REZUMATUL TEZEI DE DOCTORAT

„Eficientizarea serviciilor de securitate din rețelele de radiocomunicații”

Autor: ing. Cristian-Gabriel Apostol

Email: crs.apostol@gmail.com, tel: 0761 693 445

Conducător de doctorat: prof.univ.dr.ing. Ciprian Răcuciu

În cadrul **Capitolului I**, sunt prezentate elementele introductive ale lucrării de față, câteva aspecte generale referitoare la standardele de comunicații radio și a securității oferite de acestea. Apoi este prezentat scopul principal al lucrării și obiectivele secundare urmărite pentru atingerea acestuia. Rezultatele obținute parcurgând aceste etape pot fi regăsite în cadrul capitolelor următoare.

Capitolul II este dedicat prezentării principalelor trăsături ale securității informației, punându-se accent pe tehnicile aplicate în această lucrare. Serviciile de securitate sunt definite, pentru ca apoi mecanismele de securitate folosite pentru punerea în practică a serviciilor de securitate să fie descrise.

În cadrul **Capitolului III** sunt prezentate standardele de comunicații pe purtătoare radio, realizându-se o paralelă din punct de vedere tehnologic între familia rețelelor celulare și familia rețelelor wireless. Această paralelă este realizată de asemenea și din punct de vedere cronologic, pentru a evidenția principalele tehnologii ce au condus la dezvoltarea noilor standarde radio.

Capitolul IV se focalizează pe descrierea tehnicilor de autentificare a abonaților din rețele radio, urmărind tehnologiile prezentate în cadrul Capitolului III. În acest capitol se realizează trecerea în revistă a mecanismelor de securitate utilizate de către rețelele radio, punând accent pe cel de autentificare. Conceptul autentificării entităților reprezintă o componentă notabilă a Securității Informaționale, cu importanță deosebită în cadrul rețelelor actuale și a dezvoltărilor viitoare ale acestora, deoarece de multe ori partea de criptare este bazată pe autentificarea entităților și a datelor vehiculate între acestea. Analiza autentificării în cadrul rețelelor radio actuale este realizată în **Capitolul IV**, iar propuneri de îmbunătățire ale acestor metode se pot regăsi în cadrul Capitolelor **V și VI**.

Capitolul V are un caracter aplicativ, analizând procesul de autentificare în cadrul rețelelor WiMAX și eficientizând acest proces cu ajutorul aplicării certificatelor digitale pe o rețea existentă cu o întrerupere minimă a serviciilor oferite. Îmbunătățirea autentificării cu impact minim asupra serviciilor oferite, ce pot fi critice și cu o importanță deosebită în cadrul securității naționale reprezintă un obiectiv al acestei lucrări. Tot în cadrul acestui capitol este analizată autentificarea noilor rețele LTE implementate la nivel global, identificându-se o vulnerabilitate notabilă a autentificării și propunând o îmbunătățire a acesteia bazată pe introducerea conceptului de „Vector de Securitate”.

În **Capitolul VI** sunt realizate aplicații, propuneri și îmbunătățiri are algoritmilor de securitate ce se pot aplica în rețelele radio interconectate, evidențiind componentele ce se pot securiza și rolul fiecăruia dintre acești algoritmi.

Pe lângă problemele clasice luate în calcul în cadrul securizării unei rețele de radiocomunicații de către standardele existente, există anumite vulnerabilități neabordate de standarde, pe care dorim să le soluționăm. Securizarea datelor de planificare a rețelelor radio folosind tehnicile de watermarking, atât pe timpul transmiterii cât și pe timpul stocării este

discutată și aprofundată, acesta reprezentând un alt obiectiv al tezei de față. Mai precis se dorește dezvoltarea unor algoritmi de Watermarking Digital folosind Teoria Haosului, ce pot fi utilizați pentru a proteja imaginile și graficele confidențiale de planificare a rețelelor. Acești algoritmi sunt împărțiți în două categorii: algoritmi fragili și algoritmi robuști în funcție de rolul pe care îl pot avea, de protecție a integrității datelor sau de autentificare a originii acestora.

În cadrul acestor rețele putem transmite date în mod clar sau criptat. Ambele metode sunt abordate de standardele existente, dar folosirea metodelor steganografice pot asigura transmiterea securizată a mesajelor, fără a atrage atenția atacatorilor. Aceasta tehnică este analizată și exemplificată în cadrul tezei, cu propuneri de îmbunătățire în cadrul **Capitolului VI**.

În cadrul acestui capitol se va analiza de asemenea securitatea oferită de standarde în ceea ce privește transportul informațiilor de la stațiile de bază până la punctul de acces al serviciilor, abordând posibilitatea de a crește nivelul de securitate al rețelelor celulare prin securizarea acestor interfețe folosind protocolul IPSEC.

Capitolul VII este reprezentat de concluziile finale ale lucrării, evidențiază principalele contribuții atât teoretice cât și practice aduse de cercetarea realizată în cadrul programului de pregătire doctorală și marchează direcțiile viitoare de cercetare.