1. Fondamenti della Sicurezza Informatica

1.1 Concetti Base e Obiettivi

La sicurezza informatica mira a proteggere i sistemi informatici e le informazioni da minacce e accessi non autorizzati. I pilastri fondamentali sono:

La riservatezza garantisce che le informazioni siano accessibili solo a chi ne ha diritto. Questo principio viene implementato attraverso meccanismi di controllo degli accessi e crittografia, assicurando che anche se i dati vengono intercettati, rimangano incomprensibili a chi non possiede le chiavi appropriate.

L'integrità assicura che le informazioni non vengano alterate in modo non autorizzato. Questo obiettivo viene raggiunto attraverso l'uso di funzioni di hash crittografiche e firme digitali, che permettono di rilevare qualsiasi modifica ai dati originali.

La disponibilità garantisce che le risorse e le informazioni siano accessibili quando necessario. Questo aspetto richiede sistemi ridondanti, backup regolari e meccanismi di difesa contro attacchi di tipo Denial of Service (DoS).

1.2 Minacce e Vulnerabilità

Le minacce alla sicurezza informatica possono essere classificate in:

Minacce passive, come l'intercettazione di comunicazioni, che non modificano i dati ma compromettono la riservatezza. Queste minacce sono particolarmente insidiose perché spesso difficili da rilevare.

Minacce attive, come la modifica di dati o l'inserimento di codice malevolo, che alterano attivamente il sistema o le informazioni. Queste minacce possono compromettere sia l'integrità che la disponibilità dei sistemi.

Minacce interne, provenienti da utenti autorizzati che abusano dei loro privilegi. Questa categoria è particolarmente pericolosa perché gli attaccanti hanno già accesso legittimo al sistema.

2. Crittografia

2.1 Fondamenti Teorici

La crittografia moderna si basa su solidi principi matematici e teorici. Il Principio di Kerckhoffs stabilisce che la sicurezza di un sistema crittografico deve dipendere esclusivamente dalla segretezza della chiave, non dall'algoritmo stesso. Questo principio è fondamentale perché:

- Permette la valutazione pubblica degli algoritmi
- Facilita la standardizzazione dei sistemi di sicurezza
- Riduce i costi di implementazione e manutenzione
- Aumenta la fiducia nella sicurezza del sistema

La complessità computazionale è un altro concetto fondamentale. Un sistema crittografico è considerato sicuro se il tempo necessario per forzarlo con i migliori algoritmi conosciuti è praticamente proibitivo.

2.2 Crittografia Simmetrica

La crittografia simmetrica utilizza la stessa chiave per cifrare e decifrare. Questa approccio offre:

Velocità di elaborazione elevata, rendendola ideale per la cifratura di grandi quantità di dati. Gli algoritmi simmetrici sono tipicamente 1000-10000 volte più veloci di quelli asimmetrici.

Sicurezza provata matematicamente quando implementata correttamente. La sicurezza dipende dalla lunghezza della chiave e dalla qualità dell'algoritmo.

2.2.1 Algoritmi Principali

DES (Data Encryption Standard) è stato il primo standard di cifratura largamente adottato. Utilizza:

- Blocchi di 64 bit
- Chiave effettiva di 56 bit
- 16 round di cifratura
- Rete di Feistel per la struttura interna

3DES (Triple DES) è un'evoluzione del DES che applica l'algoritmo tre volte con chiavi diverse:

- Chiave totale di 168 bit
- Maggiore sicurezza del DES
- Compatibilità con sistemi esistenti
- Più lento del DES singolo

AES (Advanced Encryption Standard) è lo standard attuale:

- Blocchi di 128 bit
- Chiavi di 128, 192 o 256 bit
- Struttura a matrice di stati
- Ottimizzato per implementazioni hardware e software

2.3 Crittografia Asimmetrica

La crittografia asimmetrica utilizza coppie di chiavi matematicamente correlate. Ogni utente possiede:

- Una chiave pubblica per la cifratura
- Una chiave privata per la decifratura

2.3.1 RSA

RSA è l'algoritmo asimmetrico più diffuso. Il suo funzionamento si basa su:

La difficoltà di fattorizzare il prodotto di due numeri primi grandi. Questo problema matematico è considerato computazionalmente intrattabile per numeri sufficientemente grandi.

La generazione delle chiavi avviene attraverso i seguenti passi:

1. Scelta di due numeri primi grandi p e q
2. Calcolo di n = p × q
3. Calcolo di φ(n) = (p-1) × (q-1)
4. Scelta di e coprimo con φ(n)
5. Calcolo di d tale che (e × d) mod φ(n) = 1

Le operazioni di cifratura/decifratura utilizzano:

- Cifratura: C = M^e mod n
- Decifratura: M = C^d mod n

2.3.2 Altri Algoritmi Asimmetrici

ECC (Elliptic Curve Cryptography):

- Basato su curve ellittiche su campi finiti
- Chiavi più corte per la stessa sicurezza di RSA
- Più efficiente in termini di risorse
- Ideale per dispositivi mobili e IoT

El Gamal:

- Basato sul problema del logaritmo discreto
- Utilizzato principalmente per firma digitale
- Permette cifratura probabilistica

2.4 Funzioni di Hash Crittografiche

Le funzioni di hash sono fondamentali per:

- Verifica dell'integrità dei dati
- Firme digitali
- Memorizzazione sicura delle password

Caratteristiche essenziali:

- Resistenza alla preimmagine
- Resistenza alla seconda preimmagine
- Resistenza alle collisioni

Algoritmi principali:

- MD5 (considerato non sicuro)
- SHA-1 (obsoleto)
- SHA-2 e SHA-3 (standard attuali)

3. Sicurezza delle Reti

3.1 Firewall

Un firewall è un sistema di sicurezza che controlla il traffico di rete secondo regole predefinite. La sua efficacia dipende da:

Posizionamento strategico nella rete:

- Perimetrale per protezione da Internet
- Interno per segmentazione della rete
- DMZ per servizi pubblici

Politiche di sicurezza appropriate:

- Default deny per massima sicurezza
- Regole specifiche per servizi necessari
- Logging e monitoraggio

3.1.1 Tipologie di Firewall

Packet Filter:

- Analisi a livello di rete e trasporto
- Veloce ed efficiente
- Limitato nell'ispezione del contenuto
- Ideale per filtraggio base

Application Layer:

- Analisi completa del traffico applicativo
- Supporto per autenticazione
- Capacità di caching e ottimizzazione
- Maggior impatto sulle prestazioni

Stateful Inspection:

- Mantiene stato delle connessioni
- Decisioni basate sul contesto
- Miglior compromesso prestazioni/sicurezza

3.2 NAT (Network Address Translation)

Il NAT è una tecnologia fondamentale per:

- Conservazione indirizzi IP pubblici
- Nascondere la struttura interna della rete
- Facilitare il routing tra reti private

3.2.1 Varianti NAT

Static NAT:

- Mappatura 1:1 tra indirizzi
- Utilizzato per servizi pubblici
- Configurazione manuale
- Maggior controllo

Dynamic NAT:

- Pool di indirizzi pubblici
- Assegnazione automatica
- Più flessibile
- Gestione automatica delle connessioni

PAT (Port Address Translation):

- Multiplazione delle connessioni
- Massimo risparmio di indirizzi pubblici
- Gestione complessa dei protocolli

3.2.2 Tecniche Avanzate

Port Forwarding:

- Redirezione selettiva delle porte
- Accesso a servizi interni
- Configurazione per servizio
- Gestione rischi di sicurezza

Port Triggering:

- Apertura dinamica delle porte
- Basato sul traffico uscente
- Utile per applicazioni complesse
- Maggior sicurezza del port forwarding

3.3 VPN (Virtual Private Network)

Le VPN creano tunnel sicuri attraverso reti non fidate:

- Cifratura del traffico
- Autenticazione degli endpoint
- Tunneling dei protocolli
- Politiche di routing

3.3.1 Protocolli VPN

IPSec:

- Sicurezza a livello IP
- Supporto modalità trasporto e tunnel
- Forte sicurezza
- Complesso da configurare

SSL/TLS:

- Sicurezza a livello applicativo
- Più semplice da implementare
- Attraversamento NAT facilitato
- Supporto web nativo

3.3.2 Architetture VPN

Site-to-Site:

- Connessione tra sedi remote
- Configurazione permanente
- Alta affidabilità
- Gestione centralizzata

Remote Access:

- Accesso utenti mobili
- Configurazione dinamica
- Integrazione con autenticazione
- Supporto per diverse piattaforme

3.4 Sicurezza Wireless

3.4.1 Bluetooth

Architettura di sicurezza:

- Frequency Hopping per resistenza alle interferenze
- Autenticazione dispositivi
- Cifratura del canale
- Gestione chiavi

Livelli di sicurezza:
6. Non sicuro
7. Sicurezza a livello servizio
8. Sicurezza a livello link

Vulnerabilità:

- Bluejacking
- Bluesnarfing
- Man-in-the-Middle
- Jamming

3.4.2 Wi-Fi

Standard di sicurezza:

- WEP (obsoleto)
- WPA/WPA2 (PSK e Enterprise)
- WPA3 (ultimo standard)

Meccanismi di protezione:

- Autenticazione
- Cifratura
- Gestione chiavi
- Protezione integrità

4. Gestione della Sicurezza

4.1 Politiche di Sicurezza

Una politica di sicurezza efficace deve includere:

- Definizione degli obiettivi
- Assegnazione delle responsabilità
- Procedure operative
- Gestione degli incidenti
- Formazione degli utenti

4.2 Monitoraggio e Controllo

Il monitoraggio continuo richiede:

- Sistemi di logging
- Analisi del traffico
- Rilevamento intrusioni
- Gestione degli alert
- Procedure di risposta

4.3 Disaster Recovery

Un piano di disaster recovery deve prevedere:

- Backup regolari
- Siti alternativi
- Procedure di ripristino
- Test periodici
- Documentazione aggiornata