Raport de Cercetare

Etapa Nr. 1, Proiect PN-II-RU-TE-2014-4-1501

Securitate criptografică pentru sisteme embedded şi reţele folosite în vehicule

Autori

Dr. Ing. Bogdan Groza (director proiect)
Dr. Ing. Pal-Ştefan Murvay (postdoctorand)
Dr. Ing. Horaţiu Eugen Gurban (postdoctorand)

Universitatea Politehnica Timisoara

Noiembrie 2015

Raport de Cercetare

Etapa Nr. 1, Proiect PN-II-RU-TE-2014-4-1501

Prezentul raport adresează activitatea ştiinţifică aferentă etapei 1 a proiectului PN-II-RU-TE-2014-4-1501, Cryptographic Security for Automotive Embedded Systems and Networks (cSEAMAN). În conformitate cu propunerea de proiect, etapa 1 abordează obiectivul:

O1. Implementarea funcţiilor criptografice pe dispozitive embedded de clasă automotive

Având ca activitate de bază evaluarea capabilităţilor criptografice ale unor platforme cu microprocesoare folosite în sisteme embedded. Desigur că, dat fiind timpul scurt de la demararea proiectului şi aşa cum a fost şi menţionat în contract, în acest an putem prezenta doar o parte preliminară de rezultate. Aceste rezultate se bazează pe studiul unor platforme ţintă (alegerea unor dispozitive embedded) şi evaluarea resurselor de care acestea dispun în vederea dezvoltării unor soluţii de securitate criptografică.

Structura prezentului raport este după cum urmează. În capitolul 1 prezentăm pe scurt câteva platforme şi modul în care acestea au fost alese, punctând însă asupra capabilităţilor lor computationale (ce sunt determinante în vederea posibilităţilor de dezvoltare a unor soluţii criptografice). Dedicăm capitolului 2 pentru studiul preliminar al capabilităţilor criptografice precum şi al cerinţelor existente în acest domeniu. În capitolul 3 prezentăm o scurtă imagine asupra interconectivităţii care justuifică necesitatea securităţii dar ne oferă şi posibilitatea de a studia posibilitatea de aplicare a soluţiilor discutate – un aspect frecvent uitat este că securitatea poate fi aplicată doar omogen, adică (cu excepţiile de rigoare) nu putem pretinde mecanisme de securitate diferite pentru noduri ce sunt parte a aceluiaşi canal de comunicare. Capitolul 3 oferă astfel de imagine într-un context mai realist. În capitolul 4 sintetizăm concluziile acestui raport.

1. Studiu asupra dispozitivelor embedded de clasa automotive, resurse şi capabilităţi

În automobilele moderne, componentele ce îndeplinesc diferite funcțiuni au la bază dispozitive electronice de control care sunt realizate în jurul unor microcontrollere cu resurse și capabilități armonizate cu funcţiile care le întreprind (unele mai solicitante computational, altele mai puţin). Producătorii de dispozitive electronice oferă o gamă largă de microcontrolere destinate utilizării în domeniul automotive.

Pentru a fi calificat ca dispozitiv ce poate fi utilizat în industria automotive, un circuit integrat trebuie să suporte condițiile de funcționare specificate în documentul AEC-Q100 [1] – o colecție de cerințe stabilite de un consorțiu de companii ce desfăşoară activități în acest domeniu. Aceste cerințe se referă la comportamentul circuitelor integrate în diferite condiții precum cele date date de variații de temperatură și umiditate sau la diferite caracteristici electronice. În plus față de aceste caracteristici de bază fiecare microcontroller mai este dotat cu o serie de module ce vizeaza functiunea pentru care acesta va fi utilizat.

Pentru a evalua performantele criptografice ale microcontrollerelor utilizate în domeniul automotive s-a realizat un studiu având ca subiect o serie de platforme din rândul celor disponibile. S-a avut în vedere pe de-o parte răspândirea în produsele auto a circuitelor integrate în funcție de cota de piață a producătorilor. Tabelul următor ilustrează primii 10 producători de circuite integrate de clasa automotive după cota de piață conform referinţei [2].

Rang	**Companie**	**Cota piață**
1	Renesas Electronics Corporation	10,4%
2	Infineon Technologies	9,3%
3	STMicroelectronics	7,4%
4	Freescale Semiconductor	7,2%
5	NXP	6,4%
6	Robert Bosch	5,6%
7	Texas Instruments	5,5%
8	On Semiconductor	3,7%
9	Toshiba	2,5%
10	Micron Technology	2,4%
	Altele	39,4%

Tabel 1 Topul producătorilor de circuite integrate de clasă automotive

Pe de alta parte, au fost alese platforme cu resurse și capabilități variate pentru acoperirea tuturor funcționalităților ce trebuie deservite în interiorul autovehiculelor. Există o serie de parametrii ce influențează natura și performanțele mecanismelor de securitate ce pot fi utilizate pe o anumită platformă: arhitectura (dimensiunea regiștrilor), frecvența de lucru, memoria disponibilă și prezența unor module criptografice HW. Tabelul 2 prezintă platformele incluse în studiul nostru alături de parametrii relevanți amintiți mai sus.

În ceea ce privește arhitectura microcontrolerele utilizate în domeniu, acestea prezintă arhitecturi pe 8, 16 sau 32 de biți. Această caracteristică influențează dimensiunea codului obiect generat pentru implementarea SW a primitivelor criptografice ceea ce poate face diferența când memoria disponibilă este limitată. O arhitectură pe 32 biți este de preferat dar duce la creșterea costurilor dacă este utilizată în aplicații pentru care acest lucru nu se justifică precum controlul geamurilor sau al sistemului de iluminare.

Frecvența de lucru a microcontrollerelor se reflectă în viteza cu care sunt executate instrucțiunile atomice din codul obiect generat în urma compilării și prin urmare afectează viteza de execuție a programelor. Platformele studiate de noi în această fază de documentare acoperă o gamă variată de fercvențe de lucru caracteristice funcționalităților pentru care a fost conceput fiecare dispozitiv. Putem distinge astfel trei categorii de platforme:

i. prima categorie prezintă putere redusă de calcul cu frecvențe de până la 20 MHz pentru aplicații care necesită un volum mic de procesare de informații,

ii. o a doua categorie este caracterizată de frecvențe de lucru de ordinul zecilor de MHz folosite în module cu un nivel mediu de complexitate,

iii. o a treia categorie există pentru aplicații care necesită o cantitate considerabilă de procesare de date precum instrumentele de bord cu grafică avansată sau unitățile de control pentru blocul motor unde frecvențele utilizate se situează peste valoarea de 100 MHz în arhitecutri pe 32 de biți.

Dispozitiv	**Lățime regiștrii**	**Frecvența maximă**	**Memorie RAM / Flash / Date**	**HW criptografic**
Renesas				
R5F10PGJLNA	16-bit	32 MHz	20 KB / 256 KB / 8 KB	-
UPD70F4018M1GMA9	32-bit	160 MHz	256 KB / 2 MB / 32 KB	-
Infineon				
SP37	8-bit	12 MHz	256 KB / 6 KB / 31 B	-
TC1782	32-bit	180 MHz	176 KB / 2.5 MB / 128 KB	-
TC1797	32-bit	180 MHz	224 KB / 4 MB / 14 KB	-
STM				
SPC56EC74L7	32-bit	120 MHz	256 KB / 3MB / 64 KB	Criptare/decriptare AES-128 Autentificare CMAC AES-128
Freescale				
MC9S12C128	16-bit	50 MHz	4 KB / 128 KB / -	-
MC9S12DJ256	16-bit	50 MHz	12 KB / 256 KB / 4 KB	-
MC9S12XDT512	16-bit	80 MHz	20 KB / 512 KB / 4 KB	-
S12ZVHY64	16-bit	32 MHz	4 KB / 64 KB / 2 KB	-
MPC5604B/C	32-bit	64 MHz	48 KB / 512 KB / 64 KB	-
MPC5646C	32-bit	120 MHz	256 KB / 3 MB / 64 KB	Criptare/decriptare AES-128 (ECB, CBC) Autentificare CMAC AES-128 SHE Secure boot protocol

				TRNG și PRNG bazat pe AES-128
MCIMX6Q6AVT10AC	32-bit	1 GHz	256 KB	Criptare/decriptare: AES-128, AES-192, AES-256, DES, 3DES, și ARC4 Funcții hash și HMAC: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, și MD-5 RSA (până la 4096 bit) și ECC (până la 1023 bit), TRNG și PRNG
MCIMX6U1AVM08AB	32-bit	800 MHz	128 KB	
NXP				
Texas Instruments				
MSP430F2274	16-bit	16 MHz	1 KB / 32 KB / -	-
TMS320F28335	32-bit	150 MHz	68 KB / 512 KB / -	-
TMS5703137-ZWT	32-bit	180 MHz	256 KB / 3 MB / 64 KB	-
TMS470MF06607	32-bit	80 MHz	64 KB / 640 KB / 128 KB	-

Tabel 2 Parametrii platformelor incluse in studiu

Memoria internă este un alt factor ce caracterizează complexitatea aplicațiilor țintă pentru un microcontroller. O memorie RAM de dimensiuni mici limitează complexitatea software-ului în ceea ce privește numărul de variabile folosite și cantitatea de informații ce poate fi stocată pe stivă. Platformele studiate sunt dotate cu memorii RAM între 1 și 256 KB. Memoria Flash este utilizată pentru stocarea SW-ului limitând dimensiunea aplicației. Am identificat dispozitive cu meorii Flash de dimensiuni între 6 KB și 4 MB. Unele platforme dispun și de o memorie de date care poate să fie de tip EEPROM sau Flash. Această memorie este utilizată de obicei pentru stocarea de date de configurare.

2. Studiu asupra dispunerii microcontrolerelor într-o arhitectură in-vehicle

Noile generații de autovehicule se remarcă prin caracteristici tehnice superioare dar şi printr-un număr tot mai mare de facilitați care sporesc comfortul și siguranța pasagerilor. Această evoluţie se datorează integrării dispozitivelor electronice de control în subsistemele componente ale autovehiculelor, care se traduc printr-un număr tot mai mare de microcontrolere, senzori şi actuatoare, care nu doar controlează un subsistem din autovehicul dar transmit si recepţionează informații prin intermediul magistralelor de comunicație. Topologiile de comunicaţie folosite în autovehicule devin din ce in ce mai complexe, integrând un număr tot mai mare de magistrale de comunicație. A discuta despre dispozitivele

embedded din secţiunile anterioare în absenţa unei viziuni asupra arhitecturii interne şi amplasării lor echivalează cu a discuta despre piesele unui joc fără tabla pe care stau, de unde necesitatea acestei secţiuni.

Cele mai întâlnite magistrale fiind: CAN, LIN, MOST si FlexRay. Magistrala CAN (Controller Area Network), este cea mai răspândită, fiind folosită în toate clasele de autovehicule. Topologia sugerată în Figura 1 conține două magistrale CAN: powertrain CAN și comfort CAN. Pentru a interconecta microcontrolerele care controlează motorul, cutia de viteze, sistemul de frânare anti-blocare (ABS), sistemul de control al tracțiunii integrale (All-Wheel Drive, AWD), subsistemele de securitate pasivă (acţionarea airbag-urilor si a centurilor de siguranță) este folosit un bus CAN de mare viteza (High speed CAN). Aceste controlere sunt conectate la o magistrala CAN dedicată, powertrain CAN, conexiunea cu celelalte rețele fiind realizată prin intermediul unui gateway central. În topologia propusă ECU-urile ABS si AWD sunt conectate la powertrain CAN dar și la magistrala FlexRay. Topologia a fost creată având ca exemplu topologia de la un vehicul top Audi A8 [3].

Funcțiile de control a habitaclului (controlul temperaturii și umidității (HVAC), acționare geamurilor/oglinzi, ajustare poziție/încălzire scaune), funcțiile suport (monitorizarea presiunii din pneuri – TPMS (Tire Pressure Monitoring System), asistența la parcare) sunt implementate pe microcontrolere care sunt connectate la aceeași retea CAN în cazul topologiei propuse dar pot fi distribuite în mai multe rețele CAN. Magistrala LIN (Local Interconnect Network) este folosită în conjuncție cu celelalte magistrale, actuatoarele si senzorii sunt conectați utilizând aceasta magistrală la dispozitivul electronic de control. În cazul controlerelor de la uşi (ECU – front/rear – left/right) acestea sunt contectate la actuatoare, conectarea acestora la magistrala LIN realizându-se prin intermediul unor microcontrolere cu o putere de procesare redusă. Magistrala FlexRay interconectează modulul de asistență șofer, modulul de procesare a imaginilor precum și modulele ABS și AWD. Modelarea securităţii pe o astfel de topologie inspirată din realitate este o prioritate a proiectului, concomitent cu prima lună de activitate a proiectului noi am reuşit publicarea unui rezultat preliminar [8].

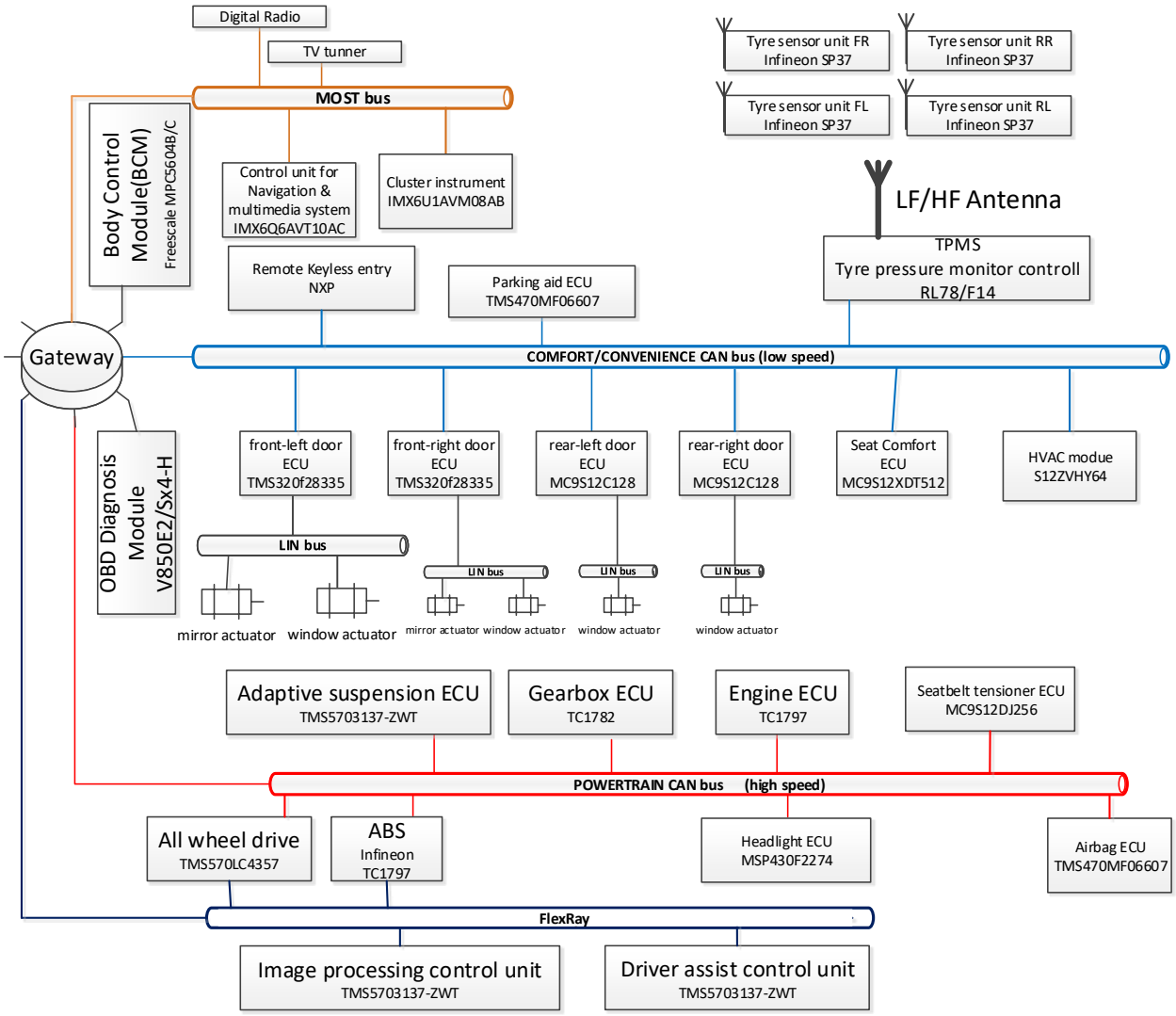

Figura 1. Posibilă arhitectură de reţea in-vehicle folosind dispozitive embedded specifice (prezentate în secţiunile anterioare)

3. Studiu asupra capabilităţilor şi cerinţelor pentru funcţii criptografice

Datorită numărului ridicat de vulnerabilitățți semnalate în ultimii ani, interesul pentru dezvoltarea unor sisteme de securitate pentru utilizarea în vehicule a crescut, lucru confirmat de lucrări ce apar în fiecare an [4], [5], [6], [9]. Acest fapt a determinat producătorii de microconrollere de clasă automotive să ofere dispozitive cu suport criptografic HW. Marea majoritate a dispozitivelor disponibile în acest moment sunt în continuare lipsite de suport criptografic HW dar se remarcă o creștere a numărului de astfel de produse aflate în curs de dezvoltare (ex.: familiile Renesas RH 850, Infineon AURIX sau SPC56B/C de la STM).

Funcționalitățile puse la dispoziție prin suportul HW variază de la o platformă la alta. Majoritatea platformelor includ suport HW pentru implementarea AES-128, algoritm de criptare simetric ce poate fi folosit atât la criptarea/decriptarea datelor cât și la autentificare prin implementarea CMAC (cod de autentificare a mesajelor bazat pe un algoritm de criptare) bazat pe AES-128. Unele platforme precum MPC5646C și iMX6 includ și generatoare de numere aleatoare necesare pentru implementarea unor protocoale de autentificare. Pe platforme din gamilia iMX6 regăsim suport pentru o serie de funcții hash coduri simetrice și asimetrice. Din păcate unii producători nu oferă în mod public informații complete despre caracteristicile modulelor HW criptografice oferind acces la acestea doar pe baza semnării unui NDA – ceea ce face cercetarea publică problematică. Din fericirea evoluţia securităţii arată că soluţia cea mai bună o reprezintă întotdeauna standardele publice, e.g., AES, RSA şi implementările publice, i.e., open-source.

Pentru a evalua performanțele criptografice ale dispozitivelor folosite în domeniul automotive au fost alese câteva platforme (marcate pe fond gri in tabelul 2) din cele incluse în studiul caracteristicilor. Acestea au fost alese astfel încât să reprezinte prin caracteristicile lor toate categoriile de microcontrollere utilizate în vehicule urmând ca pe acestea (sau cel puţin o parte din ele) să desfăşurăm experimente în perioada ce urmează. Ca ţintă de implementare în zona funcţiilor de criptare simetrice am fixat următoarele ca fiind de interes:

- AES ca fiind standardul current în domeniul codurilor bloc şi imposibil de ignorat,
- KATAN32 pentru că este un cod bloc light-weight larg utilizat,
- PRESENT un al cod bloc light-weight, larg utilizat, mai recent decât KATAN32,
- SPECK şi SIMON două coduri bloc ligh-weight propuse de NSA, mult mai eficiente computaţional decât cele anterioare,

Nu trebuie însă să uităm că ţinta principal în sisteme automotive nu este confidenţitatea informaţiei (realizată prin criptări simetrice) ci autenticitatea adică posibilitatea că într-adevăr informaţia provine de la o anume sursă. Fără autenticitate poarta în faţa unor atacuri prin injecţie de mesaje rămâne deschisă. Din fericire oricare din codurile bloc, inclusive cele mai sus menţionate, poate fi utilizat în construcţii de tip CBC-MAC sau CMAC pentru a asigura autenticitate. Dar, în mod traditional autenticitatea este asigurată prin coduri MAC care e construiesc peste funcţii hash. Pentru aceasta considerăm de interes şi următoarele funcţii hash pentru a fi implementate pe dispozitivele embedded ce le avem ca ţintă:

- MD5 deşi nu poate fi considerat sigur datorită numeroaselor atacuri prin coliziune, reprezintă un baseline pentru cerinţele computaţionale,
- SHA1 şi succesorul său SHA2 care este vechiul standard în funcţii,
- SHA3 care este noul standard ales prin competiţie publică, construit pe candidatul Keccak,

- BLAKE este unul dintre finaliştii SHA3, acesta este cel mai puţin intensive computational, aproape de MD5 la cerinţe, dar mai sigur (cel putin pe moment).

La finalizarea obiectivului O1 vom putea furniza un raport mai complet asupra performaţelor şi posibilităţilor de integrare a acestor criptosisteme pe platformele anterior enumerate. De asemenea prin obiectivele O2, O3, O4 şi O5 vom utiliza aceste rezultate pentru construcţia de protocoale.

4. Concluzii

Resursele computaţionale în dispozitive embedded variază de la foarte limitate la foarte generoase, un lucru la care ne aşteptam. Momentan, suportul existent pentru funcţii criptografice (implementat în hardware sau software de către producători) este foarte limitat dar resursele de calcul existente garantează posibilitatea implementărilor la nivel software (recent noi am reuşit dezvoltarea unor soluţii de Securitate criptografică inclusiv pe dispozitive extrem de limitate computational precum senzorii TPMS [7]). La fel cum standardele curente în automotive precum AUTOSAR care specific în mod expres implementarea funcţiilor criptografice în automotive sunt garanţia că aceste soluţii nu doar pot fi implementate ci vor fi cu celeritate adoptate de producători. Am reuşit de asemenea să obţinem o imagine preliminară de ansamblu asupa modului în care aceste dispozitive se interconecteză şi co-există într-o arhitecură automotive. Deţinem în laboratoarele noastre o bună parte din aceste echipamente pentru a desfăşura experimente şi implementări şi de asemenea prin prezentul proiect am derulat achiziţii pentru următoarele kit-uri de dezvoltare: i) kit dezvoltare Freescale bazat pe platforma S12 pentru clustere de vehicule, ii) kit dezvoltare Freescale bazat pe platforma Qorivva pentru sisteme complexe de control şi diagnoză în vehicule şi iii) un kit de dezvoltare ZedBoard care va permite dezvoltare de implementări hardware pe lângă un core ARM în scopul obţinerii unor performanţe ridicate şi eficienţă în consumul de resurse (microprocesoarele ARM sunt considerate de mulţi ca fiind perspectiva de viitor pentru unităţi infotainment şi alte aplicaţii automotive). Având în vedere timpul limitat acest raport se concentrează doar pe acest studiu asupra componentelor şi funcţiilor criptografice pe care ne vom axa, urmând să fie completat cu rezultate experimentale în lunile ce urmeză, pe măsura avansării noastre în cercetare.

Referinţe

[1] ***, Automotive Electronics Council, *Failure mechanism based stress test qualification for integrated circuits*, AEC - Q100 - Rev-H, September 11, 2014 (available at http://www.aecouncil.com/Documents/AEC_Q100_Rev_H_Base_Document.pdf).

[2] ***, *Automotive Semiconductors Supplier Rankings Adjusted Based on Further Analysis, IHS Says*, 26 Martie 2015, press.ihs.com, (available at http://press.ihs.com/press-release/automotive/2014-automotive-semiconductors-supplier-rankings-adjusted-based-further-ana)

[3] ***, Audi A8 2010, Electrical and network system, Self-study Programme 459, AUDI AG.

[4] Lin, Chung-Wei, Qi Zhu, and Alberto Sangiovanni-Vincentelli. "Security-Aware Modeling and Efficient Mapping for CAN-Based Real-Time Distributed Automotive Systems." Embedded Systems Letters, IEEE 7.1 (2015): 11-14.

[5] Othmane, Lotfi Ben, Harold Weffers, Mohd Murtadha Mohamad, and Marko Wolf. "A Survey of Security and Privacy in Connected Vehicles." In Wireless Sensor and Mobile Ad-Hoc Networks, pp. 217-247. Springer New York, 2015.

[6] Shreejith, Shanker, and Suhaib A. Fahmy. "Security aware network controllers for next generation automotive embedded systems." Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015.

[7] Solomon, Cristina, and Bogdan Groza. "LiMon-Lightweight Authentication for Tire Pressure Monitoring Sensors, 1st Workshop on the Security of Cyber-Physical Systems, 2015.

[8] Vasile, Paula, Bogdan Groza, and Stefan Murvay. "Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay." Proceedings of the WESS'15: Workshop on Embedded Systems Security. ACM, 2015.

[9] Woo, Samuel, Hyo Jin Jo, and Dong Hoon Lee. "A practical wireless attack on the connected car and security protocol for in-vehicle can." Intelligent Transportation Systems, IEEE Transactions on 16.2 (2015): 993-1006.