GEORGE EMIL PALADE UNIVERSITY OF MEDICINE, PHARMACY, SCIENCE, AND TECHNOLOGY OF TÂRGU MUREȘ

DOCTORAL SCHOOL OF LETTERS, HUMANITIES AND APPLIED SCIENCES

INFORMATICS

UNIVERSITY OF GENEVA

SCHOOL OF ECONOMICS AND MANAGEMENT

INFORMATION SYSTEMS

TRUSTED SOFTWARE-DEFINED VEHICLES

Joint PhD Thesis

by

Teri LENARD

Scientific Supervisors:
Prof. Béla GENGE - G. E. Palade University of Medicine, Pharmacy, Science, and Technology of Târgu Mureș, Romania
Dr. Niels A. NIJDAM - University of Geneva, Switzerland
Dr. Anastasija COLLEN - University of Geneva, Switzerland
Prof. Dimitri KONSTANTAS - University of Geneva, Switzerland

2024

Capitolul 1

Introducere

Sistemele definite de software au apărut în ultimele decenii ca o arhitectură orientată pe servicii care utilizează componentele fizice ale unui sistem ca o fundație agnostică pentru construirea unui mediu software controlabil și bogat în funcționalități software [1]. O arhitectură orientată pe servicii încapsulează grupuri de servicii software distribuite pe un sistem de rețea. Prin intermediul unui sistem orientat pe servicii, proiectanții pot defini interfețe de comunicare standardizate flexibile, separarea și abstractizarea serviciilor de componentele fizice prin virtualizare, actualizări continue de la distanță, cât și monitorizarea sistemului și managementul acestuia [2]. Recent, beneficiile tehnologice și operaționale ale unei arhitecturi orientate pe servicii au început să fie adoptate de producătorii care dezvoltă arhitecturi electrice/electronice [3]. Motivația acestui fenomen constă în mai multe limitări impuse de o arhitectură electrică/electronică, în ceea ce privește de întreținerea sistemului, de actualizare a software-ului, de implementare a funcțiilor și de gestionare. O arhitectură electrică/electronică necesită acces fizic și, de obicei, intervenție umană pentru a efectua aceste operațiuni. În consecință, dispozitivele electrice/electronice (de exemplu, senzori, unități de control) au fost proiectate cu o durată de viață lungă.

Un exemplu concret de arhitectură electrică/electronică este cea a sistemelor automotiv, ce se poate definii ca un sistem distribuit ce a fost proiectat pentru a oferii o infrastructură de comunicare rezistentă la erorile, ce poate gestiona în siguranță funcționalitățile autovehiculului [4]. Arhitectură electrică/electronică a sistemelor automotiv a fost concepută pentru a fi autonomă și deconectată de la Internet [5]. Arhitectura vehiculelor contemporane și viitoare, va conține funcționalități software complexe, capabile să proceseze date provenite de la senzori (de exemplu, GPS, LiDAR, ultrasunete, video) pentru a obține autonomia vehiculului [6], comunicare cu infrastructura orașului și cloud pentru a optimiza planificarea rutelor [7], sau raportarea datelor către servicii externe pentru managementul serviciilor [8]. În consecință, acest lucru implică necesitatea interconectării cu infrastructura și menținerea persistentă a conexiunilor dintre serviciile vehiculului și cloud.

Pentru a îndeplinii aceste funcționalități, arhitectura electrică/electronică a automobilelor este complementată cu o arhitectură orientată spre servicii, transformând vehiculul tradițional într-un vehicul definit software. Conform lui Liu, Zhang și Zhao [1], baza vehiculelor definite software constă în componentele fizice funcționale (de exemplu, senzori digitali și analogici, unități de control), care sunt interconectate prin canalele de comunicare, peste care software-ul funcțional și de control este implementat pentru a gestiona funcțiile vehiculului. La nivelul de arhitectură orientată pe servicii, baza constă într-un sistem de operare de timp real și un middleware pentru a permite comunicarea între servicii, peste care se află stratul de servicii și aplicații. Aici, funcțiile vehiculului sunt implementate ca aplicații funcționale sau de servicii. În cele din urmă, serviciile cloud asistă și comunică cu stratul de servicii din interiorul vehicolului.

Teza de fază propune următoarele contribuții. Serviciul de distribuție a cheilor este propus ca soluție pentru distribuirea în siguranță a cheilor criptografice de criptare de termen lung și chei criptografice de autentificare de termen scurt pentru aplicații funcționale și servicii. Un al doilea serviciul de distribuție a cheilor este propus pentru distribuirea cheilor de autentificare simetrice de termen scurt între grupuri de servicii care trebuie să interacționeze cu unități de control limitate din punct de vedere computațional care funcționează la nivelul arhitecturii electrice/electronice. Totodată, serviciul de autentificare a datelor este introdus ca un serviciu de securitate care agreghează și autentifică mai multe seturi de mesaje, ce permite în paralel verificarea independentă a datelor. Un sistem de detecție a intruziunilor și un firewall a fost proiectat pentru monitorizarea rețelei de comunicare. În cele din urmă, un serviciu de logare în siguranța este utilizat pentru a înregistra, semna și raporta alertele de securitate.

Corectitudinea proiectării serviciilor de securitate propuse este demonstrată prin intermediul logicii Burrows-Abadi-Needham (BAN). Ulterior, proprietățile de securitate verificate cu logica BAN sunt analizate în cadrul modelului adversarului Dolev-Yao. Mai apoi, este propus un model de încredere este propus. Prin acest model este investigat modul în care comportamentul serviciilor este afectat atunci când un atacator este prezent în sistem. Un model de proces decizional markovian este utilizat pentru a modela încrederea ca probabilități ale unui atac de a fi cu succes sau de a fi detectat în sistem. În ceea ce privește evaluarea experimentală, serviciile de securitate au fost implementate într-o platformă de tip testbed. Testbed-ul a fost folosit pentru efectuarea evaluărilor de securitate și performanță. Pe platforma testbed, a fost efectuată o evaluare experimentală extinsă pentru a măsura resursele de calcul necesare și de rețea ale serviciilor propuse și pentru a reproduce scenariile de atac investigate în modelul de încredere.

1.1 Motivația Cercetării

Principala problemă cu care s-a confruntat arhitectura electrică/electronică a sistemelor automotiv a fost lipsa elementelor de securitate încorporate în proiectarea sa inițială. În consecință, aceasta a declanșat un domeniu de cercetare activ [9]. În prezent, atât mediul academic, cât și industrial sunt conștiente de nevoia securității în aceste sisteme [10]. Problemele de securitate, amenințările și provocările au fost cercetate și definite pe larg în literatura de specialitate [11], iar eforturile în vederea standardizării practicilor necesare sunt realizate de organizații specifice. Stratul orientat pe servicii introdus suplimentar în vehiculele definite software prezintă provocări și dificultăți de securitate [12]. Pham și Xiong [13] au confirmat această afirmație prin studiul lor în care au explorat probleme și soluții de securitate emergente care vizează vehiculele autonome conectate. Acest argumentul este întărit și de Nanda et al. [14] care și-au exprimat îngrijorarea cu privire la dificultatea de a estima impactul amenințărilor cibernetice vehicule definite software.

Unificarea arhitecturii vehiculelor definite software cu securitatea și încrederea, necesită evaluări și analize suplimentare. În plus față de testarea tradițională a calității implementării, serviciile de securitate necesită mai întâi definirea unor specificații formale în faza de proiectare. În al doilea rând, specificația formală trebuie să fie verificată prin dovezi formale pentru a determina corectitudinea serviciului și pentru a identifica probleme de proiectare. Acest lucru se face, de obicei, sub anumite ipoteze privind abilitățiile adversarilor. În plus, dovedirea corectitudinii unui serviciu de securitate în mod individual nu este suficientă. Specificația unui serviciu de securitate trebuie să fie validată în raport cu alte servicii preconizate a fi executate în paralel. Odată ce corectitudinea formală a unui serviciu de securitate este validată, următorul pas este implementarea. Prin abstractizarea de detaliile tehnice (de exemplu, securitatea codului), ultimul pas implică replicarea proprietăților și a modelului adversarial în experimente și validări într-un sistem real.

Pe baza celor menționate mai sus, urmatoarele întrebări de cercetare (IC) au fost definite:

- **IC1**: Cum se poate definii încrederea, și care este abordarea cea mai potrivită pentru asigura încrederea în contextul vehiculelor definite software?
- **IC2**: Ce proprietăți de încredere se pot dobândii prin proiectarea serviciilor de securitate prin intermediul componentelor fizice de securitate la nivelul de servicii al vehiculelor definite software?
- **IC3**: Ce abordări formale trebuie urmate pentru a demonstra corectitudinea sistemului de servicii de securitate propus?

1.2 Obiective Științifice

Scopul Obiectivelor Științifice (OC) este acela de a ghida în direcția potrivită cercetarea științifică, în vederea proiectării, implementării și verificării corespunzatoare a solutilor de securitate și de încredere propuse. Așadar, patru obiective de cercetare au fost definite:

- **OC1**: Identificarea unui sistem de comunicare ce suferă schimbări în arhitectură, de la o arhitectură electrică/electronică la o arhitectură orientată pe servicii.
- **OC2**: Definirea unui set de recomandări pentru asigurarea securității și al încrederii în arhitectura de sistem identificată în OC1..
- **OC3**: Adresează recomandăriile de securitate și încredere definite în OC2, prin proiectarea unui sistem de servicii de securitate corespunzător arhitecturii de sistem identificate în OC1.
- **OC4**: Efectuează experimentele, validările, verificările necesare pentru a demonstra corectitudinea proiectării și implementării serviciilor de securitate.

1.3 Structura Tezei

Teza este structurată pe următoarele capitole:

- **Capitolul 2**: Adresează fundamentele teoretice și terminologia în contextul vehiculelor definite software, și din jurul conceptului de încredere. Acest capitol prezintă două definiții distincte pentru conceptul de încredere: încrederea „tare" (hard trust) și încrederea „ușoară" (soft trust). Totodată, acest capitol oferă o analiză profundă a literaturii științifice acoperind metode de modelare a încrederii, cât și servicii de securitate în contextul vehiculelor definite software. Acest capitol se înceie prin propunerea unui set de recomandări prin care se poate garanta încrederea in vehicule definite software.
- **Capitolul 3**: Cel de al treilea capitol al tezei prezintă proiectarea sistemului de servicii de securitate propus. Fiecare serviciu de securitate propus este descris formal, prezentând în paralel funcționalitățile sale principale, cât și rolul pe care îl are în întregul sistem.
- **Capitolul 4**: În capitolul patru, o analiză formală a serviciilor de securitate a fost efectuată. Analiza formală a serviciilor de securitate include o analiză pe baza logicii Burrows–Abadi–Needham (BAN) logic unde a fost determinată corectitudinea proiectării serviciilor. După aceea, o analiză de securitate automată a fost considerată sub modelul adversarial Dolev-Yao prin intermediul utilitarului

Scyther. În final, o analiză probabilisitică a fost efectuată printr-un model de încredere bazat pe procese de decizie markoviene.

- **Capitolul 5**: Complementează capitolul precedent prin intermediul evaluării performanței și a securității servicilor propuse. Scopul acestor experimente este acela de a oferii măsurători legate de consumul resurselor computaționale și cel al încărcării de rețea din perspectiva implementării serviciilor. Aceste evaluări și experimente au fost efectuate pe o platformă de testare implementată pentru a replică un sistem automotiv simplificat.

- **Capitolul 6**: În final, capitolul șase concluzionează cercetarea tezei prin a oferii răspunsuri întrebărilor de cercetare ridicate, și verifică faptul că obiectivele de cercetare au fost adresate de către rezultatele tezei. Totodată, acest capitol prezintă principalele contribuții științifice ale tezei.

Capitolul 2

Context și Literatura de Specialitate

Cel de al doilea adresează contextul și analizează literatura de specialitate în legătură cu conceptul de încredere, securitate, și vehicule definite software. Două definiții ale încrederii au fost identificate în literatura științifică în contextul securității sistemelor informatice, și anume încrederea ușoară (soft trust) și încrederea tare (hard trust). În ambele cazuri, definiții concise sunt date, împreună cu terminologia lerevantă. Scopul aici este de a investiga posibilele direcții din literatura științifică care au scopul de a definirea încrederii în contextul securității sistemelor, nu în mod specific vehiculelor definite software. Din definițiile identificate, literatura de specialitate este analizată din punct de vedere al modele de încredere și al serviciilor de securitate.

2.1 Software-Defined Vehicles

Schimbarea în arhitectură a sistemelor automotive de la o arhitectură electrică/electronică la o arhitectură orientată pe servicii, și în final la vehicule definite software, a fost în principal influențată de către cererile de cerențiele și funcționalitățile noi necesare de a fi integrate în sistemele automotiv pentru a îmbunătății calitatea serviciilor oferită, siguranța sistemului și al regularizărilor impuse. Inițial, sistemele automotiv electrice/electronice au suferit prima schimbare majoră cu introducerea unităților de control și a protocolului de comunicare Controller Area Network (CAN) [15]. Acum, sistemele automotiv beneficiază de canale de comunicare cu rate de transmitere ridicate, sisteme de asistență inteligentă la condus, diverse servicii digitale, și funcționalități ce permit decizii autonome ale vehicolului [16]. Din punct de vedere al arhitecturii de sistem, sistemele automotiv electrice/electronice conțin dispozitive încorporate de control și comunicare, senzori digitali și analogici, actuatori, gateway-uri, sistem de diagnoză, și o interfață de comunicare om-mașină. Toate aceste componente și sisteme sunt distribuite pe mai multe subrețele, și au ca și ultimul scop de a controla

funcționalitățile unui vehicul. Arhitectura orientată pe servicii pe de altă parte, conține un număr de funcționalități distincte. Aceasta are ca și scop interconectarea mai multor domenii de comunicare in vehicul. În fiecare domeniu, funcționalitățile unităților de control sunt implementate în una sau mai multe platforme cu capacități computaționale ridicate [5]. Totodată, in arhitectura orientată pe servicii, sunt prezente unități de procesare date cu capacități de calcul ridicat capbile să ia decizii în timp real [17].

2.2 Definiția Conceptelor de Încredere și Securitate

Conceptul de încredere reprezintă un principiu fundamental pe baza căruia relațiile umane au fost construite, menținute și distruse. Diego [18] definește conceptul de încredere ca o probabilitate subiectivă pe care un agent o are asupra altui agent sau grupuri de agenți că aceștia vor efectua anumite acțiuni. Deoarece această definiție provine din științele sociale, în literatura științifică a sistemelor de securitate, conotația încrederii poate varia de la context la context. În consecință, clarificăm noțiunea de încredere prin două definiții distincte: încrederea ușoară (soft trust) și încrederea tare (hard trust).

Definiția Încrederii Ușoară (Soft Trust)

Prima definiție a încrederii găsită în literatura științifică este încrederea ușoară. Încrederea ușoară ca și concept este frecvent definită ca fiind gradul de probabilitate subiectivă cu care un agent evaluează faptul că un alt agent sau grup de agenți va efectua o anumită acțiune [18]. În contextul sistemelor de securitate, o abordare comună utilizată pentru a adresa problema încrederii este modelarea și gestionarea încrederii. Abordările de modelare și gestionarea încrederii permit sistemelor să funcționeze mai fiabile, stimulând și îmbunătățind cooperarea între nodurile sistemului [19]. Adoptat în domeniul securității sistemelor din științele sociale, tehnicile de modelare și gestionarea încrederii descriu încrederea ușoară ca fiind o valoare măsurabilă ce evoluează în timp. O relație de încredere este stabilită între un membrii sau participanții sistemului. Un participant într-o relatție de încredere consideră că relația este demnă de încredere dacă un participant implicat în această relație este în măsură să îndeplinească o sarcină specifică [18]. Modelarea încrederii analizează modul în care evoluează încrederea într-un grup compus din mai mulți participanți, pe baza unei serii de observații curente și trecute ce servesc ca date de intrare pentru funcțiile de măsurare a încrederii [19]. Gestionarea încrederii, pe de altă parte, se concentrează pe colectarea observațiilor necesare pentru a stabili relații de încredere și monitorizarea dinamică și gestionarea relațiilor.

Definiția Încrederii Tari (Hard Trust)

Problema încrederii într-o componentă a sistemului devine mai complexă odată cu introducerea celei de-a doua definiții. Înainte de a sublinia ce este încrederea tare, trebuie să trebuie să recunoaștem că implicația de bază a încrederii într-un echipament sau chiar într-o bucată de software, poate manifesta subtilități care duc la concluzia că încrederea nu poate fi realizată într-un sistem. Problema devine mai gravă dacă luăm în considerare argumentul lui Thompson [20] că încrederea devine mai complexă pe măsură ce coborâm scara de la software, la dezvoltator, sau aspecte juridice și sociale. Gollmann [21] a ridicat problema că încrederea este un termen nepotrivit care să fie asociat cu securitatea sistemelor. El își susține afirmația motivând că încrederea este un termen frecvent utilizat greșit în domeniul securității, subliniind faptul că definițiile încrederii sunt dependente de context și pot fi interpretate diferit în funcție de subdomeniul de cercetare în domeniul securității, cu cazuri extreme cazuri extreme în care încrederea este interpretată complet greșit pentru a desemna un concept contrar.

O platformă care poate ajuta la construirea componentelor necesare pentru apărarea sistemului este standardul Trusted Platform Module (TPM). O observație importantă aici este să nu interpretăm greșit termenii care înconjoară TPM-ul cu conceptul de încredere, așa cum a fost definit anterior. TPM-ul reprezintă o rădăcină de încredere ce încapsulează setul minim de funcționalități de securitate pe care o platformă (de exemplu, un echipament) trebuie să îl dețină pentru a oferi o descriere verificabilă a platformei. Inițial destinat aplicațiilor de sistem orientate către utilizator în prezent, standardul TPM se ramifică în domenii precum Internetul obiectelor (IoT) și sistemele automotiv [22]. Acest standard a fost dezvoltat pentru a descrie o componentă de securitate care poate servi drept bază pentru proiectarea și punerea în aplicare a serviciilor de securitate. Deoarece TPM-urile sunt componente fizice, acestea trebuie integrate în etapa de proiectare a arhitecturii sistemului. TPM-urile sunt doar o componentă fizică care pot: genera și stoca în siguranță chei criptografice, executa operațiuni criptografice (de exemplu, criptare, hashing, semnătură digitală), să efectueze boot-uri de încredere și măsurate și oferă capabilitatea de atestare de la distanță. În consecință, primitivele și proprietățile criptografice ale TPM pot reprezenta, la nivel de serviciu, o bază solidă pentru obținerea unei încrederi tari în componenta sistemului.

2.3 Tehnici de Modelare a Încrederii

Modelarea încrederii ușoare este, în cele din urmă, un mecanism de securitate conceput pentru a impune interacțiuni fiabile și de încredere în cadrul unui grup de agenți. În plus, în mecanismele de luare a deciziilor, modelarea încrederii se concentrează pe pedepsirea nodurilor necooperante (de exemplu, nodurile neîncrezătoare) care tind să perturbe comportamentul funcțional așteptat al rețelei. În consecință, este esențial ca o tehnică de modelare a încrederii soft să fie rezistentă la amenințări. Atacurile de încredere îmbină

aspecte din atacurile tradiționale orientate spre rețea cu comportamentul răuvoitor pe care agenții îl exercită în grupurile sociale.

Secțiunea de față explorează tehnici de modelare a încrederii în diferite sisteme informatice. Tehnicile abordate sunt tehnici bazate pe probabilități și tratarea incertitudinii în informații, tehnici fuzzy, modele bayesiene, machine learning, sau tehnici de formare a grupurilor.

2.4 Servicii de Securitate

Domeniul serviciilor de securitate în contextul sistemelor automotiv reprezintă un domeniu de cercetare abordat în detaliu în ultimii ani, prin lucrări individuale și articole de analiză. Martinez-Cruz et al. [11] și Rathore et al. Rathore et al. [10] oferă studii cuprinzătoare ale problemelor, amenințărilor, provocărilor și cele mai relevante soluții pentru securitatea sistemelor la bordul vehiculelor. În mod similar, Lokman, Othman, și Abu-Bakar [23] acoperă subiectul sistemului de detectare a intruziunilor în sistemele automotiv, oferind o analiză comparativă a soluțiilor existente. Lucrări mai recente, cum ar fi Rathore et al. [10] motivează în continuare necesitatea unor mecanisme de securitate solide. Autorii își menționează îngrijorarea cu privire la evoluția continuă a rețelelor de vehicule (de exemplu, vehicule inteligente și interconectate) și amenințările care pot apărea ca urmare a acestui proces. Pentru a aborda în continuare viitoarelor probleme de securitate în sistemele automotiv, Pham și Xiong [13] au explorat amenințările la adresa securității și soluțiile existente care vizează în special vehiculele autonome conectate. Deoarece sistemele automotiv devin din ce în ce mai conectate, tehnologia este împinsă spre comunicarea între vehicule și conexiunea persistentă cu servicii externe; prin urmare, este dificil de estimat impactul pe care amenințările îl vor avea asupra securității sistemului [14].

Secțiunea de față explorează servicii existente în literatura de specialitate ce au ca și scop protejarea unui sistem automotiv, cum ar fi servicii de distribuire de chei criptografice, autentificare date, detectarea intruziunilor și monitorizarea rețelei de comunicare, cât și de logare sigură a datelor.

2.5 Recomandări pentru Asigurarea Încrederii în Vehicule Definite Software

Pentru a începe construirea lanțului de încredere în vehiculele definite software, este obligatoriu pentru încrederea tare să existe o componentă a sistemului (de exemplu, software sau fizică) care să fie de încredere de la la început (de exemplu, o pereche de chei criptografice, certificate de încredere, o componentă hardware). Analiza noastră evidențiază faptul că componentele de securitate fizice precum modulele de securitate hardware (HSM) sau TPM-urile pot servi drept rădăcină de încredere pentru a crea

lanțul de încredere al sistemului. Aceste componente de securitate permit unităților de control dintr-un vehicul definit software să execute protocoale de distribuire de chei pentru comunicarea securizată, identificarea, autentificarea datelor, atestarea și autorizare, pe baza primitivelor de securitate stocate în componenta de securitate fizică.

Monitorizarea și analiza comunicațiilor implică prezența firewall-urilor și a sistemelor de detectare a intruziunilor. Prin intermediul firewall-urilor, se poate realiza delimitarea rețelei și filtrarea traficului. Prin intermediul sistemelor de detecție al intruziunilor, frecvența, conținutul sau periodicitatea transmiterii mesajelor pot fi determinate dacă acestea corespund unor comportamente anormale (de exemplu, malițioase). Necesitatea acestor componente de securitate este motivată și de faptul că există întotdeauna un risc pentru o componentă a sistemului, care participă la schimburi de comunicații sigure, să fie compromisă. În astfel de cazuri, firewall-urile pot limita raza de acțiune a atacatorului, iar sistemel de monitorizare pot detecta dacă traficul generat de atacator este legat de comportamente anormale comportamente anormale. Atunci când are loc o detecție (de exemplu, a fost detectată prezența unui atac) sau o eroare în serviciile de schimb de comunicații securizate, trebuie generate alerte de securitate. Prin logare securizată logare, alertele pot fi protejate împotriva atacatorilor care intenționează să șteargă intervenția lor în sistem.

Modelarea încrederii ușuare intervine în înțelegerea impactului, consecințelor și propagării unui atac în sistem și modul în care mecanismele de apărare reacționează. Având în vedere că un vehicul definit software rulează mai multe componente de securitate (de exemplu, servicii), parametrii de încredere pot fi definiți ca rezultatul în termeni de evenimente care rezultă din astfel de servicii. De exemplu, având în vedere că există componente într-un vehicul definit software care schimbă date autentificate, eșecurile ulterioare multiple în autentificarea datelor pot defini o metrică de încredere legată de securitatea comunicațiilor. Dacă eșecurile în autentificarea datelor apar pe o perioadă lungă de timp, acest lucru poate indica prezența unui atacator sau o defecțiune a sistemului. În mod similar, dacă un vehicul definit software raportează de-a lungul timpului că au apărut comportamente anormale, alertele generate scad gradul de încredere al acestuia. Detecțiile și erorile provenite de la componentele de securitate trebuie să fie înregistrate și raportate în siguranță.

Capitolul 3

Proiectarea Serviciilor de Securitate pentru Vehicule Definite Software

Teza contribuie la literatura științifică prin propunerea unei arhitectură de servicii de securitate pentru vehiculele definite software care include mecanisme de apărare de securitate. Arhitectura propusă a serviciilor de securitate include două servicii de distribuție a cheilor de distribuție, care îndeplinesc sarcina de actualizare a cheilor de criptare pe termen lung și a cheilor de autentificare pe termen scurt. În plus, servciul de autentificare date este introdus pentru a permite serviciilor și unităților de control să agregheze mai multe etichete de autentificare într-o singură structură de date care poate fi verificată independent. Un serviciul firewall și unul de detectare al intruziunilor sunt propuse ca o soluție pentru monitorizarea și filtrarea traficului de comunicații, impunerea delimitării rețelei și pentru a efectua inspecția detaliată a pachetelor. În cele din urmă, este propus un serviciul capabil să stocheze sigur alerte de securitate. Standardul Trusted Platform Module este introdus în proiectarea serviciilor de securitate ca o componentă fizică de securitate pentru a ajuta serviciile propuse să efectueze în siguranță operațiuni criptografice.

3.1 Arhitectura Propusă

Pentru a completa vehiculul definit software cu servicii de securitate, au fost proiectate cinci servicii de securitate. Cheile criptografice sunt distribuite prin două servicii distincte servicii distincte. Primul serviciul de distribuție a cheilor a fost conceput pentru a distribui chei criptografice de criptare pe termen lung și de autentificare pe termen scurt. Cheia pe termen lung este distribuită prin intermediul unui set de chei principale partajate. În plus, cheia pe termen lung este valorificată periodic, la intervale de timp mai scurte, pentru a actualiza cheile de autentificare. Deși acest serviciu

este conceput în mod intenționat pe baza standardului Trusted Platform Module, un al doilea serviciu de distribuție a cheilor a fost proiectat pentru a actualiza chei de autentificare pe termen scurt fără a fi nevoie de un TPM, vizând unităţi de control cu capacitate de calcul redusă. Mesajele schimbate de unitățile de control și servicii sunt autentificate prin intermediul serviciului de autentificare a datelor care utilizează un serviciu de distribuție a cheilor pe termen scurt pentru a obține cheia necesaă acestui proces. Serviciul firewall și sistemul de detectare a intruziunilor monitorizează și filtrează pachetele, impune delimitarea rețelei și efectuează inspecția detaliată a pachetelor pe baza unui fișier de reguli. Atunci când o alertă este generată sau o eroare apare în sistem, se generează o alertă de securitate care este transmisă către serviciul de stocare sigură care le înregistrează prin intermediul stardatului TPM.

3.2 Servicii de Distribuire a Cheilor

În teza de față, sunt propuse două servicii distincte de distribuție a cheilor. În ambele servicii, există două roluri, un distribuitor de chei și un grup de receptori al cheilor. Primul serviciu conține trei funcționalități distincte. În primul rând, distribuitorul este responsabil cu publicarea sigură a cheilor criptografice simetrice de criptare pe termen lung. În mod similar, acesta permite distribuirea dinamică a cheilor pentru chei de autentificare de scurtă durată. În al treilea rând, acest serviciu permite receptorilor să se sincronizeze cu distribuitorul de chei prin intermediul unui mecanism de sincronizare al cheilor. Pe de altă parte, al doilea serviciu este propus ca o alternativă pentru distribuția cheilor, ce utilizează un algoritm de traversare al unui lanțului hash invers ca funcție de derivare a cheii, pentru unități de control limitate din punct de vedere computațional.

3.3 Serviciul de Autentificare Date

Serviciul de autentificare date folosește o strucură de date de tipul bloom filter pentru agregarea etichetelor de autenficiare. Printr-o asemenea abordare, este permis unu emițător de date să comunice cu un grup de receptori, ce pot verifica independent etichetele în funcție de mesajele monitorizate. Serviciul de autentificare date decuplează procesul de verificare a datelor de procesul de transmitere. Totodată, acest serviciu folosește o cheie de autentificare simetrică pentru calcularea etichetelor de autentificare.

3.4 Serviciul Firewall și de Detecție al Intruziunilor

Această secțiune prezintă un serviciul firewall cu stare propus, împreună cu un sistem de detectare a intruziunilor bazat pe semnături. În scopuri demonstrative, protocolul CAN este utilizat pentru a arăta cum poate fi concepută o astfel de soluție poate fi concepută. Prin utilizarea unui set de reguli de tip listă albă și listă neagră, firewall-ul este capabil

să filtreze cadre CAN și secvențe de cadre CAN. În mod similar, serviciul de detecție al intruziunilor extinde proprietățile firewall-ului cu capacitatea suplimentară de a efectua o inspecție aprofundată a pachetelor la nivelul octeților din cadrele CAN.

3.5 Serviciul de Jurnalizare Sigură

Jurnalele sigure sunt necesare pentru o monitorizare și o analiză corespunzătoare a sistemului. Pe lângă alertele de securitate, evenimentele care denotă intruziuni în sistem sau erori în serviciile de securitate, evenimentele critice ale sistemului trebuie înregistrate periodic și raportate către autorităților de încredere pentru verificare și răspuns. Dacă aceste proprietăți nu sunt garantate de serviciul de jurnalizare, jurnalele sunt vulnerabile la manipularea de către actori amenințători care pot să falsifice istoricul jurnalelor comise ulterior atacului lor. Serviciul de jurnalizare sigură este propus pentru a înregistra în mod securizat aceste evenimente generate de către serviciile propupse prin intermediul standardului Trusted Platform Module.

Capitolul 4

Analiza Formală a Securității Serviciilor

Analiza formală a securității serviciilor permite verificarea proiectării prin demonstrarea corectitudinii acestora. Acest aspect poate include analiza simbolică și demonstrarea teoremei, logica formală sau verificarea modelului. Rezultatele obținute în urma unei analize formale sunt strict legate de ipoteza și modelul de atacator luat în considerare. În cele din urmă, ipotezele ridicate cu privire la capacitățile atacatorului determină dacă, într-un anumit scenariu, proiectarea analizată este corectă sau nu.

În primul rând, serviciile propuse au fost analizate cu logica BAN [24] pentru a verifica raționamentul anumitor proprietăți de securitate ale serviciilor. Ulterior, dovezile de corectitudine obținute din logica BAN au fost extinse în continuare cu o analiză de securitate în cadrul modelului adversarial Dolev-Yao [25] utilizând utilitarul Scyther. Serviciile de securitate care au fost analizate aici sunt serviciile de distribuire de chei și cel de autentificare date.

Un model de analiză al încredere a fost creat bazat pe un procese de decizie markoviene. Printr-o astfel de abordare, a fost modelat serviciul de autentificare date, serviciile de monitorizare rețea și cel de stocare sigură al alertelor. În acest context s-a studiat comportamentul acestora atunci când în sistem sunt prezente atacuri care vizează comunicarea. Natura probabilistică a modelului markovian a permis examinarea modului în care încrederea sistemului evoluează în timp în funcție de diferite probabilități de atac. Parametrii modelului au fost examinați pentru a permite selectarea optimă al acestora astfel încât probabilitatea de succes al unui atac sa fie minimă.

4.1 Determinarea Correctitudinii Servicilor prin logica Burrows–Abadi–Needham

Logica BAN este o logică formală care este utilizată pentru a analiza proiectarea protocoalelor de securitate. Scopul logicii BAN este de a oferi un cadru prin care un

proiectant poate demonstra corectitudinea unui protocol de securitate dintr-un punct de vedere formal, făcând abstracție de particularitățile implementării. Logica BAN este luată în considerare pentru a verifica corectitudinea de proiectare a serviciilor de distribuire chei și de autentificare date din punct de vedere formal. Logica BAN a fost aplicată pentru a demonstra corectitudinea și de a verifica proiectarea serviciilor de distribuire chei și autentificare date. Prin intermediul formalismului oferit de logica BAN, proprietățiile de securitate ale serviciilor menționate au fost verificate prin intermediul unor obiective de autentificare definite în timpul proiectării. Rezultatele pozitive obțiunute prin intermediul acestei verificări formale contribuie direct la încrederea în serviciile de securitate analizate.

4.2 Determinarea Correctitudinii Servicilor în Modelul Adversarial Dolev-Yao

Pentru a demonstra corectitudinea serviciilor de securitate din punct de vedere al unui model adversarial Dolev-Yao utilitarul Scyther a fost considerat. În modelul adversarial Dolve-Yao, se presupune că atacatorul controlează canalul de comunicare, unde acesta poate să recepționeze, trimită și modifica mesaje transmise. Totodată, atacatorul poate executa aceleași operații criptografice ca și actorii sau rolurile implicate în serviciile analizate daca acesta cunoaște cheile corespunzătoare. În acest utilitar, au fost definite specificațiile serviciilor de distribuire chei și serviciului de autentificare date. Pentru fiecare serviciu în parte au fost definite cerințele necesare ce trebuie să fie vericate. Aceste cerințe au ca și scop verificarea proprietăților de securitate exercitate de către serviciile analizate. Celei trei servicii analizate au fost verificate individual și în scenarii multiprotocol. Rezultatele obținute din aceste verificări formale arată că toate cerințele definite sunt verificate în scenarii individuale și multiprotocol.

4.3 Analiza Încrederii printr-un Model de Decizie Markov

Având în vedere setul de servicii de securitate propuse în teză, serviciul de autentificare a datelor se diferențiază prin natura sa probabilistică. Acesta decuplează procesul de autentificare a datelor de transmiterea efectivă a mesajului. Datorită acestui faptu utilizează o structură probabilistică de date pentru agregarea etichetelor de autentificare, prezentând o probabilitate fals pozitivă la interogarea elementelor, ceea ce permite unui atacator să injecteze mesaje modificate în timpul transmiterii. În plus, pentru ca un astfel de atac, există o probabilitate de detecție de către serviciile ce monitorizează rețeaua de comunicare. În funcție de configurația acestora, evenimentul va fi filtrat, blocat sau înregistrat ca o alertă de securitate alertă.

Pentru a modela acest scenariu, și pentru a analiza încrederea în serviciile implicate, un model de decizie markovian a fost proiectat ce conține următoare trei procese:

1. Transmițătorul: Rulează serviciul de autentificare a datelor împreună cu procesul receptor pentru a face schimb de mesaje autentificate. Trimite periodic un număr cunoscut de mesaje care necesită autentificare și, ulterior, filtrul Bloom care trebuie să fie verificate de receptor

2. Receptor: Ascultă mesajele trimise și execută procesul de verificare a mesajelor primite cu filtrul Bloom. În paralel, monitorizează rețeaua pentru mesaje injectate și generează alerte privind detectarea atacurilor

3. Atacator: Încearcă periodic să injecteze mesaje falsificate pentru a înșela procesul de autentificare.

4.3.1 Experimente și Rezultate

Un număr de patru experimente au fost efectuate pentru a analiza modul în care încrederea serviciilor de securitate este influențată atunci când apare o probabilitate de injectare a mesajului. Aici, am determinăt parametrii modelului de încredere cei mai afectați atunci când apare o probabilitate de injectare a mesajului are loc. Prin investigarea și analiza parametrilor modelului am ales parametrii cei mai potriviți ai modelului astfel încât probabilitatea de succes a unui atac de injectare să fie minimizată și detectarea acestuia să fie maximizată.

Capitolul 5

Evaluare Experimentală

Ulterior verificării și analizei formale, urmează implementarea serviciilor. În consecință, a fost dezvoltată o platformă de testare pentru a reproduce un mediu automotiv simplificat. Implementarea servește drept bază pentru evaluarea securității și performanței serviciilor propuse. Pe această platformă au fost efectuate două experimente de securitate pentru a investiga influența atacurilor asupra serviciului de autentificare date și a celor de monitorizare a rețelei. Scopul acestor experimente de securitate a fost să reproducă scenarile considerate în modelul de încredere, atacurile și rezultatele obținute în capitolul anterior. Mai apoi, au fost efectuate o serie de măsurători de performanță pentru fiecare dintre serviciile de securitate propuse. Această evaluare abordează consumul resurselor, împreună cu supraîncărcarea rețelei de comunicații. Pentru serviciul de autentificare de date, s-au efectuat măsurători pentru a determina timpul necesar pentru crearea și verificarea datelor. În cazul serviciilor de monitorizare a rețelei, a fost măsurată performanța acestora pentru un număr diferit de reguli. În cele din urmă, au fost efectuate măsurători computaționale privind operațiunile criptografice utilizate de serviciile de securitate cu TPM-ul. În ceea ce privește supraîncărcarea rețelei de comunicare, serviciul de autentificare date și cel de distribuire de chei au fost evaluate în mod specific, deoarece acestea reprezintă serviciile care necesită cea mai mare lățime de bandă.

5.1 Platforma de Testare

Platforma de testare dezvoltată replică rețeaua și componentele unui sistem automotiv. Componentele hardware utilizate sunt plăci de dezvoltare Raspberry Pi modelele 3B și 4, care rulează Raspberry Pi OS Lite, cu versiunea kernel 5.15 și Debian bullseye. Fiecare placă are conectat un OPTIGA SLx 9670 TPM 2.0, și un controler CAN MCP2515 cu un transceiver CAN TJA1050. TPM 2.0 OPTIGA SLx 9670 a fost considerat adecvat pentru cazul de față, deoarece a fost dezvoltat de Infineon special pentru domeniul automotiv. Platforma de testare conține trei interfețe de comunicare: interfața CAN

pentru comunicare între echipamente, interfața Message Queue Telemetry Transport (MQTT) pentru comunicare internă între servicii, și interfata TPM-ul pentru executarea funcțiilor acestuia de către un serviciu. Din punct de vedere al implementării, serviciul de autentificare date a fost implementat în python și în C/C++, serviciile de distribuire chei în python, serviciul de protejare date în python, iar serviciul firewall și de detecție al intruziunilor in C++.

5.2 Evaluarea Securității

Această secțiune analizează două scenarii de atac. Primul scenariu se concentrează pe serviciul de autenficare date, prin investigarea modului în care acesta reacționează în fața unui atac de tip injectare de mesaje. Al doilea scenariu îl extinde pe primul și arată cum reacționează serviciile de monitorizare a rețelei de comunicare în cazul mai multor posibile atacuri de tipul injectare de mesaje. Aceste scenarii replică modelul de atacator considerat în analiza formală din capitolul precedent, iar rezultatele obținute arată faptul că chiar daca există o probabilitate mică a unui atac cu succes, acesta la randul lui, este detectat de catre mechanismele de monitorizare a rețelei.

5.3 Evaluarea Performanței

5.3.1 Evaluarea Consumului Resurselor de Calcul

Secțiunea de față oferă măsurători computaționale din punct de vedere al consumului de resurse efectuate pe platforma de testare. Au fost luate în considerare patru scenarii distincte. Primul scenariu acoperă comenzile TPM-ului care sunt utilizate frecvent în serviciile de securitate. Mai apoi, timpii de calcul pentru funcțiile de construcție și verificare ale utilizate în serviciul de autentificare date. După aceea, performanța de serviciilor de monitorizare rețea este măsurată pentru diferite seturi de reguli și configurații diferite. În cele din urmă, algoritmul de traversare a lanțului hash invers utilizat în distribuirea de chei este evaluat.

5.3.2 Evaluarea Încărcării de Rețea

Integrarea unui nou serviciu de comunicații într-un sistem are ca și consecință încărcarea reței cu mesaje suplimentare. În sistemele automotiv, este imperativ să se mențină încărcarea rețelei de comunicare la un nivel acceptabil pentru a se asigura că sistemul își menține comportamentul normal de funcționare. Serviciile de comunicație de securitate sunt cunoscute ca având o încărcare crescută atunci când transmit date criptate, etichete de autentificare sau semnături digitale. În cazul unei rețele CAN, câmpul de date conține 64 de biți. În consecință, mesajele transmise de serviciile de securitate trebuie să fie împărțite în mai multe secvențe de mesaje CAN. Deși există mai multe variante ale

standardului CAN ce permite transmiterea mesajelor la viteze de până la 1Mbit/s și 5Mbit în cazul CAN-FD în conformitate cu ISO 11898-1, este esențial să se determine încărcarea rețelei de comunicare a serviciilor de securitate propuse pentru viteze de transmitere reduse. În consecință, supraîncărcarea de comunicare este măsurată pentru viteze de transmisie de 125kbit/s și 250kbit/s. Rezultatele obținute arată faptul ca serviciile analizate aduc o încărcătura acceptabila pentru o rețea de tipul CAN, cu ratele de transmitere precizate mai sus.

Capitolul 6

Concluzii Generale

Ultimul capitol al tezei oferă răspunsuri la întrebarile de cercetare (IC) ridicate la începutul cercetării, și determină dacă obiectivele de cercetare (OC) propuse au fost îndeplinite. Totodată, acest capitol menționează limitările cercetării, iar mai apoi prezintă contribuțile științifice. În final, direcțiile viitoare de cercetare sunt prezentate și discutate.

6.1 Răspunsuri la Întrebările de Cercetare

IC1: Cum se poate definii încrederea, și care este abordarea cea mai potrivită pentru asigura încrederea în contextul vehiculelor definite software?

Răspuns: Pentru a raspunde la prima întrebare de cercetare, în capitolul 2 al tezei, o analiza existinsă a literaturii științifice a fost realizată pentru a investiga terminologia, definițiile cât și metodele existente în contextul încrederii și cel al securității vehiculelor definite software. În consecință, două abordări distincte au fost identificate. Prima abordare tratează încrederea din punct de vedere al securității clasice al vehiculelor definite software, under serviciile de securitate au ca și scop apărarea sistemului în fața intervenților malițioase. Cea de a doua abordare, studiază modul în care încrederea poate fi modelată și este capabilă de a analiza modul în care serviciile de securitatea reacționează în momentul în care au de a face cu o intervenție malițioasă.

IC2: Ce proprietăți de încredere se pot dobândii prin proiectarea serviciilor de securitate prin intermediul componentelor fizice de securitate la nivelul de servicii al vehiculelor definite software?

Răspuns: În etapa de cercetare și proiectare (capitolul 2 și 3), a fost decis că componentele fizice de securitate reprezintă doar o componentă de bază ce ajută în proiectarea sigură a serviciilor de securitate. În același timp, a fost decis faptul că rolul

serviciilor de securitate este acela de a proteja sistemul de atacuri și intervenții malițioase. Așadar, abilitatea serviciilor de securitate de a rezista atacurilor determina nivelul de încredere. În capitolul 4, un model de încredere a fost proiectat în care încrederea a fost definită pe baza mai multor stări și comportamente generate de serviciile de securitate propuse. De exemplu, în cazul serviciului de autentificare a datelor, probabilitatea de fals pozitiv la interogarea unui element este considerată ca o metrică de încredere. În cazul serviciului firewall și cel de detecție al intruziunilor, a fost luat în considerare numărul de detecții declanșate de un atacator, iar în cazul serviciului de logare, numărul de alerte înregistrate. Prin intermediul modelului de încredere propus au fost obținute rezultate cuantificabile privind modul în care serviciile menționate reacționează atunci când se confruntă cu diferite atacuri. Analiza modelului de încredere ne-a ajutat să alegem cei mai potriviți parametrii ai sistemului pentru a minimiza probabilitatea de succes a unui atac.

IC3: Ce abordări formale trebuie urmate pentru a demonstra corectitudinea sistemului de servicii de securitate propus?

Răspuns: Pentru a demonstra corectitudinea serviciilor de securitate propuse, trei metodologii formale au fost considerate. În primul rând, analiza logică BAN a fost luată considerată pentru a verifica, raționaliza și corecta posibilele probleme în proiectarea serviciilor. După aceea, serviciile de securitate propuse au fost verificate în cadrul modelului adversarial Dolev-Yao pentru a determina corectitudinea acestora. În acest caz, am utilizat utilitarul Scyther pentru a investiga, găsi și corecta greșelile de proiectare care pot fi exploatate de un adversar. Prin utilitarului Scyther am efectuat analize individuale și multiprotocol. Rezultatele obținute arată că serviciile de securitate propuse nu sunt vulnerabile la atacurile multi-protocol. În al treilea rând, un model de încredere Markov Decision Process (MDP) a fost folosit pentru a investiga modul în care un atacator poate influența comportamentul funcțional al serviciilor de securitate și modul în care un atac cu succes poate fi în influența negativ comportamentul serviciilor.

6.2 Obiectivele Științifice Adresate

OC1: Identificarea unui sistem de comunicare ce suferă schimbări în arhitectură, de la o arhitectură electrică/electronică la o arhitectură orientată pe servicii.

Răspuns: Scopul OC1 este acela de a identifica un sistem definit software ce integrează un nivel de arhitectura orientată pe servicii peste un nivel existent electric/electronic. Capitolul 2 al tezei motivează necesitatea integrării componentelor de securitate în proiectarea unui asemenea sistem. Analiza literaturii de specialitate ne-a orientat către

sistemele automotive ce îndeplinesc acest criteriu. Acestea, initial au fost proiectate ca un sistem independent, neconectat la internet, care a avut ca și scop controlarea și gestionarea functionalităților vehicolului. Acum, sisteme automotiv încep să încorporeze componente software proiectate și implementate peste nivelul electric/electronic existent.

OC2: Definirea unui set de recomandări pentru asigurarea securității și al încrederii în arhitectura de sistem identificată în OC1.

Răspuns: După adresarea OC1, in OC2 și prin intermediul capitolului 2 a fost determinată diferența dintre terminologia încrederii și cea a securității. După aceea, literatura de specialitate a fost analizată pentru a identifica metodele cele mai potrivite pentru a modela încrederea și a asigura securitatea vehiculelor definite software. Pe baza acestor lucruri a fost dedus că serviciile de securitatea au ca și scop protejarea sistemului de atacuri și intruziuni malițioase. În același timp, mecanismele de modelare a încrederii sunt necesare pentru a determina și investiga modul în care comportamentul serviciilor de securitate reacționează în fața unui atac.

OC3: Adresează recomandăriile de securitate și încredere definite în OC2, prin proiectarea unui sistem de servicii de securitate corespunzător arhitecturii de sistem identificate în OC1.

Răspuns: Pentru a adresa OC3, in capitolul 3 al tezei a fost proiectat un sistem de servicii de securitate pe baza recomandărilor identificate în capitolul 2. Aceste servicii sunt:

- Serviciul de distribuire de chei de lungă și scurtă durată într-un grup de servicii.
- Serviciul de distribuire de chei de scurtă durată pentru echipamente cu capacități computaționale reduse.
- Serviciul de autentificare a datelor ce permite agregarea etichetelor de autentificare, cât și verificarea lor independentă într-o singură structură de date.
- Serviciul firewall și de detectare al intruziunilor pentru monitorizarea rețelei de comunicare pe baza unor reguli prestabilite.
- Serviciul de stocare sigură al alertelor de securitate.

Din perspectiva încrederii, în capitolul 4 a fost proiectat un model de decizie markovian pe baza căruia a fost investigat modul în care serviciile de securitate reacționează în diferite scenarii de atac. Prin intermediul acestui model, au fost obținute rezultate cantitative pe baza cărora au fost determinați parametrii optimi ai sistemului analizat astfel încât probabilitatea de succes a unui atac sa fie minimă.

OC4: Efectuează experimentele, validările, verificările necesare pentru a demonstra corectitudinea proiectării și implementării serviciilor de securitate.

Răspuns: Scientific Objective (SO)4 was accomplished in two phases. In the first phase (i.e., chapter 4), we used BAN logic, the Scyther tool, and PRISM model checker to validate, analyze and demonstrate the correctness of the proposed security services. Subsequently, we developed in chapter 5 a testbed platform that replicates Software-Defined Vehicle (SDV) communication. In the testbed plaform, prototype implementation of the proposed security services were integrated. The testbed was used to conduct benchmarking measurements to determine the computational and communication overhead of the security services. Additionally, security experiments were performed to replicate the attacks considered in chapter 4 for the trust model. The testbed contains multiple CAN communication channels, and Electronic Control Units (ECUs). Moreover, the testbed incorporates automotive-specific Trusted Platform Modules (TPMs), linux-based embedded development boards, CAN communication interfaces, controllers, and transceivers.

6.3 Contribuții Științifice

Contribuțile științifice ale tezei de față sunt sumarizate în cele ce urmează, în ordinea capitolelor tezei.

Capitolul 2

1. O analiza extinsă a literaturii în contextul modelelor de încredere cât și al serviciilor de securitate în domeniul automotive, ce încapsulează aproximativ 200 de articole științifice.

2. Definirea termenilor specifici și a unui set de recomandări pentru a asigura încrederea în vehicule definite software.

Capitolul 3

1. Proiectarea unui serviciu de distribuire de chei criptografice de tipul lungă și scurtă durată într-un grup de servicii.

2. Proiectarea unui serviciu de distribuire de chei criptografice de scurtă durată pentru echipamente cu capacități computaționale reduse.

3. Proiectarea unui serviciu de autentificare a datelor ce permite serviciilor și unităților de control agregarea etichetelor de autentificare, cât și verificarea independentă al acestora.

4. Proiectarea unui serviciul firewall și de monitorizare a intruziunilor bazat pe reguli.

5. Proiectarea unui serviciul de stocare sigură al alertelor de securitate.

Capitolul 4

1. Determinarea corectitudinii din punct de vedere al proiectării serviciilor de distribuire de chei, și de autentificare date prin intermediul logicii BAN.

2. Determinarea corectitudinii din punct de vedere al proiectării serviciilor de distribuire de chei, și de autentificare date prin intermediul unei analize formale având asumpțile modelului adversarial Dolev-Yao.

3. O analiză extinsă a încrederii în serviciile de autentificare date, firewall și detectare a intruziunilor, cât si de logare sigură, prin intermediul unui model de tip MDP, prin care s-a determinat evoluția încrederii în sistemul considerat în momentul în care există atacuri în sistem.

Capitolul 5

1. Proiectarea și implementarea unei platforme de testare.

2. Evaluarea securității serviciului de autentificare a datelor și a serviciului firewall și de monitorizare a intruziunilor în contextul atacurilor de tip injectare mesaje.

3. Evaluarea extinsă a performanței serviciilor de securitate propuse în contextul platformei de testare.

4. Evaluarea costului computational pentru standardul TPM în contextul platformei de testare.

5. Implementarea și dezvoltarea platformei de testare cu sursă deschisă în cadrul proiectului DIAS (*https://dias-project.com/*), ce a servit ca un demonstrator pentru servicii de securitate în sisteme automotiv.

6. Participarea în cadrul unui eveniment de tip Hackathon denumit Hack-A-Truck [1] organizat de consortiul proiectului DIAS, unde experți în securitate cibernetică au testat serviciul firewall și cel de detecție al intruziunilor.

[1] https://dias-project.com/node/74

Referințe

[1] Zongwei Liu, Wang Zhang, and Fuquan Zhao. "Impact, Challenges and Prospect of Software-Defined Vehicles". In: *Automotive Innovation* 5.2 (Apr. 2022), pp. 180–194. ISSN: 2096-4250. DOI: 10.1007/s42154-022-00179-z.

[2] James Taylor Faria Chaves and Sergio Antonio Andrade de Freitas. "A Systematic Literature Review for Service-Oriented Architecture and Agile Development". In: 2019, pp. 120–135. DOI: 10.1007/978-3-030-24308-1_11.

[3] Marcel Rumez et al. "An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures". In: *IEEE Access* 8 (2020), pp. 221852–221870. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.3043070.

[4] Hailong Zhu et al. "Requirements-Driven Automotive Electrical/Electronic Architecture: A Survey and Prospective Trends". In: *IEEE Access* 9 (2021), pp. 100096–100112. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3093077.

[5] Jan Becker. "Operating System for Software-defined Vehicles". In: *ATZelectronics worldwide* 17.5 (May 2022), pp. 40–45. ISSN: 2524-8804. DOI: 10.1007/s38314-022-0756-6.

[6] Araz Taeihagh and Hazel Si Min Lim. "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks". In: *Transport Reviews* 39.1 (Jan. 2019), pp. 103–128. ISSN: 0144-1647. DOI: 10.1080/01441647.2018.1494640.

[7] Ahmad Alalewi, Iyad Dayoub, and Soumaya Cherkaoui. "On 5G-V2X Use Cases and Enabling Technologies: A Comprehensive Survey". In: *IEEE Access* 9 (2021), pp. 107710–107737. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3100472.

[8] Meriem Benyahya et al. "Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments". In: *Computers & Security* 122 (Nov. 2022), p. 102904. ISSN: 01674048. DOI: 10.1016/j.cose.2022.102904.

[9] Akib Anwar et al. "Security assessment of in-vehicle communication protocols". In: *Vehicular Communications* (July 2023), p. 100639. ISSN: 22142096. DOI: 10.1016/j.vehcom.2023.100639.

[10] Rajkumar Singh Rathore et al. "In-Vehicle Communication Cyber Security: Challenges and Solutions". In: *Sensors* 22.17 (Sept. 2022), p. 6679. ISSN: 1424-8220. DOI: 10.3390/s22176679.

[11] Alfonso Martinez-Cruz et al. "Security on in-vehicle communication protocols: Issues, challenges, and future research directions". In: *Computer Communications* 180 (Dec. 2021), pp. 1–20. ISSN: 01403664. DOI: 10.1016/j.comcom.2021.08.027.

[12] Hrvoje Vdovic, Jurica Babic, and Vedran Podobnik. "Automotive Software in Connected and Autonomous Electric Vehicles: A Review". In: *IEEE Access* 7 (2019), pp. 166365–166379. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2019.2953568. URL: https://ieeexplore.ieee.org/document/8901126/.

[13] Minh Pham and Kaiqi Xiong. "A survey on security attacks and defense techniques for connected and autonomous vehicles". In: *Computers & Security* 109 (Oct. 2021), p. 102269. ISSN: 01674048. DOI: 10.1016/j.cose.2021.102269.

[14] Ashish Nanda et al. "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions". In: *IEEE Wireless Communications* 26.4 (Aug. 2019), pp. 60–65. ISSN: 1536-1284. DOI: 10.1109/MWC.2019.1800503.

[15] N. Navet et al. "Trends in Automotive Communication Systems". In: *Proceedings of the IEEE* 93.6 (June 2005), pp. 1204–1223. ISSN: 0018-9219. DOI: 10.1109/JPROC.2005.849725.

[16] Matthias Traub, Alexander Maier, and Kai L. Barbehon. "Future Automotive Architecture and the Impact of IT Trends". In: *IEEE Software* 34.3 (May 2017), pp. 27–32. ISSN: 0740-7459. DOI: 10.1109/MS.2017.69. URL: https://ieeexplore.ieee.org/document/7927914/.

[17] Mukul Anil Gosavi, Benjamin B. Rhoades, and James M. Conrad. "Application of Functional Safety in Autonomous Vehicles Using ISO 26262 Standard: A Survey". In: *SoutheastCon 2018*. IEEE, Apr. 2018, pp. 1–6. ISBN: 978-1-5386-6133-8. DOI: 10.1109/SECON.2018.8479057.

[18] Gambetta Diego. "Can We Trust Trust?" In: *Trust: Making and Breaking Cooperative Relations*. Ed. by Diego Gambetta. Blackwell, 1988, pp. 213–237.

[19] Marcela Mejia et al. "A review of trust modeling in ad hoc networks". In: *Internet Research* 19.1 (Jan. 2009), pp. 88–104. ISSN: 1066-2243. DOI: 10.1108/10662240910927849. URL: https://www.emerald.com/insight/content/doi/10.1108/10662240910927849/full/html.

[20] Ken Thompson. "Reflections on trusting trust". In: *Communications of the ACM* 27.8 (Aug. 1984), pp. 761–763. ISSN: 0001-0782. DOI: 10.1145/358198.358210.

[21] Dieter Gollmann. "Why Trust is Bad for Security". In: *Electronic Notes in Theoretical Computer Science* 157.3 (May 2006), pp. 3–9. ISSN: 15710661. DOI: 10.1016/j.entcs.2005.09.044. URL: https://linkinghub.elsevier.com/retrieve/pii/S1571066106002891.

[22] Trusted Computing Group. *TCG TPM 2.0 Automotive Thin Profile For TPM Family 2.0; Level 0*. 2020. URL: https://trustedcomputinggroup.org/resource/tcg-tpm-2-0-library-profile-for-automotive-thin/.

[23] Siti-Farhana Lokman, Abu Talib Othman, and Muhammad-Husaini Abu-Bakar. "Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review". In: *EURASIP Journal on Wireless Communications and Networking* 2019.1 (Dec. 2019), p. 184. ISSN: 1687-1499. DOI: 10.1186/s13638-019-1484-3.

[24] Michael Burrows, Martin Abadi, and Roger Needham. "A logic of authentication". In: *ACM Transactions on Computer Systems* 8.1 (Feb. 1990), pp. 18–36. ISSN: 0734-2071. DOI: 10.1145/77648.77649.

[25] D. Dolev and A. Yao. "On the security of public key protocols". In: *IEEE Transactions on Information Theory* 29.2 (Mar. 1983), pp. 198–208. ISSN: 0018-9448. DOI: 10.1109/TIT.1983.1056650.