Azzolini Riccardo 2020-10-29

Sicurezza nelle reti wireless

1 Mitigazione del rischio

Prima di mettere in sicurezza un sistema, bisogna effettuare un'analisi dei rischi, individuando le vulnerabilità del sistema, le dipendenze / relazioni reciproche tra tali vulnerabilità, e la loro *expoiltability* (possibilità di sfruttarle concretamente per compiere attacchi sul sistema). Solo a questo punto si introducono le opportune contromisure, che possono essere suddivise in:

- *management countermeasures* (contromisure gestionali);
- *operational countermeasures* (contromisure operative);
- *technical countermeasures* (contromisure tecniche).

Ad esempio, nell'ambito di una LAN wireless (WLAN), le principali contromisure per ciascuna di queste categorie sono:

- Management countermeasures:
  - identificare chi nell'organizzazione può utilizzare la WLAN;
  - identificare ogni accesso a Internet richiesto;
  - descrivere chi può installare gli access point e gli altri dispositivi wireless;
  - fornire delle limitazioni sulla localizzazione degli access point;
  - descrivere il tipo di informazione che può essere inviata su un link wireless;
  - definire impostazioni di sicurezza standard per gli access point;
  - descrivere la configurazione hardware e software di ogni dispositivo;
  - fornire delle linee guida sull'uso delle tecniche di cifratura e di altri software di sicurezza;
  - definire la frequenza degli interventi rivolti al testing della sicurezza.
- Operational countermeasures:
  - controllo di accesso (per mezzo di identificazione tramite foto, lettori di badge e/o dispositivi biometrici);
  - protezione del perimetro esterno tramite videocamere.

- Technical countermeasures: comprendono soluzioni software e hardware.
  - Soluzioni software:
    * configurazione degli access point;
    * patch e aggiornamenti software;
    * autenticazione (mediante username e password, smart card, biometria, Public Key Infrastructure, o una combinazione delle precedenti);
    * firewall;
    * Intrusion Detection System;
    * encryption.
  - Soluzioni hardware:
    * smart card;
    * VPN;
    * Public Key Infrastructure;
    * biometria.

1.1 Configurazione degli access point

La configurazione degli access point deve comprendere:

- il cambiamento dei parametri di default, tra cui in particolare l'SSID e la chiave/password di accesso;
- il controllo della funzione di reset;
- l'utilizzo della funzionalità MAC ACL per permettere la connessione solo a dispositivi conosciuti;
- l'utilizzo del DHCP.

1.2 VPN

Una *VPN* (*Virtual Private Network*) fornisce un accesso remoto sicuro a una LAN, tipicamente di una sede aziendale, permettendo a utenti remoti o altre sedi di usufruire di tale rete privata, come se ne facessero direttamente parte.

Essa si basa tipicamente su un meccanismo di *IP tunneling*, cioè inserimento di un pacchetto IP dentro un altro pacchetto IP, usando *IPSec* (che impiega opportune tecniche crittografiche) per garantire confidenzialità, integrità, autenticazione, ecc.

Lo svantaggio di una VPN è che non è una soluzione "self-managing", "plug-and-play", poiché richiede una configurazione manuale.

2 Successivi standard di sicurezza Wi-Fi

Dopo il WEP, che come visto aveva numerose debolezze, sono stati definiti diversi altri standard di sicurezza, che hanno risolto in modo incrementale tutte queste vulnerabilità. Tali standard sono WEP 2, IEEE 802.1X, IEEE 802.11i e WPA.

2.1 WEP 2

La seconda versione di WEP aveva l'obiettivo di superare i problemi presenti nella prima versione, ma in pratica tale obiettivo non fu affatto raggiunto.

La principale novità di WEP 2 è l'aumento della lunghezza della chiave, da 40/104 bit a 128 bit. Se da un lato ciò risolve il problema che le chiavi fossero troppo corte, dall'altro non cambia il fatto che le chiavi fossero statiche, dunque rimane la possibilità di attacchi Initialization Vector Collision. Inoltre, non viene affrontata la problematica della mancanza di autenticazione degli access point, quindi è ancora possibile che i client si associno ad access point non autorizzati.

2.2 IEEE 802.1X

Lo standard IEEE 802.1X definisce un generico framework di controllo di accesso basato su **EAP**, **Extensible Authentication Protocol**.

Questo standard realizza una mutua autenticazione tra il client e l'access point, consultando un apposito server di autenticazione *RADIUS* o *Kerberos*. Si evita così la presenza di access point non autorizzati ("rogue access point").

Inoltre, è consentita una generazione e distribuzione dinamica delle chiavi.

2.3 IEEE 802.11i

Lo standard IEEE 802.11i include lo schema di autenticazione EAP definito da 802.1X.

Inoltre, l'algoritmo di cifratura RC4 usato nel WEP viene sostituito con **AES** (*Advanced Encryption Standard*), un algoritmo più robusto che usa chiavi a 128, 192 o 256 bit (ed è l'algoritmo adottato come standard, ad esempio, dal governo degli Stati Uniti).

Infine, viene introdotto il **TKIP**, **Temporal Key Integrity Protocol**, che risolve il problema dell'Initialization Vector: a partire dalla **master key** (la chiave segreta statica), esso generando in dinamicamente diverse chiavi a 128 bit, chiamate **temporal key**, così che una stessa chiave non venga mai utilizzata due volte. I cambiamenti di chiave avvengono automaticamente in background, in modo trasparente all'utente.

L'uso di chiavi dinamiche tramite TKIP rende impossibili gli attacchi Initialization Vector Collision, e risolve anche il problema dell'impiego della stessa chiave per l'autenticazione e l'encryption (un altro dei problemi del WEP).

2.4 Wi-Fi Protected Access

WPA (**Wi-Fi Protected Access**) è uno standard derivata da 802.11i, che come quest'ultimo include 802.1X e TKIP. L'autenticazione EAP viene usata per le reti Enterprise, mentre vengono introdotte altre modalità di autenticazione per applicazioni "Small Office / Home Office" (SOHO) e Public Access.

WPA per SOHO è finalizzato all'uso in reti nelle quali non è disponibile un server di autenticazione centrale, come abitazioni e piccoli uffici. Invece dell'autenticazione EAP, esso lavora utilizzando una **pre-shared key**, cioè una chiave distribuita prima che il sistema inizi a lavorare. Questa chiave viene usata direttamente solo nella fase iniziale di autenticazione (quando l'utente la inserisce per connettersi alla rete), dopodiché TKIP deriva dinamicamente da essa le chiavi per le operazioni di encryption.

Invece, WPA per Public Access è pensato per gli "hot spot" Wi-Fi pubblici.