Zabezpečení IT infrastruktury automobilů

Bc. Patrik Kocian

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Patrik Kocian**
Osobní číslo:	**A16153**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení IT infrastruktury automobilů**
Téma anglicky:	**Securing of the IT Infrastructure in Cars**

Zásady pro vypracování:

1. **Vytvořte přehled nástrojů na testování zabezpečení IT infrastruktury.**
2. **Popište komponenty komunikační soustavy nacházející se v automobilech.**
3. **Identifikujte hrozby IT infrastruktury v automobilech.**
4. **Identifikujte zranitelnosti vybraných komponent.**
5. **Otestujte vybranou platformu IT infrastruktury automobilu.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **SMITH, Craig. The car hacker's handbook: a guide for the penetration tester. San Francisco: No Starch Press, 2016. ISBN 1-59327-703-2.**
2. **WEIDMAN, Georgia. Penetration testing: a hands-on introduction to hacking. San Francisco: No Starch Press, 2014. ISBN 978-1-59327-564-8.**
3. **Cyber Security and Resilience of smart cars: Good practices and recommendations. Heraklion: ENISA [European Union Agency For Network And Information Security], 2016. ISBN 978-92-9204-184-7.**
4. **Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [online]. 2016. Dostupné také z: http://standards.sae.org/j3061_201601/**
5. **CURRIE, Roderick. Developments in Car Hacking[online]. SANS Institute, 2016. Dostupné také z: https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21. 5. 2018

.....
podpis diplomanta

ABSTRAKT

Diplomová práca rieši problematiku zabezpečenia IT infraštruktúry automobilov. Úvodná časť predstavuje priblíženie základných princípov fungovania komponentov IT infraštruktúry a je doplnená o prehľad nástrojov vhodných na využitie pri testovaní zabezpečenia týchto komponentov. Výstup práce tvorí prezentácia identifikovaných hrozieb číhajúcich na automobily z pohľadu kybernetickej bezpečnosti a zraniteľností, ktoré môžu byť zneužité predstavenými hrozbami.

Kľúčové slová: IT infraštruktúra, automobily, kybernetická bezpečnosť, hrozby, zraniteľnosti

ABSTRACT

The diploma thesis solves issues related to securing of IT infrastructure of cars. Initial part presents approach to the basic principles of the operation of IT infrastructure components and is complemented by overview of suitable tools for security testing of these components. The output of the thesis consists of presentation of identified threats lurking on cars from cyber security point of view and vulnerabilities that can be misused by threats.

Keywords: IT infrastructure, cars, cyber security, threats, vulnerabilities

Touto cestou by som sa rád poďakoval vedúcemu mojej diplomovej práce pánovi Ing. Davidovi Malníkovi, PhD. za poskytnuté rady a vedenie pri tvorbe práce. Ďalej by som sa chcel poďakovať mojim blízkym za podporou počas celého štúdia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Technológie rapídne napredujú každým dňom a sú skoro v každej časti našich životov. Inak tomu nie je ani pri automobiloch. Keď pred niekoľkými rokmi neboli v autách takmer žiadne elektronické zariadenia, dnes je tomu naopak. Skoro v každej časti je nejaký elektronický komponent. Moderná automobily už nie sú len obyčajné prostriedky slúžiace na prepravu, ale zároveň poskytujú mnohé možnosti spríjemnenia, uľahčenia a bezpečnosti pri preprave. Svojimi funkciami sú porovnateľné s počítačmi či už konektivitou, preto sa nazývajú aj „connected cars“ alebo výpočtovou výkonnosťou. Ako je dobre známe pri počítačoch treba klásť dôraz na bezpečnosť, pretože hrozby číhajú na každom rohu a kybernetické útoky stále rastú. Rovnako je to aj pri automobiloch, keďže poskytujú skoro rovnaké možnosti ako počítače. Avšak, dôraz na bezpečnosť je podstatne nižší.

Moderné automobily alebo „connected cars“ predstavujú prepojenie mnohých elektronických riadiacich jednotiek prostredníctvom zberníc, čím vytvárajú siete, podobné tým aké sú známe pri počítačoch. Skoro každá funkcia, ktorá potrebuje výpočtovú silu má vlastnú riadiacu jednotku napojenú na zbernicu. Zbernice sa delia podľa kritickosti ich funkcií, napr. pre zábavu a média nie je kritickosť taká vysoká ako pri riadení volantu alebo ovládaní bŕzd. Tieto zariadenia spolu s ostatnými komponentami IT infraštruktúry poskytujú široké spektrum možností na útok rôznym činiteľom ohrozenia. Pri nedostatočnom zameraní sa na bezpečnosť daných komponentov pri ich vývoji alebo nasadzovaní vznikajú zraniteľnosti, ktoré môžu byť zneužité.

Automobily predstavujú vysokú finančnú hodnotu, čo môže útočník využiť na dočasné poškodenie a vyžadovať financie na návrat do pôvodného stavu. Tiež predstavujú nástroj využiteľný na zranenie alebo ešte na horšie účely, čo je ďalší dôvod na zvýšený záujem o zabezpečenie proti útokom za účelom ovplyvnenia ovládania prípadne prevzatia kontroly nad vozidlom.

Cieľom práce je vytvoriť základný prehľad komunikačnej sústavy využívanej v automobiloch, prehľad nástrojov využiteľných na otestovanie bezpečnosti, identifikovať hrozby, ktoré číhajú na automobily z hľadiska kybernetickej bezpečnosti, tiež identifikovať zneužiteľné zraniteľnosti vo vybraných komponentoch a vykonať test platformy.

I. TEORETICKÁ ČÁST

1 KOMUNIKAČNÁ SÚSTAVA V AUTOMOBILOCH

Moderné automobily obsahujú mnoho elektronických riadiacich jednotiek (ECU – electronic control unit), ktoré poskytujú možnosť pokročilých funkcií. Prepojené sú vnútri vozidla pomocou sériových zberníc a používajú na komunikáciu rôzne protokoly. Ďalší spôsob je bezdrôtová komunikácia, ktorá slúži na rozšírenie možností prepojenia s vozidlom, na pohodlnosť a zjednodušenie používania a samozrejme na bezpečnosť.

Inovácie prinášajú aj ďalšie možnosti komunikácie ako sú komunikácia vozidla s vozidlom (V2V – vehicle to vehicle) a vozidla s infraštruktúrou (V2I – vehicle to infrastructure), no tieto dve možnosti nebudú predmetom tejto práce.

1.1 Zbernice a protokoly

Zbernicové systémy zaisťujú hlavne komunikáciu sietí a senzorov vo vozidle, ale využívajú ich aj na posielanie správ na kontrolu správania sa vozidla a obsahu správ evidovaných v danom čase. Za riadenie prenosu paketov v zbernicových systémoch sú zodpovedné zbernicové protokoly.

Výber konkrétnych zberníc a protokolov podľa vhodnosti a charakteru si určuje sám výrobca automobilov. Asi najznámejšia zbernica CAN (Controller Area Network – sieť riadiacich systémov) je uložená na štandardnom mieste vo vozidlách a je propojená na konektor OBD-II (On-Board Diagnostics – palubná diagnostika).

Vo vozidlách je viac druhov zberníc špecifických najmä podľa určenia a ich funkcie, ktoré sú hodnotené podľa kritickosti. Management RPM (Revolutions Per Minute – otáčky za minútu) a brzdový systém sú hodnotené ako kritické, preto ich komunikácia sa sa uskutočňuje pomocou vysoko rýchlostných zbernicových prepojení. Naopak pri funkciách ako napr. zamykanie dverí alebo ovládanie klimatizácie, ktoré sú hodnotené ako nekritické, sa komunikácia uskutočňuje na stredne a nízko rýchlostných zbernicových prepojeniach [1].

1.1.1 Lokálna prepojovacia sieť

LIN (Local Interconnect Network – lokálna prepojovacia sieť) je najlacnejší systém sériovej komunikácie, kde nie je vyžadovaná implementácia multiplexných sietí s vyššou šírkou pásma ako napr. CAN zbernica. LIN bola vyvinutá súborom významných spoločností automobilového priemyslu (Daimler, Volkswagen, BMW, Volvo...) na dopĺňanie CAN a je bežne používaná vo vozidlách.

LIN klaster pozostáva z jedného "master" a viacerých "slave" uzlov pripojených na spoločnú zbernicu. Na dosiahnutie lacnej implementácie je fyzická vrstva definovaná ako samostatný drôt pracujúci na 12 V s dátovou rýchlosťou obmedzenou na 20 Kbit/s, kvôli limitom na elektromagnetickú interferenciu. LIN neústi do OBD konektoru, ale je často používaná namiesto priamych CAN paketov na ovládanie ovládacích prvkov jednoduchých zariadení.

Rámec správy LIN obsahuje hlavičku, ktorú vždy posiela "master" a časť na odpoveď, ktorú môže poslať "master" alebo "slave".

Hlavička			Odpoveď	
Zlom	Synchro-nizácia	Identifiká-tor	Dáta	Kontrolný súčet

Obr. 1. Rámec správy LIN [3], upravil Kocian, 2018

Zlom slúži na oznámenie začiatku rámcu správy. Obsahuje najmenej 13 dominantných bitov, po ktorých nasleduje jeden recesívny bit ako oddeľovač.

Pole synchronizácie umožňuje podriadeným zariadeniam, ktoré vykonávajú automatickú detekciu prenosovej rýchlosti, merať dobu prenosovej rýchlosti a upraviť ich interné prenosové rýchlosti za účelom synchronizácie so zbernicou.

Pole identifikátor poskytuje identifikáciu každej správy v sieti a tiež určuje, ktoré uzly v sieti prijímajú alebo reagujú na každý prenos. Zbernica LIN poskytuje celkovo 64 identifikátorov. ID čísla 0 až 59 sa používajú na nosiče signálov (dátové) rámce, 60 a 61 sa používajú na prenášanie diagnostických údajov, 62 je vyhradené pre užívateľom definované rozšírenia a 63 je vyhradené pre budúce vylepšenia protokolov.

Pole dáta môže obsahovať až 8 bajtov dát.

Zbernica LIN definuje použitie jedného z dvoch kontrolných algoritmov na výpočet hodnoty v poli osembitového kontrolného súčtu. Klasický kontrolný súčet sa vypočíta sčítaním samotných dátových bajtov a vylepšený kontrolný súčet sa vypočíta sčítaním dátových bajtov a chráneného ID.

Tento typ zbernice sa zvyčajne používa na ovládanie zamykania dverí, ovládanie klimatizácie, bezpečnostné pásy, strešné okno, osvetlenie, ovládanie okien a zrkadiel a podobne [1][2][3].

1.1.2 CAN zbernica

V osemdesiatych rokoch bola vyvinutá firmou Bosch pre mutliplexovú komunikáciu medzi elektronickými riadiacimi jednotkami vo vozidlách, čo malo za následok zníženie celkového množstva kabeláže. Navyše poskytuje možnosť elektronickým riadiacim jednotkám zdieľanie senzorov medzi sebou, čo pravdepodobne zapríčinilo jej popularitu a momentálne je najpoužívanejšou v automobilových sieťach.

CAN zbernica je zložená z krúteného páru medených drôtov (CAN high a CAN low). V roku 1994 sa stala štandardom medzinárodnej organizácie pre štandardizáciu (ISO – International Standard Organization. Jej výhoda spočíva v nízkej cene, robustnosti a ohraničeným komunikačným oneskoreniam. Rýchlosť prenosu dát dosahuje 1 Mbit/s.

V CAN môžu byť dáta segmentované v niekoľkých rámcoch a môžu byť prenášané periodicky, aperiodicky alebo na vyžiadanie (t.j. klient-server). Rámec CAN je označený identifikátorom prenášaným vnútri rámca, ktorého číselná hodnota určuje prioritu rámca. Existujú dve verzie protokolu CAN, ktoré sa líšia veľkosťou identifikátora: CAN 2.0A (alebo štandardná CAN) s identifikátorom o veľkosti 11 bitov a CAN 2.0B (alebo rozšíreným CAN) s identifikátorom o veľkosti 29 bitov. Avšak vo vozidlách sa využíva štandardná CAN, pretože poskytuje dostatočné množstvo identifikátorov [2][4][5].

Na nasledujúcom obrázku je zobrazená dátová správa štandardnej (2.0A) CAN zbernice.

	Riadenie prístupu na zbernici			Riadiace informácie			Dátová oblasť	CRC			
	SOF	Identifikátor	RTR	IDE	r0	Dĺžka dát	0 až 8 bajtov dát	CRC	ACK	EOF	IFS
Veľkosť [bit]	1	11	1	1	1	4	0 - 64	16	2	7	3

Obr. 2. Rámec správy podľa špecifikácie CAN 2.0A [4], upravil Kocian, 2018

SOF (Start of Frame – začiatok rámca) – označuje začiatok správy a používa sa na synchronizáciu uzlov po nečinnosti.

Identifikátor - určuje prioritu avýznam správy, čím nižšia je binárna hodnota, tým vyššia je jej priorita.

RTR (Remote Transmission Request – žiadosť o vzdialený prenos) – slúži k rozlíšeniu, či ide o dátovú správu alebo žiadosť o prístup ku zbernici.

IDE (Identifier Extension – rozšírenie identifikátora) – oznamuje, že sa prenáša štandardný CAN identifikátor bez rozšírení.

r0 – rezervovaný bit pre prípadné budúce zmeny štandardu.

Dĺžka dát – obsahuje počet bajtov prenášaných dát.

Dáta – môže byť prenášaných až 64 bitov dát.

CRC (Cycling Redundancy Check – kontrola cyklickým kódom) - obsahuje kontrolný súčet predchádzajúcich aplikačných údajov na detekciu chýb. Jeho veľkosť je 15 bitov plus 1 bit oddeľovač.

ACK (Acknowledgment – potvrdenie) – slúži na potvrdenie integrity dát. Veľkosť sú 2 bity z toho jeden je potvrdzovací a druhý je oddeľovací.

EOF (End of Frame – koniec rámca) – označuje koniec rámca, resp. správy.

IFS (Interframe Space – medzera medzi správami) - obsahuje čas požadovaný ovládačom na presun správne prijatého rámca do jeho správnej pozície v oblasti vyrovnávacej pamäte správy.

CAN sa využíva napr. na: elektronickú parkovaciu brzdu, elektricky ovládané dvere, ovládanie motora, svetiel a podobne [2][4][5].

1.1.3 FlexRay zbernica

Flexray zbernica umožňuje vysokorýchlostnú komunikáciu, čo znamená až 10 Mbit/s. Práve preto je využívaná pre komunikáciu citlivú na čase ako napr. šoférovanie po drôte, brzdenie po drôte a iné. V porovnaní so zbernicou CAN je cena implementácie vyššia, preto sa využíva v technologicky špičkových systémoch.

Zložená je štandardne z krútenej dvojlinky, ale môže tiež podporovať dvojkanálové prispôsobenie, čím sa dokáže zvýšiť šírku pásma a toleranciu voči chybám. Podobne ako u CAN sa zvyčajne implementuje len jeden pár.

Podporované sú dve topológie, prvá je zbernica, v ktorej sa štandardne vyskytuje a druhá z podporovaných je topológia v tvare hviezdy, ktorú využíva aj Ethernet. U hviezdy je centrálnym aktívnym zariadením Flexray rozbočovač komunikujúci s ostatnými uzlami. Rovnako ako pri zbernici CAN aj pri FlexRay zbernicovej topológii je dôležité korektné odporové zakončenie. V prípade potreby sa môže skombinovať topológia zbernice a hviezdy, čím vznikne hybridné usporiadanie [1].

Na nasledujúcom obrázku je možné vidieť cyklus u FlexRay, ktorý sa skladá zo štyroch častí a kde dĺžka každého cyklu sa stanovuje v čase návrhu.

Statická časť	Dynamická časť	Okno symbolov	Nečinná časť

Obr. 3. FlexRay komunikačný cyklus [1], upravil Kocian, 2018

V statickej časti sú obsiahnuté vyhradené miesta pre údaje vždy rovnakého významu a naopak v dynamickej časti miesta obsahujúce dáta rôznych reprezentácií. Časť okno symbolov používa sieť na signalizáciu a posledná nečinná časť slúži na synchronizáciu [1].

Základné zloženie paketov, ktoré zapadajú do cyklu v statickej aj dynamickej časti, je z hlavičky, dát a CRC.

Hlavička					Dáta	CRC
Status *(5 bitov)*	ID rámca *(11 bitov)*	Dĺžka dát *(7 bitov)*	CRC hlavičky *(11 bitov)*	Počítanie cyklu *(6 bitov)*	Dĺžka dát *x 2 bajty*	*3 bajty*

Obr. 4. Rozloženie FlexRay paketu [1], upravil Kocian, 2018

5 bitov v statuse sú:

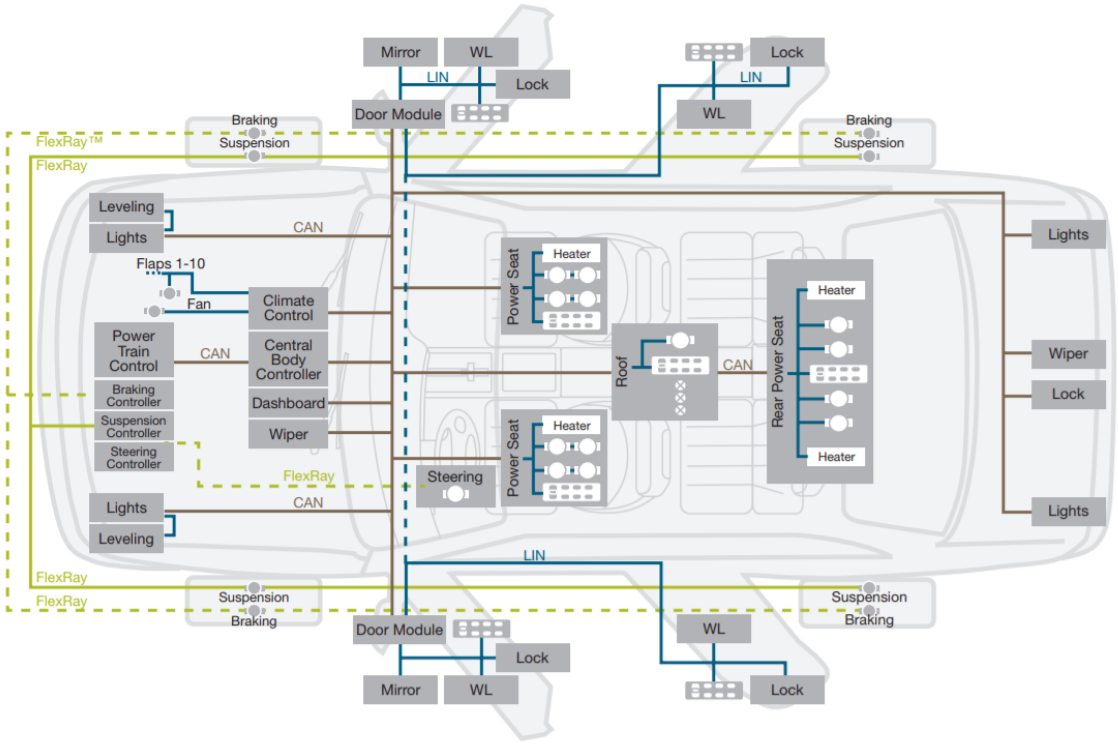
- vyhradený bit,
- indikátor preambuly dát,
- nulový indikátor rámca,
- indikátor synchronizácie rámca,
- indikátor spustenia rámca.

ID rámca je slot, kde by mal byť paket prenesený, keď je použitý pre statický slot. Keď je paket určený pre dynamický slot, ID predstavuje prioritu tohto paketu.

Dĺžka dát je číslo v slovách a môže mať dĺžku až 127 slov, čo znamená, že FlexRay paket môže prenášať 254 bajtov dát – viac ako 30-krát viac ako CAN paket.

CRC hlavičky slúži na detekciu chýb v hlavičke a počítanie cyklu sa používa ako počítadlo komunikácie, ktoré sa zvyšuje pri každom spustení komunikačného cyklu.

ECU je schopné čítať predchádzajúce statické časti, čo mu umožňuje vygenerovať výstupné hodnoty založené na tých predchádzajúcich vstupoch v tom istom cykle. Napríklad, ak ECU potrebuje poznať polohu kolies za účelom ďalšej manipulácie s nimi a tieto údaje sú na prvých štyroch miestach v statickej časti, ECU ich prečíta a do ďalších miest môže uložíť nové hodnoty [1].



Obr. 5. Využitie zberníc v automobiloch [6]

1.1.4 MOST zbernica

MOST (Media Oriented System Transport – prenos pre systémy zamerané na médiá) sa začala vyvíjať spoločenstvom MOST Cooperation, čo je konzorcium automobiliek a dodávateľov komponentov, v roku 1998. Je to multimediálna sieť poskytujúca prenos multimediálnych dát s rýchlosťou až do výšky 24,8 Mbit/s pri synchrónnom prenose a 14,4 Mbit/s pri asynchrónnom prenose. Na rozdiel od CAN a FlexRay využíva kruhovú topológiu alebo topológiu virtuálnej hviezdy podporujúcej až 64 pripojených zariadení. Jedno zariadenie na zbernici sa správa ako master, ktorý ma za úlohu posúvať rámce do topológie.

MOST poskytuje tri varianty rýchlostí: MOST25, MOST50 a MOST150.

Obyčajný MOST alebo MOST25 je zložený z plastových optických vlákien a údaje prenáša na vlnovej dĺžke červeného svetla pri 650 nm pomocou LED

Pri MOST50 je šírku pásma zdvojnásobená a dĺžka rámca je zvýšená na 1025 bitov. Prenos údajov u MOST50 zvyčajne prebieha na netienených krútených pároch (UTP – Unshielded Twisted Pair) namiesto optických vlákien.

MOST150 využíva Ethernet a frekvenciu rámcov je zvýšená na 3072 bitov (150 Mbit/s) – približne šesťnásobok šírky pásma MOST25.

Každý MOST rámec má tri kanály:

- synchrónny – streamované dáta (audio/video),
- asynchrónny – paketovo distribuované dáta (TCP/IP),
- ovládací – ovládacie a nízko rýchlostné dáta (HMI - Human Machine Interface – rozhranie medzi človekom a strojom).

Preambula *(4 bity)*	Popis hraníc *(4 bity)*	Synchrónne dáta	Asynchrónne dáta	Ovládanie *(16 bitov)*	Ovládanie rámca *(7 bitov)*	Parita *(1 bit)*

Obr. 6. Rámec MOST [1], upravil Kocian, 2018

Preambula synchronizuje jadro MOST a jeho vnútorné funkcie s bitovým tokom.

Popis hraníc označuje počet 4 bajtových blokov dát použitých pre synchrónne dáta v dátovom bloku ak sú synchrónne aj asynchrónne dáta naraz posielané v jednom rámci.

Časť pre synchrónne dáta sa väčšinou používa na prenos dát v reálnom čase ako audio/video. Prenos asynchrónnych dát je väčšinou používaný pre väčšie bloky a ak je potrebná väčšia šírka pásma. Spolu môžu mať 0 až 480 bitov.

Ovládacie dáta slúžia hlavne na komunikáciu medzi oddelenými uzlami na zbernici. Ďalšie pole slúži na ovládanie rámca a obsahuje statusové bity. Nakoniec parita slúži na detekciu chýb [1][2][7].

Tab. 1. Porovnanie zberníc

	Typ zbernice			
	LIN	**CAN**	**FlexRay**	**MOST**
Rýchlosť prenosu dát	20 Kbit/s	1 Mbit/s	10 Mbit/s	25 Mbit/s (150 Mbit/s)
Využitie	Ovládanie klimatizácie, zamykania dverí, okien, zrkadiel atď.	Ovládanie motora, svetiel, elektronickej parkovacej brzdy atď.	Šoférovanie po drôte, brzdenie po drôte atď.	Multimédiá
Fyzická vrstva	1 Cu	2 Cu	2 Cu	Optické vlákno

1.1.5 Ethernet

Hlavné dôvody prechodu na Ethernet je nízka cena a pokročilá technológia ponúkajúca väčšiu šírku pásma, čo je predovšetkým dôležité pre infotainment a bezpečnosť. MOST a FlexRay navyše strácajú podporu.

Ethernet v automobiloch je veľmi podobný ako v klasických počítačových sieťach. CAN pakety sú často zabalené ako UDP (User Datagram Protokol – užívateľský datagramový protokol) a audio je prenášané ako VoIP (Voice over Internet Protocol – hlas cez Internetový protokol). Za využitia akejkoľvek topológie poskytuje Ethernet rýchlosť prenášania dát rýchlosťou až 10 Gbit/s.

Výrobcovia automobilov začínajú používať štandard IEEE 802.1AS určený pre AVB (Audio Video Bridge – audio video most) podporujúci QoS (Quality of Service – kvalita služby) a tvarovanie prenosu dát za využitia časovo synchronizovaných paketov UDP. Synchronizácia týchto paketov je zaistená algoritmom „best master clock“, ktorý stanovuje hlavný časovací uzol. Synchronizácia hlavného (master) uzla je bežne vykonaná s externým zdrojom ako napr. GPS alebo palubný oscilátor a s ostatnými uzlami sa zosynchronizuje za pomoci odoslaných časovaných paketov od dĺžke 10 ms, pričom slave uzol zasiela odpoveď vo forme žiadosti o oneskorenia. Z tejto výmeny je následne vypočítaný časový posun [1][2].

1.1.6 Protokoly

ISO-TP protokol alebo tiež ISO 15765-2 zastúpený v CAN zberniciach je štandard zodpovedný za uskutočnenie prenosu dát a jeho výhoda spočíva v rozšírení 8 bajtového limitu až na 4095 bajtov za pomoci reťazenia paketov. Jeho hlavné využitie je v diagnostike a prenose Keyword protokolových správ. Avšak pri potrebe prenosu veľké množstvo dát cez CAN zbernicu je takisto vhodný.

CANopen Protokol takisto poskytuje rozšírenie CAN protokolu. Napriek tomu sa viac používa v priemyselných aplikáciách než v automobiloch.

SAE J1850 Protokol je starší a pomalší ako CAN a lacnejší na implementáciu. Sú dva typy protokolov [1]:

- **PWM** (Pulse Width Modulation – impulzová šírková modulácia) – zastúpený je na pinoch 2 a 10, pričom využíva diferenciálnu signalizáciu. Jeho využitie je najmä vo vozidlách Ford. Prevádzkové napätie je 5 V s rýchlosťou prenosu 41,6 Kbit/s na dvojvodičovej zbernici..
- **VPW** (Variable Pulse Width – variabilná šírka impulzu) – na rozdiel od PWM prebieha komunikácia na jednovodičovej zbernici, umiestnený je len na pine 2 prevažne vo vozidlách General Motors a Chrysler. Prevádzkové napätie je 7 V s rýchlosťou 10,4 Kbit/s.

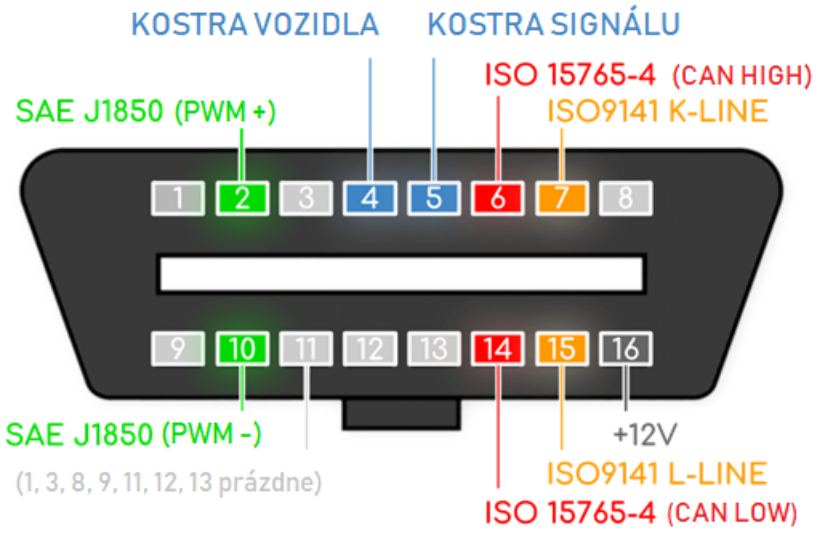
Keyword protokol 2000 (ISO 14230) alebo KWP2000 je diagnostický protokol, ktorý sa stal štandardom a môže byť použitý na niekoľkých transportných vrstvách. Do OBD II je pripojený na pine 7 a vyskytuje sa vo vozidlách vyrábaných v Spojených štátoch po roku 2003. Dĺžka správy môže dosahovať až 255 bajtov.

ISO 9141-2 alebo K-line je variácia KWP2000 používaná najmä v európskych vozidlách. Pripojenie je na pine 7 prípadne podľa potreby na pine 15 [1][8].

1.1.7 OBD II

Systémy palubnej diagnostiky sú dnes neodmysliteľnou súčasťou väčšiny vozidiel. Ich podstata spočíva vo funkcii autodiagnostiky a hlásenia chýb, ktoré sú určené na vyhľadávanie informácií o stave celého vozidla alebo jednotlivých častí. OBD II konektor je ľahko dostupný pre majiteľa a rovnako aj pre servisného technika.

Štandardné umiestnenie OBD II konektoru je v blízkosti volantu. Na nasledujúcom obrázku je zobrazené rozloženie pinov podľa ISO 15031-3. Pri 16 pinoch musia byť 4. a 5. uzemnené a 16. je pre 12 V napájanie z batérie [8].



Obr. 7. Rozloženie pinov OBD II konektoru [9]

1.2 ECU

Elektronická riadiaca jednotka je vstavané elektronické zariadenie dá sa povedať, že počítač, ktorý číta a spracováva údaje z mnohých senzorov naprieč vozidlom a následne na základe týchto údajov riadi a ovláda ďalšie časti vozidla ako sú napr. motor, elektrické okná, nastavenie sedadiel a pod.

Základné časti ECU sú hardware a software (firmware). Zložené je z mnohých elektronických súčiastok na doske plošných spojov, pričom najdôležitejší je mikropočítačový čip spolu s EPROM (Erasable Programmable Read-Only Memory – mazateľná programovateľná pamäť len na čítanie) alebo Flash pamäťou. Software (firmware) je tvorený súborom kódov, ktoré sú vykonávané v mikropočítačoch.

Moderné automobily plné elektronických systémov majú bežne 50, 70 a viac elektronických riadiacich jednotiek, napr. Škoda Superb, rok výroby 2008, ich má 36. Ich rozloženie môžeme vidieť na nasledujúcom obrázku [10][11][12].

Obr. 8. Umiestnenie elektronických riadiacich jednotiek v Škode Superb [12]

Podľa využitia môžeme ECU rozdeliť do 5 skupín [10]:

- ECM (Engine Control Module – riadiaci modul motora),
- EBCM (Electronic Brake Control Module – elektronický riadiaci modul brzdy),
- PCM (Powertrain Control Module – riadiaci modul pohonnej jednotky),
- VCM (Vehicle Control Module – modul riadenia vozidla),
- BCM (Body Control Module – riadiaci modul karosérie).

ECM je riadiaca jednotka v spaľovacom motore, ktorá má na starosti ovládanie rôznych funkcií, ako sú vstrekovanie paliva, zapaľovanie, systém riadenia otáčok pri voľnobehu a pod. Riadenie týchto častí je podmienené vstupnými hodnotami a údajmi z rôznych senzorov (napr. teplota chladiacej kvapaliny, prietok vzduchu, poloha kľuky atď.).

Modul ECM má schopnosť učenia sa o motore počas riadenia auta za účelom sledovania zmien v tolerancii senzorov a pohonov na motore. Aby sa tieto hodnoty nemusel učiť pri každom novom naštartovaní odznova, sú ukladané v pamäti RAM, ktorá je napájaná autobatériou [10].

EBCM je riadiaca jednotka predstavená v sedemdesiatych rokoch za účelom zlepšenia brzdového účinku pri akýchkoľvek poveternostných aj cestných podmienkach. Používa sa v module ABS (Anti-lock Braking System – protiblokovací brzdový systém). Päť vstupov ovplyvňuje reguláciu brzdových systémov a tieto sú [10]:

- Brzdy – vstupné informácie o stave brzdového pedálu, v digitálnej alebo analógovej forme.
- Pohon 4x4 – vstupné informácie o aktuálnom využívaní systému pohonu všetkých štyroch kolies.
- Zapaľovanie – vstupné informácie o umiestnení kľúča v zapaľovaní a o stave motora či je naštartovaný alebo nie.
- Rýchlosť vozidla – informácie o rýchlosti vozidla.
- Rýchlosť kolies – informácie o rýchlosti všetkých štyroch kolies.

PCM monitoruje a riadi reguláciu otáčok, klimatizáciu, nabíjanie a automatickú prevodovku. Vstupy dodávané do PCM sú od: snímača polohy škrtiacej klapky, snímača rýchlosti výstupného hriadeľa, snímača rýchlosti vozidla, snímača otáčok motora, brzdového spínača, ovládača tempomatu, zapaľovania atď. Pomocou týchto vstupov sa riadi ovládanie prevodovky, ovládanie ventilov cez výstupy PWM, spojka meniča krútiaceho momentu a riadenie relé ochrany prevodovky [10].

VCM má na starosti systémy ako:

- elektronický posilňovač riadenia,
- adaptívny tempomat,
- systém riadenia airbagov,
- elektronický stabilizačný program.

Tieto riadiace jednotky sú pripojené k rôznym druhom senzorov, aby boli schopné ovládať rôzne systémy. Aj z toho hľadiska sú štandardne umiestnené v strede automobilu medzi pasažiermi a motorom. Aby boli schopné správne určiť silu na nasadenie čelných airbagov potrebujú prijímať informácie zo snímačov ako sú napr. snímače nárazu, hmotnosti cestujúcich, polohy sedenia, uhlu volantu atď.

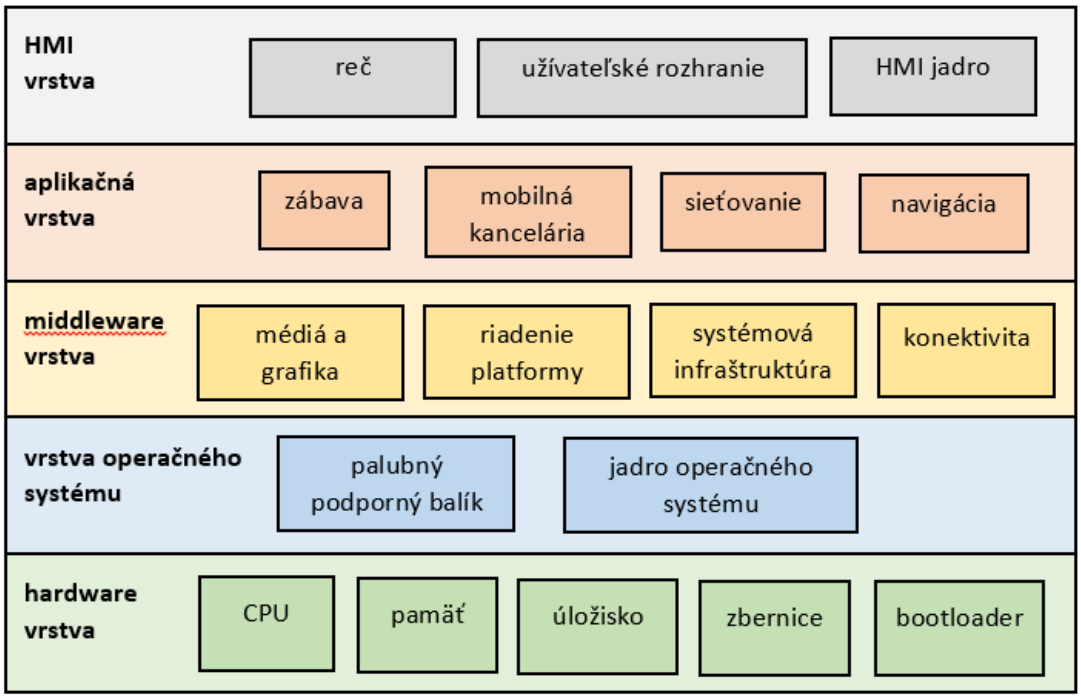
BCM má na starosti riadenie sedadiel, stieračov, elektrické okná a o sklápaciu strechu v kabrioletoch [10][11][12].

1.3 Infotainment

Infotainment alebo IVI (In-Vehicle Infotainment – infotainment vo vozidle) predstavuje spojenie dvoch, v dnešnej dobre veľmi vyžadovaných vecí, ktorými sú informácie a zábava. Práve infotainment ponúka informácie a zábavu, ktoré je možné ovládať prostredníctvom HMI pozostávajúceho z audio/video rozhraní, klávesníc, dotykových obrazoviek atď. Okrem iného sa v poslednej dobre stalo neodmysliteľnou súčasťou aj prepojenie smartphonov, čo samozrejme moderné infotainment systémy poskytujú či už vo forme pripojenia na telefonovanie, prehrávanie hudby, zrkadlenie obrazovky alebo pripojenia k Internetu.

Z hľadiska bezpečnosti, na ktorú je momentálne kladený vysoký dôraz boli zavedené určité opatrenia v systémoch IVI, ktoré majú zabrániť rozptyľovaniu vodiča.

Základná štruktúra a všeobecná architektúra systému IVI sa skladá v základe z viacerých prepojených hardwarových a softwarových komponentov. Keď sa pozrieme bližšie je možné IVI popísať pomocou vrstiev, kde úplne najnižšie sa nachádza hardwarová vrstva a naopak najvyššie je to HMI vrstva, ktorá poskytuje prepojenie človeka so systémom. Jednotlivé vrstvy sú prepojené rozhraním, aby boli schopné medzi sebou komunikovať a každá vrstva ešte obsahuje ďalšie technologické bloky, ktoré poskytujú požadovanú funkcionalitu systému [13].



Obr. 9. Architektúra IVI platformy [14], upravil Kocian, 2018

HMI vrstva: HMI je ústredným rozhraním pre používateľa systému. Prostredníctvom nej má užívateľ možnosť interakcie s daným systémom IVI. Na základe vstupov od užívateľa sa riadi a stará sa o zobrazenie hlavnej jednotky HMI, ktorá je zodpovedná za včasné a správne spracovanie požiadaviek a reakciu na všetky podnety používateľov prichádzajúce do systému, ako sú napr. rozpoznávanie reči, vstupy tlačidiel a vstupy dotykovej obrazovky.

Aplikačná vrstva: Obsahuje podobné aplikácie aké je možné nájsť aj v iných mobilných zariadeniach ako sú Bluetooth, telefón, kalendár, webový prehliadač, multimediálny zábavný systém atď. Ponuka dostupných aplikácií je bohatá a ponúka možnosť prispôsobenia.

Middleware vrstva: Jej cieľom je zjednodušiť komunikáciu a vstupy/výstupy dát medzi vrstvami pod ňou a nad ňou, čiže aplikačnej a vrstvy operačného systému. Obsahuje komponenty a rozhrania v softwari, ktoré vypĺňajú dieru medzi tými dvomi vrstvami, čím zabezpečuje bezproblémovú funkčnosť.

Vrstva operačného systému: Využíva sa celá škála operačných systémov (Microsoft, QNX, Microltron, Android, Linux, GENIVI atď.). Táto vrstva obsahuje aj ovládače, ktoré sú špecifické pre automobilové vstupy a výstupy.

Hardware vrstva: Základom tejto vrstvy je dostatočne výkonný hardware, najmä procesor a firmware, ktoré majú za úlohu zavedenie a plynulý beh operačného systému. Musí však obsahovať aj vstupné a výstupné zariadenia, aby bol IVI schopný komunikovať so zvyškom vozidla napr. prostredníctvom zberníc [13][14]..

1.4 Bezdrôtová komunikácia

V dnešnej dobe najžiadanejší spôsob komunikácie, pretože je najpohodlnejší, šetrí čas aj miesto a je jednoduchý. Užívatelia potrebujú neustále prepojenie či už svojho mobilného zariadenia s automobilom, automobilu s Intrernetom alebo častí automobilu medzi sebou.

1.4.1 Bluetooth

Pôvodným zámerom technológie Bluetooth bolo nasadenie na PAN (Personal Area Network – osobná sieť) pri ad hoc pripojení na krátke vzdialenosti s nízkymi nákladmi a nízkym napätím. Jeho popularita rýchlo rástla v mnohých odvetviach a výnimkou nebol ani automo-

tive priemysel vo forme bezdrôtovej siete v automobiloch. Dnes sa využíva najmä na spárovanie mobilného telefónu s automobilom a následné využívanie ako hands-free systému na uskutočňovanie telefonátov. Keďže zákon zakazuje používanie mobilných telefónov za jazdy je Bluetooth vynikajúca technológia. U verzie 4.0 sa používa frekvenčné pásmo 2,4 GHz a rýchlosť 24 Mbit/s [15].

1.4.2 Wi-Fi

Akýkoľvek typ siete IEEE 802.11 môže niesť názov Wi-Fi. Príkladom sietí 802.11 je:

- 802.11a (až 54 Mbit/s),
- 802.11b (až 11 Mbit/s),
- 802.11g (až 54 Mbit/s),
- 802.11n (až 600 Mbit/s) a
- 802.11ac (až takmer 3,5 Gbit/s).

Hlavné využitie týchto sietí je vo forme WLAN (Wireless Local Area Network – bezdrôtová lokálna sieť). Pri rôznych štandardoch 802.11 sú rozdiely v ponúkanej šírke pásma, frekvencii (2,4/5GHz), pokrytí, bezpečnostnej podpore a preto aj v podporovaných aplikáciách. Pre multimediálne, hlasové a video aplikácie v zastavaných oblastiach je vhodný štandard 802.11a, avšak oproti štandardu 802.11b ponúka kratší rozsah, čoho následok je potreba menej prístupových bodov na pokrytie veľkých oblastí. Kompatibilný je aj štandard 802.11g, ktorý je vhodný na nahradenie 802.11b, kvôli vyššej bezpečnosti a vyššej šírke pásma [15].

1.4.3 Celulárna sieť

Najčastejšie používaný štandard LTE (Long Term Evolution) pre vysokorýchlostnú bezdrôtovú komunikáciu (sťahovanie až 172,8 Mbit/s a odosielanie až 57,6 Mbit/s) pre mobilné dátové zariadenia, ako sú aj automobily. Zásadná vec na používanie celulárnych sietí je SIM karta, najlepšie podporujúca LTE, ktorá je vložená do určeného zariadenia v automobile (hotspot, LTE modem atď). Podporovaných býva až osem zariadení pripojiteľných pomocou Wi-Fi. Na spárovanie je možné použiť osobné identifikačné číslo alebo NFC (Near Field Communication – komunikácia v blízkom poli). Oproti ostatným bezdrôtovým technológiám spočíva výhoda v rýchlosti presnou [16].

1.4.4 Rádiová frekvencia

Rádiofrekvenčná komunikácia môže poskytnúť ďalšiu funkčnosť vozidla a pohodlie vodiča, čo umožňuje širokú škálu bezpečnostných a komfortných funkcií, ako sú PKES (Passive Keyless Entry and Start – pasívny bezkľúčový vstup a štart), diaľkové otváranie, TPMS (Tire Pressure Monitoring System – kontrola tlaku v pneumatikách), imobilizér a pod.

Imobilizér (známy aj ako transpondérový kľúč) obsiahnutý v kľúči využíva technológiu RFID (Radio Frequency Identification – rádiofrekvenčná identifikácia). Funguje na princípe autorizácie, kedy dochádza ku vloženiu kľúča do zapaľovania a následne je kľúč požiadaný o overenie. Tento spôsob zaisťuje ochranu pred fyzickým falšovaním kľúčov a krádeži vozidla zablokovaním zámku. Úspešná autorizácia prebehne len v prípade, že bol daný kľúč vopred spárovaný a motor môže byť naštartovaný. RFID technológia využíva nízke frekvencie v rozmedzí 120 až 135 kHz, pričom môže pracovať v režime pasívnom aj aktívnom [17].

Systém PKES takisto využíva technológiu RFID na čítanie informácií z kľúča, ktorý môže na rozdiel od kľúča s imobilizérom ostať vo vrecku vodiča. Antény sú umiestnené vo vnútri a na obvode vozidla, aby bolo zaistené správne zachytávanie informácií. V tomto prípade PKES využíva RFID signály s nízkou frekvenciou a UHF (Ultra High Frequency – ultra vysoká frekvencia) signál na odomknutie alebo spustenie vozidla. V prípade, že sú zaznamenané UHF signály bez prítomnosti nízkofrekvenčných, čo znamená neprítomnosť kľúča, ich vozidlo ignoruje. Vozidlo vyšle výzvu na šifrovanie pre kľúč, ktorý túto výzvu vyrieši pomocou svojho mikropočítača a zareaguje UHF signálom. Na uistenie sa o prítomnosti kľúča vo vnútri vozidla sa zväčša využíva triangulácia polohy. Po vybití batérie v kľúči sa nič nedeje, pretože obsahuje skrytý fyzický kľúč. S ním je možné aj odomknúť aj naštartovať, aj keď na naštartovanie je opäť využívaná RFID technológia [1][17].

Systémy kontroly tlaku v pneumatikách môžeme rozdeliť na dva druhy, priamy a nepriamy. Nepriamy funguje na základe zmeny rýchlosti otáčania kolesa, čím deteguje nižší tlak. Využíva senzory ABS, takže nepotrebuje samostatný systém na prenos informácií. Na druhej strane, priamy TPMS obsahuje senzor v každej pneumatike, kde meria tlak a posiela informácie bezdrôtovo do ECU. Tieto TPMS používajú rádiové frekvencie na komunikáciu

s ECU, ktorá sa líši medzi zariadeniami, ale zvyčajne to je 315 MHz alebo 433 MHz UHF za využitia amplitúdovej alebo frekvenčnej modulácie. TPMS môžu využívať aj Bluetooth, ktorý má väčší rozsah, ale ponúka možnosť bezpečnej komunikácie[1].

Záver kapitoly

Komunikačné systémy vo vozidlách predstavujú naozaj širokú škálu jednotlivých zariadení. Zbernicové systémy a protokoly, ktoré slúžia na komunikáciu medzi riadiacimi jednotkami, senzormi a akčnými členmi, u ktorých sú rôzne možnosti aplikácie závisiace od kritickosti komunikácie, kde LIN zbernica sa používa na najmenej kritické implementácie ako sú ovládanie sedadiel, osvetlenia atď, CAN, ktoré slúžia na ovládanie motora, FlexRay zase na tie kritické ako sú riadenie po drôte a MOST zbernice na multimédiá. Rozhranie na pripojenie sa do sieti zberníc poskytuje konektor OBD-II, ktorý je pripojený na CAN.

Na riadenie určitých akčných členov slúžia ECU, ktoré sa delia na päť druhov podľa ich využitia od najdôležitejších ako riadenie motora až po tie najmenej dôležité ako sú riadenie napr. sedadiel.

Neodmysliteľnou účasťou komunikačných systémov je infotainment, ktorý poskytuje užívateľom prepojenie medzi nimi a autom a poskytuje im pomoc aj zábavu. Na správne fungovanie infotainmentu je potrebná bezdrôtová komunikácia, ktorá pohodlne prepája užívateľské prenosné zariadenia s automobilom (Bluetooth, Wi-Fi, celulárne siete) alebo prvky automobilu ako sú bezkľúčové odomykanie a štartovanie a kontrola tlaku v pneumatikách.

2 NÁSTROJE NA TESTOVANIE IT INFRAŠTRUKTÚRY

Trh ponúka širokú paletu rôznych nástrojov, ktorými je možné testovať zabezpečenie automobilov, odpočúvať komunikáciu, prekonávať zabezpečenie a vykonávať mnoho ďalších aktivít. Rozsah a kvalita použitia môže závisieť od dostupnosti daného nástroja, voľne dostupný, lacnejší alebo drahší.

2.1 Hardware

Hardwarové nástroje sa dajú využiť hlavne na odpočúvanie komunikácie na CAN zbernici a na injektovanie paketov. Voľba závisí od preferencií a najmä od ceny, kde sa úroveň pohybuje od hobby používateľov až po profesionálne zariadenia schopné pracovať s viacerými zbernicami naraz [1].

CANtact

CANtact je open source rozhranie pre PC z USB na CAN. Jednoducho prepojiteľné s OBD II konektorom a ľahko programovateľné v Python knižnici. Podporované je na Windowse, Linuxe aj Macu, pri cene okolo 60 USD [18].

Freematics OBD-II

Je malý OBD II emulátor so 16 pinovým portom. Jeho výhodou je grafické rozhranie, ktorým môže byť ovládaný ak je pripojený pomocou USB alebo bezdrôtovo s iOS zariadeniami [19].

Arduino Shields

Zariadenia Arduino sú schopné podporovať konektivitu CAN pomocou Arduino shieldov, ktoré sú lacné a jednoduché na pridanie k Arduinu. Aby ich bolo možné použiť na prepojenie s CAN musia obsahovať MCP2515 jednotku. Jedine DFRobot shield využíva STM32 oplývajúci vyššou rýchlosťou a väčšou pamäťou [1].

Raspberry Pi

V porovnaní s Arduinom je výhodnejší z hľadiska použitia Linuxového nástroja SocketCAN bez potreby rozšírenia hardwaru, pretože poskytuje operačný systém Linux. Rovnako ako Arduino neobsahuje rozhranie pre CAN a je potrebné ho rozšíriť o shield [1].

ELM-USB

Je rozhranie medzi OBD II a USB, pričom je kompatibilné so zariadeniami ELM-323/327 výhodou je podpora všetkých protokoly. Ďalšou výhodou je kompatibilita s mnohými softwarovými nástrojmi ako sú OBDTester, pyOBD alebo všelijaké voľne dostupné verzie OBD II softwarov [20].

ELM327

Poskytuje viacero variantov prepojenia s OBD II, sú to Bluetooth, Wi-Fi, USB a sériový port. Kompatibilný je so všetkými automobilmi a môže byť používaný prostredníctvom prepojenia s Windowsom, Windows Phone, Androidom a aj iOS [21].

GoodThopter

GoofThopter je open source zariadenie s CAN rozhraním, založená na zariadení GoofFet, momentálne podporujúce len vysokorýchlostný CAN vysielač MCP2551 a samostatný CAN ovládač s rozhraním MCP2515 [22].

CAN232 a CANUSB

CAN 232 je malé modré rozhranie pripojiteľné do RS232 portu na PC a na druhej strane do CAN. Na spracovanie stačí obyčajný software ako aj na port 232. CANUSB je zase rozhranie medzi USB na PC a CAN zbernicou. Opäť nevyžaduje navyše ďalšie ovládače alebo software [23].

EVTV CANdue

Táto doska poskytuje USB konektor a 2 Mbit EEPROM a vysielač CAN, ktorý nebol umiestnený na Arduino Due, čo bol v podstate predchodca pre EVTV CANdue [24].

VSCOM Adapter

VSCOM Adapter umožňuje prepojenie PC a CAN zbernice prostredníctvom USB, ktorý používa protokol LAWICEL a tiež je pracuje s linuxovými can-utils [25].

CrossChasm C5

CrossChasm C5 rozhranie s CAN zbernicou poskytuje viacero verzií s komunikačnými rozhraniami ako Bluetooth, nízkoenergetický Bluetooth alebo celulárne siete, ale aj USB. Podporuje prekladač na konvertovanie CAN správy do formátu OpenXC [26].

CAN Bus Y-Splitter

CAN Bus Y-Splitter je obyčajné zariadenie alebo konektor DLC (Data Link Connector – linkový konektor) rozdelený na dva konektory, čo umožňuje pripojiť dve zariadenia naraz. Výhoda spočíva v tom, že môže byť pripojené ovládacie zariadenie a sniffer naraz [1].

HackRF

HackRF je zariadenie od spoločnosti Great Scott Gadgets. Tento open source hardwarový projekt môže prijímať a vysielať signály od 1 MHz do 6 GHz. Je to open source zariadenie a môže byť prepojené aj pomocou USB [27].

Macchina M2

Macchina sa skladá z dvoch hlavných častí: z dosky rozhrania a procesorovej dosky. Doska rozhrania umožňuje hardwaru komunikovať s automobilovými protokolmi. Obsahuje tiež dve vysokorýchlostné CAN rozhrania, jedno jednodrôtové rozhranie, LIN a staršie OBD

protokoly. Procesorová doska je hlavne Arduino Due s USB portom, slotom na pamäťovú kartu a pamäťou EEPROM. Modulárna architektúra umožňuje vylepšenia a rozšírenia. Obsahuje aj XBee kompatibilnú zásuvku na pridanie Bluetooth, Wi-Fi alebo celulárnych sietí [27].

ChipWhisperer Toolchain

ChipWhisperer ponúka mnoho zariadení na potreby výskumu bezpečnosti embedded zariadení. Je to open source software a hardware vhodný na vykonávanie útokov vedľajšími kanálmi [28].

2.2 Software

Rovnako ako u hardwarových nástrojov sú na trhu rôzne open source nástroje, ktoré sú dostupné pre každého a tiež drahšie nástroje, ktoré ponúkajú rozšírené možnosti.

Linuxové nástroje

Linux sám o sebe podporuje CAN ovládače a tiež je možné využiť podporovanú sadu can-utils na prácu s CAN, ktorá ponúka mnohé možnosti. Pracuje vo forme príkazového riadku a vďaka open source je jednoduché rozšíriť funkčnosť na iné nástroje [1].

Wireshark

Wireshark je známy a veľmi populárny nástroj na zachytávanie sieťovej komunikácie a v prípade využitia Linux a SocketCAN je možné ho použiť na prácu s CAN zbernicami. Na pomoc pri dekódovaní alebo triedení paketov zo zbernice nemá ďalšie funkcie, avšak, aj napriek tomu je užitočný [29].

Kayak

Kayak poskytuje grafické rozhranie založené na jazyku Java na diagnostiku a monitorovanie CAN. Je tiež založený na SocketCAN. Má niekoľko pokročilých funkcií, ako je sledovanie

GPS a možnosti záznamu a prehrávania. Kompatibilita je zaistená na Linux, MAC aj Windows systémoch [30].

O2OO

O2OO je open source software na dátové zaznamenávanie z OBD-II, ktorý pracuje s ELM327 na ukladanie údajov do SQLite databázy a následne ich dokáže zobrazovať vo forme grafov. Jeho výhodou je podpora čítania údajov GPS [31].

PyOBD

PyOBD - tiež známy ako PyOBD2 a PyOBD-II je diagnostický nástroj určený pre zatiadenia ELM327. Umožňuje komunikáciu s ECU, zobrazovanie chybových správ, zobrazovanie nameraných hodnôt atď. Celý je napísaný v Pythone [32].

SavvyCAN

SavvyCAN bol tiež navrhnutý spoločnosťou EVTV.me, aby bol schopný komunikovať s hardwarovými sniffermi, ako napríklad EVTV Due. SavvyCAN je open source, Qt nástroj založený na grafickom rozhraní, ktorý pracuje na viacerých operačných systémoch. Obsahuje niekoľko funkcií, ako sú zobrazenie zbernice CAN vo forme grafov, rozlíšenie súborov protokolov, nástroje na reverzné inžinierstvo a bežné funkcie na zachytávanie komunikácie na CAN [24].

Caring Caribou

Caring Caribou bol navrhnutý, aby spĺňal funkciu ako Nmap, ale pre prácu s automobilmi. Jeho výhodou je napr. schopnosť robiť diagnostické služby hrubou silou alebo funkcia CAN sniff-and-send [33].

UDSim

UDSim je simulátor s grafickým rozhraním, ktorý dokáže emulovať rôzne moduly vo vozidle. Má schopnosť učenia sa z komunikácie a je vhodný na bezpečnostné testy,

UDSim má tri režimy: učenie, simulácia a útok. V režime učenia identifikuje moduly, ktoré reagujú na diagnostické požiadavky UDS a monitoruje odpovede. V simulačnom režime simuluje vozidlo na zbernici CAN. V útočnom režime potom poskytuje rýchly fuzzing [33].

Octane

Octane slúži na odpočúvanie komunikácie a na injektovanie paketov do CAN, pričom poskytuje grafické rozhranie. Momentálne je podporovaný len v systéme Windows [34].

RomRaider

RomRaider je open source nástroj pre tuning vytvorený za účelom poskytnúť možnosť prehliadania, zaznamenávania a tuningovania riadiacich jednotiek Subaru. Obsahuje intuitívne grafické rozhranie a logovanie údajov, aby bolo ovládanie jednoduché pre každého [35].

Komodo

Komodo slúži hlavne na odpočúvanie komunikácie. Rozhranie je buď pre jednu alebo dve CAN zbernice. Na komunikáciu s nimi je k dispozícii Komodo GUI alebo Komodo API a prináša možnosť napísania svojho softwaru [36].

Vehicle Spy

Vehicle Spy je komerčný nástroj, čo sa prejavuje aj na cene, ktorý je špeciálne navrhnutý pre reverzné inžinierstvo protokolov CAN a ďalších komunikačných protokolov, na diagnostiku, ECU simuláciu, získavanie dát, automatizované testovanie a pod. Hlavnou myšlienkou pri zrode bola produktivita, čo znamená, že má byť ľahká na používanie. Podporuje siete ako sú Ethernet, CAN, LIN, MOST, FlexRay a K-Line [37].

Záver kapitoly

Trh ponúka veľké množstvo nástrojov v rôznych cenových rozpätiach, mnohé sú open source, čiže je možné si ich vylepšovať a upravovať a tiež vyvíjať si ku hardwaru vlastný

software. Cena odráža množstvo a pokročilosť funkcií. Veľa z predstavených nástrojov ponúka možnosti na zachytávanie komunikácie najmä na CAN zbernici ale aj bezdrôtovej komunikácie.

II. PRAKTICKÁ ČÁST

3 HROZBY IT INFRAŠTRUKTÚRY AUTOMOBILOV

Rýchlym vývojom technológií a inováciami v populárnych oblastiach ako cloud computing alebo IoT (Internet of Things – internet vecí) vznikli z áut prepojené zariadenia tzv. „connected cars“. Na jednej strane tieto technologické pokroky ponúkajú široké možnosti a príležitosti, no na druhej strane ponúkajú výzvy pre narušiteľov čo predstavuje hrozby. Preto je podstatné sa zaoberať pri vývoji aj kybernetickou bezpečnosťou, ktorá by mala byť súčasťou každej novej technológie [38].

3.1 Metódy modelovania hrozieb

Modelovanie hrozieb je spôsob určený na identifikovanie kybernetických hrozieb v rozsahu cieľov, motivácie a zraniteľností, ktorý obsahuje určitú štruktúru. Po identifikácii hrozieb na daný systém nasleduje zvolenie vhodných riešení a opatrení, ktoré zaistia v najlepšom prípade odstránenie (čo je málokedy možné), prevenciu alebo zmiernenie hrozieb [39].

Metód na modelovanie hrozieb je mnoho, avšak ich využitie sa líši. Preto si predstavíme niektoré z nich, uplatniteľné pri informačných systémoch, ku ktorým majú connected cars najbližšie:

- Cyber Kill Chain,
- DREAD,
- OCTAVE,
- PASTA,
- STRIDE,
- TARA,
- TRIKE.

3.1.1 Cyber Kill Chain

Cyber Kill Chain metóda predstavuje pohľad na kroky nepriateľa, ktoré musí podstúpiť, aby dosiahol svoj cieľ. U každého kroku sa snaží útočník určitým spôsobom dosiahnuť svoj cieľ a postúpiť k ďalšiemu kroku, pretože vynechaním alebo nezdarením sa jedného kroku nie je možné dostať sa ďalej. Práve toto je nevýhoda pre útočníka, ale naopak výhoda pre obrancu. Stačí prerušiť alebo znemožniť jeden krok a útok sa nepodarí.

Metóda identifikuje sedem krokov útočníka, ktorý musí zvládnuť všetky od prvého až po šiesty, aby sa dostal k finálnemu kroku.

Sedem krokov metódy Cyber Kill Chain:

- **Prieskum** – nepriateľ plánuje útok, prebieha výskum, identifikácia a výber cieľa, pričom pre obrancu je dôležitá detekcia a najlepšie prerušiť už tento krok.
- **Zbrojenie** – nepriateľ tvorí napríklad škodlivý kód, ktorý nevie obranca predpovedať.
- **Dodanie** – napr. škodlivý kód je dodaný cieľu rôznymi spôsobmi a pre obrancu predstavuje tento krok najvhodnejší čas ubrániť sa a prerušiť útok.
- **Exploitácia** – útočník sa snaží zneužiť zraniteľnosť v cieľovom systéme; obranca musí využívať bezpečnostné systémy a učiniť svoje systémy odolnejšie, aj keď pri nových exploitoch to môže byť náročné.
- **Inštalácia** – zvyčajne dochádza k inštalácii napr. backdooru na zaistenie zaistiť vzdialeného prístupu; obranca by mal detegovať a zaznamenávať inštalačnú aktivitu a následne analyzovať malware.
- **Ovládanie a riadenie** – útočník získa prístup na ovládanie cieľového systému pomocou predošlého malwaru; obranca musí zamedziť komunikácii útočníka s cieľovým systémom.
- **Akcie na dosiahnutie cieľov** – útočník ma prístup k cieľovému systému a môže ho ovládať ako by bol pri ňom; čím dlhšie má útočník tento prístup, tým väčší to môže mať dopad, preto je dôležité detegovať tento stav a prerušiť ho.

Táto metóda môže odborníkom na strane obrancu alebo obete poskytnúť vžitie sa do útočníka, a pochopiť jeho uvažovanie a následne sa vhodne postaviť k riešeniu zabezpečenia. Samozrejme. treba analyzovať predošlé útoky a všímať si podobné znaky útokov. Pri používaní tejto metódy má obranca až sedem možností zamedziť útoku a tiež sa dostať o krok pred potenciálneho nepriateľa [40].

3.1.2 DREAD

DREAD metóda je navrhnutá ako schéma pre klasifikáciu rizika predstavovaného každou hrozbou, pričom dochádza ku kvantifikovaniu, porovnávaniu a priorizovaniu daných hodnôt rizika. Skratka vznikla z počiatočných písmen kategórií, ktorých je päť.

DREAD kategórie sú:

- **Damage Potential** (potenciálne poškodenie) – definuje poškodenie, ktoré môže útok spôsobiť na systém.
- **Reproducibility** (rozmnožovanie) – stanovuje náročnosť rozmnožovania útoku. Ideálne je keď sa útok nemôže zopakovať.
- **Exploitability** (schopnosť exploitovania) – predstavuje náročnosť a potrebné znalosti potrebné na vykonania útoku.
- **Affected users** (ovplyvnení užívatelia) – predstavuje množstvo užívateľov, ktorí môžu byť ovplyvnení útokom.
- **Discoverability** (schopnosť objavenia) – stanovuje náročnosť objavenia hrozby, pričom sa väčšinou stanovuje najvyššia hodnota.

Táto metóda má stupnicu 1 až 10 pre každú kategóriu spomenutú vyššie. Po stanovení tohto čísla sa celkové riziko vypočíta podľa nasledujúceho vzorca:

DREAD riziko = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5

V tomto prípade platí čím vyššie číslo tým vyššie riziko [41].

Tab. 2. Hodnotenie DREAD metódy [1], upravil Kocian, 2018

Celkovo	**Stupeň rizika**
5 – 7	nízke
8 – 11	stredné
12 – 15	vysoké

Tab. 3. Systém hodnotenia metódy DREAD [1], upravil Kocian, 2018

	Hrozba		
Kategória	**Vysoká**	**Stredná**	**Nízka**
D	Môže narušiť bezpečnostný systém a získať plnú dôveru a nakoniec získať kontrolu nad prostredím	Môže vyniesť citlivé údaje	Môže vyniesť triviálne informácie
R	Je vždy rozmnožiteľná	Môže byť rozmnožená iba v určitých podmienkach	Veľmi náročné na rozmnoženie aj pri informáciách o zraniteľnosti
E	Umožňuje vykonať exploit aj nováčikovi	Umožňuje skúsenému útočníkovi vytvoriť útok, ktorý môže byť opakovaný	Umožňuje vykonanie útoku len veľmi skúsenému útočníkovi s hlbokými znalosťami
A	Zasiahne všetkých užívateľov, vrátane zákazníkov	Zasiahne len niektorých užívatešov	Zasiahne len veľmi malé množstvo užívateľov
D	Môže byť ľahko nájdená na verejne publikovanom útoku	Ovplyvní takmer nepoužívané časti (útočník musí byť veľmi kratívny, aby našiel škodlivé využitie)	Je nepravdepodobné, že útočník nájde spôsob na exploitáciu

3.1.3 OCTAVE Allegro

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation – vyhodnotenie kritických hrozieb, aktív a zraniteľností pre prevádzku) metóda bola navrhnutá za účelom poskytnutia rozsiahleho hodnotenia rizík v spoločnosti. Zameriava sa hlavne na informačné aktíva v spojení s ich používaním, skladovaním, prenosom, spracovaním a vo výsledku s ich vystavením hrozbám a zraniteľnostiam. Vypracovanie hodnotenia touto metódou je možné rôznymi spôsobmi ako napr. v štýle workshopu, spolupráce, s využitím pracovných listov a dotazníkov [42].

OCTAVE metóda je uskutočnená v ôsmich krokoch [42]:

- **1. krok: Stanovenie kritérií merania rizika** – organizačné mechanizmy, ktoré sa použijú na vyhodnotenie účinkov hrozieb na poslanie a obchodné ciele organizácie.
- **2. krok: Vytvorenie profilu informačných aktív** – profil je reprezentáciou informačného aktíva, ktorý opisuje jeho jedinečné vlastnosti, kvality, charakteristiky a hodnotu.

- **3. krok: Identifikácia kontajnerov pre informačné aktíva** – kontajnery opisujú miesta, kde sú informačné aktíva uložené, prepravované a spracované.
- **4. krok: Identifikácia oblastí znepokojenia** – začína proces identifikácie rizika brainstormingom o možných podmienkach alebo situáciách, ktoré môžu ohroziť informačné aktíva organizácie.
- **5. krok: Identifikácia scenárov hrozieb** – oblasti znepokojenia identifikované v predchádzajúcom kroku sa rozširujú do scenárov ohrozenia, ktoré podrobnejšie opisujú vlastnosti hrozby.
- **6. krok: Identifikácia rizík** – dôsledky pre organizáciu ak sa realizuje hrozba sú zachytené, čím sa dokončí obraz rizika.
- **7. krok: Analýza rizík** – je vypočítané jednoduché kvantitatívne meranie rozsahu, do akého je organizácia ovplyvnená hrozbou.
- **8. krok: Výber prístupu na zmiernenie hrozieb** – organizácie určujú, ktoré riziká vyžadujú zmierňovanie a vypracujú stratégiu na zmiernenie týchto rizík.

3.1.4 PASTA

PASTA (Process for Attack Simulation and Threat Analysis – proces na simuláciu útokov a analýzu hrozieb) je prístup zameraný na aktíva alebo riziká pre modelovanie hrozieb. Poskytuje dôležité informácie o stratégii znižovania rizika a bezpečnosti spoločnosti, čo zaručuje, že výsledky tejto metódy môžu byť použité nielen technickými pracovníkmi spoločnosti, ale aj managementom. Metóda PASTA sa vykonáva v siedmich fázach a každá fáza má inú úlohu, ktorú je potrebné vykonať, aby bolo možné prejsť do ďalšej fázy [43].

Tieto fázy sú [43]:

- Fáza 1: Stanovenie cieľov.
- Fáza 2: Definovanie technického rozsahu.
- Fáza 3: Rozklad aplikácie.
- Fáza 4: Analýza hrozieb.
- Fáza 5: Analýza slabostí a zraniteľností.
- Fáza 6: Modelovanie a simulácia útokov.
- Fáza 7: Analýza a management hrozieb.

3.1.5 STRIDE

STRIDE je metóda modelovania hrozieb vyvinutá spoločnosťou Microsoft. Je vo forme klasifikačnej schémy, kde sa podľa druhov exploitov charakterizujú hrozby [41].

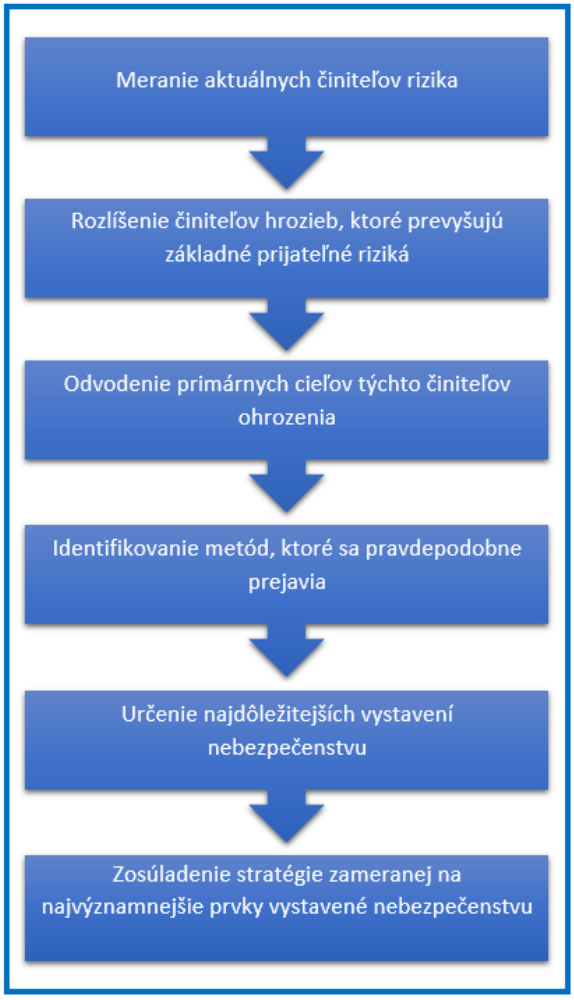
Názov STRIDE je skratka pre [41]:

- **Spoofing** – predstavuje predstieranie identity, teda vydávanie sa za niekoho iného. Predstavuje hrozbu najmä pre aplikácie, ktoré majú mnoho užívateľov.
- **Tampering** (narušenie) – predstavuje zámerné zmenenie obsahu paketov a tým potenciálne narušenie overovanie na strane klienta.
- **Repudiation** (odmietnutie) – predstavuje vyhlásenie, že akcia nebola vykonaná.
- **Information disclosure** (vyzradenie informácií) – znamená poskytnutie prístupu k informáciám, ku ktorým by v inom prípade nemal daný subjekt prístup.
- **Denial of service** (odmietnutie služby) – je bežný typ útoku, ktorý má za cieľ zahltiť systém falošnými požiadavkami do takej miery, že to nezvládne a tým pádom nebude schopný reagovať na normálne požiadavky.
- **Elevation of privileges** (zvýšenie privilégií) – predstavuje pozdvihnutie privilégií na úkony, na ktoré nie je bežne prístup.

3.1.6 TARA

Metóda TARA (Threat Agent Risk Assesment – hodnotenie rizík činiteľa ohrozenia) od Intelu z cenového hľadiska (nakoľko zaoberať sa každou zraniteľnosťou je drahé) priorizuje oblasti, ktoré vykazujú najviac kritické vystavenie hrozbám. Identifikuje činiteľov ohrozenia predstavujúcich najväčšie riziko, ciele, ktoré chcú dosiahnuť a pravdepodobné metódy využité pri dosahovaní cieľov. Hlavným cieľom tejto metódy je určiť najpravdepodobnejšie vektory útokov. Výhoda tejto metódy spočíva najmä určení najkritickejších vystavení hrozbám, čo ušetrí náklady pri ich zmierňovaní.

Nasledujúci obrázok znázorňuje šesť krokov procesu modelovania hrozieb za účelom nájdenia najkritickejších oblastí [44].



Obr. 10. Proces metódy TARA [44], upravil Kocian, 2018

Metóda TARA je založená na troch hlavných komponentoch (knižniciach), ktoré pomáhajú dosiahnuť stanovený cieľ [44].

- Threats Agent Library (TAL – knižnica činiteľov ohrozenia) – unikátna štandardizovaná knižnica, ktorá obsahuje typy činiteľov hrozby so spoločnými atribútmi.
- Common Exposure Library (CEL – knižnica vystavenia hrozbám) – obsahuje známe bezpečnostné zraniteľnosti.
- Methods and Objectives Library (MOL – knižnica metód a cieľov) – obsahuje zoznam známych cieľov činiteľov hrozieb spolu s najpravdepodobnejšou metódou, ktorá bude použitá na dosiahnutie týchto cieľov.

3.2 Modelovanie hrozieb automobilov

Po predstavení a priblížení si prístupov a metód na modelovanie hrozieb budú aplikované niektoré z nich pre prípad automobilov. Tieto metódy nie sú určené výhradne pre automobilový priemysel, preto je potrebné ich trochu upraviť, aby pasovali pre náš prípad.

3.2.1 TARA

Metóda TARA je založená na popisoch činiteľov hrozieb a ich príslušných atribútoch, ako sú motivácia, cieľ, zručnosti, zdroje, metódy útoku a spôsoby útoku. Metóda nie je časovo náročná a požadované poznatky a vstupné informácie sú prístupné, čo je jeden z dôvodov, prečo bola v tomto prípade vybraná pre modelovanie hrozieb. Je tiež veľmi prispôsobivá a môže sa uplatniť v rôznych priemyselných odvetviach, ako v zdravotníctve alebo v našom prípade pri connected cars.

Pri tejto metóde sa postupuje podľa šiestich krokov, ktoré poskytujú informácie na vytvorenie stratégie zameranej najvýznamnejšie prvky vystavené nebezpečenstvu.

- Meranie aktuálnych činiteľov ohrozenia
- Rozlíšenie činiteľov ohrozenia, ktorí prevyšujú základné prijateľné riziká
- Odvodenie primárnych cieľov týchto činiteľov ohrozenia
- Identifikovanie metód, ktoré sa pravdepodobne prejavia
- Určenie najdôležitejších vystavení nebezpečenstvu
- Zosúladenie stratégie zameranej na najvýznamnejšie prvky vystavené nebezpečenstvu

Prvý a druhý krok budú vykonané len do miery identifikovania činiteľov ohrozenia a teda nebude vykonané ich kvantitatívne hodnotenie, pretože pre nás je v tomto prípade najdôležitejšie určiť hrozby, čo odpovedá piatemu kroku.

3.2.2 TAL – Knižnica činiteľov ohrozenia

Pôvodná TAL knižnica od Intelu, neprispôsobená pre connected cars, stanovuje 21 činiteľov ohrozenia a ku každému 8 atribútov [45]. Avšak, ENISA predstavuje vo svojom reporte [46]

ďalšie činitele, ktoré sú relevantné pre náš prípad, preto bola o tieto, pôvodná tabuľka rozšírená. Intel vylepšil svoju metódu na modelovanie hrozieb a k ôsmim atribútom bol pridaný ďalší, konkrétne motivácia, o ktorého dôležitosti niet pochýb [47].

Činitele ohrozenia

Činiteľom ohrozenia je jednotlivec alebo skupina „útočníkov“, ktorí môžu vykonať „útok“. Môže to byť ľudský druh (úmyselný alebo neúmyselný) alebo prírodný druh (povodeň, požiar atď.). V tomto prípade sa samozrejme bude jednať o ľudský druh [48].

V našom prípade môžu činitele ohrozenia predstavovať [45][46]:

- **Anarchista*** – človek odmietajúci akúkoľvek štruktúru alebo autoritu a má málo zábran. Jeho konanie je zvyčajne vo forme násilia, ničenia majetku a pod.
- **Civilný aktivista*** – človek vysoko motivovaný, ale nenásilný, ktorý koná vždy kvôli nejakej príčine. Tento činiteľ ohrozenia by som spojil s hacktivistom, pretože sa v podstate jedná o to isté.
- **Hacktivista** – vysoko motivovaný, ale nenásilný človek, s príčinou svojho konania, ktorú považuje za správnu, väčšinou je príčina politická.
- **Informačný partner** – ide o osoby, s ktorými spoločnosť zdieľa citlivé informácie, ktoré sú spôsobené zlými mechanizmami ochrany súkromia vo vnútri spoločnosti.
- **Interný špión** – odborník v získavaní dát, ako interný pracovník s cieľom získať duševné vlastníctvo, osobné a obchodné údaje.
- **Iracionálny jednotlivec*** – niekto s nelogickým zámerom a iracionálnym správaním.
- **Konkurent** – konkuruje danej spoločnosti tým, že kradne duševné vlastníctvo alebo obchodné údaje.
- **Kybernetický terorista** – ľudia, ktorí používajú násilie na podporu osobných presvedčení a sociopolitických cieľov.
- **Kybernetický vandal** – získava potešenie z narušenia rôznych systémov a ničenia majetku, napr. únos webu, využitie malwaru atď.
- **Nedbalý zamestnanec** – súčasný zamestnanec, ktorý kvôli zvýšeniu efektívnosti práce obchádza niektoré bezpečnostné mechanizmy, ale nemá v úmysle poškodiť spoločnosť.

- **Nedostatočne vzdelaný zamestnanec** – súčasný zamestnanec, ktorý nevedomky zneužíva systém alebo ochranné mechanizmy spoločnosti.
- **Nespokojný zamestnanec** – súčasný alebo bývalý zamestnanec s dostatočnými znalosťami alebo prístupom k systémom spoločnosti.
- **Online sociálny hacker** – odborník v oblasti sociálneho inžinierstva, ktoré umožňuje analyzovať a chápať správanie a psychológiu sociálnych cieľov.
- **Organizovaný zločin** – vlastní významné zdroje a rôzne spôsoby na dosiahnutie svojich cieľov, napr. násilie alebo krádež údajov.
- **Právny protivník*** – oponent v súdnom konaní proti spoločnosti s cieľom narušenia spoločnosti alebo získania údajov.
- **Predajca –** obchodný partner, ktorý hľadá konkurenčnú výhodu za účelom zisku.
- **Radikálny aktivista** – vysoko motivovaný, koná kvôli nejakej príčine s cieľom narušenia alebo ničenia.
- **Script kiddies** – mladí ľudia s nízkou úrovňou zručností, ktorí používajú informácie dostupné na Internete na spustenie kybernetického útoku.
- **Senzáciechtivý** – osoba, ktorá si želá prilákať pozornosť verejnosti využitím akejkoľvek známej metódy, hľadá „15 minút slávy“.
- **Skorumpovaný vládny úradník** – človek, ktorý zneužíva svoje právomoci na získavanie zdrojov z danej spoločnosti.
- **Vládny kybernetický bojovník** – štátom sponzorovaný bojovník s dobrými zdrojmi na vykonanie narušenia štátnom meradle ktorý môže byť použitý na spôsobenie škody organizáciám, infraštruktúre či ľuďom prostredníctvom narušenia sietí, využitím malwaru a pod.
- **Vládny špión** – osoba financovaná vládou, ktorá má dôveru ako interný zamestnanec, väčšinou mu ide o krádež duševného vlastníctva a obchodných dát.
- **Zberač dát** – profesionálny zberač údajov, väčšinou kradne duševné vlastníctvo, osobné alebo obchodné údaje.
- **Zlodej** – osoba pracujúca s jednoduchým motívom zisku.

Činitele ohrozenia označené hviezdičkou (*) je možné považovať za malé až irelevantné hrozby pre prípad automobilov z hľadiska kybnernetickej bezpečnosti z dôvodu ich zamerania.

K predajcovi je vhodné doplniť **servisného technika**, na základe dôvery k nemu a tak môže zaobchádzať s vozidlom ako chce, môže nainštalovať malware, ukradnúť osobné údaje a pod.

Atribúty činiteľov ohrozenia

Metodológia TARA definuje rôzne atribúty, ktoré identifikujú špecifické charakteristiky každého činiteľa ohrozenia [45][47].

- **Úmysel** – definuje úmysel činiteľa ohrozenia, či má úmysel spôsobiť škodu alebo nie. Sú dve kategórie pre tento atribút: bez nepriateľského zámeru a s nepriateľským zámerom.
- **Prístup** - definuje prístup k cieľu, interný alebo externý.
- **Výsledok** – definuje cieľ, čo sa očakáva, že bude dosiahnuté . Možné výsledky sú: akvizícia/krádež, obchodná výhoda, ujma na reputácii a technická výhoda.
- **Obmedzenia** – predstavujú právne a etické limity, ktoré obmedzujú činiteľa ohrozenia pri dosahovaní svojho cieľa. Možnosti sú: etický kódex, právne, mimoprávne (menej významné), mimoprávne (veľmi významné).
- **Zdroje** – definujú v akom zložení pracuje činiteľ ohrozenia a z toho vyplývajú aj zdroje, ktoré má k dispozícii. Možnosti sú: individuálna osoba, klub, súťaž, tím, organizácia a vláda.
- **Zručnosti** – definujú úroveň zručností a skúseností. Možnosti sú: žiadna, minimálna, operatívna alebo zdatná.
- **Cieľ** – definuje kroky, ktoré podstúpi činiteľ ohrozenia, aby dosiahol zaumienený výsledok. Možnosti sú: kopírovanie, odmietnutie, poškodenie, zničenie, vzatie alebo všetko/„nedbám“.
- **Viditeľnosť** – definuje v akom rozsahu chce činiteľ ohrozenia odhaliť svoju identitu. Možnosti sú: otvorená, skrytá, tajná alebo „nedbám“.
- **Motivácia** - definuje motiváciu, ktorá stojí za činnosťou každého z činiteľov hrozieb. Možnosti sú: náhoda, donútenie, nespokojnosť, dominancia, ideológia, notoričnosť, firemný zisk, osobný finančný zisk, osobné uspokojenie a nepredvídateľná.

Pri napadnutí napr. bezpečnostných asistenčných systémov môže dôjsť k poškodeniu vozidla alebo dokonca aj zraneniu vodiča respektíve pasažierov, preto je vhodné pridať do výsledkov

okrem pôvodných možnosti aj ďalšie dve navyše: **materiálne škody** a **zranenie pasažierov**. K nim je vhodné pridať ešte ďalšiu možnosť a to **popularita**, pretože ako uvádza [28], napr. hacktivista vyžaduje svojím konaním určitú popularitu a pozornosť médií.

Pri návrhu tejto metódy pre informačné systémy sa nepočítalo so zranením ani pri cieľoch útočníka, čo je ale možné pri útoku na automobil. Preto je opäť vhodné pridať jednu možnosť, **zranenie**, aj do cieľov.

Tieto pridané možnosti sú v knižnici TAL označené symbolom „ + “.

Na základe zoznamu činiteľov ohrozenia a ich atribútov z predchádzajúcej časti bola zostavená nasledujúca knižnica TAL. Táto knižnica je vhodná pre určenie potencionálnych činiteľov ohrozenia pri vývoji, výrobe a prevádzke automobilov.

Tab. 4. Knižnica TAL pre automobily [45], upravil Kocian, 2018

TY ČINITEĽA ROZENIA	BEZ NEPRIATEĽSKÉHO ZÁMERU			NEPRIATEĽSKÝ ZÁMER																					
	Nedbalý zamest-nanec	Nevzde-laný za-mestna-nec	Infor-mačný partner	Anar-chista	Civilný aktivista	Hacktivista	Interný špión	Iracio-nálny jednotli-vec	Konku-rent	Kyber-netický terorista	Kyber-netický vandal	Nespo-kojný zamest-nanec	Online sociálny hacker	Organi-zovaný zločin	Právny protivník	Predajca / ser-visný technik	Radi-kálny aktivista	Script kiddies	Senzá-ciechtivý	Skorum-povaný vládny úradník	Vládny kyb. bo-jovník	Vládny špión	Zberač dát	Zlodej
Interný																									
Externý																									
Získanie/krádež																									
Business výhoda																									
Materiálne škody +																									
Zranenie pasažierov +																									
Újma na reputácii																									
Technická výhoda																									
Popularita +																									
Etický kódex																									
Právne																									
Mimo právne (menej)																									
Mimo právne (viac)																									
Individuálna osoba																									
Klub																									
Súťaž																									
Tím																									
Organizácia																									
Vláda																									
Žiadne																									
Minimálne																									
Prevádzkové																									
Odborné																									
Kopírovanie																									
Zamietnutie																									
Zranenie +																									
Zničenie																									
Poškodenie																									
Vzatie																									
všetko / „nedbám“																									
Otvorená																									
Skrytá																									
Tajná																									
„nedbám“																									
Náhodná																									
Donútenie																									
Nespokojnosť																									
Dominancia																									
Ideológia																									
Notoričnosť																									
Firemný zisk																									
Osobný finančný zisk																									
Osobné uspokojenie																									
Nepredvídateľná																									

3.2.3 MOL – Knižnica metód a cieľov

Knižnica metód a cieľov znázorňuje, ako to aj z názvu vyplýva, hlavne ciele a metódy, ktoré budú pravdepodobne použité na dosiahnutie týchto cieľov. Ďalej je zobrazená motivácia činiteľov ohrozenia a dopad ich konania na automobil [44].

Knižnica MOL určená pre informačné systémy [44] špecifikuje metódy a dopady, ktoré neodpovedajú moderným automobilom, preto bolo potrebné tieto atribúty patrične upraviť, aby odpovedali rovnako aj činiteľom ohrozenia. Podľa Institution of Engineering and Technology, ktorý uvádza motívy a ciele kybernetických hrozieb [49] a podľa FireEye, ktorý uvádza hrozby [50] boli upravené atribúty pre metódy a dopady nasledovne:

- **Metódy:**
  - ***Krádež osobných/obchodných údajov*** – sem spadajú rôzne údaje získané napr. z aplikácií v infotainmente, údaje o jazdách, údaje o polohe, údaje z vývoja, výroby atď.
  - ***Denial of Service*** – sem spadá najmä ransomware, pri ktorom dochádza k zašifrovaniu a do zaplatenia výkupného nie je možné použitie.
  - ***Ovplyvnenie ovládania auta*** – značí, že môže dôjsť napr. obmedzeniu alebo znemožneniu ovládania hlavných riadiacich častí vozidla alebo niektorých systémov.
  - ***Nepovolené vniknutie*** – využitím bezpečnostných nedostatkov napr. v diaľkovom zamykaní alebo v bezkľúčovom štartovaní.
  - ***Nepredvídateľná*** – u niektorých činiteľoch ohrozenia sa môžu objaviť metódy, ktoré je ťažké dopredu stanoviť.
- **Dopady**:
  - *Ujma na súkromí*
  - *Finančná strata*
  - *Krádež auta alebo jeho obsahu*
  - *poškodenie auta (áut), zranenie*
  - *Ujma na reputácii*

Tab. 5. Knižnica MOL [44][51], upravil Kocian, 2018

Činiteľ ohrozenia	**Útočník**					**Cieľ**		**Metóda**					**Dopad**				
	Prístup	*Dôvera*				*Motivácia*	*Cieľ*	Krádež osobných/obchodných údajov	Denial of Service	Ovplyvnenie ovládania auta	Nepovolené vniknutie	Nepredvídateľná	Ujma na súkromí	Finančná strata	Krádež auta alebo jeho obsahu	Poškodenie auta (áut), zranenie	Ujma na reputácii
		Žiadna	Čiastočná	Zamestnanec	Administrátor												
Anarchista	Externý	✓				Ideológia	Zničenie				✓			✓			✓
Civilný aktivista	Externý	✓				Ideológia	Zisk/krádež, poškodenie reputácie	✓			✓			✓			✓
Hacktivista	Externý	✓				Ideológia	Poškodenie reputácie	✓					✓				✓
Informačný partner	Interný		✓			Firemný zisk	Obchodná výhoda					✓	✓				✓
Interný špión	Interný		✓	✓	✓	Osobný finančný zisk	Zisk/krádež	✓					✓	✓			
Iracionálny jednotlivec	Externý	✓				Nepredvídateľná	„nedbám“					✓		✓			✓
Konkurent	Externý	✓				Firemný zisk	Technická výhoda	✓									✓
Kybernetický terorista	Externý	✓				Ideológia	Fyzická ujma, škoda			✓						✓	✓
Kybernetický vandal	Externý	✓				Dominancia	Osobné potešenie	✓	✓	✓			✓	✓	✓	✓	✓
Nedbalý zamestnanec	Interný		✓	✓	✓	Nehoda/chyba	Neškodný zámer					✓	✓				✓
Nespokojný zamestnanec	Interný		✓	✓	✓	Nespokojnosť	Poškodenie reputácie, škoda	✓		✓			✓	✓			
Nevzdelaný zamestnanec	Interný		✓	✓	✓	Nehoda/chyba	Neškodný zámer					✓	✓				✓
Online sociálny hacker	Externý	✓				Osobný finančný zisk	Zisk/krádež	✓						✓			
Organizovaný zločin	Externý	✓				Firemný zisk	Zisk/krádež	✓	✓	✓	✓		✓	✓	✓	✓	
Právny protivník	Externý		✓			Donútenie	Zisk/krádež	✓					✓	✓			✓
Predajca/servisný technik	Interný			✓	✓	Finančný zisk firemný aj osobný	Zisk/krádež	✓	✓				✓	✓			
Radikálny aktivista	Externý	✓				Ideológia	Materiálna škoda	✓	✓	✓			✓			✓	✓
Script kiddies	Externý	✓				Osobné uspokojenie	Popularita	✓	✓	✓			✓	✓			✓
Senzáciechtivý	Externý	✓				Notoričnosť	Popularita	✓					✓				✓
Skorumpovaný vládny úradník	Externý		✓			Osobný finančný zisk	Zamietnutie	✓						✓			
Vládny kyb. bojovník	Externý	✓				Dominancia	Fyzická ujma, škoda	✓	✓	✓						✓	
Vládny špión	Interný		✓	✓	✓	Ideológia	Technická výhoda	✓	✓	✓	✓			✓		✓	
Zberač dát	Externý	✓				Firemný zisk	Technická výhoda	✓					✓				✓
Zlodej	Externý/ interný	✓	✓	✓	✓	Osobný finančný zisk	Zisk/krádež				✓		✓		✓		

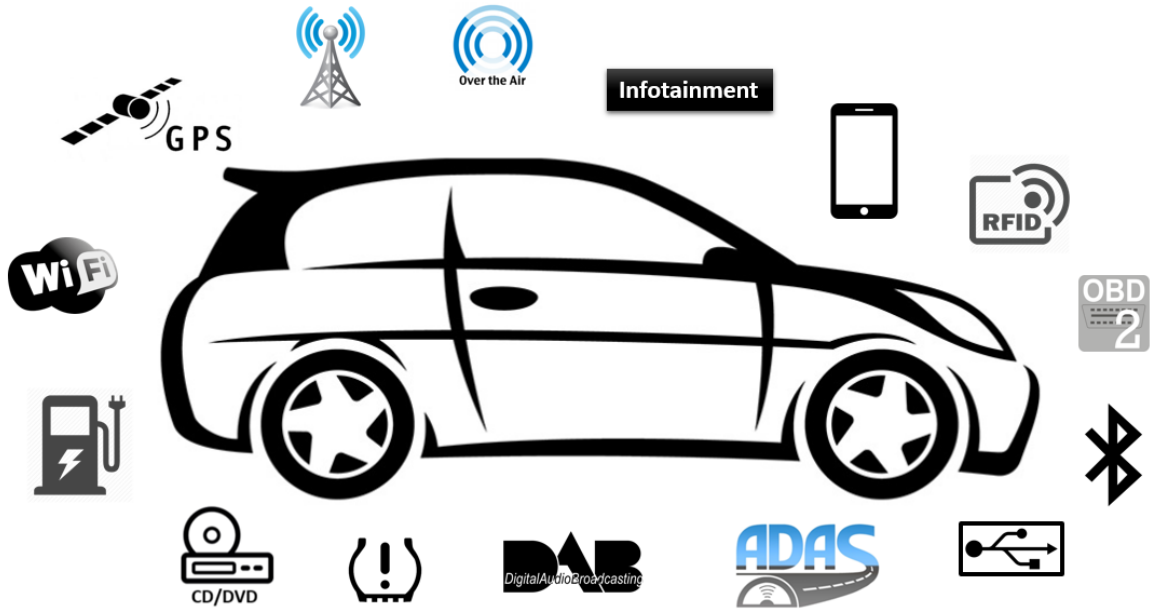
3.2.4 CEL – Knižnica vystavenia hrozbám

Knižnica CEL uvádza vo všeobecnosti bezpečnostné zraniteľnosti a vystavenia hrozbám IT systémov. V našom prípade sa bude jednať o spojenie s „connected cars“. Keďže táto knižnica obsahuje citlivé údaje žiadna spoločnosť ju verejne nezobrazí, a preto nie je známa ani jej štruktúra.

Na účely tejto práce boli zvolené nasledujúce atribúty, ktoré opisujú každú hrozbu uvedenú v knižnici:

- Prístup – stanovuje, či je prístup k danej technológii, systému alebo komponentu fyzický alebo bezdrôtový.
- Dopad – stanovuje aký dopad môže mať hrozba. Možností sú rovnaké ako v knižnici MOL okrem ujmy na reputácii.

Nasledujúci obrázok zobrazuje body, ktorými by mohli byť, boli alebo sú útoky na moderné automobily tzv. “connected cars“ vykonávané.



Obr. 11. Body útokov na automobily

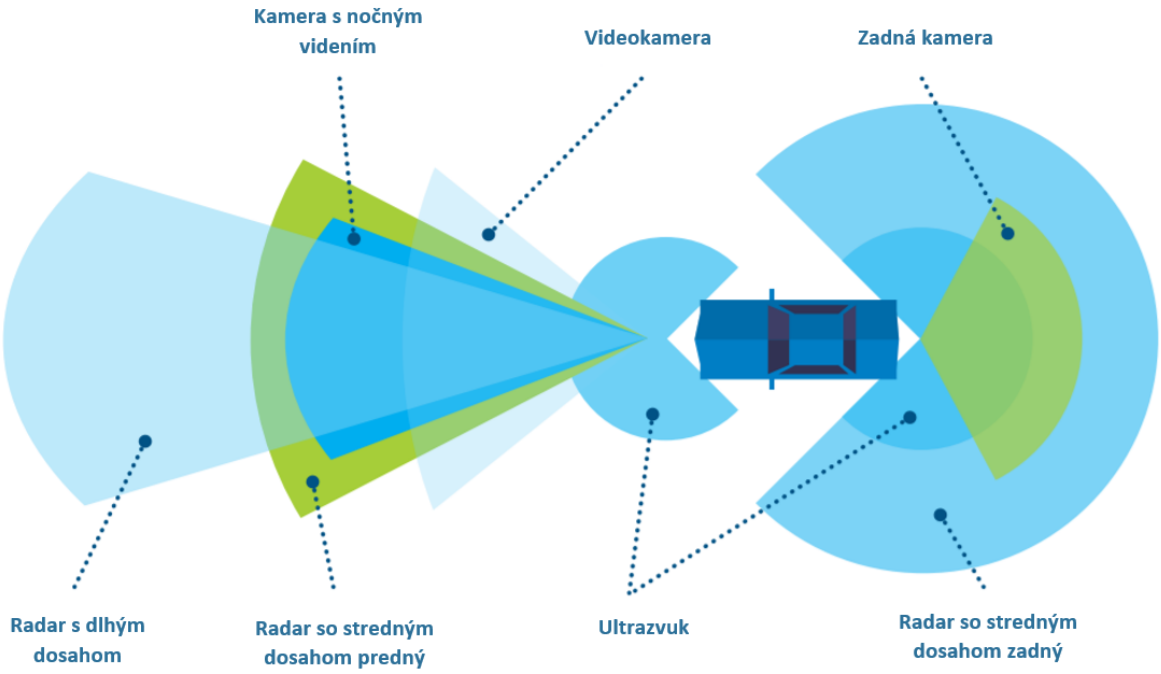
Podľa predchádzajúcich útokov a hrozieb (uvedených nižšie v tejto podkapitole) číhajúcich na automobily bola zostavená nasledujúca knižnica CEL.

Tab. 6. Knižnica CEL

Vystavenie hrozbe	**Prístup**		**Možný dopad**			
	Fyzický	*Bezdrôtový*	*Ujma na súkromí*	*Finančná strata*	*Krádež auta alebo jeho obsahu*	*Poškodenie auta (áut), zranenie*
ADAS	✓	✓				✓
Aplikácie na vzdialené pripojenie		✓	✓	✓	✓	✓
Bluetooth		✓	✓	✓		
CD/DVD prehrávač	✓			✓		
Celulárna sieť		✓	✓		✓	✓
GPS		✓	✓			
Infotainment		✓	✓	✓		
Nabíjací port pre elektrické vozidlá	✓		✓			
OBD II	✓			✓	✓	
PKES		✓			✓	
Rádio (DAB)		✓				✓
TPMS		✓	✓	✓		
Update vzduchom		✓		✓		
USB	✓			✓		
Wi-Fi		✓	✓			

ADAS

ADAS (Advanced Driver Assistance System – pokročilý asistenčný systém) sa používa v mnohých moderných automobiloch. Skladá sa z jednotlivých subsystémov ako sú adaptívny tempomat, asistent brzdenia, prevencia kolízie, vybočenia z jazdných pruhov a mnoho ďalších [52].



Obr. 12. Príklad ADAS senzorov [52], upravil Kocian, 2018

Útočníci majú rôzne možnosti, napríklad môžu generovať nepravdivé údaje na snímacej platforme, meniť dáta na internom komunikačnom kanáli, generovať nežiaduce výstupné ADAS dáta na riadiacej platforme, meniť výstupné dáta na internej komunikácii na ovládanie ECU, manipulovať s firmwarom a softwarom na výstupnej platforme čím by sa spôsobilo zlyhanie systému [52].

APLIKÁCIA NA VZDIALENÉ PRIPOJENIE

Moderné automobily ponúkajú možnosť ovládania niektorých funkcií diaľkovo prostredníctvom aplikácie v smartphone. Táto funkcia umožňuje vodičom odomknúť, lokalizovať vozidlo, zapnúť vykurovanie alebo dokonca spustiť motor auta. Veľmi praktická aplikácia má však svoju nevýhodu a to, že poskytuje dobré rozhranie na zneužitie útočníkom, čím môžu vzniknúť veľké škody [53][54][55].

BLUETOOTH

K útoku môže dôjsť z nespárovaného prenosného zariadenia alebo zo spárovaného (nepravdepodobné). Keď dochádza k synchronizácii prenosného zariadenia s vozidlom musí byť táto požiadavka spracovaná ECU. V niektorých vozidlách je signál bluetooth spracovaný

priamo rádiom. To znamená, že útočník môže spustiť kód na infotainmente, nahrať poškodené informácie ako napr. poškodený adresár, určený na vykonanie kódu a pod. [1][56].

CD/DVD PREHRÁVAČ

CD/DVD môže byť infikované škodlivým kódom, ktorý vykoná nejakú škodlivú akciu. Útočník by mohol použiť napr. sociálne médiá, aby si obete stiahli nejakú infikovanú skladbu. Po prehratí by mohlo dôjsť k prepísaniu pôvodného softwaru tým infikovaným. Ďalšia možnosť môže byť nahratie updatu poškodeným firmwarom [57].

Výskumníkom z Californskej a Washingtonskej univerzity sa podarilo pridať kód k digitálnemu hudobnému súboru, čím ho premenili na trójskeho koňa. Následne ho napálili na CD a tým môžu upraviť firmware v infotainmetne a získať k nemu prístup, prípadne aj k iným systémom vozidla [58].

CELULÁRNA SIEŤ

Moderná automobily sú vybavené portom na SIM kartu, čo umožňuje využívať pripojenie na Internet prostredníctvom celulárnych sietí. Túto komunikáciu je možné odpočúvať, zachytávať a upravovať prípadne penetračne testovať využívané protokoly. čím môže byť dokonca dosiahnutý prístup do vnútornej siete z akéhokoľvek miesta. Takto sa podarilo ovládať infotainmet, riadenie volantu a dokonca aj vypnúť motor na automobile značky Jeep Charliemu Millerovi a Chrisovi Valaskovi [1][59][60].

GPS

GPS (Global Positioning System – systém určovania polohy) je náchylný na spoofing útoky, čo umožňuje útočníkovi odkloniť vozidlo alebo urobiť takéto systémy nefunkčné. Z pohľadu ochrany osobných údajov hrozbu predstavuje získanie navštevovaných miest alebo domácej adresy. Študentom z univerzity v Texase sa podarilo takýmto spôsobom odkloniť loď, ktorá o tom ani nevedela [61].

INFOTAINMENT

U moderných automobiloch nie je možné, aby bol systém infotainment úplne oddelený od ostatných systémov, pretože by nebola možná jeho úplná funkcionalita. Väčšinou je prepojený so zbernicami priamo a akési oddelenie je len na úrovni softwaru vo forme mikropočítačového filtrovania, ktoré usmerňuje príkazy a komunikáciu. Avšak ako uvádza [56] toto predelenie je možné obísť prepísaním kontroléra, čo umožní prístup ku zbernici. Ďalší spôsob narušenia systému infotainmet je stiahnutie podvrhnutej infikovanej aplikácie [62].

NABÍJACÍ PORT PRE ELEKTRICKÉ VOZIDLÁ

Hlavnou hrozbou pre nabíjací port elektrického vozidla je použitie nabíjacích staníc. Tieto stanice sú zvyčajne pripojené k Internetu a majú prístup k osobným údajom vodiča pri pripojení auta k nabíjacej stanici. Boli vykonané scenáre útokov, ktorých výsledok bol krádež identity, finančné krádeže a útoky DoS (Denial of Service – odmietnutie služby) [63].

OBD II

Port OBD II vyžaduje fyzický prístup k vozidlu a ohrozuje bezpečnosť vozidla, pretože umožňuje priame pripojenie k zbernici CAN. Existujú špeciálne výkonné nástroje, ktoré eliminujú potrebu fyzického prístupu a môžu obsahovať zneužiteľné zraniteľnosti.

Vnútorné funkcie automobilu môžu upravené prostredníctvom určitého softwaru, ktorý je overovaný špeciálnymi kľúčmi. Tieto kľúče je možné získať reverzným inžinierstvom diagnostického softwaru alebo útokom hrubou silou [59][62].

PKES

Bežný útok zahŕňa zachytenie frekvencie a kódu odoslaného z kľúča od auta, ktorý sa zlodeji pokúsia použiť na vozidlo, aby ho odblokovali a mohli ho vykradnúť alebo ukradnúť [64].

RÁDIO DAB

U novších automobilov DAB (Digital Audio Broadcasting – vysielanie digitálneho zvuku) rádio neprijíma už iba zvukové signály, ale aj dátové signály, obrázky, text, čo umožňuje

posielanie a vykonávanie kódov. Bezpečnostnému výskumníkovi z NCC sa úspešne podarilo vykonať útok na automobil pomocou DAB rádia, kedy vytvoril falošnú stanicu a vyslal kód. ktorým bol schopný prevziať kontrolu nad brzdami [65][66].

TPMS

TPMS vysiela špecifické identifikačné číslo, ktoré môže byť použité na identifikáciu vozidla a ako také môže byť použité na sledovanie konkrétnych vozidiel. Komunikáciu je jednoduché odpočúvať a dokonca aj injektovať pakety, pretože nevyužíva žiadne šifrovanie a ECU nevyužíva žiadne overovanie. Výskumníkom sa podarilo z auta idúceho vedľa cieľového auta vysielať falošné správy o tlaku v pneumatikách a dokonca znefunkčniť ECU pre TPMS aktivovaním a deaktivovaním upozornenia o nízkom tlaku v pneumatikách [67].

UPDATE VZDUCHOM

Útočníci môžu reverzným inžinierstvom získať údaje (kľúče, príkazy a pod.) z firmwareu alebo môžu pozmeniť firmware, čo môže mať za následok zmenu funkcie niektorých systémov.

Napríklad Tesla používa metódu podpísania kódu. Znamená to, že všetky nové aktualizácie firmwaru Tesla, ktoré budú prenášané na diaľku budú obsahovať jedinečný kryptografický kľúč posilňujúci internú sieť vozidiel [59][62].

USB

Je ďalší spôsob na prenos škodlivého softwaru alebo upraveného updatu [1].

WI-FI

Veľa moderných automobilov obsahuje Wi-Fi, ktoré slúži ako hotspot pre mobilné telefóny a iné mobilné zariadenia. Tieto hotspoty zvyčajne prepájajú Internetové pripojenie vozidla s mobilným telefónom alebo slúžia ako vstupný bod pre multimédiá. Útočník môže jednoducho nastaviť falošný Wi-Fi prístupový bod, na ktorý sa pripojí automobil. Touto metódou dvaja čínski bezpečnostní výskumníci mohli manipulovať funkciami niektorých systémov

(brzdy, sedadlá, strešné okno) modelu Tesla S. Avšak Tesla rýchlo zareagovala a túto chybu odstránila [59].

Záver kapitoly

Na výber z metód na modelovanie hrozieb pri rôznych procesoch a odvetviach je mnoho, no konkrétne pre automobilový priemysel nie je vyhradená alebo prispôsobená žiadna metóda. Z toho dôvodu bola vybraná metóda TARA, ktorá sa zdala byť najvhodnejšia jej obsahom, spôsobom tvorenia a vyhodnotením.

Metóda TARA sa skladá z troch knižníc a každá má iný cieľ a tým pádom aj obsah. Prvá je knižnica činiteľov ohrozenia, kde sú predstavení potenciálni útočníci s rôznymi atribútmi ako sú ich motivácia, cieľ schopnosti a pod. Druhá je knižnica metód a cieľov, kde sú zobrazené ciele. metódy útočníkov predstavených v predchádzajúcej knižnici a dopady na daný systém. Posledná tretia knižnica vystavenia hrozbám zobrazuje konkrétne hrozby s dopadom na automobil.

4 ZRANITEĽNOSTI IT INFRAŠTRUKTÚRY AUTOMOBILOV

V predošlej kapitole boli predstavené hrozby pôsobiace na moderné automobily, ktoré môžu zneužiť zraniteľnosti v jednotlivých systémoch. Táto kapitola zas predstaví zraniteľnosti vybraných komponentov IT infraštruktúry, ak vôbec nejaké existujú. Zraniteľnosti sú pre výrobcov automobilov závažné skutočnosti, preto ich mnoho nie je zverejnených alebo sú postupom času opravené, čo je ten lepší prípad.

4.1 TOP 10 zraniteľnosti

Jedná sa o zraniteľnosti na softwarovej úrovni týkajúce sa infotainmentu a telematiky. Podľa spoločnosti Rogue Wave Software môžeme zhrnúť tieto zraniteľnosti do 10 skupín, ktoré sú zoradené zostupne podľa výskytu [68]:

- problémy s vyrovnávajúcou pamäťou,
- riadenie prístupu,
- expozícia informácií,
- nesprávna validácia vstupov,
- nesprávne riadenie prístupu,
- riadenie zdrojov,
- chyby v kóde,
- injekcia kódu,
- kryptografické nedostatky a
- numerické chyby.

4.1.1 Problémy s vyrovnávacou pamäťou

Jedna z najznámejších zraniteľností „buffer overflow“ alebo pretečenie vyrovnávacej pamäti vzniká, keď sa program snaží uložiť dáta do vyrovnávacej pamäti viac ako je schopná uniesť alebo keď sa snaží uložiť dáta mimo túto pamäť. Často to býva spôsobené napr. nekontrolovaním veľkosti vstupov, „pointerom“, ktorý ukazuje mimo rozsah tejto pamäte alebo je starý a ukazuje na pôvodné miesto, chyba umožňujúca písať mimo pamäť atď. Následky môžu byť padnutie systému, možnosť vykonania škodlivého kódu a pod. [69].

Ako príklad môžeme uviesť zraniteľnosť CVE-2017-9647, pri ktorej sa jedná o „stack buffer overflow“ (pretečenie na zásobníku), teda pretečenie na zásobníku volania. Táto zraniteľnosť sa vyskytuje na TCU (Telematics Control Unit – telematická riadiaca jednotka) od spoločnosti Continental. Ovplyvnené sú modely značiek BMW, Ford, Infiniti a Nissan Leaf. Útočník môže túto chybu využiť na neoprávnené vyzradenie informácií, vykonanie škodlivého kódu alebo znefunkčniť infotainment [70][71].

4.1.2 Riadenie prístupu

Jedná sa o spôsob udeľovania prístupu k danému obsahu niektorým subjektom a ostatným zase nie. Spadá sem akákoľvek zraniteľnosť, ktorá je spojená s riadením povolení, privilégií alebo iných bezpečnostných možností spojených s prístupom [72].

Ako príklad môžeme uviesť zraniteľnosť CVE-2017-14937, ktorá sa týka prístupu na CAN zbernicu v dôsledku nedostatočného zabezpečenia autentifikácie, kde nie je limit na pokusy a je možných len 256 kľúčových párov. Následok tejto zraniteľnosti môže byť detonácia airbagov a následne spôsobenie zranenia pasažierov [73].

Ďalším príkladom je zraniteľnosť CVE-2015-5611, týkajúca sa systému UConnect vo vozidlách Fiat, Chrysler, Jeep, Dodge a Ram. Táto chyba umožňovala útočníkom v rovnakej celulárnej sieti získať neoprávnený prístup k infotainmentu, ktorý je priamo prepojený so zbernicou CAN a tým pádom bolo možné získať prístup aj k riadeniu volantu a brzd. Po slávnom hacknutí Jeepu Cherokee Millerom a Valaskom došlo k odstráneniu tejto chyby [74].

4.1.3 Expozícia informácií

Pri tejto zraniteľnosti sa jedná o vyzradenie (poskytnutie neoprávneným osobám) citlivých informácií či už úmyselne alebo neúmyselne, prostredníctvom rôznych možností ako sú napr. obyčajne poslané údaje, chybové správy, debugové správy, údaje v pamäti cache atď. [68][75].

Ako príklad môžeme uviesť zraniteľnosť CVE-2017-9663, kde sú uložené citlivé údaje vo forme nešifrovaného textu. Útočník by touto chybou mohol získať šifrovací kľúč. Ovplyvnené sú OnStar systémy u General Motors [76].

4.1.4 Nesprávna validácia vstupov

Validácia vstupov je dôležitá, aby útočník nebol schopný použiť vstupy v neočakávanej forme pre daný systém čím môže dôjsť k ovplyvneniu chodu systému, svojvoľné nakladanie so zdrojmi alebo spustenie kódu a pod [77].

Ako príklad môžeme uviesť zraniteľnosť CVE-2017-9212, kde dochádza k pádu multimediálneho systému ak je spárované mobilné zariadenie pomocou bluetooth a v názve má %x alebo %c. Následok je teda pád systému [78].

4.1.5 Nesprávne riadenie prístupu

Dochádza k nesprávnemu obmedzovaniu prístupu neoprávnených osôb k určitým zdrojom alebo dokonca nie je vôbec využívanie obmedzovanie prístupu. Na dosiahnutie správneho riadenia prístupu by mali by byť využívané authentication, autorization a accounting (autentifikácia, autorizácia a účtovanie) [79].

Ako príklad môžeme uviesť zraniteľnosť CVE-2017-12695, kde je nesprávne riadenie prístupu na OnStar systéme vozidiel General Motors. Po úspešnom napadnutí tejto chyby je možné resetovať užívateľské heslo [80].

4.1.6 Riadenie zdrojov

Zraniteľnosti sú spojené s nesprávnym riadením vytvárania, používania, prenosu alebo ničenia systémových zdrojov [81].

4.1.7 Chyby v kóde

Sem spadajú zraniteľnosti, ktoré nie sú zahrnuté v ostatných kategóriách ako napr. problémy s generovaním kódu, žiadne alebo nesprávne spracovanie chýb, alebo času a pod. [68].

4.1.8 Injekcia kódu

V základe sa jedná o injektovanie kódu, ktorý je následné vykonaný daným systémom. Väčšinou tento problém spočíva v žiadnom alebo slabom overovaní vstupov a výstupov ako sú povolené znaky, formát a množstvo [82].

Ako príklad môžeme uviesť zraniteľnosť CVE-2018-1170, ktorá umožňuje útočníkovi injektovať správy do zbernice CAN prostredníctvom zraniteľnej aplikácii Customer-Link od Volkswagen-u a HTC Customer-Link Bridge. Táto chyba vyplýva z nedostatočného zabezpečenia updatu firmwaru [83].

4.1.9 Kryptografické nedostatky

Veľmi dôležitá časť pri bezpečnosti je nepochybne kryptografia, ktorá môže mať nedostatky napr. pri nezašifrovaní citlivých údajov, nedostatočne silných šifrách, problémoch s kľúčovým managementom a pod. [68].

4.1.10 Numerické chyby

Pri tejto zraniteľnosti sa jedná najmä o chyby vzniknuté pri konvertovaní číselnými typmi, počítaní čísel, integer overflow a pod. [68].

4.2 Aplikácie na vzdialený prístup

Mikhail Kuzin a Victor Chebyshev začiatkom roku 2017 otestovali sedem aplikácií (neuvádzajú ktoré) na vzdialený prístup, kde sa zamerali na potenciálne nebezpečné funkcie (napr. krádež vozidla), či je nejako zabránené reverznému inžinierstvu (napr. obfuskácia), či aplikácia kontroluje root povolenia, či kontroluje, že zobrazované rozhranie naozaj patrí danej aplikácii (ochrana pred phishingom) a nakoniec, či kontroluje integritu (ochrana pred pozmenením obsahu) [84].

Tab. 7. Výsledok testu aplikácií na vzdialený prístup [84]

Aplikácia	Funkcie	Obfuská-cia kódu	Nezašifrované prihlasovacie údaje	Ochrana proti pre-krytiu	Detekcia root povo-lení	Kontrola integrity
1.	Odomykanie dverí	Nie	Áno (login)	Nie	Nie	Nie
2.	Odomykanie dverí	Nie	Áno (login a heslo)	Nie	Nie	Nie
3.	Odomykanie dverí, štart motora	Nie	-	Nie	Nie	Nie
4.	Odomykanie dverí	Nie	Áno (login)	Nie	Nie	Nie
5.	Odomykanie dverí, štart motora	Nie	Áno (login)	Nie	Nie	Nie
6.	Odomykanie dverí, štart motora	Nie	Áno (login)	Nie	Nie	Nie
7.	Odomykanie dverí, štart motora	Nie	Áno (login a heslo)	Nie	Nie	Nie

Ako je možné vidieť z tabuľky uvedenej vyššie výsledky sú veľmi zlé, pretože nekontrolujú integritu, nedetegujú root povolenia, nemajú ochranu proti prekrytiu a taktiež nepoužívajú žiadny spôsob na ochranu proti reverznému inžinierstvu, teda obfuskáciu. Navyše prihlasovaciu údaje sú často nešifrované vo forme bežného textu. Z toho vyplýva, že pri napadnutí týchto aplikácií je možné získať prístup k vozidlu jeho odomknutím.

4.3 CAN

CAN zbernica je už dosť stará technológia, ktorá bola navrhnutá tak, aby spĺňala požiadavky na ľahkú váhu, čím ušetrila veľa miesta a robustnosť. Avšak, vtedy jej tvorcovia ani nepomýšľali na bezpečnosť a nejaké útoky, ktoré môžu prísť o desiatky rokov. To je dôvod prečo táto populárna zbernica obsahuje niekoľko zraniteľností [85].

4.3.1 Segmentácia

Z hľadiska bezpečnosti je segmentácia siete veľmi dôležitá a mal by sa na to brať ohľad už pri návrhu, pretože ak má nejaký komponent v tejto sieti zraniteľnosť a tá je zneužitá, útočník

sa môže jednoducho dostať aj k ostatným, napr. citlivým, komponentom. Pri ochrane segmentov je vhodné využívať proxy a firewally, aby sa útočníkovi zamedzil prístup do ostatných častí. Avšak, zbernica CAN nebola navrhnutá so segmentáciou. Pomocou nej sú prepojené mnohé ECU komunikujúce medzi sebou, čo znamená, že aj napr. riadiaca jednotka elektrických okien vie potenciálne komunikovať s riadiacou jednotkou bŕzd atď. Keby sa pri návrhu dbalo na bezpečnosť nebolo by možné, aby systémy napr. infotainmentu a komfortu mali prístup ku kritickým systémom [85].

4.3.2 Autentifikácia

Ako už bolo spomenuté CAN zbernica prepája riadiace jednotky s rôznymi funkciami a teda správy od niektorých jednotiek sú dostupné pre všetky ostatné riadiace jednotky. Ako príklad môžeme uviesť CAN správu nesúcu informácie o RPM, ktorá je dostupná pre všetky uzly bez ohľadu na to, či si ju vyžiadali. Ostatné uzly počúvajú na sieti a čakajú na špecifickú správu, ktorú rozoznajú podľa ID. Toto funguje bez problémov do doby kým sa nepripojí nejaké neautorizované zariadenie, ktoré môže vysielať škodlivé správy, pretože CAN neposkytuje bezpečnostné opatrenia tohto typu. Pre útočníka je dôležité pochopiť a naučiť sa ako funguje CAN protokol a musí byť schopný upravovať ID a dáta v rámcoch, aby mohol posielať podvrhnuté správy. Ovplyvnením správania jednotlivých ECU hrozia nielen nesprávne fungovanie ale závažné ujmy či už na majetku alebo na zdraví prípadne na životoch [85][86].

4.3.3 Šifrovanie

Keďže sa pri vývoji nedbalo na bezpečnosť, CAN zbernica preto nevyužíva pri komunikácii šifrovanie. Navyše by vtedy šifrovanie len spomaľovalo celý proces. Nešifrovaná komunikácia zapríčiňuje možnosť útočníkovi odpočúvať s pomerne lacným hardwarom a softwarom. Samozrejme bez šifrovania nie je možné zaistiť ani autenticitu a integritu a tak útočník môže bez väčších problémov vysielať správy aké chce [85][86].

Záver kapitoly

Moderná automobily sú pokročilé vo využívaných technológiách, no napriek tomu sa nekladie dostatočný dôraz na ich zabezpečenie. Predstavené boli top 10 zraniteľnosti, ktoré môžu byť spojené najmä infotainmentom a telematikou, ale nie je vylúčené ich zastúpenie aj pri iných komponentoch. Ku nim boli poskytnuté konkrétne zraniteľnosti z databázy. Najčastejšie sa vyskytujúce sú problémy s vyrovnávacou pamäťou (buffer overflow), riadenie prístupu a vyzradenie informácií.

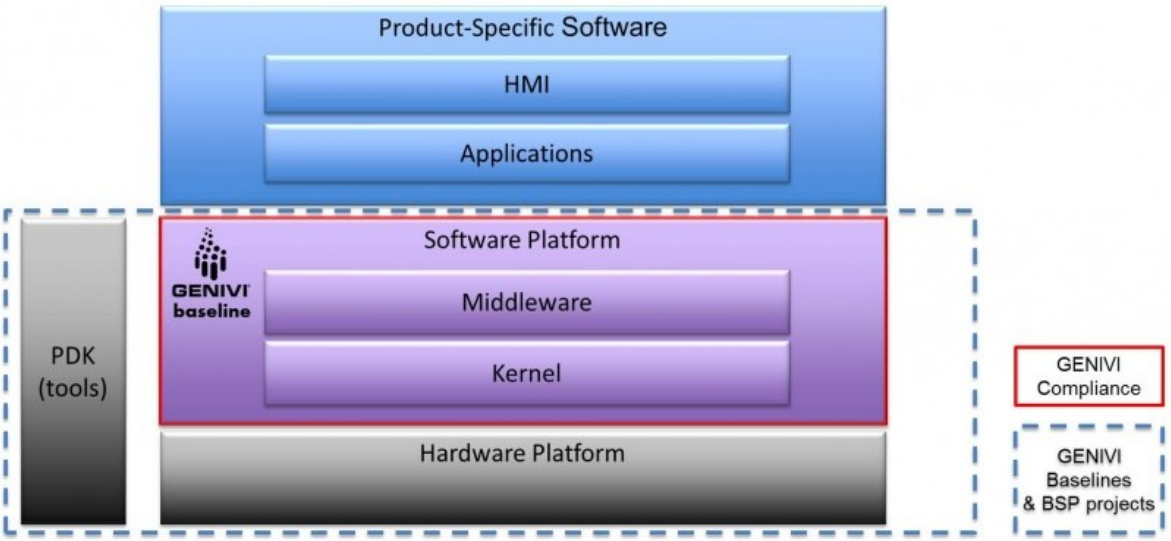
Dvojica výskumníkov otestovala vybrané aplikácie slúžiace na vzdialené ovládanie automobilu, ktoré boli testované na bezpečnostné mechanizmy. Dá sa zhodnotiť, že všetky zlyhali z hľadiska bezpečnosti, avšak po testovaní boli vývojári kontaktovaní, preto sa očakáva, že tieto problémy budú vyriešené aspoň čiastočne.

Nakoniec asi najdôležitejšia časť IT infraštruktúry automobilov CAN zbernica, ktorá bola vyvinutá veľmi dávno bez ohľadu na bezpečnosť obsahuje tiež tri podstatné zraniteľnosti, ktorými sú nedostatočná segmentácia, autentifikácia a šifrovanie, čo umožňuje útočníkovi odpočúvať komunikáciu na zbernici a následne aj posielať svoje (škodlivé) správy.

5 TEST PLATFORMY

V dnešnej dobre moderných automobilov je populárne využívanie open source infotainmentov umožňujúce spolupodieľanie sa na vývoji. Preto bol zámer využiť takúto možnosť a emulovať funkcie prostredníctvom počítača. Navyše dostať sa k infotainmentov konkrétnych výrobcov nie je jednoduché.

Zvolená bola platforma od GENIVI aliancie s názvom GENIVI meta-ivi. Postavená je na Yocto GENIVI Baseline, čo je spojenie GENIVI middlewaru a Linuxového jadra (kernelu) ako je možné vidieť aj na nasledujúcom obrázku [87].



Obr. 13. Zobrazenie Yocto GENIVI Baseline [87]

Medzi podporovaným hardwarom sú uvedené zariadenia, ktoré môžu byť emulované pomocou QEMU, čo je generický a open source nástroj na emuláciu a virtualizáciu [87][88].

Tieto zariadenia sú zobrazené v nasledujúcej tabuľke.

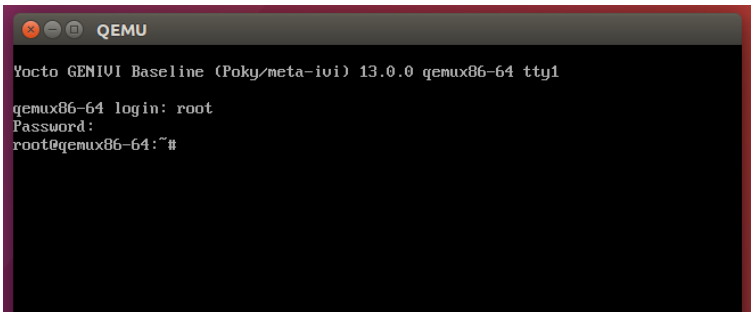
Tab. 8. Podporovaný hardware [89]

QEMU (ARMv7)	emulované zariadenie: vexpressa9
QEMU (IA-32)	emulované zariadenie: qemux86
QEMU (x86-64)	emulované zariadenie: qemux86-64
QEMU (ARM64)	emulované zariadenie: qemuarm64

Cieľom bolo emulovať zariadenie qemux86-64.

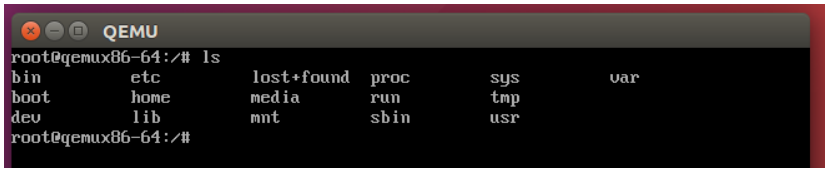
Na spustenie tejto platformy je potrebné vytvoriť „image“, čo bol dlhý a komplikovaný proces s mnohými problémami. Práve kvôli problém s vytváraním bolo potrebné použiť verziu meta-ivi/13.0.0 (najnovšia verzia je 14.0.0). Vytváranie „image-u“ prebiehalo v Ubuntu prostredníctvom virtualizačného nástroja VMware Workstation 14 Player.

Yocto GENIVI Baseline bohužiaľ neobsahuje grafické rozhranie a preto je ho v QEMU možné využiť len vo forme príkazového riadku ako je možné vidieť aj na nasledujúcom obrázku.



Obr. 14. Yocto GENIVI Baseline v QEMU

Avšak, pri pohľade na koreňový adresár vyzerá tento systém rovnako ako ostatné Linuxové systémy.



Obr. 15. Koreňový adresár v QEMU

Veľa možností teda tento systém neponúka, preto bolo skontrolované, či nebeží aspoň nejaká sieťová komunikácia a či tam nie sú otvorené porty. Po vykonaní príkazu „ip addr“ bola získaná adresa 192.168.7.2/24, ktorá bola otestovaná nástrojom „nmap“ na prítomnosť otvorených portov.

Nájdený bol len jeden otvorený port 3490/tcp, čo predstavuje Colubris Management Port, teda nič štandardné.

```
Nmap scan report for 192.168.7.2
Host is up (0.0027s latency).
PORT     STATE SERVICE
3490/tcp open  unknown
MAC Address: 52:54:00:12:34:02 (QEMU virtual NIC)
```

Obr. 16. Výsledok skenu na otvorené porty

Po zadaní tejto adresy spolu s portom do prehliadača sa zobrazilo niečo neidentifikovateľné.

Obr. 17. Výsledok vyhľadania danej adresy

Z predchádzajúceho postupu je možné konštatovať, že bohužiaľ testovanie bezpečnosti tejto platformy nebude možné prostredníctvom emulátora. Navyše open source platforma neobsahuje užívateľské rozhranie, pretože to je spôsob akým sa môžu výrobcovia áut odlišovať. Na vývoj, testovanie a rozširovanie tejto platformy je vhodné využívať niektoré hardwarové nástroje, ktoré stoja v stovkách USD [90].

Záver kapitoly

Táto kapitola mala obsahovať test platformy využívanej v automobilových infitainmentoch. Voľba padla na open source platformu z dôvodu dostupnosti, avšak ako sa ukázalo daná platforma obsahuje middleware a Linuxové jadro, ktoré nebolo možné otestovať z pohľadu bezpečnosti.

ZÁVER

Hlavným cieľom diplomovej práce bola identifikácia hrozieb z pohľadu činiteľov, ktorí predstavujú ohrozenie, ich motivácia, spôsob a metóda vykonania útoku a tiež komponenty využiteľné na vykonanie útoku. Ďalej identifikácia zraniteľností vyskytujúcich sa na vybraných komponentoch IT infraštruktúry a vykonanie testu platformy infotainmentu.

V teoretickej časti sú popísané základné funkcie a spôsoby fungovania komunikačných kanálov a komponentov IT infraštruktúry, medzi ktoré patria napr. zbernice prispôsobené na určené funkcie a síce CAN, LIN, MOST, Flexray a najmodernejšia technológia Ethernet. Líšia sa spôsobom využitia podľa kritickosti komunikácie na týchto zberniciach, od prenosu multimédií až po riadenie volantu alebo bŕzd po drôte. Ďalej sú predstavené riadiace jednotky rozdelené podľa ich funkcie a aj protokoly zaisťujúce komunikáciu. Komunikácia prebieha nielen po drôte ale aj bezdrôtovo. Najčastejšie využívané bezdrôtové technológie sú Bluetooth, WiFi a celulárna sieť. Okrem nich, samozrejme aj rádiová frekvencia zastupujúca systémy ako imobilizéry, bezkľúčové štartovanie alebo kontrola tlaku v pneumatikách. Bezpečnosť týchto systémov je možné otestovať pomocou rôznych hardwarových a softwarových nástrojov v rôznych cenových reláciách, čomu odpovedajú aj poskytované funkcie.

Praktická časť sa venuje identifikácii hrozieb, kde sú spočiatku predstavené činitele ohrozenia vplývajúce na automobily, v tomto prípade sú to osoby ako napr. externí hacktivisti, kybernetickí vandali alebo interní zamestnanci. Následne sú zobrazené motívy, ktoré ich ženú, metódy útokov a dopady na dané systémy. Tieto informácie sú doplnené o ohrozené komponenty IT infraštruktúry, ktoré by mali podstúpiť dostatočné zabezpečenie. Jeden z najviac rizikových komponentov môžeme považovať OBD-II konektor, pretože je priamo pripojený na CAN zbernicu, ktorá má prístup k väčšine systémov.

V ďalšej časti sú identifikované zraniteľnosti na infotainmente a na telemtrickej jednotke, ktoré sú zoradené do top 10 najviac vyskytujúcich sa. Sú veľmi podobné zraniteľnostiam nachádzajúcim sa na bežných IT systémoch. Najviac vyskytujúca sa zraniteľnosť je spojená s vyrovnávajúcou pamäťou, čo môže mať za následok padnutie systému alebo vykonanie škodlivého kódu. Podstatné sú aj aplikácie na vzdialený prístup, pretože poskytujú funkcie ako odomykanie auta na diaľku alebo naštartovania, čo predstavuje veľkú hrozbu pri zneužití. U aplikácií boli zistené veľké nedostatky, ktoré by mali byť čo najskôr odstránené. V neposlednom rade je dôležitá zbernica CAN, u ktorej sa vyskytujú zraniteľnosti ako nedostatočná respektíve žiadna autentifikácia, šifrovanie a segmentácia.

V závere mal byť vykonaný test platformy infotainmentu, avšak po dlhom vytváraní imagu a následnom spustení v emulátore sa preukázalo, že nie je možné dostatočné testovanie, pretože neobsahuje grafické rozhranie len middleware a jadro (kernel). Po získaní IP adresy bol vykonaný scan na otvorené porty, kde sa našiel jeden otvorený, avšak nie taký, ktorý by poskytoval nejakú štandardnú službu. Na vývoj a testovanie využívajú vývojári hardware, ktorý nie je ľahko dostupný a je dosť potrebný.

SEZNAM POUŽITÉ LITERATURY

[1] SMITH, Craig. *The car hacker's handbook: a guide for the penetration tester*. San Francisco: No Starch Press, 2016. ISBN 1-59327-703-2.

[2] NAVET, Nicolas a Françoise SIMONOT-LION. *In-vehicle communication networks - a historical perspective and review* [online]. 31. August 2013 [cit. 2018-04-04]. Dostupné z: http://nicolas.navet.eu/publi/trends2013.pdf

[3] Introduction to the Local Interconnect Network (LIN) Bus. *National Instruments* [online]. 24. 8. 2016 [cit. 2018-04-04]. Dostupné z: http://www.ni.com/white-paper/9733/en/

[4] POLÁK, Karel. Sběrnice CAN. *Elektrorevue: časopis pro elektrotechniku* [online]. 16. 6. 2003, **2003**(21) [cit. 2018-04-04]. ISSN 1213-1539. Dostupné z: http://www.elektrorevue.cz/clanky/03021/index.html

[5] CORRIGAN, Steve. *Introduction to the Controller Area Network (CAN)* [online]. Dallas: Texas Instruments, 2002, May 2016 [cit. 2018-04-04]. Dostupné z: http://www.ti.com/lit/an/sloa101b/sloa101b.pdf

[6] *In-Vehicle Networking: LIN/CAN/RF/FlexRay™ Technology* [online]. NXP Semiconductors [cit. 2018-04-04]. Dostupné z: https://www.nxp.com/docs/en/brochure/BRINVEHICLENET.pdf

[7] SCHMID, Markus. *Automotive Bus Systems* [online]. Atmel [cit. 2018-04-04]. Dostupné z: https://theeshadow.com/files/S40MY2005/pg29_32_autobussyste.pdf

[8] *CAN: Automotive Diagnostic Command Set User Manual* [online]. Austin: National Instruments, December 2009 [cit. 2018-04-05]. Dostupné z: http://www.ni.com/pdf/manuals/372139d.pdf

[9] OBD2 EXPLAINED: A SIMPLE INTRO. *CSS Electronics* [online]. Højbjerg, 2018 [cit. 2018-04-05]. Dostupné z: https://www.csselectronics.com/screen/page/simple-intro-obd2-explained

[10] ECU Designing and Testing using National Instruments Products. *National Instruments* [online]. 7. 11. 2009 [cit. 2018-04-05]. Dostupné z: https://web.archive.org/web/20131221083019/http://www.ni.com/white-paper/3312/en/

[11] AMIRTAHMASEBI, Kasra a Seyed JALALINIA. *Vehicular Networks – Security, Vulnerabilities and Countermeasures* [online]. Göteborg, 2010 [cit. 2018-04-05].

Dostupné z: http://publications.lib.chalmers.se/records/fulltext/123778.pdf. Master thesis. Chalmers University of Technology. Vedoucí práce Tomas Olovsson.

[12] SAJDL, Jan. ECU (Electronic Control Unit). *Autolexicon.net: ... s námi uvidíte pod kapotu* [online]. [cit. 2018-04-05]. Dostupné z: http://www.autolexicon.net/cs/articles/ecu-electronic-control-unit/

[13] KLAVMARK, Anders a Terje VIKINGSSON. *Study on Open Source In-Vehicle Infotainment (IVI) Software Platforms* [online]. Gothenburg, 2015 [cit. 2018-04-07]. Dostupné z: http://publications.lib.chalmers.se/records/fulltext/218477/218477.pdf. Master of Science thesis. Chalmers University of Technology. Vedoucí práce Per Larsson-Edefors.

[14] MARISETTY, Suresh, Durgesh SRIVASTAVA a Joel Andrew HOFFMANN. An Architecture for In-Vehicle Infotainment Systems. *Dr.Dobb's: The world of software development* [online]. 29. 1. 2010 [cit. 2018-04-07]. Dostupné z: http://www.drdobbs.com/embedded-systems/an-architecture-for-in-vehicle-infotainm/222600438?pgno=1

[15] NOLTE, Thomas, Hans HANSSON a Lucia Lo BELLO. *Wireless Automotive Communications* [online]. [cit. 2018-04-07]. Dostupné z: https://pdfs.semanticscholar.org/92e9/7a65fd2f8cb8e2e61f7543be7573ed8d50ae.pdf

[16] KENIA, Aadarsh, Sneha KADAM a Pooja PURUSHOTHAMAN. IN-VEHICLE INFOTAINMENT SYSTEMS. *International Journal of Advanced Computational Engineering and Networking* [online]. Vashi, Sep-2013, **1**(7), 27-32 [cit. 2018-04-07]. ISSN 2320-2106. Dostupné z: http://www.iraj.in/journal/journal_file/journal_pdf/3-24-139087682327-32.pdf

[17] FRANCILLON, Aurelien, Boris DANEV a Srdjan CAPKUN. *Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars*[online]. Zurich, 2010 [cit. 2018-04-07]. Dostupné z: https://eprint.iacr.org/2010/332.pdf

[18] EVENCHICK, Eric. CANtact: The Open Source Car Tool. *CANtact* [online]. [cit. 2018-04-22]. Dostupné z: http://linklayer.github.io/cantact/

[19] Freematics OBD-II Emulator MK2. *Freematics* [online]. c2014-2016 [cit. 2018-04-22]. Dostupné z: https://freematics.com/pages/products/freematics-obd-emulator-mk2/

[20] ELM-USB OBD2 Interface. *OBDTester* [online]. SECONS, c2007-2018 [cit. 2018-04-22]. Dostupné z: http://www.obdtester.com/elm-usb

[21] ELM327. *ELM327* [online]. c2018 [cit. 2018-04-22]. Dostupné z: http://elm-327.eu/

[22] GoodThopter12. *Sourceforge* [online]. [cit. 2018-04-22]. Dostupné z: http://good-fet.sourceforge.net/hardware/goodthopter12/

[23] CAN tools by LAWICEL AB. *Can232* [online]. Sweden: Lawicel, c1997-2017 [cit. 2018-04-22]. Dostupné z: https://www.can232.com/

[24] EVTVDue Microcontroller. *EVTV Motor Verks* [online]. c2018 [cit. 2018-04-22]. Dostupné z: http://store.evtv.me/proddetail.php?prod=EVTVDue2

[25] CAN Bus Adapters. *VScom* [online]. Vision Systems, c1993-2015 [cit. 2018-04-22]. Dostupné z: http://www.vscom.de/can-bus-adapters.htm

[26] CrossChasm C5 Interfaces. *Openxcplatform* [online]. Ford Motor Company, c2017 [cit. 2018-04-22]. Dostupné z: http://vi-firmware.openxcplatform.com/en/master/platforms/crosschasm-c5.html

[27] Car Hacking Tools. *Hacker Equipment* [online]. London, c2018 [cit. 2018-04-22]. Dostupné z: https://hacker.equipment/car-hacking-tools/

[28] ChipWhisperer®. *NewAE Technology* [online]. NewAE Technology, c2016 [cit. 2018-04-22]. Dostupné z: https://newae.com/tools/chipwhisperer/

[29] About Wireshark. *Wireshark* [online]. [cit. 2018-04-22]. Dostupné z: https://www.wireshark.org/

[30] MEIER, Jan-Niklas. Kayak. *Kayak* [online]. [cit. 2018-04-22]. Dostupné z: http://kayak.2codeornot2code.org/

[31] FERRIS, Ben. Resource: List of Car hacking tools, Car security tools and Car security resources. *Peerlyst* [online]. San Francisco, 31 Aug 2017 [cit. 2018-04-22]. Dostupné z: https://www.peerlyst.com/posts/resource-list-of-car-hacking-tools-car-security-tools-and-car-security-resources-ben-ferris

[32] PyOBD - Open-source OBD-II diagnostics. *OBDTester* [online]. SECONS, c2007-2018 [cit. 2018-04-22]. Dostupné z: http://www.obdtester.com/pyobd

[33] FALETRA, Lorenzo. Car-hacking-tools. *Github* [online]. 8 Oct 2016 [cit. 2018-04-22]. Dostupné z: https://github.com/ParrotSec/car-hacking-tools

[34] BORAZJANI, Parnian, Christopher EVERETT a Damon MCCOY. *OCTANE: An Extensible Open Source Car Security Testbed* [online]. [cit. 2018-04-22]. Dostupné z: https://pdfs.semanticscholar.org/f61e/4312185bb7aa7b0795db6533dc9d3c989300.pdf

[35] RomRaider. *Romraider* [online]. 2016 [cit. 2018-04-22]. Dostupné z: http://www.romraider.com/

[36] Komodo CAN Duo Interface Quick Start Guide. *TotalPhase* [online]. Total Phase, c2018 [cit. 2018-04-22]. Dostupné z: https://www.totalphase.com/support/articles/200801873-Komodo-CAN-Duo-Interface-Quick-Start-Guide

[37] Vehicle Spy Enterprise. *Interpid Control Systems* [online]. Intrepid Control Systems, c2005-2018 [cit. 2018-04-22]. Dostupné z: https://www.intrepidcs.com/products/software/vehicle-spy/

[38] CANADAM, Ramdev. Automotive Cyber Security: Threat, Guidelines, and challenges. *Stanford University* [online]. Stanford: Stanford University, July 28, 2017 [cit. 2018-05-03]. Dostupné z: https://mse238blog.stanford.edu/2017/07/ramdev10/automotive-cyber-security-threat-guidelines-and-challenges/

[39] MAGAR, Alan. *State-of-the-Art in Cyber Threat Models and Methodologies* [online]. Sphyrna Security, March 2016 [cit. 2018-05-06]. Dostupné z: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803699_A1b.pdf

[40] *Gaining The Advantage: APPLYING CYBER KILL CHAIN® METHODOLOGY TO NETWORK DEFENSE* [online]. Leidos, 07. 2016 [cit. 2018-05-03]. Dostupné z: https://cdn2.hubspot.net/hubfs/91979/gaining-the-advantage-cyber-kill-chain.pdf

[41] Threat Risk Modeling. *OWASP* [online]. 13 July 2017 [cit. 2018-05-05]. Dostupné z: https://www.owasp.org/index.php/Threat_Risk_Modeling#Identify_Threats

[42] CARALLI, Richard, James STEVENS a William WILSON. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* [online]. Pittsburgh: Carnegie Mellon University, May 2007 [cit. 2018-05-06]. Dostupné z: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[43] UCEDAVELEZ, Tony. *Real World Threat Modeling Using the PASTA Methodology* [online]. VerSprite, 2012 [cit. 2018-05-06]. Dostupné z: https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf

[44] ROSENQUIST, Matthew. *Prioritizing Information Security Risks with Threat Agent Risk Assessment* [online]. January 5, 2010 [cit. 2018-05-06]. Dostupné z: http://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf

[45] CASEY, Timothy. *Threat Agent Library Helps Identify Information Security Risks* [online]. Intel Corporation, September 2007 [cit. 2018-05-06]. Dostupné z: https://communities.intel.com/docs/DOC-23853

[46] *ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* [online]. EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Heraklion, JANUARY 2018 [cit. 2018-05-06]. DOI: 10.2824/967192. ISSN 2363-3050. ISBN 978-92-9204-250-9. Dostupné z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[47] CASEY, Timothy. *Understanding Cyberthreat Motivations to Improve Defense* [online]. Intel Corporation, 2015 [cit. 2018-05-06]. Dostupné z: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf

[48] Threat agent template. *OWASP* [online]. 20 June 2008 [cit. 2018-05-06]. Dostupné z: https://www.owasp.org/index.php/Threat_agent_template

[49] *Automotive Cyber Security: An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles* [online]. Institution of Engineering and Technology [cit. 2018-05-06]. Dostupné z: https://www.theiet.org/sectors/transport/topics/autonomous-vehicles/articles/auto-cs.cfm

[50] *CONNECTED CARS: THE OPEN ROAD FOR HACKERS* [online]. Milpitas, CA: FireEye, JUNE 2016 [cit. 2018-05-06]. Dostupné z: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/connected-cars-the-open-road-for-hackers.pdf

[51] PUSHPAKUMAR, Harikrishnan. *Understanding the threat landscape in e-government infrastructure for business enterprises*. Delft, 2015. Master of Science Thesis. Delft University of Technology. Vedoucí práce Dr. Ir. W. Pieters.

[52] ZHAO, Meiyuan. Advanced Driver Assistant System: Threats, Requirements, Security Solutions. *Intel Corporation* [online]. [cit. 2018-05-08]. Dostupné z: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/advanced-driver-assistant-system-paper.pdf

[53] GREENBERG, Andy. THIS GADGET HACKS GM CARS TO LOCATE, UNLOCK, AND START THEM. *Wired* [online]. 07.30.15 [cit. 2018-05-08]. Dostupné z: https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/

[54] LEYDEN, John. Grand App Auto: Tesla smartphone hack can track, locate, unlock, and start cars. *The Register* [online]. 25 Nov 2016 [cit. 2018-05-08]. Dostupné z: https://www.theregister.co.uk/2016/11/25/tesla_car_app_hack_enables_car_theft/

[55] CHARLTON, Alistair. BMW ConnectedDrive hack sees 2.2 million cars exposed to remote unlocking. *International Business Times* [online]. February 2, 2015 [cit. 2018-05-08]. Dostupné z: https://www.ibtimes.co.uk/bmw-connecteddrive-hack-sees-2-2-million-cars-exposed-remote-unlocking-1486215

[56] MILLER, Charlie a Chris VALASEK. *Remote Exploitation of an Unaltered Passenger Vehicle* [online]. August 10, 2015 [cit. 2018-05-06]. Dostupné z: http://illmatics.com/Remote%20Car%20Hacking.pdf

[57] YADAV, Aastha, Gaurav BOSE, Radhika BHANGE, Karan KAPOOR, N.Ch.S.N IYENGAR a Ronnie CAYTILES. Security, Vulnerability and Protection of Vehicular On-board Diagnostics. *International Journal of Security and Its Applications* [online]. 2016, 2016, **10**(4), 405-422 [cit. 2018-05-08]. DOI: http://dx.doi.org/10.14257/ijsia.2016.10.4.36. ISSN 1738-9976 IJSIA. Dostupné z: http://www.sersc.org/journals/IJSIA/vol10_no4_2016/36.pdf

[58] MCMILLAN, Robert. With hacking, music can take control of your car: emote-controlled car hacking is a real possibility, researchers say. *ITWorld* [online]. IDG Communications, MARCH 14, 2011 [cit. 2018-05-06]. Dostupné z: https://www.itworld.com/article/2748225/security/with-hacking--music-can-take-control-of-your-car.html

[59] HOW TO ENSURE AUTOMOTIVE CYBERSECURITY IN THE NEXT-GEN VEHICLES [PART 1]. *Infopulse* [online]. December 11, 2017 [cit. 2018-05-08].

Dostupné z: https://www.infopulse.com/blog/how-to-ensure-automotive-cyber-security-in-the-next-gen-vehicles-part-1/

[60] GREENBERG, Andy. THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE. *Wired* [online]. Wired, 08.01.16 [cit. 2018-05-06]. Dostupné z: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[61] SAARINEN, Juha. Students hijack luxury yacht with GPS spoofing: No alarms triggered. *ITNews* [online]. nextmedia, Jul 30 2013 [cit. 2018-05-06]. Dostupné z: https://www.itnews.com.au/news/students-hijack-luxury-yacht-with-gps-spoofing-351659

[62] JASEK, Sławomir. *CONNECTED CAR SECURITY THREAT ANALYSIS AND RECOMMENDATIONS* [online]. SecuRing, 2015-10-08 [cit. 2018-05-06]. Dostupné z: https://www.securing.pl/wp-content/uploads/2015/10/SecuRing-Connected-Car-Security-Threat-Analysis-and-Recommendations.pdf

[63] VAAS, Lisa. How to hack an electric car-charging station. *Naked security* [online]. 17 MAY 2013 [cit. 2018-05-09]. Dostupné z: https://nakedsecurity.sophos.com/2013/05/17/how-to-hack-an-electric-car-charging-station/

[64] SMITH, Luke. Is your car this easy to steal? Shock video reveals cars hacked and stolen in one minute. *Express* [online]. Nov 27, 2017 [cit. 2018-05-09]. Dostupné z: https://www.express.co.uk/life-style/cars/884792/car-stolen-keyless-entry-hack-Mercedes-Solihull-Birmingham-UK

[65] DAVIS, Andy. Broadcasting your attack: Security testing DAB radio in cars. *Black hat USA 2015* [online]. NCC group, 2015 [cit. 2018-05-08]. Dostupné z: https://www.nccgroup.trust/globalassets/resources/uk/presentations/2015/august/ncc-group-15-davis-broadcasting-your-attack-security-testing-dab-radio-in-cars.pdf

[66] VALLANCE, Chris. Car hack uses digital-radio broadcasts to seize control. *BBC News* [online]. BBC, 22 July 2015 [cit. 2018-05-06]. Dostupné z: http://www.bbc.com/news/technology-33622298

[67] ROUF, Ishtiaq, Rob MILLER, Hossen MUSTAFA, et al. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. *USENIX Security* [online]. California: USENIX Association Berkeley, 2010

[cit. 2018-05-06]. Dostupné z: http://www.winlab.rutgers.edu/~gruteser/papers/xu_tpms10.pdf

[68] *TOP AUTOMOTIVE SECURITY VULNERABILITIES OF 2015* [online]. Rogue Wave Software, 12/17/2015 [cit. 2018-05-21]. Dostupné z: https://www.rogue-wave.com/sites/rw/files/attachments/RW-Top-10-Automotive-WP-FNL-12-17-2015.pdf

[69] Buffer Overflow. *OWASP* [online]. 06/29/2016 [cit. 2018-05-]. Dostupné z: https://www.owasp.org/index.php/Buffer_Overflow

[70] CVE-2017-9647 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 08/07/2017 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2017-9647

[71] Advisory (ICSA-17-208-01): Continental AG Infineon S-Gold 2 (PMB 8876). *ICS-CERT: Industrial Control Systems Cyber Emergency Readiness Team* [online]. July 27, 2017 [cit. 2018-05-21]. Dostupné z: https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01

[72] Broken Access Control. *OWASP* [online]. 22 April 2010 [cit. 2018-05-21]. Dostupné z: https://www.owasp.org/index.php/Broken_Access_Control

[73] CVE-2017-14937 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 10/20/2017 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2017-14937

[74] CVE-2015-5611 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 07/21/2015 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2015-5611

[75] CWE-200: Information Exposure. *Common Weakness Enumeration* [online]. Bedford, MA: The MITRE Corporation, March 29, 2018 [cit. 2018-05-21]. Dostupné z: https://cwe.mitre.org/data/definitions/200.html

[76] CVE-2017-9663 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 01/09/2018 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2017-9663

[77] CWE-20: Improper Input Validation. *Common Weakness Enumeration* [online]. Bedford, MA: The MITRE Corporation, March 29, 2018 [cit. 2018-05-21]. Dostupné z: https://cwe.mitre.org/data/definitions/20.html

[78] CVE-2017-9212 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 05/23/2017 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2017-9212

[79] CWE-284: Improper Access Control. *Common Weakness Enumeration* [online]. Bedford, MA: The MITRE Corporation, March 29, 2018 [cit. 2018-05-21]. Dostupné z: https://cwe.mitre.org/data/definitions/284.html

[80] CVE-2017-12695 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 01/09/2018 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2017-12695

[81] CWE/SANS TOP 25 Most Dangerous Software Errors: Risky Resource Management. *SANS* [online]. June 27, 2011 [cit. 2018-05-21]. Dostupné z: https://www.sans.org/top25-software-errors

[82] Code Injection. *OWASP* [online]. 12/31/2013 [cit. 2018-05-21]. Dostupné z: https://www.owasp.org/index.php/Code_Injection

[83] CVE-2018-1170 Detail. *NIST: NATIONAL VULNERABILITY DATABASE* [online]. Gaithersburg, MD, 03/01/2018 [cit. 2018-05-21]. Dostupné z: https://nvd.nist.gov/vuln/detail/CVE-2018-1170

[84] KUZIN, Mikhail a Victor CHEBYSHEV. Mobile apps and stealing a connected car. *Securelist* [online]. AO Kaspersky Lab., February 16, 2017 [cit. 2018-05-21]. Dostupné z: https://securelist.com/mobile-apps-and-stealing-a-connected-car/77576/

[85] CURRIE, Roderick. *Developments in Car Hacking* [online]. SANS Institute, 2016 [cit. 2018-05-21]. Dostupné z: https://www.sans.org/reading-room/whitepapers/internet/developments-car-hacking-36607

[86] AVATEFIPOUR, Omid a Hafiz MALIK. State-of-the-Art Survey on In-Vehicle Network Communication (CAN-Bus) Security and Vulnerabilities. *International Journal of Computer Science and Network* [online]. 5 Feb 2018 [cit. 2018-05-21]. Dostupné z: https://arxiv.org/abs/1802.01725

[87] Meta-ivi: GENIVI Yocto Baseline. *GENIVI Projects* [online]. GENIVI, Apr 04, 2018 [cit. 2018-05-21]. Dostupné z: https://at.projects.genivi.org/wiki/display/PROJ/meta-ivi#meta-ivi-MetaiviBSPsforSpecificHardware

[88] QEMU: the FAST! processor emulator. *QEMU* [online]. [cit. 2018-05-21]. Dostupné z: https://www.qemu.org/

[89] Meta-ivi/13.0.0. *GENIVI Projects* [online]. GENIVI, Dec 12, 2017 [cit. 2018-05-21]. Dostupné z: https://at.projects.genivi.org/wiki/pages/viewpage.action?pageId=14976439

[90] Hardware Board Availability for Compliant Implementations. *GENIVI* [online]. GENIVI Alliance, c2018 [cit. 2018-05-21]. Dostupné z: https://www.genivi.org/hardware-boards

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ABS	Anti-lock Braking System – protiblokovací brzdový systém
ACK	Acknowledgment - potvrdenie
ADAS	Advanced Driver Assistance System – pokročilý asistenčný systém
AVB	Audio Video Bridge – audio video most
BCM	Body Control Module – riadiaci modul karosérie
CAN	Controller Area Network – sieť riadiacich systémov.
CEL	Common Exposure Library – knižnica vystavenia hrozbám
CRC	Cycling Redundancy Check – kontrola cyklickým kódom
DAB	Digital Audio Broadcasting – vysielanie digitálneho zvuku
DLC	Data Link Connector – linkový konektor
DoS	Denial of Service – odmietnutie služby
EBCM	Electronic Brake Control Module – elektronický riadiaci modul brzdy
ECM	Engine Control Module – riadiaci modul motora
ECU	Electronic Control Unit – elektronická riadiaca jednotka.
EOF	End of Frame – koniec rámca
EPROM	Erasable Programmable Read-Only Memory – mazateľná programovateľná pamäť len na čítanie
GPS	Global Positioning System – systém určovania polohy
HMI	Human Machine Interface – rozhranie medzi človekom a strojom
IDE	Identifier Extension – rozšírenie identifikátora
IEEE	Institute of Electrical and Electronics Engineers – Inštitút pre elektrické a elektronické inžinierstvo
IFS	Interframe Space – medzera medzi správami
IOT	Internet of Things – internet vecí
IP	Internet Protocol – Internetový protokol

ISO	International Standard Organization – Medzinárodná organizácia pre štandardizáciu
IVI	In-Vehicle Infotainment – infotainment vo vozidle
LIN	Local Interconnect Network – lokálna prepojovacia sieť
LTE	Long Term Evolution – dlhodobá evolúcia (4G)
MOL	Methods and Objectives Library – knižnica metód a cieľov
MOST	Media Oriented System Transport – prenos pre systémy zamerané na médiá
NFC	Near Field Communication – komunikácia v blízkom poli
OBD	On-Board Diagnostics – palubná diagnostika.
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation – vyhodnotenie kritických hrozieb, aktív a zraniteľností pre prevádzku
PAN	Personal Area Network – osobná sieť
PASTA	Process for Attack Simulation and Threat Analysis – proces na simuláciu útokov a analýzu hrozieb
PCM	Powertrain Control Module – riadiaci modul pohonnej jednotky
PKES	Passive Keyless Entry and Start – pasívny bezkľúčový vstup a štart
PWM	Pulse Width Modulation – impulzová šírková modulácia
RFID	Radio Frequency Identification – rádiofrekvenčná identifikácia
RPM	Revolutions Per Minute – otáčky za minútu.
QoS	Quality of Service – kvalita služby
RTR	Remote Transmission Request – žiadosť o vzdialený prenos
SOF	Start of Frame – začiatok rámca
TAL	Threats Agent Library – knižnica činiteľov ohrozenia
TARA	Threat Agent Risk Assesment - hodnotenie rizík činiteľa hrozby
TCP	Transmission Control Protocol – protokol riadenia prenosu
TCU	Telematics Control Unit – telematická riadiaca jednotka

TPMS	Tire Pressure Monitoring System – kontrola tlaku v pneumatikách
UDP	User Datagram Protokol – užívateľský datagramový protokol
UDS	Unified Diagnostic Services – zjednotené diagnostické služby
UHF	Ultra High Frequency – ultra vysoká frekvencia
UTP	Unshielded Twisted Pair – netienený krútený pár
VCM	Vehicle Control Module – modul riadenia vozidla
VoIP	Voice over Internet Protocol – hlas cez Internetový protokol)
VPW	Variable Pulse Width – variabilná šírka impulzu
V2I	Vehicle-to-Infrastructure – vozidlo s infraštruktúrou.
V2V	Vehicle-to-Vehicle – vozidlo s vozidlom
WLAN	Wireless Local Area Network – bezdrôtová lokálna sieť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK