Universitatea Politehnica Timișoara
Facultatea de Automatică și Calculatoare

Securitatea rețelelor wireless: Amenințări și soluții moderne

Securitatea sistemelor de calcul

An universitar 2024-2025

Marogel Dragoș-Florinel

Anul 3, CTI-TI
E-mail: dragos.marogel@student.upt.ro

Table of Contents

Introducere

Rețelele wireless au devenit o componentă fundamentală a infrastructurii digitale globale, permițând comunicații fără fir în numeroase contexte, de la rețele domestice și instituționale până la medii industriale și spații publice. Popularitatea acestor rețele este susținută de mobilitatea și ușurința în utilizare pe care le oferă. Cu toate acestea, natura deschisă a mediului wireless generează riscuri de securitate semnificative, necesitând soluții moderne și eficiente de protecție. Această lucrare explorează cele mai comune amenințări care vizează rețelele wireless și propune contramăsuri tehnice și organizatorice pentru combaterea acestora.

Definiția și importanța rețelelor wireless

Rețelele wireless sunt infrastructuri de comunicație care folosesc unde electromagnetice pentru a transmite informații între dispozitive, eliminând necesitatea cablurilor fizice. Aceste rețele sunt esențiale în contextul actual, caracterizat printr-o cerere crescută de mobilitate, accesibilitate și interconectivitate. Ele permit conectarea dispozitivelor mobile la internet, susțin rețelele inteligente (smart homes, smart cities) și sunt vitale în cadrul rețelelor industriale (Industrial IoT).

Evoluția si creșterea utilizării rețelelor wireless

Standardele IEEE 802.11 au evoluat constant, începând cu 802.11b și ajungând în prezent la 802.11ax (Wi-Fi 6) și 802.11be (Wi-Fi 7 în dezvoltare), fiecare generație oferind viteze mai mari, latență redusă și eficiență energetică sporită. În paralel, rețelele celulare au trecut prin mai multe generații (3G, 4G, 5G), extinzând posibilitățile de acces la internet mobil de mare viteză. Această expansiune rapidă a determinat o expunere mai mare la amenințări cibernetice, punând presiune pe sistemele de protecție ale utilizatorilor și furnizorilor de servicii.

Provocarile de securitate asocitate

Rețelele wireless reprezintă o componentă fundamentală a infrastructurii moderne de comunicații, însă acestea prezintă o serie de vulnerabilități specifice, datorită naturii lor deschise și a accesului facil la mediul de transmisie (undele radio). Comparativ cu rețelele cablate, unde accesul fizic este o condiție preliminară pentru interceptare, rețelele wireless sunt expuse în mod inerent riscurilor externe. Printre cele mai semnificative amenințări de securitate se numără:

Amenintari asupra retelelor wirless

Atacuri de tip Eavesdropping

Atacurile de tip *eavesdropping* (interceptarea pasivă a traficului) implică ascultarea sau capturarea datelor transmise între dispozitive wireless, fără consimțământul sau cunoștința participanților. Acestea sunt posibile în special în rețele nesecurizate sau care utilizează protocoale de criptare învechite, precum WEP (Wired Equivalent Privacy), care pot fi sparte în doar câteva minute folosind unelte disponibile public. Informații sensibile, precum date de autentificare, mesaje private sau detalii bancare, pot fi astfel expuse.

Atacuri Man-in-the-Middle

Atacuri *Man-in-the-Middle* presupun interceptarea activă a comunicației dintre două părți, prin care atacatorul se interpune între dispozitive fără ca acestea să detecteze prezența sa. În contextul rețelelor wireless, acest tip de atac este facilitat de absența unor mecanisme stricte de identificare a punctelor de acces. Prin redirecționarea traficului sau prin falsificarea pachetelor, atacatorul poate modifica sau fura date sensibile în timp real.

Atacuri de tip Deauthentication

Protocolul IEEE 802.11 nu impune criptarea pachetelor de deautentificare, ceea ce permite unui atacator să trimită mesaje falsificate de tip *deauthentication* către un client, forțând deconectarea acestuia de la rețea. Acest lucru poate fi folosit ca preambul pentru alte atacuri, cum ar fi *Rogue Access Point* sau capturarea pachetelor de tip *handshake* pentru ulterioră spargere prin atacuri de tip dicționar.

Atacuri de tip Rogue Access Point

Un *Rogue Access Point* reprezintă un punct de acces instalat în mod malițios, fără autorizarea administratorilor rețelei. Atacatorii pot clona un punct de acces legitim (prin tehnica *Evil Twin*), cu scopul de a păcăli utilizatorii să se conecteze la o rețea falsă. Odată conectați, utilizatorii pot fi supuși interceptării traficului, atacurilor de tip *phishing* sau infectării cu malware.

Atacuri de tip Brute-force si Dictionary Attack

Rețelele Wi-Fi protejate prin WPA/WPA2 se bazează pe parole pre-partajate (PSK – Pre-Shared Key). Dacă aceste parole sunt slabe sau ușor de ghicit, ele pot fi sparte folosind atacuri automate care testează un număr mare de combinații posibile (*brute-force*) sau folosesc liste comune de parole (*dictionary attack*). Aceste atacuri pot deveni și mai eficiente dacă atacatorul reușește să capteze *handshake*-ul inițial al unei sesiuni de autentificare.

Atacuri de exploatare a firmware-ului routerelor

Multe dispozitive de rețea utilizează firmware învechit sau care nu este actualizat regulat, lăsând deschise breșe de securitate cunoscute. Atacatorii pot profita de aceste vulnerabilități pentru a obține controlul asupra routerului, a intercepta traficul, a modifica setările DNS sau chiar pentru a lansa atacuri asupra altor rețele (*pivoting*).

Soluții moderne pentru protecția rețelelor wirless

Protocoale de securitate avansate

Utilizarea protocoalelor moderne, precum WPA3 (Wi-Fi Protected Access 3), aduce îmbunătățiri semnificative față de predecesorii săi, oferind criptare individuală pentru fiecare sesiune și protecție împotriva atacurilor de tip *brute-force* prin *Simultaneous Authentication of Equals (SAE)*.

Autentificare si control al accesului

Implementarea unor metode robuste de autentificare, precum 802.1X, împreună cu servere RADIUS, permite controlul granular al accesului la rețea și elimină dependența de parole pre-partajate. De asemenea, integrarea cu sisteme de autentificare multifactorială (MFA) adaugă un strat suplimentar de protecție.

Segmentarea retelei si monitorizarea activa

Segmentarea rețelei (ex. VLAN-uri) limitează extinderea unui atac în interiorul infrastructurii, iar monitorizarea activă a traficului prin soluții de tip IDS/IPS (Intrusion Detection/Prevention Systems) permite detectarea comportamentelor anormale sau a activităților malițioase în timp real.

Configurarea corecta a routerului Wi-Fi

Configurare riguroasă a routerului presupune: schimbarea parolelor implicite, dezactivarea funcțiilor nesigure (ex. WPS), actualizarea regulată a firmware-ului, dezactivarea transmiterii SSID-ului, și utilizarea unei parole complexe pentru accesul administrativ.

Utilizarea VPN pentru conexiuni sigure

Utilizarea rețelelor virtuale private (VPN) oferă un tunel criptat între utilizator și rețeaua de destinație, protejând astfel datele de interceptare, în special în rețelele publice sau nesecurizate.

Soluții avansate pentru protectia utilizatorilor finali

Instalarea de soluții de securitate endpoint (antivirus, firewall personal, EDR) pe dispozitivele utilizatorilor este esențială pentru detectarea și blocarea atacurilor directe sau a tentativelor de infectare prin intermediul rețelei wireless.

Bibliografie

1. William Stallings, *Wireless Communications & Networks*, Pearson Education, 2nd Edition.

2. RFC 8110 – *Guide to Wi-Fi Security*.

3. IEEE Security & Privacy Journal – articole relevante pe tema securității în rețele wireless.

4. Wi-Fi Alliance – standarde și ghiduri oficiale pentru implementarea WPA3 și a protocoalelor moderne.

5. C. Kaufman, R. Perlman, M. Speciner – *Network Security: Private Communication in a Public World*, Prentice Hall.

6. IEEE Std 802.11-2020 – Standardul oficial pentru rețele locale wireless (LAN).