**Studiu de caz despre protocoalele Wi-Fi: WPA și WPA2**

Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy, and Anwar Althubyani

-referat-

Rețelele wireless sunt utilizate pe scară largă pentru activități precum banking online, cumpărături, partajarea informațiilor și comunicare, oferind flexibilitate și mobilitate pentru dispozitive precum smartphone-uri și laptopuri. Acest lucru face ca securizarea rețelelor wireless să fie esențială pentru protejarea confidențialității și intimității utilizatorilor. Wi-Fi Protected Access (WPA și WPA2) sunt cele mai utilizate protocoale la nivel global pentru securitatea wireless. Această lucrare analizează avantajele, vulnerabilitățile și slăbiciunile acestora, concluzionând cu recomandări pentru îmbunătățirea funcționalității lor.

Tehnologia Wi-Fi a devenit omniprezentă de la sfârșitul secolului al XX-lea, fiind utilizată pe scară largă în case, școli, spitale și spații publice. Permite utilizatorilor să se conecteze și să partajeze date oricând și oriunde, folosind dispozitive precum smartphone-uri și laptopuri. Totuși, deoarece rețelele Wi-Fi se bazează pe canale cu acces deschis, partajate de mai mulți utilizatori, schimbul securizat de date este esențial.

Securitatea Wi-Fi a devenit un domeniu important de cercetare, iar în timp au fost dezvoltate diverse protocoale pentru a face față vulnerabilităților emergente. Dintre acestea, se remarcă trei protocoale principale: **WEP (Wired Equivalent Privacy)**, primul protocol de criptare introdus în standardul IEEE 802.11; **WPA (Wi-Fi Protected Access)**, creat pentru a rezolva deficiențele WEP; și **WPA2**, o versiune îmbunătățită bazată pe standardul IEEE 802.11i, concepută pentru a spori securitatea comunicațiilor wireless după limitările WEP și WPA.

**Wi-Fi Protected Access (WPA)** a fost introdus de grupul IEEE 802.11 Task Group I (TGi) pentru a îmbunătăți securitatea protocolului WEP. WPA utilizează **Temporal Key Integrity Protocol (TKIP)** și funcționează în două moduri: **Pre-Shared Key (PSK)** și **Enterprise**. Modul Enterprise oferă o securitate superioară, dar este mai dificil de configurat decât PSK.

TKIP îmbunătățește criptarea prin trei componente principale:

1. **Michael**: un cod de integritate a mesajului (MIC) pentru verificarea autenticității datelor.
2. **Secvențierea pachetelor**: un număr de secvență pentru fiecare pachet, asigurând actualitatea acestuia.
3. **Mixarea cheilor per pachet**: generarea unei noi chei de 128 de biți pentru fiecare pachet.

WPA folosește algoritmul de criptare **RC4**, similar cu WEP, dar îmbunătățit prin amestecarea cheii de bază cu vectorul de inițializare (IV) înainte de criptare. TKIP protejează împotriva atacurilor de tip replay prin utilizarea unităților MSDU și MPDU.

Astfel, WPA oferă o securitate mai robustă decât WEP, fiind un pas intermediar către protocoale mai avansate precum WPA2.

**Mecanismele de autentificare WPA** utilizează standardul IEEE 802.1x pentru a autentifica utilizatorii și a gestiona cheile, necesitând o cheie de 64 de biți pentru Michael și una de 128 de biți pentru funcția de mixare. WPA oferă două moduri: **WPA Personal** și **WPA Enterprise**. **WPA Personal (WPA-PSK)** este folosit în rețele casnice sau de birouri mici, fără un server de autentificare, în care clientul și punctul de acces împart o cheie pre-partajată de 256 biți, care nu este transmisă direct și din care se generează MIC (64 biți) și cheia de criptare (128 biți). În schimb, **WPA Enterprise** este folosit în rețele de afaceri, nu utilizează o cheie partajată, ci un protocol de autentificare extensibil (EAP), care asigură autentificarea bidirecțională și necesită un server **RADIUS** pentru securizarea traficului wireless.

**Wi-Fi Protected Access 2 (WPA2)**, adoptat în 2004, este considerat cel mai sigur protocol pentru rețelele wireless. WPA2 utilizează algoritmul **AES (Advanced Encryption Standard)** pe 128 de biți pentru criptare și autentificare. În WPA2 există două moduri de autentificare: **Pre-Shared Key (PSK)** și **Enterprise**, iar pentru generarea cheilor se folosește **Pairwise Transient Key (PTK)** în locul TKIP. În locul algoritmului Michael, WPA2 folosește **CCMP (Counter Mode CBC MAC Protocol)**, aplicând AES pentru criptare și CCM pentru asigurarea integrității datelor. Procesul de criptare în WPA2 implică pași precum incrementarea unui număr de pachet (PN), crearea unui bloc Nonce și generarea unui text criptat folosind cheile temporare și datele MPDU (Medium Access Control Protocol Data Unit). Decriptarea se face prin inversarea procesului de criptare, extrăgând valorile AAD și nonce din MPDU criptat, confirmând astfel integritatea și recuperând datele clare. În ceea ce privește mecanismele de autentificare, există două tipuri de sisteme de gestionare a cheilor: unul bazat pe o **cheie partajată** (mai simplu, dar mai puțin sigur) și altul care utilizează un **server de autentificare** pentru generarea cheilor prin protocolul **802.1x**, asigurând o securitate superioară. În acest din urmă caz, se generează chei temporare (PTK) și se folosesc schimburi de tip **4-way handshake** pentru verificarea și activarea criptării pachetelor.

**Integritatea datelor: WPA și WPA2**  
WPA utilizează algoritmul **Michael (MIC)** pentru a verifica integritatea mesajului și se bazează pe **Packet Sequencing** pentru a preveni atacurile de tip replay. În schimb, WPA2 folosește **CCMP** (Counter Mode with Cipher Block Chaining MAC Protocol) pentru a asigura integritatea atât a datelor, cât și a antetului pachetului. WPA folosește un număr de secvență de 48 de biți pentru a preveni atacurile de replay și pentru a mixa cheia de criptare cu secvența de numere, detectând și eliminând pachetele cu numere de secvență incorecte.

**Michael (MIC)** este folosit în WPA pentru a proteja integritatea datelor împotriva modificărilor, calculând o valoare de etichetă pe baza unui algoritm predefinit, iar procesul de verificare se face comparând eticheta trimisă cu cea calculată de receptor.

Pe de altă parte, **CCMP**, care necesită o actualizare hardware, este considerat o soluție mai bună, utilizând **AES** în modul **CCM** (Cipher Block Chaining MAC) pentru protecția autenticității și integrității. CCMP utilizează un număr de pachet de 48 de biți pentru a preveni atacurile de replay și asigură atât confidențialitatea, cât și integritatea pachetului. Procesul de integrare a datelor în WPA2 se desfășoară în cinci etape: incrementarea numărului de pachet (PN), construcția Nonce, construirea antetului CCMP, construirea datelor adiționale de autentificare (AAD), și criptarea cu CCM.

**Puncte slabe ale WPA/WPA2:**  
Deși schemele de securitate WPA/WPA2 sunt destul de puternice, au fost identificate câteva vulnerabilități minore, fără a reprezenta riscuri semnificative dacă se respectă recomandările de securitate. O vulnerabilitate majoră a WPA-PSK este atacul prin dicționar, care vizează captura celor patru pași ai handshake-ului între client și AP. Aceasta permite atacatorilor să aplice un atac de forță brută asupra cheii pre-partajate (PSK), deoarece informațiile necesare sunt transmise în clar. Deși WPA-PSK utilizează o cheie de 256 de biți, slăbiciunea sa provine din derivarea cheii principale (PMK) prin funcția PBKDF2, care poate fi spartă prin atacuri brute force dacă SSID-ul este cunoscut.

**Puncte forte ale WPA/WPA2:**  
WPA și WPA2 au adus îmbunătățiri semnificative în securizarea rețelelor Wi-Fi. Aceste protocoale folosesc criptare de date îmbunătățită, inclusiv prin utilizarea **TKIP** și a unei funcții de verificare a integrității, iar WPA2 utilizează **AES** pentru criptarea datelor, considerat mult mai sigur. În plus, WPA/WPA2 implementează autentificare mutuală pentru a preveni capturarea cheii de criptare și extinderea lungimii **IV** la 48 de biți pentru a proteja împotriva atacurilor de tip replay. Modurile **Enterprise** folosesc autentificarea **802.1X** și servere **RADIUS**, oferind un control și o securitate superioară rețelelor. De asemenea, ambele protocoale includ un mecanism de reînnoire a cheilor pentru a menține securitatea constantă.

Autorul incearca un **scenariu de atac**, ce descrie procesul de capturare a handshake-ului de autentificare WPA/WPA2 și utilizarea aircrack-ng pentru a sparge cheia pre-partajată (PSK).

**Pașii atacului pentru spargerea WPA/WPA2:**

1. **Configurarea rețelei țintă:** Se stabilește rețeaua țintă care utilizează criptare WPA2.
2. **Capturarea handshake-ului de autentificare:** Se activează modul monitor pe interfața wireless pentru a monitoriza pachetele. Se folosește comanda airodump-ng pentru a captura pachetele, specificând canalul și BSSID-ul punctului de acces.
3. **Atac activ de deautentificare:** Se folosește comanda Aireplay-ng pentru a efectua un atac de deautentificare asupra unui client conectat la rețea. Acest atac forțează clientul să se reconecteze la rețea și să genereze un nou handshake, care este capturat.
4. **Capturarea handshake-ului complet:** După deautentificare, se obține cu succes handshake-ul de patru pași (Four-Way Handshake) între client și punctul de acces.
5. **Lansarea unui atac prin dicționar:** Se utilizează Aircrack-ng pentru a lansa un atac prin dicționar, încercând fiecare parolă dintr-un fișier de dicționar. Aircrack-ng compară fiecare parolă cu handshake-ul capturat pentru a identifica cheia corectă.
6. **Verificarea parolei:** Fiecare parolă din dicționar este verificată prin 4096 de iterații HMAC-SHA1 pentru a calcula cheia master temporară (PMK). După identificarea parolei corecte, cheia pre-partajată (PSK) este descifrată cu succes.
7. **Rezultatul atacului:** După finalizarea atacului, cheia pre-partajată (PSK) este obținută, iar rețeaua poate fi accesată.

**Pași pentru protejarea împotriva atacurilor WPA-PSK:**

1. **Utilizarea unei parole mai complexe:** Evită utilizarea unei parole scurte sau ușor de ghicit. Se recomandă o parolă de cel puțin 20 de caractere, care să conțină o combinație de litere mari și mici, cifre și simboluri, pentru a proteja PSK împotriva atacurilor prin dicționar.
2. **Schimbarea SSID-ului:** Schimbarea SSID-ului nu îmbunătățește semnificativ securitatea, dar poate ajuta la prevenirea conectării accidentale a utilizatorilor la rețele greșite și face mai dificilă identificarea rețelei de către atacatori.
3. **Implementarea mecanismului D-WPA-PSK:** Folosirea unui mecanism de actualizare periodică a PSK, în care AP trimite un număr aleatoriu tuturor clienților la intervale regulate. După ce clienții primesc numărul, un nou PSK este generat și distribuit, iar rețeaua se reconfigurează. Aceasta reduce șansele ca un atacator să poată sparge PSK, având ca rezultat o securitate îmbunătățită a rețelei WLAN.

În concluzie, lucrarea discută despre dezvoltarea noilor protocoale Wi-Fi, WPA și WPA2, și caracteristicile lor de securitate. WPA asigură confidențialitatea și intimitatea utilizatorului prin criptarea TKIP și Michael pentru integritatea datelor. Cu toate acestea, WPA are încă vulnerabilități în procesul de autentificare și integritate a datelor, motiv pentru care a fost creat WPA2. WPA2 introduce un nou mecanism de integritate a datelor, denumit CCMP, și necesită echipamente hardware actualizate pentru instalare. Lucrarea prezintă, de asemenea, un scenariu de atac, demonstrând că, în ciuda îmbunătățirilor de securitate, unele vulnerabilități persistă.