Internet Security

Con la diffusione di Internet, la sicurezza delle informazioni è diventata una questione fondamentale. È essenziale proteggere i dati sia a livello fisico che durante la loro trasmissione da un nodo all'altro. Per garantire questa protezione, sono state sviluppate diverse misure di sicurezza, note complessivamente come Internet Security.

Alla base dell'Internet Security vi è la Raccomandazione X.800, che definisce un insieme di requisiti di sicurezza che ogni sistema deve soddisfare:

- Autenticazione: assicurare l'identità dei soggetti coinvolti nella trasmissione
- Controllo degli Accessi: proibizione dell'uso di una risorsa da parte di soggetti non autorizzati
- Confidenzialità: protezione della riservatezza dei dati, poiché nessun soggetto terzo vi deve accedere durante la trasmissione
- Integrità: certezza che i dati non siano stati alterati da soggetti non autorizzati
- Non ripudiabilità: protezione contro la negazione di un soggetto coinvolto nella trasmissione

La strategie di sicurezza principali nella trasmissione dei dati si incentrano o sull'oscurazione o sul confinamento. Qualsiasi sia quella adottata, nella progettazione del servizio di sicurezza si deve:

1. Utilizzare un algoritmo per trasformare i dati in chiaro in dati crittografati
2. Generare le chiavi da utilizzare per crittografare e decrittografare
3. Sviluppare un metodo per la condivisione sicura delle chiavi
4. Specificare un protocollo che permetta di utilizzare sia l'algoritmo che le chiavi in modo sicuro

La Crittografia

La crittografia è l'insieme di tutte le procedure che hanno lo scopo di nascondere il significato di un messaggio tranne che al legittimo destinatario. Alla base vi è un cifrario, che ci permette di trasformare ogni carattere del testo in chiaro. Per cifrare un testo occorrono un algoritmo di cifratura e una chiave per decifrarlo.

Uno dei cardini della teoria della crittografia è il principio di Kerckhoffs, secondo il quale la sicurezza di un sistema crittografico è basata esclusivamente sulla conoscenza della chiave.

Esistono molti sistemi di crittografia, si possono classificare in vario modo:

1. Tipo di operazioni usate per cifrare il testo:
   - Crittografia a sostituzione
   - Crittografia a trasposizione
2. Modo in cui il testo in chiaro viene elaborato:
   - Crittografia a blocchi
   - Crittografia a flusso
3. Numero di chiavi distinte utilizzate:
   - Crittografia a chiave simmetrica
   - Crittografia a chiave asimmetrica

Crittografia Simmetrica e Asimmetrica

La crittografia a chiave simmetrica si basa sull'utilizzo di una sola chiave usata sia per cifrare che per decifrare. La crittografia a chiave asimmetrica utilizza due chiavi per ciascun soggetto, una privata e una pubblica.

A seconda dell'uso delle chiavi:

- Confidenzialità: viene utilizzata la coppia di chiavi del destinatario
- Autenticazione: viene utilizzata solo la coppia di chiavi del mittente
- Tutte: utilizzando entrambe le coppie di chiavi

Le due chiavi devono essere matematicamente correlate ma non ricavabili l'una dall'altra.

Gli Algoritmi DES e Triple DES

Il DES (Data Encryption Standard) è un algoritmo sviluppato negli anni '70 e basato su:

- Confusion: rende confusa la relazione tra testo in chiaro e testo cifrato
- Diffusion: altera la struttura del testo in chiaro

Funzionamento:

- Input: blocchi da 64 bit, chiave a 56 bit
- Permutazione iniziale
- Suddivisione in due semiblocchi da 32 bit (L_0, R_0)
- Generazione di 16 chiavi da 48 bit
- Operazioni di espansione, XOR, compressione con S-box
- Permutazione finale
- Inversione dei semiblocchi e decrittazione simmetrica (DES^{-1})

Triple DES:

- Applica il DES tre volte con tre chiavi diverse (Crypt → Decrypt → Crypt)
- Usa chiavi da 192 bit (128 effettivi)

Altri algoritmi derivati:

- IDEA: blocchi da 64 bit, chiave da 128
- AES: blocchi da 128 bit, chiavi da 128, 192, 256
- CAST: blocchi da 64 o 128 bit, chiavi da 128 o 256

L'algoritmo RSA

RSA è un algoritmo a chiave pubblica, sicuro grazie alla difficoltà della fattorizzazione.

Generazione chiavi:

- Scegliere p e q
- Calcolare n = p × q e φ(n) = (p − 1)(q − 1)
- Scegliere e coprimo con φ(n)
- Calcolare d tale che d × e ≡ 1 mod φ(n)
- Pubblica: (e, n), Privata: (d, n)

Crittografia:

- c = m^e mod n

Decrittografia:

- m = c^d mod n

RSA è sicuro ma lento. Oggi è usato soprattutto per lo scambio della chiave simmetrica.

La Firma Digitale e gli Enti Certificatori

La firma digitale ha valore legale e si basa su un sistema a chiavi asimmetriche. Per garantire l'identità del firmatario intervengono i certificatori, che rilasciano un certificato digitale.

Formati riconosciuti:

- pkcs#7 (p7m): usato dalla PA
- PDF: accordo Adobe–CNIPA del 2006 (RFC 3778)
- XML: molto usato in ambito bancario e sanitario

Il processo di firma digitale:

- Si crea un'impronta (message digest) con una funzione di hash
- Si firma questa impronta con la chiave privata del mittente

Per firmare serve un kit composto da:

- Dispositivo sicuro

- Software di firma