UNIVERSITATEA NATIONALA DE STIINTA SI TEHNOLOGIEPOLITEHNICA BUCURESTI

Facultatea de Stiinte Aplicate
Teoria Codarii si Stocarii Informatiei

TEMA PROIECT:

Securitatea rețelelor comunicațiilor 5G

COORDONATOR STIINTIFIC:

OPRINA Andrei

Student masterand:

GAVRILA Eduard-Andrei

Cuprins

1. Introducere

Prin definirea comunicației se înțelege transmisia la distanță de informații tip voce, text, imagine statică sau dinamică sau transmisii multimedia. Pentru a comunica, suportul transmisie poate fi un cablu, reprezentând un conductor electric, fibra, reprezentând un conductor optic, dar și spațiul liber, prin unde radio sau raze de lumină în infraroșu.

Datorită evoluției neașteptate a comunicațiilor mobile, rețelele au fost dezvoltate de la rețele 2G pana la inovațiile rețelelor 5G. Evoluția comunicațiilor mobile definește modul în care ne conectam datorită progresiei continue a tehnologiei, dar a reușit și dezvoltarea unei varietăți de aplicații și servicii, care au ajuns să definească modul în care se interacționează cu lumea din jur. Nu numai că s-a ajuns la dezvoltarea de aplicații și servicii, dar descoperirea și optimizarea rețelelor 5G a ajuns să satisfacă cerințele tot mai mari ale utilizatorilor, datorită utilizării în viața cotidiană.

1.1. Evoluția comunicațiilor mobile

- 1G – Sistemele 1G, lansate în anii 1980, reprezintă începutul comunicațiilor mobile, primul sistem 1G comercial a fost NMT(Nordic Mobile Telephone) și AMPS(Advanced Mobile Phone System) pentru Statele Unite ale Americii. Pentru a transmite vocea, sistemele 1G foloseau modularea de frecvență, acestea fiind complet analogice, neavând servicii de date și capacitate limitată, având calitatea sunetului scăzută. Securitatea acestor sisteme deținea probleme majore, semnalele nefiind criptate. Dimensiunile mari ale telefoanelor, costurile ridicate și capacitățile limitate ale rețelei au facut acest sistem ca fiind limitat.
- 2G - Aceste sisteme au fost introduse în anii 1990, fiind o tranziție majora la tehnologiile digitale, standardul predominant fiind GSM(Global System fo Mobile Communications). Criptarea semnalelor si eficiența spectrului radio au fost datorate tehnicilor de multiplexare prin diviziune temporală(TDMA) și acces multiplu prin diviziune de cod(CDMA). O dată cu apariția acestor sisteme, au fost introduse serviciile SMS și transferuri limitate de date.
- 3G - Cu apariția acestor sisteme în anii 2000, a fost îmbunătațită viteza de transfer a datelor și capacitatea rețelei. Folosirea tehnicilor avansate de CDMA și multiplexare prin diviziune de frecvență(FDM) au permis viteze de transfer de date de la 2Mbps până la 14.4 Mbps cu HSPA(High Speed Packet Access). Serviicle au fost îmbunătățite prin acces la internet, e-mail, videoconferințe și aplicații multimedia.
- 4G – Sistemele 4G au apărut ca răspuns a cerințelor tot mai mare în ceea ce privește transferul de date, standardele principale fiind LTE(Long Term Evolution) si LTE-A(LTE-Advanced). Pentru creșterea eficienței

spectrului si capacității rețelei au fost utilizate OFDMA(Orthogonal Frequency Division Multiple Access) și MIMO(Multiple Input Multiple Output). Nu numai că viteza de 1 Gbps a fost atinsă, dar aceste sisteme au facilitat apariția streamingurilor video de înaltă calitate (HD și 4K), jocurilor online, realitate augmentată și virtuală.

- 5G- Sistemele 5G reprezintă cea mai recentă evoluție a comunicațiilor mobile, create pentru a susține o gamă largă de aplicații și servicii avansate. Tehnologia utilizată în sistemele 5G este dată de utilizarea frecvențelor milimetrice, beamforming, massive MIMO și networc slicing pentru viteze mari de transfer de până la 10 Gbps și latență sub o milisecundă. Codarea avansată a canalului, cum ar fi LDPC și Polar Codes, asigură fiabilitatea și eficiența transmisiei datelor. Cu ajutorul acestor sisteme, serviciile în care sunt utilizate sunt Internet of Things(IoT), vehicule autonome, telemedicină, VR, permițând o conectivitate foarte bună în timp real. Impactul pe care aceste sisteme l-a avut a fost impresionant, transformând infrastructurile de comunicații, creșterea economiei digitale, îmbunătățirea serviciilor publice și a vieții prin aplicații inteligente și interconectate.

Generație	Tehnologie	Inovații
1G	NMT,AMPS	Comunicații analogice
2G	GSM, cdmaOne	Digitalizare, SMS, criptare
3G	UMTS, CDMA2000	Internet mobil și videoconferințe
4G	LTE, LTE-A	Streaming HD, jocuri online, realitate augmentată
5G	NR(New Radio)	IoT, latență ultra-redusă, vehicule autonome

1. Evoluția rețelelor mobile

Evoluția comunicațiilor mobile a fost marcată de tranziții tehnologice majore și inovații care au revoluționat modul în care interacționăm cu lumea din jurul nostru. Fiecare generație a adus îmbunătățiri semnificative în viteza, în capacitatea și fiabilitatea rețelelor de comunicații.

2. Importanța 5G în viața de zi cu zi

1.2. Necesitatea securitatii in retelele de comunicatii

În contextul actual al dezvoltării tehnologice rapide și al dependenței din ce în ce mai mari de tehnologia informației și comunicațiilor, securitatea rețelelor de comunicații reprezintă o prioritate absolută. Rețelele de comunicații sunt absolut necesare pentru funcționarea statului modern, asigurând transferul rapid al informațiilor esențiale pentru instituțiile publice, pentru companii și pentru cetățeni. Din acest motiv, protejarea lor împotriva atacurilor cibernetice a devenit o necesitate.

Creșterea numărului, volumului și complexității atacurilor cibernetice reprezintă o dovadă clară a vulnerabilității rețelelor de comunicații. Atacurile de tip DDoS (Distributed Denial of Service) au ca scop întreruperea accesului public la site-urile web ale unor instituții esențiale. Acest tip de atac urmărește să creeze confuzie și panică în rândul populației și să submineze încrederea cetățenilor în capacitatea statului de a-i proteja. Într-o lume conectată, astfel de întreruperi pot afecta nu doar accesul la informații, ci și funcționarea eficientă a serviciilor publice.

Atacurile nu sunt surprinzătoare având în vedere contextul, dar, cu toate acestea, ele subliniază importanța măsurilor proactive și reactive pentru a asigura securitatea rețelelor de comunicații.

Un alt aspect critic este necesitatea unei cooperări strânse între instituțiile guvernamentale și echipele de răspuns la incidente. Orice tip de atac

demonstrează că răspunsul eficient depinde de o reacție rapidă și coordonată. Schimbul rapid de informații între echipele de securitate și administratorii tehnici poate reduce semnificativ impactul unui atac. Totodată, este nevoie de investiții constante în infrastructură și în soluții de protecție cibernetică pentru a menține un nivel adecvat de securitate în fața amenințărilor în continuă evoluție.

De asemenea, resursa umană joacă un rol esențial în securizarea rețelelor de comunicații. Specialiștii în securitate cibernetică trebuie să fie bine pregătiți și motivați pentru a face față noilor amenințări. Este esențială dezvoltarea continuă a competențelor acestora prin programe de formare și perfecționare.

1.3. Importanța securității în rețelele 5G

Având în vedere utilizarea critică a rețelelor 5G, importanța securității rețelelor 5G este foarte importantă, având în vedere implicațiile pe care le poate avea o breșă de securitate sau un atac cibernetic asupra funcționării societății și siguranței cetățenilor.

Rețelele 5G sunt de-a dreptul o revoluție tehnologică, dată fiind viteza mare, latența redusă și capacitatea mare de conectare a dispozitivelor simulat. O data cu apariția acestor rețele, noi orizonturi au fost deschise în domenii precum:

- Medicina și telemedicina
  - Este permisă realizarea de intervenții chirurgicale de la distanță, monitorizarea pacienților în timp real și gestionarea eficientăa datelor de sanate
- Transportul autonom
  - Deoarece vehiculele autonome nu comunică doar între acestea, ci și cu infrastructura inteligentă din trafic, este necesară o latență extrem de mică pentru a lua decizii în timp real
  - Interferențele în rețea pot cauza întârzieri în comunicare, iar atacurile cibernetice pot compromite sisstemele de control ale vehiculelor
- Industria 4.0
  - Integrează tehnologii avansate pentru IoT(Internet of Things) și inteligența artificiala(AI)

- Rețelele 5G oferă o viteză mare, o latență redusă și o multitudine de dispozitive conectate simultan, ceea ce duce la transformarea procesului de producție și automatizarea acestora
- Securitatea este esențială mai ales în funcționarea eficientă a fabricilor, unde sistemele și mașinile comunică și se coordonează autonom

2. Evoluția rețelelor mobile

2.1. Principalele caracteristici ale tehnologiilor anterioare

De la primele rețele 1G, evoluția rețelelor mobile a marcat o schimbare semnificativă în modul de comunicare și interacționare cu tehnologia. Pornind de la 1G, acestea au permis doar convorbiri telefonice simple, introduse in anii 1980 și au continuat până la apariția telecomunicațiilor digitale 2G. Diferența majoră dintre aceste 2 generații este că semnalele radio utilizate de rețeaua 1G sunt analogice, iar rețelele 2G sunt digitale, dar și apariția sms-urilor.

În anii 2000, rețelele 3G au crescut viteza de transfer al datelor și au permis utilizatorilor să acceseze internetul și aplicații multimedia, iar 4G, cu viteze de până la 1 Gbps, a deschis drumul pentru streaming de înaltă calitate și jocuri online.

Tehnologia 5G reprezintă apogeul evoluției rețelelor mobile, oferind viteze de transfer de până la 10 Gbps, o latență extrem de mică și capacitatea de a conecta milioane de dispozitive simultan. Tehnologiile esențiale din spatele 5G, precum utilizarea frecvențelor milimetrice, massive MIMO și beamforming, permit o performanță superioară, reducând interferențele și îmbunătățind acoperirea rețelelor. De asemenea, tehnologia de network slicing permite crearea unor rețele virtuale dedicate, care răspund nevoilor specifice ale diferitelor aplicații critice, cum ar fi vehiculele autonome sau telemedicina.

2.2. Caracteristici ale 5G

Tehnologia 5G aduce o serie de caracteristici inovative care o diferențiază semnificativ de generațiile anterioare de rețele mobile. Aceste caracteristici nu doar că îmbunătățesc experiența utilizatorilor, dar și susțin dezvoltarea unor tehnologii și aplicații critice, care nu ar fi fost posibile fără capacitățile avansate ale 5G. Cele mai importante caracteristici ale rețelelor 5G sunt:

- Viteza mare de transfer
  - 5G atinge viteze de transfer de date de până la 10 Gbps, de aproximativ 100 de ori mai rapide decât 4G. Această viteză mare este esențială pentru streaming-ul de înaltă calitate

(inclusiv 4K și 8K), descărcarea rapidă a fișierelor mari și îmbunătățirea experienței utilizatorilor în aplicațiile de realitate augmentată și virtuală.

- Latență redusă
  - reducerea latenței la mai puțin de 1 milisecundă. Acest lucru este crucial pentru aplicații care necesită o reacție în timp real. Latența scăzută permite ca dispozitivele conectate să reacționeze aproape instantaneu la comenzi.
- Capacitatea de a conecta un număr mare de dispozitive
  - 5G poate suporta milioane de dispozitive conectate simultan. Acest lucru este esențial pentru dezvoltarea Internet of Things (IoT), unde mii de dispozitive inteligente trebuie să fie conectate și să comunice între ele.
- Eficiență energetică
  - Rețelele 5G sunt concepute pentru a fi mai eficiente din punct de vedere energetic, permițând dispozitivelor să consume mai puțină energie în comparație cu tehnologiile anterioare, în special în cazul dispozitivelor conectate continuu la rețea.
- Flexibilitatea rețelelor
  - Network slicing: această tehnologie permite crearea unor „rețele virtuale” dedicate pentru aplicații specifice, fiecare cu cerințe proprii de viteză, latență și securitate.
- Tehnologii avansate de antene
  - Massive MIMO și beamforming: Massive MIMO (Multiple Input, Multiple Output) și beamforming sunt tehnologii care permit rețelelor 5G să gestioneze mai multe semnale simultan și să transmită date către utilizatori din diferite direcții.
- Utilizarea frecvențelor milimetrice
  - 5G utilizează banda de frecvențe milimetrice (de la 24 GHz până la 100 GHz). Aceste frecvențe permit o capacitate mai mare de transmisie a datelor, dar au o acoperire mai limitată și o penetrare mai mică a pereților.

3. Provocările de securitate în rețelele 5G

În ceea ce privește implementarea rețelelor 5G, tehnologia a deschis noi orizonturi, dar a adus și o serie de provocări de securitate ce necesită o atenție sporită. În ciuda beneficiilor semnificative, rețelele 5G sunt expuse unor riscuri de securitate, iar protejarea datelor și infrastructurilor devine o prioritate esențială. Printre principalele provocări se numără atacurile cibernetice, protecția confidențialității și securitatea dispozitivelor IoT.

3.1. Atacuri Cibernetice

Pe măsură ce rețelele 5G permit o conectivitate mult mai extinsă, acestea devin ținte pentru atacuri cibernetice sofisticate. Atacatorii pot exploata vulnerabilitățile rețelelor 5G pentru a lansa diverse tipuri de atacuri, care pot paraliza infrastructurile sau ataca serverele de bază care gestionează datele rețelei. În plus, atacurile de phishing și malware pot fi folosite pentru a compromite dispozitivele conectate și pentru a intercepta datele sensibile. Atacurile la nivelul rețelei 5G pot include interferențe cu semnalele, accesul neautorizat la rețele sau chiar sabotaje de infrastructură, având un impact semnificativ asupra stabilității rețelelor de telecomunicații și asupra utilizatorilor.

3.2. Confidențialitate și protecția datelor

Rețelele 5G permit transferuri de date mult mai mari și mai rapide, dar acest lucru rezultând o expunere crescută a datelor utilizatorilor. Datele sensibile, cum ar fi informațiile personale, istoricul de localizare și comunicațiile private, pot fi vulnerabile în fața atacurilor cibernetice sau chiar la interceptarea lor. Protecția confidențialității este esențială, iar măsurile de securitate trebuie să fie implementate riguros, inclusiv criptarea datelor, autentificarea multi-factor și controlul accesului pentru a preveni scurgerile de informații și pentru a proteja datele sensibile de accesul neautorizat.

3.3. Atacuri la nivelul rețelei

Rețelele 5G au capacitatea de a asigura o lățime de bandă mult mai mare decât predecesoarele sale și de a conecta mai multe dispozitive simultan, însă aceasta expune rețelele la atacuri cibernetice. Atacurile la nivelul rețelei pot include atât atacuri interne, din partea actorilor rău intenționați cu acces la infrastructura rețelei, cât și atacuri externe. Un exemplu pentru definirea acestor tipuri de atacuri pot fi atacurile de „interceptare a semnalului”, acestea permițând unui atacator să capteze și să manipuleze traficul de date dintre dispozitivele conectate la rețea, ceea ce duce la furtul de informații sau chiar compromiterea infrastructurii rețelei. De asemenea, riscurile la nivelul rețelei includ și vulnerabilitățile în tehnologiile de virtualizare și în managementul rețelelor care pot fi exploatate pentru a câștiga acces neautorizat.

3.4. Securitatea dispozitivelor IoT

Un alt domeniu de securitate în rețelele 5G este securitatea dispozitivelor IoT (Internet of Things), deoarece fiecare dispozitiv poate reprezenta o potențială vulnerabilitate. Dispozitivele IoT au resurse limitate, iar multe dintre ele nu dispun de măsuri de securitate suficiente, ceea ce le face vulnerabile în fața atacurilor. Aceste dispozitive pot fi utilizate ca puncte de intrare pentru atacuri, permițând atacatorilor să acceseze rețelele interne ale unei organizații sau să destabilizeze serviciile. Dispozitivele IoT beneficiază de o complexitate și o diversitate mult mai mare care duce la gestionarea și actualizarea acestora mai dificilă pentru operatorii de rețele, ceea ce poate duce la riscuri suplimentare de securitate.

3.5. Vulnerabilitățile rețelelor 5G

O dată cu dezvoltarea rețelelor 5G, acestea au o infrastructură mai complexă comparativ cu rețelele anterioare, ceea se duce la apariția unor noi vulnerabilități.

Atunci când vine vorba de vulnerabilitățile pe care acestea le dezvoltă, se poate vorbi despre:

- Arthitectura distributită și virtualizată
  - Rețelele 5G beneficiază de o arhitectură distribuită a rețelei, dar și de funcționarea virtualizată a acestora, mai exact NFV(Network Functions Virtualization). Arhitectura distribuită și virtualizată implică implementarea funcțiilor de rețea în cloud, iar acestea introduc o vulnerabilitate prin mai multe puncte de acces ce pot fi exploatate de către atacatori, date fiind nodurile de rețea, care printr-un singur atac asupra lor, pot afecta întreaga rețea
- Rețele Software-Defined
  - Această tehnologie permite gestionarea centralizată și flexibilă a traficului de date, iar un atac asupra comenzii SDN oferă oricărui atacator control asupra întregii rețele, ducând la compromiterea datelor
- Interoperabilitatea între furnizori
  - Pentru dezvoltarea rețelelor 5G este necesară colaborarea mai mult furnizori prin mai multe echipamente și servicii, având fiecare propriile standarde și metode de implementare. Dacă securitatea între echipamentele furnizorilor este neglijată, se crează o breșă ce permite pătrunderea în rețea
- Actualizarea software-ului și gestionarea patch-urilor
  - Având un număr mare de dispozitive conectate și o rețea dinamică, rețelele 5G necesită o actualizare constantă a software-ului și gestionarea patch-urilor, deoarece pot lăsa rețelele expuse în fața unui atac
- Vulnerabilități fizice
  - Infrastructura fizică a rețelelor 5G, cum ar fi stațiile de bază și echipamentele de rețea, poate fi ținta unor atacuri fizice sau sabotaje, deoarece orice acces neautorizat la aceste echipamente poate permite interceptarea traficului de date, alterarea configurațiilor și întreruperea serviciilor de comunicații.
- End-User Devices
  - Având o gamă largă de dispozitive conectate, cum ar fi smartphone-urile, dispozitive IoT sau vehicule autonome, acestea pot fi folosite ca puncte de acces pentru a ataca rețeaua centrală

Creșterea atacurilor și a încercărilor compromiterii rețelelor a dus la dezvoltarea măsurilor de protecție în vederea combaterii vulnerabilităților prin:

- Implementarea standardelor de securitate la nivel international
- Monitorizarea continua a infrastructurii
- Evaluarea periodică a riscurilor
- Colaborarea între operatori, furnizori și autoritățile abilitate

Nu doar că este dificilă gestionarea vulnerabilităților rețelelor 5G, dar aceasta necesită o coordonare constantă dar și investiții constante pentru a asigura un mediu de comunicare protejat și sigur.

3.6. Vulnerabilitatea metodelor de exploatare

În timp ce tehnologia este într-o continuă evoluție, metodele de explaotare a rețelelor 5G devin tot mai complexe, având în vedere caracteristicile avansate ale rețelelor, cum ar fi vitezele mari sau latența scăzută, ce oferă noi oportunități pentru atacatori.

Principalele vulnerabilități ce sunt asociate metodelor de exploatare, sunt:

- Exploatarea configurațiilor
  - O configurație incompletă sau greșita a echipamentelor și a software-ului rețelelor 5G duc la o exploatare avansată pentru obținerea accesului neautorizat asupra rețelei. Inorectitudinea configurării firewall-ului poate duce la permiterea atacurilor de tip Man-in-the-Middle
- Atacuri pe baza informațiilor publice
  - Informațiile publice despre arhitectură oricărei rețele și a sistemelor utilizate pot fi foarte utile pentru identificarea punctelor slabe. Tehnica de OSINT(Open Source Intelligence) permite atacatorilor indetificarea echipamentelor furnizorilor, ceea ce duce la planficicarea atacurilor precise pe baza informațiilor obținute
- Software-ul neactualizat
  - Necesitatea actualizării regulate este absolut importanta, deoarece aceasta poate elimina vulnerabilitățile de securitate descoperite. Un software neactualizat permite atacuri de tip

Remote Code Execution, atac prin care se preia controlul funcțiilor critice ale rețelei

- Atacuri pe baza inteligenței artificale
  - Având dublă utilizare, atât pentru atac cât și pentru apărare, inteligența artificială permite atacatorilor să folosească algoritmi AI pentru identificarea vulnerabilităților, ceea ce duce la creșterea eficienței atacurilor, dar și pentru dezvoltarea metodelor de deep fake pentru inducerea în eroare a sistemelor de autentificare biometrică
- Dispozitivele IoT compromise
  - Dispozitivele IoT sunt integrate în rețelele 5G, iar nesecurizarea acestora poate compromite dispozitivele și pot fi folosite ca puncte de acces asupra infrastructurii, fiind foarte ușor folosite pentru atacuri de tip DDoS(Distributed Denial of Service)

Pentru a limita vulnerabilitățile metodelor de exploatare, operatorii și furnizorii trebuie sa implementeze mecanisme de monitorizare, să aplice actualizările de securitate la momentul potrivit și să efectueze audit pentru a identifica metode noi de exploatare.

4. Măsuri de securitate

Măsurile de securitate pentru rețelele 5G sunt esențiale pentru prevenirea amenințărilor, dar și pentru combaterea amenințărilor cibernetice, în ceea ce privește protecția datelor și a integrității comunicațiilor

4.1. Tehnologii de criptare

Una din cele mai importante medote de securitate o reprezintă criptarea datelor transmise în rețelele 5G, deoarece se asigură confidențialitatea informațiilor, prevenind astfel interceptarea acestora de către persoane neautorizate. Tehnologiile de criptare care se utilizează în rețelele 5G sunt criptarea End-to-End, care garantează protecția datelor pe întreg traseul lor, ceea ce duce la împiedicarea accesării conținutului comunicării, chiar daca se reușeste interceptarea datelor aflate în tranzit, dar și algorimti de criptare avansați, precum AES(Advanced Encryption Standard) și SHA-3(Secure Hash Algorithm), care oferă niveluri ridicate de securitate împotriva atacurilor brute-force.

O alta tehnologie importantă de criptare este criptarea transportului TLS/SSL, deoarece această metodă protejează datele transmise între dispozitive si servere, ceea ce duce la prevenirea interceptării și a falsificării informațiilor în timpul transferului de date.

În rețelele 5G, criptarea identității utilizatorului este la fel de importantă precup criptarea informațiilor, deoarece aceasta metodă duce la prevenirea interceptării și urmăririi utilizatorului, ceea ce sporește confidențialitatea și protejarea informațiilor personale.

Toate aceste tehnologii de criptare sporesc reducerea riscurilor atacurilor de tip Man-in-the-Middle și la protecția datelor împotriva accesului neautorizat.

4.2. Protecția comunicațiilor

Prevenirea interceptărilor este esențială în ceea ce privește protecția comunicațiilor în rețelele 5G, dar mai este esențială și prevenirea întreruperii servicilor și manipulării acestora. Măsurile de protecție a comunicațiilor includ autentificarea mutuală, care verifică reciproc identitatea dispozitivului și rețeaua, ceea ce reduce riscul conectării la rețele false.

Protecția împotriva atacuilor DoS și DdoS se efectuează prin implementarea unor sisteme de detecție IDS/IPS ce permit identificarea și blocarea rapidă a atacurilor, menținând astfel disponibilitatea serviciilor de comunicații.

Segmentarea rețelei și monitorizarea continuă a traficului sunt de asemenea două metode importante pentru protecția comunicațiilor, deoarece segmentarea traficului de rețea în diferite rețele logice reduce suprafața de atac și limitarea răspândirii breșelor de securitate, iar monitorizarea traficului ajută la detecția activității suspecte în timp real, ceea ce poate fi o metodă extrem de esențială pentru a preveni atacurile înainte de producerea unor daune semnificative.

Evaluarea periodică de securitate și testarea rețelei sunt esențiale pentru identificarea potențialelor puncte slabe si pentru validarea eficacității măsurilor de securitate implementate.

5. Reglementări și standarde de securitate pentru rețelele 5G

Funcționalitatea și implementarea rețelelor 5G necesită respectarea unor standarde internaționale pentru garantarea securității și funcționării oprime a infrastructurii de comunicații, dar și respectarea unor reglementări stricte. Aceste reglementări și standarde sunt stabilite de organizații internaționale și autorități guvernamentale pentru a asigura siguranța în care rețelele 5G pot opera. În plus, protocoalele de securitate sunt esențiale în protejarea datelor și a comunicațiilor împotriva amenințărilor cibernetice.

5.1. Organizații ce definesc standardele de securitate

Responsabile pentru definirea standardelor de securitate în rețelele 5G sunt următoarele organizații internațioanle:

1. 3GPP(3rd Generation Partership Project)

3GPP este organizația principală care dezvoltă și stabilește specificațiile tehnice pentru rețelele 3G, 4G și 5G. Pentru securitatea 5G, 3GPP definește măsuri de securitate pentru autentificare, criptare, protecția datelor și integritatea comunicațiilor.

2. ETSI(European Telecommunications Standards Institute)

ETSI contribuie la standardizarea tehnologiilor de telecomunicații în Europa și dezvoltă standardele de securitate pentru 5G. ETSI are grupuri de lucru dedicate securității cibernetice și protecției infrastructurii critice.

3. GSMA(Global System for Mobile Communications Association)

GSMA oferă orientări pentru operatorii de rețele mobile privind securitatea 5G. „5G Cybersecurity Knowledge Base” elaborată de GSMA servește drept referință pentru gestionarea riscurilor și implementarea măsurilor de securitate în rețelele 5G.

4. IETF(Internet Engineering Task Force)

IETF dezvoltă și promovează protocoale de securitate utilizate în rețelele 5G, cum ar fi TLS (Transport Layer Security) și IPsec (Internet Protocol Security), care protejează datele în tranzit.

5. ENSIA(European Union Agency for Cybersecurity)

ENISA joacă un rol central în consolidarea securității cibernetice în Uniunea Europeană, oferind evaluări de risc, recomandări și bune practici pentru protejarea rețelelor 5G împotriva amenințărilor cibernetice.

5.2. Reglementări guvernamentale

În toate guvernele din întreaga lume se implementează reglementări specifice pentru securitatea rețelelor 5G, ce vizează protecțiia infrastructurii critice, dar și protecția datelor utilizatorilor. Reglementările guvernamentale cele mai importante sunt:

1. Cybersecurity Act

Acest act a fost adoptat în anul 2019 pentru a consolida rolul ENSIA și de a introduce un cadru comun de certificare a seceurității cibernetice pentru produse, servicii, dar și pentru infrastructura 5G.

2. 5G Toolbox

Această reglementare oferă un set de măsuri și recomandări pentru statele membre ale Uniunii Europene pentru a securiza rețelele 5G, prin cerințe de diversificare a furnizorilor și prin evaluarea riscurilor de securitate

3. CLOUD Act(SUA)

Prin această lege, autorităților americane le este permis să solicite date de la furnizorii de servicii cloud, indiferent daca datele sunt stocate sau nu în afara Statelor Unite ale Americii. Fiecare rețea 5G trebuie sa respecte reglementările în ceea ce privește protecția datelor în funcție de locul în care operează

5.3. Protocoale de securitate

Pentru a proteja comincațiile, dar și datele transmise prin rețelele 5G, este necesară apicarea unor protocoale de securitate, printre care se numără:

- IPsec (Internet Protocol Security)
  - IPsec oferă securitate pentru comunicațiile la nivelul IP, asigurând confidențialitatea, integritatea și autentificarea pachetelor de date transmise în rețelele 5G.
- TLS (Transport Layer Security)
  - TLS protejează datele transmise între dispozitive și servere, prin criptare și autentificare pentru aplicațiile care se află în rețea
- HTTPS (HyperText Transfer Protocol Secure)
  - Protocolul HTTPS asigură securitatea comunicațiilor pe web prin criptarea traficului, fiind esențial pentru aplicații și servicii care rulează în orice rețea, dar mai ales în rețelele 5G
- Diameter
  - Diameter este un protocol de autentificare și autorizare utilizat în rețelele 5G pentru a gestiona cererile de acces și a asigura securitatea între nodurile rețelei.

6. Dezvoltarea securității rețelelor 5G

Fiind o rețea destul de avansată, rețelele 5G sunt într-o dezvoltare continuă, influențată de evoluțiile tehnologiei, de necesitatea implementării unor măsuri de securitate și de colaborarea internațională pentru a crea un sistem global protejat împotriva amenințărilor cibernetice.

Implementarea 5G nu aduce doar beneficii, aceasta necesitând o atenție sporită și constantă pentru abordarea vulnerabilităților și riscurilor asociate

6.1. Evoluția tehnologiilor

Rețelele 5G sunt cu un pas înainte față de generațiile anterioare de tehnologii mobile, 3G și 4G, introducând progrese semnificative atât în performanță, cât și în securitate. Rețelele 5G folosesc virtualizarea funcțiilor de rețea pentru a crea o infrastructură flexibilă și scalabilă. Aceasta permite gestionarea centralizată și automatizată a traficului și securității.

„Network slicing" permite împărțirea unei singure rețele 5G în mai multe subrețele virtuale, fiecare destinată unui anumit tip de serviciu, cum ar fi dispozitivele IoT sau vehiculele autonome. Această segmentare oferă o izolare mai bună a datelor și aplicațiilor, reducând riscurile de securitate.

Inteligența artificială și machine learning reprezintă de asemenea o evulție importantă a rețelelor 5G, deoarece sunt utilizate pentru a detecta și preveni atacurile cibernetice în timp real, analizând volume mari de date și identificând tipare anormale. Aceste tehnologii contribuie la automatizarea proceselor de securitate și la îmbunătățirea capacităților de răspuns.

6.2. Cooperarea internațională

Securitatea rețelelor 5G nu poate fi asigurată doar la nivel național, de aceea s-a ajuns la cooperarea internațională, care este esențială pentru stabilirea unui cadru comun de securitate și pentru combaterea amenințărilor globale. Principalele aspecte ale cooperării internaționale sunt standardizarea globală, prin organizații internaționale precum 3GPP, ETSI și ITU (International Telecommunication Union), care stabilesc standarde globale pentru securitatea

rețelelor 5G, partajarea informațiilor deoarece țările colaborează pentru schimbul rapid de informații privind vulnerabilitățile și atacurile cibernetice, prin platforme precum CERT (Computer Emergency Response Team) și ENISA.

Un alt aspect important este colaborarea public-privat, pentru că guvernele și companiile de telecomunicații colaborează pentru dezvoltarea unor măsuri eficiente de securitate, introducând cercetarea comună, exerciții de simulare a incidentelor de securitate, dezvoltarea unor soluții de securitate și exerciții la nivel internațional în ceea ce privește securitatea cibernetica.

7. Colcuzii

Rețelele 5G reprezintă un progres tehnologic semnificativ, dar în același timp cu provocări complexe de securitate. Această nouă tehnologie, datorită capacității sale de a conecta un număr mare de dispozitive și de a susține infrastructuri critice, necesită măsuri de securitate mai avansate decât precedentele tehnologii. Importanța securității în rețelele 5G nu trebuie neglijată, întrucât orice vulnerabilitate poate afecta atât utilizatorii, cât și funcționarea unor sectoare esențiale ale economiei și societății.

Un principal motiv îl reprezintă protejarea confidențialității și a datelor utilizatorilor deoarece informațiile circulă la viteze mari și sunt stocate pe o varietate de dispozitive, iar o breșă de securitate poate duce la compromiterea unor date esențiale. De aceea, implementarea unor tehnologii solide de criptare și a unor metode eficiente de protecție a datelor este necesară pentru a garanta securitatea informațiilor transmise prin rețelele 5G.

Pe lângă protecția datelor, securitatea rețelelor 5G asigurară funcționarea infrastructurilor critice, de la transportul informațiilor până la sistemele de sănătate și comunicațiile de urgență, toate acestea depinzând de stabilitatea și securitatea rețelelor 5G. Un atac cibernetic poate perturba aceste servicii vitale, afectând întreaga societate și economie. Prin urmare, măsurile de securitate trebuie să fie implementate în mod riguros și adaptate permanent la noile amenințări.

Evoluția continuă a tehnologiei 5G determină și o evoluție a măsurilor de securitate, deoarece pe măsură ce amenințările devin mai sofisticate, soluțiile de securitate trebuie să fie mai bune. Inteligența artificială și machine learning sunt esențiali în detectarea și prevenirea atacurilor cibernetice. De asemenea, criptarea va trebui să fie permanent actualizată la metode de atac și să se adapteze pentru a oferi protecție împotriva amenințărilor.

Un alt aspect esențial pentru evoluția securității rețelelor 5G este cooperarea internațională, deoarece amenințările cibernetice nu se rezumă doar la o anumită țară, ci la o întreagă rețea de comunicații, iar colaborarea între state, organizații și operatori de rețele este importantă pentru a crea un sistem de securitate la nivel global. Standardele internaționale și reglementările comune contribuie la asigurarea unui nivel similar de securitate și la facilitarea schimbului de informații între părțile implicate.

În concluzie, securitatea rețelelor 5G reprezintă un aspect fundamental pentru viitorul comunicațiilor deoarece fără măsuri sporite de securitate, riscurile pot compromite beneficiile acestei tehnologii avansate. Perspectivele asupra evoluției securității în rețelele 5G sugerează o continuă adaptare și inovare, cu scopul de a proteja utilizatorii, datele și infrastructurile critice. Funcționalitatea rețelelor 5G depinde de capacitatea de a oferi securitate, iar eforturile concertate ale autorităților, operatorilor și organizațiilor internaționale sunt esențiale pentru un viitor digital sigur și stabil.

Bibliografie

1. Ion Bogdan. Comunicații Mobile.
2. Conf. Univ. Dr. Digulescu Angela. Evoluția tehnologiei 5G
3. Ion Bica. Securitatea rețelelor: Principii și practici
4. Nicolae Țăpuș. Securitatea și protecția datelor în rețelele de comunicați

https://sts.ro/ro/aspecte-privind-securitatea-comunicatiilor-si-serviciilor-digitale/

https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/ro/

https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-EMF-health.aspx

https://ro.wikipedia.org/wiki/1G

http://repository.utm.md/bitstream/handle/5014/3623/Conf_UTM_2010_I_pg70-73.pdf?sequence=1&isAllowed=y

https://www.puterea.ro/provocarile-implementarii-tehnologiei-5g-cat-de-importanta-este-standardizarea-securitatii-pentru-operatorii-de-retele-mobile/

http://repository.utm.md/handle/5014/13394

https://www.internetmobile.ro/consideratii-de-securitate-in-retelele-de-telecomunicatii-5g/

https://www.ancom.ro/masuri-de-securitate_5048

https://digital-strategy.ec.europa.eu/ro/policies/5g-research-standards

https://www.telework.ro/ro/performante-si-standarde-in-comunicatiile-prin-retele-5g/?srsltid=AfmBOornC0bV6Wkp-yNBFh8ujkWfX36mWezOcKFW8Hs_99H0JyAZrkDB

https://www.internetmobile.ro/securitatea-in-retelele-de-telecomunicatii-5g-cu-5g-core/