



Sicurezza dei sistemi e delle reti¹

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2013/14



WPA

802.11i
(WPA2)

Wireless
Sensor
Network

Secure data
aggregation
Secure
localization

Lezione XX: WPA



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



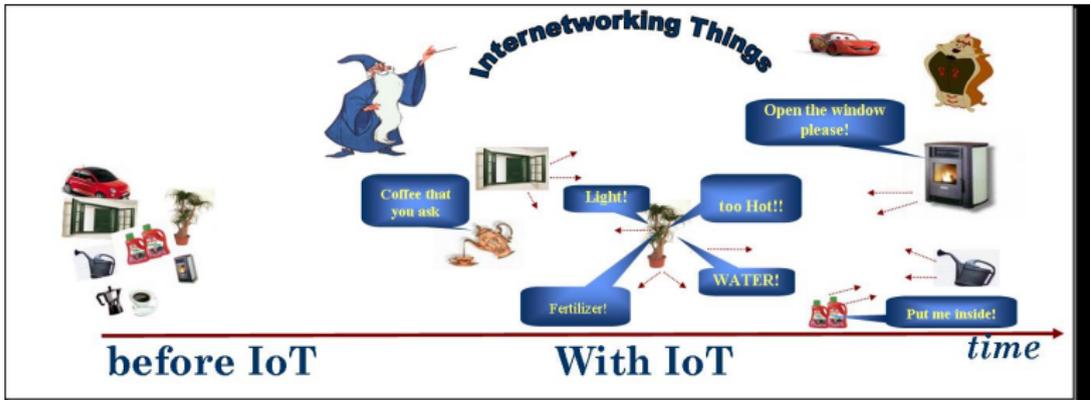
Un attaccante può forzare una dissociazione allo scopo di:

- 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



- Ogni oggetto dell'ambiente in cui siamo immersi potrebbe diventare un **nodo intelligente** di una rete di sensori.
- La realizzazione di servizi richiede lo scambio di dati e computazioni.



- Le interazioni sono spesso **decentralizzate**
- Potenza **limitata**: alimentazione, capacità di calcolo, di memorizzazione, di primitive crittografiche
- Comunicazioni wireless
- malicious displacement, impersonation, and tampering



Perché la crittografia tradizionale non è sufficiente

hop-by-hop, ma in ogni nodo è in chiaro

end-to-end, ma serve qualche segreto condiviso o crittografia
asimmetrica (generalmente considerata
irrealizzabile in WSN)

Castelluccia *et al.* [TOSN 2009]:

- end-to-end stream cipher: $C \oplus K = E \Rightarrow E \oplus K = C$
- usando *modular addition* ($+^m$) invece dello *xor*:
 $C +^m K = E \Rightarrow (E_1 + E_2) = (C_1 + C_2) +^m K$
- In questa maniera **gli aggregatori non necessitano la chiave**



Non è sempre nota a priori.

- nodi sparsi casualmente, mobili, ecc.
- in questo caso non è un dato topologico di sistema, o semplicemente *trasmesso*
- viene *calcolato* da una *base station* con le informazioni ricevuto da **nod**i **collaboranti**

WPA

802.11i
(WPA2)

Wireless
Sensor
Network

Secure data
aggregation
Secure
localization



Un protocollo di localizzazione

Multilateration

- Un certo numero di **landmark** o **ancore** v_i vengono usate per la verifica
- I landmark scambiano beacon con i nodi da localizzare e trasmettono informazioni sui **range**

Several attacks known:

Node displacement

Wormholes (fabricated communication links)

Distance enlargement (con nodi fake)

Dissemination of false position and distance information (con nodi compromessi)

Sicurezza delle
reti

Monga

WPA

802.11i
(WPA2)

Wireless
Sensor
Network

Secure data
aggregation

Secure
localization



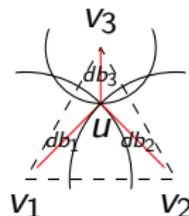
- Ogni verificatore calcola dei *distance bound* db_i rispetto a un nodo sconosciuto u
- Un attaccante che controlla **un solo nodo** può *ritardare* un beacon, ma non accelerarlo: quindi può solo apparire piú *lontano*, non piú vicino.

Čapkun *et al.* [IEEE JSACOMM 2006]

Servono almeno 3 verificatori di cui la base station (sink) si fida.

- 1 Determina u' in modo che minimizzi la somma dei delta fra i db_i e la distanza $u' - v_i$
- 2 Se la somma è maggiore dell'errore atteso \rightsquigarrow **malicious**
- 3 Altrimenti:

Se u' è contenuto in almeno un triangolo di verificatori: l'informazione è sicura, perché qualsiasi falsificazione deve accorciare un db_i





Alla fine la base station può marcare le posizioni come

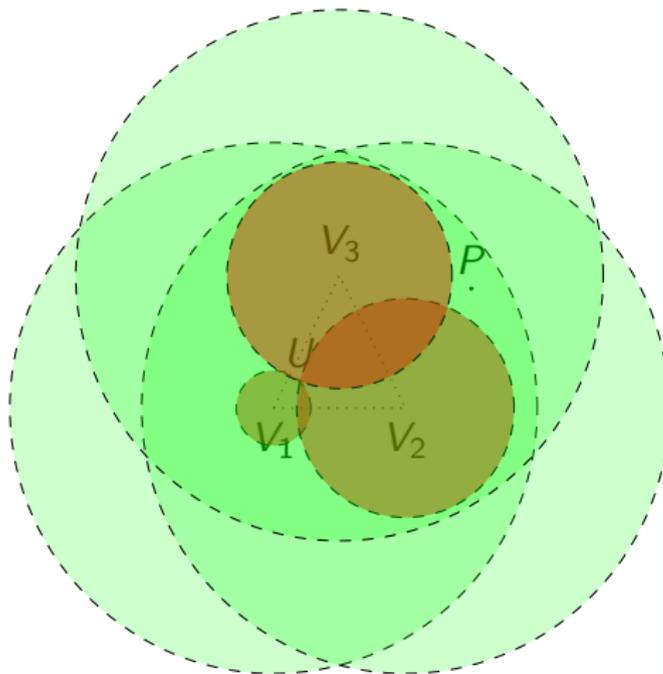
Robust almeno un triangolo di verificatori “certifica” il dato.

Malicious l'errore è troppo elevato perché sia casuale

Unknown

L'attaccante può decidere dove piazzarsi (U) e quale posizione falsificare (P)

- Senza “restringere” distanze



- Power range **green**
- Distance bound **red**

Sicurezza delle reti

Monga

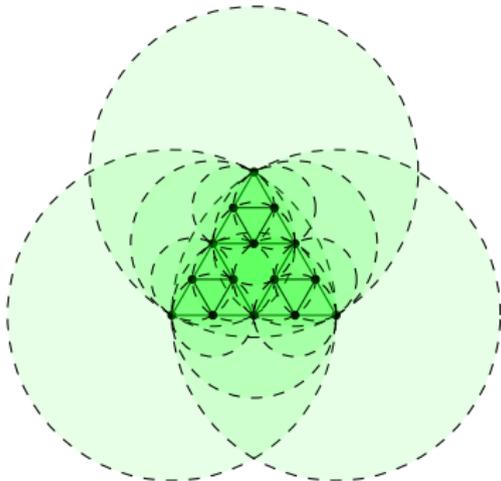
WPA

802.11i
(WPA2)

Wireless
Sensor
Network

Secure data
aggregation

Secure
localization



<i># ver.</i>	<i>max. deception</i>
3	0.2516 <i>R</i>
6	0.1258 <i>R</i>
15	0.0629 <i>R</i>
42	0.02145 <i>R</i>
123	0.015725 <i>R</i>
366	$7.8625 \cdot 10^{-3} R$