MINISTERUL EDUCAȚIEI ȘI CERCETĂRII
UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE
POLITEHNICA BUCUREȘTI

Şcoala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

REZUMAT TEZĂ DE DOCTORAT

Ing. Cezar Gabriel DUMITRACHE

CONTRUBUȚII ÎN SECURIZAREA IoT UTILIZÂND SISTEME INTELIGENTE DE SECURITATE

CONTRIBUTIONS IN SECURING IoT USING SMART SECURITY SYSTEMS

Conf. Dr. Ing. Constantin Viorel Marian
Univ. Politehnica din Bucureşti

Conducător de doctorat

BUCUREŞTI 2026

Capitolul 1

Introducere

Comunicațiile și tehnologia informației au luat o amploare de neimaginat acum câțiva ani fiind motorul de dezvoltare la nivel planetar. Acestea au cunoscut acest ritm de dezvoltare pentru că au apărut diferite noi tehnologii care au adus plus valoare prin costuri mai reduse de producție și prin eficiență mai mare din punct de vedere energetic. Totuși, chiar dacă au fost proiectate beneficiind de o mare experiență acumulată de-a lungul timpului, au venit la pachet și cu o serie de vulnerabilități ce au fost descoperite doar când acestea au fost implementate în producție. Un astfel de exemplu care este folosit chiar și în prezent la o scară foarte mare chiar dacă prezintă vulnerabilități, este protocolul WPA2 . Acesta este folosit într-un mod intens de fiecare dintre noi fiind chiar "impus" de providerii de internet prin dispozitivele pe care aceștia le oferă în custodie clienților pentru perioada în care oferă acestora servicii de internet. Acest lucru a determinat creșterea nevoii de specialiști care să se ocupe de acest domeniu pentru că orice tip de organizație nu poate funcționa cu breșe de securitate fiind necesară asigurarea securității pentru a preveni incidentele nedorite și care ar genera pierderi semnificative.

1.1 Prezentarea domeniului tezei de doctorat

Am ales să abordez conceptul de securitate cibernetică prin studierea protocolului de criptare a datelor WPA2-Enterprise într-o rețea fără fir deoarece acesta aduce beneficii din punct de vedere al securității și cu ajutorul lui se poate studia securitatea pentru Internetul Obiectelor (IoT). Aceste obiecte au crescut exponențial fiind introduse în viața noastră întru-un număr din ce în ce mai mare. Acestea în marea lor majoritate au fost conectate prin intermediul Wi-FI într-un mod total nesecurizat și astfel fiind transformate în ținte foarte ușor de abordat de către orice persoană care deține minime cunoștințe tehnice. Cu toate că se constată o scădere a numărului de incidente în domeniul securității conform ENISA, este imperios necesar ca organizațiile să își constituie echipe specializate în securitate și datorită faptului că a crescut complexitatea acestora conform aceluiași studiu.

1.2 Scopul tezei de doctorat

Scopul tezei este de a aduce contribuții în realizarea securității IoT prin implementarea unor sisteme și politici de securitate prezentate pentru majoritatea sistemelor de operare și dezvoltarea unui dispozitiv cu ajutorul căruia să asigur securizarea acestor obiecte la nivelul rețelelor fără fir pentru a micșora posibilitatea apariției unor breșe în astfel de rețele, oferind totodată o soluție practică, scalabilă și adaptabilă diverselor scenarii de utilizare, capabilă să prevină și răspundă în mod eficient la atacurile cibernetice specifice mediilor IoT care sunt regăsite atât în mediile publice, în zonele casnice cât și în zonele industriale. În acest context mi-am propus să analizez în profunzime particularitățile amenințărilor cibernetice asociate mediilor IoT, punând accent pe vectorii de atac frecvent întâlniți, pe impactul acestora asupra securității datelor și funcționării dispozitivelor conectate. Studiul include o evaluare comparativă a mecanismelor de securitate existente în principalele sisteme de operare utilizate în IoT, subliniind avantajele și limitările fiecăruia. De asemenea, lucrarea propune o arhitectură proprie de securizare a rețelelor fără fir, integrând componente hardware și software concepute pentru protecția rețelei propusă pentru a fi securizată.

1.3 Conţinutul tezei de doctorat

Teza de doctorat este structurată în 7 capitole împreună cu lista tabelelor, lista figurilor și lista abrevierilor folosite. În Capitolul 1 am prezentat partea introductivă a domeniului tezei de doctorat prin care am descris diferite tipuri de atacuri și noi tipuri de atacuri asupra tuturor dispozitivelor existente. Am studiat aceste tipuri de atacuri și tehnici de apărare împotriva lor pentru a dezvolta diferite metode și tehnici de protecție în fața lor.

În capitolul 2 am descris tehnicile care pot fi implementate pentru a ne putea proteja rețeaua de aceste atacuri la diferite nivele.

Capitolul 3 debutează cu diferite tipuri de implementări pentru detectarea intruziunilor și continuă cu metode și acțiuni pentru protecția diferitelor dispozitive care au implementate diferite sisteme de operare.

În capitolul 4 am descris standarde și protocoale de criptare, de autentificare folosite în mediul fără fir și metode de protecție folosite în acest mediu fără fire. Am descris inclusiv protocolul 802.1.x pe care l-am folosit pentru securizarea dispozitivelor IoT mai vechi care nu sunt capabile de a interacționa prin intermediul acestui protocol.

Capitolul 5 debutează cu descrierea topologiei folosite pentru testarea dispozitivelor, continuă cu descrierea modului de lucru al dispozitivelor și totodată am introdus și concluziile în urma implementării dispozitivelor de securitate.

Capitolul 6 este cel mai interesant deoarece tratează autentificarea dispozitivelor într-o rețea Wi-Fi prin intermediul certificatelor digitale și prin folosirea blockchain-ului ca mijloc de securizare suplimentar. Pot spune că acest lucru

nu mai este întâlnit la ora actuală. Autentificarea dispozitivelor într-o rețea Wi-Fi utiliziând blockchain-ul fiind realizrea mea în urma cercetărilor efectuate. Prin acest lucru am adus un nou concept pentru a securiza autentificarea unui dispozitiv cu resurse minime.

Concluziile finale, rezultatele și contribuțiile mele originale au fost rezervate pentru a fi prezentate în capitoloul 7

Capitolul 2

Tehnici de combatere a noilor tipuri de atacuri

Pentru a proteja rețeaua organizației și implicit utilizatorii, se impun a fi luate masuri în concordanță cu actualele amenințări prezente. Primele acțiuni care trebuiesc implementate, sunt cele care se vor regăsi pe dispozitivele de rețea cât și pe cele folosite de utililizatori. Printre acestea regăsim politicile de securitate care vor fi folosite atât la nivel soft cât și la nivel fizic.

2.1 La nivel fizic

Protejarea serverelor și a dispozitivelor cu ajutorul cărora se realizează comunicarea, prin dispunerea acestora în încăperi prevazute cu încuietori, senzori de mișcare, senzori termici și camere de supraveghere. Securitatea fizică poate fi definită ca având două componente principale: arhitectura clădirii și tipurile de echipamente și dispozitive folosite.

Protejarea din punct de vedere al divulgării unor date esențiale prin dispunerea monitoarelor astefel încât doar utilizatorul să poată vizualiza datele expuse prin intermediul acestuia.

Protejarea porturilor fizice de intrare ieșire pentru ca acestea să nu poată fi accesate decât de personalul autorizat și desemnat să le folosească.

2.2 La nivel soft

Se vor implementa diferite politici de securitate atât la nivel de dispozitiv de rețea, cât și la nivel de dispozitiv final, implementarea lor făcându-se în mod centralizat. Printre acestea enumerez:

Crearea de vlanuri, astfel realizându-se microsegmentarea rețelei cu ajutorul căreia micșorăm posibilitatea compromiterii întregii rețele. Eventual compromiterea se va realiza doar pe un segment de rețea.

Dezactivarea protocoalelor nefolosite de la nivelul dispozitivelor cum ar fi DTP.

Crearea de administratori care vor avea un acces de nivel mediu pentru depanarea și rezolvarea problemelor apărute.

Crearea de utilizatori care nu vor avea acces decât la resursele necesare pentru îndeplinirea sarcinilor și atribuțiilor.

Politică prin care, după scurgerea unei perioade de timp în care nu se înregistrează activitate, dispozitivul să se blocheze. Pentru deblocare să fie necesară reintroducerea username-ului și a parolei aferente.

La introducerea greșită a parolei de doua sau de mai multe ori, utilizatorul să nu se mai poată autentifica o perioadă de timp.

Introducerea unor politici centralizate astfel încât un utilizator să nu poată folosi dispozitivul decât intr-un anumit interval de timp în care acesta ar trebui să se regăsească în timpul programului de lucru. Pentru a putea să folosească dispozitivul în afara acestui interval acesta va trebui să se adreseze administratorului de rețea pentru a i se permite lucrul în afara programului.

Crearea unor procese de back-up zilnic sau săptămânal.

Implementarea unor politici astefel încât în caz de dezastru infrastructura să fie reinițializată foarte repede.

2.3 Tehnici de protecție pentru atacuri ARP

Pentru protecția ARP se poate configura pe dispozitive DAI (Dynamic ARP Inspection) de layer 2 cât și pe dispozitive de layer 3 prin activarea DHCP snooping sau definirea interfețelor de încredere.Totuși trebuie avută multă grijă atunci când sunt implementate deoarece dacă nu se configurează adecvat se ajunge la blocarea pachetelor ARP legitime. De asemenea trebuie luată în considerare puterea de calcul care poate influența performanța rețelei cu toate că aduce un nivel de securitate foarte mare.

2.4 Tehnici de protecție pentru atacuri IP

Având în vedere că protocoalele de comunicare au fost create doar pentru a se comunica la distanță și că acestea nu au fost dezvoltate pentru a fi eficiente din punct de vedere al securității, în decursul timpului persoane rău intenționate au dezvoltat fel de fel de tipuri de atacuri pentru a accesa informațiile vehiculate prin intermediul acestor rețele. Iată câteva moduri de protejare împotriva acestora :

- Filtrarea IP cu ajutorul Firewall-urilor pentru oprirea accesului neautorizat;
- Folosirea numelor publice în locul IP-urilor.
- Angajații nu vor iniția conexiuni din rețeaua gazdă.
- Securizarea subdomeniilor.
- Validarea IP pentru prevenția atacurilor Spoofing IP;
- Utilizarea protocoalelor de criptare;

2.5 Tehnici de protective împotriva atacului ICMP

Împotriva acestui tip de atac ne putem proteja prin impunerea de acces list-uri, astfel blocând traficul acestui protocol, putând permite folosirea numai acolo unde este necesar

2.6 Tehnici de protective împotriva atacului de tip DOS şi DDOS

Este recomandat ca rețelele, aplicațiile și infrastructura IT să fie protejate printr-o abordare de securitate multistrat. Această metodologie poate integra soluții precum firewall-uri, rețele private virtuale, sisteme anti-spam, filtre de conținut și alte mecanisme complementare. Scopul este de a asigura monitorizarea continuă a activităților din rețea și identificarea anomaliilor legate de identitatea utilizatorilor, care pot indica tentative de atacuri de tip DDoS. Este necesar a se implementa un plan în cazul în care un astfel de atac are loc. O altă unealtă foarte eficientă în combaterea atacurilor de tip DDoS este crearea de liste de acces.

2.7 Tehnici de protecție împotriva atacului tip SPOOFING

Un astfel de atac poate fi contracarat prin aplicarea unor măsuri preventive, cum ar fi:

- DHCP SNOOPING pe porturile cu grad de încredere ridicată. DHCP SNOOPING se bazează pe adresele MAC sursă și poate determina dacă provin dintr-o sursă sigură sau mai puțin sigură, astfel filtrând mesajele de tip DHCP provenite din surse nesigure.
- uRPF. Când un ruter primește un pachet de tip unicast acesta se va uita după destinația acestuia pentru a-l trimite către destinatar pe fără a mai verifica și sursa IP.

Cu ajutorul acestei tehnologii, ruterul va verifica și sursa iar dacă aceasta nu va face parte din ip-urile setate ca fiind legitime, va arunca aceste pachete , astfel oprind atacurile de tip spoofing. Această abordare contribuie semnificativ la prevenirea atacurilor de tip spoofing, sporind reziliența infrastructurii rețelei în fața tentativelor de compromitere sau acces fraudulos. De asemenea, ea se aliniază principiilor moderne de securitate rețea, care promovează filtrarea bidirecțională și controlul riguros al fluxurilor de date pe baza identității verificate a participanților la comunicație.

Capitolul 3

Măsuri pentru prevenirea intruziunilor

3.1 Politici de sercuritate pentru dispozitivele finale

Recomandări de prevenire și securitate pentru stațiile de lucru. Securitatea stațiilor de lucru poate fi realizată prin implementarea unor metode cu ajutorul cărora să fie facilitat controlul lor pe mai multe paliere deoarece ideea de confidențialitate nu se leagă cu ideea de securitate pentru un simplu utilizator care nu deține abilități necesare pentru luarea unor măsuri în ceea ce privește securitatea în mediul online.

De aceea se impune implementarea unor politici de securitate pe stațiile de lucru cum ar fi:

IDENTIFICAREA – Măsură necesară pentru identificarea utilizatorului stației în vederea stabilirii grupului din care acesta face parte pentru a-i fi aplicate politicile de securitate necesare.

AUTENTIFICAREA – Se poate realiza prin mai multe tipuri de verificări: token, SID, parole, SIM card, verificarea datelor biometrice și altele, însă pentru o mai mare securitate se recomandă folosirea a cel puțin două metote simultan.

3.2 Măsuri pentru prevenirea intruziunilor în sistemele informatice:

Actualizarea dispozitivelor hardware și a software-ului folosit. Prin păstrarea actualizării software-ului și în special a sistemului de operare se reduce semnificativ riscul ca acesta să fie compromis.

- Fiecare utilizator trebuie să se asigure că are instalat, configurat și activat un produs antivirus instalat pe pe sistemul care îl folosește și recomandat ar fi ca la anumite intervale de timp acesta să execute o scanare completă pentru a verifica existența unor programe malițioase.
- Dezactivarea serviciilor telnet și SSH în caul în care acestea nu sunt folosite.

- Elaborarea unor politici care să impună utilizatorilor utilizarea unor parole complexe. O parolă trebuie :
- Să aibă cel puțin 12 caractere (14+ este mai bine)
- Parolele trebuie să includă litere mari și mici, cifre și simboluri speciale.
- Parolele nu trebuie salvate în locuri nesigure, ci doar memorate.
- A se folosi autentificarea cu doi factori acolo unde este posibil.
- Pentru a reține mai ușor parolele complexe, se poate utiliza o expresie mnemonica sau o frază de acces

3.2.1 Cu sistem de operare WINDOWS

- Dezactivarea Remote Desktop (Control Panel \ System and security \ Allow remote acces \ Properties \ Remote Desktop \ Don't allow remote connections to this computer.
- Politica parolelor:
- Politici folosite pe conturile de domeniu sau locale care determină setările acestora cum ar fi aplicarea acestora și viața acestora.
- Setări pentru vârsta parolelor.
- Setări prin care durata de timp în care un cont va fi blocat din sistem.
- Politicile de securitate pot fi configurate folosind :

GROUP POLICY OBJECT EDITOR:
"Computer Configuration\Windows Settings\Security Settings\Acount Policies\"

- Creare backup a sistemului de operare

3.2.2 Cu sistem de operare LINUX

- Crearea de utilizatori cu privilegii diferite în funcție de îndatoririle fiecăruia în organizație.
- Schimbarea parolei default.
- Implementarea auditării sistemului și a unui sistem de recuperare a datelor în caz de dezastru.
- Pentru conexiuunile de la distanță se recomandă implementarea SSH sau HTTPS.
- Configurarea IP Tables (închiderea porturilor nefolosite).
- Implementarea unei politici prin care la o perioada determinată, utilizatorii să își schimbe parolele de autentificare, inclusiv parolele introduse să îndeplinească criterii de complexitate.
- Implementarea unei politici prin care la o perioada determinată de inactivitate, sistemul să fie blocat iar pentru deblocare să fie necesară introducerea user-name și a parolei de autentificare.
- Restrângerea dreptului de acces a terminalului de comandă.

3.2.3 Metode şi acţiuni pentru protecţia dispozitivelor de layer 2

- Prima măsura care trebuie luată, este protecția fizică. Este necesar ca dispunerea acestor dispozitive să nu ofere acces decât persoanelor abilitate să

efectueze mentenanță și modificări prin dispunerea acestora în încăperi dotate cu incuietoare, senzori de mișcare, camere de supraveghere sau fără nici una din aceste măsuri în funcție de cât de importante sunt informațiile vehiculate prin intermediul acestora.

- A doua măsură este dezactivarea porturilor care nu vor fi folosite și puse într-un vlan nefolosit.
- Următoarea măsură se referă la microsegmentarea rețelei prin implementarea vlan-urilor.
- Întotdeauna a se folosi același ID de vlan dedicat pentru toate porturile în trunk.
- Implementarea redundanței la nivelul SNMP pe fiecare vlan în parte.
- Implementarea port-security pentru a stopa atacurile de tip flood împotriva adreselor MAC și pentru a stopa atacurile de tip DHCP starvation.
- Dezactivarea trunk-urilor pe toate porturile nefolosite și setarea acestora în modul acces împreună cu asignarea acestora unui vlan nefolosit în rețea.
- Dezactivarea negocierii trunk-urilor în mod automat pe toate porturile. Negocierea să se efectueze în urma unei configurații efectuată în mod manual.
- Crearea de conturi cu acces limitat pentru mentenanță.
- Pe cât posibil limitat accesul de la distanță iar când acest lucru nu este posibil, a se folosi protocoale sigure de comunicare cum ar fi SFTP sau SSL/TLS și folosirea unui vlan dedicat special pentru management.
- Microsegmentarea rețelei prin implementarea vlanurilor.
- Implementarea DHCP Snooping pe vlanurile considerate a fi vulnerabile la atcurile de tip DHCP starvation și DHCP spoofing.
- Implementarea DAI pentru a preveni atacurile de tip ARP spoofing și ARP poisoning.

3.2.4 Metode şi acţiuni pentru protecţia dispozitivelor de layer 3 (rutere şi switch-uri de layer 3)

- Dezactivarea protocolului http și activarea protocolului https.
- Crearea de utilizatori cu privilegii diferite în funcție de îndatoririle fiecăruia în organizație.
- În funcție de protocolul de rutare folosit se impune protejarea cu parole a link-urilor create în urma adiacenței dintre dispozitivele de rutare a traficului. Prin criptarea EIGRP sau OSPF ruterele se vor autentifica reciproc și în acest fel se vor evita false update-uri de rutare din surse necunoscute.
- Implementarea ACL. (Acces control list)
- Dezactivarea tuturor serviciilor care nu sunt folosite.
- Criptarea tuturor parolelor
- Implementarea IDS și IPS.
- Implementarea uPRF.

3.2.5 Implementarea I.D.S.

La nivelul unei oraganizații mari se impune crearea unui departament a cărui menire să fie protecția împotriva criminalității cibernetice și din care va trebui să facă parte în

mod obligatoriu și așa numiții analiști de securitate. Analiștii sunt adesea rugați să investigheze incidentele și să ofere un plan de acțiune în cazul unui atac. Pentru protecția împotriva a acestor tipuri de atacuri se impune instalarea în rețea a unui antivirus puternic și bine configurat inclusiv pe dispozitivele finale care sunt folosite de utilizatori. Totodată rețeaua va fi protejată prin implementarea unor firewall-uri de ultimă generație, sisteme de prevenire a intruziunilor și cooptarea unor analiști pentru analizoarele de trafic.
Acest departament va trebui să fie capabil să implementate și să manipuleze: analizoare de trafic, firewal-uri, să implementarea SIEM ,să implementeze SNMP.
Pentru detectarea unui comportament anormal al dispozitivelor din componența rețelei, SNMP dă posibilitatatea analiștilor de securitate să consulte log-urile generate de dispozitive, iar aceștia prin acest proces având acces la informații deosebit de prețioase pentru determinarea unor amenințări dacă există.
Cu informațiile oferite de dispozitive, un analist poate apela la diferitele lor surse de informații despre amenințări pentru a identifica familia specifică din care face parte eventuala amenințare. O astfel de platformă care ajută la identificarea unui hash sau unui fișier prin oferirea de informații este VirusTotal.com

3.3 Instruirea utilizatorilor

O altă componentă foarte importantă pentru protecția unei organizații constă în instruirea utilizatorilor.

Pentru sporirea securității organizației în mediul virtual se impune instruirea propriilor angajați pentru folosirea cât mai corectă a dispozitivelor inrterconectate și pentru evitarea unor atacuri de tip pshihing sau fishing, vfishing,smishing,typosquatting

Această activitate are un rol esențial în familiarizarea utilizatorilor din cadrul organizației cu metodele și tehnicile utilizate de atacatori pentru a obține informații sensibile. Aceste informații pot fi ulterior folosite pentru a compromite securitatea sistemelor, fie prin furt de date, fie prin introducerea de programe malițioase.

Tipuri de activități care trebuiesc desfășurate:

Informarea și instruirea pentru prevenirea scurgerii de date. Este important ca utilizatorii să fie informați cu privire la dezvăluirea datelor importante ale organizației chiar și în mod involuntar. Un exemplu îl constituie inclusiv trimiterea unui laptop la service în urma unei defecțiuni fără a îndepărta mediul de stocare

Utilizatorii să trateze întotdeauna circumspect email-urile prin care se solicită oferirea de date cu caracter personal.

A nu se accesa o adresă web dintr-un email nesolicitat.

La primirea unor email-uri prin care se solicită date personale, trebuie verificată legitimitatea acestora prin apelarea directă a companiei la numărul oficial și trebuie verificat domeniul de unde acesta a fost transmis.

Se impune crearea unor reguli și proceduri pentru ca în caz de dezastru fiecare utilizator să aplice anumiți pași prestabiliți pentru a limita daunele în organizație. Pe lângă măsurile tehnice, implementarea unei politici interne clare privind utilizarea dispozitivelor personale și accesul la rețeaua organizației este imperativă. Prin aplicarea acestor politici, se poate preveni propagarea amenințărilor cibernetice prin

intermediul dispozitivelor nesecurizate sau compromise

Capitolul 4

Măsuri de protecție în mediul Wi-Fi

4.1 Standarde și protocoale în mediul Wi-Fi

Pentru a putea înțelege mediul în care voi lucra, este necesar un scurt istoric despre diferitele standarde folosite și modul în care au fost introduse de-a lungul timpului. În tabelul 4.1 am evidențiaat evoluția standardelor Wi-Fi din familia IEEE 802.11, fiecare dintre acestea aducând îmbunătățiri semnificative în ceea ce privește viteza de transfer, frecvențele utilizate și eficiența rețelei. Standardul 802.11a, dezvoltat în 1999, a fost o soluție timpurie pentru rețele rapide în banda de 5 GHz, însă raza sa de acoperire era limitată de capacitatea redusă de penetrare a semnalului. În paralel, 802.11b, deși mai lent (11 Mbps), a fost mai utilizat datorită stabilității în banda de 2,4 GHz. Ulterior, 802.11g a combinat avantajele celor două, oferind viteze de 54 Mbps în banda de 2,4 GHz, cu o acoperire bună și performanță acceptabilă.

Un salt major s-a produs cu apariția 802.11n în 2009, care a adus tehnologia MIMO, crescând vitezele teoretice până la 300 Mbps. Dezvoltarea a continuat cu 802.11ac, finalizat în 2013, care a introdus operarea dual-band și capacitatea de a deservi mai mulți clienți simultan, atingând viteze de ordinul gigabiților (până la 2,3 Gbps). În prezent, 802.11ax (Wi-Fi 6) optimizează performanța în rețelele aglomerate și reduce consumul de energie prin funcția Target Wake Time, fiind compatibil cu toate cele trei benzi: 2,4 GHz, 5 GHz și 6 GHz.

Cel mai recent, 802.11be (Wi-Fi 7) vine ca o extensie a lui ax, concentrându-se pe creșterea vitezei și scăderea latenței pentru aplicații avansate, cum ar fi realitatea virtuală sau streaming-ul video 8K. Introducerea funcției Multi-Link Operation permite conexiuni simultane pe mai multe benzi, îmbunătățind semnificativ stabilitatea și performanța generală a rețelei. În ansamblu, fiecare generație a adus inovații importante, reflectând cerințele tot mai mari ale utilizatorilor pentru conectivitate rapidă, stabilă și eficientă.

4.2 Protocoale de criptare Wi-FI

Wpa - Este un protocol folosit pentru criptarea datelor folosite într-o rețea fără fir. Deși a apărut în urma slăbiciunilor precedentului său protocol Wep, pentru a spori

securitatea, o dată cu trecerea timpului a reușit aceași perfomanță și a devenit foarte vulnerabil la atacuri.

Wpa 2 – Același lucru se poate spune și despre WPA2 . Este tot un protocol de criptare a datelor într-o rețea fără fir și ca și precedentul a devenit foarte vulnerabil la atacuri.

Wpa 2 Enterprise – Despre acest protocol se poate spune la ora actuală că oferă o protecție ridicată deoarece folosește autentificarea utilizatorilor într-o rețea fără fir prin intermediul unui server Radius sau Kerberos și se pot face aceste identificări inclusiv pe baza certificatelor digitale .

RADIUS Server – RADIUS este un protocol și un software client-server care permite accesarea de la distanță a unui dispozitiv (controler, acces point) să comunice cu un server central pentru a autentifica utilizatorii și pentru a le acorda acces la resurse prin autorizarea acestuia în funcție de accesul solicitat.

IEEE 802.1X și RADIUS – Acesta este un protocol de criptare a datelor cu ajutorul unui server Radius. Capacitatea de integrare cu LDAP reprezintă un avantaj pentru organizații, asigurând o gestionare optimizată a autentificării și controlului accesului în întreaga infrastructură IT. Este de foarte multe ori regăsit în literatura de specialitate și sub denumirea de WPA2 Enterprise. Impreună cu EAP-TLS creează premisele unei rețele fără fir foarte eficientă din punct de vedere al securității.

Avantajul major al acestui sistem constă în faptul că autentificarea nu se bazează pe simple parole, ci pe certificate individuale, semnate de o autoritate de certificare, reducând semnificativ riscul compromiterii accesului prin metode brute-force sau phishing. În mediile enterprise, această arhitectură este completată adesea de politici de acces bazate pe roluri, care restricționează resursele disponibile în funcție de identitatea utilizatorului și nivelul său de privilegii. În plus, integrarea cu infrastructuri deja existente, precum Active Directory, permite o gestionare mai simplă pentru un răspunsprompt în caz de incidente.

4.3 Protocoale de autentificare

- LEAP - Este un protocol dezvoltat de către CISCO. Sistemul utilizează o variantă adaptată a protocolului MS-CHAP, care, deși asigură autentificarea, prezintă vulnerabilități în criptarea credențialelor. Din această cauză, se recomandă implementarea unor parole complexe pentru a compensa slăbiciunile de securitate inerente.
- EAP-FAST - Acesta folosește două faze pentru autentificare. În prima fază inițierea se face printr-un handshake TLS și ridică un tunel pentru a face un schimb de chei protejat între client și serverul de autentificare. Odată ce tunelul de comunicație este stabilit cu succes, procesul intră în etapa secundară de autentificare, unde se verifică credențialele specifice utilizatorului sau dispozitivului. Clientul și serverul stabilesc celelalte politici de autorizare și autentificare. Acesta oferă o gamă largă de configurații cu ajutorul cărora se pot stabili reguli clare. Inclusiv dacă se folosesc certificate sau nu.
- PEAP - Este un protocol care încapsulează EAP intr-un tunel TLS criptat și autentificat. Procesul funcționează ca o verificare dublă:
- Prima fază - mai întâi se configurează un canal criptat.
- Faza doua - se completează autentificarea propriu-zisă.

- EAP-TLS - la nivel internațional este văzut ca fiind o tehnică de securizare a datelor foarte eficientă datorită faptului că autentificarea dispozitivelor este reciprocă fiind necesar ca atât serverul cât și clientul să dețină certificate pentru autentificare. Apoi după ce aceste certificate sunt identificate se va crea chei pentru sesiunea respectivă și pe care dispozitivele le vor folosi pentru a încheia autentificarea. Acest tip de autentificare este eficient în special împotriva unui atac foarte întâlnit : Man in the middlle. Este eficient și datorită faptului că arată cine accesează rețeaua la orice moment dat deoarece autentificarea prin acest protocol se bazează pe certificatele digitale încorporate în fiecare dispozitiv.Practic autentificarea se simplifică și este și mai sigură pentru faptul că sunt folosite certificaele digitale.
- EAP-TTLS - spre deosebire de precedentul protocol, acesta folosește două faze de autentificare. În prima fază se folosec procedurile TLS standard, după care folosește un tunel creat pentru client unde acesta se autentifică la server prin intermediul EAP, PAP sau MSCHAP.
- EAP-TTLS/PAP – reprezintă o variantă hibridă de autentificare ce combină securizarea transportului și mecanismul de autentificare. Problema aici apare prin faptul că parolele sunt transmise prin text simplu necriptat putând fi cu ușurință interceptate și folosite de persoane rău intenționate prin folosirea acestora. Totodată procesul de configurare este dificil (Raj n.d.). Este nevoie de o persoană cu cunoștințe avansate pentru a configura acest protocol și dacă lăsăm configurarea pe dispozitivele finale în baza utilizatorilor, se poate spune că este o idee proastă deoarece pot interveni eventuale întârzieri și de aici în lanț pot surveni alte probleme.
- EAP-TTLS/MSCHAP- Acesta este un protocol PPP care este activat prin negocierea algoritmului CHAP. Serverul de acces solicită clientului o provocare de la egal la egal și un răspuns de autentificare pe care sunt suprapuse pachetele „Răspuns” și „Succes” pentru a facilita autentificarea reciprocă. Totodată și clientul trimite solicitare către server prin care solicită acestuia să demonstreze că știe parola utilizatorului. În caz că acesta nu va răspunde cererii, clientul va întrerupe în mod automat conexiunea.

4.4 Metode pentru protecția WI-FI :

- ✓ Schimbarea parolei de acces la un interval cât mai mic de timp;
- ✓ Dezactivarea transmisiei publice cu numele rețelei;
- ✓ Implementarea filtrării MAC;
- ✓ Implementarea protocolului 802.1.X;
- ✓ Implementarea certificatelor digitale;
- ✓ Folosirea TLS;
- ✓ Limitarea puterii semnalului reduce vizibilitatea rețelei în zone neautorizate, minimizând riscul de interceptare.
- ✓ Segmentarea rețelei prin VLAN-uri izolează dispozitivele sensibile, prevenind accesul lateral în caz de breșă.
- ✓ Monitorizarea traficului în timp real permite detectarea rapidă a activității suspecte sau a intruziunilor.

- ✓ Actualizarea firmware-ului ruterelelor și punctelor de acces închide vulnerabilități cunoscute, sporind rezistența la exploitări.
- ✓ Dezactivarea serviciilor inutile (ex: UPnP, WPS) elimină potențiale puncte slabe în configurarea dispozitivelor.
- ✓ Politicile stricte de parole măresc dificultatea spargerii acestora prin atacurile brute-force.
- ✓ Autentificarea cu doi factori adaugă un strat suplimentar de securitate, chiar dacă parola este compromisă.
- ✓ Izolarea clienților într-o rețea wireless previne comunicarea directă între dispozitive.
- ✓ Logarea evenimentelor de autentificare și acces.
- ✓ Testarea periodică a securității prin scanare de vulnerabilități.
- ✓ Blocarea adreselor IP suspecte.
- ✓ Backup-ul configurațiilor asigură recuperarea rapidă în caz de defecțiune sau atac fiind o foarte buna politică de implementat în caz de dezastru

Pentru a asigura securitatea rețelelor Wi-Fi, este esențială adoptarea mai multor măsuri complementare. În primul rând, schimbarea regulată a parolei de acces previne accesul neautorizat în cazul în care aceasta ar fi compromisă, limitând astfel perioada în care un atacator poate exploata rețeaua

Capitolul 5

Arhitectură Wireless pentru securizarea IoT

5.1 Arhitectura propusă

În cadrul acestui proiect, am realizat un sistem de securitate destinat dispozitivelor IoT, utilizând două plăci Raspberry Pi. Prima placă găzduiește un server FreeRadius, responsabil cu autentificarea utilizatorilor conectați la rețeaua Wi-Fi. A doua placă este destinată conectării dispozitivelor IoT wireless care nu suportă protocolul 802.1X.

Pentru analiza performanței conexiunilor stabilite, a fost utilizată aplicația Iperf3. Un aspect important în realizarea securității la nivelul dispozitivelor este utilizarea unei punți logice între interfața wireless și cea Ethernet, permițând astfel redirecționarea pachetelor la nivelul 2 al modelului OSI. În acest mod, comunicarea cu rețeaua wireless securizată a oricărui dispozitiv I.o.T. se poate realiza prin intermediul ethernet.

5.2 Montaj experimental

Pentru a realiza o comunicație securizată, am realizat montajul experimental: două plăcuțe de dezvoltare Raspberry Pi, un ruter Asus și un dispozitiv IoT. In montajul propus am folosit un laptop în postura de IoT. Acest montaj permite testarea în condiții reale a unui scenariu frecvent întâlnit în mediile industriale sau casnice inteligente, unde anumite dispozitive nu pot fi modificate pentru a susține protocoale avansate de autentificare, dar trebuie totuși integrate într-o rețea securizată. Primul pas a fost instalarea unui sistem de operare care a fost folosit de plăcuța Raspiberry Pi folosit pentru rularea FreeRadius, respectiv o versiune de linux pentru Raspiberry PI pentru a mă folosi de protocolul WPA 2 Enterprise.

În arhitectura propusă sunt foarte importante cele două placuțe care gazduiesc elementele principale. Este nevoie de un server Radius, un autentificator (controler wireless sau Acces-Point), un dispozitiv care face translatare de pachete (bridge) și clienți (dispozitive IoT)..

Pentru ca un client să se conecteze la o rețea wireless și pentru a iniția o conexiune este necesar ca acesta să fie capabil de a folosi protocolul 802.1.x. Primul pas a fost instalarea FreeRadius.Apoi pasul doi a fost să introduc adresa IP a autentificatorului (Acces Point sau controloer Wi-Fi) și parola care va fi folosită pentru autentificarea acestuia). În acest moment am creat o rețea Wi-Fi securizată prin intermediul protocolului wpa2-enterprise sau prin intermediul protocolului 802.1x

Încă de la început trebuie spus că pentru ușurința testului am folosit o conexiune securizată bazată doar pe username și parolă fără a folosi certificate digitale. În momentul în care această conexiune este funcțională nu mai rămâne de făcut nimic altceva decât să creez și să implementez și aceste certificate digitale pentru a spori securitatea conexiunii.

Dispozitivul propus pentru a securiza conexiunile între dispozitive de tip mai vechi care în mod normal nu pot fi folosite cu protocolul 802.1X și rețeaua constituită:

O altă plăcuță Raspberry-Pi 4 cu ajutorul căreia am conectat un dispozitiv de tip IoT ce are în componență o conexiune de tip Ethernet. Adică orice dispozitiv pe care îl voi conecta la topologie, o voi face prin intermediul unui patch-cord de la placa de rețea ethernet a Raspberry-Pi la placa de rețea a respectivului dispozitiv.

5.3 Concluzii

Prin intermediul acestui tip de arhitecturi am realizat conexiune securizată între dispozitivul IoT (laptop) și rețeaua fără fir securizată. Consider că am realizat ceva foarte util pentru a interconecta diferite dispozitive într-un mod securizat folosindu-mă de protocolul 802.1x. De reținut este și faptul că prin aceastp arhitectură se realizează un consum foarte scăzut de energie.

Pentru a aduce un plus de securitate, se va dezactiva SSID-ul din panoul de configurare al Acces-Point-ului și se vor introduce certificate digitale atât pe server cât și pe clienții care se vor conecta la rețeaua Wi-Fi acest lucru făcând ca rețeaua astfel setată să fie aproape imposibil de penetrat. Ca și o ultimă concluzie spun că deși sunt mai multe lucrări care tratează despre un “bridge” între Wi-Fi și Ethernet, nici una dintre acestea nu folosește rețeaua fără fir securizată prin intermediul 802.1

Capitolul 6

Sistem de autentificare Wi-Fi prin blockchain

6.1 Autentificarea Wi-Fi

Din imensul spaţiu care priveşte securitatea cibernetică eu am ales să atac zona care priveşte securitatea wireless. Pentru a creşte securitatea sunt disponibile şi la îndemână o mulţime de unelte cu ajutorul cărora să putem reaaliza acest lucru având în vedere câte de complex este domeniul securităţii.

Când discutăm despre securitatea unei reţele, partea tehnică este întodeauna cea care atrage atenţia însă nu trebuie uitată protecţia fizică care de multe ori joacă un rol determinant în acest domeniu. Totodată trebuie luată în seamă şi partea administrativă care ajută la atribuirea de roluri şi de stabilire a acesului fiecărui utilizator doar către partea la care are acces pentru a-şi desfăşura activitatea.

Acest lucru l-am realizat prin folosirea blockchain-ului, ceea ce este o inovație în domeniu. La ora actuală acest tip de autentificare într-o rețea Wi-Fi nu este încă folosită. Așadar prin introducerea acestui tip de autentificare împreună cu implementrea certificatelor digitale, se realizează o securitate aproape impenetrabilă.

Prin implementarea smart contractelor se realizează automatizarea autentificării și autorizării, astfel reducându-se riscul accesului neautorizat. Pentru realizarea experimentului am creat o topologie formată din: o plăcuță Raspberry Pi pe care am Instalat FreeRadius și blockchain-ul Ganache iar aceasta este conecatată prin ethernet la ruterul Asus pe care l-am folosit pe post de autentificator Hash-urile generate din certificatele digitale au fost stocate în blockchain, permițând verificarea identității fără a mai depinde de o bază de date centralizată. Astfel, se elimină un punct critic de vulnerabilitate și se crește reziliența rețelei în fața atacurilor de tip spoofing sau falsificare de identitate. De asemenea, utilizarea FreeRADIUS asigură compatibilitatea cu protocoalele standard de autentificare, facilitând integrarea în infrastructura deja existentă. În plus, utilizarea smart contractelor permite aplicarea automată a politicilor de acces, fără a fi necesară intervenția manuală. Acest lucru reduce semnificativ erorile umane și crește eficiența procesului de control al accesului.

6.2 Crearea certificatelor digitale

Pe măsură ce rețelele IoT, infrastructurile critice și sistemele industriale devin tot mai interconectate, devine esențial faptul ca fiecare dispozitiv să fie identificat și autentificat într-un mod securizat. Pentru a preveni accesul neautorizat, soluțiile actuale implementează protocolul TLS alături de certificate digitale emise de o entitate de încredere, cunoscută sub numele de Autoritate de Certificare.

O Autoritate de Certificare este o instituție de încredere care confirmă identitatea diverselor entități și le furnizează certificate digitale. Prin semnarea acestor certificate cu propria sa cheie privată, autoritatea de certificare asigură autenticitatea identității respectivei entități. Această metodă oferă un nivel ridicat de încredere în comunicarea dintre dispozitive, garantând că datele transmise provin din surse verificate.

Funcțiile principale ale unei CA în raport cu dispozitivele conectate sunt:

- Verifică identitatea producătorului/dispozitivului.
- Emite un certificat digital personalizat.
- Permite validarea identității acelui dispozitiv într-un sistem.
- Un certificat digital este un document electronic care leagă o cheie publică de identitatea unui dispozitiv. Este semnat de o CA și conține:

Informații despre dispozitiv.
Cheia publică a dispozitivului.
Informații despre CA-ul emitent.
Perioada de valabilitate.
Semnătura digitală a CA-ului.

Autentificarea se realizează printr-un proces numit TLS mutual authentication, în care atât serverul, cât și dispozitivul își dovedesc identitatea cu certificate semnate de o autoritate de certificare de încredere.

Procesul de pregătire.
Dispozitivul generează o pereche de chei: una privată și una publică.

Pentru realizarea experimentului am instalat pe o plăcuța Raspberry Pi softul FreeRadius și blockchain-ul folosit și pentru teste Ganache pentru a stoca hash-urile generate din certificatele digitale create. Totodată am și creat o autoritate de certificare pentru a semna certificatele digitale. Primul pas a fost să creez autoritatea de certificare folosindu-mă de OpenSSL.

6.3. Determinarea folosirii EAP

Pentru a folosi autentificarea prin intermediul protocolului TLS am modificat secțiunea “authorize” din cadrul fișierului sites-enabled care este folosit de FreeRadius. Am introdus secțiunea check_blockchain prin care se inițializează verificarea hash-urilor stocate în blockchain-ul local Ganache. După vrificarea acestora prin intermediul scriptului Python, daca răspunsul returnează orice diferit de 0 atunci se va transmite autentificatorului mesajul „reject”. Dacă însă mesajul va fi 0 atunci se va transmite autentificatorului mesajul „acces acepted”.

6.4. Implementare script Python

Acesta în primă fază citește certificatul, apoi calculează hash-ul certificatului după care adaugă prefixul 0x în fața hash-ului deja calculat pentru a-l compara în formatul deja depozitat, după care se conectează la blockchain-ul local și generează compararea hash-ului calculat cu cel deja stocat în blockchain. Apoi dacă acesta returnează 0 atunci certificatul este identic cu unul din cele înmagazinate anterior iar dacă acest lucru nu este real atunci va returna valoarea 1.

6.5. Generarea hash-urilor din certificatele digitale

Pentru a genera has-urile din certificatele digitale generate pentru clienți am folosit comanda openssl x509 -in cez.crt -outform DER | sha256sum | awk '{print $1}'. Așadar am creat aceste hash-uri în mod manual prin introducerea în consolă a comenzii. În urma aplicării se generează un hash folosind ultilitarul OpenSSL pentru certificatele existente. Prima parte a comenzii "-in cez.crt", specifică fișierul certificatului de intrare, în format PEM (cel mai frecvent: codificat Base64 cu -----BEGIN CERTIFICATE-----). Parametrul „-outform DER" convertește certificatul din format PEM în format binar DER. Ulterior, comanda sha256sum calculează amprenta digitală a certificatului în format DER, iar awk extrage doar valoarea hash-ului, care este apoi stocată pe blockchain pentru validare ulterioară., necesar pentru obținerea unui hash precis și unitar al conținutului certificatului. Apoi partea "-outform DER", convertește certificatul din format PEM în format binar DER, care este o formă larg utilizată pentru generarea hash-urilor. Iar prin partea "awk '{print $1}'" se extrage doar has-ul generat ignorând numele fișierului.

6.6. Stocarea hash-urilor în Ganache

Prin intermediul Remix Etherium am stocat hash-urile generate anterior în Ganache. Acesta este un instrument util în dezvoltarea de aplicații Ethereum, deoarece generează automat mai multe conturi blockchain cu solduri prestabilite de Ether de test. Acest Ether nu are valoare reală, permițând efectuarea de teste fără costuri. Interacțiunea cu această rețea locală simulată este extrem de rapidă, iar fiecare tranzacție și eveniment poate fi urmărit în timp real. Astfel, dezvoltatorii pot testa funcționalitatea contractelor inteligente într-un mediu controlat și predictibil. În cadrul proiectului meu, am utilizat această rețea locală pentru a simula stocarea și verificarea hash-urilor generate din certificatele digitale. Acest proces asigură că identitatea fiecărui client poate fi validată în mod sigur, fără a expune datele sensibile. Cu ajutorul Remix Etherium am scris un smart contract în care am stocat has-urile

generate anterior din certificatele digitale pentru ca apoi prin intermediul scriptului Python în timpul autentificării unui dispozitiv FreeRadius să verifice suplimentar și dacă has-ul generat din certificatul digital prezentat de dispozitiv este identic cu hash-ul depozitat in blockchain.

Capitolul 7

Concluzii

7.1. Rezultate obținute

Rezultatele pe care le-am obținut în urma integrării acestor tehnologii pentru securizarea IoT într-o rețea Wi-Fi sunt:

Securitate foarte ridicată prin folosirea certificatelor digitale și a tehnologiei blockchain astfel în acest mod crescând rezistența la atacuri.

Consumul de energie foarte scăzut datorită folosirii plăcuțelor RaspberryPi.

Reducerea costurilor prin implementarea contractelor inteligente cu ajutorul cărora se automatizează procesul de autentificare reducând intervenția umană, astfel reducându-se și costurile.

7.2. Contribuții originale

În cadrul acestei lucrări am proiectat și implementat o topologie de rețea securizată, caracterizată printr-un consum energetic minim, costuri reduse de implementare și cerințe hardware modeste. Acest lucru l-am realizat prin utilizarea plăcuțelor RaspberryPi, în combinație cu aplicații software open-source, care nu presupun achiziționarea unor licențe comerciale.

Totodată, procesul de autentificare a fost extins și personalizat prin intermediul limbajelor de programare Python și Solidity. Acestea au fost utilizate pentru dezvoltarea unor module funcționale care permit atât controlul logic al autentificării, cât și integrarea cu un smart-contract integrat în blockchain.

Elementul inovator al arhitecturii propuse constă în consolidarea mecanismului de securitate prin adăugarea unui strat suplimentar de protecție în faza de autentificare a dispozitivelor în rețea. Mai precis, au fost generate amprente (hash-uri) ale identităților utilizatorilor, care sunt stocate într-un contract inteligent pe blockchain. Verificarea acestor amprente este realizată automat, printr-un script personalizat, dezvoltat în Python și integrat în fluxul de autorizare al serverului FreeRadius. Acest mecanism asigură o autentificare descentralizată, verificabilă și rezistentă la manipulare, sporind considerabil nivelul de încredere și securitate al rețelei.

7.3. Lista lucrărilor originale

Pe toată perioada stagiului doctoral au fost publicate zece articole din care șase ca prim autor.

[1] C.-G. Dumitrache, C. V. Marian, G. Predusca, F.M. Barbu, M. Neferu, "Wireless Authentication System for Internet of Things using FreeRADIUS and Blockchain," RRST-EE, Vol. 70 No. 4, 2025, doi: https://doi.org/10.59277/RRST-EE.2025.4.26

[2] C.-G. Dumitrache and P. Anghelescu, "Design and Implementation of a Secure Communication Architecture for IoT Devices," JSAN, vol. 14, no. 4, p. 64, Jun. 2025, doi: 10.3390/jsan14040064.

[3] C.-G. Dumitrache, G. Gheorghe, P. Gabriel, and G. Mariuca-Roxana, "Device For Securing IoT In The Wireless Environment," in 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Iasi, Romania: IEEE, Jun. 2024, pp. 1–6. doi: 10.1109/ecai61503.2024.10607458.

[4] C.-G. Dumitrache, C. A. Ghita, G. Predusca, L. D. Circiumarescu, N. Angelescu, and D. C. Puchianu, "The Efficiency of Routing Protocols, OSPF and EIGRP, Using Graphical Network Simulator-3 and Python," in 2024 28th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania: IEEE, Oct. 2024, pp. 194–199. doi: 10.1109/icstcc62912.2024.10744665.

[5] C.-G. Dumitrache, G. Predusca, G. Gavriloaia, N. Angelescu, D. Circiumarescu, and D. C. Puchianu, "Comparative analysis of routing protocols using GNS3, Wireshark and IPerf3," in 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Ploiesti, Romania: IEEE, Jun. 2022, pp. 1–6. doi: 10.1109/ecai54874.2022.9847499.

[6] C. G. Dumitrache, G. Predusca, L. D. Circiumarescu, N. Angelescu, and D. C. Puchianu, "Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer," in 2017 5th International Symposium on Electrical and Electronics Engineering (ISEEE), Galati: IEEE, Oct. 2017. doi: 10.1109/iseee.2017.8170694.

[7] A. Frâncu, G. Preduşcă, L. D. Cîrciumărescu, N. Angelescu, D. C. Puchianu, and C.G Dumitrache, "Examining IP Network Routing Protocols with Packet Tracer and Cisco Equipment," The Scientific Bulletin of Electrical Engineering Faculty, vol. 25, no. 1, pp. 68–73, Jun. 2025, doi: 10.2478/sbeef-2025-0011.

[8] S. Cristian, P. Gabriel, C. Denisa, A. Nicoleta, P. Dan, and C.-G. Dumitrache, "Analysis of web traffic using MPLS technology," in 2022 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania: IEEE, Nov. 2022, pp. 1–4. doi: 10.1109/isetc56213.2022.10009987.

[9] A. Frâncu, G. Predușcă, L. D. Cîrciumărescu, N. Angelescu, D. C. Puchianu, and C.-G. Dumitrache, “Examining IP Network Routing Protocols with Packet Tracer and Cisco Equipment,” The Scientific Bulletin of Electrical Engineering Faculty, vol. 25, no. 1, pp. 68–73, Jun. 2025, doi: 10.2478/sbeef-2025-0011.

[10] G. Predușcă, D. Circiumarescu, C.-G. Dumitrache, and C. Stănescu, “Analysis of a Fiber Optical Link Using Octave,” The Scientific Bulletin of Electrical Engineering Faculty, vol. 22, no. 1, pp. 1–6, Jul. 2022, doi: 10.2478/sbeef-2022-0007.

[11] C. Stănescu, G. Predușcă, D. Circiumarescu, and C.-G. Dumitrache, “Determination of Distance in Fiber Optical Communications Networks,” The Scientific Bulletin of Electrical Engineering Faculty, vol. 22, no. 1, pp. 1–6, Jul. 2022, doi: 10.2478/sbeef-2022-0012.

7.4. Perspective de dezvoltare ulterioară

O posibilă extindere a funcționalităților propuse pentru această lucrare constă în implementarea unui mecanism suplimentar de securitate bazat pe identificatori hardware unici. Mai exact, generarea unui hash suplimentar, derivat din adresa MAC a dispozitivului care solicită accesul la rețea. Acest hash ar putea fi stocat în blockchain, alături de celelalte informații de autentificare, consolidând astfel arhitectura de control al accesului.

Prin includerea acestui element de identificare fizică, se adaugă un strat suplimentar de verificare, ceea ce face semnificativ mai dificilă, dacă nu chiar imposibilă, pătrunderea în rețea a unui dispozitiv neautorizat, chiar și în scenarii în care datele de autentificare ar fi compromise. Mecanismul propus ar spori nu doar securitatea generală a sistemului, ci și reziliența acestuia la atacuri de tip spoofing sau man-in-the-middle.