Funcționalități îmbunătățite de securitate cu dispozitive Android în vehicule

Teză de doctorat – Rezumat

pentru obținerea titlului științific de doctor la
Universitatea Politehnica Timișoara
în domeniul de doctorat Calculatoare și Tehnologia Informației
de

Ing. Tudor-Sebastian Andreica
Conducător științific: Prof. univ. dr. ing. Bogdan-Ioan Groza

Iunie, 2024

În ultimele decenii s-au înregistrat progrese semnificative în industria automotive, mai ales în ceea ce privește electronica. Componentele mecanice tradiționale folosite în vehicule au fost înlocuite treptat cu componente inteligente. Tot mai multe componente sunt acum echipate cu procesoare care rulează programe software, făcându-le mai flexibile, cum ar fi de exemplu capacitatea de a suporta multiple protocoale de comunicație și diagnosticare. Dezvoltările recente în tehnologie, care includ apariția vehiculelor electrice și hibride, a mașinilor autonome și a mașinilor conectate, au avut un impact semnificativ asupra industriei automotive. Este de așteptat ca aceste avansuri tehnologice să contureze viitorul industriei, făcând-o mai sustenabilă și eficientă.

Unitatea infotainment este sistemul central de control al divertismentului în mașină și al altor funcții, cum ar fi selectarea modurilor de condus ale mașinii, activarea și dezactivarea funcțiilor de asistență pentru șofer (ADAS), controlul climatizării, încălzirea scaunelor și controlul camerei cu unghi de 360 de grade. Unitățile infotainment moderne sunt succesoarele radiourilor auto care au fost instalate în vehicule încă din anii 1920 în scopuri de divertisment. Progresele din următoarele decenii au inclus introducerea radiocasetofoanelor de tip 8-track tapes și a casetofoanelor cu casete compacte în anii 1960, urmate de introducerea CD player-ului în anul 1984. La începutul secolului 21, sistemele audio pentru vehicule au început să se adapteze la standardele moderne de stocare al conținutului digital, cum ar fi unitățile de tip USB și cardurile de memorie. De asemenea, scopul unităților infotainment a fost extins pentru a incorpora și alte funcționalități, cum ar fi de exemplu navigația, telematica și diagnosticarea la distanță. Unitățile infotainment sunt echipate cu procesoare performante, memorii cu spațiu mare de stocare și sisteme de operare moderne precum Android. Unitățile au în componență un ecran de afișare și diverse sisteme de interfațare a utilizatorilor cu unitățile, cum ar fi controalele rotative și ecranele tactile. Pe lângă caracteristicile clasice precum radio AM/FM, redarea CD-urilor și al DVD-urilor, unitățile infotainment sunt capabile de a comunica cu alte dispozitive inteligente folosind Bluetooth, Wi-Fi sau conectivitate celulară, dispun de navigație GPS și pot fi utilizate pentru controlul mai multor funcții ale mașinii. De asemenea, unitățile infotainment moderne rulează aplicații precum Apple CarPlay și Android Auto, care permit șoferilor să-și conecteze telefoanele mobile la sistemul de infotainment al mașinii pentru a controla muzica, navigația și alte aplicații care rulează pe telefoanele inteligente prin intermediul interfeței unității infotainment. În ansamblu, unitățile infotainment joacă un rol important în furnizarea

Fig. 1. Unitatea infotainment PNI A8020 (utilizată în mai multe lucrări științifice ale autorului)

serviciilor de divertisment și conectivitate pentru șoferi și pasageri, servind în același timp și ca sistem central de control pentru alte funcții importante ale mașinilor. Datorită capabilităților lor computaționale și al conectivității, unitățile infotainment pot fi utilizate și în aplicații de securitate, acesta fiind subiectul principal abordat în această teză. Figura 1 prezintă unitatea infotainment PNI A8020, una dintre cele două unități utilizate în configurațiile experimentale folosite în această teză.

Odată cu beneficiile noilor funcționalități adăugate vehiculelor moderne, inclusiv unitățile infotainment menționate mai sus, apar și efecte secundare care trebuiesc luate în considerare. În urmă cu douăzeci de ani, securitatea cibernetică nu reprezenta o problemă în industria automotive. Cu toate acestea, odată cu integrarea de noi funcționalități și tehnologii în vehicule, securitatea a devenit un subiect critic întrucât avansurile tehnologice pot deschide calea către diverse atacuri cibernetice. În ultimii ani au existat numeroase incidente și studii de securitate care au demonstrat efectele atacurilor cibernetice asupra mașinilor și au crescut gradul de conștientizare referitor la securitate în industria automotive. Câteva dintre acestea sunt sugerate mai jos:

- În 2015, Miller și Valasek, doi cercetători în securitate cibernetică, au efectuat un atac la distanță asupra unui Jeep Cherokee. Aceștia au reușit să obțină controlul asupra câtorva sisteme ale vehiculului, inclusiv asupra direcției și al frânei [1]. Acest incident, raportat de revista Wired, a determinat rechemarea în service a 1,4 milioane de vehicule [2].
- Vehiculele Tesla, binecunoscute pentru utilizarea unora dintre cele mai avansate tehnologii din industria automotive au fost, de asemenea, subiectul mai multor atacuri cibernetice. Nie et al., cercetători de la Keen Security Lab of Tencent, au reușit să efectueze două atacuri la distanță asupra diferitelor modele Tesla în 2016 [3] și 2017 [4]. Aceștia au reușit să compromită diverse sisteme ale mașinii, cum ar fi Instrument Cluster (IC), display-ul

central de informații (CID) și Gateway-ul, obținând astfel acces la magistrala CAN și putând să injecteze mesaje malițioase.

- Conform unui articol publicat de revista Wired [5], un studiu efectuat de clubul auto Allgemeiner Deutscher Automobil-Club (ADAC) din München a evaluat vulnerabilitatea a zeci de mașini la atacurile de tip amplificare radio care pot extinde raza de acțiune a cheii wireless a șoferului fără ca acesta să fie conștient, permițând unui atacator să deschidă și chiar să pornească mașina. Studiul a concluzionat că 24 de modele de vehicule de la 19 producători diferiți au fost vulnerabile la acest tip de atac.

Apariția acestor incidente subliniază importanța implementării unor măsuri robuste de securitate cibernetică în sectorul automotive. De asemenea, evidențiază eforturile continue atât ale cercetătorilor, cât și ale hackerilor, de a descoperi și a exploata vulnerabilitățile vehiculelor moderne. Prin urmare, este crucial pentru producătorii de automobile și furnizorii de componente să investească în mod constant în cercetarea și dezvoltarea securității cibernetice pentru a ține pasul cu noile amenințări.

Obiectivele cercetării. Obiectivul principal al acestei teze este de a îmbunătăți securitatea vehiculelor folosind dispozitive Android, cum ar fi unitățile infotainment și telefoanele inteligente, care au devenit omniprezente în automobilele moderne. Mai specific, teza își propune să atingă următoarele obiective:

1) Investigarea potențialului criptografiei bazate pe operații de asociere bilineară în diverse aplicațiile de securitate automotive, utilizând atât microcontrolere, cât și unități infotainment instalate în vehicule;
2) Propunerea unui sistem securizat de control al accesului la vehicul bazat pe scheme de identitate și semnături de grup, utilizând telefoane inteligente cu sistem de operare Android;
3) Dezvoltarea unei soluții bazate pe telefoane inteligente pentru securizarea comunicației între vehicule folosind criptografia bazată pe identitate;
4) Propunerea de sisteme eficiente de detecție a intruziunilor pentru magistrala CAN, cu accent pe implementarea acestora pe dispozitive care rulează Android (cum ar fi unitățile infotainment sau chiar telefoanele inteligente).

Contribuții majore În această teză se explorează utilizarea dispozitivelor Android, care oferă capacități de procesare și conectivitate mai extinse în comparație cu unitățile de control electronice obișnuite din domeniul automotive, pentru îmbunătățirea securității automobilelor. Principalele contribuții ale acestei teze pot fi rezumate astfel:

1) Evaluarea mai multor biblioteci criptografice bazate pe operații de asociere bilineară pe dispozitive Android și microcontrolere automotive, precum și o prezentare a patru posibile scenarii de utilizare al acestor blocuri criptografice [6];
2) Propunerea unui sistem securizat de control al accesului la vehicul bazat pe telefoane inteligente, care se bazează pe un concept mixt compus din controlul accesului bazat pe roluri (RBAC) și controlul accesului bazat pe atribute (ABAC). Pentru a asigura securitate și confidențialitate sunt folosite tehnici criptografice moderne precum cele bazate pe identitate și semnături de grup. De asemenea, este prezentată o implementare proof-of-concept pentru a demonstra fezabilitatea conceptului propus [7];
3) Explorarea fezabilității de securizare a comunicației între vehicule utilizând criptografia bazată pe identitate, extrasă din numerele de înmatriculare ale mașinilor. În acest scop, s-au efectuat experimente pentru citirea numerelor de înmatriculare folosind telefoane inteligente [8];

4) Evaluarea mai multor algoritmi de învățare automată ca posibile soluții pentru sisteme de detecție a intruziunilor (IDS) în ceea ce privește performanța detecției de intruziuni pe seturi de date CAN și CAN-FD colectate de la vehicule reale [9];
5) Propunerea unei soluții pentru detecția de intruziuni care constă într-o instanță a unui sistem IDS instalată local pe unitățile infotainment Android din fiecare vehicul și un sistem IDS centralizat care rulează în cloud și procesează datele provenite de la mai multe vehicule. Această soluție include raportarea intruziunilor în conformitate cu standardul ISO/SAE 21434, acompaniată de analize de tip TARA [10].

Aceste contribuții ale autorului se regăsesc într-o serie de publicații în reviste și conferințe ISI. În [6], autorul explorează aplicațiile criptografiei bazate pe operații de asociere bilineară în mai multe scenarii automotive. Autorul a evaluat două biblioteci software care conțin scheme criptografice bazate pe operații de asociere bilineară, atât pe dispozitive Android, cât și pe microcontrolere automotive. De asemenea, această lucrare exemplifică patru scenarii automotive care ar putea beneficia de aceste scheme criptografice ca soluții de securitate. Operațiile de asociere bilineară servesc ca bază pentru tehnici criptografice moderne precum semnăturile bazate pe identitate și semnături de grup. Aceste tipuri de semnături au fost propuse de către autor ca soluții pentru a securiza sistemul de control al accesului la vehicule folosind telefoane inteligente prezentat în [7]. Sistemul de control al accesului auto propus în [7] se bazează pe o politică de control al accesului bazată pe roluri și atribute pentru a asigura securitate și confidențialitate. Suitele de protocoale de securitate includ blocuri criptografice moderne, inclusiv semnături bazate pe identitate și grup, precum și primitive asimetrice și simetrice clasice. De asemenea, lucrarea include o implementare proof-of-concept pe dispozitive Android care demonstrează fezabilitatea soluției propuse. Protocolul permite folosirea diferitor tehnologii de comunicație, cum ar fi NFC, Bluetooth și Wi-Fi, și a fost testat folosind mai multe telefoane inteligente, unități infotainment Android și un microcontroler certificat pentru industria de automobile. În [8], autorul a propus o soluție de securitate pentru comunicația între vehicule. În abordarea propusă, numerele de înmatriculare sunt folosite ca identificatori unici pentru derivarea cheilor publice aferente unui sistem criptografic bazat pe identitate, care permite vehiculelor să stabilească un canal de comunicație securizat. Mai multe experimente constând în citirea numerelor de înmatriculare folosind telefoane inteligente au fost efectuate pentru a demonstra fezabilitatea abordării propuse. De asemenea, viteza de execuție a primitivelor criptografice propuse a fost evaluată pe telefoanele inteligente, dovedind că dispozitivele Android actuale pot gestiona aceste scheme criptografice într-un mod eficient din punct de vedere al execuției. Autorul a contribuit, de asemenea, la securitatea rețelelor vehiculare prin propunerea de soluții pentru sistemele de detecție a intruziunilor în [9] și [10]. În [9], autorul a evaluat un grup de clasificatoare binare pentru detectarea intruziunilor și a propus un sistem IDS în două etape pentru magistrala CAN. Sistemul propus a fost evaluat în timp real folosind o configurație experimentală formată din microcontrolere automotive și dispozitive Android, cu seturi de date CAN colectate de la vehicule reale. În [10], s-a propus un sistem de detecție al intruziunilor mai avansat, proiectat pentru a rula atât pe unitățile infotainment Android, cât și în aplicații care rulează în cloud. În timp ce sistemul IDS instalat local rulează în fiecare vehicul, sistemul IDS implementat în cloud operează cu date CAN care provin de la mai multe grupuri de vehicule și este actualizat cu cele mai recente tipuri de atacuri. În plus, rezultatele clasificării sistemului IDS care rulează în cloud sunt analizate ulterior de o echipă de management al incidentelor conform recomandărilor din standardul ISO/SAE 21434, iar rezultatele sunt stocate pe Blockchain pentru transparență și trasabilitate.

Pe lângă subiectele anterioare care formează nucleul acestei teze, autorul tezei a mai contribuit

la alte câteva cercetări în domeniul securității vehiculelor. În [11], autorul a evaluat starea memoriei SRAM neinițializată în mai multe microcontrolere automotive. Memoria SRAM neinițializată oferă un model unic pe fiecare dispozitiv datorită imperfecțiunilor fizice și poate fi exploatată cu succes în mecanisme de securitate precum identificarea prin amprentare sau extragerea cheilor criptografice, utilizând atât afinitatea față de unele stări fixe, cât și a deviației față de acestea. Autorul a contribuit la experimentele practice din [12], care prezintă o soluție low-cost pentru chei auto wireless cu capacități de partajare a drepturilor bazată pe microcontrolerul MSP430. O altă contribuție a autorului este evaluarea algoritmilor de securitate folosiți pentru detectarea și prevenirea intruziunilor pentru vehiculele comerciale pe un microcontroler automotive de înaltă performanță [13]. În plus, autorul a contribuit la conceptul prezentat în [14], care propune arhitecturi rezistente la adversari pentru magistrale CAN. Autorul a asistat la dezvoltarea configurației experimentale, care constă într-o rețea de 8 unități de control electronice (ECU-uri), un Bus Guardian și alte componente. De asemenea, el a implementat și a evaluat algoritmii propuși pe microcontrolerele S12. Autorul tezei a mai contribuit la lucrarea din [15], care studiază influența cablajului asupra modelului de tensiune, care a fost frecvent propus ca sursă pentru identificarea dispozitivelor transmițătoare în rețelele CAN.

Per total, autorul a contribuit la 10 articole științifice care prezintă diverse aplicații de securitate automotive, dintre care primele 5 articole formează nucleul acestei teze:

1) Tudor Andreica, Bogdan Groza, and Pal-Stefan Murvay. ”Applications of Pairing-Based Cryptography on Automotive-Grade Microcontrollers,” In *Computer Safety, Reliability, and Security,* pages 331–343, 2018.
2) Bogdan Groza, Tudor Andreica, Adriana Berdich, Pal-Stefan Murvay, and Eugen Horatiu Gurban. ”PRESTvO: Privacy Enabled Smartphone Based Access to Vehicle On-Board Units,” *IEEE Access,* 8:119105–119122, 2020.
3) Tudor Andreica and Bogdan Groza. ”Secure V2V Communication with Identity-based Cryptography from License Plate Recognition,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS),* pages 366–373, 2019.
4) Tudor Andreica, Christian-Daniel Curiac, Camil Jichici, and Bogdan Groza. ”Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus,” *IEEE Access,* 10:95161–95178, 2022.
5) Tudor Andreica, Adrian Musuroi, Alfred Anistoroaei, Camil Jichici, and Bogdan Groza. ”Blockchain Integration for in-Vehicle CAN Bus Intrusion Detection Systems with ISO/SAE 21434 Compliant Reporting,” *Scientific Reports*, 14:8169, 2024.
6) Bogdan Groza, Pal-Stefan Murvay, and Tudor Andreica. ”Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers,” in *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications,* page 109–120, 2016.
7) Bogdan Groza, Tudor Andreica, and Pal-Stefan Murvay. ”Designing wireless automotive keys with rights sharing capabilities on the MSP430 microcontroller,” in *International Conference on Vehicle Technology and Intelligent Transport Systems,* 2017.
8) Camil Jichici, Bogdan Groza, Radu Ragobete, Pal-Stefan Murvay, and Tudor Andreica. ”Effective Intrusion Detection and Prevention for the Commercial Vehicle SAE J1939 CAN Bus,” *IEEE Transactions on Intelligent Transportation Systems,* 23(10):17425–17439, 2022.
9) Bogdan Groza, Lucian Popa, Tudor Andreica, Pal-Stefan Murvay, Asaf Shabtai, and Yuval Elovici. ”PanoptiCANs - Adversary-resilient Architectures for Controller Area Networks,”

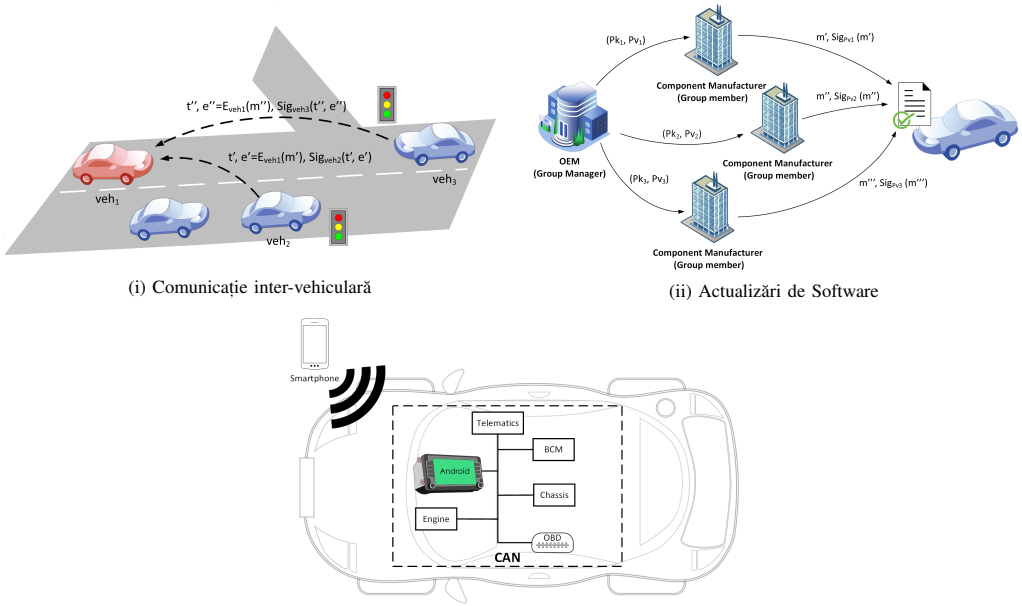
in *Computer Security – ESORICS 2022,* pages 658–679, 2022.

10) Lucian Popa, Camil Jichici, Tudor Andreica, Pal-Stefan Murvay and Bogdan Groza, "Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks", *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023)*, 2023.

În comparație cu unitățile de control electronice folosite actual în industria automotive, dispozitivele Android au procesoare mai puternice și capacități de comunicație wireless. Această teză evidențiază și demonstrează cum aceste caracteristici avansate pot îmbunătăți securitatea comunicației între vehicule și mediul extern, în special în scenarii precum controlul accesului la vehicule, comunicația între vehicule și securitatea rețelelor din vehicul. În cele ce urmează sunt prezentate informații referitoare la celelalte capitole din teză.

Capitolul 2 explorează patru scenarii automotive care ar putea beneficia în mod semnificativ pe baza folosirii unei operații criptografice mai moderne, și anume operația de asociere bilineară. Această operație deschide calea către construirea unor sisteme criptografice avansate, cum ar fi semnăturile compacte, semnăturile de grup, și criptările și semnăturile bazate pe identitate. Semnăturile compacte pot fi folosite pentru autentificarea datelor transmise pe rețele de comunicație din vehicule, cum ar fi magistrala CAN, care are un câmp de date de cadru limitat. Pentru securizarea actualizărilor de software over-the-air se pot folosi semnăturile de grup, deoarece componentele vehiculelor sunt fabricate de zeci de furnizori. În acest context, producătorul de automobile (OEM) și furnizorii de componente pot deveni membri a unui grup în care fiecare membru poate semna și autoriza patch-urile de software în numele grupului. Cu toate acestea, doar OEM-ul, în calitate de manager de grup, poate dezvălui inițiatorul unei semnături în caz de dispute. Securitatea comunicației între vehicule poate fi îmbunătățită folosind criptografia bazată pe identitate, care elimină necesitatea infrastructurii cu chei publice (PKI). Cele trei scenarii automotive menționate anterior sunt sugerate în Figura 2. În plus, schemele bazate pe identitate combinate cu semnături de grup pot fi folosite ca soluție de securitate pentru sistemele avansate de control al accesului auto. În continuare, capitolul 2 prezintă rezultate experimentale în ceea ce privește timpul de execuție și consumul de memorie flash pentru două biblioteci de software criptografice care utilizează operații de asociere bilineară. Evaluările au fost efectuate pe o unitate infotainment Android, un telefon inteligent Android și două microcontrolere automotive. Rezultatele experimentale aferente schemelor bazate pe operații de asociere bilineară au fost comparate cu cele ale algoritmilor RSA și DSA, indicând faptul că schemele bazate pe operații de asociere bilineară necesită mai puțină memorie pentru implementare în anumite cazuri, dar sunt în general mai intensive din punct de vedere computațional. În ansamblu, rezultatele sugerează că schemele bazate pe operații de asociere bilineară sunt fezabile pentru a fi implementate pe dispozitive automotive și pot fi utilizate cu succes în securitatea diferitelor scenarii automotive, în special datorită beneficiilor suplimentare care nu pot fi obținute cu algoritmi criptografici clasici cu cheie publică, precum DSA și RSA.

Capitolul 3 prezintă o propunere pentru securizarea comunicațiilor între vehicule folosind semnături bazate pe identitate, cu identități extrase din numerele de înmatriculare. Deoarece infrastructura cu chei publice (PKI) nu este încă adoptată universal în contextul comunicațiilor între vehicule și gestionarea cheilor reprezintă o provocare semnificativă, semnăturile bazate pe identitate pot fi o alternativă bună la algoritmii de cheie publică tradiționali ca soluție de securitate. Studiul din acest capitol explorează utilizarea semnăturilor bazate pe identitate pentru stabilirea unui canal de comunicație securizat între două vehicule, folosind numerele de înmatriculare drept identități din care sunt derivate cheile publice. În acest sens, au fost propuse două protocoale pentru două scenarii de comunicație diferite. Primul scenariu ține cont



(i) Comunicație inter-vehiculară

(ii) Actualizări de Software

(iii) Securitatea rețelelor vehiculare

Fig. 2. Aplicații ale operațiilor de asociere bilineară în Industria Automotive

de situația în care două vehicule sunt în raza de comunicație directă, în timp ce al doilea scenariu ia în considerare situația în care vehiculele sunt în apropiere, dar nu sunt în raza de comunicație directă, iar comunicație între cele două vehicule este mediată de un vehicul vecin comun. Pentru a demonstra fezabilitatea conceptului, a fost dezvoltată o aplicație Android care utilizează Wi-Fi Direct pentru a facilita comunicația între vehicule și care citește numerele de înmatriculare ale vehiculelor folosind camera telefonului. Folosind această aplicație au fost efectuate experimente practice cu privire la distanțele și unghiurile la care pot fi citite numerele de înmatriculare. Aceste experimente au fost efectuate folosind două telefoane inteligente Samsung, care rulează Android și sunt echipate cu camere de înaltă calitate. Configurația experimentală este prezentată în Figura 3. Adițional, algoritmii criptografici folosiți în protocoalele de handshake propuse au fost evaluați din punct de vedere al vitezei de execuție pe cele două telefoane. Rezultatele experimentale sugerează că numerele de înmatriculare pot fi citite la o distanță de până la 50 de metri și la un unghi de până la 60 de grade în condiții meteorologice bune. Evaluarea funcțiilor criptografice indică faptul că telefoanele moderne pot gestiona în mod rezonabil primitivele bazate pe identitate. Cu toate acestea, datorită constrângerilor stricte de timp ale comunicației între vehicule, acestea pot fi folosite doar pentru stabilirea unui canal de comunicație securizat bazat pe primitive simetrice care sunt executate mult mai rapid.

Capitolul 4 prezintă o soluție securizată de control al accesului la vehicul implementată pe telefoane Android și unități infotainment. Sistemul propus utilizează o politică de control al accesului bazată pe roluri, combinată cu atribute, permițând utilizatorilor să acceseze diferite funcționalități ale vehiculului folosind telefoanele lor Android. Accesul la funcțiile vehiculului este condiționat printr-o politică de control al accesului bazată pe drepturi, similară unei tabele de alocare a fișierelor (FAT) folosită în sistemele de operare actuale. Această politică permite utilizatorilor să efectueze operațiuni de citire, scriere sau executare asupra

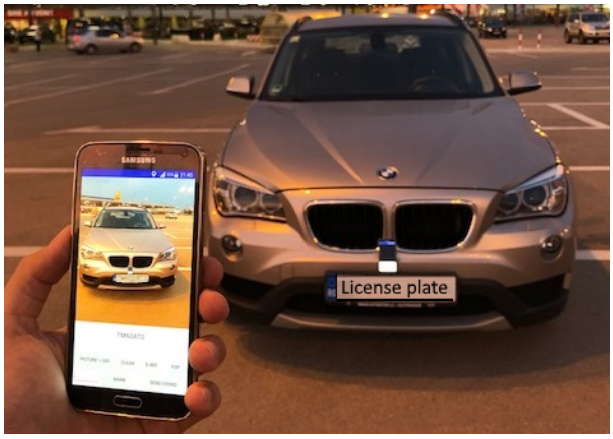


Fig. 3. Telefoanele inteligente și mașina din experimentele efectuate în [8]

diverselor funcționalități ale vehiculului. Figura 4 oferă o privire de ansamblu a conceptului propus. Obiectivele de securitate și confidențialitate ale sistemului propus sunt realizate folosind

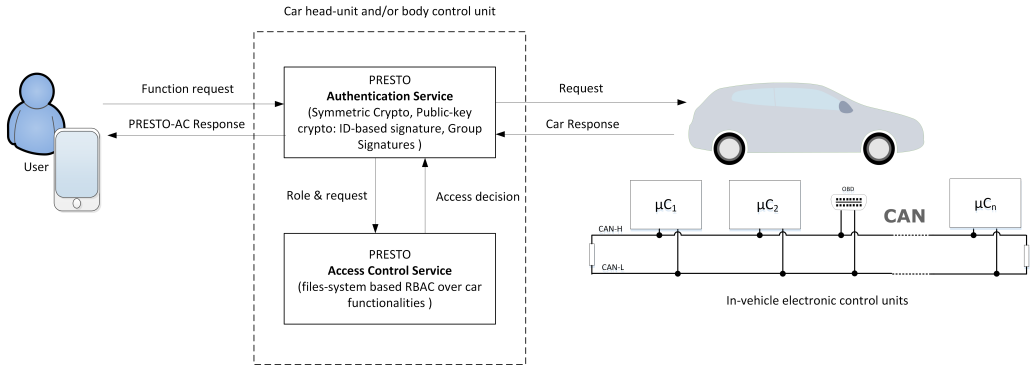
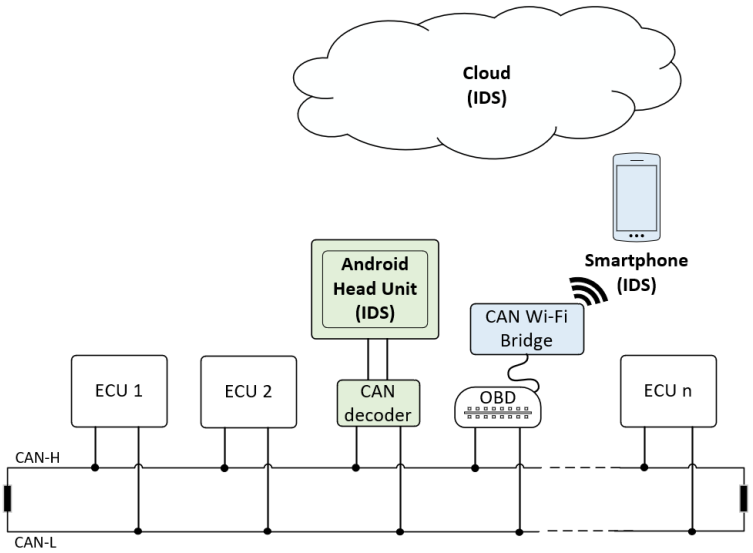


Fig. 4. Privirea de ansamblu al sistemului propus în [7]

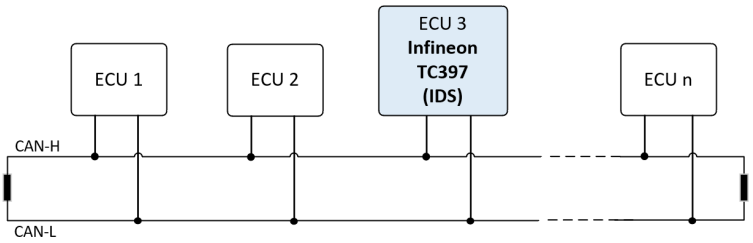
protocoale la nivel de aplicație care permit utilizarea diferitelor tehnologii de comunicație, cum ar fi Bluetooth, Wi-Fi și NFC. Protocoalele de securitate folosesc diverse blocuri criptografice, inclusiv scheme simetrice și asimetrice tradiționale, precum și algoritmi mai avansați, cum ar fi semnăturile de grup și semnăturile bazate pe identitate. Semnăturile de grup sunt folosite pentru a obține confidențialitate deoarece vehiculele pot identifica doar rolurile care le accesează, cum ar fi proprietarul, șoferul, pasagerul sau tehnicianul, dar nu și entitățile individuale din spatele acestor roluri. Utilizarea semnăturilor bazate pe identitate facilitează gestionarea cheilor publice și o face mai intuitivă. De asemenea, în acest capitol este prezentată o aplicație proof-of-concept pentru a evidenția fezabilitatea sistemului propus de control al accesului la vehicul. Procedurile care facilitează partajarea drepturilor și executarea funcționalităților au fost implementate complet folosind tehnologiile de comunicație Bluetooth, Wi-Fi și NFC și au fost evaluate pe diverse telefoane și unități infotainment Android. În plus, toate schemele criptografice incluse în protocoalele de securitate au fost evaluate în materie de timpi de

rulare. Rezultatele indică faptul că soluția propusă de control al accesului la vehicul poate fi implementată în practică folosind telefoane și unități infotainment Android.

Capitolul 5 discută implementarea sistemelor de detecție a intruziunilor pentru magistrala CAN pe unitățile infotainment Android și pe ECU-urile din vehicule. în acest sens, au fost propuse două configurații care pot fi implementate în vehiculele moderne: una folosind unități infotainment Android sau telefoane mobile, iar cealaltă folosind microcontrolere automotive. Cele două configurații sunt ilustrate în Figura 5. Pentru fiecare configurație, au fost prezentate



(i) Sistem IDS rulat pe dispozitive Android



(ii) Sistem IDS rulat pe microcontrolere automotive

Fig. 5. Cele două scenarii abordate pentru detectarea intruziunilor în [9]

arhitecturi specifice, și s-a discutat integrarea sistemelor IDS pe dispozitivele Android și pe ECU-urile din vehicule în conformitate cu standardele AUTOSAR. Ulterior s-a propus un sistem IDS în două etape, în care prima etapă detectează atacurile de tip replay și flooding verificând timpul de sosire al cadrelor și ID-urile CAN, iar cea de a doua etapă utilizează algoritmi de învățare automată pentru a detecta atacurile de tip fuzzing. Pentru a evalua sistemul de detecție al intruziunilor propus s-au colectat seturi de date CAN de la vehicule reale, care au fost mai apoi extinse cu atacuri folosind o configurație de simulare CANoe. Douăsprezece algoritmi tradiționali de machine learning au fost evaluați ca posibili candidați pentru etapa a doua a sistemului IDS propus. Prima parte a evaluării, adică evaluarea offline, s-a realizat pe seturile de date CAN folosind un laptop echipat cu un procesor de performanță înaltă. Ulterior, patru

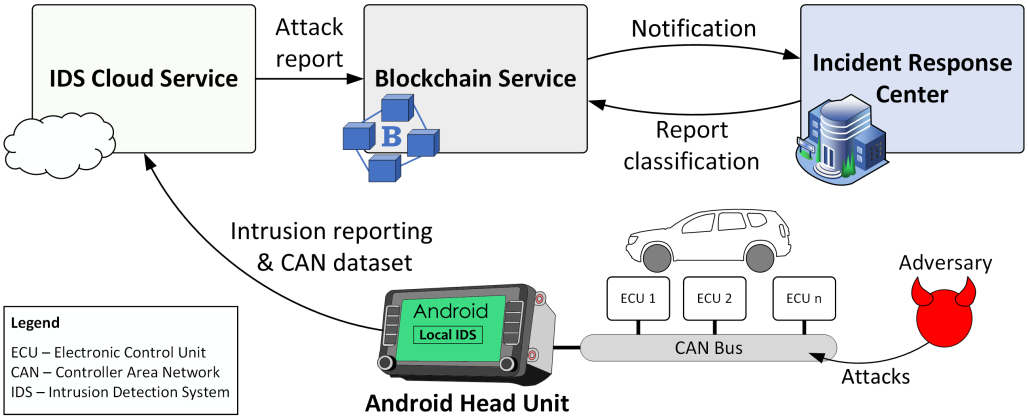


Fig. 6. Privirea de ansamblu al sistemului de detecție și raportare al intruziunilor propus în [10]

algoritmi din cei doisprezece au fost selectați pentru o evaluare online (în timp real) pe mai multe dispozitive Android și microcontrolere automotive folosind un setup experimental care simulează rețelele CAN ale vehiculelor reale. Precizia de detecție a algoritmilor la evaluarea online a fost ușor mai mică decât cea a evaluării offline, subliniind astfel faptul că există anumiți factori care pot influența performanța detecției intruziunilor în timp real. Acest rezultat este extrem de important, deoarece multe propuneri din literatură sunt evaluate doar offline. De asemenea, rezultatele experimentale din Capitolul 5 au arătat că algoritmii de învățare automată constituie o provocare în ceea ce privește viteza de execuție și cerințele de memorie, ceea ce îi face dificil de implementat pe ECU-urile clasice. Pe de altă parte, dispozitivele Android demonstrează un mare potențial pentru integrarea sistemelor de detecție a intruziunilor pentru magistralele CAN.

Capitolul 6 prezintă o soluție avansată de detecție a intruziunilor care utilizează unități infotainment Android, un serviciu cloud, un centru de răspuns la incidente și un serviciu Blockchain. Figura 6 oferă o privire de ansamblu a conceptului propus. În abordarea propusă, vehiculele rulează un sistem IDS instalat local pe unitățile infotainment, care raportează evenimentele de intruziune CAN la un sistem IDS care rulează în cloud și care evaluează date CAN de la mai multe vehicule. Sistemul IDS din cloud este în permanență actualizat cu cele mai recente tipuri de atacuri. Rezultatele clasificării sistemului IDS rulat în cloud sunt analizate în continuare de către o echipă specializată de răspuns la incidente. În cazul unui atac se efectuează o analiză TARA conform standardului ISO/SAE 21434, iar rapoartele rezultate sunt stocate pe Blockchain pentru a asigura transparența și trasabilitatea incidentelor raportate. Sistemul IDS propus a fost proiectat cu capacități de transfer learning, permițând atacurilor învățate pe un vehicul să fie detectate și pe alte vehicule. IDS-ul a fost evaluat pe seturi de date CAN colectate de la trei vehicule identice, demonstrând o bună performanță în detectarea intruziunilor. Cu toate acestea, acuratețea a fost ușor mai mică atunci când IDS-ul a fost evaluat pe alte vehicule decât cel utilizat pentru antrenament. Acest lucru se datorează în mare parte datorită micilor diferențe ale traficului CAN între vehicule. În continuare, algoritmul IDS propus a fost evaluat din punct de vedere al timpului de execuție pe o unitate infotainment și o mașină virtuală rulată în cloud, demonstrând că algoritmul IDS propus poate fi implementat eficient pe aceste dispozitive. În final, acest studiu demonstrează că atât capacitățile computaționale extinse cât și avantajele

protocoalelor de comunicație wireless ale unităților infotainment Android pot fi valorificate pentru implementarea de sisteme avansate de detecție a intruziunilor în vehicule.

Capitolul 7 prezintă concluziile tezei de doctorat. În rezumat, teza evidențiază avantajele utilizării unităților infotainment Android în aplicațiile de securitate vehiculară. Experimentele practice au demonstrat că aceste dispozitive au capacități computaționale puternice care pot gestiona scheme criptografice complexe, precum semnăturile de grup și semnăturile bazate pe identitate, dar și algoritmi de învățare automată pentru sistemele de detecție a intruziunilor. În plus, capacitățile lor de comunicare wireless le fac potrivite pentru o varietate de funcții, inclusiv comunicarea V2V, sistemele de control al accesului la vehicule și sistemele de detecție a intruziunilor bazate pe cloud. În ansamblu, concluziile acestei teze sugerează că unitățile infotainment Android ar putea juca un rol esențial în îmbunătățirea securității vehiculelor moderne.

Referințe

[1] A. Greenberg, “Hackers remotely kill a jeep on the highway - with me in it. www.wired.com,” 2015, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[2] ——, “After jeep hack, chrysler recalls 1.4m vehicles for bug fix. www.wired.com,” 2015, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[3] S. Nie, L. Liu, and Y. Du, “Free-fall: Hacking tesla from wireless to can bus,” *Black Hat USA*, vol. 25, pp. 1–16, 2017.

[4] S. Nie, L. Liu, and W. Zhang, “Over-the-air: How we remotely compromised the gateway, bcm, and autopilot ecus of tesla cars,” *Black Hat USA*, 2018.

[5] A. Greenberg, “Radio attack lets hackers steal 24 different car models. www.wired.com,” 2016, [Online; accessed 18-Januar-2023]. [Online]. Available: www.wired.com

[6] T. Andreica, B. Groza, and P.-S. Murvay, “Applications of pairing-based cryptography on automotive-grade microcontrollers,” in *Computer Safety, Reliability, and Security*, B. Gallina, A. Skavhaug, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2018, pp. 331–343.

[7] B. Groza, T. Andreica, A. Berdich, P.-S. Murvay, and E. H. Gurban, “Prestvo: Privacy enabled smartphone based access to vehicle on-board units,” *IEEE Access*, vol. 8, pp. 119105–119122, 2020.

[8] T. Andreica and B. Groza, “Secure v2v communication with identity-based cryptography from license plate recognition,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2019, pp. 366–373.

[9] T. Andreica, C.-D. Curiac, C. Jichici, and B. Groza, “Android head units vs. in-vehicle ecus: Performance assessment for deploying in-vehicle intrusion detection systems for the can bus,” *IEEE Access*, vol. 10, pp. 95161–95178, 2022.

[10] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, “Blockchain integration for in-vehicle can bus intrusion detection systems with iso/sae 21434 compliant reporting,” *Scientific Reports*, vol. 14, p. 8169, 2024.

[11] B. Groza, P.-S. Murvay, and T. Andreica, “Evaluating sram as source for fingerprints and randomness on automotive grade controllers,” in *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications*, ser. ICETE 2016. Setubal, PRT: SCITEPRESS - Science and Technology Publications, Lda, 2016, p. 109–120. [Online]. Available: https://doi.org/10.5220/0005966401090120

[12] B. Groza, T. Andreica, and P.-S. Murvay, “Designing wireless automotive keys with rights sharing capabilities on the msp430 microcontroller,” in *International Conference on Vehicle Technology and Intelligent Transport Systems*, 2017.

[13] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, “Effective intrusion detection and prevention for the commercial vehicle sae j1939 can bus,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 17425–17439, 2022.

[14] B. Groza, L. Popa, T. Andreica, P.-S. Murvay, A. Shabtai, and Y. Elovici, “Panopticans - adversary-resilient architectures for controller area networks,” in *Computer Security – ESORICS 2022*, V. Atluri, R. Di Pietro, C. D. Jensen, and W. Meng, Eds. Cham: Springer Nature Switzerland, 2022, pp. 658–679.

[15] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, “Impact of wiring characteristics on voltage-based fingerprinting in controller area networks,” in *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2023, pp. 000231–000236.