Raport Ştiinţific Nr. 2

Proiect PN-III-P1-1.1-TE-2016-1317

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

(anul 2019)

Echipa

Prof. Habil.Dr. Ing. Bogdan Groza
S.l.Dr. Ing. Pal-Ştefan Murvay
S.l.Dr. Ing. Horaţiu Eugen Gurban
Drd. Ing. Adriana Maria Berdich
Drd. Ing. Lucian Tudor Popa

Universitatea Politehnica Timişoara

Decembrie 2019

Raport Ştiinţific Nr. 2

Proiect PN-III-P1-1.1-TE-2016-1317

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

Prezentul raport adresează activitatea ştiinţifică desfăşurată în cadrul proiectului **Proiect PN-III-P1-1.1-TE-2016-1317, Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente (PRESENCE)** în anul 2019. Stadiul curent de implementare al proiectului este menţinut la zi pe site-ul proiectului http://www.aut.upt.ro/~bgroza/projects/presence/index.html şi poate fi consultat pentru detalii suplimentare la acest raport (de ex., detalii din publicaţiile asociate ce sunt prea ample pentru a fi incluse în prezentul raport).

În conformitate cu contractul de finanţare, în anul 2018 am derulat ***Etapa 2 – Configurarea si controlul la distanta al vehiculelor cu dispozitive mobile inteligente***. Rezultatele acestei activităţi au fost estimate în contractul de finanţare la 3-4 lucrări susţinute în conferinţe şi 3 lucrări trimise către reviste ISI cu factor de impact 0.5-3. Am reuşit să îndeplinim şi chiar să depăşim această estimare, având în anul 2019 un total de 6 lucrări în conferințe (4 având doar autori din proiect, 2 cu co-autori din proiect), 2 lucrări acceptate în jurnale ISI Q1 şi 2 lucrări în curs de evaluare (trimise) la jurnale ISI. Lista celor publicate este după cum urmează:

- Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, TRICKS - time TRIggered Covert Key Sharing for Controller Area Networks, IEEE Access, vol. 7, 2019 - [J1] (Q1, IF 4.098)
- Bogdan Groza, Pal-Stefan Murvay, Identity-Based Key Exchange on In-Vehicle Networks: CAN-FD & FlexRay, Sensors, 22, 2019 - [J2] (Q1, IF 3.031)
- Bogdan Groza, Horatiu Gurban, Lucian Popa, Adriana Berdich, Pal-Stefan Murvay, Car-to-Smartphone Interactions: Experimental Setup, Risk Analysis and Security Technologies , 5th International Workshop on Critical Automotive Applications: Robustness & Safety (CARS), 2019 - [C1]

- Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, CarINA - Car sharing with IdeNtity based Access control re-enforced by TPM, 2nd International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms, SAFECOMP Workshops (STRIVE), 2019 - [C2]
- Tudor Andreica, Bogdan Groza, Secure V2V Communication with Identity-based Cryptography from License Plate Recognition, The Second International Workshop on Intelligent Transportation and Connected Vehicles Technologies (ITCVT), 2019 - [C3]
- Lucian Popa, Bogdan Groza, Pal-Stefan Murvay, Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers, Workshop on Industrial Security and IoT (WISI), in conjunction with the 14th International Conference on Availability, Reliability and Security, 2019 - [C4]
- Adrian Musuroi, Bogdan Groza, Stefan Murvay and Horatiu Gurban, Security for low-end automotive sensors: a tire-pressure and rain-light sensors case study, 9th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS), 2019 - [C5]
- Mario Vasile, Bogdan Groza, DeMetrA - Decentralized Metering with user Anonymity and layered privacy on Blockchain, 23rd International Conference on System Theory, Control and Computing (ICSTCC), 2019 - [C6]

Cu excepția lucrărilor [C5] şi [C6], toate lucrările au exclusiv autori membri în prezentul proiect şi prezintă la acknowledgement doar acest proiect ca sursă de finanțare (pentru lucrările [C5] şi [C6] primul autor a fost student la dizertaţie sub îndrumarea prof. Groza, fără a fi membru în proiect). Lucrările în curs de evaluare nu le putem enumera din motive de confidențialitate, afirmăm însă că sunt trimise la jurnale bune şi cu factori de impact apropiat sau mai mare decât cele deja acceptate. Lista de lucrări ştiinţifice este menţinută la zi şi poate fi consultată pe site-ul proiectului http://www.aut.upt.ro/~bgroza/projects/presence/publications.html

În cele ce urmează sintetizăm rezultatele obţinute în jurul activităților din proiect derulate în acest an şi pe baza lucrărilor publicate.

A1. Configurarea vehiculelor la distanta folosind servicii cloud

Înlocuirea cheilor clasice folosite pentru accesul la vehicule cu chei digitale este un pas natural în evoluția tehnologică a automobilelor. În acest context, folosirea telefonului mobil (smartphone) ca şi cheie si configurarea la distanță prin Internet (cloud) devin imediate. În această activitate ne-am concentrat pe două direcții: pe de o parte pe crearea unei chei de maşină pe telefonul mobil (implementare în Java pentru Android) care poate opera la distanţă prin canale TCP (sistemul de control al accesului în Java poate fi

imediat portat pe o maşină virtuală ce rulează în cloud), pe de altă parte pe folosirea unui serviciu cloud existent pentru un scenariu ipotetic de gestionare a unei flote de maşini, i.e., car-sharing (pentru aceasta am studiat posibilitatea de implementare şi integrare în Microsoft Azure).

În lucrarea [3] am propus un protocol de acces și control de la distanță al funcționalităților din vehicule folosind telefoane mobile inteligente. Folosirea telefoanelor mobile pentru accesul la vehicule aduce o serie de beneficii, precum flexibilitatea de a adăuga noi aplicații, accesul la anumite componente sau dispozitive specifice ale mașinii și posibilitatea de delegare a drepturilor către alți utilizatori (un alt context benefic este cel al identificării mașinilor cu telefoane mobile după numerele de înmatriculare despre care am publicat de asemenea rezultate în [6]). Toate aceste beneficii sunt înglobate în conceptul nostru propus în [3]. Interfața grafică a aplicației PRESTO este reprezentată în Figura 1. Implementarea a fost făcută în Android Studio folosind mediul de programare Java. Folosind această interfață utilizatorii au posibilitatea de a accesa cu ușurință funcționalitățile vehiculului asupra cărora aceștia au drepturi și tot din această interfață pot delega drepturi unei alte persoane.

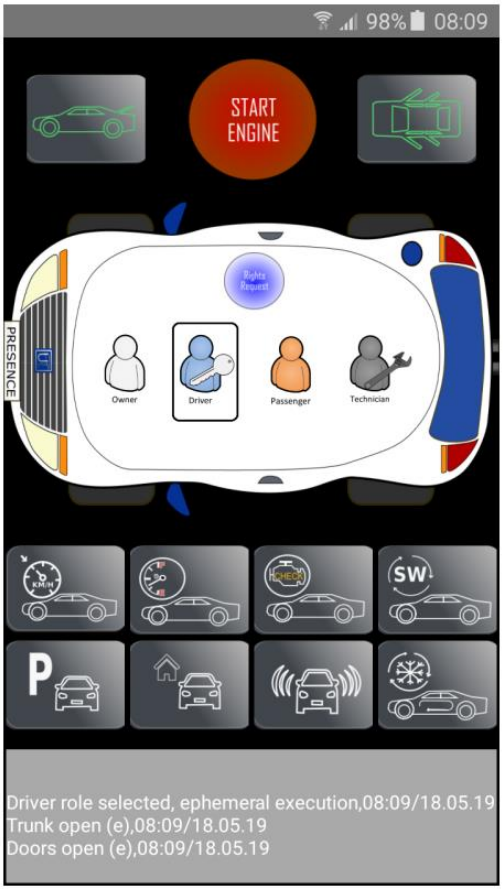

Figura 1. Interfață grafică a aplicației PRESTO

În conceptul propus, am considerat că există numeroase funcționalități ale vehiculelor care pot fi accesate într-un mod independent folosind telefonul inteligent. De asemenea, am luat în calcul faptul că

aceste funcționalități trebuie să fie accesate doar de persoanele autorizate. Prin urmare, propunerea noastră include accesul pe bază de roluri. Un utilizator se poate autentifica unui vehicul în unul dintre următoarele roluri: proprietar, șofer, tehnician auto, copil (minor), valet sau pasager, etc. Fiecare dintre aceste roluri au acces asupra unui set predefinit de funcționalități ale automobilului.

Figura 2 oferă o imagine de ansamblu asupra sistemului adresat în conformitate cu lucrarea în curs de publicare [3]. Un utilizator poate solicita o anumită funcționalitate a mașinii care urmează să fie executată de o unitate de control electronică din vehicul. Într-un prim pas, un serviciu de autentificare verifică identitatea și rolul utilizatorului. Dacă această etapă este depășită cu succes, identitatea și rolul utilizatorului fiind corecte, cererea este transmisă mai departe către serviciului de control al accesului. Acest serviciu verifică dacă rolul utilizatorului are autorizare de execuție asupra funcționalității cerute. În cazul unei decizii pozitive, cererea este transmisă spre vehicul pentru a fi executată. După execuție, autovehiculul trimite înapoi un mesaj de răspuns utilizatorului. În ultimul pas, utilizatorul recepționează mesajul de răspuns care indică dacă solicitarea sa a fost executată cu succes sau dacă cererea a fost respinsă.

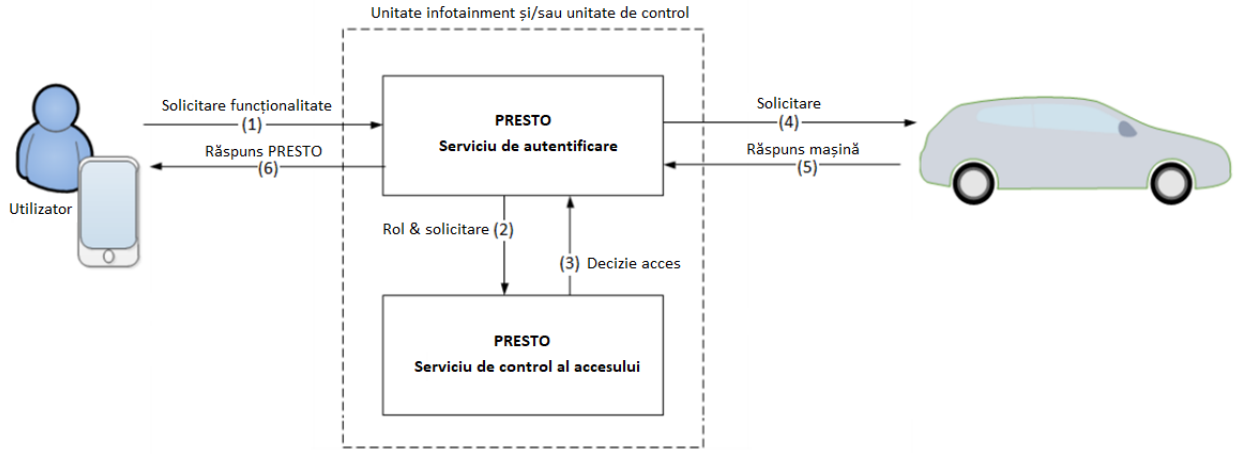

Figura 2. Sistemul de control al accesului în PRESTO

Din punct de vedere al interfețelor de comunicație am decis să folosim Bluetooth, Wi-Fi și NFC (Near-Field Communication). Primele două interfețe sunt propuse și analizate ca posibile tehnologii de comunicație între telefonul inteligent și mașină dar şi pentru posibilitatea de portare pe maşini virtuale ce rulează în cloud (comunicaţia WiFi are la bază socket-uri a căror utilizare este generic şi deci portabilă pe maşini virtuale în cloud), pe când tehnologia NFC este analizată ca interfață de comunicație între două telefoane inteligente în cazul execuției de delegare al drepturilor de la un utilizator la altul. În cadrul experimentelor noastre am decis să folosim patru telefoane inteligente, două sisteme infotainment și un microcontroler folosit în industria auto. Trei dintre cele patru telefoane folosite sunt fabricate de către

Samsung, dar sunt modele diferite, J5, S5 si S7. Cel de al patrulea telefon este un LG Optimus P700. Unitățile infotainment sunt bazate pe Android, una fiind produsă de ERISIN iar cealaltă de PNI. Micocontroler-ul automotive pe care l-am folosit este un Infineon Aurix TC297. Setup-ul nostru experimental cu cele doua unități infotainment și un telefon inteligent este reprezentat în Figura 3.

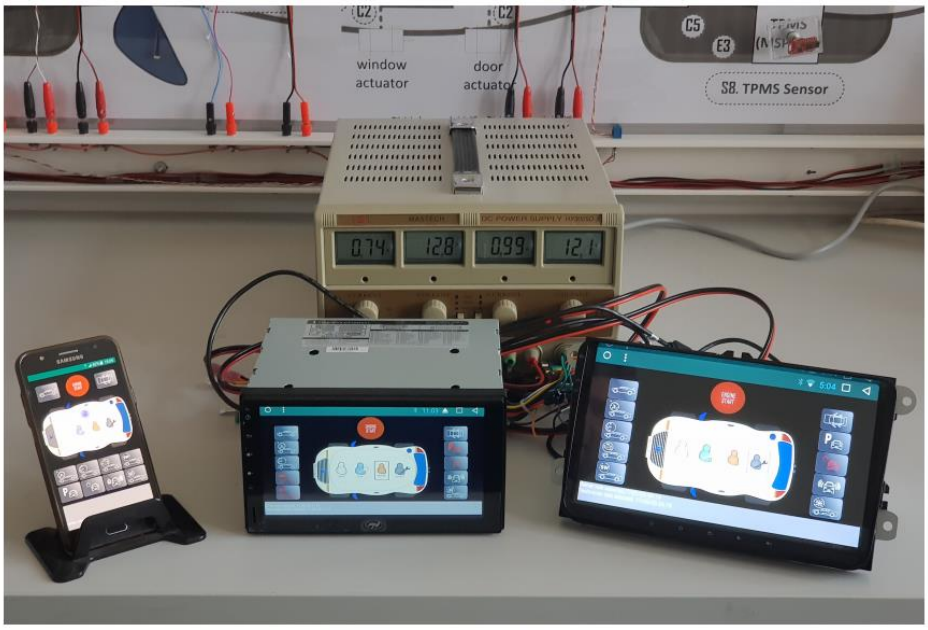

Figura 3. Unitățile infotainment și unul dintre telefoanele folosite în experimentele noastre

Odată realizată aplicația de control la distanță prin intermediul telefonului mobil, ne-am propus investigarea tehnologiei cloud. Pe de o parte aceasta poate fi folosită pentru un potențial deployment al aplicației create (mai exact a sistemului de control al accesului) pe de altă parte am încercat să imaginăm un scenariu nou de car sharing pentru a putea demara o nouă lucrare de cercetare. Tehnologia cloud este folosită în tot mai multe aplicații pentru vehicule, pentru a stoca informații despre vehicule și utilizator. Un exemplu ar fi cunoscutele aplicații folosite pentru a stoca istoricul vehiculului (mecanic, service, accidente) și pentru a notifica proprietarul când trebuie să se prezinte cu mașina la service, pentru revizii, diagnoză. etc. Un alt scenariu de utilizare este închirierea mașinilor folosind tehnologia cloud pentru a stoca date despre flota de vehicule și despre clienți, dar și pentru a comunica între vehicul și client.

Noi ne-am propus să folosim tehnologia cloud pentru a realiza această din urmă aplicaţie, mai exact, un sistem de gestionare a accesului la o flotă de mașini (în principiu un scenariu de car sharing). O tentativă inițială a fost să folosim tehnologia Blockchain pe care am investigat-o în alt context automotive în [9]. În cele din urmă am ales să folosim serviciul de cloud Microsoft Azure, dezvoltat de Microsoft. În conformitate cu site-ul producatorului (https://portal.azure.com/), Microsoft Azure este o platformă care

oferă servicii precum: calcul în cloud folosind mașini virtuale (Virtual Machines), servicii cloud (Cloud Services), serviciul de aplicație (App Service), rețele virtuale (Virtual networks), adrese IP publice (Public IP addresses), adrese IP rezervate (Reserved IP addresses), conexiuni (connections), tabele de rutare (Route tables), firewall, stocare (storage), de ex. conturi de stocare (Storage accounts), servicii de sincronizare ale datelor stocate (Storage Sync Services), etc., baze de date de ex. baze de date SQL (SQL databases), servere SQL (SQL servers), Azure SQL, baze de date Azure pentru servere MySQL (Azure database for MySQL servers), mașini virtuale SQL (SQL virtual machines), etc.

Dintre aceste servicii oferite de Azure noi am folosit: serviciul aplicație (App Service) + mobile, o baza de date SQL (SQL database), un server SQL (SQL server) și un cont de stocare (storage account). Sistemul propus de noi, conține o bază de date SQL, stocată în Cloud, în care sunt stocate date despre fiecare mașină. Pentru a accesa datele din baza de date SQL, am dezvoltat o aplicație Android formată din: i) partea de client SDK, care în cazul nostru este proiectul Android dezvoltat în Android Studio și implementat în java, ii) partea de server, backend, pe care noi am ales să o implementăm în .NET, iii) serviciul aplicație Azure (Azure App Service) prin care se face conexiunea la o baza de date din cloud, dar totodată pe acest serviciu aplicație se lansează (deploy) partea de server (backend) a aplicației mobile.

În primul rând am creat o bază de date SQL în portalul Azure oferit de Microsoft, apoi am creat un serviciu de aplicație web (web app service) în care am specificat prin MobileAppsManagement_EXTENSION_VERSION că dorim să dezvoltăm o aplicație mobilă. De asemenea am mai specificat string-ul de conexiune la baza de date SQL și limbajul de programare în care va fi dezvoltată partea de server (backend) a aplicației (.NET în cazul nostru). În aplicația Andoid (Java), care rulează pe telefonul mobil folosim link-ul serviciului de aplicație web (web app service) creat pentru a ne conecta la partea de server a aplicației. După cum am precizat anterior, partea de server (backend) a aplicației, am ales să o dezvoltăm în .NET. Pentru aceasta am creat un proiect web ASP.NET, în Visual Studio, proiect în care am definit tabela din baza de date SQL. Când lansăm aplicația în Azure, selectăm serviciul de aplicație web (web app service) creat anterior, iar tabela se generează automat în daza de date SQL.

Scenariul imaginat care stă la baza unei publicaţii noi în proiect (distinctă de [3] dar încă nefinalizată, urmând să fie detaliată în raportul final) este prezentat în Figura 4. În acest scenariu, flota de maşini pusă la dispoziție de producător (sau furnizor de servicii de închiriere) este înregistrată în cloud şi pe un server de gestionare a cheilor. Clienţii, folosind aplicația de pe telefonul mobil vor putea primi drepturi de acces la flotă. Cererea de drepturi se face printr-un protocol criptografic de tip oblivious-transfer pentru a păstra anonimitate asupra achiziției. Vom detalia acest protocol şi datele tehnice în raportul următor, momentan datele sunt confidențiale fiind încă nepublicate.

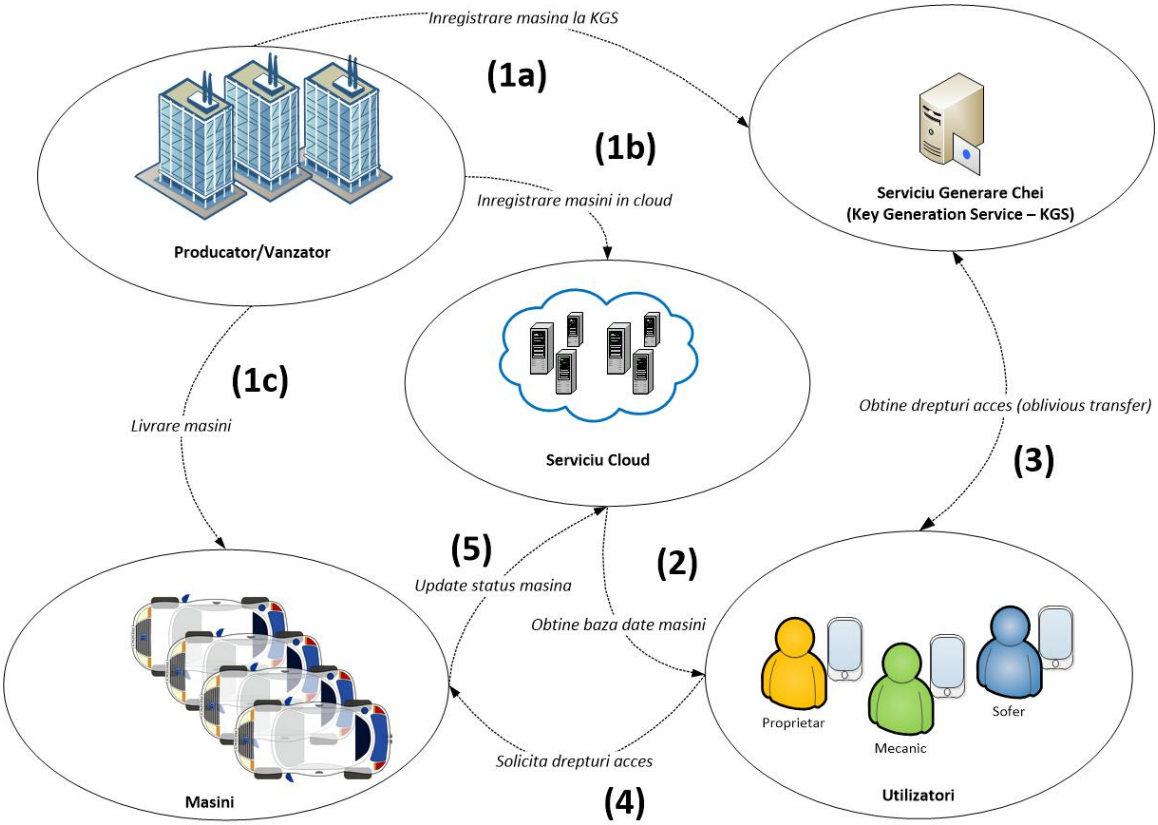

Figura 4. Schema de principiu a sistemului de acces la o flota de masini prin cloud

A2. Accesul si controlul la distanta asupra vehiculelor, simulare folosind un model experimental

Pentru a evalua funcționalitățile ce ar putea fi înglobate într-un model experimental, am condus o scurtă cercetare în zona aplicațiilor mobile deja oferite de marii producători din zona auto. Rezultatele sunt publicate în [4]. In acest moment mulți producători oferă aplicații pentru accesarea unor funcționalități ale mașinilor prin utilizarea dispozitivelor mobile. Tabelul 1 rezumă o parte din comenzile de la distanță puse la dispoziția utilizatorului de către producătorul auto prin intermediul aplicației oficiale destinate dispozitivelor mobile inteligente (acesta este doar un scurt rezumat bazat pe informațiile preluate din materialele de prezentare a producătorilor de autovehicule, deoarece nu putem avea acces direct la toate aceste mașini). În acest tabel am luat în considerare următoarele aplicații: MyOpel (1), MyChevrolet (2), Tesla (3), BMW Connected (4), Audi MMI Connect (5), Mercedes me (6), Volkswagen Car-Net Security Service (7), Volvo On Call (8) and Toyota Remote Connect (9).

Funcționalitățile furnizate sunt foarte diverse, de la funcțiile de comandă a dispozitivelor media până la pornirea fără cheie a motorului. Aplicațiile destinate dispozitivelor mobile sunt de asemenea buni candidați pentru activarea de la distanță a unor funcționalități de pilot automat. Un exemplu este funcția denumită de Tesla *enhanced summon*, în care aplicația Tesla este utilizată pentru a trimite o cerere la distanță către mașină pentru ca aceasta să navigheze autonom din locul unde este parcată către locația șoferului.

Funcționalitate	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Blocare/deblocare uși	X	X	X	X	X	X	X	X	X
Pornire autovehicul din aplicație	–	–	X	–	–	–	–	–	–
Claxon	X	X	–	X	–	–	X	X	–
Aprinde, stinge faruri	X	X	X	X	–	–	X	X	–
Start/stop motor	–	X	X	–	–	–	–	X	X
Încălzire scaune	–	–	X	–	–	–	–	X	–
HVAC pornit/oprit	–	–	X	X	–	X	X	X	–
HVAC referință temp.	–	–	X	–	–	–	X	–	–
Degivrare parbriz	–	–	–	–	–	–	X	–	–
Ventilație/închidere plafon	–	–	X	–	–	–	–	–	–
Activare/dezactivare mod valet	–	–	X	–	–	–	–	–	–
Comenzi multimedia	–	–	X	–	–	–	–	–	–

Tabelul 1. Funcționalități oferite prin intermediul aplicaților mobile

De asemenea unii producători auto oferă posibilitatea raportării stării martorilor de bord precum și interogarea si vizualizarea raportului de diagnoză. Modelul experimental actual are la bază modelul experimental al proiectului nostru anterior CSEAMAN care apare in Figura 5 (am fost preocupați si de creșterea securității unor subansamble cum ar fi modulul TPM despre care am publicat rezultate în [8]). La acest am adăugat elemente care fac posibila conectarea dispozitivelor mobile la autovehicul, modelul experimental propus fiind descris în [4]. In acest context a fost utilizată o placa de dezvoltare Raspberry Pi 3 aceasta oferind posibilitatea interconectării cu dispozitivele mobile prin WiFi si Bluetooth şi totodată funcţionează ca şi gateway către CAN bus (magistrala de pe care devin accesibile toate funcționalitățile din vehicule).

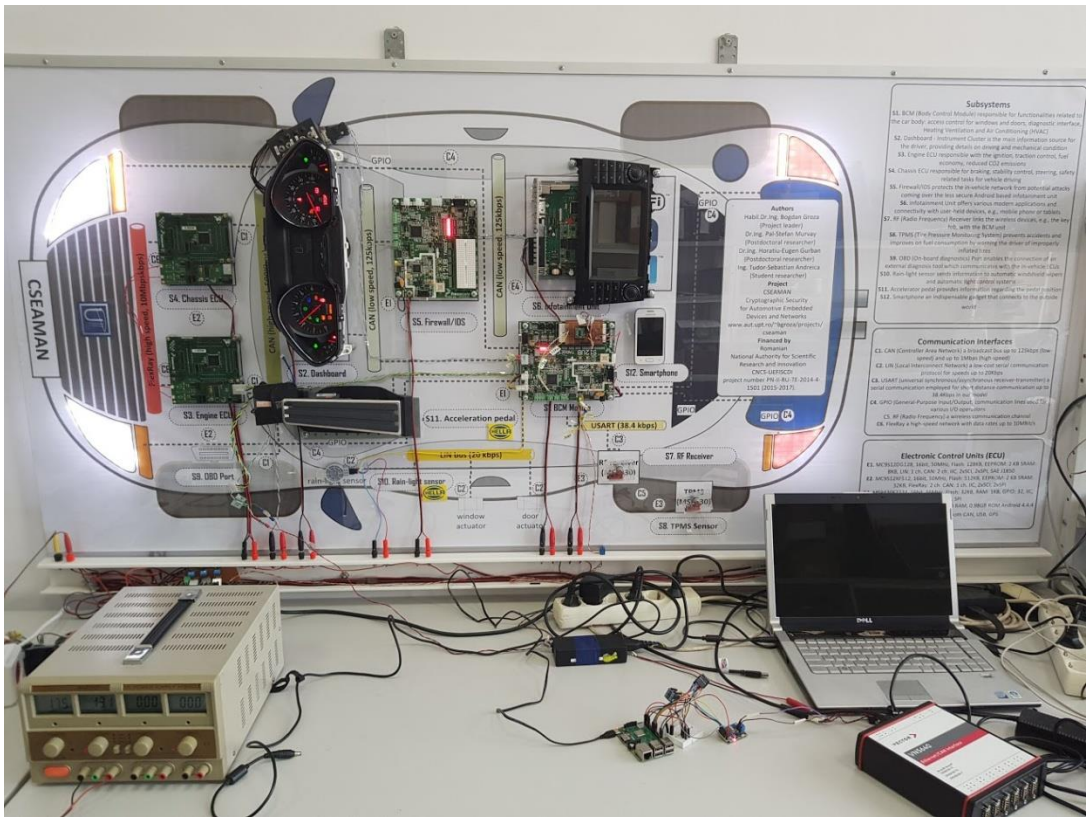

Figura 5. Standul experimental utilizat (model experimental din proiectul CSEAMAN)

Placa de dezvoltare Raspberry Pi 3 este capabilă să ruleze diverse distribuții Linux, de exemplu Fedora, Arch precum și sistemul de operare oficial Raspbian, propus de producător (bazat pe Debian), care îi oferă avantajele accesului ușor la toate instrumentele Linux și o capacitatea mare de adaptare la numeroase proiecte open-source. Microprocesorul Raspberry Pi 3, ARM Cortex A53, nu dispune de un controler CAN încorporat. Din acest motiv am ales să utilizăm o placă suplimentară conectată prin SPI care încapsulează un controler CAN (Microchip MCP2515) și un transceiver CAN (NXP TJA1050). Pentru implementare am folosit SocketCAN, un set de drivere pentru interfețe CAN.

Aplicația dezvoltată poate transmite informații către dispozitive mobile astfel încât se pot monitoriza și comanda diferite funcționalități implementate pe standul experimental. Astfel se poate monitoriza de la distanță tensiune bateriei și se poate monitoriza dar si comanda starea farurilor, stopurilor, semnalizărilor și avariei. De asemenea a fost implementată o aplicație software care să transmită mesajele pe magistrala CAN necesare funcționării modulelor din standul experimental, astfel nu mai exista necesitate utilizării produselor software comerciale specifice domeniului automotive precum CANoe sau CANalyzer în standul experimental. O discuție cu privire la modelul experimental a fost publicată de noi în lucrarea

[4]. Nu în ultimul rând am reușit să venim cu propuneri noi pentru realizarea negocierii de cheie în rețele in-vehicle publicate în lucrările [1], [2] și [7].

A.3. Tehnologii de crestere a securitatii, module TPM

Industria Automotive se află în continuă dezvoltare în ceea ce privește adopția de mecanisme criptografice şi a unor subsisteme hardware cu capabilități criptografice. Un exemplu de astfel de sistem este procesorul criptografic TPM realizat în conformitate cu standardul ISO/IEC 11889. Acțiunile de bază ale unui procesor TPM specificate în standard sunt: i) utilizarea unei chei unice de identificare pentru dovedirea autenticității acestuia numită EK (endorsement key), ii) utilizarea unei chei unice utilizate la memorarea cheilor generate de către dispozitiv numită SRK (storage root key), iii) generarea de numere pur aleatoare (TRNG), iv) generarea și memorarea de chei criptografice simetrice și de perechi de chei criptografice asimetrice folosind numere pur aleatoare, v) realizarea de funcții criptografice fără cheie precum calculul de funcții hash criptografice (e.g. SHA-256), vi) realizarea de operații criptografice (e.g., RSA-2048), calculul de coduri de autentificare al mesajelor (e.g. HMAC-SHA256) sau calculul semnăturii mesajelor (e.g. ECC-256), vii) utilizarea de interfețe seriale standard de comunicare cu microcontrolere și/sau microprocesoare (ex. SPI, I^2C).

Din echipamentele TPM existente, doar o parte pot fi folosite în industria autovehiculelor deoarece standardele automotive implică cerințe stricte referitoare la temperaturile de funcționare ale dispozitivelor și nu numai. Din această categorie, am utilizat în cadrul proiectului de cercetare procesorul Infineon OPTIGA TPM care face parte din familia de procesoare compatibile cu sistemele automotive. OPTIGA TPM SLI9670 este conform cu aceste standarde dar singurul model de procesor din familia OPTIGA TPM disponibil într-un echipament de dezvoltare cu interfață serială ce a putut fi utilizat este OPTIGA TPM SLB9670 ce are la bază un microcontroler cu arhitectură pe 16 biți, 7kB de memorie persistentă și 1kB pentru procesarea datelor transmise/recepționate. Modulul OPTIGA TPM SLB9670 poate realiza toate funcțiile specificate în standardul TPM 2.0 (ISO/IEC 11889:2015, Părțile 1-4) și are o interfață SPI care poate fi utilizată pentru transferul datelor de la și către un microcontroler. Echipamentele utilizate în cadrul proiectului de cercetare sunt prezentate în Figura 6. Rezultatele au fost publicate în lucrarea [5].

Pentru a putea comunica cu un dispozitiv TPM de pe placa de dezvoltare Raspberry Pi a fost necesar să modificăm kernel-ul sistemului de operare Raspbian conform cu informațiile specificate de producătorul de echipamente TPM Infineon și să folosim varianta modificată în cadrul experimentelor. Având sistemul de operare compatibil cu dispozitivele TPM și modulul hardware conectat la Raspberry Pi, pentru a putea

comunica folosind interfața SPI către modulul OPTIGA TPM, am folosit bibliotecile software disponibile pe GitHub (https://github.com/tpm2-software).

Pentru a putea instala și configura bibliotecile software am transmis comenzi prin linia de comandă din interfața terminal a plăcuței Raspberry Pi accesibilă de pe calculator prin portul SSH din conexiunea la internet a plăcii de dezvoltare.

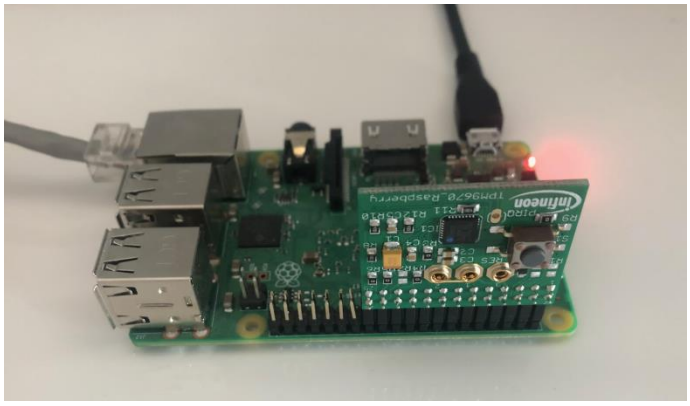

Figura 6. Raspberry Pi și modulul cu procesor OPTIGA TPM SLB9670

Utilizând biblioteca tpm2-tools, pe baza celorlalte biblioteci tpm2-software, am putut să transmitem comenzi către modulul TPM și să măsurăm timpul de execuție a următoarelor acțiuni evaluate experimental în Tabelul 2 (aceleași acțiuni au fost măsurate și pe Raspberry Pi, Samsung Note 8 și Infineon TC297).

Metodă criptografică	Timp rulare
Generarea perechii de chei RSA	220 ms
Încărcarea cheii publice RSA pe TPM	220 ms
Semnătură RSA	324 ms
Verificarea semnăturii RSA	198 ms

Tabelul 2. Rezultate computaționale folosind OPTIGA TPM SLB9670

În contextul integrării modulului TPM în industria automotive, cu scopul realizării unui mecanism de schimb de date securizat între dispozitive mobile și autovehicule moderne, am definit un scenariu de car-sharing. Pe baza scenariului definit, o persoană, prin intermediul telefonului mobil, cere acces la anumite funcții din mașină care să poată fi realizate direct de către telefon (ex. deschiderea ușilor, pornirea motorului, aprinderea farurilor). În funcție de numărul de acțiuni la care acesta are acces, va primi autorizarea din partea echipamentului ce joacă rolul unui dispozitiv de încredere utilizat pentru car-sharing, schimb de informații fiind prezentat în Figura 7.

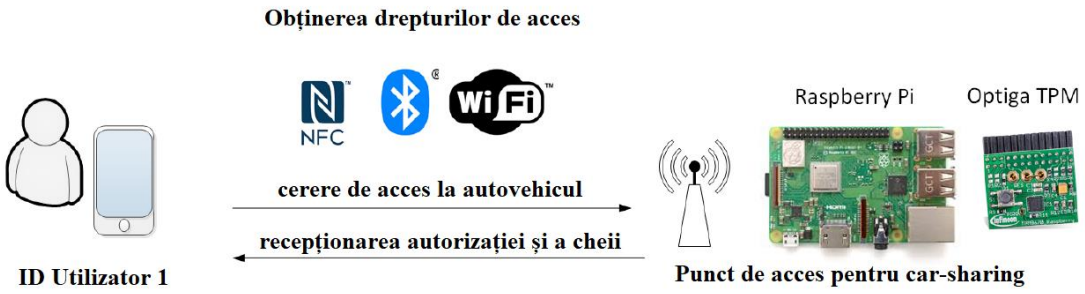

Figura 7. Cererea de acces la funcțiile mașinii către dispozitiv și recepționarea autorizației și a cheii de acces

Astfel, ne-am folosit modulul TPM ca și co-procesor pentru a asigura stocarea cheilor de securitate private și publice utilizate și pentru a realiza toate calculele criptografice necesare autorizării dispozitivelor mobile cu scopul de a realiza diferite acțiuni din exteriorul sau în interiorul autovehiculelor. În cadrul lucrării publicate [5] metodele implementate pentru comunicarea cu modulul TPM pe Raspberry Pi cât și alte metode testate (ex. pe dispozitivul mobil) sunt prezentate în detaliu pentru a evidenția posibilitatea de car-sharing autorizat pe baza identității folosind module TPM.

A.4. Asocieri pe baza de date din ecosistem, folosirea de date audio-vizuale

Acest obiectiv vine în continuarea asocierii bazate pe date de la accelerometre dezvoltată în etapa anterioară. Am dorit prin acest obiectiv să abordăm asocierea folosind date audio-vizuale. Am constat însă că informația de tip video nu este foarte convenabil de utilizat, am găsit o singura lucrare care adresa asocierea între mașini și telefoane mobile [11], deoarece camera video epuizează bateria foarte repede și poate fi ușor obturată. Ne-am propus în acest caz să folosim canalele audio și să amprentăm telefoanele mobile pe baza sunetului emis de acestea astfel încât un dispozitiv, cum ar fi o unitate de infotainment din maşină, să poată amprenta un telefon mobil. În primul rând oferim o imagine de ansamblu a experimentelor. Prezentăm dispozitivele folosite, tool-urile folosite, precum și configurația mediului și scenariile de experimente.

Am folosit patru smartphone-uri echipate cu difuzor și microfon: Samsung Galaxy S7 Edge, Samsung Galaxy J5, LG Optimus P700 și Allview V1 Viper I. De asemenea, am folosit o unitate de

infotainment de la ERISIN, echipată cu un microfon. Ca instrumente de lucru, am folosit REW (Room EQ Wizard) pentru a genera un semnal LinearSweep cu o frecvență între 20Hz și 25kHz, semnal pe care l-am salvat ca fișier .wav. De asemenea, pentru analiză am folosit Matlab.

Fiecare smartphone folosit redă fișierul .wav cu semnal LinearSweep generat în REW. Pe unitatea ERISIN rulează o aplicație Android care înregistrează sunetele de pe smartphone-uri. Semnalul înregistrat este salvat ca fișier .wav. Experimentele au fost realizate într-o cameră. Distanța dintre unitatea ERISIN și smartphone-ul care redă sunetul a fost un metru. Am făcut cinci măsurători în aceleași condiții cu toate smartphone-urile.

Pentru a analiza semnalele înregistrate de unitatea ERISIN, folosim Matlab. Analiza inițială a fost făcută folosind analizatorul de semnale (Signal Analyzer App) din toolbox-ul de procesare a semnalelor (Signal Processing Toolbox). Citim datele înregistrate din fișierul .wav folosind funcția *audioread („fișier.wav”),* care returnează datele eșantionate și o rată de eșantionare pentru date.

Analiza noastră se bazează pe spectrul de putere al semnalului (power spectrum) care este calculat folosind funcția *pspectrum(date filtrate, rata de eșantionate)* care are ca parametri datele audio filtrate și rata de eșantionare a datelor. Funcția returnează spectrul de putere al semnalului și frecvențele corespunzătoare. În figura 8 arătam spectrul de putere al semnalelor audio pentru toate cele patru telefoane ultilizate: Samsung S7 (albastru), Samsung J5 (red), LG (portocaliu), Allview (mov).

Pentru a reduce zgomotul am încercat mai multe filtre. Folosim un filtru smooth, bazat pe valoarea medie a datelor, filtru care este dat de funcția *smoothdata(date audio, ”movmean”),* care are ca parametri datele audio și metoda de smooth „movmean”. Folosim filtrul bandpass care este dat de funcția *bandpass (date audio, [0,25 0,75], 0.75],’Steepness’, 0.85,’StopbandAttenuation’,60*), care are ca parametri datele audio, frecvența de bandă normalizată care a fost setată între 0,25 și 0,75, steepness-ul setat la 0,85 și StopbandAttenuation la 60dB. De asemenea, folosim filtru bandstop, care este dat de funcția *bandstop (date audio, [0,25 0,75], „Steepness”, 0,85, funcția „StopbandAttenuation”, 60)* care are aceiași parametri ca funcția pentru filtru banspass. Am mai încercat și filtrele highpass și lowpass, date de funcțiile *highpass (date audio, 0,5, „Steepness”, 0,85, „StopbandAttenuation”, 60),* respectiv *lowpass (date audio, 0,5, „Steepness”, 0,85, StopbandAttenuation”, 60),* funcții care au ca parametri datele audio, frecvența benzii de acces care a fost setată la 0,5, steepness-ul setat la 0,85 și StopbandAttenuation setat la 60dB.

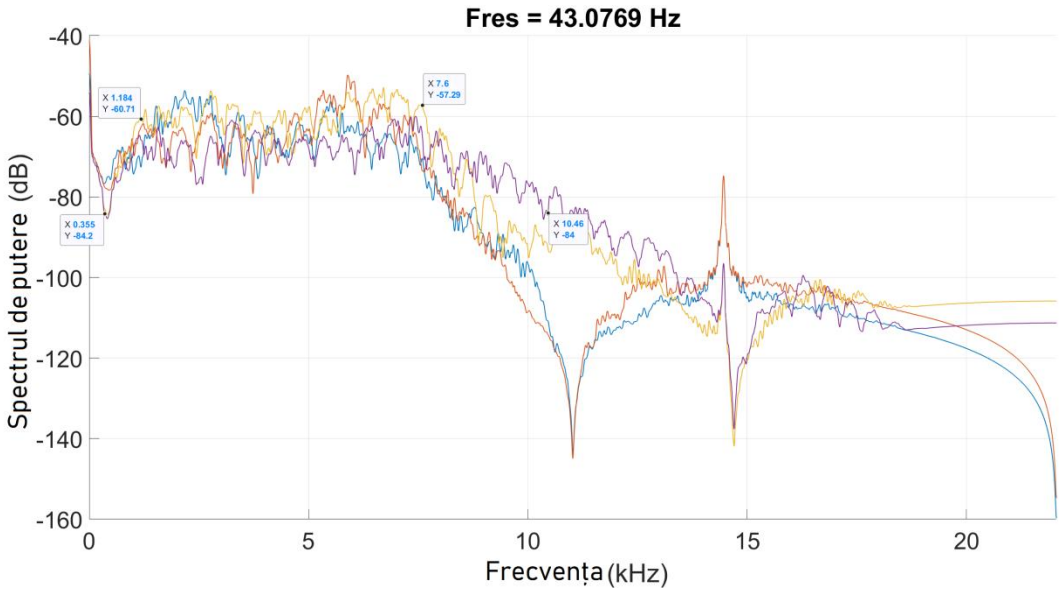

Figura 8. Spectrul de putere al unui semnal audio emis de diferite telefoane mobile și înregistrat de unitatea de infotainment

În [10] sunt amprentate dispozitive mobile pe baza datelor audio, utilizând caracteristicile extrase cu diverși algoritmi, cum ar fi coeficienții de frecvență cepstral mel (MFCC - Mel-frequency cepstral coefficients), rădăcina medie pătrată (SMR), cernoidul spectral, entropia spectrală, spectral kurtosis, tonal centroid și altele. Autorii folosesc algoritmi de clasificare precum K-NN și GMM pentru a confirma amprentele dispozitivelor. Cele mai bune rezultate sunt obținute folosind MFCC.

Am extras caracteristicile semnalelor audio folosind MFCC, cum este folosit și în [10]. În tabelul 3 prezentăm rezultatele obținute folosind clasificatorul KNN (k-nearest neighbors algorithm) pentru caracteristicile extrase cu MFCC. În Tabelul 3 prezentăm rezultatele din cinci experimente cu fiecare telefon mobil. Pentru toate cele patru smartphone-uri, am considerat caracteristicile extrase din semnalul audio de la un experiment ca date de training, iar caracteristicile extrase din semnalele audio de la celelalte patru experimente rămase ca date de test. În acest caz, telefoanele mobile sunt identificate corect.

Telefon mobil	(J5)	(S7)	(LG)	(Allview)
J5	56.36%	7.18%	2.46%	34.01%
S7	1.06%	96.57%	1.19%	1.19%
LG	12.75%	14.70%	61.43%	11.12%
Allview	28.77%	0.57%	2.83%	67.89%

Tabelul 3. KNN pentru MFCC

Concluzii

În aceasta etapă, aferentă anului 2019, proiectul nostru a abordat conform planului tehnologiile de acces la vehicule de la distanţă prin Internet şi cloud de pe dispozitive mobile inteligente. Am avut în vedere atât tehnologiile de sporire a securității prin module hardware (TPM), utilizarea unui model experimental (provenit din proiectul nostru anterior CSEAMAN şi adaptat la necesitățile proiectului curent) cât şi folosirea tehnologiilor de pairing bazate pe informații extrase din mediu (în etapa anterioară date de la accelerometre şi acum informații audio-video). Pentru a duce la bun sfârşit aceste obiective, în primul rând am explorat tehnologiile folosite de marii producători în domeniul auto. Apoi am finalizat propunerea noastră de protocol de control al accesului la maşini propunând o aplicație Android pentru controlul mașinii, bazată pe un sistem de control al accesului bazat pe roluri şi securizat prin intermediul tehnologiilor criptografice moderne.

În conformitate cu contractul ne-am angajat să susținem 3-4 lucrări în conferințe şi să trimitem 3 lucrări către reviste ISI. În anul 2019 am susținut 6 lucrări în conferințe, avem acceptate 2 lucrări în jurnale ISI Q1 şi am transmis încă 2 lucrări la jurnale Q1; toate având ca sursă unică de finanţare prezentul proiect. Prin acestea considerăm că am îndeplinit la nivel calitativ planul şi chiar l-am depăşit.

Referinţe

[1] Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, TRICKS - time TRIggered Covert Key Sharing for Controller Area Networks, IEEE Access, vol. 7, 2019

[2] Bogdan Groza, Pal-Stefan Murvay, Identity-Based Key Exchange on In-Vehicle Networks: CAN-FD & FlexRay, Sensors, 22, 2019

[3] Bogdan Groza, Tudor Andreica, Adriana Berdich, Pal-Stefan Murvay, Horatiu Gurban, PRESTvO: PRivacy Enabled Smartphone-based access To vehicle On-board units, under submission, 2019

[4] Bogdan Groza, Horatiu Gurban, Lucian Popa, Adriana Berdich, Pal-Stefan Murvay, Car-to-Smartphone Interactions: Experimental Setup, Risk Analysis and Security Technologies , 5th International Workshop on Critical Automotive Applications: Robustness & Safety (CARS), 2019

[5] Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, CarINA - Car sharing with IdeNtity based Access control re-enforced by TPM, 2nd International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms, SAFECOMP Workshops (STRIVE), 2019

[6] Tudor Andreica, Bogdan Groza, Secure V2V Communication with Identity-based Cryptography from License Plate Recognition, The Second International Workshop on Intelligent Transportation and Connected Vehicles Technologies (ITCVT), 2019

[7] Lucian Popa, Bogdan Groza, Pal-Stefan Murvay, Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers, Workshop on Industrial Security and IoT (WISI), in conjunction with the 14th International Conference on Availability, Reliability and Security, 2019

[8] Adrian Musuroi, Bogdan Groza, Stefan Murvay and Horatiu Gurban, Security for low-end automotive sensors: a tire-pressure and rain-light sensors case study, 9th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS), 2019

[9] Mario Vasile, Bogdan Groza, DeMetrA - Decentralized Metering with user Anonymity and layered privacy on Blockchain, 23rd International Conference on System Theory, Control and Computing (ICSTCC), 2019

[10] A. Das, N. Borisov, and M. Caesar. Do you hear what i hear?: Fingerprinting smart devices through embedded acoustic components. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages 441–452. ACM, 2014.

[11] J. Han, Y.-H. Lin, A. Perrig, and F. Bai. Mvsec: Secure and easy-to-use pairing of mobile devices with vehicles (cmu-cylab-14-006). 2014.