1. Fondamenti della Sicurezza Informatica

1.1 Concetti Base e Obiettivi

1. **Riservatezza**
   Garantisce che le informazioni siano accessibili esclusivamente a soggetti autorizzati. Si implementa tramite controlli di accesso e tecniche crittografiche, in modo che anche in caso di intercettazione i dati rimangano illeggibili.
2. **Integrità**
   Assicura che le informazioni non subiscano modifiche non autorizzate. Si usano funzioni hash e firme digitali per verificare che il contenuto rimanga invariato.
3. **Disponibilità**
   Garantisce che le risorse siano sempre accessibili agli utenti autorizzati, mediante sistemi ridondanti, backup regolari e difese contro attacchi DoS.

(Approfondimenti e definizioni in □cite□turn1file0□)

1.2 Minacce e Vulnerabilità

1. **Minacce Passive**
   Intercettazioni che non alterano i dati, difficili da rilevare.
2. **Minacce Attive**
   Modifiche o inserimenti di codice malevolo, che compromettono integrità e disponibilità.
3. **Minacce Interne**
   Attacchi da utenti autorizzati che abusano dei propri privilegi.

---

2. Crittografia

2.1 Fondamenti Teorici

1. **Principio di Kerckhoffs**
   La sicurezza si basa solo sulla segretezza della chiave, non sull'algoritmo, il quale è pubblico.
   (Vedi □cite□turn1file0□)
2. **Complessità Computazionale**
   Un sistema è sicuro se il tempo necessario per forzarlo è proibitivo.

2.2 Crittografia Simmetrica

1. **Definizione**
   Utilizza una singola chiave per cifrare e decifrare i dati; è molto veloce e la sicurezza dipende dalla chiave.
2. **Algoritmi Principali**
   - **DES (Data Encryption Standard):**
     Opera su blocchi di 64 bit con una chiave effettiva di 56 bit e utilizza 16 round di trasformazioni (permuta, espansione, sostituzione tramite S-box e XOR) secondo la struttura a rete di Feistel.
     (In sintesi, DES trasforma il testo in chiaro con una serie di operazioni fisse che "mescolano" i bit, rendendo difficile il recupero del messaggio originale senza la chiave.)
   - **Triple DES (3DES):**
     Migliora la sicurezza applicando il DES in cascata in modalità EDE (Encrypt–Decrypt–Encrypt) con due o tre chiavi. In pratica, il testo viene cifrato, poi decifrato e infine nuovamente cifrato, aumentando la complessità senza cambiare radicalmente la struttura di DES.
     (Riassumendo, 3DES "triplica" la sicurezza di DES, pur comportando un maggior impegno computazionale.)
   - **AES (Advanced Encryption Standard):**
     Opera su blocchi di 128 bit e supporta chiavi di 128, 192 o 256 bit, ma in questa guida non ne approfondiremo il funzionamento.

2.3 Crittografia Asimmetrica

1. **Definizione**
   Usa una coppia di chiavi correlate: la chiave pubblica, diffusa liberamente, e la chiave privata, mantenuta segreta.
2. **Algoritmo RSA**
   - **Generazione:** Scegli due grandi numeri primi p e q, calcola n = p×q e φ(n); seleziona un esponente e (coprimo con φ(n)) e calcola d tale che (e×d) mod φ(n) = 1.
   - **Operazioni:**
     - Cifratura: C = M^e mod n
     - Decifratura: M = C^d mod n

(Dettagli in □cite□turn1file0□)

1. **Altri Algoritmi**
   - **ECC:** Offre sicurezza simile a RSA con chiavi più corte, ideale per dispositivi con risorse limitate.
   - **El Gamal:** Basato sul logaritmo discreto, usato per firme digitali e cifratura probabilistica.

2.4 Funzioni di Hash Crittografiche

1. **Scopi:**
   Verifica integrità, supporto per firme digitali e memorizzazione sicura delle password.
2. **Caratteristiche:**
   - Resistenza alla preimmagine, alla seconda preimmagine e alle collisioni.
3. **Algoritmi:**
   - **MD5:**
     Funziona paddeando il messaggio fino a raggiungere una lunghezza multipla di 512 bit, aggiungendo la lunghezza originale, inizializzando registri con valori fissi e processando il messaggio in blocchi con operazioni non lineari, rotazioni e XOR, producendo un digest a 128 bit.
     (In breve, MD5 trasforma il messaggio in un "riassunto" fisso di 128 bit, anche se oggi non è considerato sicuro.)
   - **SHA:**
     (Es. SHA-1) Il messaggio viene paddato e diviso in blocchi di 512 bit, processato in 80 round di operazioni (rotazioni, somme e funzioni non lineari) con cinque registri inizializzati, producendo un hash a 160 bit.
     (Sinteticamente, SHA genera un digest che "riassume" il messaggio e offre resistenza alle modifiche, sebbene SHA-1 sia ora considerato obsoleto.)

---

3. Sicurezza delle Reti

3.1 Firewall

1. **Definizione e Funzioni**
   Controlla il traffico tra interfacce, filtrando i pacchetti in base a regole predefinite.
   - Può essere hardware o software e opera a vari livelli dello stack (dal fisico all'applicativo).
2. **Tipologie:**
   - **Packet Filter:** Analizza singoli pacchetti (stateless).
   - **Proxy Server:** Filtra a livello applicativo, con caching e analisi del contenuto.
   - **Firewall Stateful:** Considera lo stato della comunicazione per un filtraggio più accurato.

(Dettagli in □cite□turn1file3□)

3.2 NAT e PAT

1. **NAT:**
   Traduce indirizzi IP interni in pubblici, permettendo a reti private di accedere a Internet.
2. **PAT:**
   Modifica le porte per gestire più connessioni con un singolo IP pubblico.

3.3 Sicurezza Wireless

1. **Bluetooth:**

```
- Utilizza Frequency Hopping Spread Spectrum e Time Division Duplexing.
- Forma piconet (fino a 8 dispositivi) e, eventualmente, scatternet per coperture estese.
- Distinzione tra link SCO (point-to-point) e ACL (broadcast).
```

_
2. **Wi-Fi:**
   Breve menzione degli standard di sicurezza (WEP, WPA/WPA2, WPA3) e dei meccanismi di autenticazione e cifratura.

---

4. Gestione della Sicurezza

4.1 Politiche di Sicurezza

1. **Obiettivi e Modelli:**
   Definiscono regole e procedure per confinare gli utenti e proteggere le risorse.
   - Si basano su modelli come AAA (Authentication, Authorization, Auditing) e su sistemi di controllo accessi DAC e MAC.
2. **Implementazione:**
   - **DAC:** Gli utenti gestiscono autonomamente i diritti.
   - **MAC:** Restrizioni impostate dall'amministratore, ideali in ambienti ad alta sicurezza.
   - **MAC+DAC:** Combina flessibilità e restrizione per isolare le risorse.

4.2 Monitoraggio e Controllo

1. **Logging e Auditing:**
   Registrazione degli eventi di autenticazione, accesso e operazioni, con vari livelli di dettaglio.
2. **Strumenti di Monitoraggio:**
   Software e dispositivi che analizzano il traffico di rete per rilevare anomalie.

4.3 Disaster Recovery

1. **Backup e Ripristino:**
   Strategie di backup regolari e procedure di ripristino per garantire continuità operativa.
2. **Piani di Contingenza:**
   Definizione di procedure e sedi alternative, con test periodici per verificarne l'efficacia.