Azzolini Riccardo 2020-10-27

Sicurezza nelle reti wireless

1 Requisiti di sicurezza

Per poter essere considerato sicuro, qualunque sistema (non solo una rete wireless) deve soddisfare i seguenti requisiti:

- **Autenticazione**: bisogna essere sicuri circa l'identità degli attori della comunicazione.

  L'autenticazione può essere implementata mediante tecniche *connection-oriented* (password, challenge-response) oppure *document-oriented* (digital signature, token).

- **Confidenzialità**: le informazioni scambiate tra gli attori della comunicazione devono essere accessibili solo a tali attori.

  La confidenzialità è ottenuta mediante gli algoritmi di **encryption** (cifratura), che si suddividono in due categorie:

  - algoritmi a **chiave segreta** o **simmetrica** (ad esempio DES, 3DES, AES), in cui si criptano e decriptano le informazioni con la stessa chiave, che deve dunque essere mantenuta segreta;
  - algoritmi a **chiave pubblica** (ad esempio RSA e Diffie-Hellman), nei quali le informazioni vengono criptate con appunto una chiave pubblica, nota a tutti, e poi decriptate con una chiave diversa, detta **chiave privata** perché è nota solo al destinatario.

- **Integrità**: nessuno deve poter modificare il contenuto informativo dei messaggi inviati tra gli attori della comunicazione.

  Anche questo requisito è ottenuto per mezzo degli algoritmi di encryption (a chiave segreta o a chiave pubblica).

- **Non-repudiation**: nessun attore della comunicazione deve poter negare la "paternità" di un messaggio da esso inviato.

  Per soddisfare questo requisito si ricorre alla *digital signature*, che è essenzialmente l'uso "al contrario" di un algoritmo di encryption a chiave pubblica: il mittente cripta il messaggio con la propria chiave privata, e il destinatario lo decripta con la corrispondente chiave pubblica; se il messaggio viene decriptato correttamente, ciò significa che è stato sicuramente criptato dal mittente.

- **Autorizzazione**: un attore deve poter accedere a una risorsa solo se ha il permesso di farlo.

In realtà, è impossibile realizzare un sistema che sia del tutto sicuro: ogni contromisura che si può introdurre per prevenire determinati attacchi ha delle vulnerabilità intrinseche. Allora, un sistema si considera sicuro se le informazioni contenute al suo interno possono diventare accessibili all'esterno solo quando esse non hanno più valore.

2 Minacce alla sicurezza Wi-Fi

Una rete wireless, ad esempio Wi-Fi, ha di per sé un livello di sicurezza molto più debole rispetto a una rete wired: tutti i rischi presenti nelle reti wired valgono anche per quelle wireless, ma in più si ha anche la possibilità di effettuare attacchi "da remoto", senza bisogno di un collegamento cablato alla rete.

Alcuni degli attacchi che possono essere effettuati su una rete wireless sono:

- accessi non autorizzati;
- intercettazione di dati sensibili non criptati;
- presenza di access point non autorizzati, che potrebbero raccogliere i dati di utenti che si connettono ad essi senza verificare a quale rete si stiano realmente collegando;
- *Denial of Service* (DoS), cioè inondare la rete di traffico per renderla inutilizzabile;
- *masquerade* ("mascherarsi" dietro l'identità di un'entità autorizzata per accedere alla rete, ed eventualmente compiere atti malevoli);
- corruzione di dati sensibili (violandone l'integrità);
- violazione della privacy dei legittimi utenti e monitoraggio dei loro movimenti;
- furto di dispositivi portatili, che possono fornire informazioni sensibili;
- introduzione di virus, o in generale codice malevolo.

3 Tecniche di sicurezza

Data la vulnerabilità delle reti wireless, le problematiche relative alla sicurezza devono essere considerate sin dalla fase di progettazione, al fine di introdurre opportune contromisure, facendo un adeguato compromesso tra rischi, utilizzabilità e performance.

Per mantenere la sicurezza in una rete wireless bisogna, ad esempio:

- avere una completa conoscenza della topologia della rete, con un inventario di tutte le zone wireless e dei dispositivi mobili che vi si connettono;

- creare frequenti backup dei dati;
- eseguire periodicamente test sulla sicurezza;
- applicare patch / aggiornamenti software di sicurezza;
- monitorare l'industria/tecnologia wireless, in modo da rilevare nuovi rischi.

4 Protocollo WEP

Inizialmente, nelle reti Wi-Fi non era prevista alcuna misura di sicurezza. Il primo protocollo di sicurezza introdotto è **WEP**, **Wired Equivalent Privacy**, standardizzato nel 1999. Come indica il nome, tale protocollo aveva l'obiettivo di fornire un livello di sicurezza equivalente a quello delle reti LAN cablate, ma in realtà si è rivelato molto debole (per questo motivo, sono poi stati introdotto altri protocollo di sicurezza Wi-Fi, fino a raggiungere un livello di sicurezza accettabile).

WEP fornisce una protezione solo di tipo *point-to-point*, a livello data-link, cioè tra le stazioni (dispositivi) Wi-Fi e l'access point. Non è invece fornita alcuna protezione *end-to-end*, che comprenda la tratta di rete (cablata) tra l'access point e l'altro endpoint della comunicazione; se si vuole garantire sicurezza anche qui, bisogna impiegare altri mezzi per ottenerla.

Per l'autenticazione e la confidenzialità, WEP usa l'algoritmo di cifratura a chiave segreta **RC4** (con due chiavi, rispettivamente di 40 e 104 bit), mentre per verificare l'integrità dei dati usa una checksum **CRC-32**.

4.1 Autenticazione

Il protocollo WEP prevede tre modalità di autenticazione:

- due modalità **non-cryptographic**, che non usano algoritmi di cifratura:
  - **Closed System Authentication**, che permette a una staszione di unirsi alla rete solo se conosce l'SSID dell'access point (una stringa identificativa della BSS);
  - **Open System Authentication**, che invece accetta anche una stringa vuota come SSID (*NULL authentication*), quindi permette a qualunque stazione di connettersi;
- una modalità **cryptographic**, detta **Shared Key**, che usa RC4, permettendo a una stazione di unirsi alla rete solo se dimostra di condividere la chiave di cifratura.

L'autenticazione mediante Shared Key usa uno schema challenge-response basato sulla conoscienza, da parte del client e dell'access point, di una chiave segreta (shared secret). La procedura di challenge-response è la seguente:

1. il client (la wireless station) invia all'access point una richiesta di autenticazione;
2. l'access point risponde inviando al client una *random challenge* (in pratica un numero casuale);
3. il client cripta il challenge usando l'algoritmo RC4 con la chiave segreta, e invia il risultato all'access point;
4. l'access point decripta il messaggio, usando la stessa chiave segreta, verifica che il risultato sia uguale al challenge trasmesso inizialmente (ciò significa che la chiave usata per criptarlo era quella corretta), e in tal caso invia al client una conferma.

4.2 Confidenzialità

Anche per la confidenzialità, come per l'autenticazione, WEP usa l'algoritmo RC4.

Il **plaintext** (messaggio in chiaro) è composto dal contenuto informativo vero e proprio (*payload*) e da un checksum che serve a verificarne l'integrità. Per ottenere il **ciphertext** (messaggio criptato) da trasmettere sul canale wireless, l'algoritmo RC4 genera una sequenza di bit che dipende dalla chiave, e calcola l'OR esclusivo di tale sequenza con il plaintext.

Il destinatario, che conosce la chiave usata dal mittente, può far generare all'algoritmo RC4 la stessa sequenza di bit e metterla in OR esclusivo con il ciphertext, ottenendo così il plaintext decriptato (perché, matematicamente, fare una seconda volta l'OR esclusivo con la stessa sequenza di bit annulla l'effetto del primo OR esclusivo, dando come risultato il messaggio in chiaro originale).

4.3 Initialization Vector

Per come funziona l'algoritmo RC4, bisognerebbe assolutamente evitare che due messaggi vengano criptati con la stessa chiave, altrimenti questi risulterebbero molto facili da decriptare senza conoscere la chiave. A tale scopo, il WEP adotta un **Initialization Vector** (IV, vettore di inizializzazione), un numero a 24 bit che viene combinato con la chiave segreta, in modo da ottenere una chiave diversa per ogni pacchetto. Questo valore viene trasmesso in chiaro all'interno di ciascun pacchetto, perché il destinatario deve conoscerlo al fine di ricavare la chiave per decriptare il messaggio ricevuto.

In realtà, un Initialization Vector di 24 bit è *troppo corto*: la stessa chiave viene riutilizzata dopo un tempo relativamente breve. Ad esempio, una stazione che trasmette pacchetti

di 1500 byte ciascuno a una velocità di 11 Mbps esaurisce i 2^{24} valori dell'Initialization Vector in

$$\frac{1500 \cdot 8\,\text{bit}}{11\,\text{Mbps}} \cdot 2^{24} = \frac{12\,000\,\text{bit}}{11 \cdot 10^6\,\frac{\text{bit}}{\text{s}}} \cdot 2^{24} \approx 18\,000\,\text{s}$$

cioè circa 5 ore, dopodiché inizia a riutilizzare valori (e quindi chiavi) già usati. Così, un hacker può abbastanza facilmente trovare due messaggi criptati con la stessa chiave: in tal caso, si parla di **Initialization Vector Collision**.

Siano P_1 e P_2 due plaintext da criptare con una chiave segreta k e uno stesso valore v dell'Initialization Vector. Come detto prima, l'algoritmo RC4 funziona generando una sequenza di bit $\text{RC}(v, k)$, che dipende da v e k, e facendone l'OR esclusivo con il plaintext. Allora, i ciphertext C_1 e C_2 sono ottenuti da P_1 e P_2 come segue:

$$C_1 = P_1 \text{ XOR } \text{RC}(v, k)$$
$$C_2 = P_2 \text{ XOR } \text{RC}(v, k)$$

Un hacker in ascolto sulla rete potrebbe captare entrambi i ciphertext, e da questi, grazie alle proprietà matematiche dell'OR esclusivo, risalire a $P_1 \text{ XOR } P_2$ pur non conoscendo la chiave k:

$$\begin{aligned}
&C_1 \text{ XOR } C_2 \\
&\quad = (P_1 \text{ XOR } \text{RC}(v, k)) \text{ XOR } (P_2 \text{ XOR } \text{RC}(v, k)) && [\text{definizioni di } C_1 \text{ e } C_2] \\
&\quad = (P_1 \text{ XOR } P_2) \text{ XOR } (\text{RC}(v, k) \text{ XOR } \text{RC}(v, k)) && [\text{commutatività e associatività}] \\
&\quad = (P_1 \text{ XOR } P_2) \text{ XOR } 0 && [A \text{ XOR } A = 0] \\
&\quad = P_1 \text{ XOR } P_2 && [A \text{ XOR } 0 = A]
\end{aligned}$$

Ci sono poi delle tecniche che permettono di ricavare i singoli plaintext P_1 e P_2 da $P_1 \text{ XOR } P_2$.

4.4 Integrità

La tecnica utilizzata da WEP per cercare di garantire l'integrità delle informazioni si basa su una checksum **CRC-32**. Per ogni payload da trasmettere, viene calcolata una tale checksum, che prende il nome di *frame check sequence*, e viene inserita nel pacchetto prima che questo venga criptato. Quando il destinatario riceve un pacchetto, dopo averlo decriptato, ricalcola la checksum del payload, e verifica che questa corrisponda con quella presente nel pacchetto: se così non fosse, significherebbe che i dati trasmessi sono stati alterati, violandone l'integrità.

Il CRC-32 è però *lineare*: nonostante la cifratura con RC4, un hacker che modifica dei bit nel messaggio criptato, può "aggiustare" anche la checksum, in modo che il messaggio finale sia apparentemente corretto, e può fare ciò senza bisogno di conoscere la chiave di cifratura.

4.5 Limiti di sicurezza del WEP

Il WEP ha numerose debolezze / vulnerabilità:

- L'autenticazione non è efficace:
  - L'autenticazione non-cryptographic, anche Closed System, non fornisce alcun livello di sicurezza, poiché si basa solo sulla conoscenza dell'SSID (senza richiedere invece una password/chiave), ma ogni access point, per annunciare la sua presenza, trasmette in broadcast delle **beacon frame** che contengono in chiaro il suo SSID, quindi chiunque può conoscerlo e dunque accedere alla rete.
  - Non si verifica l'identità del client (solo che esso conosca la chiave segreta), né quella dell'access point (non si ha una *two-way authentication*).
  - Si usa la stessa chiave per l'autenticazione Shared Key e per le operazioni di cifratura finalizzate alla confidenzialità.
  - Sono possibili attacchi *man-in-the-middle* (un attore malevolo si mette "in mezzo" ai due legittimi attori della comunicazione, facendo a loro insaputa da tramite per i messaggi che questi si scambiano, in modo da poterli leggere ed eventualmente alterare).
- Si ha un basso livello di confidenzialità:
  - Si possono inserire access point non autorizzati.
  - La natura broadcast del traffico wireless permette a un hacker di raccogliere i pacchetti trasmessi per eseguire un attacco di Initialization Vector Collision.
  - Le chiavi crittografiche sono corte (40 o 104 bit) e condivise (quindi ci sono tanti utenti che ne sono a conoscenza, aumentando la probabilità che queste vengano compromesse), e non possono essere aggiornate automaticamente e frequentemente.
- L'integrità dei pacchetti è garantita in modo superficiale, a causa della linearità della checksum CRC-32 utilizzata a tale scopo.
- Si ha un basso livello di *availability*, cioè è facile effettuare attacchi Denial of Service, che compromettano l'usabilità della rete.

  Un particolare tipo tipo di DoS che può essere eseguito in una rete wireless è il *jamming*: un utente malevolo trasmettere deliberatamente un segnale che interferisce con i segnali wireless legittimi, causando la caduta delle connessioni alla rete.

Un'altra possibilità è che un utente non malevolo provochi accidentalmente un DoS, ad esempio effettuando il download di file di grandi dimensioni: ciò terrebbe occupata per molto tempo la rete, negando l'accesso ad altri utenti.