



# Sicurezza dei sistemi e delle reti<sup>1</sup>

Mattia Monga

Dip. di Informatica  
Università degli Studi di Milano, Italia  
[mattia.monga@unimi.it](mailto:mattia.monga@unimi.it)

a.a. 2014/15



Sicurezza delle  
reti

Monga

Problemi  
intrinseci

WEP

WPA

802.11i  
(WPA2)

# Lezione XVIII: Reti wireless



La prima rete **wireless** nasce nel 1971 fra le isole dell'arcipelago delle Hawaii (ALOHANET).

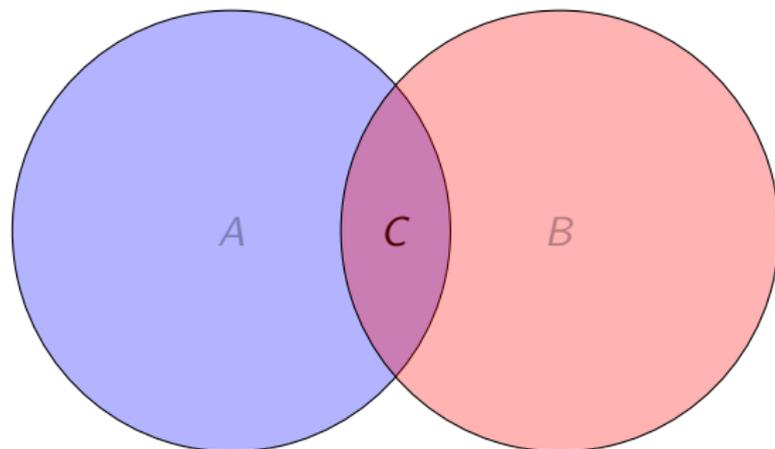
Dagli anni '90 hanno avuto una enorme diffusione:

- Trasmissione via onde radio
- Bassi costi infrastrutturali
- Flessibilità nell'utilizzo



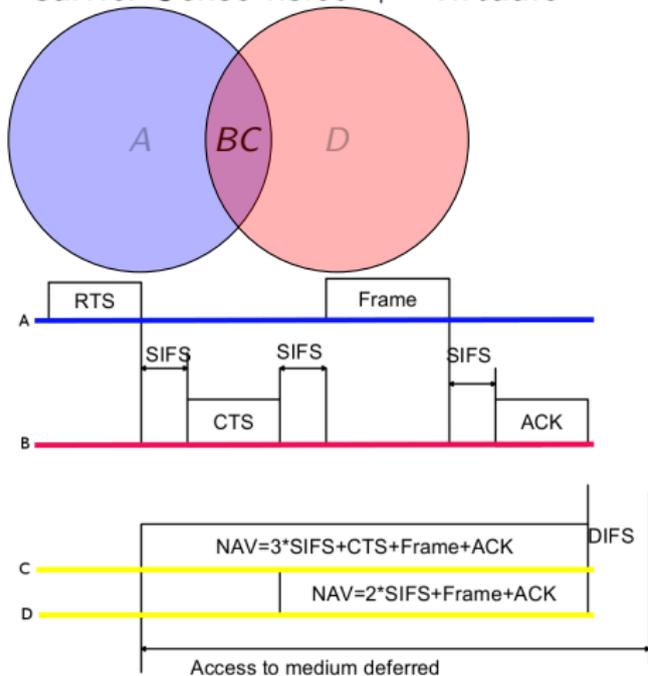
Dal punto di vista della sicurezza:

- Segnali intrinsecamente **broadcast**
- Anche se, a differenza delle LAN cablate, il canale non è necessariamente “condiviso” fra tutti, perché ci possono essere range di ricezione diversi
- Attenuazioni e interferenze



*A* non sente *B*, ma esiste comunque una zona di collisione dei due segnali: non si può usare il meccanismo di Ethernet.

## Carrier Sense fisico + "virtuale"



- $A \rightarrow B$
- **Tempi standard**  
SIFS < PIFS < DIFS < EIFS
- A, ricevuto il CTS, fa partire un timer per l'ACK
- C sente RTS (e CTS), D solo CTS



Gli standard IEEE per le LAN wireless sono raccolti nella famiglia 802.11

- 802.11a 5GHz, 54Mb/s teorico, circa 20Mb/s, 12 canali
- 802.11b 2.4GHz, 11Mb/s (5.9 Mb/s TCP 7.1 Mbit/s UDP)
- 802.11g 2.4GHz, 54Mb/s teorico, circa 25Mb/s
- 802.11i (WPA2) standard di sicurezza
- 802.11n standard recente che permette bande elevate e l'uso congiunto di più antenne



**Access point (AP)** o modalità infrastruttura: ogni nodo spedisce i pacchetti tramite un AP (che poi li gira verso una rete cablata o wireless)

**Ad hoc** un nodo scambia i frame direttamente con un altro

**Monitor** una scheda di rete riceve tutti i frame



- Ogni nodo è contrassegnato dal suo numero MAC
- Ogni AP è contrassegnato da un **Service Set Identifier (SSID)**
  - L'AP annuncia il SSID con regolarità (**beaconing**)
  - I nodi fanno **scanning** di un AP, passivo o attivo (**probe request**)
  - Il MAC dell'AP è detto BSSID



**Associazione** usato dai nodi per connettersi ad un AP, quando ci si trova nell'ambito della sua portata

**Autenticazione** usato dai nodi per avere il permesso di ricevere e spedire dati



## Le reti wireless 802.11

- Trasmissioni broadcast, con tecniche di *carrier sense* particolari
- La modalità infrastrutturale prevede AP cui ci si deve associare



- Il segnale è facile da **intercettare**
- Il segnale è facile da **disturbare**
- In alcuni casi il nodo può avere ridotte capacità di calcolo



- Eavesdropping
- Denial of service
- Spoofing e message replay

L'identificazione di un nodo è spesso affidata al solo numero MAC: facilmente falsificabile (e per di più il traffico lecito è accessibile all'attaccante!)



Wired Equivalent Privacy (WEP) 1999, tutt'ora abbastanza diffuso.

- Shared key di 40, 104 o 232 bit (WEP key)
- Le chiavi sono identificate da un keyID di un byte, perché un nodo ne può avere più di una
- Le chiavi devono essere trasmesse tramite un canale sicuro (offline a tempo di setup)
- Non c'è protezione fra coloro che conoscono la chiave (come in una LAN Ethernet)



## Chiave condivisa $K$

- 1 un nodo  $N$  manda una richiesta all'access point  $AP$
- 2  $AP$ : challenge  $w = a_1 \dots a_{16}$  di  $16 \times 8 = 128$ bit
- 3  $N$ : genera **initialization vector**  $IV$  (24 bit), calcola  $m = RC4(IV|K) \oplus w$  e manda  $r = IV|m$
- 4  $AP$  controlla  $RC4(IV|K) \oplus m = w$



- Sul canale viaggiano  $w$  e  $r = IV|(RC4(IV|K) \oplus w)$ .
- Poiché  $A \oplus B \oplus B = A$ , un attaccante può calcolare  $RC4(IV|K)$ .
- Siccome l'IV lo sceglie il nodo (e può essere riutilizzato!), l'attaccante può autenticarsi con qualsiasi challenge  $w'$  mandando  $r = IV|(RC4(IV|K) \oplus w')$



In WEP il controllo d'integrità dei pacchetti è ottenuto con un semplice CRC del pacchetto (senza elementi segreti).

- $CRC(A \oplus B) = CRC(A) \oplus CRC(B)$
- l'attaccante può alterare un pacchetto e iniettarne di nuovi



Un pacchetto  $p$  sul canale è  $x = (p|CRC(p)) \oplus RC4(IV|K)$

- L'attaccante intercetta  $x$  e manda  $x' = (p'|CRC(p')) \oplus x$
- 

$$\begin{aligned}x' &= (p'|CRC(p')) \oplus (p|CRC(p)) \oplus RC4(IV|K) \\ &= ((p' \oplus p)|(CRC(p') \oplus CRC(p))) \oplus RC4(IV|K) \\ &= ((p' \oplus p)|(CRC(p' \oplus p))) \oplus RC4(IV|K)\end{aligned}$$

- Scegliendo opportunamente  $p'$  l'attaccante manda ciò che vuole



L'injection è ancora piú facile.

- Come visto nell'autenticazione, l'attaccante può conoscere un  $RC4(IV|K)$  legittimo
- A questo punto può iniettare  $IV|m|CRC(m) \oplus RC4(IV|K)$  con  $m$  qualsiasi (gli  $IV$  possono essere riutilizzati)

# Fragmentation attack



Sicurezza delle  
reti

Monga

Problemi  
intrinseci

WEP

WPA

802.11i  
(WPA2)

I primi 8 byte dei frame 802.11b sono fissi

IP	AA AA 03 00 00 00 08 00
ARP	AA AA 03 00 00 00 08 06

L'attaccante può quindi ottenere i primi 8 byte di  $RC4(IV|K)$ . È possibile frammentare un messaggio in frammenti di 4 byte + 4 byte di integrity check e utilizzare la chiave così trovata.



Le reti wireless rendono il canale facilmente accessibile agli attaccanti: occorre usare contromisure crittografiche.

- Wired Equivalent Privacy
- Un protocollo mal progettato con innumerevoli vulnerabilità



WI-FI Protected Access (WPA) nato nel 2002 per superare WEP

- Utilizzabile sullo stesso hardware
- Superando le vulnerabilità di WEP



- Sostituisce CRC con un nuovo algoritmo per l'integrity check (Michael)
- Usa ancora RC4, ma impedisce replay e correlazioni con Temporal Key Integrity Protocol (TKIP).



Due modalità:

- Home-and-Small-Office: Pre-shared Key (PSK) analogo a WEP
- Enterprise: usa 802.1X e un authentication server connesso all'access point con una rete *wired*



- Ogni nodo (supplicant) condivide una chiave segreta con l'authentication server (Remote Authentication Dial-In User Service, RADIUS)
- L'access point riceve le richieste del nodo e le gira al RADIUS dal quale riceve l'ok all'autenticazione



## Misure di sicurezza introdotte da WPA/TKIP

- TKIP usa una *pairwise master key* (PMK) generata diversamente per ogni nodo
- la PMK viene usata per generare 4 *pairwise transient keys* (PTK) da 128 bit.
- le PTK sono diverse in ogni sessione di associazione con un AP



Le PTK vengono generate con un 4-handshake a partire da:

- un numero casuale con seme PMK
- MAC del nodo
- MAC dell'AP
- nonce generati dal nodo e dall'AP



- 2 PTK vengono usate da Michael per l'integrity check
- Michael è soggetto ad un attacco per cui bastano  $2^{29}$  (invece di  $2^{64}$ ) tentativi per falsificarlo
- perciò 2 failure escludono un nodo per un minuto



Per evitare che gli IV vengano riutilizzati, TKIP introduce i TKIP sequence counter (TSC).

- 48 bit divisi in 3 blocchi da 16 (con 24 bit, dopo 5120 trasmissioni è piú probabile avere collisioni che no)
- questo permette di riutilizzare RC4, spesso cablato nello hardware



I pacchetti che non superano l'integrity check vengono scartati;  
2 scarti portano alla dissociazione per 1 minuto.

- L'attaccante intercetta pacchetti con IV (in chiaro)
- Modifica l'IV con valori maggiori del contatore
- L'integrity check fallisce, causando DoS



WPA è un protocollo nato per superare i limiti di WEP, funzionando sui medesimi device.

- RC4 based
- Algoritmo crittografico per l'integrity check
- IV non riutilizzabili



WPA nasce “per mettere una pezza a WEP”. In realtà l’IEEE stava elaborando uno standard di sicurezza che è stato completato solo nel 2004

- 802.11i
- Wi-Fi Alliance ha prodotto uno standard compatibile con 802.11i chiamato WPA2



Al contrario di WPA, non permette di riutilizzare lo hardware WEP.

- Crittografia basata su AES
- Autenticazione PSK o 802.1X (come WPA)
- Counter mode-CRC MAC Protocol (CCMP) usa AES-128 in counter mode per autenticazione, confidenzialità e integrità: senza IV in chiaro



Il counter mode AES permette di trasformare un block cipher in uno stream cipher usando valori successivi di un “counter”: il messaggio  $M$  viene spezzato in blocchi di 128 bit

$$C_i = AES_K(i) \oplus M_i$$

CCMP inoltre (per questo servono 2 PTK) usa il cipher-block chaining message authentication code (CBC-MAC) in cui ogni blocco dipende dalla corretta cifratura del precedente.



CCMP è ritenuto piuttosto sicuro, ma rimangono alcune vulnerabilità generali

- DoS
- Attacchi rollback
- Dissociazioni e de-autenticazioni



Un attaccante può forzare una dissociazione allo scopo di:

- tentare un attacco di rollback
- intercettare i pacchetti utilizzati durante l'autenticazione (per esempio per tentare un dictionary attack)



WPA2 è un protocollo correntemente considerato sicuro (specie nella forma 802.1X)

- Basato su AES-128 (CCMP)
- Rimangono alcuni problemi intrinseci (DoS)
- Nel caso PSK: i dictionary attack