UNIVERSITATEA DE STAT DIN MOLDOVA

Facultatea de Matematică și Informatică

Departamentul de Informatică

**SOLUȚII VIABILE DE SECURITATE WIRELESS**

Țurcanu Cristian

Chișinău, 2022

CUPRINS

[Introducere 2](#_Toc115350377)

I. [Bluetooth 3](#_Toc115350378)

II. [WLAN 6](#_Toc115350379)

[Concluzie 10](#_Toc115350380)

[Bibliografie 11](#_Toc115350381)

# Introducere

Rețelele fără fir au o diferență cardinală în structura sa comparativ cu cele cu fir: semnalele se transmit printr-un mediu comun, deci orice utilizator ce are echipamentul necesar poate de facto primi orice semnal din rețeaua dată, chiar dacă acestea nu sunt destinate lui. Această diferență oferă oportunitatea de a asculta orice informații transmise și impune necesitatea de a securiza comunicațiile la nivel de date. De asemenea, asigurarea securității este un proces continuu, deci modernizarea sistemelor este un proces inevitabil ce se va întâmpla cu orice tip de rețea. În cadrul lucrării date vor fi descrise două tactici de modernizare a standartelor de rețele fără fir, care inițial aveau vulnerabilități critice de securitate, însă au fost actualizate pentru utilizarea sigură a acestora de către utilizatori în jurul lumii.

# I. Bluetooth

În primul rând, standartul Bluetooth oferă patru moduri de securitate ce specifică timpul în care se efectuează procedurile de securitate. Primul mod niciodată nu folosește proceduri de securitate, al doilea folosește autorizarea la nivel logic, însă deja după crearea legăturii fizice, al treilea efectuează procedurile la crearea legăturii fizice, iar al patrulea folosește autorizarea după crearea legăturii fizice și logice. Primul mod nu oferă niciun grad de securitate și este folosit doar pentru compatibilitate, iar modul al patrulea este folosit numaidecât la conecțiunea dintre dispozitive de versiune Bluetooth 2.1 și mai sus. Modul 4 de asemenea folosește 5 niveluri de securitate ce specifică necesitatea de criptare, interacțiunile utilizatorului la crearea legăturii, protecția MITM și folosirea algoritmilor criptografici aprobați de FIPS. Sistemul dat este astfel de complicat din cauza necesității de compatibilitate totală, diferenței de specificații și lipsei de standartizare a securității dispozitivelor Bluetooth lansate inițial.

La crearea legăturii dintre dispozitive se stabilește cheia simetrică care se va folosi pentru criptarea mesajelor transmise, care se numește Link Key. În modurile de securitate 2 și 3 se folosește generarea cheii prin tastarea unui cod PIN în ambele device-uri. Dispozitivele se vor autentifica prin verificarea PIN-ului comun și vor crea legătura[2].

În modul de securitate 4 se folosește metoda SSP (Secure Simple Pairing) ce oferă mai multe opțiuni de asociere a dispozitivelor în dependență de opțiunile de input și output prezente.

Prima opțiune numită Numeric Comparison se folosește pe dispozitivele ce pot arăta un cod de șase cifre pe ecranele sale și permit utilizatorului să introducă răspunsul “Da” sau “Nu”. La crearea legăturii, fiecare dispozitiv va arăta un cod de șase cifre pe ecran, și în caz că acestea coincid utilizatorul apasă “Da”, în caz contrar introduce “Nu”. Comparativ cu autentificarea prin PIN, codul dat nu se folosește la crearea Link Key-ului, astfel chiar dacă o persoană terță are acces la acest cod, acesta nu va putea folosi codul pentru obținerea cheii.

Passkey Entry se folosește în cazul când un dispozitiv poate arăta output, pe când celălalt poate doar transmite input (ex. tastatură). În cazul dat, dispozitivul cu ecran afișează un cod de șase cifre pe care utilizatorul îl va introduce pe dispozitivul de input. Analog opțiunii de mai sus, codul dat nu se folosește la crearea cheii.

Just Works se folosește în cazul când cel puțin un dispozitiv nu are nici opțiuni de input, nici de output. Opțiunea dată efectuează autentificarea conform metodei Numeric Comparison, însă utilizatorul este cerut să accepte conexiunea fără să verifice codul generat, astfel Just Works nu oferă protecție împotriva atacurilor MITM.

Out of Band (OOB) este creat pentru dispozitivele ce suportă o tehnologie cu sau fără fir (ex. Near Field Communication, NFC) comună pentru descoperirea dispozitivelor și schimb de date criptografice. În cazul tehnologiei NFC, metoda OOB permite asocierea dispozitivelor prin simpla atingere a lor și confirmarea conexiunii de către utilizator. Este important de reținut că pentru a face procesul de împerechere cât mai sigur, tehnologia OOB folosită trebuie să fie proiectată și configurată pentru a mitiga ascultarea pasivă și atacurile MITM.

De asemenea, SSP folosește algoritmul ECDH (Elliptic Curve Diffie-Hellman) pentru stabilirea Link Key-ului, implementând metode de criptografie cu cheie publică, astfel cheia dată este protejată împotriva atacurilor pasive și MITM.

Analog modurilor de securitate de mai sus, există moduri de securitate și servicii ce oferă niveluri diferite de protecție, de la criptare totală până la transmiterea datelor fără nicio protecție. Deși specificațiile Bluetooth cer ca să fie folosit cel mai sigur mod suportat de ambele dispozitive, în cazul utilizării unor aparate vechi pot să fie ignorate toate măsurile de securitate pentru a păstra compatibilitatea, astfel dispozitivele vechi sunt prime ținte pentru atac.

Atacurile Bluetooth în mare parte folosesc vulnerabilitățile versiunilor vechi pentru a exploata problemele hardware-ului sau ingineria socială pentru a manipula utilizatorul. Spre exemplu, Bluesnarfing și Bluebugging lucrează doar pe dispozitivele create până în anul 2003, iar Bluejacking și BlueStumbling se previn prin folosirea modului de descoperire doar în caz strict necesar, fără a lăsa acesta întotdeauna pornit[3] Există însă și opțiunea de asociere Just Works care este vulnerabilă la atacurile MITM[1], astfel pentru a preveni atacurile se recomandă de a utiliza politici de conectare ce refuză modul de conectare Just Works sau pur și simplu oprirea serviciului Bluetooth când acesta nu se utilizează.

Deoarece Bluetooth a fost inițial creat fără ca să urmeze standartele internaționale pentru rețele fără fir, astfel multe dispozitive nu erau compatibile între ele, iar securitatea în mare parte pur și simplu lipsea. Versiunile noi de Bluetooth au rezolvat vulnerabilitățile și automat folosesc modul de securitate cel mai sigur, însă în cazul conexiunii cu dispozitivele vechi acestea impun transmiterea mesajelor cu securitate slabă pur și simplu pentru că nu suportă alte opțiuni. Deși dispozitivele de tip vechi sunt foarte greu de găsit, acestea pot fi folosite în companii mai conservative ce rar modernizează echipamentul, precum instituțiile de stat și de învățământ, deci pericolul nu este niciodată exclus.

# II. WLAN

Analog altor rețele fără fir, WLAN-urile trebuie să susțină câteva obiective de securitate, cele mai des necesare fiind:

* Confidențialitatea - asigură faptul că mesajele nu pot fi citite de terțe părți,
* Integritatea - detectarea modificărilor intenționate și neintenționate a mesajelor transmise,
* Disponibilitatea - utilizatorii pot accesa rețeaua oricând au nevoie de ea,
* Controlul accesului - restrângerea drepturilor de acces a utilizatorilor la rețea.

Obiectivele de securitate pentru rețelele LAN cu fir și fără fir de fapt sunt aceleași, ca și cele mai mari pericole a acestor rețele, precum ascultarea pasivă și analiza traficului, atacurile Denial of Service, mascaradă, MITM, retransmiterea și modificarea mesajelor. Comparativ cu rețelele cu fir, în care pentru a ataca rețeaua este necesar accesul fizic la infrastructura acesteia sau compromiterea unui dispozitiv din rețea, WLAN-urile pot fi ușor accesate fiind în raza de acțiune a semnalelor lor[5].

Până la adoptarea standartului IEEE 802.11i și framework-ului său RSN (Robust Security Network), IEEE 802.11 avea o multitudine de vulnerabilități. Mulți producători au implementat măsuri proprietare de securitate pentru a compensa defectele standartului, însă acestea deseori nu erau compatibile între ele.

Inițial specificațiile IEEE 802.11 defineau două metode de validare a identității dispozitivelor în rețea - autentificare prin sistem deschis și autentificare prin cheie partajată.

Autentificarea prin sistem deschis necesită doar SSID-ul AP-ului (Acces Point) și adresa MAC a dispozitivului utilizator. SSID-ul este transmis prin broadcast în format text clar, iar adresa MAC este o valoare unică pe 48 biți ce este setată permanent și identifică dispozitivul de rețea. Această adresă poate fi utilizată pentru a autoriza anumite dispozitive în rețea, însă deoarece MAC-ul nu este criptat la trimitere, acesta poate fi ușor interceptat și identificat dacă e permis accesul dispozitivului după filtrul de adrese. MAC-urile adaptoarelor de rețea pot fi ușor modificate prin software, deci e extrem de ușor de a intra în rețea sub alt nume. De asemenea în procesul dat nu se autentifică AP-ul, astfel utilizatorul nu are niciun mod de a cunoaște dacă comunică cu AP-ul real sau unul fals cu același SSID. Astfel, autentificarea prin sistem deschis nu oferă servicii de siguranță suficiente pentru a fi sigur de orice identitate din rețea și poate fi ușor exploatată.

Autentificarea prin cheie partajată era presupusă să fie mai sigură ca autentificarea prin sistem deschis, însă este tot așa de nesigură. Aceasta folosește o cheie criptografică secretă numită WEP (Wired Equivalent Privacy) Key care este partajată de utilizatori și AP-uri. Autentificarea decurge printr-o schemă de tip challenge-response în care se verifică cunoașterea cheii. Utilizatorul inițiază autentificarea, după ce AP-ul trimite o valoare aleatoare pe 128 biți. Folosind cheia WEP, utilizatorul criptează valoarea dată și o trimite înapoi, iar AP-ul confirmă corectitudinea criptării și astfel prezența cheii. Pentru criptare se folosește algoritmul RC4 care generează o secvență de date numită key stream, iar la criptarea sau decriptarea informațiilor se aplică operația XOR dintre date și key stream.

Autentificarea dată de asemenea este slabă deoarece AP-ul nu e autentificat la utilizator, astfel utilizatorul nu poate afla dacă comunică cu un access point legitimat. De asemenea, schemele unilaterale challenge-response s-au dovedit a fi slabe în majoritatea cazurilor, și chiar dacă acest algoritm oferă protecție împotriva atacurilor de retranslare pentru autentificare, acestea încă sunt slabe împotriva MITM și atacurilor offline brute force și de tip dicționar. De asemenea, un ascultător ar putea afla porțiunea necesară din key stream pur și simplu captând datele inițiale și criptate și efectuând operația XOR asupra lor. De asemenea, deoarece algoritmul dat autentifică dispozitivele și nu utilizatorii, părțile terțe ar putea obține accesul asupra unui dispozitiv autentificat și folosi cheia WEP pe orice alt dispozitiv e suportă WEP.

O altă vulnerabilitate a autentificării prin cheie partajată este faptul că aceasta cere ca toți utilizatorii a rețelei să folosească aceeași cheie sau același set mic de chei de acces. Acest fapt reduce posibilitatea de răspundere a fiecărui utilizator, iar în caz de compromitere a cheii aceasta trebuie modificată cât mai repede pentru a preveni atacurile ulterioare. De asemenea, WEP nu oferâ suport de management a cheilor, astfel trebuie să implementeze metodele proprii degenerare și distribuire a cheilor, cel mai des distribuind acestea manual pe fiecare dispozitiv și AP din rețea. Acest fapt sever blochează posibilitatea de a administra o rețea pe scară largă, astfel WEP fiind greu de utilizat în cadrul rețelelor corporative mari.

Protocolul WEP folosește cifrul RC4 pentru a cripta datele transmise și a le proteja împotriva atacurilor pasive. Standartul pentru WEP folosește doar 40 de biți de cheie, însă producătorii oferă echipament cu lungimi de cheie de 128 și chiar 256 biți. În caz ideal lungimea cheii oferă o protecție mai mare, însă metodele criptografice folosite în WEP are defecte care nu se rezolvă prin chei de lungime mare.

Majoritatea atacurilor la criptarea WEP se bazează pe vulnerabilitățile a IV (vector de inițializare). Spre exemplu IV-ul este transmis ca text clar, astfel în urma monitorizării traficului este posibilă obținerea cheii. De asemenea, WEP nu specifică cum anume se obține valoarea IV, astfel deseori se folosesc valori statice cunoscute sau resetarea la zero. Dacă două mesaje criptate au același IV și este cunoscut textul clar a oricărui dintre mesaje, atunci este relativ ușoară obținerea textului clar a celuilalt mesaj. În mare parte deoarece multe mesaje folosesc header-uri asemănătoare sau alte conținuturi ușor de identificat, e posibilă obținerea textului inițial cu efort minim. Chiar și în cazul incrementării IV-ului acesta este vulnerabil la atac. IV-ului sunt alocați 24 biți, adică aproximativ 17 milioane valori unice, astfel într-o rețea încărcată întregul spațiu de IV-uri poate fi utilizat în câteva ore. Chiar și la alegerea aleatoare a IV-ului după paradoxul zilei de naștere două IV-uri au șansa de colizie de 50% după 212 frame-uri.

Un alt pericol este analiza traficului rețelei, care poate oferi informații despre ce părți comunică în ce intervaluri de timp. De asemenea e posibilă determinarea conținutului mesajelor, astfel în caz de serii scurte de activitate pot fi cauzate de terminale la distanță sau mesengere, iar serii lungi și stabile de trafic pot fi cauzate de videoconferințe. Analize mai sofisticate ar putea determina sistemul de operare folosit în baza lungimilor unor frame-uri transmise. În afara criptării datelor WEP nu oferă protecție împotriva atacurilor pasive, precum adăugarea padding-ului de lungime aleatoare sau transmiterea mesajelor cu conținut generat aleator.

WEP verifică integritatea mesajelor folosind checksum-ului CRC-32, astfel în cazul necorespunderii checksum-ului transmis de cel real AP-ul va ignora mesajul, oferind o oarecare protecție împotriva atacurilor MITM.

Algoritmul CRC-32 însă este vulnerabil la atacuri de tip bit flipping, în care partea terță modifică mesajul neștiind concret conținutul său. În cazul algoritmului dat atacatorul va ști exact ce biți din checksum vor fi modificați la modificarea biților din text. Autorii WEP au crezut că criptarea mesajului va proteja frame-urile împotriva bit flipping-ului, însă o proprietate a cifrului RC4 este că criptarea se efectuează prin XOR-ul textului clar la key stream. Schimbând valoarea unui bit din text criptat va schimba același bit din text clar, astfel criptarea dată nicicum nu protejează împotriva acestui atac. CRC-32 este proiectat doar pentru a detecta erori de transmisiune și nu atacuri criptografice intenționale, astfel în cazul dat e recomandată folosirea unui checksum criptografic ce modifică mai mulți biți la schimbarea unui bit din text.

WEP de asemenea nu folosește countere de frame-uri sau marcaje de timp, astfel este vulnerabil la atacuri de retransmitere a mesajelor.

Standartul IEEE 802.11i introduce conceptul de RSN (Robust Security Network), care este o rețea fără fir securizată ce permite doar crearea a asocierilor de tip RSNA (Robust Security Network Association). Conexiunile date folosesc schema de management a cheilor numită 4-Way Handshake, care este un protocol ce asigură că ambii participanți dețin un PMK (Pairwise Master Key) și sincronizează setarea cheilor temporare. Participanții obțin PMK-ul prin unul din două moduri: cheia poate fi deja configurată pe fiecare device, astfel ea se numește PSK (pre-shared key), sau este distribuită în procesul de autentificare prin EAP (Extensible Authentication Protocol). Administratorii rețelelelor corporative vor prefera folosirea EAP pentru formarea conexiunilor din cauza dificultății de gestionare a cheilor PSK, pe când rețelele de casă sau ad-hoc vor folosi PSK datorită ușurinței de setare inițială.

În urma analizei protocolului WEP au fost descoperite numeroase vulnerabilități critice care permit atacul ușor a rețelei. Standartul IEEE 802.11i a rezolvat această problemă pur și simplu lansând un nou standart de securitate ce nu este compatibil cu WEP, astfel impunând fiecare utilizator să procure echipament de tip nou. Tactica dată însă a fost necesară pentru că vulnerabilitățile WEP erau prea severe ca să poată fi rezolvate printr-un update de software, iar o altă soluție pur și simplu nu există. De asemenea această tactică rezolvă vulnerabilitățile la 100%, astfel utilizatorii nu vor fi nevoiți să se asigurede securitatea rețelei la fiecare conexiune. Desigur, acest fapt nu exclude riscurile moderne precum punctele false de acces[4], însă acestea se bazează pe ingineria socială și nu vulnerabilități de hardware, care se rezolvă prin educarea continuă a utilizatorilor.

# Concluzie

Domeniul de securitate informațională se bazează pe rezolvarea vulnerabilităților găsite și prevenirea lor prin proiectarea standartelor actuale de siguranță. Acest proces e continuu, deoarece întotdeauna se găsesc vulnerabilități în sisteme, iar cu modernizarea hardware-ului se face mai rapidă atacul prin forță brută, ceea ce asigură modernizarea continuă a securității sistemelor din jur. Spre exemplu, WLAN-urile au trecut de la protocolul WEP prin modernizarea totală a hardware-ului, iar Bluetooth folosește algoritmi criptografici siguri, însă păstrează compatibilitatea cu dispozitivele vulnerabile.

# Bibliografie

1. Detaliile atacului asupra SSP

<https://pages.nist.gov/mobile-threat-catalogue/lan-pan-threats/LPN-15.html>

1. Guide to Bluetooth Security, 2017

<https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final>

1. Lista vulnerabilităților Bluetooth

<https://pages.nist.gov/mobile-threat-catalogue/search.html?query=bluetooth>

1. Lista vulnerabilităților Wi-Fi

<https://pages.nist.gov/mobile-threat-catalogue/lan-pan.html>

1. Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf>