1. Sicurezza Wireless

La sicurezza nelle reti wireless è fondamentale poiché la trasmissione in aria rende i dati potenzialmente accessibili a chiunque si trovi nel raggio di copertura.

1.1 WEP (Wired Equivalent Privacy)

- **Introduzione**: Primo protocollo di sicurezza per 802.11 (1999)
- **Meccanismo**: Utilizza algoritmo RC4 con chiavi da 64 o 128 bit
- **Problemi critici**:
  - Vettore di inizializzazione (IV) troppo corto (24 bit)
  - Riutilizzo di chiavi
  - Autenticazione debole
  - Metodo di gestione delle chiavi inadeguato
  - CRC-32 non crittografico per l'integrità

1.1.1 Vulnerabilità

- Collisioni degli IV (dopo circa 5000 pacchetti)
- Attacchi statistici (FMS/KoreK)
- Possibile decifrazione completa in pochi minuti
- WEP è considerato completamente insicuro oggi
- Non deve essere mai utilizzato in ambienti di produzione

1.1.2 Funzionamento

1. L'access point e il client condividono una chiave segreta
2. Viene generato un IV casuale
3. IV + chiave segreta formano la chiave di cifratura
4. RC4 genera uno stream di chiavi basato sulla chiave di cifratura
5. I dati vengono cifrati con XOR tra dati e stream di chiavi
6. Il pacchetto inviato contiene IV in chiaro + dati cifrati

1.2 WPA (Wi-Fi Protected Access)

- **Introduzione**: Soluzione intermedia introdotta nel 2003 dopo i problemi di WEP
- **Meccanismo**: Usa TKIP (Temporal Key Integrity Protocol) basato ancora su RC4

1.2.1 Miglioramenti rispetto a WEP

- IV più lungo (48 bit)

- Mixing function per le chiavi
- Message Integrity Check (MIC) con algoritmo Michael
- Distribuzione chiavi dinamica (chiavi cambiate periodicamente)
- Contromisure attive contro attacchi

1.2.2 Modalità operative

- **WPA-Personal (WPA-PSK)**:
  - Usa passphrase condivisa
  - Adatto per piccole reti
  - Vulnerabile ad attacchi di dizionario sulla passphrase
- **WPA-Enterprise**:
  - Autenticazione basata su server RADIUS e 802.1X
  - Ogni utente ha credenziali individuali
  - Più sicuro, ma richiede infrastruttura aggiuntiva

1.2.3 Vulnerabilità

- TKIP può essere attaccato (Beck-Tews attack)
- Vulnerabile ad attacchi di dizionario offline su PSK
- Possibili attacchi DoS causando rikeying

1.3 WPA2

- **Introduzione**: Standard IEEE 802.11i rilasciato nel 2004
- **Meccanismo**: Usa CCMP basato su AES invece di RC4/TKIP

1.3.1 Caratteristiche principali

- Cifratura AES-CCMP sicura ed efficiente
- Gestione chiavi robusta
- Integrità e autenticazione integrate
- Protezione contro replay attack

1.3.2 Modalità

- **Personal (PSK)**:
  - Chiave precondivisa
  - Adatta per reti domestiche/piccoli uffici
  - Protocollo handshake a 4 vie
- **Enterprise**:
  - Autenticazione basata su 802.1X e RADIUS
  - EAP (Extensible Authentication Protocol)

    - Per organizzazioni più grandi con gestione centralizzata

1.3.3 Vulnerabilità note

- **KRACK** (Key Reinstallation Attack) scoperto nel 2017
    - Sfrutta vulnerabilità nel handshake a 4 vie
    - Permette di forzare la reinstallazione di chiavi già in uso
    - Può portare a decifrazione del traffico
- Attacchi di forza bruta su password deboli
- Alcune implementazioni vulnerabili a Denial of Service

1.4 WPA3

- **Introduzione**: Introdotto nel 2018 come successore di WPA2
- **Obiettivo**: Risolvere le vulnerabilità di WPA2 e migliorare la sicurezza

1.4.1 Caratteristiche principali

- **SAE** (Simultaneous Authentication of Equals - Dragonfly)
    - Sostituisce il PSK
    - Handshake resistente agli attacchi di dizionario
    - Forward secrecy (compromettere una sessione non compromette le altre)
- **Protezione dagli attacchi di dizionario** offline
- **Crittografia robusta**: minimo 128 bit (Personal), 192 bit (Enterprise)
- **Protezione migliorata per reti pubbliche**:
    - OWE (Opportunistic Wireless Encryption)
    - Crittografia anche senza autenticazione
- **PMF** (Protected Management Frames) obbligatorio

1.4.2 Differenze con WPA2

Caratteristica	WPA2	WPA3
Handshake	4-way PSK	SAE (Dragonfly)
Protezione dizionario	No	Sì
Forward secrecy	No	Sì
Protezione reti aperte	No	Sì (OWE)
PMF	Opzionale	Obbligatorio
Complessità minima password	Nessuna	Maggiore

2. HTTPS (HTTP Secure) e SSL/TLS

HTTPS è HTTP su una connessione cifrata con SSL/TLS, essenziale per proteggere le comunicazioni web.

2.1 Funzionamento HTTPS

1. Client richiede connessione sicura al server
2. Server invia il suo certificato X.509
3. Client verifica il certificato contro CA (Certificate Authority) attendibili
4. Client genera una chiave di sessione
5. La chiave viene scambiata in modo sicuro
6. La comunicazione prosegue cifrata con la chiave di sessione

2.2 Vantaggi di HTTPS

- **Confidenzialità**: Protezione contro intercettazioni
- **Integrità**: Garanzia che i dati non siano stati alterati
- **Autenticazione**: Verifica dell'identità del server
- **SEO**: Miglior posizionamento nei motori di ricerca
- **Nuove funzionalità**: Accesso a Service Workers, HTTP/2, ecc.
- **Trust indicator**: Indicatore di sicurezza nel browser

2.3 Evoluzione dei protocolli SSL/TLS

- **SSL 2.0/3.0**: Obsoleti e vulnerabili (POODLE, BEAST)
- **TLS 1.0/1.1**: Deprecati (vulnerabili a BEAST, CRIME)
- **TLS 1.2**: Ancora ampiamente utilizzato
  - Supporta suite di cifratura moderne (AES-GCM)
  - Ancora standard in molte implementazioni
- **TLS 1.3** (2018): Versione attuale, più veloce e sicura
  - Handshake ridotto (1-RTT, 0-RTT)
  - Rimozione di algoritmi obsoleti/insicuri
  - Forward secrecy obbligatoria
  - Cifratura dei metadati del certificato

2.4 Handshake TLS 1.2 vs 1.3

TLS 1.2 Handshake (2-RTT):

1. Client → Server: ClientHello (cipher suites, random)
2. Server → Client: ServerHello, Certificate, ServerKeyExchange, ServerHelloDone
3. Client → Server: ClientKeyExchange, ChangeCipherSpec, Finished
4. Server → Client: ChangeCipherSpec, Finished
5. Comunicazione cifrata

TLS 1.3 Handshake (1-RTT):

1. Client → Server: ClientHello (guess key share, cipher suites, random)
2. Server → Client: ServerHello, CertificateVerify, Finished
3. Client → Server: Finished
4. Comunicazione cifrata

2.5 Certificati SSL/TLS

- **Componenti**:
  - Chiave pubblica del server
  - Nome del soggetto (dominio)
  - Firme digitali
  - Periodo di validità
  - Autorità di certificazione emittente
- **Tipi**:
  - **DV** (Domain Validation): verifica solo il controllo del dominio
  - **OV** (Organization Validation): verifica anche l'organizzazione
  - **EV** (Extended Validation): verifica approfondita dell'identità legale
- **Certificate Transparency**:
  - Log pubblici di tutti i certificati emessi
  - Permette di rilevare certificati fraudolenti
  - Obbligatorio per molti browser

3. Altri protocolli di sicurezza

3.1 IPsec (IP Security)

- **Definizione**: Suite di protocolli per sicurezza a livello IP (livello 3)
- **Componenti**:
  - **AH** (Authentication Header): integrità e autenticazione
  - **ESP** (Encapsulating Security Payload): confidenzialità, integrità, autenticazione
  - **IKE** (Internet Key Exchange): gestione delle chiavi e SA (Security Association)

3.1.1 Modalità operative

- **Transport mode**:
  - Protegge solo il payload del pacchetto IP
  - Header IP originale rimane intatto
  - Utilizzato principalmente per comunicazioni host-to-host
- **Tunnel mode**:
  - Protegge l'intero pacchetto IP (header + payload)

    - Incapsula il pacchetto originale in un nuovo pacchetto IP
    - Utilizzato principalmente per VPN site-to-site

3.1.2 Utilizzi comuni

- VPN site-to-site
- Protezione del traffico sensibile
- Implementazione del modello di sicurezza end-to-end
- Autenticazione senza cifratura (AH)
- Cifratura con autenticazione (ESP)

3.2 VPN (Virtual Private Network)

- **Definizione**: Tecnologia che crea un tunnel sicuro attraverso una rete non sicura (Internet)
- **Scopo**: Estendere una rete privata attraverso una rete pubblica

3.2.1 Tipi di VPN

- **Remote Access VPN**:
    - Connette un singolo utente a una rete
    - Utilizzata per lavoro remoto o accesso a risorse aziendali
- **Site-to-Site VPN**:
    - Connette intere reti tra loro
    - Usata per collegare filiali, uffici, data center

3.2.2 Protocolli VPN comuni

- **IPsec**:
    - Sicuro e robusto
    - Supportato da molti dispositivi
    - Può essere bloccato in alcune reti
- **SSL/TLS (OpenVPN)**:
    - Più facile da attraversare firewall (usa porta 443)
    - Flessibile e open-source
    - Può essere più lento di altre soluzioni
- **WireGuard**:
    - Moderno, veloce, codice compatto
    - Crittografia di ultima generazione
    - Minori funzionalità di gestione rispetto ad alternative
- **L2TP/IPsec**:
    - Combina tunneling L2TP con sicurezza IPsec

    - Supportato nativamente da molti sistemi
- **PPTP**:
    - Legacy, non considerato sicuro oggi
    - Facile da configurare e veloce
    - Da evitare per dati sensibili

3.2.3 Vantaggi delle VPN

- Privacy e anonimato online
- Accesso sicuro a risorse aziendali
- Protezione su reti Wi-Fi pubbliche
- Bypassare restrizioni geografiche
- Connessione sicura tra sedi distaccate

3.3 Bluetooth e sua sicurezza

3.3.1 Caratteristiche Bluetooth

- **Topologia**: piconet e scatternet
- **Beacon**: segnali periodici per sincronizzazione
- **Frequenza**: 2.4 GHz, frequency hopping
- **Classi di potenza**: Classe 1 (100m), Classe 2 (10m), Classe 3 (1m)
- **Versioni**: da 1.0 a 5.2, con miglioramenti di velocità e sicurezza

3.3.2 Meccanismi di sicurezza Bluetooth

- **Pairing**: processo di stabilimento della fiducia tra dispositivi
- **Bonding**: memorizzazione delle informazioni di pairing
- **Encryption**: cifratura dei dati usando AES-CCM
- **Authentication**: verifica dell'identità dei dispositivi
- **Authorization**: controllo dell'accesso alle risorse

3.3.3 Vulnerabilità Bluetooth

- **Bluejacking**: invio di messaggi non autorizzati
- **Bluesnarfing**: accesso non autorizzato ai dati
- **Bluebugging**: prendere il controllo di un dispositivo
- **KNOB** (Key Negotiation Of Bluetooth): forzare chiavi deboli
- **BlueBorne**: esecuzione di codice remoto senza pairing

4. Tecniche di attacco e difesa

4.1 Man in the Middle (MITM)

- **Definizione**: Attacco in cui l'aggressore si posiziona tra due parti comunicanti
- **Obiettivo**: Intercettare, leggere o modificare le comunicazioni senza essere rilevato

4.1.1 Metodi

- **ARP spoofing/poisoning**:
  - Corruzione tabelle ARP per reindirizzare traffico
  - Funziona solo in reti locali (stesso segmento)
- **DNS spoofing**:
  - Modificare le risoluzioni DNS
  - Reindirizza utenti a siti falsi
- **Rogue access point**:
  - AP malevolo che imita una rete legittima
  - Utenti si connettono pensando sia la rete corretta
- **SSL stripping**:
  - Downgrade da HTTPS a HTTP
  - Intercetta traffico prima della cifratura

4.1.2 Difese

- **HTTPS** (certificati validi e HSTS)
- **Certificate pinning**: verifica hardcoded dei certificati nelle app
- **Mutual authentication**: client e server si autenticano a vicenda
- **VPN**: traffico cifrato end-to-end
- **Monitoraggio tabelle ARP**
- **Packet filtering**
- **802.1X**: autenticazione a livello di porta

4.2 DOS/DDOS (Denial of Service)

- **Definizione**: Attacco che mira a rendere un servizio non disponibile ai legittimi utenti
- **DDoS**: versione distribuita che utilizza molti sistemi compromessi

4.2.1 Tipi

- **Volumetric**: sovraccarica la banda
  - UDP flood: invio massivo di pacchetti UDP
  - ICMP flood: invio massivo di pacchetti ICMP
  - Amplification: sfrutta servizi che generano risposte più grandi delle richieste
- **Protocol**: consuma risorse server
  - SYN flood: apertura di molte connessioni parziali
  - Fragmentation attack: pacchetti frammentati malformati

4.2.2 Difese

- **Filtraggio del traffico**: blocca pacchetti con caratteristiche sospette
- **Rate limiting**: limita numero di richieste da uno stesso IP
- **Load balancing**: distribuisce il carico su più server
- **Servizi anti-DDoS**: servizi specializzati come Cloudflare, AWS Shield
- **Anycast**: distribuisce il traffico su server geograficamente dispersi
- **Monitoraggio**: rileva pattern anomali
- **Sovradimensionamento**: capacità superiore al traffico massimo atteso
- **Blackholing**: indirizza il traffico malevolo verso un "buco nero"

4.3 Firewall

- **Definizione**: Sistema che filtra il traffico di rete in base a regole predefinite
- **Scopo**: Proteggere reti interne da minacce esterne

4.3.1 Tipi di firewall

- **Packet filtering**:
  - Filtra in base a informazioni dell'header (livello 3-4)
  - Controlla IP sorgente/destinazione, porte, protocollo
  - Semplice ma limitato, non analizza il contenuto
  - Stateless: non considera lo stato della connessione
- **Stateful inspection**:
  - Tiene traccia dello stato delle connessioni
  - Verifica che i pacchetti appartengano a connessioni legittime
  - Più sicuro del packet filtering
  - Mantiene una tabella delle connessioni attive
- **Application layer** (proxy):
  - Analizza il traffico a livello applicativo (livello 7)
  - Comprende i protocolli applicativi (HTTP, FTP, ecc.)
  - Può filtrare contenuti specifici
  - Più lento ma molto più sicuro
- **Next-generation**:
  - Integra funzionalità avanzate:
    - IPS (Intrusion Prevention System)
    - Antivirus
    - Deep packet inspection
    - URL filtering
    - Analisi del comportamento

4.3.2 Regole tipiche

- Default deny (blocca tutto tranne ciò che è esplicitamente permesso)
- Allow/Block in base a indirizzo IP, porta, protocollo
- Limitazione delle connessioni
- Content filtering
- Logging degli eventi

4.3.3 Architetture firewall

- **DMZ** (Demilitarized Zone):
  - Zona intermedia tra rete interna ed esterna
  - Ospita servizi accessibili dall'esterno (web, mail)
  - Protegge la rete interna anche se la DMZ è compromessa
- **Firewall perimetrali**:
  - Proteggono il confine tra rete aziendale e Internet
  - Prima linea di difesa
- **Firewall interni**:
  - Segmentano la rete interna
  - Limitano la propagazione di minacce interne

4.3.4 Firewall personali vs. di rete

- **Personali**:
  - Installati su singoli dispositivi
  - Proteggono il singolo sistema
  - Spesso integrati nei sistemi operativi
- **Di rete**:
  - Dispositivi dedicati
  - Proteggono l'intera rete
  - Gestione centralizzata
  - Maggiore potenza di elaborazione

5. Architetture di rete sicure

5.1 DMZ (Demilitarized Zone)

- **Definizione**: Sottorete fisica o logica che contiene ed espone i servizi esterni di un'organizzazione
- **Scopo**: Fornire un livello di sicurezza aggiuntivo isolando i server esposti

5.1.1 Configurazioni di DMZ

- **Single Firewall (Three-legged)**:
  - Un firewall con tre interfacce (interna, DMZ, esterna)
  - Economico ma meno sicuro
- **Dual Firewall**:
  - Firewall esterno tra Internet e DMZ
  - Firewall interno tra DMZ e rete interna
  - Maggiore sicurezza ma più costoso

5.1.2 Servizi tipicamente in DMZ

- Web server
- Email server
- DNS server pubblici
- Proxy server
- VPN concentrator
- FTP server

5.2 Difesa in profondità (Defense in Depth)

- **Definizione**: Strategia che utilizza molteplici livelli di sicurezza
- **Principio**: Se un meccanismo fallisce, ce n'è un altro che continua a fornire protezione

5.2.1 Livelli di difesa

- **Perimetro**: Firewall, router, IDS/IPS
- **Rete**: Segmentazione, VLAN, controllo accessi
- **Host**: Firewall locali, antivirus, hardening
- **Applicazione**: Sicurezza del codice, autenticazione
- **Dati**: Crittografia, controllo accessi
- **Utenti**: Formazione, policy di sicurezza

5.2.2 Vantaggi

- Nessun singolo punto di vulnerabilità
- Mitigazione del rischio in profondità
- Tempo aggiuntivo per rilevare attacchi
- Protezione da minacce interne ed esterne

5.3 Zero Trust Architecture

- **Definizione**: Modello di sicurezza che non si fida di nessuno, nemmeno degli utenti interni
- **Principio**: "Never trust, always verify"

5.3.1 Componenti chiave

- **Verifica continua**: Autenticazione per ogni accesso a risorsa
- **Micro-segmentazione**: Divisione della rete in zone isolate
- **Principio del privilegio minimo**: Accesso solo a ciò che è necessario
- **Multi-factor authentication**: Più fattori per l'autenticazione
- **Monitoraggio continuo**: Analisi comportamentale e anomalie

5.3.2 Implementazione

- Identity and Access Management (IAM)
- Software Defined Perimeter (SDP)
- Micro-segmentation
- Encryption
- Continuous monitoring e analytics

5.3.3 Vantaggi rispetto al modello tradizionale

- Riduzione della superficie di attacco
- Migliore visibilità
- Limitazione del movimento laterale degli attaccanti
- Semplificazione della conformità
- Protezione equivalente per utenti remoti e locali