SICUREZZA DELLE RETI WIRELESS

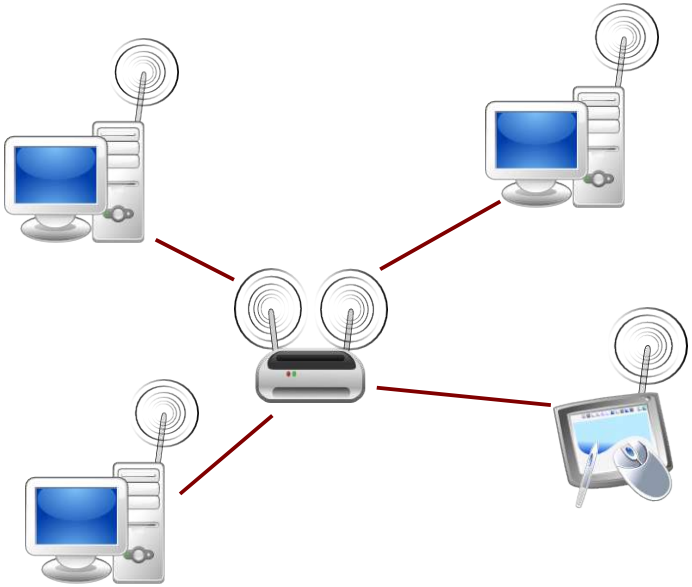
Wireless Security

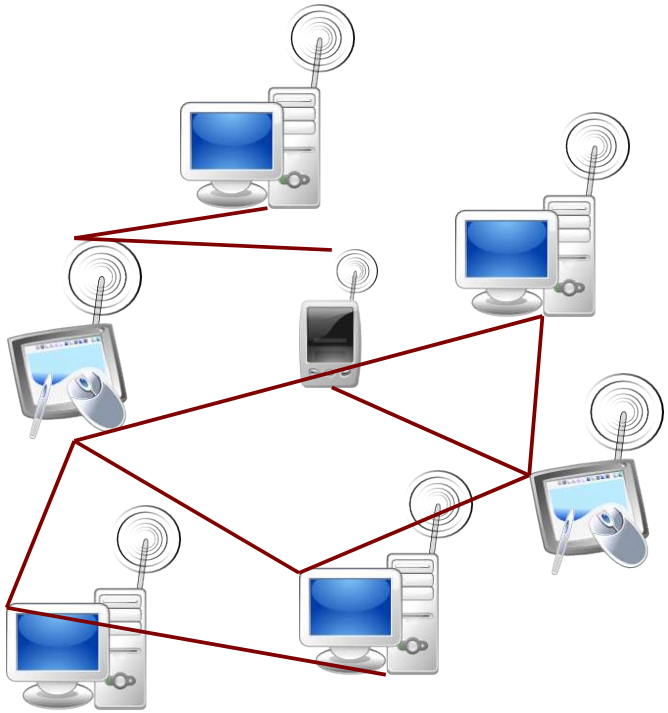
LEONARDO MACCARI: LEONARDO.MACCARI@UNIFI.IT
LART - LABORATORIO DI RETI E TELECOMUNICAZIONI
DIPARTIMENTO DI ELETTRONICA E TELECOMUNICAZIONI

TOC

Concetti di base:

- topologia:
  - Modello infrastructure (centralizzato)
  - Modello ad-hoc (distribuito)





Concetti di base:

- mancanza di limite geografico:
  - Le informazioni possono essere *sniffate* più facilmente
  - Si possono subire attacchi dall'esterno: quindi il rischio per l'attaccante è minimo
- Ridefinizione del ruolo del livello MAC:
  - Accesso inteso anche come controllo degli accessi
  - Complicazione dei Firmware e dei driver
- Risorse computazionali limitate

Hotspot

- Punti di accesso ad internet attraverso tecnologia wireless, normalmente 802.11 in modalità infrastructure.
  - Abbattimento dei costi di gestione, non c'e' cablaggio.
  - Installazione immediata.
  - Vengono utilizzati comunemente in aeroporti, stazioni, alberghi.
  - Presentano problemi di gestione: limitazione del raggio e degli accessi.

Reti ad-hoc/mesh

- Reti *spontanee*, autorganizzanti:
  - Ritrovi temporanei, riunioni.
  - Interventi in situazioni di emergenza.
  - Reti tattiche militari.
  - Ambienti con mancanza di infrastruttura (montagna, fiera).
  - Vengono utilizzate per sopperire al problema dell'ultimo miglio e per coprire aree molto estese.

Leonardo Maccari,
leonardo.maccari@unifi.

PAN - personal area network

- Reti di dimensioni ridotte utilizzate per interconnettere apparati (stampanti, computer, cellulari).
- Normalmente in modalità ad-hoc senza routing.
- La tecnologia più evoluta è lo standard Bluetooth, adesso confluito in ieee 802.15.

Legislazione

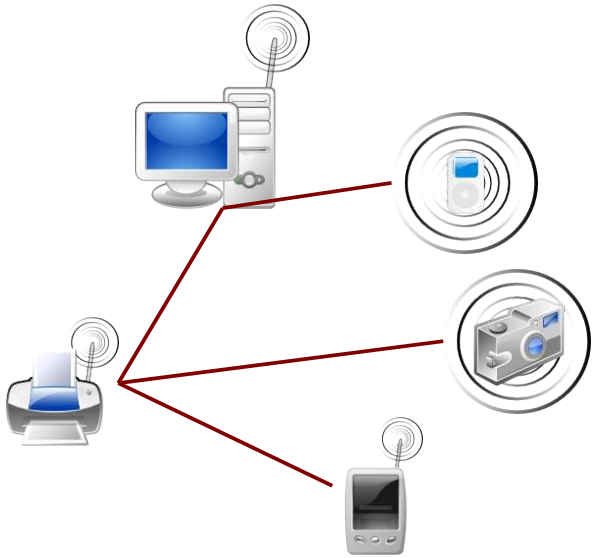
- Le reti 802.11 b/g lavorano in frequenze non regolate (2.4 GHz, banda ISM, Industrial, Scientific, Medical), quindi non sono soggette a licenza.
- Per quelle frequenze, in Italia il limite di densità di potenza trasmissibile è di 100 mW per metro quadro, che permette comunicazioni in spazio libero fino a circa 300 metri con tecnologia 802.11.
- La legge Gasparri, il decreto Landolfi e il decreto Pisanu hanno regolamentato l'utilizzo delle frequenze ISMe le modalità di autenticazione, rendendone molto complicato l'utlizzo su suolo pubblico. Questo ha frenato decisamente la diffusione di tali tecnologie sul suolo pubblico rispetto ad altri paesi.
- WiMax invece utilizza frequenze non in banda ISM, recentemente sono state bandite ed assegnate con un'asta le frequenze per l'utilizzo di WiMax e cominciano ad arrivare le prime offerte.

802.16

- WiMaxè una tecnologia nata per sostituire le connessioni cablate dalla centrale del gestore alle singole abitazioni, anche connettendo tra loro più hotspot 802.11.
- Gli standard di riferimento sono l'IEEE 802.16d del 2004, e l'IEEE 802.16e del 2005.
- Può utilizzare uno spettro di frequenze molto largo (2-66 GHz), permette collegamenti teoricamente fino a 74 Mbps e può essere utilizzato anche su distanze molto grandi (chilometri)
- Una delle sue caratterstiche più importanti è quella di offre il controllo della qualità del servizio a livello MAC.
- Offre anche una modalità ad-hoc (mesh).

Bluetooth

- Reti di piccole dimensioni, utilizzate per connettere tra di loro apparati dati (cellulari, stampanti. . .)



Bluetooth

- Frequenze: 2.4 GHz.
- Bitrate max: 720Kbps.
- Funziona normalmente in modalità ad-hoc.
- Distanze: tre categorie di potenza, dai 10 ai 100 metri.

Altre tecnologie:

- Hyperlan2: standard ETSI per reti locali wireless, con caratteristiche molto simili a 802.11
- Reti cellulari: GSM, GPRS, UMTS ...

Leonardo Maccari,
leonardo.maccari@unifi.

802.11 - Storia

1996	Prima versione dello standard 802.11, definizione dello strato MAC e delle caratteristiche di sicurezza, max bitrate 2 Mbps.
1999	802.11b, bitrate 11 Mbps.
1999	802.11a, versione per frequenze di 5GHz, bitrate 54 Mbps.
2004	802.11g, versione per frequenze di 2.4GHz, bitrate 54 Mbps.
2004	802.11i ristrutturazione dello strato di sicurezza.
200X	802.11n versione MIMO che supporta bitrate superiori a 54 Mbps.

Strato fisico

- Frequenze: 2.4 - 5 GHz.
- Bitrate: 11 - 108 (?) Mbps.
- Range: fino a 50m indoor, 300m outdoor senza linea di vista.
- Permette la mobilità.

Leonardo Maccari,
leonardo.maccari@unifi.

WiFi Alliance

Prima che gli standard 802.11 vengano rilasciati ufficialmente i maggiori produttori che formano il consorzio WiFi, rilasciano una pre-release e certificazioni sui prodotti hardware.

- In particolare, il consorzio, per rimediare all'emergenza causata dalle insicurezze riscontrate in tutte le versioni precedenti alla *i* anticipa nei propri prodotti una versione incompleta di 802.11i che chiama WPA - Wireless Protected Access. A questa segue WPA2, che corrisponde alla versione aderente a 802.11i.
- Attualmente esistono molti working group (*j,h,f*. . .) con lo scopo di arricchire il protocollo con nuove caratteristiche quali QoS, fast handoff ecc. . .

Nei prossimi paragrafi si introdurrà il funzionamento di 802.11 nelle versioni precedneti alla *i*.

Tipi di traffico:

- Pacchetti di tipo *Management*: sono tutti i pacchetti che non trasportano dati ma che vengono utilizzati dalle macchine per gestire il traffico dati.
  - Pacchetti di autenticazione e di deautenticazione.
  - Pacchetti di associazione e di deassociazione.
  - Pacchetti di Beacon . . . .

I pacchetti di management non prevedono nessuna forma di autenticazione o di cifratura.

Tipi di traffico:

- Pacchetti di tipo *Control*: sono tutti i pacchetti che non trasportano dati ma che vengono utilizzati dalle macchine per gestire l'accesso al canale, che avviene normalmente con politiche CSMA/CA.
  - Pacchetti di RTS/CTS.
  - Pacchetti di ACK . . .

I pacchetti di controllo non prevedono nessuna forma di autenticazione o di cifratura.

Tipi di traffico:

- Pacchetti di tipo *Data*: sono tutti i pacchetti che trasportano il contenuto informativo.

I pacchetti di dati possono essere cifrati ed autenticati.

WEP - Wired Equivalent Privacy

Il WEP è l'insieme delle procedure introdotte in 802.11 per garantire privacy e sicurezza delle comunicazione, oltre che controllo degli accessi. Lo scopo dichiarato è quello di fornire un livello di sicurezza equivalente a quello di una rete wired tradizionale.
Le macchine appartenenti alla rete hanno tutte una chiave in comune, detta chiave WEP.

Leonardo Maccari,
leonardo.maccari@unifi.

WEP

Il WEP prevede:

- Una chiave condivisa tra tutte le macchine della rete, per cifrare il traffico unicast e broadcast.
- Una fase di autenticazione in cui una nuova macchina dimostra di possedere la chiave.
- Un algoritmo di cifratura dei pacchetti di tipo *stream*, l'RC4.

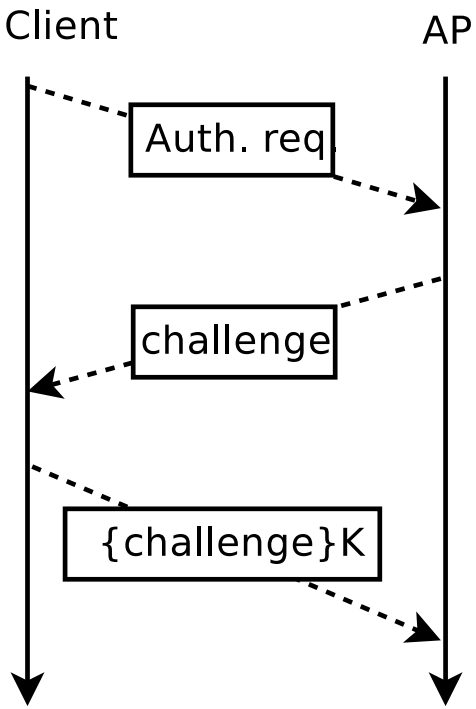
Chiave WEP:

- Una unica chiave condivisa tra tutte le macchine della rete.
  - Non esiste autenticazione dei pacchetti relativa alla singola macchina.
  - Non esistono comunicazioni segrete tra due singole macchine.
- Non esiste meccanismo automatico di *refresh* della chiave.

WEP: autenticazione Shared Key

Autenticazione

Autenticazione di tipo *shared key*, il client si deve autenticare verso l'AP dimostrando di possedere la chiave segreta.



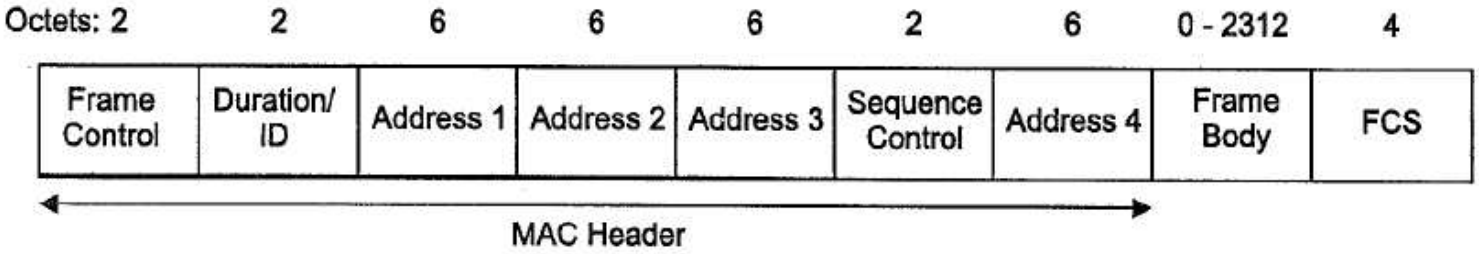
1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

WEP: autenticazione Shared Key

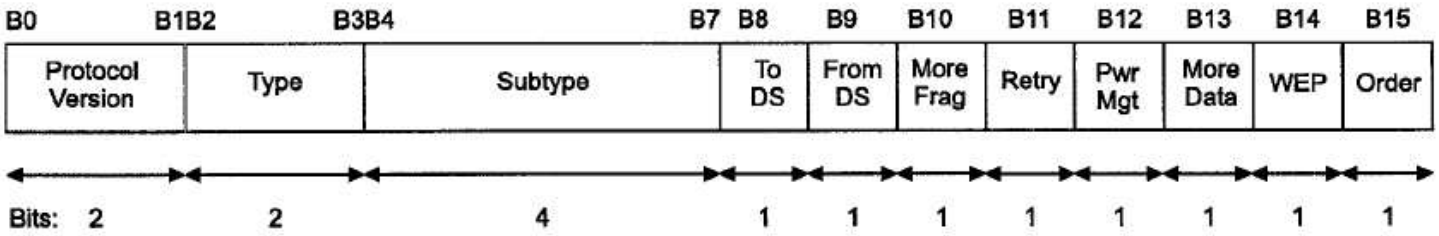
- I pacchetti sono pacchetti di management, quindi non sono autenticati nè cifrati.
- La procedura è molto veloce e quindi pensata per poter essere utilizzata come procedura di handoff rapido anche tra più AP.
- L'AP è l'unico elemento che decide chi far entrare nella rete. La gestione degli accessi è tutta sull'AP stesso.
  - Per reti costituite da più AP la gestione diventa molto complessa o del tutto statica.

Generic Frame Format:

Formato del generico frame 802.11



Formato del campo framecontrol

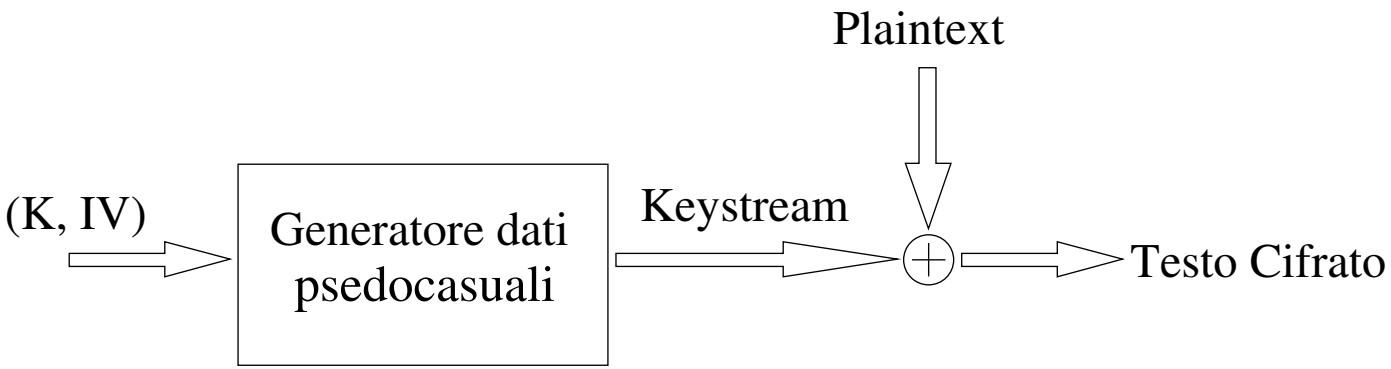


Viene cifrato solo il campo di payload del pacchetto, con un algoritmo di cifratura di tipo *stream*.

WEP: *Stream cipher*

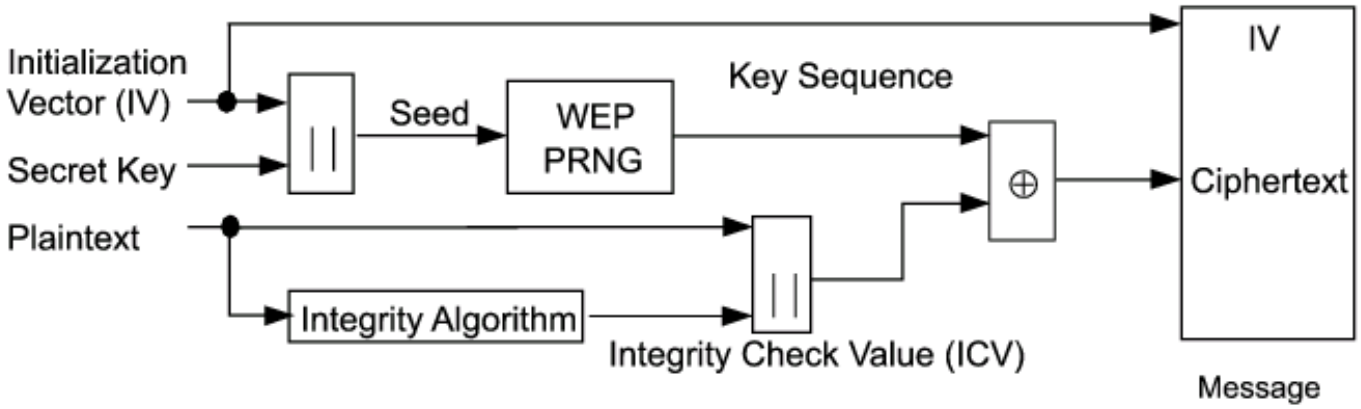
Gli algoritmi *stream* cifrano il contenuto in chiaro bit per bit, e non a blocchi di dimensione fissa.

- A partire da un segreto si genera un vettore di lunghezza variabile di dati pseudocasuali (*keystream*).
- Per rendere unico ogni pacchetto si aggiunge al segreto un vettore di inizializzazione, il *keystream* dipende dalla coppia (segreto, IV).
- Si fa lo XOR logico tra il keystream e l'informazione che si vuole cifrare
- Gli algoritmi di tipo stream sono molto veloci e facili da implementare
- Riutilizzare più volte lo stesso IV significa ripetere due volte lo stesso *keystream*. Se si conosce uno dei due pacchetti in chiaro si ricava anche il secondo...
- quindi lo stesso keystream non deve mai essere riutilizzato



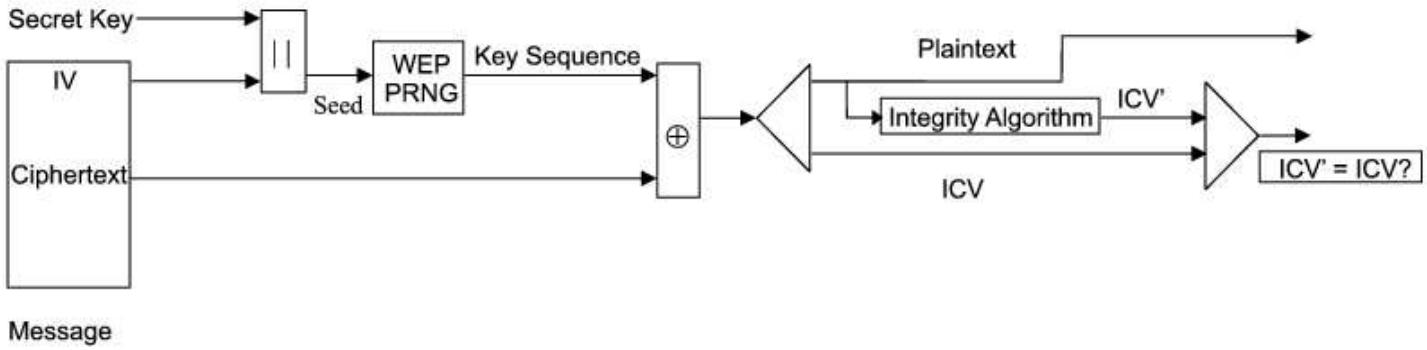
Leonardo Maccari,
leonardo.maccari@unifi.

Procedura di *encryption* con RC4:



- Si concatena la chiave WEP con il IV per generare il *seed*.
- Il blocco WEP PRNG (Pseudo Random Number Generator, basato su RC4) genera un *keystream* a partire dal *seed*.
- Sul *plaintext* (testo in chiaro) si applica un algoritmo di *error detection* (CRC-32), il CRC viene concatenato al pacchetto in chiaro.
- Si fa lo XOR con la chiave.
- Si trasmette il pacchetto con l'IV nell'header (non cifrato) e il payload cifrato.

Procedura di *decryption* con RC4:

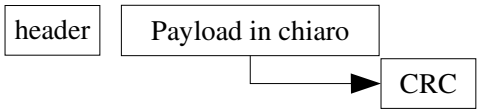


- Dal pacchetto si estrae IV e il payload cifrato.
- Da IV e la chiave WEP si ricrea il *keystream*.
- Si fa lo XOR tra il keystream e il payload ottenendo il payload in chiaro.
- Si separa il payload dal CRC e si ricalcola il CRC per verificare l'integrità.
- Cifrare anche il CRC significa che un attaccante che non conosce la chiave di cifratura può modificare il pacchetto ma non può rendere coerente il CRC.
- si ottiene in questo modo la sicurezza dell'integrità delle informazioni.

Leonardo Maccari,
leonardo.maccari@unifi.

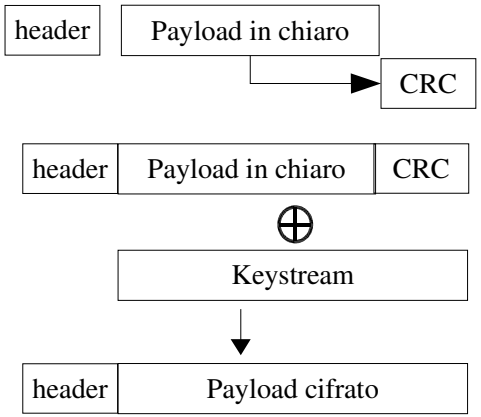
Autenticazione dei frame:

Sul payload in chiaro si calcola il CRC



Autenticazione dei frame:

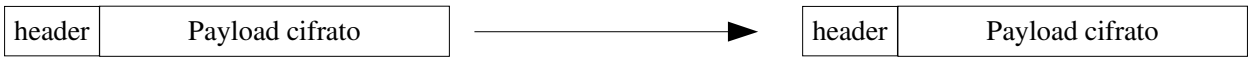
Si concatena il CRC e si fa lo XOR tra il *keystream* e il payload ottenendo il payload in cifrato.



Leonardo Maccari,
leonardo.maccari@unifi.

Autenticazione dei frame:

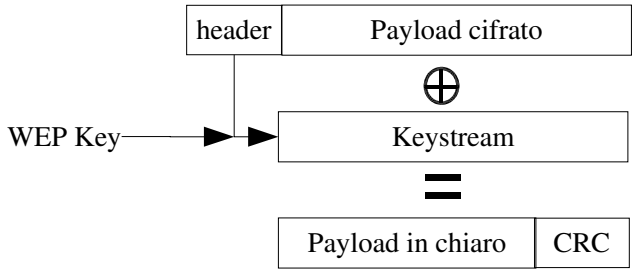
Il pacchetto viene trasmesso



Leonardo Maccari,
leonardo.maccari@unifi.

Autenticazione dei frame:

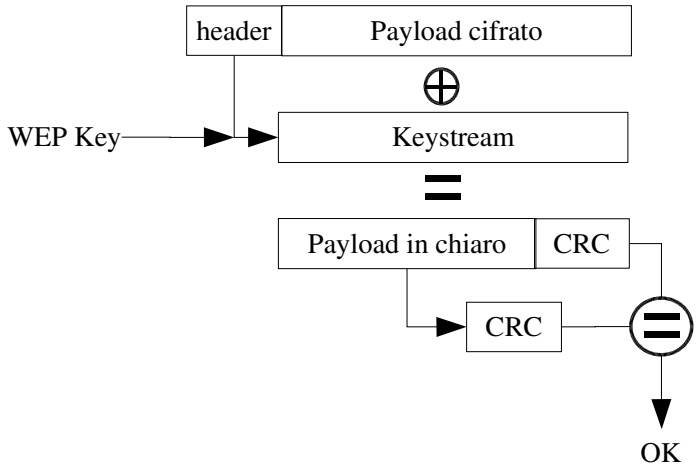
Si riceve il pacchetto, si estrae IV dall'header e si utilizza per ricalcolare il *keystream*, si esegue lo XOR con il pacchetto e si ricava in chiaro payload e CRC



Leonardo Maccari,
leonardo.maccari@unifi.

Autenticazione dei frame:

Si ricalcola in CRC dal payload in chiaro, quindi si confronta con quello ricevuto. Se i due valori coincidono la trasmissione è avvenuta senza manomissioni In questo modo si è ottenuto un controllo di integrità sul payload.



Note:

- L'autenticazione dei pacchetti non utilizza algoritmi a chiave pubblica/privata. Ci deve essere sempre un segreto condiviso in precedenza, quindi un canale sicuro.
- RC4 utilizza in 802.11b chiavi di 40 bit.
- Alcuni AP implementano un filtro sugli indirizzi MAC da far accedere alla rete per evitare accessi indesiderati.

Note:

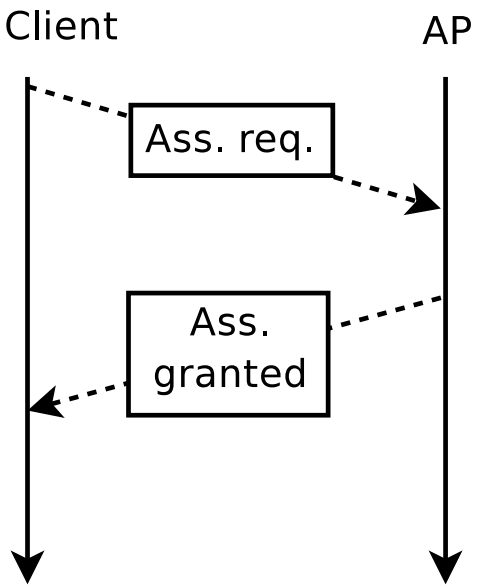
- Non esiste controllo di unicità dei pacchetti, due pacchetti possono essere identici.
- Non esiste controllo di sequenza dei pacchetti, il valore di IV viene deciso dagli apparati senza una politica definita (es: randomica, incrementale. . .)

Un attaccante può ripetere un pacchetto anche senza conoscerne il significato, saranno i protocolli di livello superiore a gestire i dati, accettandoli o rifiutandoli

802.11, dopo l'autenticazione:

Associazione

Una volta autenticato il client deve notificare all'AP che vuole entrare nella rete.



1. il client chiede di associarsi
2. AP invia una conferma

Leonardo Maccari, leonardo.maccari@unifi.

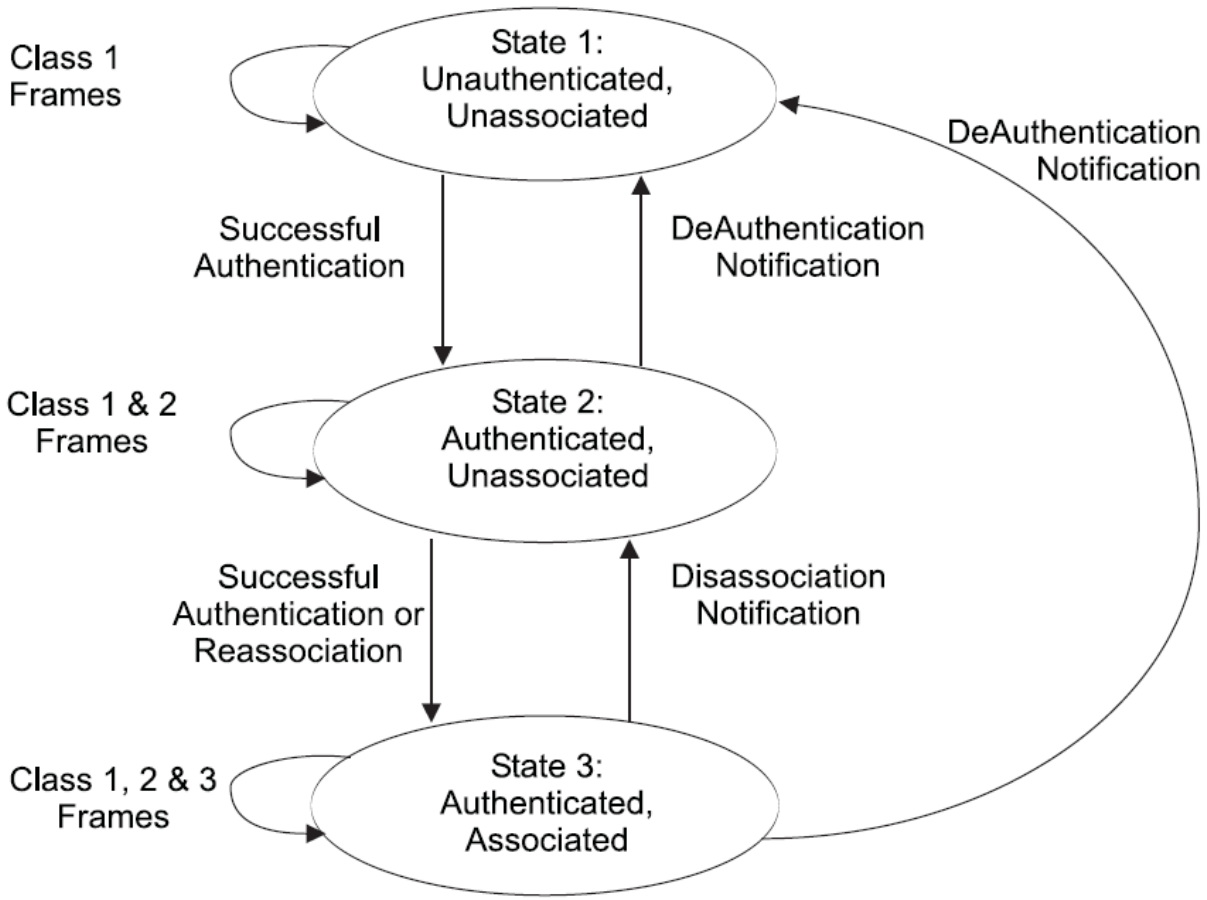
Uscita dalla rete:

Deautenticazione e deassociazione

- per deautenticare il client il AP invia un messaggio di deautenticazione e il client deve ripetere l'autenticazione
- per deassociare un client l'AP invia un messaggio di deassociazione e il client deve ripetere l'associazione
- se riceve un messaggio di deautenticazione quando è anche associato il client deve ripetere entrambe le fasi

Tutti questi pacchetti sono pacchetti di tipo management.

802.11 State machine

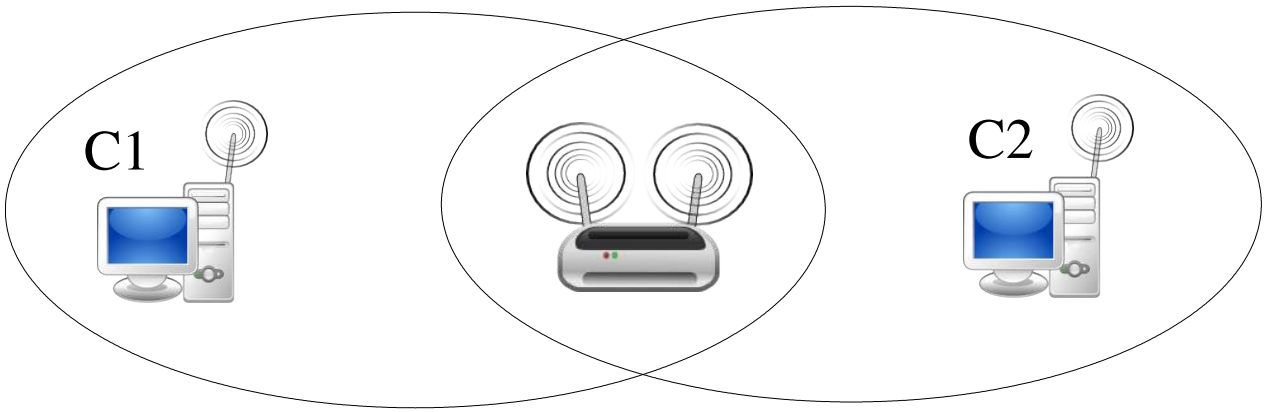


Leonardo Maccari,
leonardo.maccari@unifi.

802.11: accesso al canale

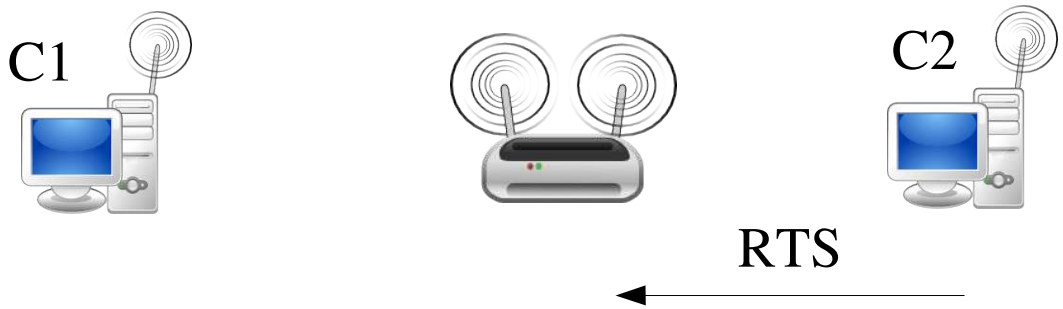
- i client della LAN condividono lo stesso canale fisico con una politica CSMA/CA
- in modalità infrastructure l'AP si comporta da centro stella, tutto il traffico viene inviato all'AP che lo ridirige ai client
- nell'intestazione di ogni pacchetto ACK/RTS c'è un campo *Duration* in cui il client specifica un periodo di tempo in cui il canale è prenotato
- in quel periodo di tempo il canale non viene utilizzato da altri client

Problema dell'hidden node



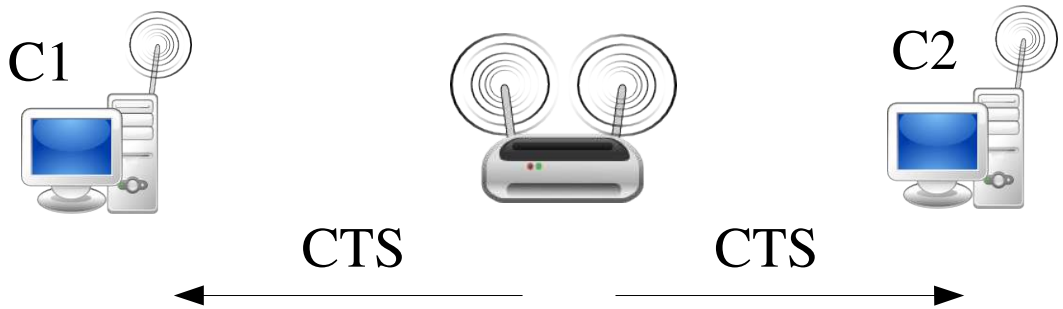
Leonardo Maccari,
leonardo.maccari@unifi.

RTS

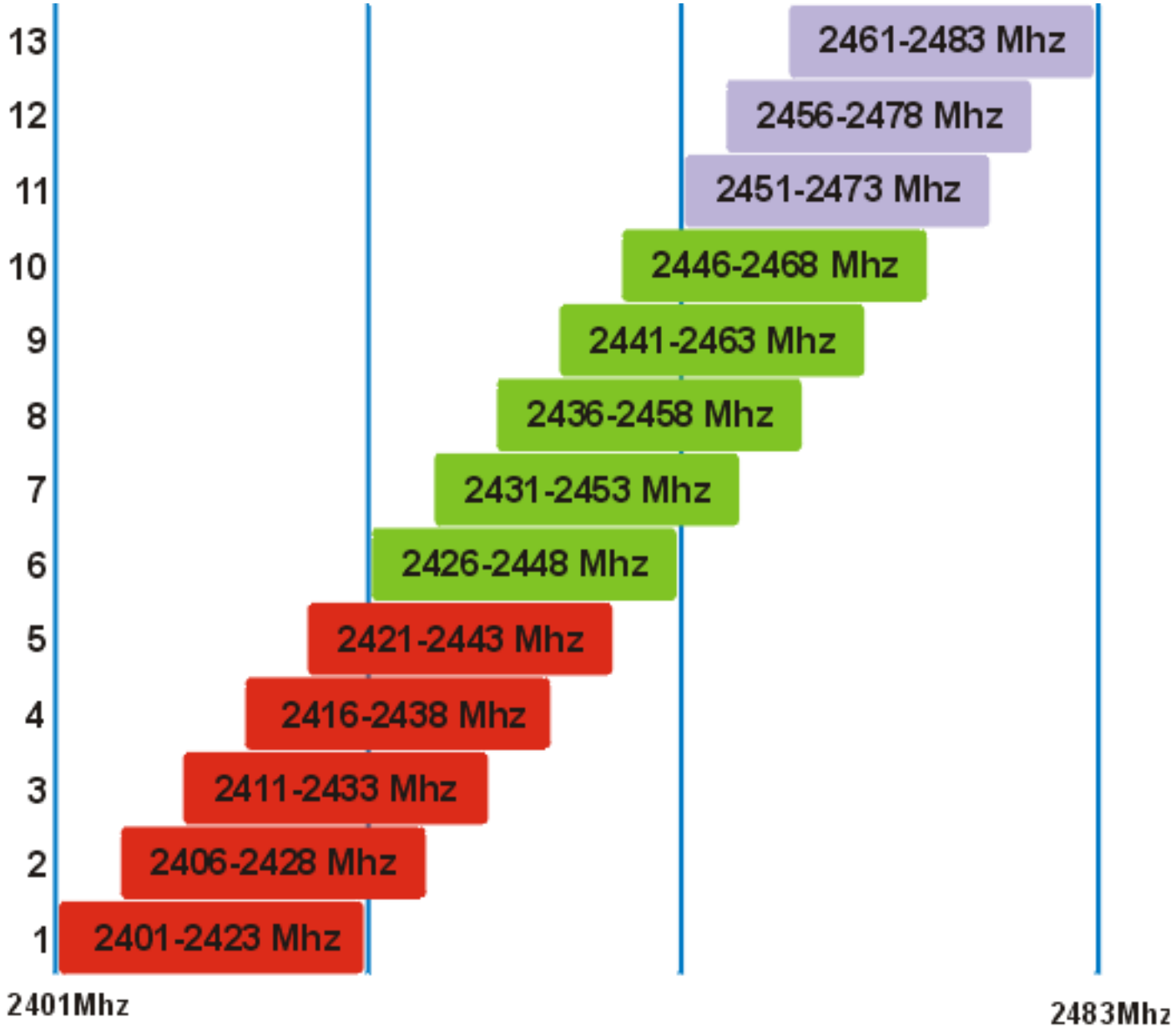


Leonardo Maccari,
leonardo.maccari@unifi.

CTS

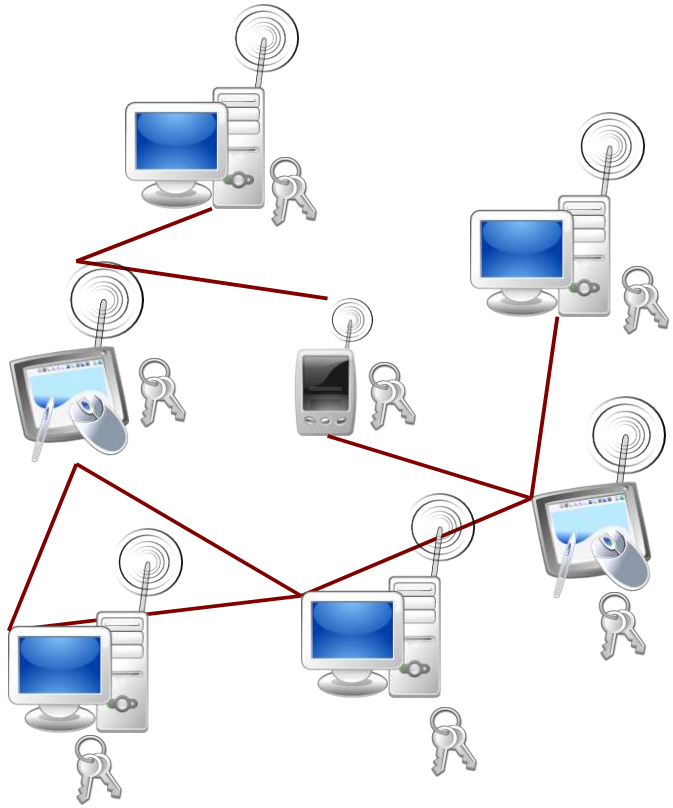


Canali 802.11



Leonardo Maccari,
leonardo.maccari@unifi.

WEP su ad-hoc



Leonardo Maccari,
leonardo.maccari@unifi.

Beacon Frame

Il beacon è un pacchetto che viene inviato dagli AP per segnalare la propria presenza. I contenuti più importanti del Beacon Frame sono i seguenti:

- Modalità: ad-hoc/infrastructure
- SSID: nome dell'access point. E' necessario specificarlo per entrare nella rete durante la fase dell'associazione.
- Privacy: definisce se l'AP supporta WEP o meno.

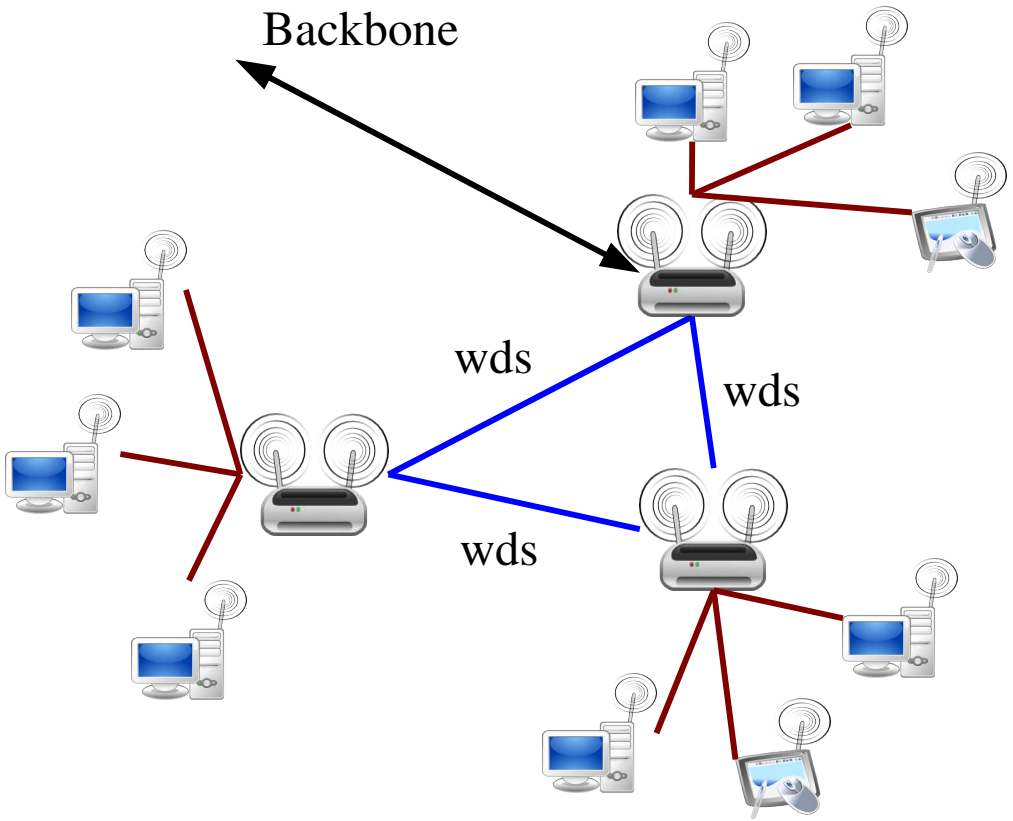
Leonardo Maccari,
leonardo.maccari@unifi.

Wireless Distribution System

Il WDS è un sistema di scambio di dati tra AP. Quando gli AP vogliono fare routing dei pacchetti tra di loro, per unire due reti distinte fisicamente in una unica rete logica devono utilizzare le interfacce WDS.

- Sulle interfacce WDS si può utilizzare WEP, ma non esiste associazione o autenticazione.
- L'utilizzo di interfacce WDS sottrae banda per il servizio della rete infrastructure.

WDS



Leonardo Maccari,
leonardo.maccari@unifi.

Protocollo:

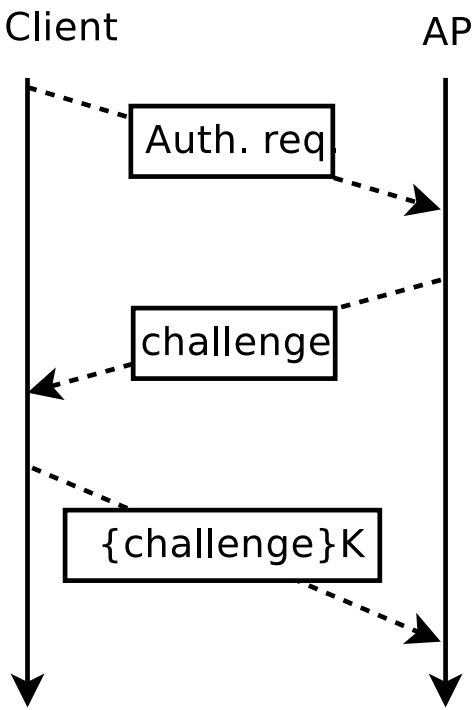
- Le insicurezze che vedremo sono relative al protocollo 802.11 nelle versioni a/b/g.
- Alcune di queste non riguardano gli algoritmi crittografici utilizzati, quindi vengono ritrovati anche nella versione *i*.

Interruzione del servizio:

Gli attacchi Denial of Service (DoS) sono attacchi mirati all'interruzione dell'erogazione del servizio.

- Se il servizio è l'accesso stesso a internet (ad esmpio un hotspot che offre connettività), il danno in termini economici è rilevante.
- Esistono situazioni Mission Critical in cui non ci si può permettere di non avere connettività (es. scadenze produttive, reti di emergenza . . .).
- L'interruzione del servizio rende all'utente una generale impressione di inaffidabilità, quindi lo allontana.

DoS sull'autenticazione/associazione



1. il client chiede di autenticarsi
2. AP risponde con un *challenge text*
3. Il client risponde con il *challenge text cifrato*

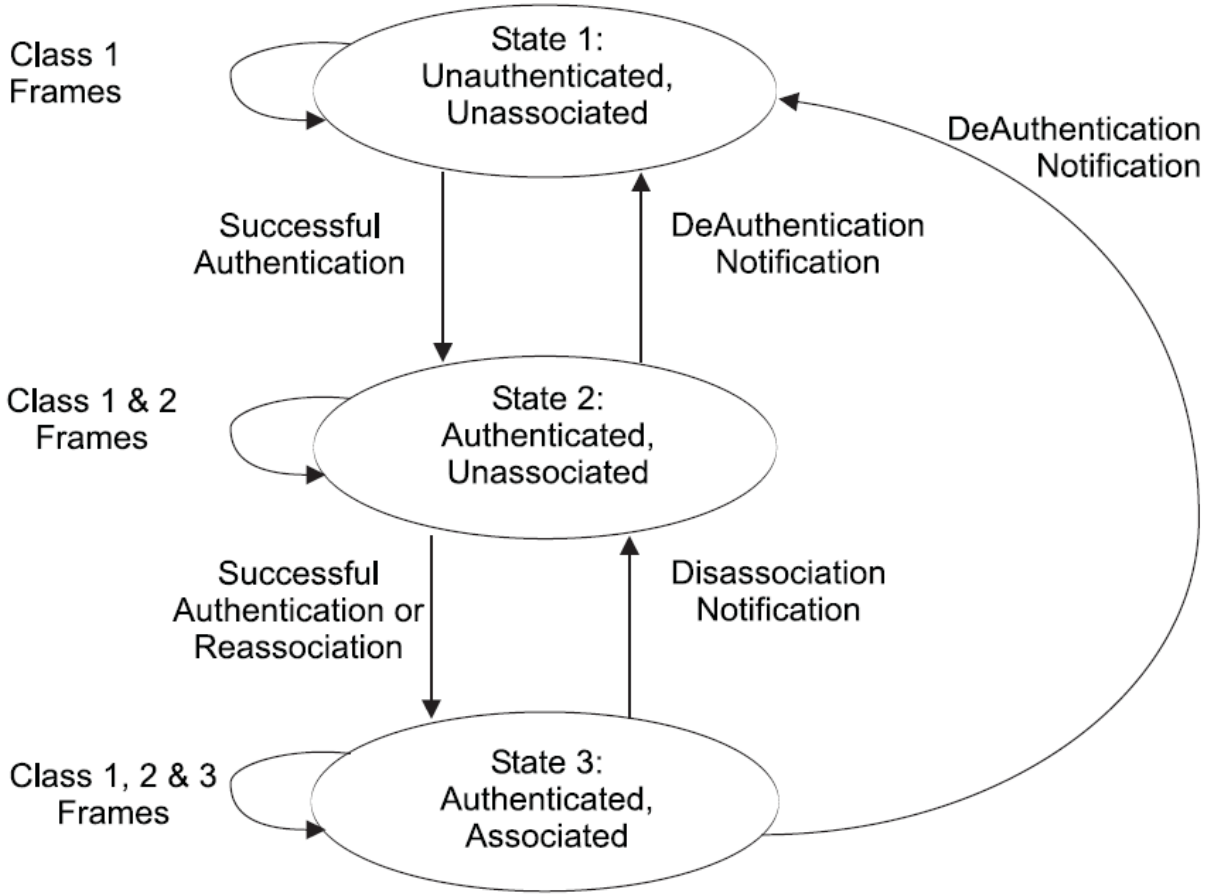
Leonardo Maccari,
leonardo.maccari@unifi.

DoS sull'autenticazione/associazione

- I pacchetti di autenticazione non sono autenticati, quindi un attaccante può falsificarli.
  - Durante la fase di ingresso l'attaccante attende l'autenticazione, e risponde al posto dell'AP con un pacchetto di deautenticazione.
  - In questo modo può evitare che le macchine entrino in rete.
  - In qualsiasi momento l'attaccante può inviare un pacchetto di deautenticazione per forzare l'uscita dalla rete di un client.
- In questo modo si può evitare che un determinato client si connetta. . .
- . . . o semplicemente tenere fuori dalla rete altri client per avere più banda a disposizione.
- L'attaccante se vuole continuare a produrre l'attacco deve continuamente stare in ascolto di nuove autenticazioni.

DoS di associazione:

Lo stesso tipo di attacco può essere fatto sull'associazione:



Leonardo Maccari,
leonardo.maccari@unifi.

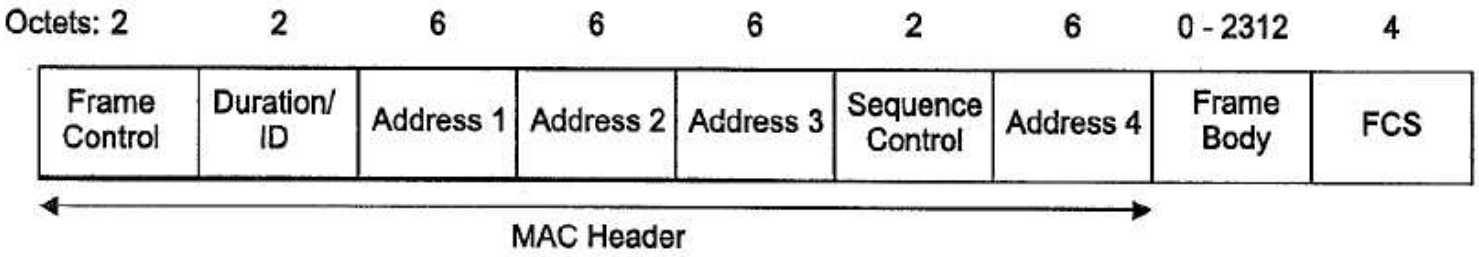
DoS di associazione:

- La differenza sta nel fatto che il secondo attacco non richiede una riautenticazione, quindi ha meno impatto.
- Può servire per far rivelare l'essid quando l'AP non lo rivela.

DoS di associazione/autenticazione:

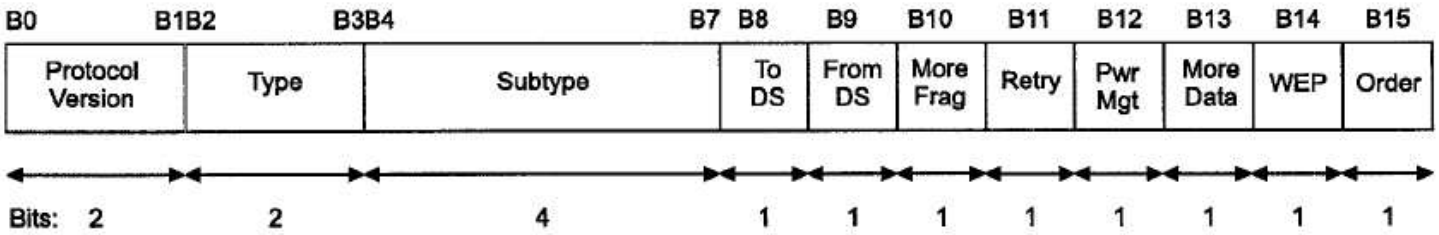
- Questo tipo di attacchi sono ancora più pericolosi se l'attaccante oltre a cambiare (*spoofare*) l'indirizzo sorgente, utilizza l'indirizzo destinazione di broadcast.
- Alcuni client sono configurabili per non accettare le richieste di deautenticazione/deassociazione in broadcast, non rispettando lo standard.

DoS sull'accesso al canale



- Il campo duration specifica il tempo per cui il canale rimarrà occupato dal mittente del pacchetto.
- Ogni macchina della rete che riceve un pacchetto qualsiasi, anche non rivolto al suo mac deve leggere e rispettare il campo duration.
- Il campo duration è espresso in microsecondi, ma l'attaccante può inviare un nuovo pacchetto prima che scada il timeout, riprenotando il canale.
- In questo modo nessuna macchina può trasmettere a parte l'attaccante.

DoS sulla modalità Power Save



- Il bit Power Save viene utilizzato dal client per segnalare all'AP che il client sta entrando in modalità power save.
- In modalità power save l'AP non trasmette il traffico al client ma bufferizza i frames e glieli invia a burst quando il client li richiede.
- Un'attaccante può inviare pacchetti *spoofati* con il bit power save settato, con una certa frequenza. In questo modo l'AP non trasmetterà mai i frames bufferizzati.
- Il risultato è un DoS che isola una singola macchina della rete senza un grosso sforzo da parte dell'attaccante.

DoS sulla saturazione della banda

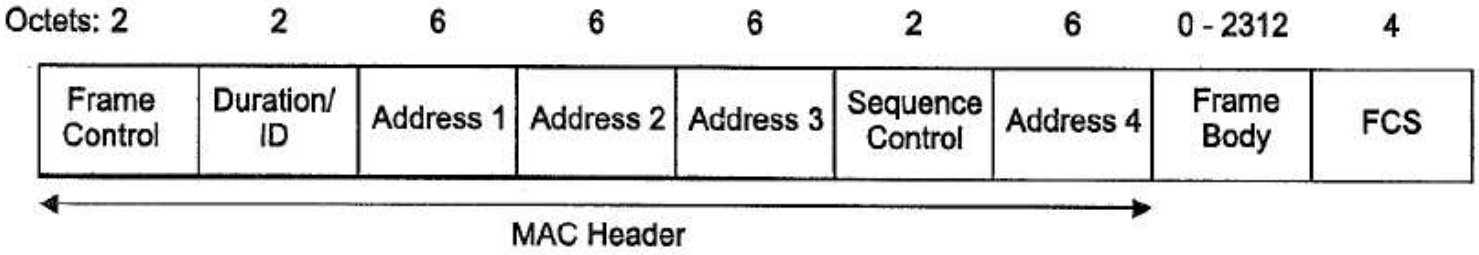
- Per trovare le macchine circostanti si utilizzano dei *probe* a livello II:
  - La macchina richiedente invia all'indirizzo di broadcast un messaggio di management di tipo *probe request*.
  - Tutte le macchine che ricevono la richiesta rispondono con un *probe reply* diretto al richiedente.
- I messaggi di probe essendo messaggi di management non vengono cifrati, quindi un attaccante li può falsificare, provocando le risposte degli altri host della rete. Ripetendo le richieste in continuazione può occupare tutta la banda disponibile, sfruttando l'effetto di riflessione degli altri host.
- Al contrario del DoS sulla deautenticazione gli host non possono evitare di rispondere ai probe in broadcast, perchè verrebbe annullata l'utilità stessa del meccanismo di probing.

DoS sullo strato fisico: jamming

- 802.11 utilizza una codifica spread spectrum, in cui il segnale viene trasmesso utilizzando una banda più larga di quanto non sarebbe necessario, aggiungendo ridondanza. A destinazione il segnale viene ricostruito in una gamma più stretta.
- In questo modo un segnale molto potente, ma concentrato su una gamma di frequenza molto stretta, viene ricevuto a destinazione, dopo la ricostruzione, come un rumore distribuito su tutta la frequenza.
- É quindi molto difficile riuscire a disturbare la ricezione di tutti i dati.

DoS sullo strato fisico: jamming

- Nonostante questo, è da notare che i pacchetti 802.11 hanno un codice di controllo degli errori:



- quindi anche se è difficile disturbare la ricezione di un intero pacchetto, se si riesce a disturbare la ricezione di un solo bit, che statisticamente è un risultato molto più accessibile, si provoca il fallimento del controllo di errore e il pacchetto viene scartato, quindi deve essere ritrasmesso.

Attacchi sui software degli AP

- Spesso gli AP presentano delle interfacce WEB di gestione.
- Le macchine collegate alla rete possono accedere all'interfaccia di gestione, da cui si possono riconfigurare gli AP.
- Si è verificato spesso che queste interfacce presentassero delle vulnerabilità, come *buffer overflow* o password attive di default che permettevano anche agli utenti della rete senza password di amministrazione di modificare delle configurazioni.
- A volte, un reset improvviso degli AP può provocare il riavvio in una modalità provvisoria, che offre anche a utenti senza credenziali di accedere all'interfaccia di gestione.

Attacchi sui software degli AP

- Gli AP devono mantenere una lista delle macchine autenticate nella rete, delle macchine associate e delle macchine che hanno richiesto l'autenticazione ma non hanno ancora completato le procedure. Quando una lista si riempie, altre richieste vengono scartate.
- Per la gestione di tali liste devono essere applicate politiche efficienti, alcuni esempi di inefficienza:
  - Le liste sono delle code a scorrimento. Quindi se la lista è piena e arriva una nuova macchina, la più vecchia viene tolta dalla lista.
    - Forgiando richieste di autenticazione false si riempie la lista e si impediscono anche le autenticazioni già in corso.
  - Le tre liste sono unite in una sola lista.
    - Rende l'effetto del difetto precedente ancora peggiore.
  - Non avviene una corretta gestione della memoria per le liste.
    - Si può produrre un buffer overrun, provocando il blocco o il riavvio dell'AP (vedi anche slide precedente).
- Esistono molti esempi di *exploit* su AP derivanti da bug di questo tipo.

Utilizzo di chiavi statiche:

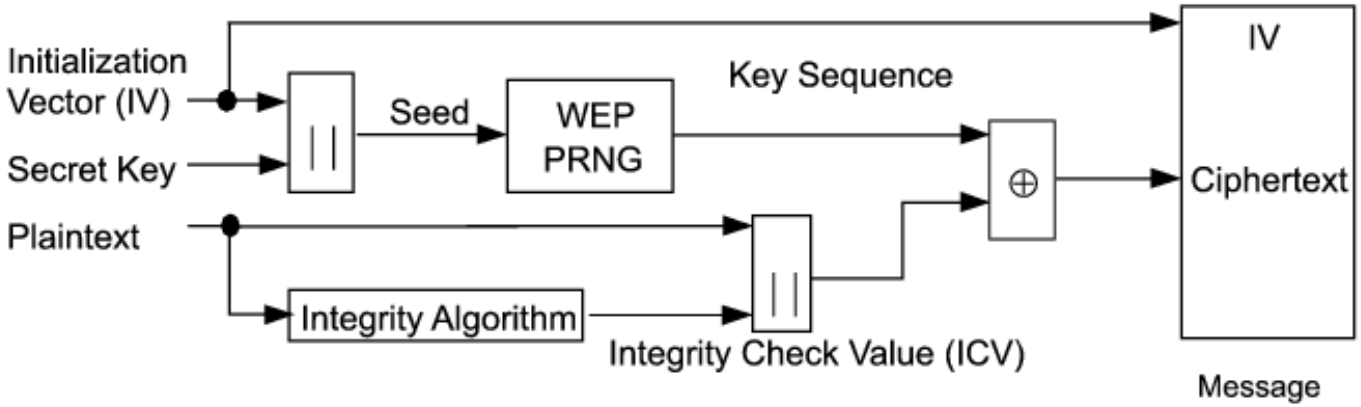
- Come detto, la chiave è unica, in questo modo non esiste nessuna segretezza, quindi autenticazione tra le macchine della stessa rete.
- Una macchina autenticata può spostare la chiave su altre macchine e lasciare che entrino.
- Anche le Access List sugli AP (che non fanno parte dello standard) sono generalmente statiche, quindi il problema della gestione è importante. Inoltre sulla maggior parte delle schede wireless è possibile cambiare l'indirizzo MAC.
- Essendo la chiave statica, tutta la fiducia è riposta nella certezza che l'algoritmo di autenticazione e cifratura sia robusto.
- Per lo stesso motivo l'AP non si autentica con le macchine.

Oracle attack:

L'autenticazione shared key è tragicamente insicura:

- Nel giro di pochi secondi passa lo stesso testo (128 byte) prima in chiaro e poi cifrato.
  - l'attaccante può recuperare un frammento di keystream che può utilizzare per inviare pacchetti nella rete, anche senza possedere la chiave WEP!
- l'attaccante può effettuare un attacco di tipo reply anche senza conoscere la chiave, spacciandosi per l'AP.
- l'attaccante può effettuare l'attacco dell'oracolo.

Procedura di cifratura RC4

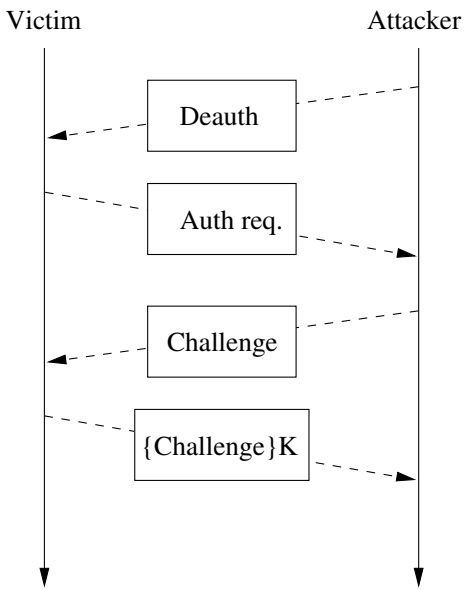


Leonardo Maccari,
leonardo.maccari@unifi.

Oracle attack:

Attacco dell'oracolo

L'attaccante non conosce la chiave segreta ma vuole inviare un messaggio nella rete



- deautentica un client
- forgia un pacchetto con un challenge text contenente i dati che vuole inviare
- il client risponde restituendo il challenge text cifrato con un certo IV, ovvero il pacchetto valido per essere inviato lungo max 128 byte

Leonardo Maccari,
leonardo.maccari@unifi.

Ancora sull'Oracolo:

- L'attacco può essere utilizzato verso un client quando nella rete non avviene autenticazione shared key per ricavare un frammento di *keystream*.
- L'attacco non ha un utilizzo concreto molto comune, ma dimostra la goffaggine con cui sono stati progettati i meccanismi di sicurezza del protocollo.

Ancora sull'autenticazione Shared Key:

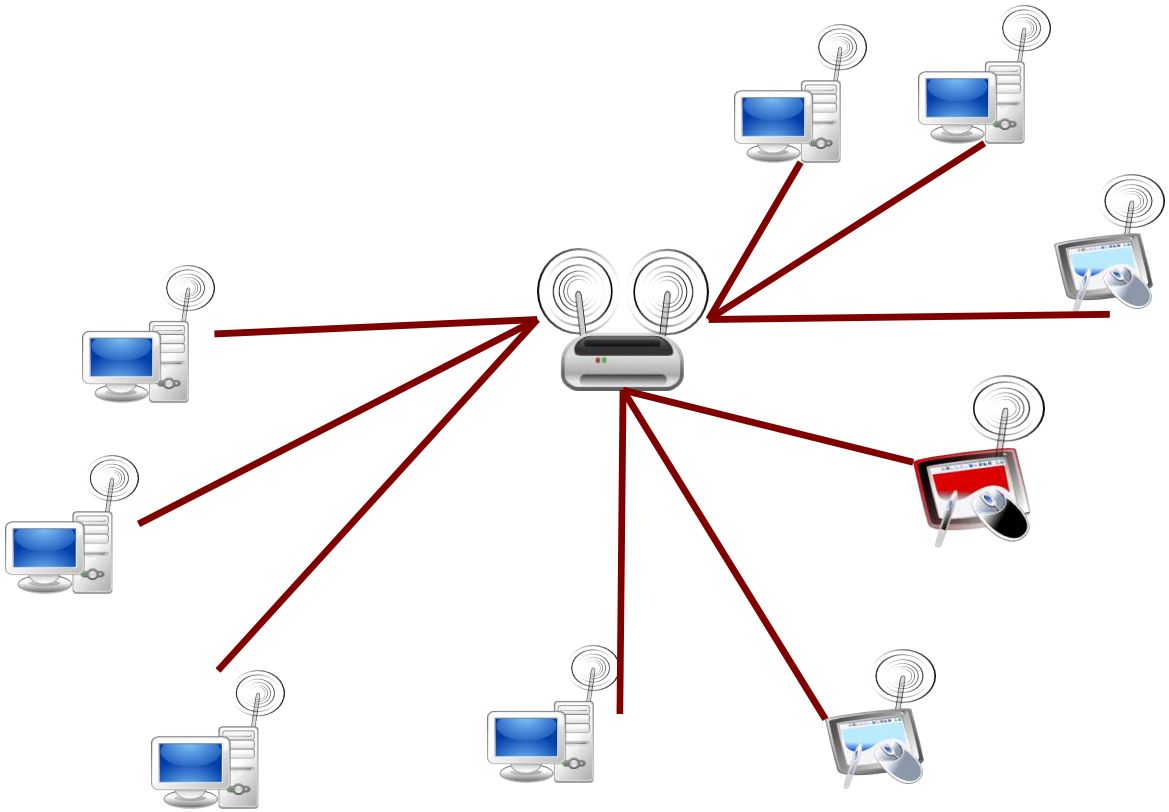
- Questi problemi hanno spinto i produttori di AP, e i gestori delle reti a preferire come scelta di default l'autenticazione open system, ovvero nessuna forma di autenticazione.
- Per evitare che chiunque entri nella rete si preferisce mascherare nei beacon l'ESSID dell'AP che è un parametro necessario per richiedere l'associazione, ma. . .
- . . . in questo modo si crea un'altra divergenza dallo standard.

Attacchi Man In The Middle

- Per attacco MITM si intende la possibilità di convogliare tutto il traffico tra due host attraverso l'attaccante, con molteplici scopi:
  - assicurarsi che il traffico che si vuole intercettare passi per la propria macchina
  - convincere una macchina che la forma di autenticazione è cambiata e che adesso non si deve più utilizzare una chiave WEP
  - poter influenzare le procedure di autenticazione e crittografia degli strati superiori (es: attacco MITM sui certificati SSL).

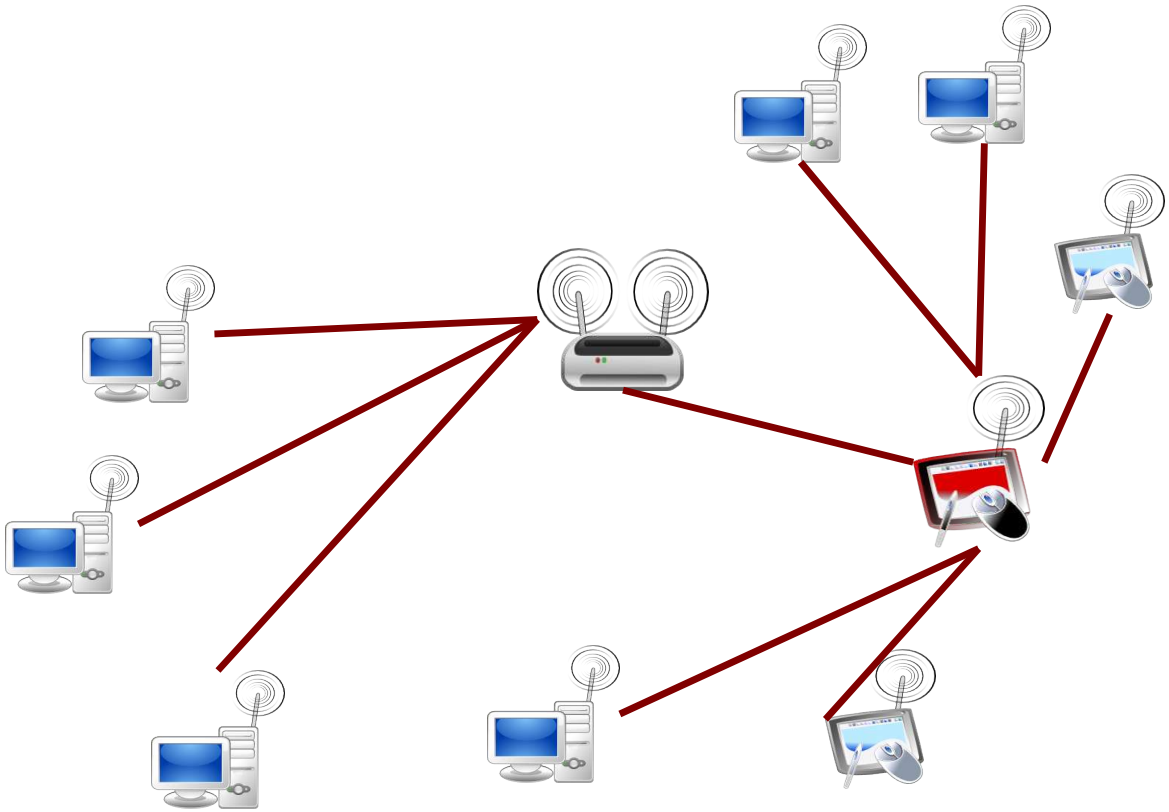
Leonardo Maccari,
leonardo.maccari@unifi.

Prima dell'attacco



Leonardo Maccari,
leonardo.maccari@unifi.

Dopo l'attacco



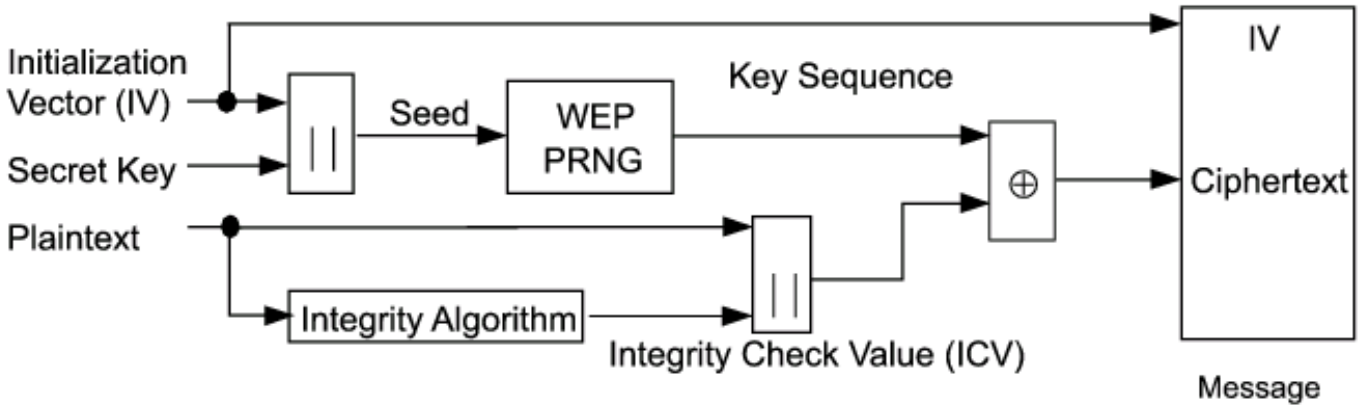
Leonardo Maccari,
leonardo.maccari@unifi.

MITM:

- Qualsiasi macchina della rete che possiede la chiave WEP può spacciarsi per AP.
- Se l'attaccante deautentica un host, l'host successivamente cercherà di ripetere l'autenticazione.
- Si genera una *race condition*, percui l'attaccante può cercare di rispondere prima dell'AP, che si può aiutare con una seconda scheda con la quale produrre un DoS sul vero AP, per favorirsi nella *gara*.
- Spesso, dopo un certo numero di disconnessioni un host cercherà di ripetere l'autenticazione su un canale diverso, facendo channel hopping.
- L'attaccante si può mettere in ascolto su un altro canale, in questo modo è sicuro che la vittima si collegherà con lui.

I finti AP si chiamano comunemente *Rogue AP*, o *Fake AP*.

Lunghezza del vettore di inizializzazione



- La non ripetizione degli IV è fondamentale per non rischiare di esporre il materiale cifrato, riutilizzare un IV infatti significa utilizzare due volte lo stesso *keystram*.
- Se si conosce il contenuto in chiaro di uno dei due pacchetti cifrati con lo stesso *keystream*, automaticamente si risale al *keystream* stesso, e quindi al contenuto di tutti i pacchetti cifrati con lo stesso IV.
- É possibile costruire un dizionario di tutti i *keystream*?

Lunghezza di IV:

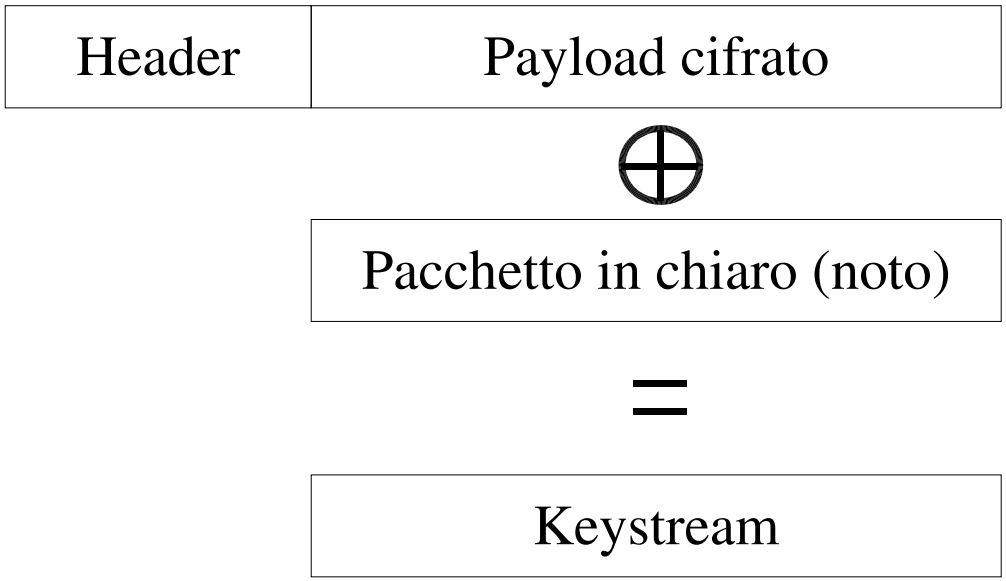
Due calcoli:

- il campo IV è lungo 24 bit $\rightarrow$ 16.777.216 IV diversi
  - ogni pacchetto tipicamente è lungo 1500 byte, quindi in totale perchè IV si ripeta devono passare circa 25G di dati, che su una rete con 30Mbit/s di banda si ottengono in circa due ore.
- Questo permette in linea teorica di poter costruire un dizionario di tutti i *keystream*.

Costruzione del dizionario:

- Per ricavare un *keystream* l'attaccante deve conoscere il contenuto del pacchetto che vede passare cifrato.
- Esistono dei pacchetti di cui il contenuto è predicibile, e che sono riconoscibili dalla lunghezza (es: DHCP request).
- Quando l'attaccante vede passare un pacchetto della lunghezza corrispondente conosce il contenuto, quindi automaticamente ricava il *keystream*.

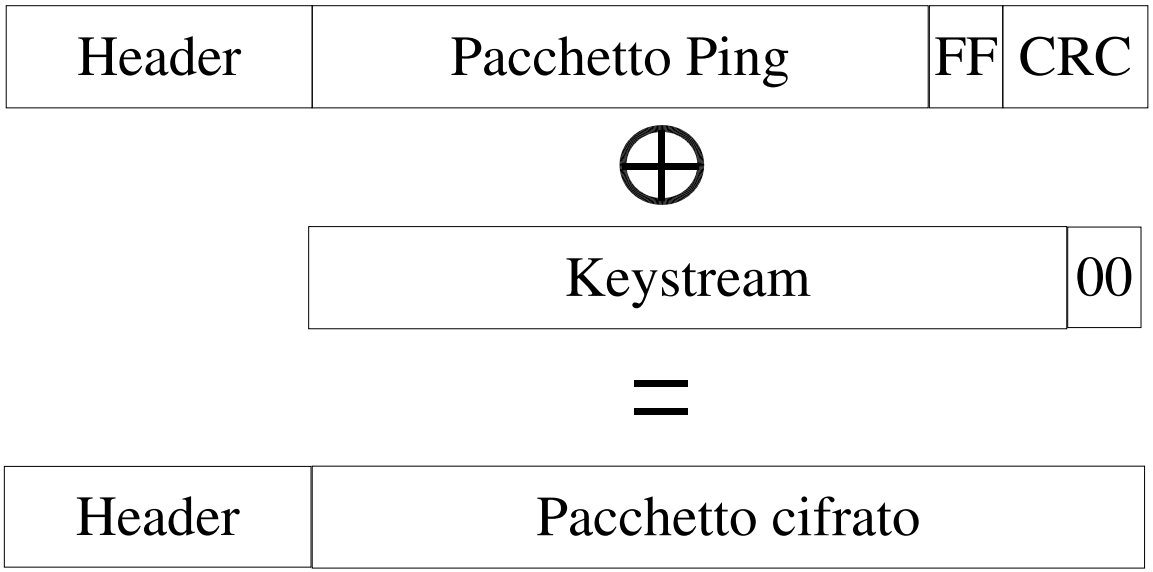
Trovare il keystream:



Estendere il keystream: chopchop attack

- Il keystream ricavato non è lungo quanto l'MTU della rete, l'attaccante deve poterlo estendere:
  - Se l'attaccante conosce un keystream lungo N bytes, forgia un nuovo pacchetto (es: Ping), più lungo di un byte.
  - Non può cifrare questo byte aggiuntivo perchè non conosce il byte aggiuntivo di keystream, quindi suppone che sia 0x00.
  - L'attaccante ricalcola il CRC, lo accoda al pacchetto e lo invia.
  - A destinazione il CRC viene verificato, se il byte di keystream non era 0x00 il CRC fallisce, e non viene ricevuta risposta. Altrimenti si riceve una risposta, quindi 0x00 era il byte giusto.
  - Se non si riceve risposta si riprova con 0x01 ...
- Mediamente, dopo 128 tentativi si ottiene il byte di estensione.
- Per ottenere tutto un *keystream* senza impattare troppo sulla rete bastano 24 ore.

Estendere il keystream:

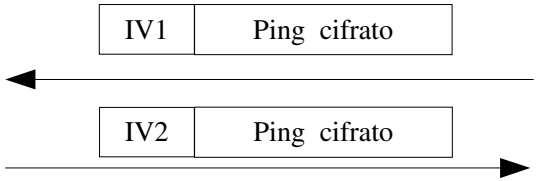


Leonardo Maccari,
leonardo.maccari@unifi.

Costruire il dizionario:

- A questo punto l'attaccante ha a disposizione un *keystream* intero. Può quindi iniettare nella rete pacchetti che vengono elaborati correttamente dalle macchine della rete.
- Esiste un'opzione del protocollo ICMP che impone ad una macchina che riceve un ping di rispondere esattamente con lo stesso pacchetto.
- L'attaccante forgia dei ping di 1500 byte, e conosce la risposta.
- La vittima risponderà utilizzando IV diversi, quindi mettendo a disposizione dell'attaccante nuovi *keystream*.

Estendere il keystream:



Due calcoli

- Per avere accesso non autorizzato ad una rete 802.11 bisogna effettuare le seguenti operazioni:
  - individuazione di pacchetto DHCP/attacco dell'oracolo $\rightarrow$ pochi secondi
  - estensione del keystream $\rightarrow$ 24 ore
  - generazione del dizionario $\rightarrow$ 3/4 ore
  - totale $\simeq$ 28 ore.
- se non si vuole rendere l'attacco troppo evidente bisogna diminuire il traffico generato e raddoppiare o triplicare il tempo occorrente
- Una volta costruito il dizionario si possono decifrare tutti i pacchetti della rete, oltre che inviarne senza conoscere la chiave segreta!

Note:

- Avendo chiavi statiche, una vita media di 28 ore è troppo breve.
- Si può costruire un dizionario perchè la sequenza degli IV non è vincolata.
- Come conseguenza alcuni produttori hanno allungato il campo IV, non rispettando lo standard.

Vulnerabilità di RC4

- Nel 2001 Fluhrer, Mantin e Shamir trovano una vulnerabilità nel modo in cui RC4 genera i *keystream*.
  - quando si utilizzano determinati IV per generare il keystream esiste una correlazione statistica tra il primo byte del keystream e la chiave segreta utilizzata. Si dice che esistono IV *deboli*
  - raccogliendo almeno 60 pacchetti cifrati a partire da IV *deboli* si può ricavare la chiave segreta!
  - NB: non si parla si un keystream, si parla della chiave segreta che viene inserita nella cifratura WEP, e che una volta compromessa dà accesso completo alla rete.

Leonardo Maccari,
leonardo.maccari@unifi.

Vulnerabilità di RC4

- Gli IV deboli sono distribuiti uniformemente nello spazio degli IV, e per ottenere 60 IV interessanti ci vogliono mediamente 4.000.000 di pacchetti cifrati
- a seconda del traffico generato dalla rete in poche ore si rompe una chiave WEP e si ottiene una chiave segreta a 40 bit!
- la complessità dell'attacco, inoltre aumenta linearmente con la lunghezza della chiave WEP
- Quindi, anche utilizzando chiavi di 128, 256 . . . bit, il tempo necessario per ottenere la chiave WEP aumenta linearmente, quindi l'attacco è sempre valido!
- Alcuni produttori corrono ai ripari impedendo ai loro AP di utilizzare IV deboli, non rispettando lo standard.

Vulnerabilità di RC4

- Nell'agosto 2004 l'hacker *KoreK* invia su un forum un programma basato su una sua ricerca statistica che evidenzia che esiste correlazione anche tra altri byte di *keystream* e la chiave WEP, rendendo l'attacco precedente ancora più facile
- successivamente vengono pubblicate nuove migliorie, per rompere una chiave WEP a 40 bit basta raccogliere qualche decina di migliaia di pacchetti cifrati e attendere un tempo di elaborazione di pochi secondi.

Note sull'algoritmo RC4:

- Le specifiche tecniche di RC4 vengono rivelate solo alcuni anni dopo la sua pubblicazione.
- La comunità scientifica quindi riceve RC4 con sospetto, e può analizzarlo veramente in ritardo.
- Utilizzare un algoritmo chiuso ha prodotto questo risultato.

Attacchi sul CRC

Il CRC è lineare rispetto all'operazione di $\oplus$. Se C è un pacchetto cifrato, M il pacchetto in chiaro e K il keystream[1]:

$$\begin{aligned} C &= K \oplus M \\ &= (K_p \parallel K_c) \oplus (M_p \parallel CRC(M)) \\ &= K_p \oplus M_p \parallel (K_c \oplus CRC(M)) \\ &\equiv C_p \parallel C_c \end{aligned}$$

Se vogliamo generare un messaggio M'_p che sia una modifica del messaggio originale M (definiamo $M'_p = M_p \oplus d$ dove d è la modifica che vogliamo apportare) e ottenere un corrispondente messaggio cifrato C' possiamo farlo:

$$\begin{aligned} C' &= K \oplus (M'_p \parallel CRC(M'_p)) \\ &= (K_p \oplus M_p \oplus d) \parallel (K_c \oplus CRC(M \oplus d)) \\ &= (K_p \oplus M_p) \oplus d \parallel (K_c \oplus CRC(M) \oplus CRC(d))) \\ &= (C_p \oplus d) \parallel (C_c \oplus CRC(d)) \end{aligned}$$

[1] col pedice p e c indichiamo la parte di payload e quella di CRC

Attacchi sul CRC

- L'attaccante può prendere un pacchetto cifrato, cambiarne il contenuto (facendo lo XOR sia del contenuto con *d*, sia del CRC con CRC(d)), reinviarlo anche senza conoscere il contenuto.
- Ad esempio, l'attaccante potrebbe cambiare parte dell'indirizzo IP destinazione (se è predicibile in qualche modo). In questo modo l'AP reinstraderebbe verso l'esterno (possibilmente verso un host controllato dall'attaccante stesso) il pacchetto, ovviamente dopo averlo decifrato.

Variante di chopchop

Lo stesso tipo di attacco può essere utilizzato per recuperare una messaggio in chiaro dato un messaggio cifrato un byte alla volta.

- L'attaccante prende un pacchetto C, ed elimina l'ultimo byte B.
- Con trasformazioni simili a quelle viste, si può ricalcolare il CRC del messaggio troncato a partire da C e da B. Ma l'attaccante non conosce B.
- Pone B=0x00, ricalcola il CRC del pacchetto troncato e lo invia.
- Se l'AP risponde qualcosa (qualsiasi risposta indica che il CRC era corretto) allora l'ultimo byte del messaggio originale è effettivamente 0x00.
- Altrimenti cicla con 0x01...

Conclusioni

- 802.11 non garantisce la disponibilità del servizio offrendo facili attacchi DoS
- WEP non garantisce l'integrità dei dati (CRC lineare)
- WEP non garantisce l'autenticazione, la segretezza, la non ripudiabilità dei dati (RC4 insicuro)
- WEP non garantisce il controllo degli accessi (autenticazione insicura)

Inoltre:

- Tutta la gestione delle chiavi si basava sulla robustezza degli algoritmi, che si sono rivelati insicuri.
- Per correre ai ripari ogni costruttore ha apportato delle modifiche non previste dello standard:
  - IV di lunghezza diversa.
  - Non utilizzo di alcuni IV.
  - Chiavi di lunghezza diversa.
  - ESSID non sponsorizati.
  - Reazioni non standard agli attacchi (per es. associazione/auth).
- Queste modifiche ovviamente rendono le reti incompatibili tra di loro.
- Nessuno di questi accorgimenti, da solo risolve i problemi di sicurezza delle 802.11.

Come utilizzare le 802.11, versioni antecedenti alla *i*

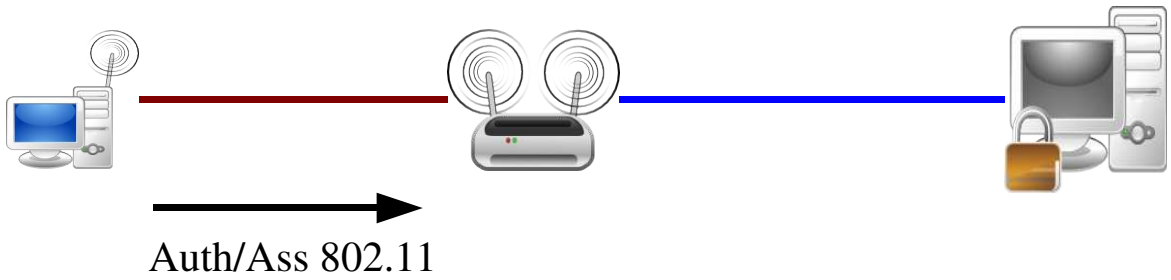
Dato per certo che, se possibile, è meglio non utilizzarle, nel caso in cui si abbia a disposizione materiale di questo tipo ci sono alcune buone pratiche da utilizzare:

- Non esporre l'ESSID. Questo rallenta o scoraggia minimenente l'attaccante.
- Utilizzare le chiavi più lunghe supportate dall'hardware.
- Cambiare spesso la chiave.
- Non utilizzare l'autenticazione Shared Key.
- Far passare il traffico comunque su una VPN.

Rimanere coscienti che nonostante questi accorgimenti la rete può essere vittima di un attacco DoS in qualisasi momento.

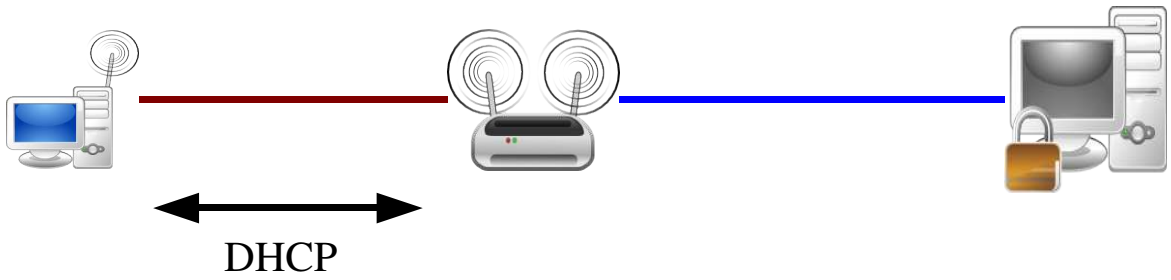
HTTP authentication

All’ingresso nella rete il client fa un’autenticazione e un’associazione in standard 802.11



HTTP authentication

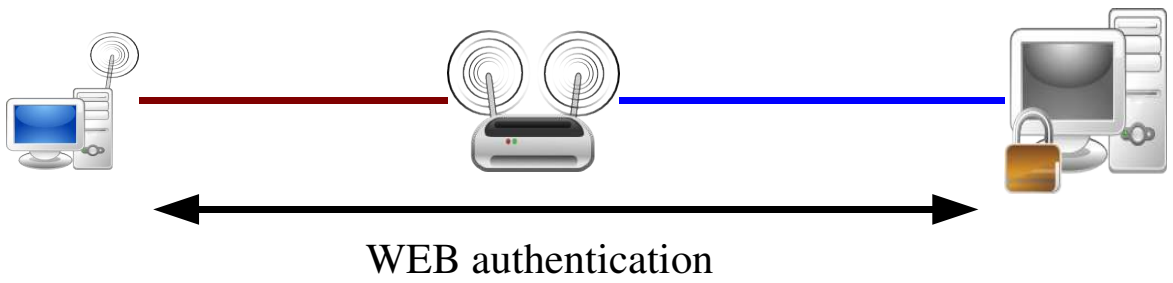
Il client riceve un indirizzo IP con DHCP



Leonardo Maccari,
leonardo.maccari@unifi.

HTTP authentication

Il client si connette alla porta 80 del server di autenticazione, e si autentica con un metodo qualsiasi (SSL, password, md5 password ecc. . .).



Leonardo Maccari,
leonardo.maccari@unifi.

HTTP authentication

- Non esiste uno standard per effettuare l'autenticazione HTTP.
- L'autenticazione deve sempre passare su SSL.
- Si introducono tutti i problemi riguardanti i livelli superiori:
  - Sicurezza del web server
  - Sicurezza del browser (eventuali problemi di cookies, di SQL injection ecc. . .)

Abbreviazioni:

802.1X	Port-Based Network Access Control standard.
WPA	Wireless Protected Access certification (vers. 1 o 2).
EAP	Extensible Authentication Protocol.
EAPoL	EAP Over LAN.
TLS	Transport Layer Security.
RADIUS	Remote Authentication Dial In User Service

Storia di 802.11i

4/2003 Nasce WPA.

6/2004 Nasce lo standard 802.11i, quindi WPA2.

Molti produttori hanno rilasciato degli aggiornamenti di firmware/driver perchè i loro vecchi prodotti pre 802.11i fossero compatibili almeno con WPA.

Novità in 802.11i

- Algoritmi di crittografia rinnovati:
  - TKIP: utilizza sempre RC4 ma in una modalità che non permette gli attacchi visti su WEP
  - CCMP: abbandona RC4 e utilizza AES per la cifratura.
- Gestione delle chiavi rinnovata:
  - WPA-PSK: pre-shared key tra macchine della rete.
  - 802.1X based authentication.

Leonardo Maccari,
leonardo.maccari@unifi.

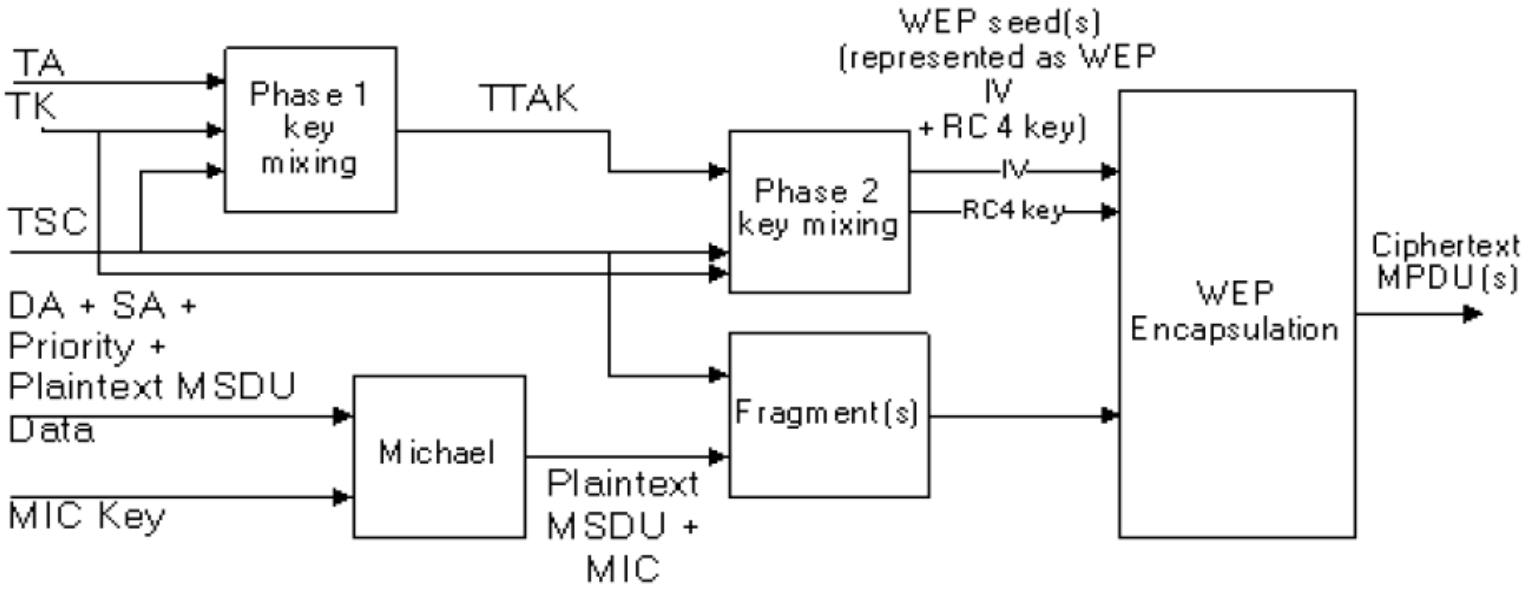
Cosa non cambia in 802.11i

- Il traffico di management.
- Il traffico di controllo.

Leonardo Maccari,
leonardo.maccari@unifi.

Cambio di algoritmi

Si utilizzano due algoritmi al posto di WEP, il TKIP o il CCMP, entrambi eliminano le problematiche di sicurezza riguardanti IV corti, chiavi craccabili, CRC ecc. . . , introducono però maggiore complessità, quindi difficilmente sono stati portati su hardware esistente



Leonardo Maccari, leonardo.maccari@unifi.

WPA e WPA2

- WPA è una versione di 802.11i che anticipa lo standard, utilizza gli algoritmi TKIP con gestione delle chiavi statica (detta anche WPA Home o WPA-PSK).
  - Gli AP o le schede client possono utilizzare TKIP con un semplice aggiornamento del firmware.
- WPA2 è la versione completa dello standard con l'utilizzo di 802.1X (WPA Enterprise).
  - Gli AP devono implementare i client RADIUS e l'algoritmo CCMP. Difficilmente realizzabile su hardware limitati.

WPA TKIP insecurity

- Negli ultimi mesi sono usciti due articoli che descrivono una variante dell'attacco chopchop per TKIP.
- Con WPA non si può ripetere due volte lo stesso IV (che prende il nome di TSC) perchè ogni ricevitore tiene un contatore degli ultimi ricevuti...
- ...ma con IEEE 802.11e (che aggiunge supporto per la QoS) esistono 8 code di ricezione diverse, ciascuna con TSC indipendente.
- L'attacco può quindi essere portato decifrando un byte per volta di un pacchetto usando le code diverse[2].

[2] *Practical attacks against WEP and WPA*
http://dl.aircrack-ng.org/breakingwepandwpa.pdf

WPA TKIP insecurity

- Quindi, anche TKIP comincia a mostrare le prime crepe. Nella pratica si può:
- decifrare un pacchetto cifrato
- recuperare un *keystream* per riutilizzarlo in una coda distinta per iniettare un pacchetto nella rete

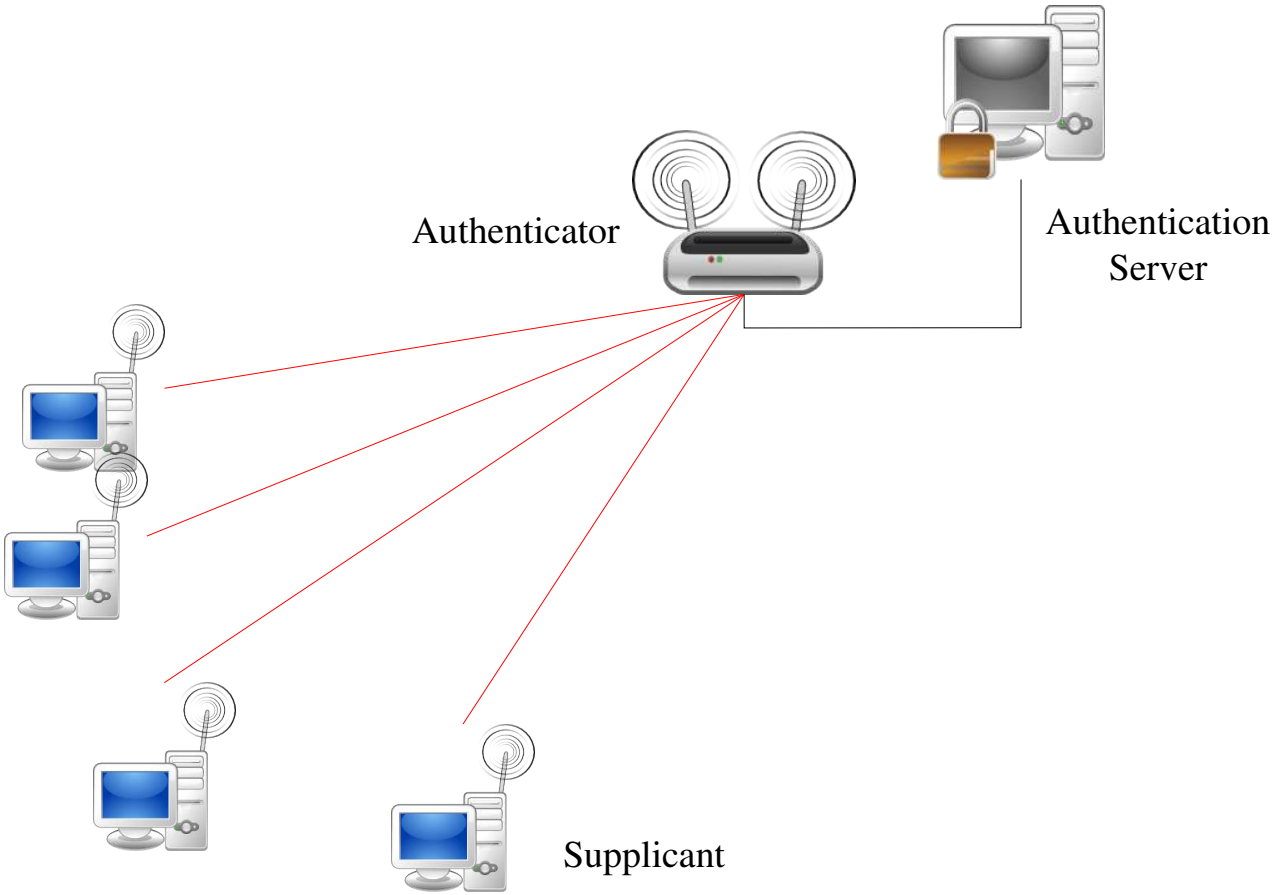
Leonardo Maccari,
leonardo.maccari@unifi.

802.1x Port-Based Network Access Control

- É uno standard che definisce dei ruoli generici per l'architettura di controllo degli accessi in reti 802.
- Si dividono i due ruoli dell' *autenticator* e dell'AP, che offre semplicemente l'accesso di livello II.
- In questo modo si ridisegna la topologia della rete, rendendola meglio gestibile.

802.1X - Topologia

I link in nero sono wired, quelli in rosso sono wireless. Il link tra *authenticator* e *authentication server* è un link che viene considerato sicuro ed è un link di livello 3

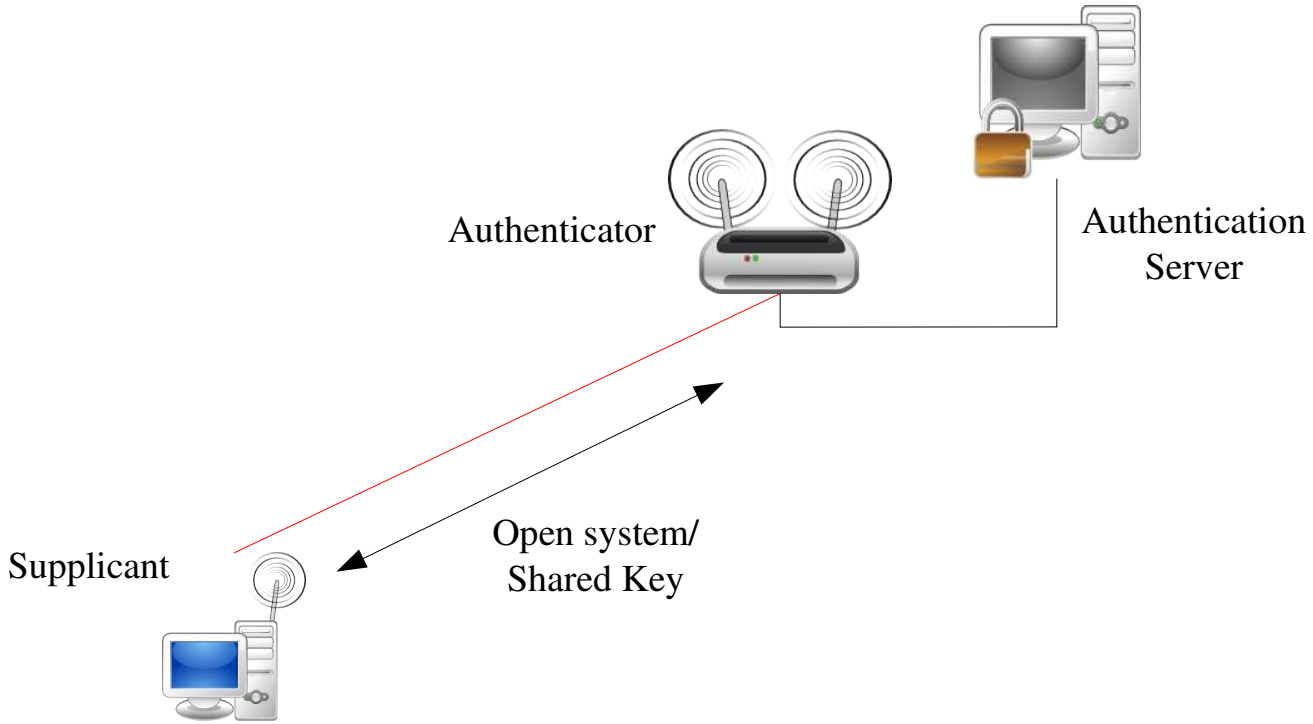


Ruoli

- *supplicant*
  - Si deve autenticare per entrare nella rete.
  - Deve generare del *keying matherial* per poter comunicare in modo sicuro con l'*authenticator*.
- *authenticator*
  - Non ha un ruolo attivo nell'autenticazione (proxy).
  - Alla fine dell'atenticazione deve possedere del *keying matherial* in comune con il *supplicant*.
  - Subito dopo deriva da questo delle chiavi per cifrare e autenticare.
- *authentication server*
  - É un database di credenziali di autenticazione, quindi è lui che autentica il *supplicant*.
  - Una volta stabilità l'identità di *supplicant* decide se farlo entrare o meno e lo comunica all'*authenticator*.
  - Anche l'*authentication server* si deve autenticare con il *supplicant*, l'autenticazione è sempre bidirezionale.

Fasi

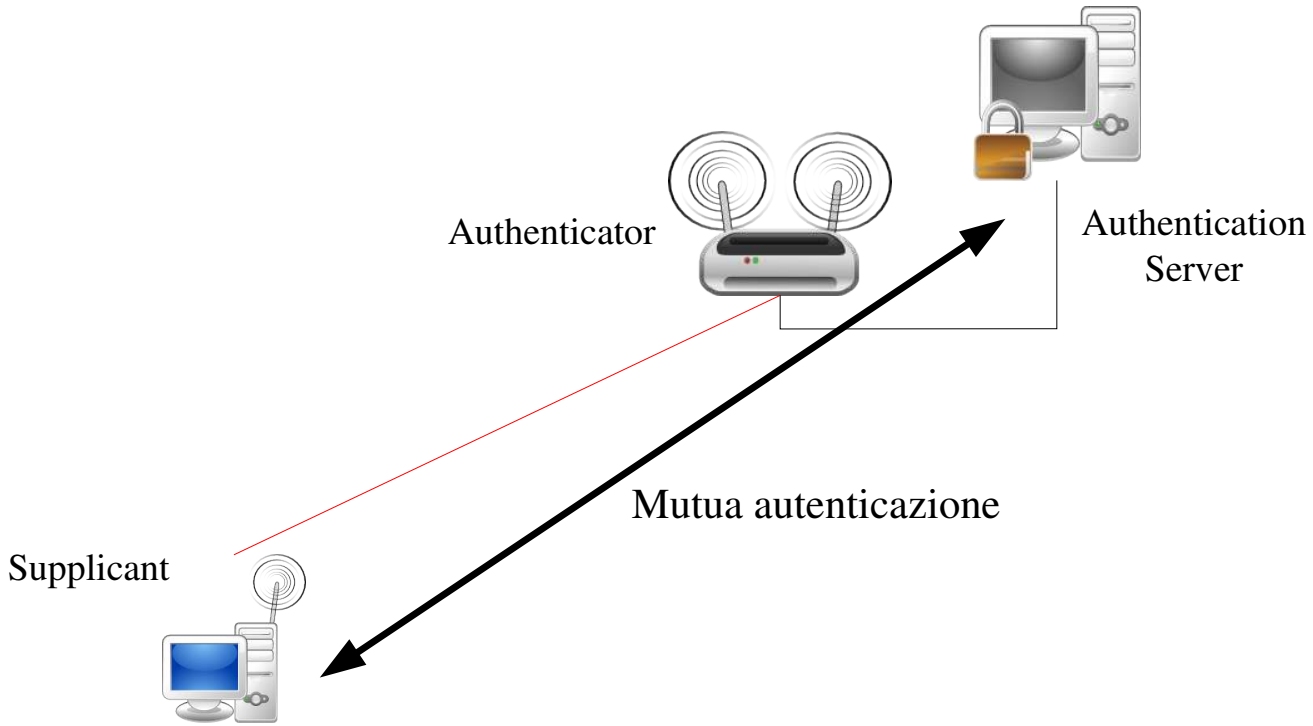
Prima fase: autenticazione 802.11 (solo per compatibilità) e associazione.



Leonardo Maccari,
leonardo.maccari@unifi.

Fasi

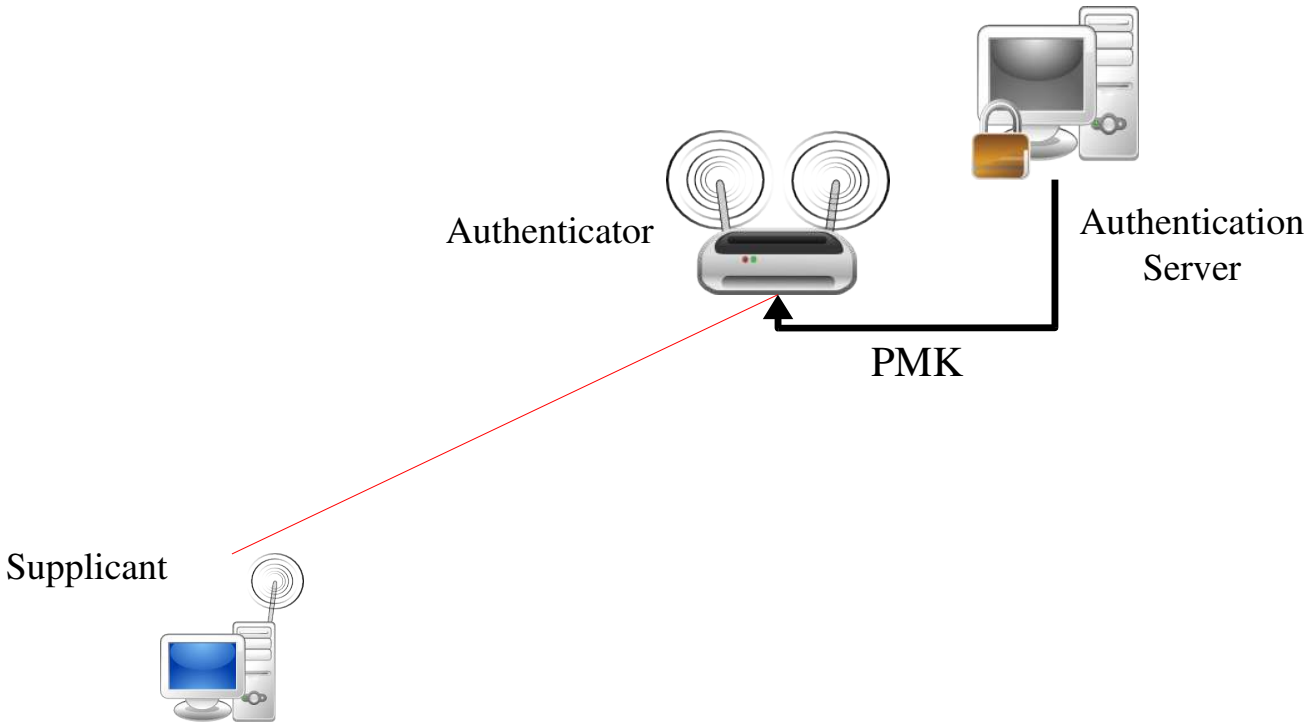
Seconda fase: autenticazione tra *supplicant* e *authentication server*. Le due macchine verificano la reciproca identità e producono una chiave simmetrica PMK (Pairwise master key).



Leonardo Maccari, leonardo.maccari@unifi.

Fasi

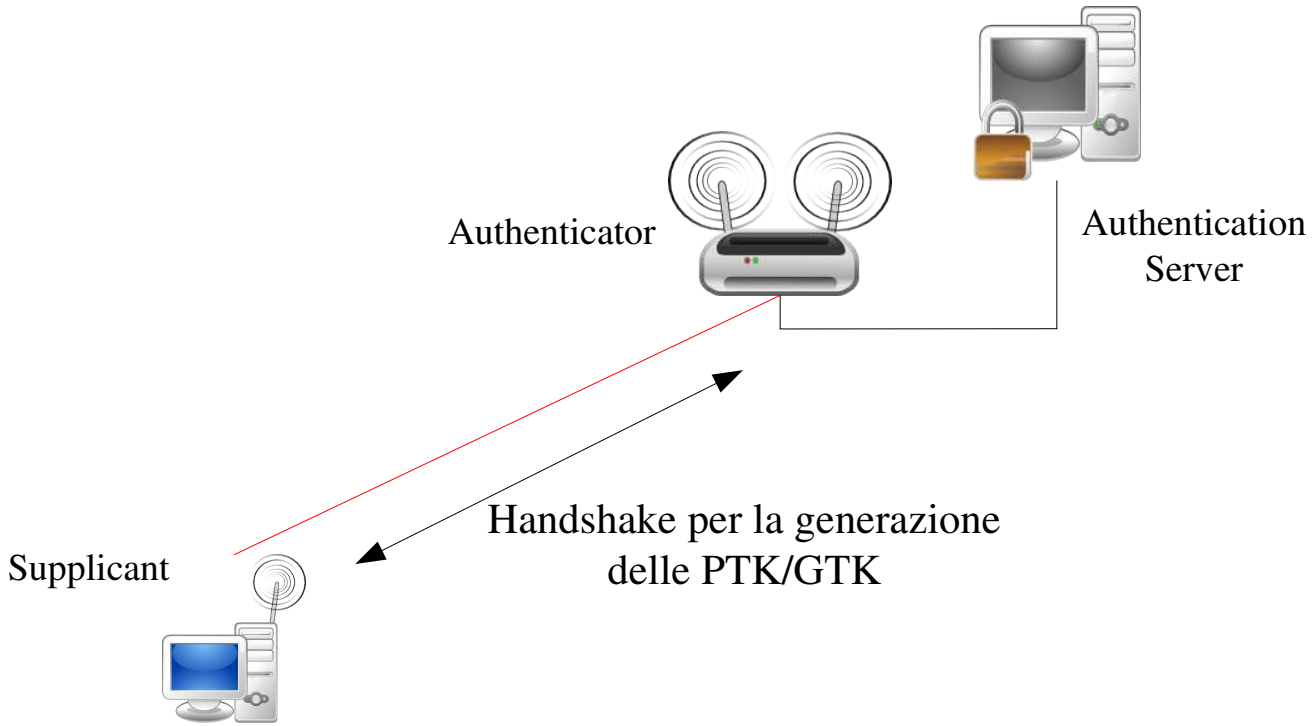
Terza fase: la PMK viene spostata sull'*authenticator*.



Leonardo Maccari,
leonardo.maccari@unifi.

Fasi

Quarta fase: a partire dalla PMK *supplicant* e *authenticator* derivano delle chiavi che verranno utilizzate per cifrare e autenticare tutti i pacchetti successivi (chiave PTK per il traffico unicast e GTK per il traffico broadcast).



- Da questo momento in poi l'*authentication server* non partecipa più alle comunicazioni se non interpellato. Saltuariamente *supplicant* e *authenticator* possono decidere di generare delle nuove GTK e PTK a partire dalla PMK che rimane la stessa (key *refresh*).
- L'*authenticator* può decidere di forzare anche una riautenticazione, e costringere il *supplicant* a ripetere l'autenticazione iniziale per generare una nuova chiave PMK.
- Un'autenticazione completa coinvolge diversi protocolli e può essere configurata in molti modi diversi.

Protocolli utilizzati:

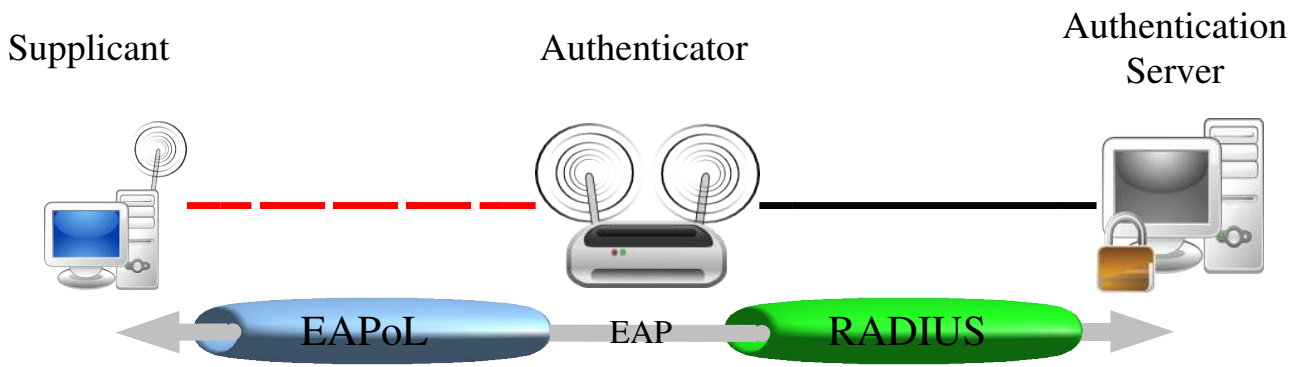
I protocolli possono essere di due tipi:

- End to End (ete): un protocollo che coinvolge due macchine virtualmente collegate, ma non fisicamente comunicanti (ad es. TCP/UDP). Nel nostro caso EAP.
- Point to Point (ptp): un protocollo che coinvolge due macchine che sono direttamente connesse (ad es. DHCP). Nel nostro caso EAPoL, ma anche, astrattamente RADIUS.

Protocolli utilizzati:

Fase 1: Standard 802.11a/b/g.

Fase 2: Tra *supplicant* e *authentication server* si usa il protocollo EAP (ete). Questo viene veicolato tra *supplicant* e *authenticator* dentro a pacchetti in formato EAPoL, e tra *authenticator* e *authentication server* attraverso il protocollo RADIUS (ptp).

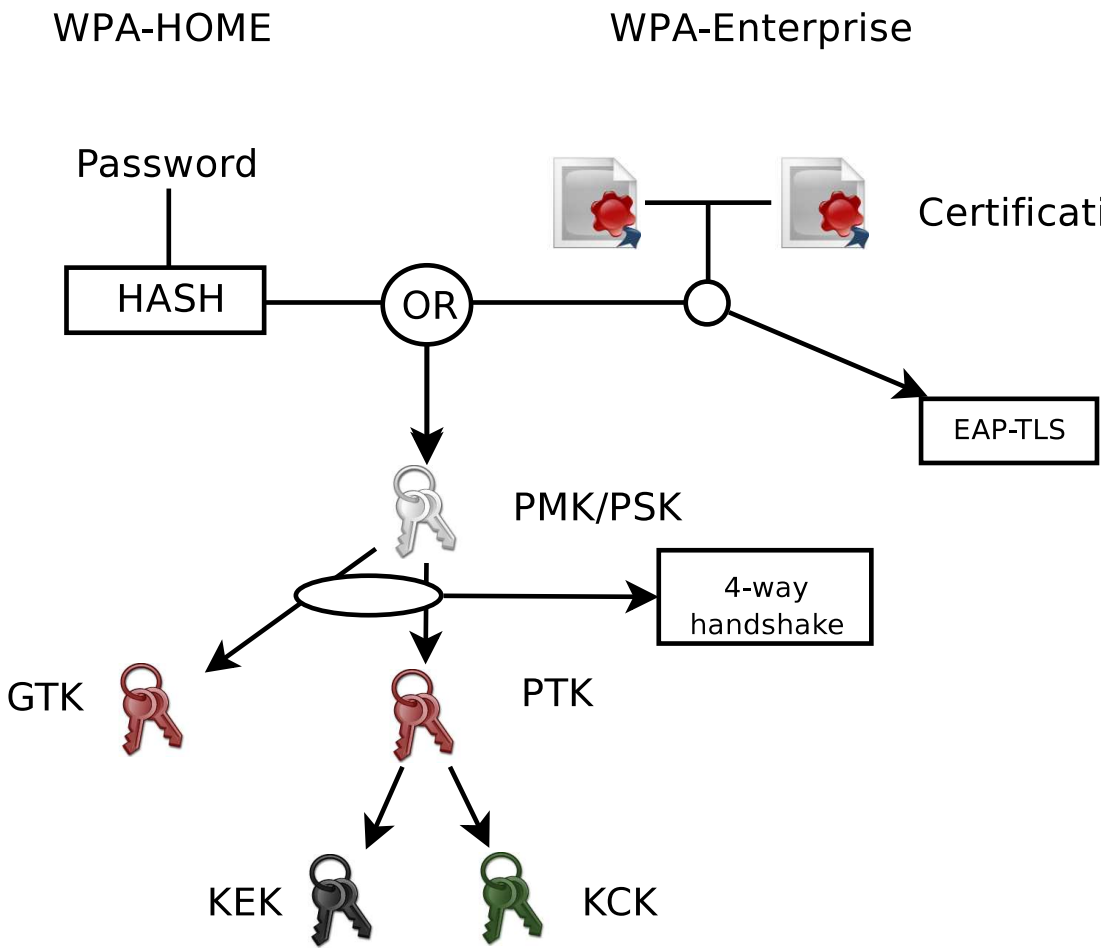


Leonardo Maccari,
leonardo.maccari@unifi.

WPA Home

- Se non si vuole utilizzare un *authentication server* si possono impostare le chiavi PMK direttamente nel *supplicant* e nell'*authenticator*. Si parla di PSK Pre-Shared Key.
- Tutto funziona nello stesso modo, ma si salta la parte di autenticazione EAP e si prosegue dagli handshake.
- Le PSK possono essere configurate in una lista, associate ai MAC address delle schede di rete dei client.
- Una PSK è costituita da 256 bit e può essere specificata come:
  - Una stringa in esadecimale: 0xa39f16ed6...
  - Una password che viene trasformata in 256 bit di chiave PSK.

Gerarchia delle chiavi



Leonardo Maccari,
leonardo.maccari@unifi.

wpa-psk

- Lo standard specifica una modalità perlomeno *consigliata* di traduzione dalla PSK al segreto:
  - PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)
- Notare che la PSK cambia anche se si cambia l'ESSID della rete.

Leonardo Maccari,
leonardo.maccari@unifi.

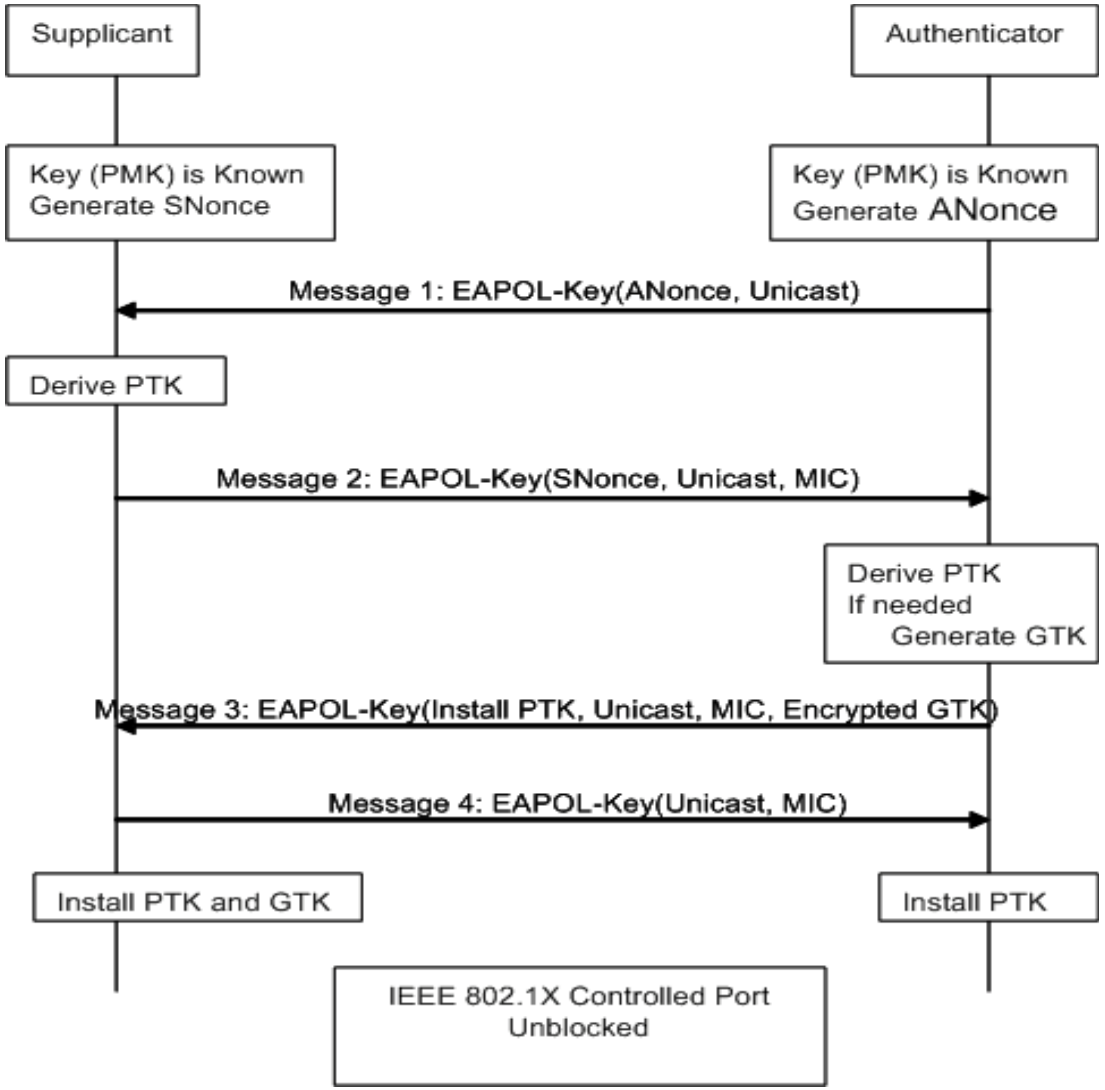
WPA-PSK

Lo standard consiglia:

- *A pass-phrase typically has about 2.5 bits of security per character, so the pass-phrase mapping converts an n octet password into a key with about 2.5n + 12 bits of security. Hence, it provides a relatively low level of security, with keys generated from short passwords subject to dictionary attack. Use of the key hash is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a pass-phrase of less than about 20 characters is unlikely to deter attacks.*

Leonardo Maccari,
leonardo.maccari@unifi.

4-way handshake



WPA-PSK

Brute force sulla password:

- La PSK viene utilizzata nel 4-way handshake per generare la PTK.
  - $PTK = PRF_{512}(PMK, ''\,stringa'', AA, SPA, Anonce, Snonce)$
- Raccogliendo i pacchetti di un 4-way handshake si può effettuare un attacco off-line utilizzando un dizionario di password.
- Per forzare un 4-way handshake si può inviare un pacchetto di deautenticazione e forzare la ripetizione di tutta la procedura.
- Per essere ragionevolmente sicuri di non poter essere vittima di attacchi di brute force bisogna:
  - scegliere pasphrase di più di 20 caratteri.
  - utilizzare PSK in esadecimale.
- Entrambe le soluzioni sono puttosto scomode.

Leonardo Maccari,
leonardo.maccari@unifi.

Riferimenti

- 802.11i overview:
- Tutorial su 802.11i
- 4-way handshake, dalla PMK alla PTK
- Un articolo introduttivo su 802.11i
- Elenco di link sulla sicurezza di 802.11
- Altre slides su 802.11i
- Descrizione di EAP, LEAP, PEAP, EAP-TLS