Raport Ştiinţific Nr. 3

(raport final, perioada 2018-2020)

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

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

echipa în perioada 2018-2020

Habil. Dr. Ing. Bogdan Groza
Dr. Ing. Pal-Ştefan Murvay
Dr. Ing. Horaţiu Eugen Gurban
Ing. Adriana Maria Berdich
Ing. Lucian Tudor Popa
Ing. Tudor Andreica
Ing. Camil Jichici

Universitatea Politehnica Timişoara

Iunie 2020

Raport Ştiinţific Nr. 3

(raport final, perioada 2018-2020)

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

Interacţiuni private şi sigure între vehicule şi dispozitive electronice inteligente

PRESENCE

Prezentul document reprezintă raportul ştiinţific final cu privire la activitatea 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 perioada 2018-2020. Rezultatele ştiinţifice din cadrul proiectului sunt menţinute la zi pe site-ul proiectului unde vom actualiza şi starea lucrărilor încă în curs de evaluare http://www.aut.upt.ro/~bgroza/projects/presence/index.html. De asemenea, recomandăm consultarea site-ului şi pentru detalii suplimentare la acest raport (în principal detalii ştiinţifice din publicaţiile asociate).

În conformitate cu contractul de finanţare, prin proiectul PRESENCE ne-am angajat că vom trimite 5 lucrări la jurnale ISI (factor de impact 0.5-3) şi 5 lucrări la conferinţe. La finalul proiectului am reuşit să acumulăm un total de: 5 lucrări deja acceptate în jurnale ISI Q1 (factor impact 3-5), 2 lucrări aflate încă în curs de evaluare la jurnale ISI Q1/Q2, şi 9 lucrări acceptate în conferinţe. Considerăm aşadar că am reuşit să îndeplinim şi chiar să depăşim aşteptările din propunerea de proiect. Lista articolelor publicate este:

[J1] -IF 4.09 Bogdan Groza, Tudor Andreica, Adriana Berdich, Pal-Stefan Murvay, Horatiu Gurban, PRESTvO: PRivacy Enabled Smartphone-based access To vehicle On-board units, *IEEE Access*, 2020.
[J2] - IF 4.09 Bogdan Groza, Adriana Berdich, Camil Jichici, Rene Mayrhofer, Secure Accelerometer-based Pairing of Mobile Devices in Multi-modal Transport, *IEEE Access*, vol. 7, 2020.
[J3] -IF 5.33 Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, Highly Efficient Authentication for CAN by Identifier Reallocation with Ordered CMACs, *IEEE Transactions on Vehicular Technology*, 2020.
[J4] - IF 4.09 Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, TRICKS - time TRIggered Covert Key Sharing for Controller Area Networks, *IEEE Access*, vol. 7, 2019.
[J5] - IF 3.03 Bogdan Groza, Pal-Stefan Murvay, Identity-Based Key Exchange on In-Vehicle Networks: CAN-FD & FlexRay, *Sensors*, 22, 2019.

[C1] Adriana Berdich, Alfred Anistoroaei, Bogdan Groza, Horatiu Gurban, Stefan Murvay, Daniel Iercan, ANTARES - ANonymous Transfer of vehicle Access Rights from External cloud Services, 3rd International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms, IEEE Vehicular Techology Conference Workshops (STRIVE), 2020

[C2] 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
[C3] 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
[C4] 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
[C5] 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.
[C6] 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
[C7] 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
[C8] Tudor Andreica, Bogdan Groza, Stefan Murvay, Applications of Pairing-Based Cryptography on Automotive-Grade Microcontrollers, 1st International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms (STRIVE 2018, SAFECOMP 2018 Workshops), Vasteras, Sweeden.
[C9] Camil Jichici, Bogdan Groza, Stefan Murvay, Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks, 11th International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2018, Bucharest, Romania.

Aşa cum se observă din lista de publicaţii, atenţia noastră a fost concentrată pe jurnale ISI Q1 respectiv pe participări în cadrul unor workshop-uri de profil automotive pentru a găsi audienţa interesată de lucrările desfăşurate în proiect. Lucrările în curs de evaluare (2 la număr) nu le putem enumera din motive de confidențialitate, precizăm însă că sunt trimise la jurnale Q1-Q2 cu factor de impact în intervalul 1-5. De asemenea mai există material în lucru pentru cel puţin încă 2 lucrări Q1-Q2 de a căror redactare ne ocupăm în continuare. Lista de lucrări ştiinţifice va fi actualizată pe site-ul proiectului de îndată ce acestea sunt acceptate. Estimăm că numărul lucrărilor cu rezultate din prezentul proiect publicate în jurnale Q1-Q2 va ajunge la nu mai puţin de 9 lucrări. În cele ce urmează prezentăm pe scurt rezultatele obţinute în cadrul activităților asociate obiectivelor din proiect, pentru detalii tehnice şi ştiinţifice rugăm consultarea directă a lucrărilor ce sunt postate şi menţinute la zi pe site-ul web al proiectului nostru http://www.aut.upt.ro/~bgroza/projects/presence/publications.html.

Etapa 1. Designul, analiza şi implementarea protocoalelor de securitate în interacţiuni vehicul - dispozitiv mobil inteligent

Prima etapă a proiectului a fost desfăşurată în anul 2018 începând cu luna Mai şi a avut trei activităţi principale: designul protocoalelor de securitate, investigarea unor tehnologii de creştere a securităţii (carduri NFC) şi utilizarea datelor din ecosistem. Acestea urmează a fi detaliate în continuare.

A1.1. Designul, analiza şi implementarea protocoalelor de securitate (prima iteraţie)

Prima iteraţie din designul, implementarea şi analiza protocolului propus pentru interacţiunea telefon mobil – maşină (intitulat de noi PRESTvO) aferentă obiectivului O1 din propunerea de proiect a constat în desemnarea funcţionalităţilor, a politicii de control a accesului, a funcţiilor cripografice utilizate şi a interfeţelor de comunicare.

Controlul accesului la maşini, aşa cum am propus în lucrarea centrală a proiectului [1] demarată odată cu activitatea A1.1 din 2018, are la bază un serviciu de control al accesului şi un serviciu de autentificare. Diagrama sistemului se regăseşte în Figura 1. Odată ce utilizatorul execută o cerere către unităţile electronice de control din maşină, serviciul de autentificare este responsabil cu identificarea utilizatorului. Odată ce utilizatorul este identificat ca un utilizator legitim al sistemului, accesul este acordat de serviciul de control al accesului în funcţie de drepturile pe care utilizatorul le deţine. Suita de protocoale de autentificare folosită este de tip challenge-response şi se bazează pe o gamă largă de funcţii criptografice simetrice şi asimetrice. În particular am folosit inclusiv scheme mai exotice precum semnăturile de grup şi semnăturile bazate pe identitate. Figura 2 evidenţiază un detaliu cu privire la protocolul de solicitare a unei execuţii. Pentru a face faţă constrângerilor real-time, protocolul de execuţie care include şi funcţii asimetrice (partea stângă a figurii) are un corespondent în partea dreaptă bazat strict pe funcţii simetrice necesare unei execuţii mari rapide. Pentru detalii recomandăm consultarea lucrării [1]. De asemenea am investigat posibilitatea utilizării unor funcţii criptografice asimetrice (inclusiv semnături de grup şi semnături bazate pe identitate) pe sisteme embedded specifice vehiculelor în lucrările [4], [5], [9], [10] şi [13] din cadrul proiectului.

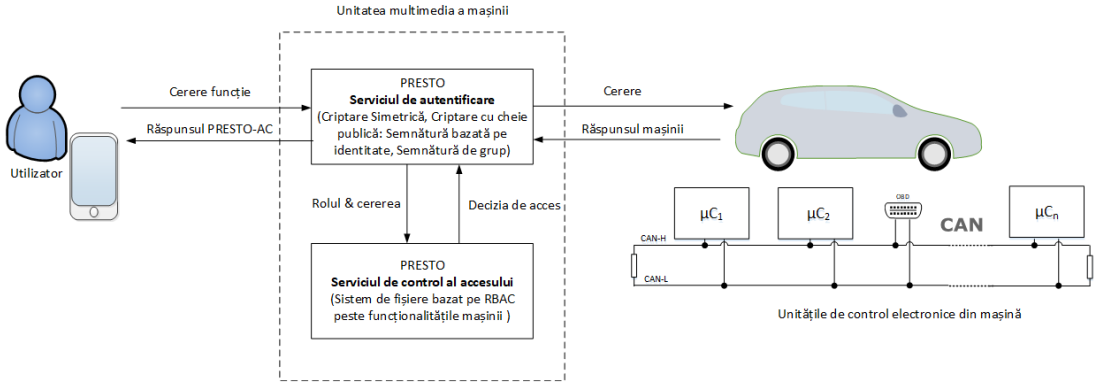
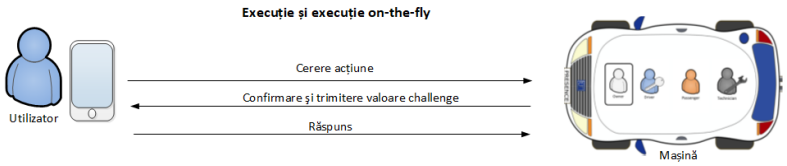


Figura 1. Sistemul de control al accesului la vehicule propus



1. Usr → Car: $m'_{\mathsf{usr}} = \{\mathsf{N_{usr}}, \mathsf{Role}, \mathsf{Atr}\}$,
$$s'_{\mathsf{usr}} = \begin{cases} \mathsf{GrSig}(\mathsf{gsk}[\mathsf{usr}], m_{\mathsf{usr}}) \ \textit{if} \ \mathsf{Usr} = \mathsf{Del} \\ \mathsf{IdSig}(\mathsf{sk}[\mathsf{usr}], m_{\mathsf{usr}}), s''^{,iv}_{own}, m'^{,iv}_{\mathsf{usr}} \ \textit{if} \ \mathsf{Usr} = \widetilde{\mathsf{Del}} \end{cases}$$
2. Car → Usr: $m_{car} = \{\mathsf{pk}_{car}, \mathsf{N}_{car}, \mathsf{SID}, \lfloor s'_{\mathsf{usr}} \rfloor_{64}\}$,
$$s_{car} = \mathsf{IdSig}(\mathsf{sk}_{car}, m_{car})$$
3. Usr → Car: $m''_{\mathsf{usr}} = \{\{\mathrm{K}_{ses}\}_{\mathsf{pk}_{car}}, \{\mathsf{act{:}exec}[i], \lfloor s_{car} \rfloor_{64}\}_{\mathrm{K}_{ses}}\}$,
$$s''_{\mathsf{usr}} = \mathsf{MAC}(\mathrm{K}_{ses}, m''_{\mathsf{usr}})$$

1. Usr → Car: $m_{\mathsf{usr}} = \{\mathsf{SID}, \{\mathsf{act{:}exec}[i]\}_{\mathrm{K}_{ses}}\}$,
$$s'_{\mathsf{usr}} = \mathsf{MAC}(\mathrm{K}_{ses}, m_{\mathsf{usr}})$$
2. Car → Usr: $m_{car} = \{\mathsf{N}_{car}, \lfloor s'_{\mathsf{usr}} \rfloor_{64}\}, s_{car} = \mathsf{MAC}(\mathrm{K}_{ses}, m_{car})$
3. Usr → Car: $s''_{\mathsf{usr}} = \mathsf{MAC}(\mathrm{K}_{ses}, s_{car})$

Figura 2. Exemplu de protocol pentru execuţie (stânga) şi execuţie rapidă (dreapta)

A1.2. Tehnologii pentru creşterea securităţii - carduri NFC

În cadrul obiectivului O2 al proiectului, ne-am concentrat atenţia pe tehnologiile de sporire a securităţii cum ar fi cardurile NFC şi modulele TPM. Mai exact, în cadrul activităţii A1.2. din 2018 am abordat tehnologia NFC şi în activitatea A2.3 din 2019 tehnologia TPM.

Near Field Communication (NFC) este o tehnologie de comunicare fără fir având distanța maximă de comunicare de aproximativ 20 cm făcând astfel parte din categoria tehnologiilor fără fir cu distanță mică de comunicație. Frecvența de operare este de 13.56 MHz, iar ratele de transfer pot varia între 106 kbits/s și 424 kbit/s. Distanța relativ mică de comunicare a protocolului NFC constituie un avantaj din punct de vedere al securității. Un alt avantaj este faptul că nu necesită asociere între dispozitive, ceea ce conduce la o utilizare mai rapidă și mai simplă de către utilizatori. Pe de altă parte, tehnologia NFC este foarte eficientă din punct de vedere al consumului de energie. Toate aceste aspecte ne-au determinat să luăm în calcul folosirea protocolului NFC ca protocol de comunicație între dispozitivele electronice folosite în cadrul conceptelor noastre. Am folosit în particular această tehnologie în lucrările [1] și [12].

În [1] am folosit tehnologia NFC pentru comunicația între telefoanele mobile inteligente facilitând astfel delegarea de drepturi de acces asupra unui vehicul de la un utilizator sau propietar către un alt utilizator. Pentru aceasta, am folosit modurile NFC reader și NFC card emulation. Telefonul folosit pentru delegarea drepturilor a funcționat în modul NFC reader, în timp ce telefonul folosit pentru recepția drepturilor a funcționat în modul NFC card emulation. Procedura de delegare a drepturilor se execută în patru pași, fiind astfel necesară schimbarea a patru mesaje între telefoanele participante utilizând protocolul de comunicație NFC. Dimensiunea pachetelor NFC transmise au fost de 254 octeți necesitând împărțirea mesajelor mai mari de 254 de octeți în pachete multiple.

Cardurile NFC sunt folosite într-o gamă largă de aplicații din diverse domenii, cum ar fi de exemplu micropayment, transport public inteligent sau controlul accesului. Folosirea acestor carduri pentru anumite aplicații aduce utilizatorilor multiple avantaje. Un prim avantaj ar fi dimensiunea redusă și portabilitatea acestor dispozitive. Un alt aspect de luat în calcul este faptul că aceste carduri sunt dispozitive pasive, ceea ce înseamnă că nu au nevoie de baterie sau altă sursă de alimentare, ci sunt alimentate de către dispozitivele de tip cititor de-a lungul unei sesiuni de comunicație folosind un câmp electromagnetic.

În [12] am folosit un card NXP Mifare Desfire EV1, ilustrat în Figura 3, pentru stocarea cheilor criptografice necesare în conceptul propus de memorare a istoricului de folosire al unui vehicul sau al unui alt aparat. Acest tip de card este compatibil cu toate cele patru niveluri ISO/IEC 14443A și suportă comenzi specifice standardului ISO/IEC 7816-4. Am decis să folosim acest tip de card datorită funcționalităților de securitate disponibile. Acesta suportă autentificare mutuală conform standardului ISO/IEC 7816-4 și oferă suport hardware pentru operații de criptare folosind DES (Data Encryption Standard) și AES (Advanced Encryption Standard) cu diverse dimensiuni de cheie. Memoria de stocare non-volatilă a cardului nostru este de 2 kilo-octeți și este organizată în aplicații și fișiere. Se pot defini până la 28 de aplicații, iar pentru fiecare aplicație se poate folosi un număr maxim de 32 de fișiere. Cardul are o cheie de tip master și poate avea definite până la 14 chei criptografice pentru fiecare aplicație. Mai mult, cardul suportă și transfer de date criptat. Pentru a facilita comunicația dintre Android și cardul NFC am folosit Taplinx SDK (Software Development Kit) care a fost dezvoltat și pus la dispoziție utilizatorilor de către firma NXP.

Tot în [12], am măsurat viteza de criptare şi decriptare folosind un telefon Android pentru a interacționa cu cardul, rezultatele fiind în ordinul a câteva sute de milisecunde şi deci acceptabile pentru scenariile practice (de exemplu timpul de acces la o maşină).

Figura 3. Dispozitivele cu capabilităţi NFC folosite: telefon mobil, card NFC şi kit embedded de dezvoltare

A1.3. Asocieri bazate pe date din ecosistem folosind date de la accelerometre

În cadrul obiectivului O3 am vizat asocierea inteligentă a dispozitivelor folosind date din mediu. În timpul funcționării, vehiculele generează anumite informații cum ar fi: vibrații, sunete, lumină etc. Toate aceste informații constituie ecosistemul vehicular care caracterizează fiecare vehicul în parte. Prezența numeroșilor senzori din dispozitivele inteligente moderne facilitează colectarea acestor date şi autentificarea se poate face pe baza acestora.

În particular, în activitatea A1.3., concretizată prin articolul [2], am adresat asocierea sigură (securizată) a smartphone-urilor pe baza datelor colectate cu ajutorul accelerometrelor din mediul diferitelor mijloace de transport: mașini, tramvai, tren, bicicletă, mers pe jos. Toate acestea sunt sugerate în Figura 4.

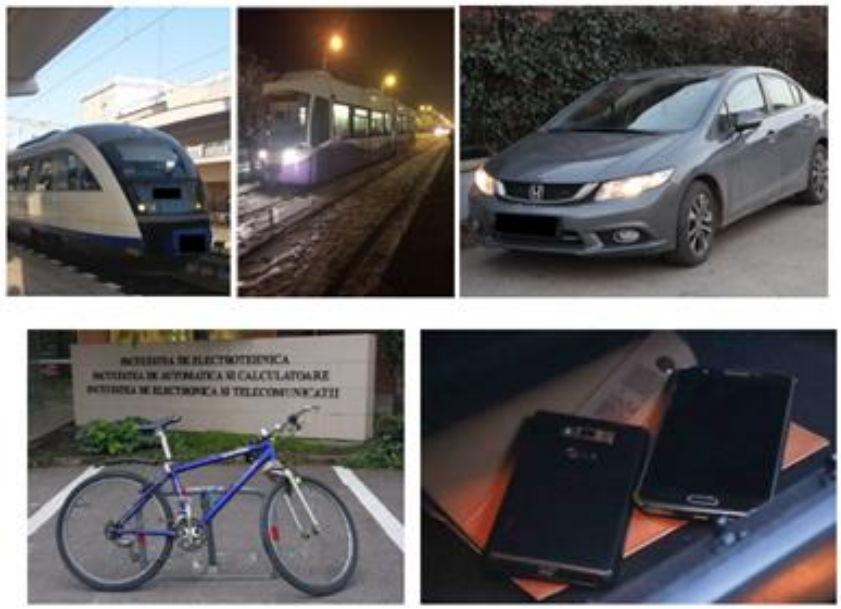


Figura 4. Mijloacele de transport și două dintre telefoanele utilizate: LG Optimus și Samsung J5

În sistemul Android, datele de la accelerometre sunt furnizate într-un sistem cartezian cu 3 axe. Pentru fiecare dintre experimentele noastre am folosit rezultanta acestor accelerații, în conformitate cu relaţia: $a = \sqrt{a_x^2 + a_y^2 + a_z^2}$. Cu ajutorul acestor date și a gamei variate de tehnici de procesare a semnalelor oferite de Matlab respectiv Mathematica: modularea sigma-delta, filtre trece-sus etc. am analizat formele de undă a accelerației rezultante, calculată pe baza datelor din diverse medii. Datele colectate în câteva scenarii sunt ilustrate în Figura 5.

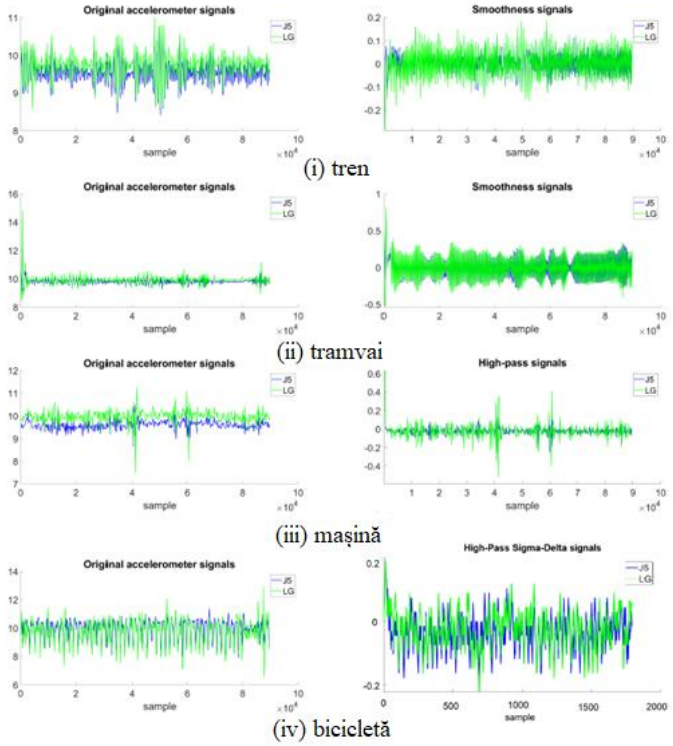


Figura 5. Datele accelerației colectate (stânga) și rezultatul aplicării tehnicilor de procesare a semnalelor (dreapta) [2]

Pe baza aplicării acestor tehnici, am extras o informație binară, care ne permite calcularea distanței Hamming a accelerațiilor extrase de la telefoane diferite situate în același mediu. Algoritmul nostru de asociere a telefoanelor are la bază identificarea de vectori binari identici (distanţa Hamming 0), din care se extrage o cheie de sesiune. De asemenea, am definit următoarele metrici de securitate pentru putea analiza nivelul de securitate a protocolului propus și pentru a măsura capacitățile adversarului de a impersona un utilizator onest:

- Probabilitatea de a ghici un octet de date (b) din l' vectori binari identici (v^0) necesară definirii nivelului de securitate:

$$\gamma = max\{Pr[b = b_i] : i = 1 \dots l', b_i \in v^0\}$$

- Entropia minimă a vectorilor binari cu distanță Hamming 0, deasemenea necesară definirii nivelului de securitate.

$$H_{min}^{v^0} = \sum_{i=1}^{l'} \log_2 \gamma = l' \log_2 \gamma$$

În Figura 6 se prezintă histograma care descrie probabilitatea de a identifica vectori identici având la bază datele extrase cu ajutorul telefoanelor LG Optimus și Samsung J5 comparativ în diferite medii de transport: tren, bicicletă, maşină, etc.

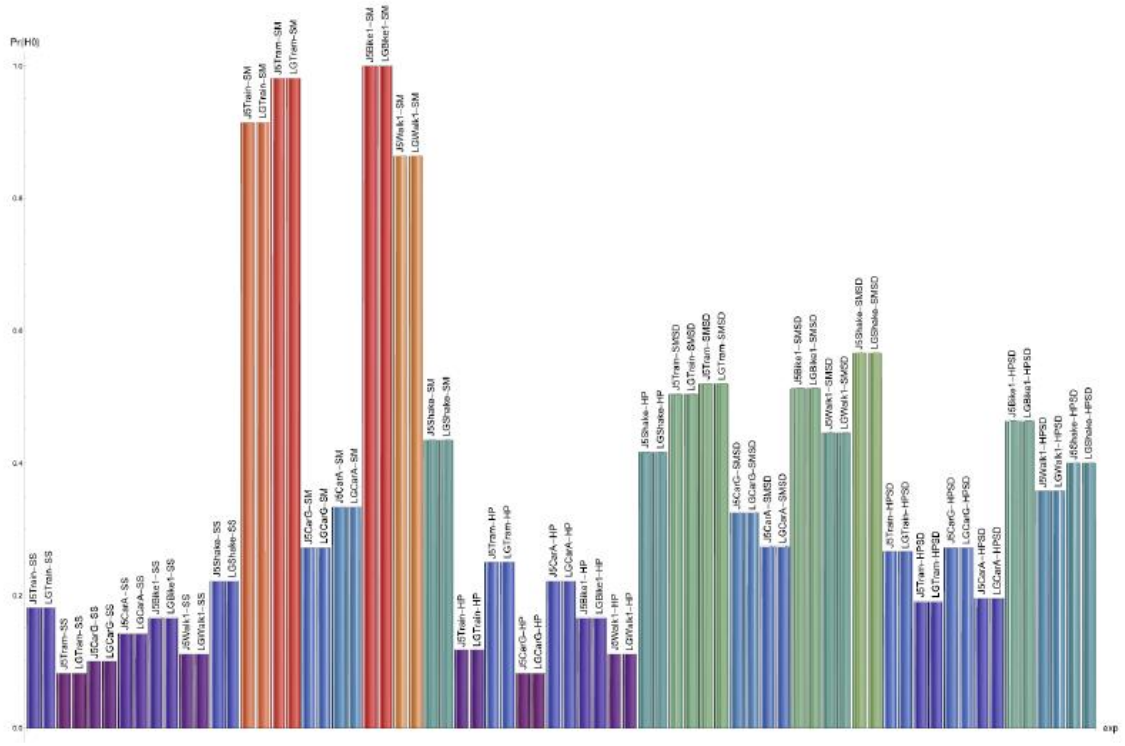


Figura 6. Probabilitatea de identificare a vectorilor identici în diferite experimente [2]

Protocolul utilizat pentru schimbul cheii de sesiune între dispozitivele mobile inteligente este de tip challenge-response și are la bază contrucțiile criptografice EKE-DH (Encrypted Key Exchange – Diffie Hellman) și SPEKE (Simple Password Exponential Key Exchange). Ca orice protocol, pentru a putea fi pus în practică, trebuie evaluat și din punct de vedere computațional. Astfel, am calculat timpul necesar operației de asociere a dispozitivelor mobile pentru EKE-DH și SPEKE, iar rezultatele sunt prezentate în Tabelul 1.

Smartphone	EKE-DH Z_P-1024 bit		EKE-DH Z_P-2048 bit		SPEKE-192 bit		SPEKE-256 bit	
	Share	Recover	Share	Recover	Share	Recover	Share	Recover
LG Optimus	42ms	64ms	230ms	411ms	94ms	39ms	145ms	70ms
Samsung J5	25ms	40ms	138ms	248ms	21ms	7ms	37ms	11ms
Samsung A3	22ms	39ms	126ms	236ms	20ms	7ms	34ms	12ms

Tabelul 1. Timpul computațional necesar operației de asociere pentru EKE și SPEKE [2]

În concluzie, rezultatele noastre arată că formele de undă ale accelerațiilor diferă semnificativ de la un mijloc de transport la altul ceea ce determină setarea unor anumiți parametri specifici în cadrul dispozitivelor mobile în funcție de mijlocul de transport în care sunt utilizate. De asemenea, fiecare mediu generează suficientă entropie pentru a putea genera o cheie de sesiune.

Etapa 2 – Configurarea şi controlul la distanţă al vehiculelor cu dispozitive mobile inteligente

Cea de-a doua etapă a proiectului, desfăşurată în anul 2019, continuă activităţile de studiu a tehnologiilor de creştere a securităţii prin module TPM şi folosirea de date audio-video din mediu, dar introduce şi utilizarea tehnologiilor cloud în accesul de la distanţă la vehicule. În cele ce urmează, descriem activităţile asociate.

A2.1. Configurarea vehiculelor la distanţă folosind servicii cloud

În cadrul obiectivului O4 din propunerea de proiect, ne-am propus să investigăm posibilitatea de a folosi tehnologii cloud pentru accesul la vehicule. Acest tip de acces este în mare parte util pentru aplicaţii de închirieri de maşini şi gestiune de flote de maşini, aplicaţii ce sunt tot mai des întâlnite în zilele noastre. Obținerea drepturilor de acces ale utilizatorilor de pe serverele externe (cloud) vine însă cu amenințări în ceea ce privește confidențialitatea datelor utilizatorului, iar aceștia pot fi urmăriți de furnizorii de servicii.

În [6] am propus, implementat și testat o soluție bazată pe un protocol de tip oblivious transfer, un bloc criptografic care permite păstrarea confidențialității utilizatorului atunci când obține acces la o anumită informaţie. Am luat în considerare inclusiv folosirea unor tehnologii existente cum ar fi CryptDB[1], în cele din urmă am considerat că este mai bine să investigăm o implementare proprie a echipei noastre folosind un protocol de tip oblivious-transfer asupra căruia avem un mult mai bun control în implementare. Implementarea a fost testată pe telefoane mobile inteligente cu Android dar și pe o unitate de navigaţie din mașină. Am folosit Microsoft Azure ca furnizor de servicii cloud pentru a stoca datele despre mașini și de asemenea am folosit și un server reprezentat printr-o mașină virtuală din cloud.

[1] https://css.csail.mit.edu/cryptdb/

Figura 7. Interfețele pentru selectarea mașinii (stânga) și control (dreapta)

În Figura 7 prezentăm interfețele din aplicația Antares Car Sharing pe care am dezvoltat-o pentru dispozitive mobile cu Android. Interfața permite utilizatorilor să selecteze din flota disponibilă mașina potrivită în funcție de caracteristicile ei specifice sau locație și permite efectuarea unei operațiuni de solicitare a drepturilor urmând procedura de plată. După obținerea cu succes a drepturilor asupra mașinii, o nouă interfață a aplicației poate fi utilizată pentru controlul funcționalităților specifice ale mașinii. Obținerea drepturilor de acces pentru o anumită mașină se face prin intermediul protocolului oblivious-transfer care permite ca selectarea unei anumite mașini să se facă într-o manieră anonimă. Ulterior, fiecare mașină își raportează starea în cloud.

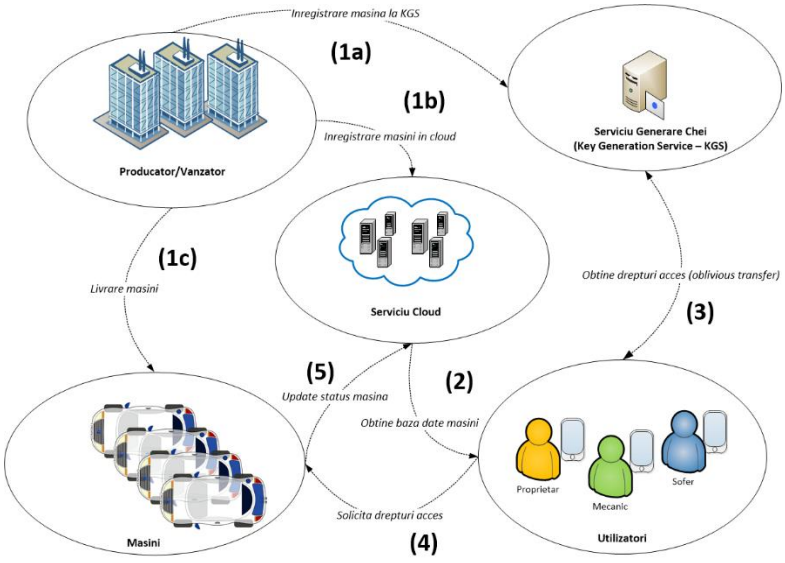


Figura 8. Schema de principiu a sistemului de acces la o flotă de mașini prin cloud

În Figura 8 prezentăm scenariul adresat în [6]. În acest scenariu, considerăm că producătorul de mașini sau furnizorul de servicii de închiriere este responsabil pentru pasul 1 care cuprinde înregistrarea mașinii la serviciul pentru generarea cheii, înregistrarea mașinii în cloud și livrarea mașinii. În pasul 2, utilizatorul obține datele mașinii din cloud, urmând ca în pasul 3 să obțină drepturi de acces de la serviciul de generare de chei, iar in pasul 4 să obțină accesul la mașină. După ce utilizatorul a obținut accesul la mașină, în pasul 5 mașina își actualizează starea în cloud. Protocolul oblivious transfer care stă la baza sistemului nostru este necesar pentru ca serviciul de generare de chei să nu știe la care mașină are acces un anumit utilizator. Acest protocol are securitatea bazată pe problema decizională Diffie-Hellman, iar noi îl implementăm folosind criptografia bazată pe curbe eliptice care asigură o reprezentare mai compactă. Acest protocol 1-la-2 poate fi ușor extins la cazul generic 1-la-n. Detaliile de implementare sunt publicate în [6].

De asemenea, am măsurat timpul computațional al protocolului pe mai multe telefoane, iar în Tabelul 2 prezentăm timpul computațional pe care l-am obținut când protocolul rulează între fiecare dispozitiv mobil (Samsung J5 și Samsung S7) și serverul Azure. Timpul de rulare este reprezentat pentru un număr maxim n=20, ceea ce permite utilizatorului anonim să selecteze peste un milion de chei distincte. De asemenea am testat următoarele curbe eliptice: secp160r1, secp192r1 și secp256r1.

	secp160r1		**secp192r1**		**secp256r1**	
n	**J5**	**S7**	**J5**	**S7**	**J5**	**S7**
4	476ms	554ms	501ms	528ms	594ms	782ms
8	971ms	1221ms	1178ms	1342ms	1216ms	2007ms
10	1176ms	1472ms	1246ms	1598ms	1413ms	2405ms
12	1515ms	1807ms	1489ms	1861ms	1639ms	2877ms
16	2041ms	2343ms	2056ms	2545ms	2185ms	3864ms
20	2525ms	3032ms	2583ms	3043ms	2810ms	4965ms

Tabelul 2. Timpul de rulare al protocolului între telefoanele mobile și serverul Azure

A2.2. Accesul și controlul la distanţă asupra vehiculelor, simulare folosind un model experimental

În cadrul obiectivului O5 din propunerea de proiect, am studiat conexiunea efectivă cu diverse subsisteme din mașini. Tot mai mulți producători de autovehicule pun la dispoziție aplicații destinate dispozitivelor mobile inteligente prin intermediul cărora este posibilă accesarea unor funcționalități ale autovehiculelor. Am studiat așadar, ca punct de pornire, funcționalitățile oferite prin intermediul aplicațiilor mobile dezvoltate de: Volkswagen, Toyota, Opel, Chevrolet, Mercedes, BMW, Audi, Tesla, Volvo. Rezultatele acestui studiu le-am publicat în [7].

În general sunt oferite funcționalități care oferă posibilitatea de a comanda și monitoriza la distanță: oprirea/pornirea motorului, blocarea/deblocarea ușilor, încălzirea scaunelor, pornirea/oprirea/configurarea sistemului de climatizare, activarea/dezactivarea sistemelor acustice precum şi a farurilor/semnalizărilor. Prin intermediul aplicațiilor mobile sunt oferite şi funcționalități de monitorizare a stării martorilor de bord, unii producători de autovehicule oferind și posibilitatea obținerii unor rapoarte de diagnoză detaliate. În acest context am adăugat o serie de funcționalități de monitorizare și comandă la distanță în interfaţa

aplicaţiei Android folosind ca punct de plecare standul experimental realizat în cadrul proiectului nostru anterior CSEAMAN. Subliniem că standul nostru experimental este la nivel proof-of-concept şi că design-ul nu include toate funcţionalităţile unei maşini reale. Schema de principiu a interacţiunii dispozitiv mobil – maşină este prezentată în Figura 9.

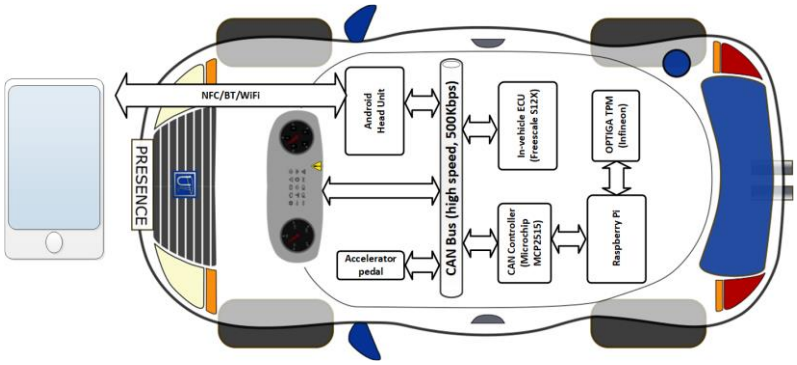


Figura 9. Schema de principiu a interacţiunii telefon mobil – vehicul (instanţiat de standul experimental al proiectului CSEAMAN)

Pentru implementarea noilor funcționalități am utilizat o placă de dezvoltare Raspberry Pi 3, aceasta oferind posibilitatea utilizării WiFI și Bluetooth pentru conectarea la dispozitivele mobile. Pentru implementarea funcționalităților de monitorizare și comandă, placa Raspberry Pi a fost conectată la modulul BCM (Body Control Module) al mașinii prin intermediul unei magistrale CAN. A fost aleasă această topologie deoarece modulul BCM implementează și funcționalități de securitate, inclusiv detecție de intruziuni, astfel de funcţionalităţi fiind de altfel adresate de noi în [3] şi [14]. Pentru a conecta Raspberry Pi la magistrala CAN a fost utilizat un controler CAN (Microchip MCP2515) precum și un transceiver CAN (NXP TJA1050). Figura 10 prezintă modelul experimental al proiectului nostru anterior CSEAMAN la care ne-am conectat prin intermediul modulului Raspberry Pi pentru a-l comanda cu ajutorul telefonului mobil.

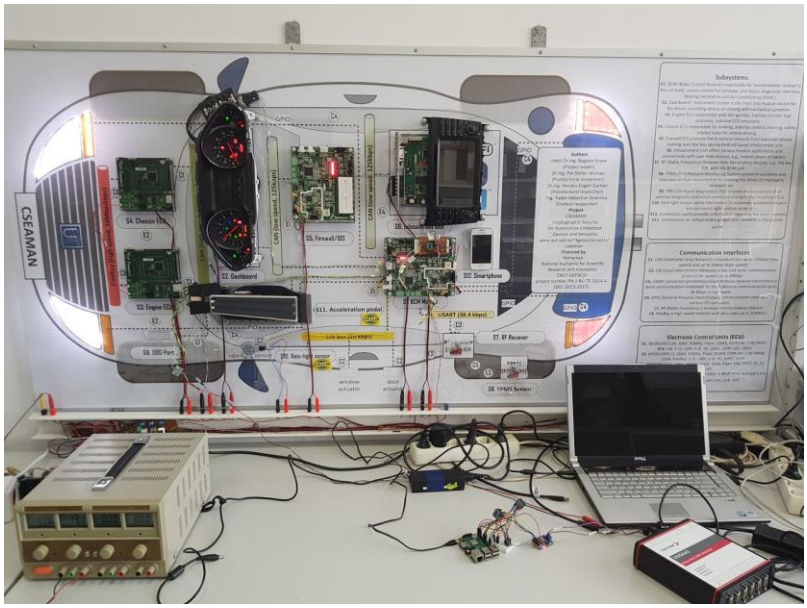


Figura 10. Modelul experimental utilizat pentru emularea unui vehicul în cadrul proiectului, model experimental rezultat din proiectul anterior CSEAMAN

Aplicația Android dezvoltată oferă facilități de monitorizare dar şi de comandă la distanță. Prin intermediul unei astfel de aplicaţii ar putea fi controlate diverse componente de pe stand, de ex., faruri, stopuri şi semnalizări. Ar fi relevante ca extensii şi monitorizarea unor periferice precum tensiunea bateriei sau a senzorilor din roţi [11]. De asemenea, datorită prezenţei instrumentului de bord în stand, este posibilă monitorizarea stării martorilor de bord corespunzători sistemelor ABS și ESP, frânei de mână, nivelului scăzut de combustibil, bateriei/alternatorului, presiunii scăzute a pneurilor. De asemenea, am utilizat pentru transmiterea și monitorizarea mesajelor CAN un software comercial, CANoe dezvoltat de compania VECTOR. Pentru ca funcționarea standului experimental să nu fie restricționată de utilizarea de software comercial a fost dezvoltată o aplicație care oferă funcționalități echivalente pentru trimiterea și monitorizarea acestor mesaje. O prezentare mai amplă a modelului experimental se găseşte în [7], respectiv [1] și [6] fac apel direct la modelul experimental.

A.2.3. Tehnologii de creştere a securităţii, module TPM

În continuarea activităţilor de sporire a securităţii (NFC) din obiectivul O2 în anul 2019 am continuat cu studiul tehnologiei TPM. Cu scopul de a propune un mecanism de acordare a privilegiilor de acces la mașină folosind funcții criptografice executate într-un mediu de execuție de încredere am utilizat un sistem conectat la un modul TPM (Trusted Platform Module). În cadrul mediului de execuție de încredere, conform cu standardul ISO/IEC 11889, un modul TPM permite verificarea autenticității pe baza unei chei unice, care nu poate fi extrasă din interiorul modulului, numită endorsement key (EK), derivarea unei chei pentru stocarea în siguranță a viitoarelor chei generate pentru metode criptografice numită storage root key (SRK), generarea de numere pur aleatoare sau de chei pentru criptografie simetrică (criptare AES-256 sau generare de coduri de autentificare a mesajelor HMAC-SHA256) sau asimetrică (criptare RSA-2048 sau semnături folosind criptografia cu curbe eliptice ECDSA-256), cât și executarea de funcții criptografice (RSA-2048, AES-256, HMAC-SHA256) folosind cheile generate. În lucrarea [8], pentru comunicația cu modulul TPM, am folosit interfața SPI accesibilă prin cele 4 linii specificate de protocol (CS, SCLK, MISO, MOSI) având ca SPI Master un modul Raspberry Pi 3 și ca SPI Slave un modul Infineon OPTIGA TPM SLB6970. Modulul Infineon OPTIGA TPM SLB6970, având toți pinii compatibili cu plăca de dezvoltare Raspberry Pi 3, a fost conectat direct la aceasta după cum se poate vedea în Figura 11.

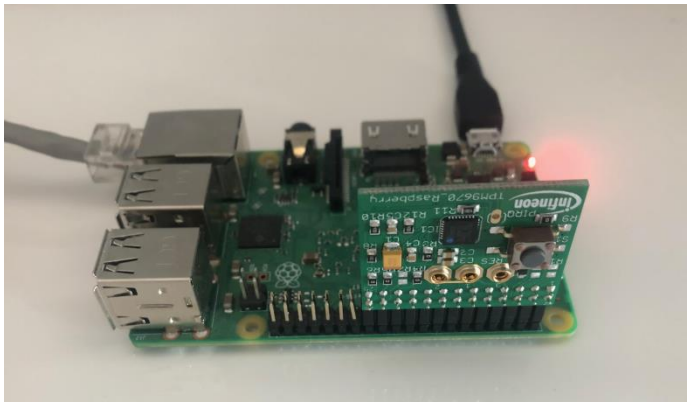


Figura 11. Modulul OPTIGA TPM SLB9670 conectat pe pinii plăcii de dezvoltare Raspberry Pi 3

Având conexiunea dintre cele două module realizată, modulul TPM fiind direct alimentat de către Raspberry Pi 3, au fost necesari mai mulți pași pentru a putea transmite comenzile către modulul TPM sau pentru interpretarea răspunsurilor primite de la acesta. Prima etapă necesară a fost activarea interfeței TPM2 în modulele din kernelul sistemului de operare al Raspberry Pi 3 prin includerea interfeței TPM2 pentru OPTIGA TPM SLB9670, recompilarea kernel-ului și includerea versiunii recompilate pe cardul de memorie unde se regăsește și sistemul de operare Raspbian. Având modulul SLB9670 recunoscut ca și modul TPM2 cu interfață SPI, pentru a transmite comenzile necesare generării și salvării cheilor în mediul sigur de stocare (en. Secure Storage), a comenzilor pentru executarea funcțiilor criptografice folosind anumite mesaje transmise de pe Raspberry Pi și cheile anterior generate, dar și pentru interpretarea răspunsului la comenzi de la modulul TPM am folosit bibliotecile software tpm2-tools, tpm2-tss și tpm2-abrmd accesibile pe Github[2].

Comandă către TPM	**Dimensiunea răspunsului (octeți)**	**Durata executării comenzii (milisecunde)**
Generare pereche chei asimetrice RSA-2048 de tipul SRK	1036	20736
Generare pereche chei asimetrice RSA-2048 pentru criptare/decriptare	280 (context cheie publică) / 192 (context cheie privată)	237
Încărcare persistentă cheie RSA-2048 în zona de stocare sigură pe baza contextului	1032	227
Criptare folosind cheia persistentă RSA	256	164
Decriptare folosind cheia persistentă RSA	256	326

Tabelul 3. Durata și dimensiunea răspunsului pentru comenzile executate de OPTIGA TPM SLB9670

Comenzile pentru criptarea și decriptarea mesajelor folosind cheia persistentă RSA prezentate în Tabelul 3 au fost utilizate pentru a realiza o semnătură bazată pe identitate propusă de Shamir și care a fost utilizată în cadrul protocolului din lucrările [1] şi [8]. Această metodă este folosită în etapa pentru acordarea privilegiilor de acces din mașină, (cu $ID_{autoturism}$), pentru o perioadă de timp (t_{start}, t_{stop}), unei persoane, (cu $ID_{persoană}$), de către un echipament autorizat din centrul de închiriere a mașinii (cu ID_{centru}). Pe baza informațiilor prezentate anterior, numite în acest context mesaj pentru autorizarea privilegiilor ($ID_{persoană}$, $ID_{autoturism}$, ID_{centru}, privilegii, t_{start}, t_{stop}), utilizatorul va recepționa o semnătură asociată mesajului de autorizare calculată de către o sursă de încredere (en. root of trust) reprezentată de un sistem cu modul TPM. Utilizatorul trebuie să folosească atât informațiile proprii cât și mesajul pentru autorizarea privilegiilor și semnătura asociată acestuia pentru autorizarea cererii de acces la anumite funcții din mașină. Etapele pentru autorizarea accesului la funcțiile cerute sunt prezentate în Figura 12.

[2] https://github.com/tpm2-software

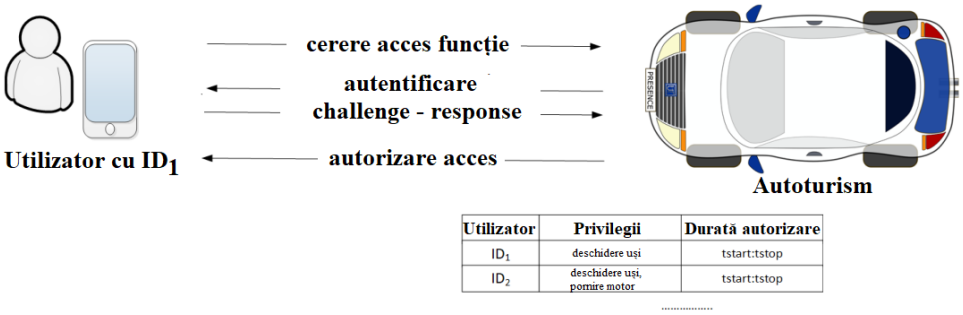


Figura 12. Autorizarea accesului pe baza informațiilor utilizatorului și a semnăturii generate de modulul TPM

Astfel, în lucrarea [8] am prezentat un scenariu aplicabil într-un caz real pentru situația în care o persoană dorește să închirieze un autoturism și să aibă accesul autorizat pe telefonul mobil la diferite funcții ale acestuia demonstrând modalitatea prin care un dispozitiv TPM poate fi utilizat și care sunt avantajele reprezentate de utilizarea acestuia în perspectiva execuției funcțiilor criptografice într-un mediu de încredere și stocarea cheilor de securitate într-o zonă de memorie sigură. Am prezentat și mecanismul de autorizare prin care utilizatorul va putea realiza diferite funcții ale autoturismului folosind un dispozitiv mobil și utilizând informațiile proprii și semnătura calculată de către un modul TPM într-un sistem din centrul de închiriere al autoturismului.

A.2.4. Asocieri pe baza de date din ecosistem, folosirea de date audio-vizuale

Acest obiectiv vine în continuarea asocierii bazate pe date din ecosistem din cadrul obiectivului O3 folosind date de la accelerometre, de data aceasta folosind date audio-video. Din studiul literaturii de specialitate am constatat că interesul este în mare parte pentru datele audio (zgomote, amprente sonore ale mediului, etc.), datele video fiind mai greu de colectat, mai voluminoase şi având factori negativi mai mari de securitate asupra utilizatorilor (de exemplu filmările efective pot afecta intimitatea utilizatorilor și necesită acord special). Am decis aşadar să ne concentrăm pe datele audio, mai exact pe zgomote din mediu şi amprente audio ale dispozitivelor (vocea subiecţilor umani este exclusă din aceleaşi motive de intimitate).

Într-una din lucrări (în curs de trimitere la un jurnal Q1 motiv pentru care nu poate fi menţionată) ne-am propus să construim un sistem de identificare a dispozitivelor mobile pe baza caracteristicilor difuzoarelor. Am amprentat difuzoarele pe baza informațiilor extrase din semnalele redate de difuzor și înregistrate de o unitate de navigație pentru mașină. În Figura 13, descriem configurația experimentală utilizată. Prin aceasta am demonstrat că un smartphone se poate amprenta pe baza înregistrărilor efectuate de o unitate de navigație din mașină, care este componenta principală în scenariul pe care îl vizăm. În acest fel, unitățile de infotainment din vehicul pot utiliza dispozitivul amprentat pentru a debloca anumite funcții și utilizatorii se pot autentifica fără a utiliza chei fizice bazate pe caracteristicile dispozitivului.

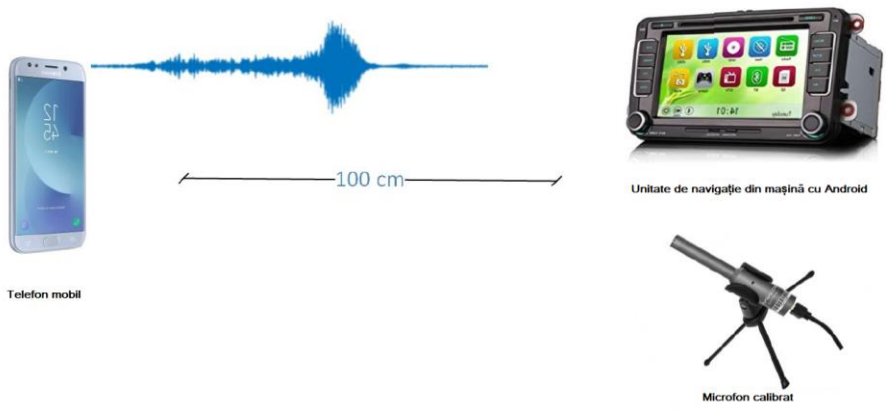


Figura 13. Prezentare sugestivă a configurației noastre experimentale: sunetul emis de un smartphone este înregistrat de o unitate de navigație din mașină sau de un microfon

Pentru experimente noi am folosit patru telefoane mobile: Samsung Galaxy S7 Edge, Samsung Galaxy J5, LG Optimus P700, Allview V1 Viper și o unitate de navigație din mașină echipată cu microfon. Fiecare telefon redă un fișier .wav care conține un semnal Linear Sweep, chirp sau un semnal periodic. Unitatea de navigație pentru mașină înregistrează semnalul și îl salvează ca fișier .wav, fișier pe care îl analizăm apoi în Matlab. În Figura 14 arătăm spectrul de putere pentru 3 tipuri se semnale chirp redate de Samsung J5.

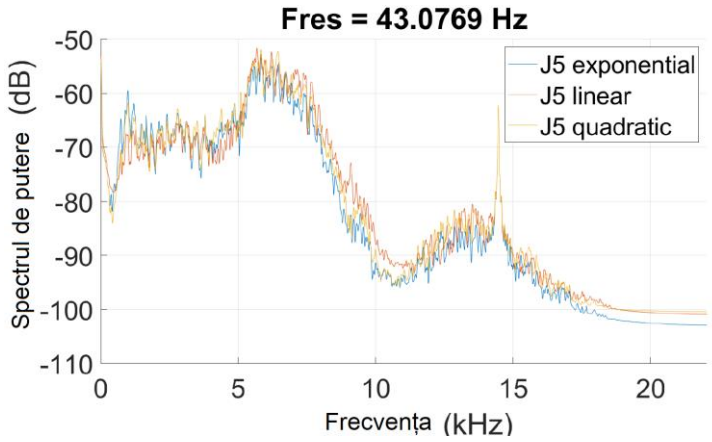


Figura 14. Spectrul de putere pentru 3 tipuri de semnale chirp redate de Samsung J5

Noi am analizat clasificarea difuzoarelor și pe baza unui semnal periodic de forma $s(t) = a * \sin(\frac{2\pi f t}{f_s})$, unde a este amplitudinea semnalului, f este frecvența, f_s este frecvența de eșantionare, iar t este timpul. Acest ton este utilizat pentru a codifica un 1, în timp ce difuzorul redă sunete, respectiv un 0, în timp ce difuzorul nu redă sunete. Fiecare telefon este folosit pentru a reda periodic secvențe de 0 și 1. În Figura 15 descriem un ton la 1kHz cu o periodicitate de 500ms, redat de cele 4 telefoane și înregistrat de unitatea de navigație.

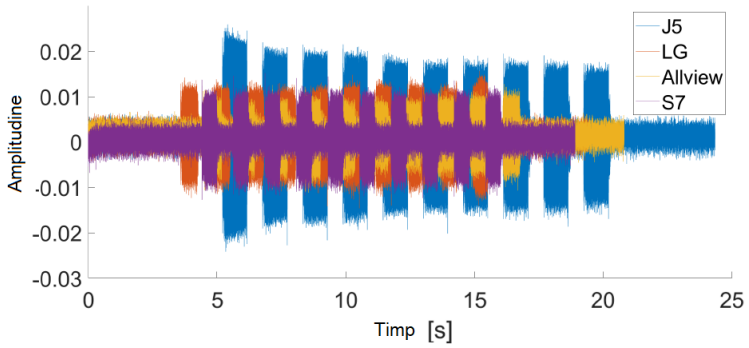


Figura 15. Ton la 1kHz cu o periodicitate de 500ms, redat de cele 4 telefoane și înregistrat de unitatea de navigație

Pentru a clasifica difuzoarele pe baza acestor semnale periodice, în primul rând am scalat semnalele, iar apoi am folosit vârfurile semnalelor audio de la cele patru smartphone-uri la 1kHz și 500ms periodicitate și înregistrate de navigație din mașină. Mai departe, am utilizat prima jumătate a fiecărui semnal audio ca date de instruire și a doua jumătate ca date de testare. În Tabelul 4 prezentăm rezultatele obținute cu mai mulți algoritmi de clasificare: Classification Trees (TREES), K-Nearest Neighbors (KNN), Naive Bayes folosind distribuție multivariabilă multivomială (NB -MVNM), Naive Bayes folosind estimarea uniformă (NB-KB), Random Forest (RF) și stimulare adaptivă folosind arbori (AdaBstM2). Aşa cum am menţionat, datele din această secţiune se află într-o lucrare în curs de evaluare la un jurnal Q1 şi momentan nu este posibil să oferim mai multe detalii.

Telefon	TREES	KNN	NB-MVNM	RF	NB-KB	AdaBstM2
J5/J5	99.33%	99.96%	99.82%	99.33%	63.25%	63.67%
S7/S7	99.94%	99.49%	99.97%	99.97%	14.86%	21.25%
LG/LG	99.32%	98.98%	99.6%	99.6%	29.52%	25.91%
AV/AV	99.78%	99.7%	99.81%	99.81%	43.89%	48.35%

Tabelul 4. Rezultatele obținute cu mai mulți algoritmi de clasificare

Etapa 3 – Evaluarea performanţelor şi montaj experimental

Cea de-a treia etapă a proiectului, desfăşurată în anul curent 2020, a vizat obţinerea unor rezultate finale, optimizări şi modificări ale protocoalelor de securitate propuse, respectiv conectarea la modelul experimental. Activităţile asociate sunt detaliate în cele ce urmează.

A.3.1. Designul analiza, şi implementarea protocoalelor de securitate, iteraţie finală

Iteraţia finală în elaborarea protocolului de control al accesului la maşină, i.e., PRESTvO, a constat în mare parte în optimizări şi verificări de securitate suplimentare. De exemplu, pentru partea de semnături criptografice bazate pe identitate Shamir şi Guillou-Quisquater, codul Java a fost implementat de noi, neavând o bibliotecă criptografică la dispoziţie care să facă acest lucru. Am avut nevoie de câteva iteraţii asupra codului sursă pentru a-l aduce la performanţele aşteptate. Codul sursă poate fi găsit pe site-ul proiectului[3,4]. Nu în ultimul rând, recenzorii de la jurnalele şi conferinţele unde au fost înaintate lucrările au cerut în mod susţinut dovezi cu privire la securitatea protocoalelor. Astfel, am fost nevoiţi să recurgem la metode formale pentru a aduce argumente convingătoare. În particular, am construit modele în limbajul IF suportat şi dezvoltat de proiectul AVISPA, codul sursă al acestora poate fi regăsit pe site-ul proiectului [5, 6].

Totodată, în iteraţia finală de dezvoltare a protocolului PRESTvO a trebuit să recurgem la îmbunătăţiri ale experimentelor computaţionale anterioare care să aducă şi rezultate comparative în ceea ce priveşte utilizarea curbelor eliptice. Varianta iniţială de protocol folosea în mare parte doar RSA, iar recenzorii au avut obiecţii cu privire la actualitatea acestui criptosistem. Considerăm că aceste obiecţii sunt doar parţial corecte, dar ne-am bucurat pe această cale să putem extinde rezultatele incluzând şi comparaţii cu variantele pe curbe eliptice. Rezultatele pot fi consultate în [1] şi [6], dar sunt de asemenea discutate şi în activitatea următoare ce vizează în mod direct măsurarea performanţelor. O altă îmbunătăţire semnificativă în designul protocolului a fost introducerea unor semnături bazate pe identitate care nu mai necesită certificate cu cheie publică şi fac posibilă asocierea cu vehiculul direct pe baza unui identificator cum ar fi numărul de înmatriculare sau numărul VIN al maşinii. Figura 16 prezintă în partea stângă interfaţa aplicaţiei şi sugerează în partea dreaptă un exemplu de asociere cu un vehicul. Testarea acestor funcţii bazate pe identitate a fost făcută de noi şi în cadrul magistralelor in-vehicle în lucrarea [5].

---

[3] http://www.aut.upt.ro/~bgroza/projects/presence/code/shamir.java

[4] http://www.aut.upt.ro/~bgroza/projects/presence/code/gq.java

[5] http://www.aut.upt.ro/~bgroza/projects/presence/code/avispa_if_exec.aslan

[6] http://www.aut.upt.ro/~bgroza/projects/presence/code/avispa_if_otf_exec.aslan

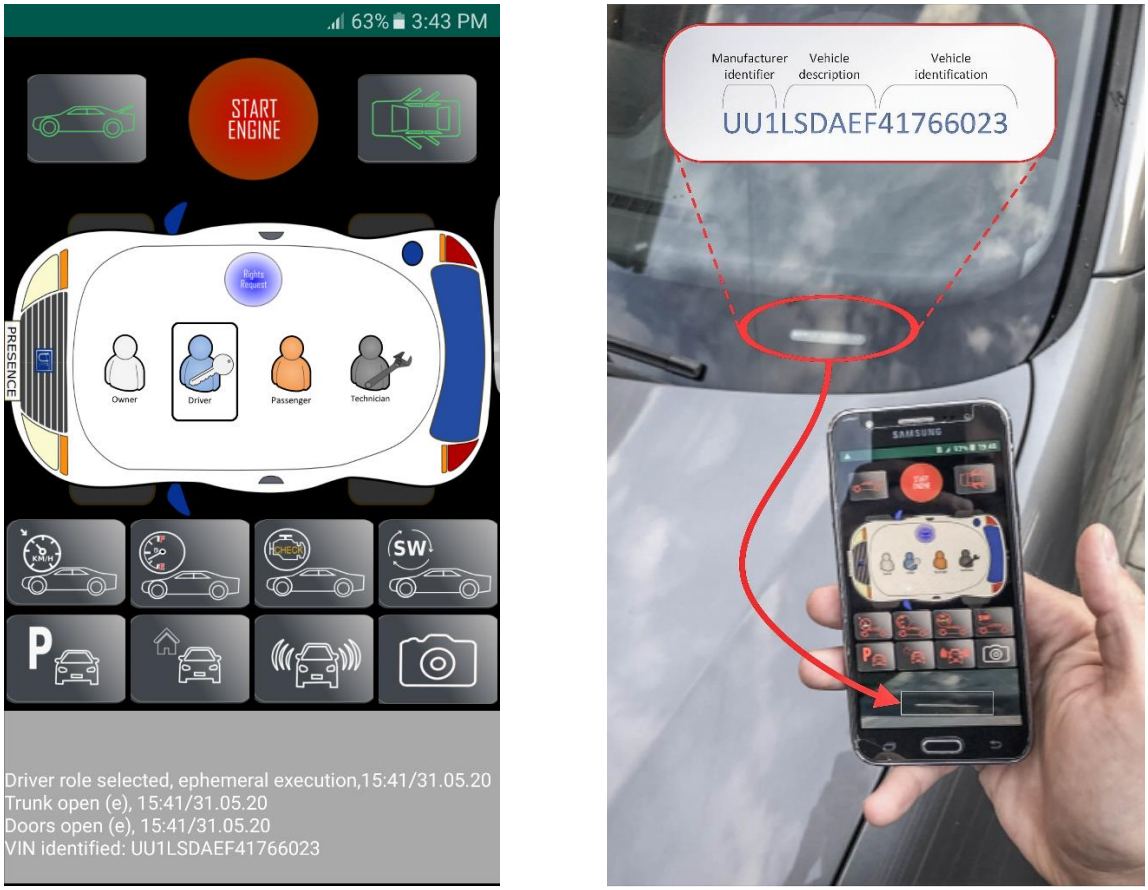


Figura 16. Interfaţa aplicaţiei Android (stânga) şi exemplu sugerat de asociere cu maşina (dreapta)

A.3.2. Evaluarea performantelor și montaj experimental

În cadrul acestei secțiuni vom prezenta rezultatele experimentale obținute utilizând telefoanele Android, unități infotainment, precum și controlerele specifice industriei automotive. Setup-ul experimental care a fost utilizat pentru testarea implementării software este prezentat în Figura 17. Din clasa controlerelor specifice automotive am ales sa folosim un controler Infineon Tricore TC297 care lucrează la o frecvență de tact de 300MHz dispunând de 8MB FLASH și 768KB RAM.

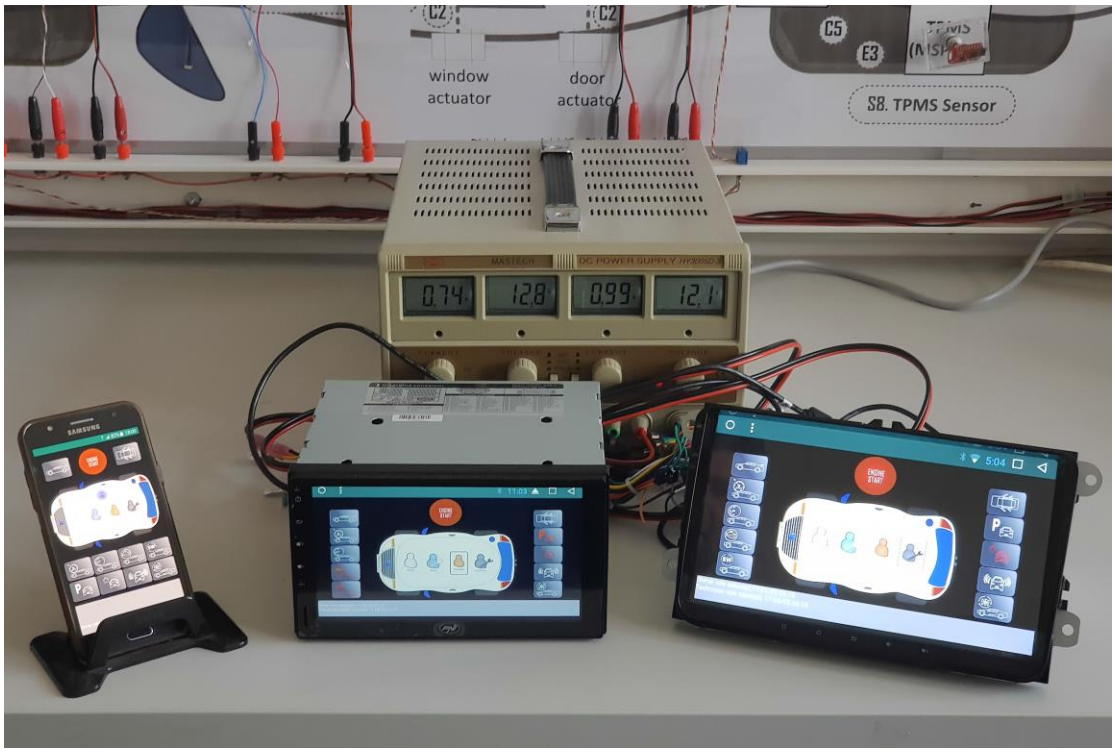


Figura 17. Unitățile infotainment și unul dintre telefoanele folosite în experimentele noastre

Am implementat în Android Studio trei proceduri ale protocolului nostru: delegare persistentă și efemeră, execuţie și execuţie rapidă. Am încercat să dezvoltam o implementare software simplă și scalabilă, astfel implementarea protocolului se bazează pe un automat cu stări finite. Sunt utilizate trei stări pentru procedurile de execuţie și execuţie rapidă și patru stări pentru procedura de delegare. Stările corespund mesajelor care sunt schimbate în timpul acestor proceduri. Pentru schema de semnături de grup (GS) am folosit biblioteca Pairings în C[7]. Aceasta conține și o aplicație demo Android care implementează semnătura de grup propusă de Boneh, adaptată și integrată în proiectul nostru.

Comunicarea Wi-Fi se bazează pe TCP/IP cu socket-uri. În acest caz, server-ul ascultă cererile de conexiuni primite iar clientul inițializează conexiunea. În setup-ul nostru telefonul inteligent este configurat ca și client, iar unitatea infotainment are rolul de server. Unitatea infotainment joacă și rolul de access point, telefoanele inteligente conectându-se la acesta.

O sinteză a timpului de calcul al primitivelor criptografice necesare utilizând diferite platforme este prezentat sub formă grafică în Figura 18. In lucrarea [1], am prezentat detaliat rezultatele obținute utilizând patru telefoane inteligente și două unități de infotainment.

[7] https://github.com/IAIK/pairings_in_c

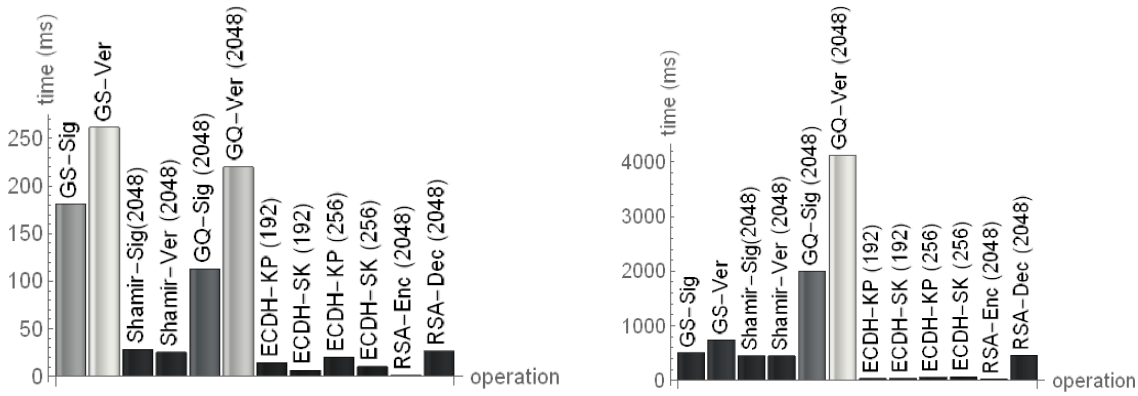


Figura 18. Timp de execuţie operaţii criptografice pe unitatea ERISIN Android (stânga) şi Infineon Tricore (dreapta)

Implementarea semnăturilor Shamir și Guillou-Quisquater (GQ) a fost dezvoltată de noi în C++ pentru controlerul Infineon şi în Java pentru dispozitivele Android. Pe dispozitivele Android, cel mai mare timp de calcul este obținut pentru semnătura de grup precum şi pentru versiunea GQ pe 2048-biți aceasta încadrându-se între 250-500ms. Pentru semnătura GQ, chiar dacă există posibilitatea obținerii unor rezultate mai bune prin optimizare, diferența de viteză este clar în favoarea utilizării semnăturii pe baza identității (IBS) propusă de Shamir. Pentru microcontrolerul Tricore, timpul de execuție devine inacceptabil pentru versiunea GQ de 2048 biți. Versiunea pe 1024 biți ar scădea nivelul de securitate astfel utilizarea semnăturii lui Shamir este singura opțiune viabilă. GS și versiunea GQ pe 2048 de biți au timpii de rulare similari pe Android, iar aceasta ne sugerează ca prin optimizare am putea obține rezultate similare şi pentru microcontrolerul Infineon.

Deoarece GS si IBS sunt utilizate rar, protocolul ar trebui să facă față unui scenariu de acces auto real. Presupunem că execuţia rapidă care se bazează numai pe criptografia simetrică este modalitatea obișnuită de accesare a mașinii, în timp ce execuția bazată pe identitate/grup este executată o singură dată pentru a stabili cheia de sesiune. RSA si ECDH au un timp de execuție mai mic decât GS și GQ, dar nu oferă avantajele semnăturilor bazate pe grup sau identitate. Daca pentru Android performanțele sunt aproximativ similare în cazul utilizării controlerului embedded, ECDH oferă timpi de execuție mult mai buni.

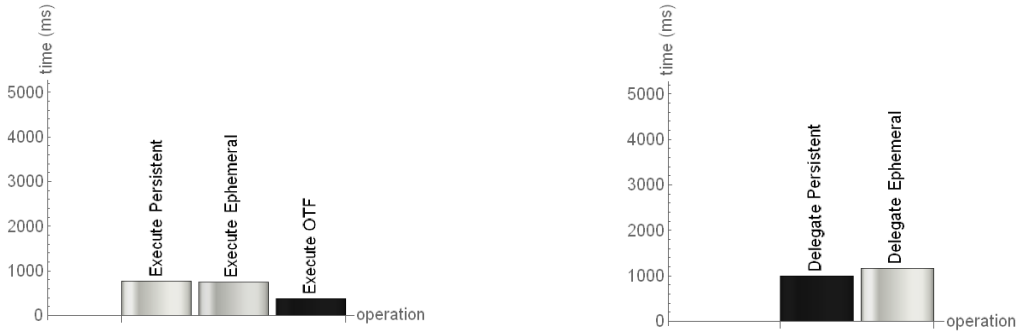


Figura 19. Timp de execuţie comanda între J5- ERISIN Android (stânga) şi delegare cu Shamir IBS S5-S7 (dreapta)

După cum se poate vedea în Figura 19, timpul de execuție în cazul utilizării unei unități infotainment Erisin pentru execuția persistentă şi efemeră utilizând Shamir IBS este sub o secundă, ceea ce ar trebui să fie suficient de rapid deoarece este necesar doar la prima execuție. Restul execuțiilor sunt efectuate on-the-fly, timpul de execuție fiind de ordinul sutelor de milisecunde (deoarece există o cheie comună partajată secretă). Prezentarea detaliată a valorilor obținute se găsește în lucrarea [1].

Concluzii

Proiectul PRESENCE a abordat probleme moderne de securitate apărute în ecosistemele formate de dispozitivele mobile inteligente şi maşini. Parte din aceste probleme sunt unilaterale şi independente aparţinând fie maşinilor, fie dispozitivelor mobile (de exemplu securitatea magistralelor din maşină sau securitatea dispozitivelor mobile în sine), iar parte sunt legate strict de interacţiunea dintre acestea (de exemplu problemele de conectivitate şi protocoale de autentificare de la telefon la maşină). Proiectul nostru a desfăşurat cercetări în toată această zona cu intenţia de a identifica problemele cele mai relevante şi de a publica lucrări ştiinţifice pe marginea acestora. Subiectele adresate sunt variate, de la tehnologii de creştere a securităţii folosind carduri NFC şi module TPM, asocieri folosind date din ecosistem (vibraţii şi sunet), utilizarea conectivităţii cloud sau securitatea sistemelor de comunicare in-vehicle. Proiectul a reuşit publicarea a cel puţin o lucrare de cercetare în legătură cu fiecare aceste subiecte. În anul 2018 am susţinut 2 lucrări în conferinţe [14], [13], în 2019 am susținut 6 lucrări în conferințe [12], [11], [10], [9], [8], [7] şi am avut acceptate 2 lucrări în jurnale ISI Q1 [5], [4], respectiv în 2020 am avut încă o lucrare publicată în cadrul unei conferinţe [6] şi încă 3 lucrări acceptate în jurnale Q1 [3], [2], [1]. Mai sunt în curs de evaluare 2 lucrări la jurnale Q1-Q2 şi încă 2 în curs de redactare. Prin acestea considerăm că am îndeplinit la nivel calitativ şi cantitativ planul de cercetare propus. Desigur, zona de cercetare a interacţiunii dintre vehicule şi dispozitive mobile inteligente este abia la început şi rămâne deschisă pentru explorări ulterioare.

Referinţe (lucrări publicate în cadrul proiectului)

[1] Bogdan Groza, Tudor Andreica, Adriana Berdich, Pal-Stefan Murvay, Horatiu Gurban, PRESTvO: PRivacy Enabled Smartphone-based access To vehicle On-board units, IEEE Access, 2020.

[2] Bogdan Groza, Adriana Berdich, Camil Jichici, Rene Mayrhofer, Secure Accelerometer-based Pairing of Mobile Devices in Multi-modal Transport, IEEE Access, vol. 7, 2020.

[3] Bogdan Groza, Lucian Popa, Pal-Stefan Murvay, Highly Efficient Authentication for CAN by Identifier Reallocation with Ordered CMACs, IEEE Transactions on Vehicular Technology, 2020.

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

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

[6] Adriana Berdich, Alfred Anistoroaei, Bogdan Groza, Horatiu Gurban, Stefan Murvay, Daniel Iercan, ANTARES - ANonymous Transfer of vehicle Access Rights from External cloud Services, 3rd International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms, VTC Workshops (STRIVE), 2020

[7] 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

[8] 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

[9] 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

[10] 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.

[11] 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

[12] 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

[13] Tudor Andreica, Bogdan Groza, Stefan Murvay, Applications of Pairing-Based Cryptography on Automotive-Grade Microcontrollers, 1st International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms (STRIVE 2018, SAFECOMP 2018 Workshops), Vasteras, Sweeden.

[14] Camil Jichici, Bogdan Groza, Stefan Murvay, Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks, 11th International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2018, Bucharest, Romania.