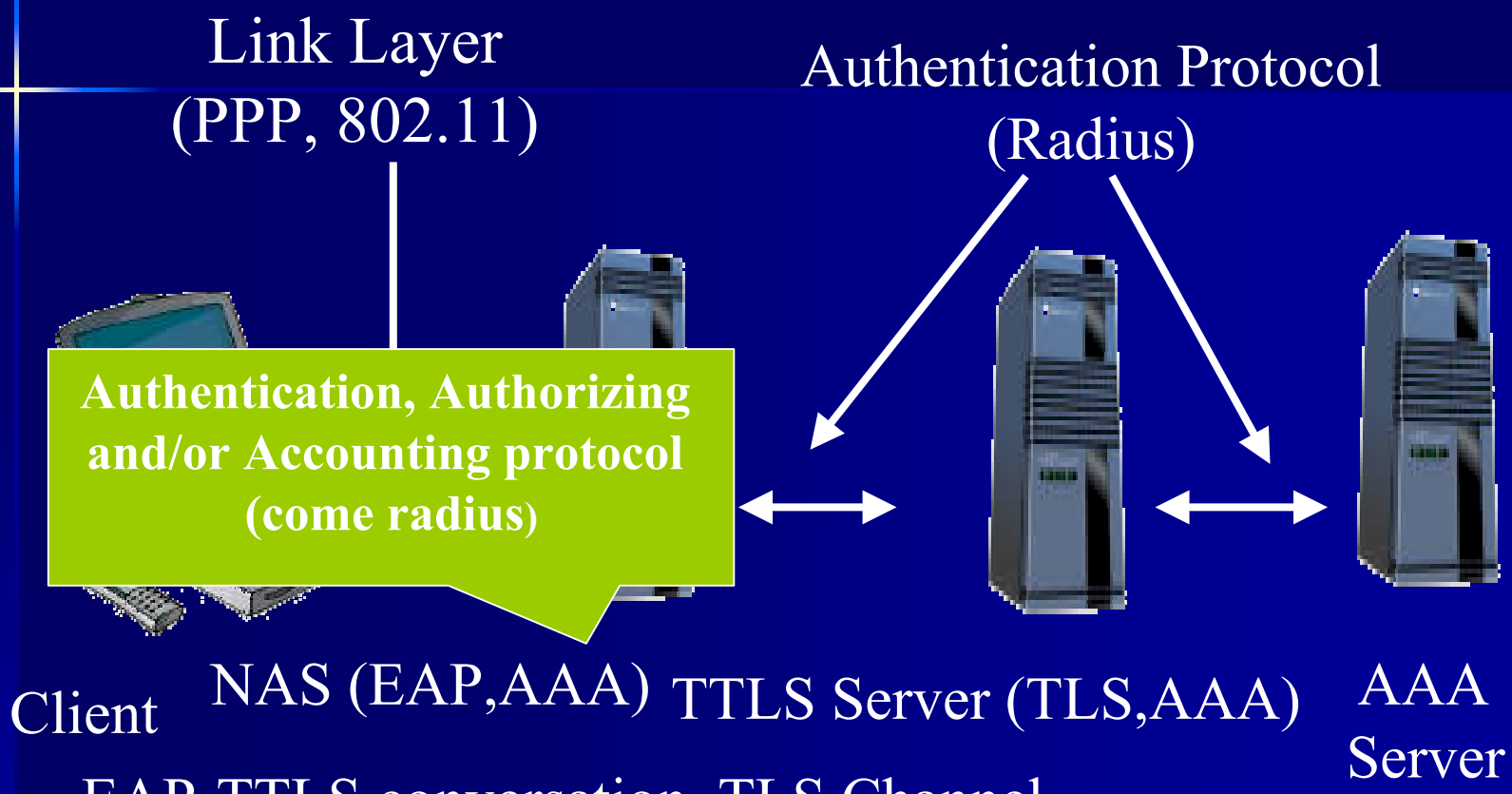
06 - I tunneled protocol

- Per utilizzare i metodi di autenticazione “tradizionali” e’ necessario creare un canale di comunicazione sicuro
- Per fare cio’ si utilizza il TLS dando vita ai metodi EAP-TTLS e EAP-PEAP
- Il vantaggio e’ l’utilizzo dei vecchi metodi di autenticazione senza dovere cambiare infrastrutture
- Lo svantaggio e’ che recentemente sono stati dimostrati alcuni attacchi man in the middle se non si prendono particolari precauzioni

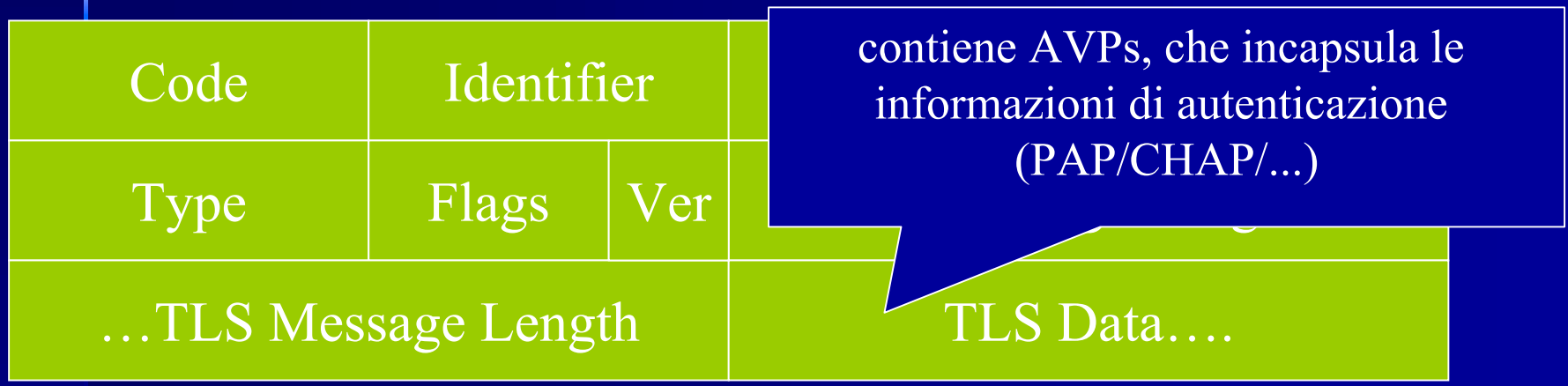
06 - EAP-TTLS

- E’ stato sviluppato in risposta alla complessita’ d’implementazione di EAP-TLS
- E’ estremamente simile al EAP-PEAP consentendo di utilizzare vecchi metodi di autenticazione mantenendo la sicurezza data dal TLS
- E’ un protocollo a due stadi, il primo dei quali server per creare un canale di comunicazione “sicuro”
- Il secondo stadio e’ normale scambio di credenziali secondo protocolli standard (pap, chap, mschapv1/v2)
- Proposto originariamente dalla funk software draft-ieft-pppext-eap-ttls-02.txt

06 - EAP-TTLS i partecianti



06 - EAP-TTLS formato del pacchetto



- Code: 1- Request 2- Response
- Identifier – Used to match response to request
- Type- 21 (EAP-TTLS)
- Flags: Length included, More fragments, Start flag

06 - EAP-TTLS AVP

- Nel PEAP le informazioni scambiate fra client e server sul tunnel TLS sono altri pacchetti EAP (EAP-MSCHAP-V2) mentre in EAP-TTLS sono scambiati AVP:
  - **attribute-values pairs**
- Il formato AVP e' formato dell'EAP-TTLS e' compatibile con il formato AVP del radius facilitando le operazioni di forwarding delle autenticazioni fra authenticators e authentication server

06 - EAP-TTLS – Fase 1

Client

EAP-Request / Identity

EAP- Response / Identity [My Domain]

EAP-Request (Type= EAP-TTLS, start)

TLS Handshake

TTLS Server

TLS Channel Established

EAP- Response (empty)

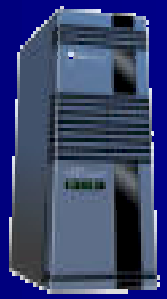
06 - EAP-TTLS – Fase 2

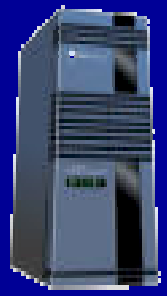
Scambio di AVP sul canale TLS di EAP-TTLS

EAP-Success/ EAP-Failure

AVPs (extracted from the TTLS records)

Success/Failure





Client

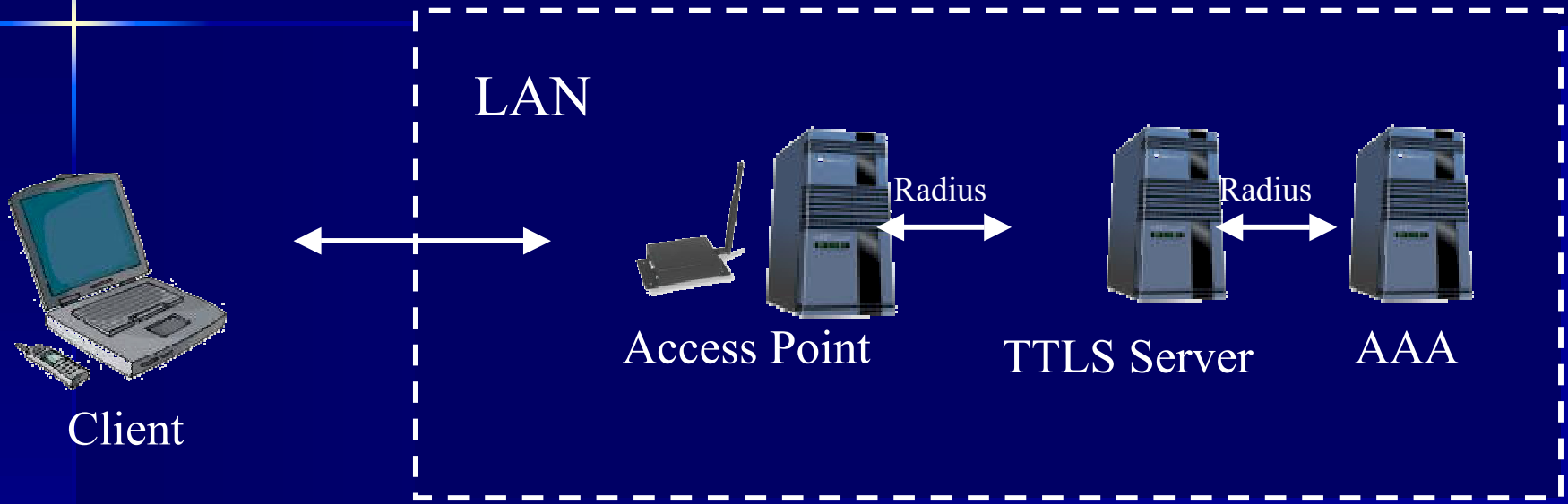
TTLS Server

AAA Server

I messaggi di scambio TTLS usano l'AP solo come pass-trough

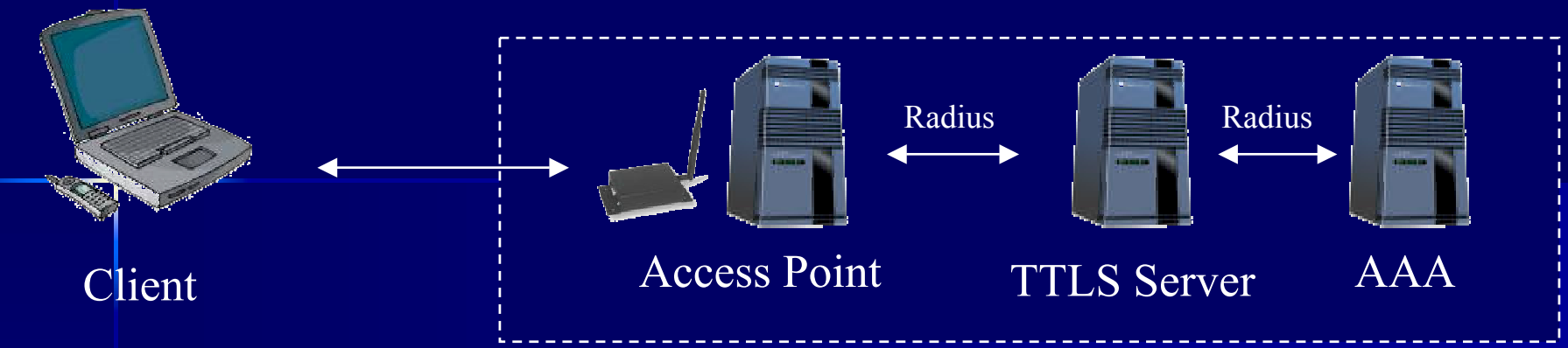
Scambio messaggi radius

06 - EAP-TTLS – Esempio



- Utilizzo del CHAP per autenticare il client
- Negoziazione degli algoritmi crittografici e chiavi

06 - EAP-TTLS – Esempio (1)



EAP-Request/Identity

EAP-Response/Identity

Radius Access Request: Data-Cipher-Suite+ EAP-Response/Identity

Radius Access Challenge: EAP-Request/TTLS-Start

EAP-Request/TTLS-Start

EAP-Response/TTLS: client_hello

RAR: EAP-Response/TTLS: client_hello

RAC: EAP-Request/TTLS (server_hello,certificate, server_key_exchange,server_hello_done)

06 - EAP-TTLS – Esempio (2)

AP-Request/TTLS (server_hello,certificate,server_key_exchange,srv_hello_don

AP-Response/TTLS (client_key_exchange,CCS,client_finish)

RAR: EAP-Response/TTLS (client_key_exchange,CCS,client_finish)

RAC: EAP-Request/TTLS (CCS, server_finish)

AP-Request/TTLS (CCS, server_finish)

AP-Response/TTLS (user_name, CHAP-Challenge&Password) Data-CipherSui

RAR: EAP-Response/TTLS (user_name, CHAP-Challenge, CHAP-Password) +Data-CipherSuite

RAR: User_name, CHAP-Challenge, Chap-Password

06 - EAP-TTLS – Esempio (3)

Radius Access-Accept [RAA]

RAC: EAP-Request/TTLS (Data-Cipher-Suite)

AP-Request/TTLS (Data-Cipher-Suite)

EAP-Response (No data)

RAR: EAP-Response (No data)

RAA: Data-Cipher-Suite, Data-Keying-Material, EAP-Success

EAP-Success

Mutua autenticazione ok!
Parametri di cifratura e chiave ok!

06 - PEAP

- Proposal in internet draft di Cisco, Microsoft, RSA Security (draft-josefsson-pppext-eap-tls-eap-02.txt)
- Autenticazione a 2 fasi
  - –Nella fase 1 viene autenticato il server creando u canale sicuro (come SSL con amazon.com)
  - –Nella fase 2 viene usato EAP sul canale sicuro. Supporterebbe vari metodi di autenticazione(GTC,MD5,etc) ma di fatto l'unico e' EAP-MSCHAP-V2
- Richiede certificato digitale solo lato server
- Supplicant solo per sistemi Microsoft
- Authentication server Microsoft IAS, Cisco ACS

06 - PEAP Authentication (il tunnel)

client

AP

RADIUS server

Client AAA Server

Certifica Authori

Start

AP blocks all requests until authentication completes

Request identity

identity

identity

Server Side Authentication

Server certificate

Server certificate

Encrypted Tunnel Established

Client Side Authentication

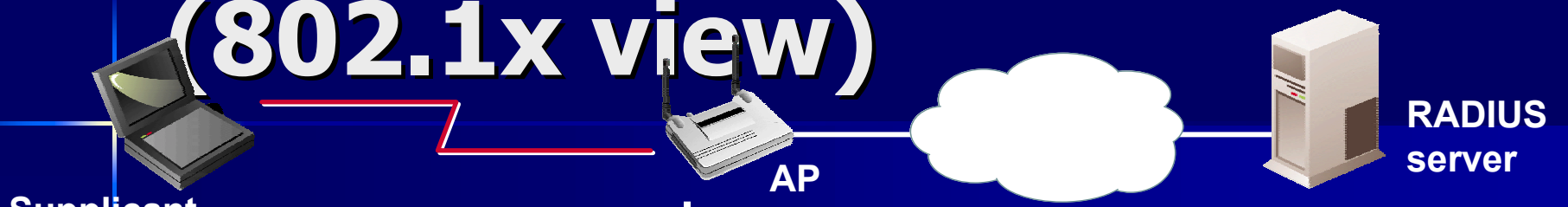
EAP in EAP Authentication

broadcast key

key length

AP invia client broadcast key, encrypted with session key

06 - PEAP Authentication (802.1x view)



EAPOL Start

Start EAP Authentication

EAP-Request/Identity

Ask client for identity

EAP -Response/Identity (NAI)

RADIUS Access request

Access Request with NAI

Server-side TLS

Client-side Authentication

Perform sequence defined by PEAP

key

RADIUS Access success (Pass session key to AP)

key

EAP success

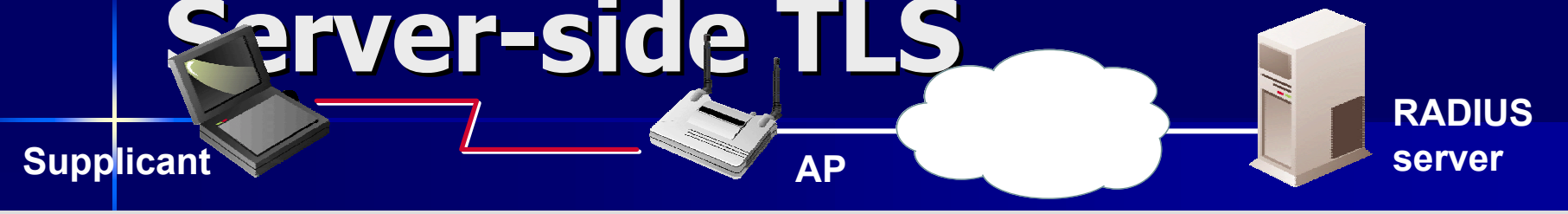
Client derives session key

EAPOL-Key (multicast)

EAPOL-Key (session parameters)

Deliver broadcast key encrypted with session key & session parameters

06 - PEAP - Fase 1: Server-side TLS



EAP-Request (TLS Start)

[EAP-Type=PEAP, Start bit set, no data]

[EAP-Type=PEAP (TLS client_hello)]

EAP-Response

[EAP-Type=PEAP (TLS server_hello, TLS certificate, TLS server_key_exchange, TLS certificate_request, TLS server_hello_done)]

[EAP-Type=PEAP (TLS client_key_exchange, TLS change_cipher_spec, TLS finished)]

EAP-Request

EAP-Response

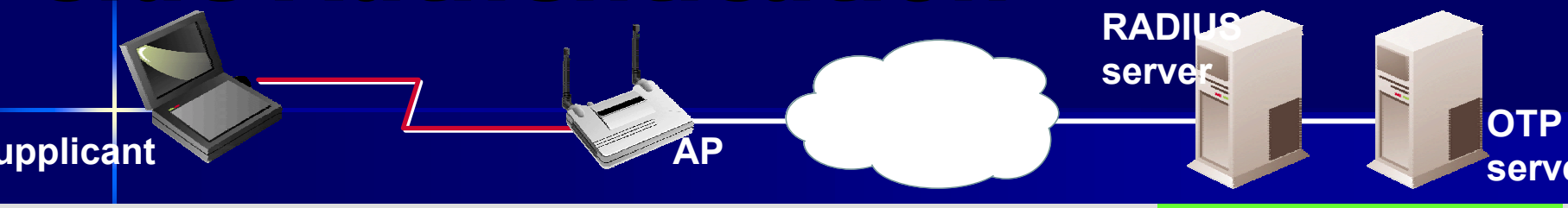
EAP-Request

[EAP-Type=PEAP (TLSchange_cipher_spec, TLS finished)]

[EAP-Type=PEAP]

EAP-Response

06 - PEAP - Fase 2: Client-side Authentication



[EAP-Type=PEAP
TLS Record {ContentType=
application data (
EAP-Request (EAP-Type=
Generic Token Card)) }]

EAP-Request

EAP-Response

[EAP-Type=PEAP
TLS Record {ContentType=
application data (
EAP-Request (EAP-Type=
Generic Token Card)) }]

EAP-Request

[EAP-Type=PEAP]

EAP-Response

[EAP-Type=PEAP
TLS Record {ContentType=
application data (
EAP-Success) }]

EAP-Success

06 - Riassumento i tunnelled protocols

- EAP-TLS e' complesso e costoso da gestire ma si integra perfettamente dove c'e' gia' una PKI
- PEAP e' implementato solo su sistemi microsoft
- PEAP e' solo all'inizio di una lunga fase di testing
- EAP-TTLS e' standard, supportato dalla maggioranza degli access point e implementato in quasi tutti i client ma poco diffuso. Si puo' usare radius opensource (freeradius)
- Sono resistenti ai seguenti attacchi:
  - Man in the middle attacks
  - intercettazione user ID & password
  - Session hijacking

06 - La scelta del metodo EAP

- Scegliere Cisco LEAP significa vincolarsi all'hardware Cisco (al massimo client Apple)
- Anche cisco sta' spingendo PEAP come alternativa
- La decisione va' presa sulla base della struttura di autenticazione esistente, se si dispone di una PKI conviene EAP-TLS
- Altrimenti le scelte sono fra PEAP e TTLS .
- Il futuro monopolio nel mercato degli hotspot del Microsoft WPS imporra' PEAP

06 - RADIUS & EAP

- Microsoft
  - OS Support: Windows 2000 Server, Windows .NET Server
  - EAP Methods: EAP-MD5, EAP-TLS
- Cisco Secure ACS v3.0 For Windows
  - OS Support: Windows NT Server 4.0, Windows 2000 Server
  - EAP Methods: Cisco LEAP, EAP-CHAP, EAP-TLS
- Funk Odyssey
  - OS Support: Windows 2000 Server, Solaris, Netware,
  - EAP Methods: EAP-TLS, EAP-TTLS, EAP-MD5, Cisco LEAP
- Interlink
  - OS Support: Solaris, HP-UX, Tru64 Unix, Red Hat Linux
  - EAP Methods: EAP-MD5, Cisco LEAP
- FreeRadius
  - OS Support: Linux, Solaris, HP-UX, AIX, OS/2, MINGW32
  - EAP Methods: EAP-MD5

06 - Wired/Wireless SUPPLICANT support

- Microsoft
  - OS Support: Windows XP
  - EAP Methods: EAP-MD5, EAP-TLS
- Meeting House Data Communications
  - OS Support: Win 98/ME, Win NT, Win 2000, Linux
  - EAP Methods: EAP-MD5, EAP-TLS
- Funk Odyssey Client
  - OS Support: Windows XP/NT/2000/98/ME
  - EAP Methods: EAP-MD5, EAP-TLS, EAP-TTLS, Cisco LEAP
- University of Maryland Open1X
  - OS Support: Linux, FreeBSD
  - EAP Methods: EAP-TLS
- Cisco 802.11 LEAP Supplicant
  - OS Support:Win XP/NT/2000/98/95/ME/CE, Linux, Mac OS 9.X
  - EAP Methods: Cisco LEAP

06 - Ethernet AUTHENTICATORS

- HP
  - Products: ProCurve 25xx, 410x, 530x
- Cisco
  - Products: Catalyst 2950*, 3550, 4000, 5000, 6000
- Enterasys
  - Products: Matrix E7/E6 Blades Firmware 5.02.03
- Nortel
  - Products: BayStack 450T, Business Policy Switch

06 - 802.11 AUTHENTICATORS

- Cisco
  - Aironet
- Enterasys
  - RoamAbout R2
- Agere System Orinoco
  - AP-2000 Access Point
- 3Com
  - WLAN Access Point 8000

06 - Proteggere il layer2 con il layer3

- Il 31% delle soluzioni WLAN “enterprise” si basa sull’utilizzo di VPN
- VPN IPSec rendono sicuro il layer3
- Aumentano la complessita’ e il costo dell’infrastruttura
- Se non ben pianificate sono molto piu’ pericolose del wifi
- Vengono spesso usate per soluzioni di WLAN VPN P-to-P e P-to-MP

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

07 - 802.11i

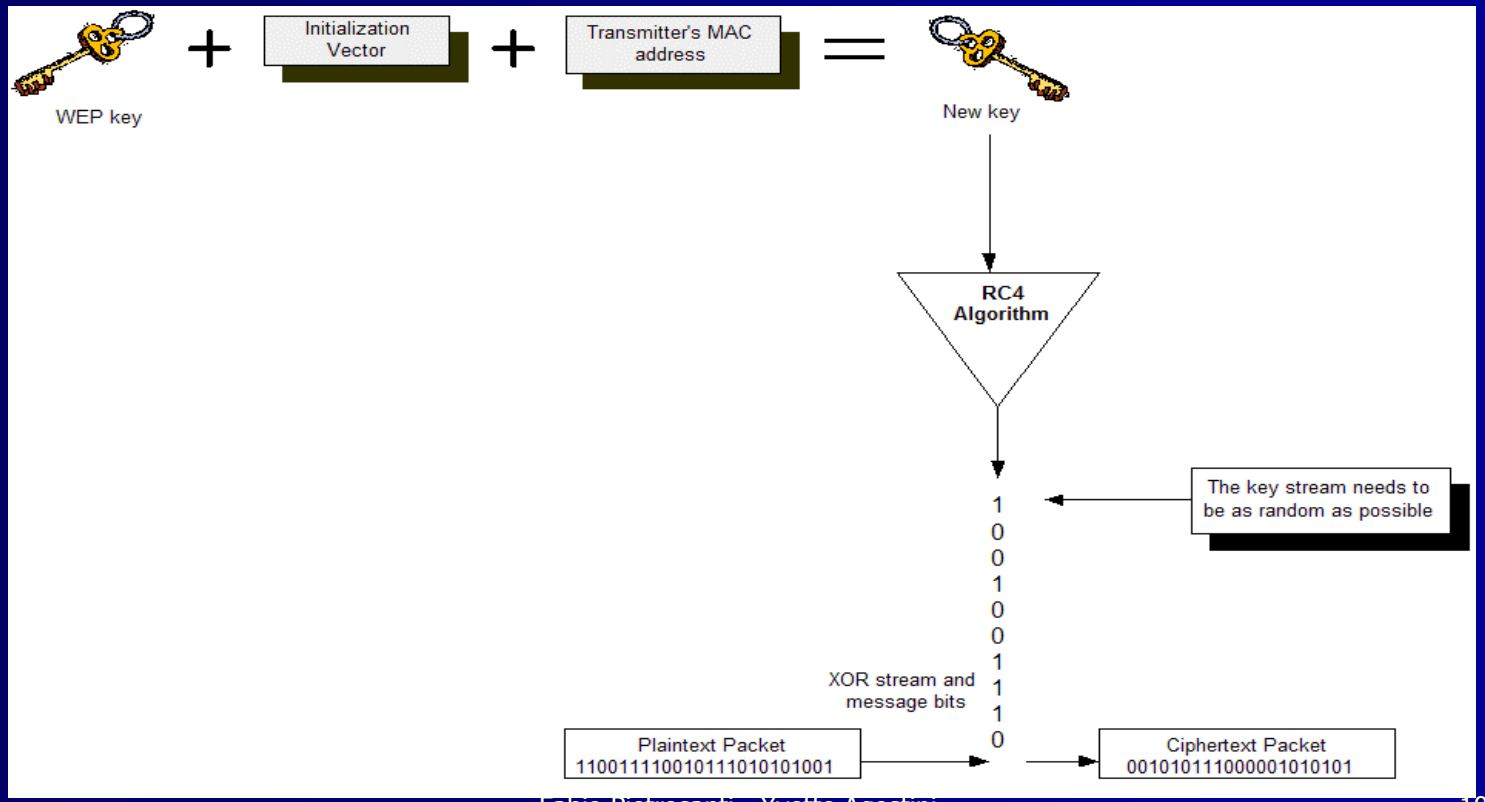
- 802.11i risolvera' finalmente i problemi di sicurezza dell'802.11
- Nella sua versione definitiva sara' necessario un cambio di hardware a causa della potenza di calcolo necessaria
- Utilizza 802.1x per l'autenticazione
- I suoi elementi sono:
  - –WPA (Wi-Fi Protected Access)
  - –TKIP (Temporal Key Integrity Protocol)
  - –Message Integrity Check (Michael)
  - –RSN (Robust Security Network)
- 802.11i non e' ancora definito completamente ma alcune sue feature sono "ready for the market" e gia' utilizzate

07 - 802.11i Security: WPA1

- IL WPA nella versione 1 si basa sul TKIP
- Una pre-implementazione del TKIP e' stata fatta da Cisco nella sua soluzione proprietaria LEAP
- TKIP elimina la necessita' di dovere cambiare hardware innalzando il livello di sicurezza
- E' una versione modificata del WEP
  - –Si basa ancora su RC4
  - –Include initialization vectors a 48-bit (anziche' 24)
  - –Ha funzionalita' di derivazione e distribuzione della chiave (rekyeing)
  - –Message Integrity Check sicuro (michael)

07 - 802.11i Security: WPA1

- Con TKIP la chiave cambia ogni 10000 pacchetti ed e' derivata da chiave temporanea+Mac address sorgente + IV di RC4



07 - 802.11i Security: WPA1

- Gli schemi di autenticazione del WPA possibili sono due:
  - EAP
  - PSK (Pre Shared Key)
- WPA-PSK richiede la configurazione di una master key sugli AP e sui client . Ci pensera' TKIP a cambiare la chiave di sessione e gestirne il rinnovo periodico.
- EAP, nelle sue declinazioni supporta gia' meccanismi per derivare la chiave
- WPA 1 non e' attualmente utilizzabile nelle reti ad-hoc
- Attualmente supportato da patch microsoft Q815485 e client commerciali (AEGIS)

07 - 802.11i WPA2

- La versione 2 del WPA sara' integrata con la versione completa di 802.11i
- WPA 2 si basa sul CCMP (Counter-Mode CBC-MAC Protocol) anche conosciuto come AES privacy algoritm
- Con 802.11i e WPA2 si utilizza l' RSN (Robust Security Network), che include meccanismi di negoziazione dinamica delle informazioni di autenticazione e cifratura tramite i "RSN Information Element"
- RSN prevede gia' l'introduzione di nuovi schemi di autenticazione se necessario bma per la cifratura i 256bit di AES possono resistere fino alla venuta della crittografia quantistica
- Il TKIP sara' opzionale ma garantira' ai device Pre-RSN di funzionare tramite aggiornamento software

07 - Riassunto WEP/TKIP/CCMP

	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits encryption, 64 bit auth	128 bits
Key Life	24-bit IV, wrap	48-bit IV	48-bit IV
Packet Key	Concat.	Mixing Fnc	Not Needed
Integrity			
Data	CRC-32	Michael	CCM
Header	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt.	None	EAP-based	EAP-based

07 - Conclusione sugli standard

- Fino all'introduzione dell'802.11i (Robust Security Network) le reti wireless NON possono considerarsi sicure!!

  e anche dopo non saranno immuni a denial of service

  100% anonimi quindi NON affidabili come una wired.

07 - Una vita di upgrade

- Introduzione di WEP128bit: Cambio Firmware
- Introduzione randomicita' IV: Cambio firmware
- Introduzione TKIP+MIC=WPA1: Cambio firmware
- Introduzione CCMP+RSN=WPA2: Cambio hardware

Agenda

- 01 introduzione alle tecnologie wireless
- 02 Wi-Fi funzionamento e stack del protocollo
- 03 Wi-Fi Il WEP
- 04 Protocolli di autenticazione
- 05 801.1X port security
- 06 I metodi EAP
- 07 802.11i lo standard venturo
- 08 Auditing network 802.11

08 - Auditing di infrastrutture wireless

- Fare auditing significa controllare cosa accade alla nostra rete
- Per controllare la rete significa conoscere gli attacchi per poterli riconoscere
- Gli attacchi possono essere mirati a:
  - Acquisire informazioni sugli utenti (rubare le credenziali di accesso)
  - Accedere alla rete wireless per fini illeciti
  - Causare interruzzioni di servizio per sabotaggi (Denial of service)

08 – Auditing way

- Detecting rouge access point
  - Analisi periodica con strumenti come kismet/netstumbler
  - Utilizzo di network intrusion detection wireless
- Detecting illegal user e intrusion attempt
  - Strumenti di analisi dei log
  - Honeypot wireless
  - FakeAP
- Distruggi la tua rete per sondarne l'affidabilita': Denial Of Service
  - Jamming del segnale
  - Airjack
  - RTS Flood

08 – Auditing equipment

- Computer portatili e palmari intelligenti (con linux!!!)
- Schede wireless potenti (200mw)
- Schede wireless con chipset prism2 (attenzione!!)
- Schede wireless con antenna diversity
- Antenne direttive e antenne omnidirezionali

08 - Fragilita' delle reti wireless

- **Un concetto importantissimo di cui bisogna rendersi conto e' che le reti wireless, per quanto si possano rendere "sicure" sono e rimarranno**

FRAGILI

- **Fragili perche' il media e' condiviso e chiunque puo' accedervi in modo completamente anonimo.**

08 - Discovery access point: Kismet, Netstumbler, etc

- Usati nel “wardriving”
- Usabili in azienda per rilevare access point e client non autorizzati (LTBACarabinieri)
- Richiede schede che supportino il “monitor mode” e il “channel hopping”
- Alcuni implementano funzionalita’ di cracking WEP
- Si dividono in:
  - Attivi (netstumber, ministumbler)
  - Passivi (Wellenreiter, kismet, airsnort, IBM WSA)

08 - Discovery access point: Network Intrusion Detection

- Veri strumenti di monitoraggio reti wireless
- Non rilevano attacchi a livelli superiori (vedi snort, ISS RealSecure, etc) come un normale
- Le soluzioni enterprise sono molto costose
- Richiedono l'integraziane con l'analisi dei log degli access point

08 - Wireless honeypot

- Una honeypot cerca di attrarre attaccanti per capirne il comportamento
- Utilizzare un'access point dedicato su una rete scollegata dalla rete aziendale
- Utilizzare sniffer su questa rete
- Ogni collegamento su questa rete e' sospetto
- Utilizzare un nome che richiama palesemente alla vostra infrastruttura
- La fantasia vi aiutera'

08 - Airsnarf, rubare password dei wireless hotspot

- HostAP+Dns hijacking+Web Server = sniff the hotspot
- http://airsnarf.shmoo.com/

08 - Fake AP, proteggere le infrastrutture con il rumore

- Generare milioni di pacchetti con SSID randomici, chiavi wep randomiche, mac address randomiche
- Impedisce all'attacker di identificare la rete reale confondendo il suo tool di scanning
- Fa' bloccare anche il discovery di reti da parte di client (richiede impostazione manuale di ssid)
- http://www.blackalchemy.to/Projects/fakeap/fake-ap.html

08 - Wep cracking accelleration

- Tramite il replaying di alcuni pacchetti broadcast (arp) o unicast(tcp acks) e' possibile accellerare il cracking del WEP
- Utilizzare reinj.c di bsdairtools per "forgiare" pacchetti visti "on the air" che rappresentano arp-request per sniffare le arp-reply e il relativo IV

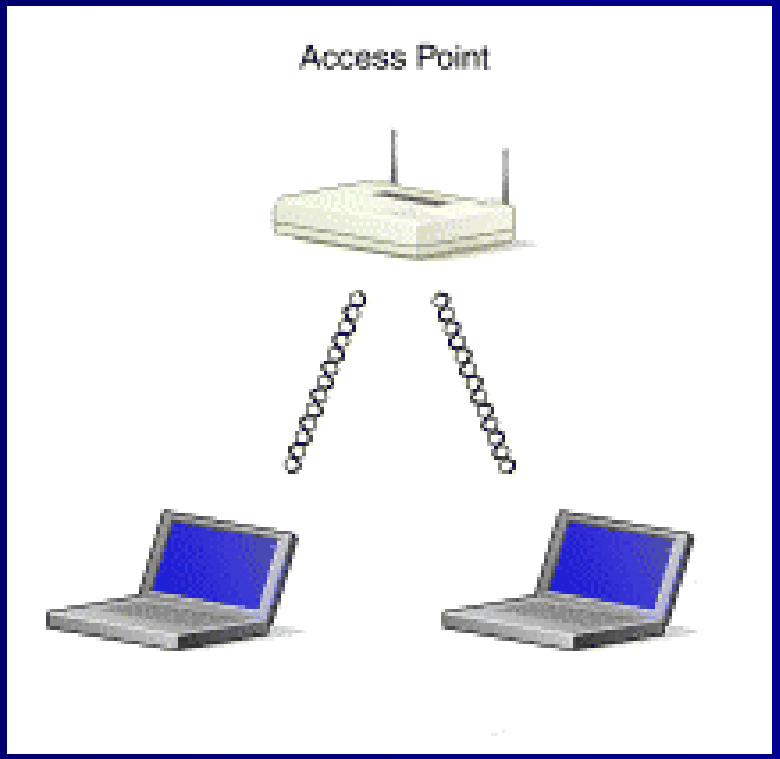
08 - Man in the middle attacks

- MITM Attack
  - Inserire un access point fra l'access point reale e il client
  - L'attacco richiede la vicinanza all'obbiettivo dell'attacco
  - Due schede wireless
- AirJack by Abaddon
  - Monkey_Jack
  - Kracker_Jack (ipsec)
  - Include tool di denial of service

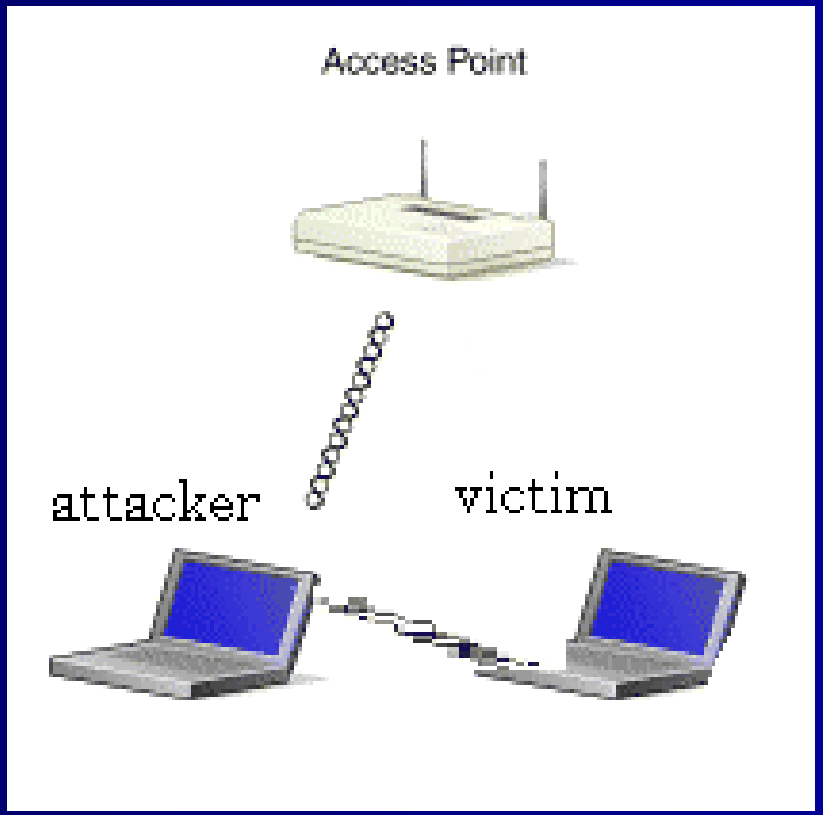
08 - Monkey-Jack

- L'attaccante lancia un DOS sulla rete wifi inviando Deassociation e Deauthentication request per tutti i client
- La vittima cerca un nuovo AP
- La vittima si associa al nostro AP fake
- L'attaccante si associa all'AP reale
- Adesso la macchina dell'attaccante fa' da proxy fra l'AP reale e quello "fake" in modo trasparente

08 - Prima di Monkey-Jack



08 - Dopo Monkey-Jack



08 - Monkey_Jack sample

```
#./monkey_jack
Monkey Jack: Wireless 802.11(b) MITM proof of concept.

Usage: ./monkey_jack -b <bssid> -v <victim mac> -C <channel number> [ -c <channel number> ]
        [ -i <interface name> ] [ -I <interface name> ] [ -e <essid> ]

       -a:  number of disassociation frames to send (defaults to 7)
       -t:  number of deauthentication frames to send (defaults to 0)
       -b:  bssid, the mac address of the access point (e.g. 00:de:ad:be:ef:00)
       -v:  victim mac address.
       -c:  channel number (1-14) that the access point is on, defaults to current.
       -C:  channel number (1-14) that we're going to move them to.
       -i:  the name of the AirJack interface to use (defaults to aj0).
       -I:  the name of the interface to use (defaults to eth1).
       -e:  the essid of the AP.

#./monkey_jack -b 00:40:96:5b:37:af -v 00:07:85:92:db:a9 -c 1 -C 8 -i aj0 -I eth1 -e "l3p3r0u
Starting Monkey in the Middle Attack:

victim: 00:07:85:92:db:a9
bssid:  00:40:96:5b:37:af

configuring airjack device...done.
forcing ourselves in the middle...done.
configuring lucent card...done.
coercing our card to associate as the victim...done.

layer 1 insertion complete.
```

08 - Come funziona Monkey_Jack

- Non c'e' per-packet autentication
  - Il client o l'AP puo' essere spoofato
- Il cliente cerca nuovi AP appena essere stato disassociato
- L'attaccante impersonifica l'AP e gli richiede di autenticarsi

08 - Denial of service

- Basta usare la fantasia
- Fino a 802.11i & WPA2 flood di pacchetti di management
- Dopo 802.11i inizieremo a giocare con i pacchetti di controllo
- Un esempio pratico? RTS flood!

Conclusioni

Attaccatevi!!

Q&Ab

Missione compiuta?

Fabio Pietrosanti – fabio@pietrosanti.it
Yvette Agostini – yvette@yvetteagostini.it