TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Eliminace rizik a hrozeb spojených s připojením vozu k internetu

Bakalářská práce

Studijní program: B6209 – Systémové inženýrství a informatika
Studijní obor: 6209R021 – Manažerská informatika

Autor práce: **Radek Cihi**
Vedoucí práce: Ing. David Kubát, Ing.Paed.IGIP

Liberec 2017

TECHNICAL UNIVERSITY OF LIBEREC
Faculty of Economics

Elimination of risks and threats according to a car connected to the internet

Bachelor thesis

Study programme: B6209 – System Engineering and Informatics
Study branch: 6209R021 – Managerial Informatics

Author: **Radek Cihi**
Supervisor: Ing. David Kubát, Ing.Paed.IGIP

Liberec 2017

Tento list nahraďte
originálem zadání.

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Anotace

Cílem této bakalářské práce je analýza a vyhodnocení bezpečnostních rizik a návrh pravidel pro práci se službou Connected Car. První část práce definuje pojem Connected Car a současnou situaci v této oblasti. Další část srovnává bezpečnostní normy navržené pro Connected Car. Následuje analýza potenciálních rizik spojených s připojením vozidla k internetu. V další části následuje vyhodnocení a vytvoření pravidel pro bezpečné využití Connected Car. Na závěr se vyhodnocuje praktický přínos v oblasti Connected Car.

Klíčová slova

Vozidlo připojené k internetu, bezpečnost, zásady bezpečnosti, Connected Car

Annotation

Elimination of risks and threats associated to a car connected to the internet

The goal of this work is the analysis and evaluation of security risks and draft of rules for safety using a service in area of Connected Car. First part defines the Connected Car and the current situation in this area. Next part compares the safety standards designed for Connected Car. Following is analysis of the potential risks associated with vehicle connectivity to the internet. The next section is followed by an evaluation and development of rules for the safe use of Connected Car. Final chapter evaluates practical contribution of rules in the field of Connnected Car.

Key Words

Vehicle connected to the internet, security, principles of safety, Connected Car

Obsah

Seznam obrázků

Seznam zkratek

ALARP	As Low As Reasonably Practicable
CC	Connected car
ECU	Electronic Control Unit
EUC	Equipment Under Control
EVITA	E-Safety Vehicle Intrusion Protected Applications
FCA	Fiat Chrysler Automobiles
GSM	Global System for Mobile Communications
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IoT	Internet of Things
OBD II	On-board Diagnostics 2nd generation
OTA	OverTheAir
SAE	Society of Automotive Engineers
TPMS	Tire Pressure Monitoring System
ČSN	Česká technická norma

Úvod

Motorová vozidla jsou nedílnou součástí našeho každodenního života, ať už z pohledu člověka, který vozidlo řídí, či chodce, který se provozu účastní. Podoba vozidla, kterou je možno vidět v historických záznamech se liší ve většině případů.

Od 18. století, kdy vozidla vznikla, uběhla už tři staletí a vozidla jako taková prošla mnoha podobami. Od automobilů poháněných parním strojem, který dokázal jet rychlostí 9 km za hodinu, po dnešní sportovní vozidla, která dokážou jet více než třiceti násobkem rychlosti. Nezměnila se pouze rychlost aut, změnil se kompletní pohled na vozidla. V dnešní době je to každodenní prostředek na cesty. Prostředek, který je využíván pro cestu do práce, do školy, na výlet. V podstatě na veškerou činnost člověka spojenou s přemístěním z bodu A do bodu B. Služby samotného automobilu se od prostého přemísťování vyvinuly ke službám, které vás dokážou nejen přepravit více než 500km na jedno natankování, ale také přitom dokážou pojmout 4 další cestující, plný zavazadlový prostor, nastavit optimální teplotu, kterou si daní cestující přejí, ale také poskytují multimediální nabídku. To jsou třeba obrazovky na zadních sedadlech, nebo vytvoření Wi-Fi hotspotu pro mobilní internet či poslech své oblíbené písničky přes připojení bluetooth. Se službami, které využívají konektivitu v automobilech, také vzrůstá riziko zneužití třetí osobou. Toto zneužití může v lepších případech skončit jen rozladěným přehrávačem, v horším případě to může vyústit ve ztrátu kontroly nad řízením vozidla, následnou nehodu a dokonce možné škody na lidských životech.

Cílem této bakalářské práce je zpracování řešení a postupu, jak Connected Car používat, a také, jak tyto služby navrhovat. Dále analýza současné situace, srovnání stávajících platných norem a následné vytvoření analýzy Connected Car z pohledu bezpečnosti. Po analýze bude následovat vytvoření pravidel pro bezpečné využití Connected Car a vyhodnocení praktického přínosu těchto pravidel v dané oblasti.

1 Současná situace v oblasti Connected Car

V následujících podkapitolách se práce bude zabývat historií Connected Car, spojitosti s IoT, současnou situací Connected Car řešení a jaké služby pod službou Connected Car vystupují. Také se kapitola bude zaobírat koncepcí na uživatelské a technologické úrovni, dále bezpečnostním pohledem na řešení a také bezpečností rizika, která z tohoto trendu plynou.

1.1 Spojitost s IoT

V dnešní době už je internet takřka „všude a ve všem“. Tento trend se nazývá Internet of Things, neboli v překladu Internet věcí. V dnešní době je to rozrůstající se technologický trend a především je to nová technologická revoluce, ve které jsou věci jako domácí spotřebiče, čidla, kamery, apod. připojeny k internetu. Podle výzkumu společnosti Ericsson by v roce 2021 mělo být připojeno přibližně 28 bilionů zařízení.[1] V dnešní době je to přibližně 15 bilionů. Z tohoto trendu plyne mnoho příležitostí, které dokážou usnadnit různý počet činností. Nicméně, jak se již ukázalo, plyne z tohoto trendu také mnoho rizik. Jedním z nich je ovládnutí zařízení, které je zrovna připojené. Člověk nemusí být vyloženě IT specialista, aby se mu to povedlo, neboť právě funkcionalita umožňující být neustále „online“ mnohdy znamená, že uživatel daného zařízení ho nemá zabezpečené a nechává tak volnou cestu ke snadnému proniknutí do zařízení. Příkladem toho byl 21. říjen minulého roku, kdy neznámí útočníci pronikli do více než 100.000 zařízení a využili je jako nástroj, který dokázal znemožnit tisícům uživatelům US použití některých služeb, které hostují na území US. Byly to služby jako např. Amazon, Spotify, HBO a Paypal.[2]

1.2 Co je to Connected Car

Slovní spojení Connected Car se skládá ze dvou anglických slov, je to slovo connected, které v překladu znamená připojený a slovo car, které v překladu znamená automobil. Toto slovní spojení znamená připojený automobil a v dnešní době to je připojení k internetu. O automobilu můžeme říci, že je „online“. Být „online“ v automobilu znamená, že neustále komunikuje s internetem a nabízí služby s tím spojené.

Prvním automobilem, který by se dal označit za „Connected Car“, byl vůz vyrobený v roce 1996 společností General Motors. Společnost se svými vozy Cadillac chtěla udělat vozidla „bezpečnější“. V jejich případě to bylo vozidlo připojené k datové síti a funkce spočívala v tom, že po aktivaci airbagu bylo pomocí datové sítě vytočeno automaticky servisní středisko a přivolána pomoc, byla to funkce připomínající dnešní tísňové volání neboli funkci e-Call, která by od roku 2018 měla být ve všech nově vyrobených automobilech, podle nařízení Evropské unie.[3]

Nynějšímu pojmu Connected Car se to ve většině technických směrů vzdaluje, avšak princip zůstal stejný, vozidlo a připojení. V dnešní době se funkcionalita Connected Car stala trendem a každá automobilka chce mít svůj způsob řešení. Otázkou zůstává, jestli to spíše není nutností kvůli konkurenční nevýhodě. Naše doba plná konektivity, kdy některé věci vyřídíte raději na smartphonu při cestě do práce než doma na osobním počítači, si to doslova žádá a absence služeb, které Connected Car nabízí, by pro některé potenciální zákazníky mohla být rozhodujícím faktorem při koupi vozu.

Od roku 1996 uplynulo 20 let a Connected Car se v mnoha věcech změnil. Od prostého zavolání na tísňovou linku při vybuchnutí airbagu k funkcionalitě e-Call, díky které vozidlo obsahuje „černou skříňku“ s údaji GPS, data o aktivaci airbagů a data ze senzorů, kterou následně odešle na tísňovou linku. Od standardizované diagnostiky k službě, která automaticky informuje v případě poruchy vozidla předem vybraného dealera, který poté kontaktuje vlastníka a naplánuje s ním servis, nebo například k webovému portálu pro správu automobilu z domova ze svého počítače nebo z mobilní aplikace. Funkcionalit je nespočetné množství, nicméně poptávkou konektivity a být stále „online“, také nastává fakt, že čím více

je vozidlo připojené, tím více je nebezpečné a méně odolné vůči vnějším vlivům a potenciálním rizikům. [4]

1.3 Jaké služby Connected Car obsahuje

Služby, které pod pojmem Connected Car vystupují, se „liší“ dle konkrétního výrobce. Rozdíl mezi těmito službami není tak markantní a většina služeb, které automobilky nabízejí, jsou ve směs stejné, ale jinak pojmenované. Prémiové automobilky poté mají extra funkce navíc, nicméně základní výbava je stejná a většinou se neliší. Služby, které Connected Car řešení nabízí, můžeme obecně rozlišit na tři skupiny:

1.3.1 Služby multimediálního systému uvnitř vozidla

Služby multimediálního systému uvnitř vozidla mají spíše informační charakter a jsou většinou spojené s infotainmentem v automobilu. Mezi tyto služby patří:

- Aplikace třetích stran
- Vlastní a obecné body zájmu
- Online dopravní informace
- Zobrazení benzínových stanic
- Novinky
- Parkovací místa
- Online plánovač tras
- Počasí

V multimediálním systému existuje několik aplikací od známých vývojářů. Například streamovací služba Spotify pro poslech hudby, či aplikace Google Earth pro 3D zobrazení map. [5][6][7]

1.3.2 Služby vzdáleného přístupu

Služby vzdáleného přístupu má většina automobilek vyřešeno jako webový portál. Webový portál, který je provázán účtem zákazníka a jeho vozidlem na základě VIN čísla. Tyto služby jsou:

- Řidičská data
- Upozornění polohy
- Parkovací místa
- Připomenutí vozidla
- Status vozidla
- Rychlostní upozornění
- Online ochrana proti krádeži

V těchto portálech jde o základní nastavení a správu vozidla, také se zde nastavují aplikace, které jsou portal-based, což znamená, že hlavní nastavení aplikace je v portálu. Je to například aplikace upozornění polohy. Tato aplikace se nastavuje v portálu, kde se nastavuje plocha, ze které by vozidlo nemělo vyjet. Tato plocha se uloží a kontroluje vozidlo, jestli se nachází v dané poloze. Jestliže vozidlo vyjede z předem vyznačené plochy, portál upozorní uživatele. Kvůli bezpečnosti se samozřejmě nejedná o kontrolu nad vozidlem, nýbrž jen o informativní účel. [5][6][7]

1.3.3 Služby proaktivní bezpečnosti

Termín proaktivní znamená přístup, který probíhá v pozadí, nicméně je neustále připraven k použití. Z hlediska služeb to může znamenat funkci, která běží neustále na pozadí a je vždy připravena. V rámci Connected Car to jsou funkce bezpečnostního charakteru. Patří mezi ně:

- Automatická notifikace při nehodě (e-Call)
- Informativní hovor
- Přivolání servisu
- Zpráva celkového stavu vozidla
- Plánování servisu vozidla

Například funkce plánování servisu vozidla přesně vystihuje termín proaktivní bezpečnost v Connected Car. Každodenním používáním vozidla dochází k opotřebovávání různých dílů. Souvislost s touto službou je taková, že když zákazníkovi dojde motorový olej, servis kontaktuje zákazníka a domluví si s ním servisní opravu v pokud možno co nejvhodnějším předstihu. Celá služba je koncipována tak, aby se především předcházelo rozsáhlejším opravám nebo nutnému objednávání náhradních dílů, a tím spojené čekací době. Je to založeno na užším vztahu klienta se servisem a co nejpřívětivějším user-experience. [5][6][7]

1.4 Konektivita Connected Car z uživatelského pohledu

Služba Connected Car je složitý technologický business proces. Na jedné straně stojí zákazník, který si žádá funkčnost a bezpečnost za co nejmenší cenu, a na druhé straně stojí vozidlo (resp. výrobce), který nabízí služby a ze služeb očekává zisk, v případě automobilky i zisk z prodeje automobilu. Ziskem ze služeb, které nabízí, zároveň přebírá odpovědnost za vše co je s jejím řešením spojené, jestliže je systém navržen špatně a vznikne pro zákazníka riziko, někdo za toto riziko musí nést odpovědnost.

Obrázek 1 - Connected car v Infotainment ŠKODA
Zdroj: ŠKODA(2016, http://www.auto-mania.cz/wp-content/uploads/2016/11/skoda-kodiaq-infotainment-1024x682.jpg)

Automobilky nejsou jedinými výrobci těchto služeb. Konkurence pro automobilky jsou externí firmy, které navrhují také řešení Connected Car. Díky těmto výrobcům se řešení dá rozdělit na řešení pomocí OBD II portu nebo defaultně uvnitř vozidla od výrobce automobilů. OBD II připojení je standardizovaný konektor, který obsahuje každé vozidlo od roku 2001a slouží pro připojení diagnostické jednotky. [7]

Externí firmy nabízejí služby, které po zakoupení a připojení OBD II jednotky slouží jako náhrada Connected Car od automobilek, nicméně funkcionalita OBD II je značně omezená a každý výrobce automobilů zpřístupňuje pomocí řídící jednotky jiný počet informací, které jdou do OBD II konektoru. A tudíž je i pro firmy, které navrhují tyto aplikace, obtížné zajistit

kompatibilitu pro všechny automobily a tudíž i některé funkce jsou omezené. Rozdíl mezi řešením od automobilek a řešením od externích firem je patrný. Řešení od externích firem je omezeno pouze na OBD II konektor a informace z toho rozhraní, zatímco řešení přímo od automobilek nabízí provázanost se systémy vozidla (např. s infotainmentem) a dokáže tak zajistit zajímavý uživatelský zážitek oproti odvolání se pouze na aplikaci ve smartphonu či portálu na domácím počítači. Tímto propojením získává automobilka náskok oproti externím výrobcům a dokáže tak disponovat velkou výhodou v konkurenčním boji, jelikož pro zákazníka je mnohem jednodušší si zvolit řešení od automobilky, už při konfiguraci svého nového vozu a nechat si vše předem nakonfigurovat automobilkou a poté jen služby využívat. Externí výrobce Connected Car služeb je proto v nevýhodné pozici a musí zaujmout svými službami. OBD II řešení musí obsahovat slot na SIM kartu a GPS čip, aby se dal považovat za Connected Car. Řešení OBD II je spíše vhodnější pro starší automobily, které Connected Car defaultně nepodporují, tímto řešením se dají „vylepšit“ vozidla staršího ročníku a částečně tím využít potenciál Connected Car. [7] [8]

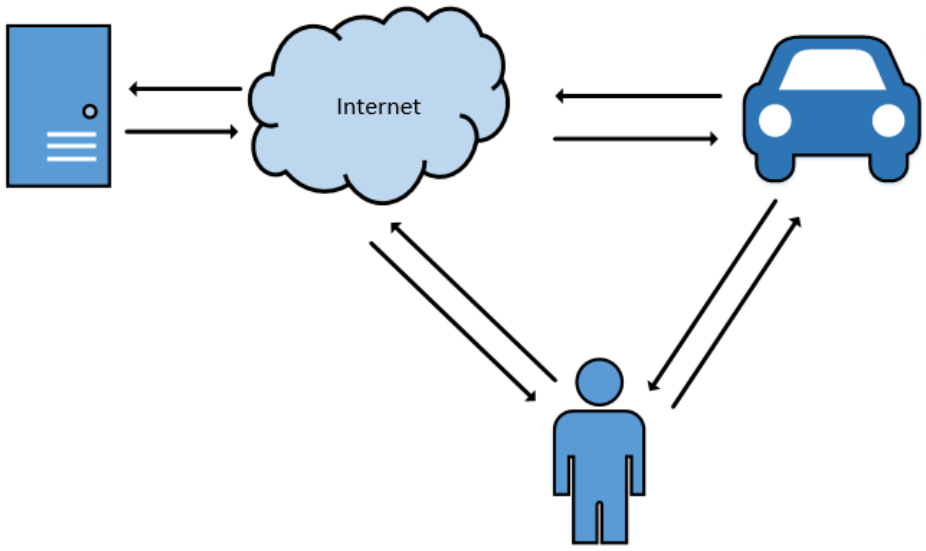
Obrázek 2 - OBD II řešení Connected Car
Zdroj: Aickar (2017, http://www.aickar-accessories.com/?product=neelam-tk206-vehicle-car-tracker-for-gsmgprsgps-system-obd-ii-device-real-time-tracking-with-sim-card-slot-anti-lostblack)

1.5 Konektivita Connected Car z technologického pohledu

Z technologického pohledu řešení Connected Car je koncept o 4 objektech a velkém množství datových toků. Viz Obrázek 3, trojúhelník komunikace tvoří tři objekty. Je to člověk, který chce využít služby Connected Car, dále je to samotné vozidlo a posledním objektem je internet.

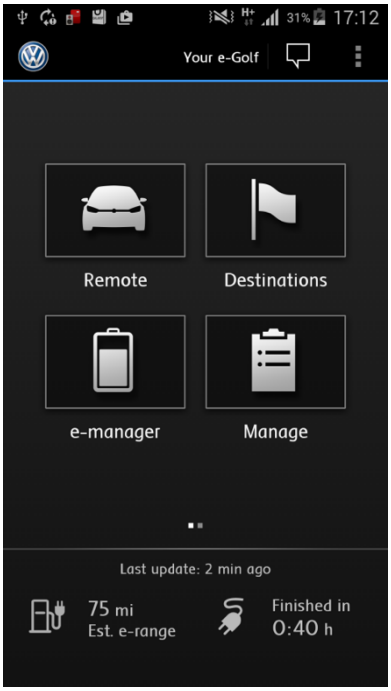
Internet v tomto schématu hraje několik klíčových rolí. Jednak je prostředníkem mezi vozidlem a zákazníkem, když se zákazník chce připojovat pomocí webového portálu či aplikace. Dále je to prostředník mezi zákazníkem v autě a tzv. back-end službou.

Pojmem back-end služba se rozumí zprostředkovatel služeb Connected Car mezi zákazníkem, internetem a vozidlem. V praxi to znamená na jedné straně uživatele, který se chce dotazovat na své služby použitím infotainmentu, a na druhé straně vozidlo obsahující infotainment a dotazuje se v navigaci na své vlastní body zájmu, které si předem vložil pomocí portálu. Uživatel vybere aplikaci navigace a vyvolá možnost vlastní body zájmu v aplikaci navigace, tímto zahájí výměnu informací mezi navigací v autě a back-end službou, v níž jsou uložena potřebná data pro aplikaci navigace.



Obrázek 3 - Komunikace mezi uživatelem, vozidlem a zprostředkovatelem
Zdroj: Vlastní

Dalším aktérem tohoto schématu je samotný zákazník, který má několik možností, jak se připojovat k autu a využívat služeb Connected Car. První možností je samotný fyzický kontakt s vozidlem. Další možností může být přistupování k službám, které se spravují pomocí vzdáleného rozhraní. Rozhraním může být například aplikace ve smartphonu či v prohlížeči jako webová stránka. Služba, spravována aplikací ve smartphonu, může být aplikace, kdy zákazník chce najít své vozidlo. Službou spravovanou pomocí webového portálu může být např. online plánování trasy.[7][9] [10]



Obrázek 4 - Connected car aplikace ve smartphonu od VW
Zdroj: VW (2016, https://play.google.com/store/apps/details?id=com.verizontelematics.vwcarnet)

1.6 Příklad automobilek, které nabízejí vlastní řešení:

Jak již bylo řečeno, Connected Car je výzva, které se chce každá automobilka nebo externí firma zhostit. V následujících odstavcích se objeví řešení od některých automobilek a řešení od externích výrobců. V práci je zmíněno pouze několik automobilek, nicméně automobilky svou snahou o integraci služeb Connected Car odvádějí velmi dobrou práci a tak už je řešení Connected Car na trhu několik.

1.6.1 VW Car-Net

Connected Car řešení od VW má název Car-Net. Toto řešení je nabízené ve formě ročního předplatného a služby jsou situovány do 4 sekcí.

První sekcí je App-Connect, které nabízí propojení smartphonu a automobilu pomocí technologie MirrorLink, AndroidAuto a Apple Carplay. Jedná se o technologie, které umožňují propojit Smartphone s Infotainmentem v autě způsobem, který umožní přístup některých aplikací z telefonu do vozidla. Může to být například navigace Google Maps, která je dostupná na všechna mobilní zařízení, a to pomocí technologie AndroidAuto. Výsledek tohoto propojení je na obrázku č. 5.

Obrázek 5 - Android Auto a aplikace Google Maps
Zdroj: Mashable (2015, http://mashable.com/2015/05/26/android-auto-hyundai-sonata/#lh4FX2LDYiq1)

Další sekcí je Guide & Inform obsahující funkce podle zakoupeného infotainmentu. První možností je infotainment PAKET BASIC a druhou je PAKET PLUS. Tyto nabízené soubory obsahují běžné služby Connected Car (např. Dopravní informace online, Parkovací místa, apod.).

Balík PAKET PLUS je obohacen jen o použití Google StreetView, Google Earth, hlasové vyhledávání zvláštních cílů a online aktualizace mapových podkladů).

Security & Service je sekce zabývající se zabezpečením a bezpečností vozidla. Mezi funkce této sekce patří (např. e-Call, Zpráva o stavu vozidla, Online alarm apod.)[10]

Obrázek 6- Connected car v infotainmentu VW
Zdroj: VW (2015, http://www.vwalhambra.com/my2016-infotainment.htm)

1.6.2 ŠKODA Connect

Automobilka ŠKODA má stejně jako VW rozlišení do sekcí. Ze vzájemné podobnosti služeb a rozvržení je možné konstatovat, že se jedná o dosti podobné řešení. Ze 4 sekcí z VW řešení je ŠKODA Connect rozděleno do 3. Jsou to sekce Infotainment Online, Care Connect a Emergency Call. První sekcí je Infotainment Online, který obsahuje informativní služby. Sekce Care Connect je služba zaměřená na vzdálený přístup k autu a proaktivní bezpečí. Mezi služby, které jsou obsaženy v tomto balíku, patří např. pozice

vozidla, jízdní data, rychlostní notifikace, plánovaný servis. Poslední je sekce Emergency Call, která je věnována funkci e-Call. Kompletní služba ŠKODA Connect je řešena pomocí ročního předplatného, stejně jako u VW Car-Net.[7]

Obrázek 7-ŠKODA Connect v infotainmentu Škoda Auto
Zdroj: ŠKODA (2016, http://www.skoda-auto.cz/chci-vuz-skoda/skoda-connect/skoda-connect/)

1.6.3 Tesla Motors

Za zajímavým projektem Connected Car stojí automobilka na plně elektrické vozy Tesla Motors. Svým chováním a postojem ke Connected Car řešení je svým způsobem jediná. Její všechny automobily nabízejí řešení Connected Car a přitom si na tomto trendu automobilka nestaví svůj marketing. Tesla Motors řešení je také bezplatné a v některých případech přitom nabízí oproti jiným automobilkám jedinečné funkce.

Tesla Motors nabízí jako jediná automobilka, tzv. OTA aktualizace, jsou to aktualizace „Over the Air“, což znamená, že vozidlo má možnost aktualizace softwaru bez nutnosti navštívení servisu. Automobilka „vyšle“ novou aktualizaci a je jen na uživateli, jestli si danou aktualizaci nainstaluje či nikoliv. Zákazníkům se tato možnost už v mnoha případech vyplatila. Příkladem může být např. kompletní redesign uživatelského prostředí v aktualizaci

verze 8.0 nebo například přidání funkce Autopilot, kdy vozidlo spolu s přítomností řidiče dokáže řídit víceméně samostatně.[11]

1.7 Příklad externích výrobců Connected Car služeb:

Jak už bylo zmíněno, ti, kteří nabízejí služby Connected Car a nejsou přímí výrobci automobilů, jsou odkázání na port OBD II, který je standardem ve všech autech.

On-board diagnostics, ve zkratce OBD II, je standard, který je definovaný několika normami. Je to port, který se nachází většinou ve spodní části interiéru v prostoru pod volantem a tím, že je definovaný normami, vzniká příležitost pro zapojení externího konektoru pro zařízení. Norma, která nařizuje povinnost OBD II portu v autě, platí od roku 2001. [13][14]

1.7.1 Mojio

Externím výrobcem, který nabízí služby Connected Car je společnost Mojio. Mojio je společnost, která vytvořila OBD II zařízení a software k němu potřebný a sdílela ho jako open-platformu pro ostatní vývojáře.

Díky zabudované GPS, Mojio umí číst polohu a rychlost vozidla, takže zde je možnost funkce upozornění polohy, kdy po nadefinování plochy by se vozidlo nemělo z této plochy vzdálit. Použití GPS polohy umožní také funkci poslední parkovací pozice. Díky softwaru, který Mojio navrhl, jsou zde statistiky jako např. efektivita jízdy, úspornost jízdy, spotřeba atd. Tyto statistické funkce je dále možno exportovat jako souhrn informací do pdf či csv.[8]

Mojio jako open-platforma spolupracuje s mobilním operátorem T-Mobile CZ, a tak v ČR vzniklo Connected Car řešení od mobilního operátora na platformě Mojio, pojmenované „CHYTRÉ AUTO“. T-Mobile toto řešení nabízí za 2 599 Kč s předplatným za 75 Kč měsíčně se smlouvou na 2 roky. Mezinárodně se toto řešení prezentuje jako SyncUP DRIVE™. [12]

Obrázek 8 - SyncUP DRIVE™ na platformě Mojio
Zdroj: T-Mobile (2015, https://explore.t-mobile.com/t-mobile-sync-up-drive)

1.7.2 Zubie

Společnost Zubie je dalším výrobcem externích řešení Connected Car. Jakožto řešení, které je omezeno pouze na OBD II port, nabízí skoro totožné funkce jako řešení Mojio. Zubie v předplatném na rok stojí $ 179.95 a oproti Mojio nabízífunkci In-carWi-Fi, tato funkce spočívá ve vytvoření hotspotu uvnitř vozidla, kdy se zákazník připojí na vytvořenou Wi-Fi síť a může surfovat po internetu. Zubie tímto vytváří možnost připojení se do internetu a surfování, ale data, která jsou spotřebována, nejsou zahrnuta v platbě předplatného, a záleží tak na operátorovi, jak má danou službu zpoplatněnou. [13]

Obrázek 9- OBD II řešení Connected Car

Zdroj: Zubie (2015, http://www.amomstake.com/wp-content/uploads/2014/01/Zubie-Key.jpg)

1.8 Bezpečnost Connected Car

Jak bylo řečeno v předchozích kapitolách, dnešní automobily už nejsou jen prostředky na dopravu. Také to jsou zařízení, která zpracují desítky gigabytů dat za hodinu. Vlastnostmi a způsobem navržení se to více podobá složitostí základní desce s plošnými spoji, než jen prostředku pro přepravu. Složitostí datových toků a celým konceptem připojení vozu k internetu sice nabízejí tato řešení zajímavé funkce, ale s přibývajícími funkcemi tu vznikají potenciální hrozby a trhliny v kódu těchto řešení. [9]

Zřejmě nejznámější situací, kdy bylo „ovládnuto“ vozidlo, byla situace z roku 2015. Pánové Charlie Miller and Chris Valasek se pokusili o převzetí kontroly nad vozidlem Jeep Cheeroke a jejich pokus byl úspěšný. Nejen že pronikly do vozidla a ovládli jeho infotainment, také dokázali převzít kontrolu systému řízení, brzd a převodovky. Dokázali to pomocí laptopu a internetu, bez blízké přítomnosti vozidla. [14] Tento případ byl názorným důkazem toho, že vozidlo dokáže být nebezpečnou zbraní. Jestliže by za laptopem nebyli dva hackeři, kteří chtěli jen dokázat, jak „děravý“ je systém, a byli by tam dva hackeři, kteří chtějí zabíjet, nic by jim v tom nebránilo. Po tomto incidentu Jeep svolal více než 1.4 Milionu

vozů kvůli kritické opravě, na kterou přišel právě díky ochotě dvojice spolupracovat na bezpečnostní záplatě.[6] [15]

Aby se předešlo situaci, která nastala s Jeep Cheerokee, a minimalizovala se rizika spojená s tímto řešením, vznikají standardizační normy pro bezpečnost při návrhu a realizaci řešení Connected Car. Následující kapitola obsahuje normy, které se věnují Connected Car a určitým pravidlům bezpečnosti.

2 Srovnání stávajících platných norem

Ve světě existuje nespočetné množství tzv. standardizačních norem. Tyto normy jsou výstupem procesu, který se nazývá standardizace. Standardizační normy se vytvářejí pro vzájemné uskupení informací mezi lidmi. Tyto normy vznikají především pro usnadnění komunikace, obchodu, měření a výroby. Výhody těchto standardů jsou více než jasné, vytvářejí vzor určitého problému a zároveň jeho řešení. Nicméně nevýhodou je, že se člověk omezí jen na předem daná pravidla, postupy a případy, které jsou určené standardem. Další nevýhodou může být například cena těchto standardů, v některých případech je investice do těchto pravidel více než značná.

Existuje několik typů standardů:

- De iure standardy – normy vytvořené skupinou expertů pověřených standardizační organizací, příkladem De iure normy je například ISBN.

- De Facto standardy – normy, které jsou určené praxí. Tímto standardem je formát .mp3. De Facto standardem se tento formát stal díky tomu, že byl rozšířen mezi lidmi.

- Otevřené standardy – normy, které jsou veřejně přístupné spolu s kompletní dokumentací. Otevřeným standardem je například protokol IP, který hraje klíčovou roli v oblasti internetu.

- Proprietární standardy – normy, které jsou tvořeny a vlastněny výhradně jednotlivcem či organizací, a použití je podmíněno poplatkem či licencí.

V oblasti automotive pojednávají tyto normy především o bezpečnosti zákazníků, nicméně jsou zde standardy začínající výrobou součástek až po standardy, kde je popsána jejich kvalita nebo postup testování.

Tato kapitola se bude zabývat normami souvisejícími s Connected Car konektivitou. Normy v Connected Car a s tím související prostředky jsou ve smyslu zabezpečení psaná pravidla a

doporučení, jak by se mělo postupovat při zabezpečení dané služby/vozidla. Případný rozbor kompletní normy je více než obsáhlý a se zabezpečením by nemusel souviset, proto zde je obsažen jen výtah a základní popis dané normy. Případně informace související se zabezpečením. V případě Connected Car existují normy od společnosti SAE. Jedná se o normu J3061a za zmínku stojí dále norma od organizace IEC s číslem 61508, která řeší bezpečnost elektronických zařízení. Jelikož je norem nespočetné množství, jsou označeny jako zkratka organizace a číslo př. ISO 11111.

2.1 IEC

Pod zkratkou IEC vystupuje International Electrotechnical Commission, což v překladu znamená Mezinárodní elektrotechnické konsorcium, které je světově uznávanou federací. Je to nezávislá organizace, která sdružuje odborníky za účelem sdílení znalostí, inovací a postupů.

2.1.1 ČSN EN 61508

Norma s číslem 61508 pojednává o obecné bezpečnosti elektronických zařízení a skládá se ze 7 částí. První čtyři jsou „normativní“, což znamená povinné, a zbytek slouží k informativním účelům. K účelu této práce slouží kapitoly, které pojednávají o obecném životním cyklu bezpečnosti, a k určování úrovně rizika. Tato norma je v práci zastoupená jako název ČSN EN 61508, nicméně jedná se o normu shodnou s ISO/IEC 61508. [17]

2.1.1.1 Životní cyklus bezpečnosti

Norma standardizuje celkový životní cyklus bezpečnosti, který je pro samotnou bezpečnost nesmírně důležitý, neboť nabízí model jednotlivých fází bezpečnosti během životnosti systému. Koncept celkového životního cyklu bezpečnosti je založen na faktu, že funkční bezpečnost není závislá na spolehlivosti. Odmítá, že pokud je systém provozně spolehlivý je zároveň bezpečný. V normě vystupuje řízení zařízení pod zkratkou EUC, což je Equipment Under Control.

První fáze s názvem Koncept pojednává o EUC a pochopení jeho prostředí tak, aby bylo možné provádět další činnost životního cyklu. Výstupem této fáze jsou informace o prostředí a nebezpečí EUC.

Druhá fáze má název Definice celkového předmětu či definice celkové oblasti užití. Tato fáze vymezuje hranice EUC a systému řízení. Stanovuje se předmět analýzy nebezpečí a rizik, nebezpečí procesu a nebezpečí okolního procesu. Výstupem této fáze je definovaný předmět nebezpečí a analýza rizika.

Třetí fází je samotná analýza nebezpečí a rizik, určuje se úroveň rizika a analyzuje se jejich přípustnost. Tato analýza je základní princip normy 61508, neboť zajišťuje vyváženost mezi opatřeními zajišťujícími bezpečnost a rizikem spojeným s řídicím systémem, proto je třeba, aby analýza byla důkladná. Podle normy se analýza skládá ze tří kroků: 1. Určení nebezpečí, 2. Analýza nebezpečí, 3. Ocenění rizika.

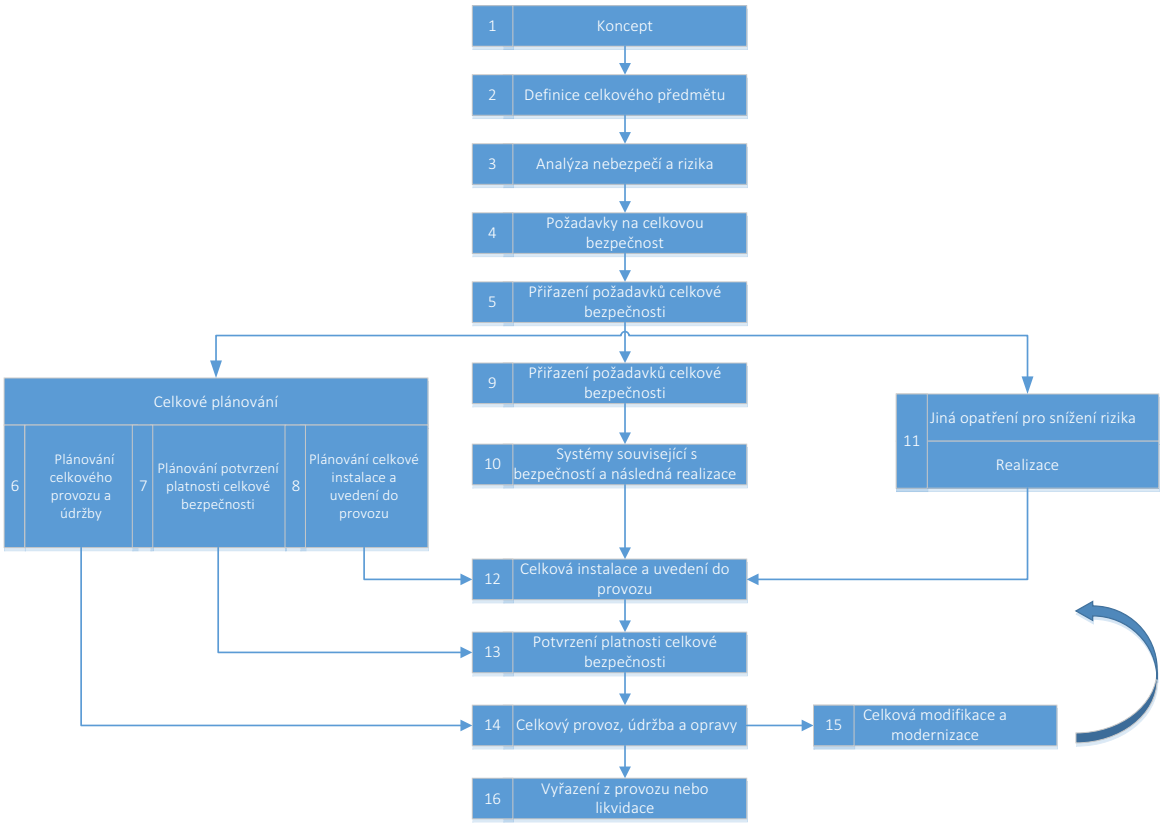
Čtvrtou fázi je stanovení požadavku pro celkovou bezpečnost zajišťující potřebné zmenšení rizika.

Pátou fází se stanovují požadavky konkrétní podoby, která vychází ze čtvrté fáze. A jsou přiřazeny jednotlivým systémům k vyprojektování ve fázích 6, 7, 8. Fáze 6, 7, 8 jsou totiž části, u kterých už nastává celkové plánování. U fáze č. 6 je to plánování celkového provozu a údržby, další fází je plánování potvrzení platnosti celkové bezpečnosti a poslední fází v oblasti plánování je poté plánování celkové instalace a uvedení do provozu. Následuje realizace, jejíž body zastupují číslo 9,10,11. Poté následuje fáze s číslem 12, která je už součástí instalace a nese název Celková instalace a uvedení do provozu, navazuje fáze 13, která se jmenuje Potvrzení platnosti celkové bezpečnosti a poslední fáze ze skupiny instalace je fáze s číslem 14 - Celkový provoz, údržba a opravy.

V případě plánované modernizace nastává fáze s názvem Celková modifikace a modernizace. Touto fází se definují nové postupy bezpečnosti a vrací se k příslušné fázi životního cyklu.

Poslední fází je už samotné vyřazení z provozu či likvidace, definují se zde například postupy pro zachování integrity po odstranění z provozu. Výsledkem je poté požadovaná funkční bezpečnost.

Kompletní diagram je zobrazen na obrázku č. 10.



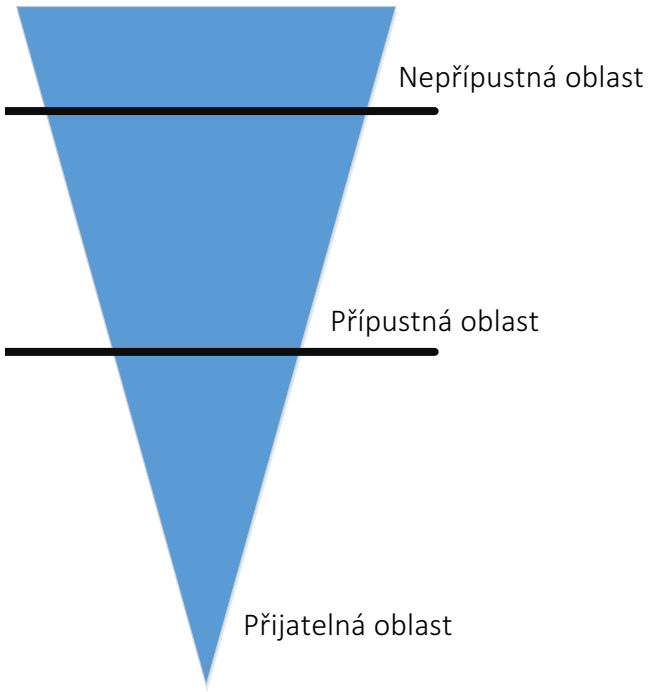
Obrázek 10 - Životní cyklus bezpečnosti dle normy ČSN EN 61508
Zdroj: ČSN EN 61508

Nutno zmínit, že tento model je pouze jen určitým přiblížením. Model nemůže nahradit kvalitní projektování a řízení, ale může být vhodně použit jako podpůrný prostředek k těmto činnostem.

2.1.1.2 Rozhodnutí o úrovni rizika

Další kapitolou ve standardu IEC 61508, kterou je vhodné zmínit, je kapitola určování rizika. Instituce při zabezpečení systémů se většinou musí rozhodovat, jaká rizika jsou ochotna

podstoupit, neboť v bezpečnosti systémů neexistuje riziko nulové. Rozhodují se mezitím, jaká rizika jsou přijatelná a jaká je třeba odmítnout. V souvislosti s rozhodováním o přijetí či odmítnutí rizika je spojen princip s názvem ALARP, z anglické zkratky As Low As Reasonably Practicable, v hrubém překladu znamená riziko co nejnižší, ale prakticky použitelné. Princip ALARP je obecný požadavek pro všechny bezpečnostně orientované systémy. Princip vymezuje tři oblasti, v nichž se riziko může vyskytovat.

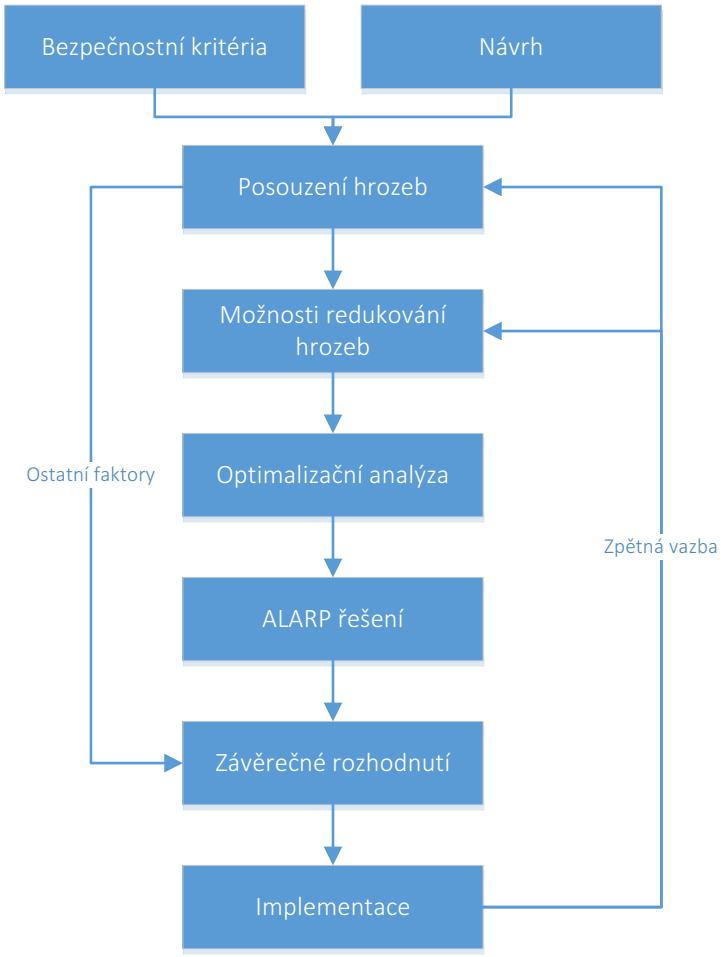


Obrázek 11- ALARP trojúhelník
Zdroj: ČSN EN 61508

První oblastí je riziko nepřípustné. Pokud se riziko vyskytuje v nepřípustné oblasti, nemůže být systém dále provozován, neboť s použitím přichází nebezpečí. Je to riziko, které spouští zmírňovací procesy, zajišťující následné snížení rizika nebo pozastavení systému, neboť přes toto riziko není možné pokračovat v provozu.

Další oblastí je riziko, které může být tolerováno za předpokladu, že instituci přináší výrazný zisk nebo výhody. Toto riziko by nemělo být přijato bezmyšlenkovitě a také by se nemělo v následné době zvětšovat, proto se pro tento případ provádí analýza nákladů a zisků. Po analýze a určení přípustnosti rizika, je toto riziko pojmenováno jako

ALARPriziko, které je prakticky nejnižší možné. Nadcházející diagram označuje proces určující ALARP riziko.



Obrázek 12 - Proces určující ALARP riziko
Zdroj: ČSN EN 61508

Tento diagram začíná dvěma procesy. Jedná se o proces bezpečnostních kritérií a návrhu. Návrh označuje samotné riziko a bezpečnostní kritéria označují souhrn pravidel, kterých by se mělo riziko držet. Společně tak vstupují do procesů, které vyhodnocují dané riziko. Další částí tohoto diagramu je proces Posouzení hrozeb, kde je posouzení daného rizika z hlediska toho, jaké konkrétní hrozby riziko představuje. Proces s názvem Možnosti redukování hrozeb je navazujícím procesem, který zvažuje možnosti a metody, díky kterým je schopno riziko omezit na takovou úroveň, aby ho bylo možné použít jako ALARP riziko. Následujícím procesem je ALARP řešení, což není nic jiného než diskuze, která vyhodnotí

všechny možné klady a zápory daného rizika a jeho přidanou hodnotu. Součástí diskuze je také detailní vyhodnocení, jestli dané riziko je vhodné přijmout či odmítnout. V následujících částích poté nastává finální rozhodnutí a implementace, kde vstupuje také zpětná vazba a posouzení stavu s případným návratem k dalším úpravám, také se znovu stanovuje závěrečné rozhodnutí s přihlédnutím k dalším nově přidaným faktorům.

Při užití praktického příkladu tohoto principu z pohledu automobilové bezpečnosti se pracuje s třemi kategoriemi rizik. V první kategorii se jedná o rizika nepřípustná, která ohrožují bezpečnost cestujících v autě. Druhou kategorií je oblast ALARP, v níž existuje riziko, nicméně automobilka v tomto případě je ochotna riziko podstoupit, neboť z tohoto rizika plynou určité výhody. Poslední oblastí je oblast přijatelná. Jsou to rizika, ze kterých neplynou žádné bezpečnostní či jiné problémy.

Z pohledu Connected Car to může být například riziko, které umožní připojení třetí strany do automobilu.

K převedení na skutečnost bude sloužit obecné riziko, kdy třetí strana, která chce zneužít cizí vozidlo, toho chce docílit za pomoci vzdáleného přístupu k autu. V prvním případě je to riziko, které by umožňovalo po přístupu do sítě vozidla zneužití řídící jednotky a ovládnutí řídících mechanizmů v autě, jako je např. brzda či plyn. Takové riziko je nepřípustné, neboť opravňuje třetí stranu ohrozit daného uživatele na životě.

Další kategorií je oblast přístupná (ALARP), příklad zde se definuje obtížněji, neboť jsou k tomu potřeba informace přímo od automobilek. Nicméně odhadem by se dalo považovat za příklad, když se třetí strana snaží připojovat na Wi-Fi síť vozidla, která je vysílána pro účastníky v autě. Rizikem je, že třetí strana prolomí ochranu a poté získá přístup do sítě vozidla. Každopádně automobilka je ochotna toto riziko podstoupit, neboť z toho plyne benefit, který umožní zákazníkovi vytvořit si z vozidla hotspot, od kterého získá přístup k internetu. Mimo jiné by automobilka měla zajistit to, že pomocí Wi-Fi sítě vozidla nebude možno se dostat do sítě vozidla, která by umožňovala ovládnutí řídících mechanizmů. Zjednodušeně řečeno bude odizolována Wi-Fi síť od sítě řídících jednotek.

V přijatelné oblasti může být riziko, které je malé a nevýznamné. V praktickém užití to může být riziko, které nijak neovlivňuje vozidlo, jeho bezpečnostní prvky a neomezuje účastníky v autě. [16]

2.1.1.3 Shrnutí ČSN EN 61508

Tato norma je celosvětovým standardem, který popisuje bezpečnostní zásady a požadavky na elektrické, elektronické a programovatelné systémy. Je to první regulace, která je nezávislá na druhu aplikace. V této práci je shrnuta jen menší část této normy, nicméně pro účel obeznámení o normách, které platí pro Connected Car, je dostatečná. V této práci je shrnuta kapitola životního cyklu, při kterém je důležité si uvědomit, že bezpečnost spočívá i v jiných faktorech než jen v systémových komponentách a je důležité ji řešit už od počátku vývoje. Další kapitolou bylo určení úrovně rizika, neboť je důležité uvědomit si, že žádný systém není možné dokonale zabezpečit a je důležité si uvědomit rizika a jejich úroveň a po určité analýze tyto rizika přijmout či snížit. [17]

2.2 SAE

Další společností, která se věnuje standardizačním normám, je Technical Standards and Development. Tato společnost je mezinárodně uznávaná pro kvalitu, bezpečnost a efektivnost jejich norem. SAE ve svém portfoliu vlastní více než 10 000 standardů. Norma, která souvisí s Connected Car, nese název SAE J3061. U této normy se nejedná přímo o Connected Car problematiku, avšak témata zmíněná v normě mají mnoho společného a pro obecné seznámení s problematikou a účel této práce jsou vhodná.

2.2.1 SAE J3061

Norma s označením SAE J3061 je soubor doporučení a principů, která se zaměřuje na kyberbezpečnost v automobilovém průmyslu. Celý název této normy je „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems“ a jak z názvu plyne, jedná se o postupy k zabezpečení automobilových systémů. Definuje životní cyklus bezpečnostních systémů,

dále zprostředkovává informace, metody a běžné nástroje při návrhu a validaci těchto systémů. Také zprostředkovává základní principy o bezpečnosti a jako poslední poskytuje základ pro budoucí rozvoj bezpečnosti těchto automobilových systémů.

Bakalářská práce se věnuje jen pouze vybraným statím z této normy. Vybrané kapitoly přibližují problematiku zabezpečení vozidla z pohledu vývoje.

2.2.1.1 Bezpečnostní potenciál systému

Co se týče vývoje systémů či zabezpečování systémů, je potřeba si uvědomit potenciál systému, který je potřeba aby byl bezpečný. Tento proces slouží k budoucímu vývoji a k porozumění této problematiky nám bude sloužit několik otázek. Na dané otázky by si měl odpovědět každý, který se problematikou zabezpečení systémů zabývá. Otázky jsou:

- Obsahuje náš systém některá citlivá data nebo osobní informace, která by mohla být předmětem útoku?
- Jakou roli hraje náš systém v kritických funkcích systému vozidla?
- Jak a s kým bude náš systém komunikovat? (Jestli vůbec)
- Bude náš systém komunikovat s ostatními účastníky provozu?
- Může být náš systém použit jako prostředek k jinému útoku?

V případě použití životního cyklu bezpečnosti ze standardu IEC 61508 se tyto otázky nachází ve fázi konceptu a definice celkového předmětu.

2.2.1.2 Analýza hrozeb a hodnocení rizik

V případě dalšího postupu životním cyklem bezpečnosti by se mělo pozastavit nad procesem **TARA** (Threat Analysis and Risk Assessment), který v překladu znamená **Analýza hrozeb a hodnocení rizik**, což je postup, při kterém se identifikují a sestavují veškeré hrozby a rizika, a navrhují se protiopatření na zmírnění rizik. Taková analýza se skládá ze tří složek:

První složkou je Analýza hrozeb. Tato analýza identifikuje potenciální hrozby systému

Druhou složkou je Klasifikace rizik. Tato složka posuzuje a klasifikuje identifikovaná rizika. Složka zvažuje závažnost možného útoku na systém a pravděpodobnost, že daný útok bude úspěšný. Pravděpodobnost, že potenciální útok může být úspěšně proveden, se označuje jako „potenciál útoku“. Potenciál útoku je definován různými faktory, které záleží na kompletní TARA analýze, nicméně v našem případě to může být například doba prorazitelnosti, odborné znalosti k útoku, zařízení nutná k útoku a příležitosti k útoku.

Poslední složkou je Analýza rizik. Tato analýza dává dohromady všechna klasifikovaná rizika a seřazuje je dle úrovní rizika. Jsou dvě možnosti, které určují úroveň rizika. První úrovní je riziko, které je přijatelné. Druhou úrovní je poté riziko, které je nepřijatelné, a je potřeba zajištění postupů, které by toto riziko snížilo.

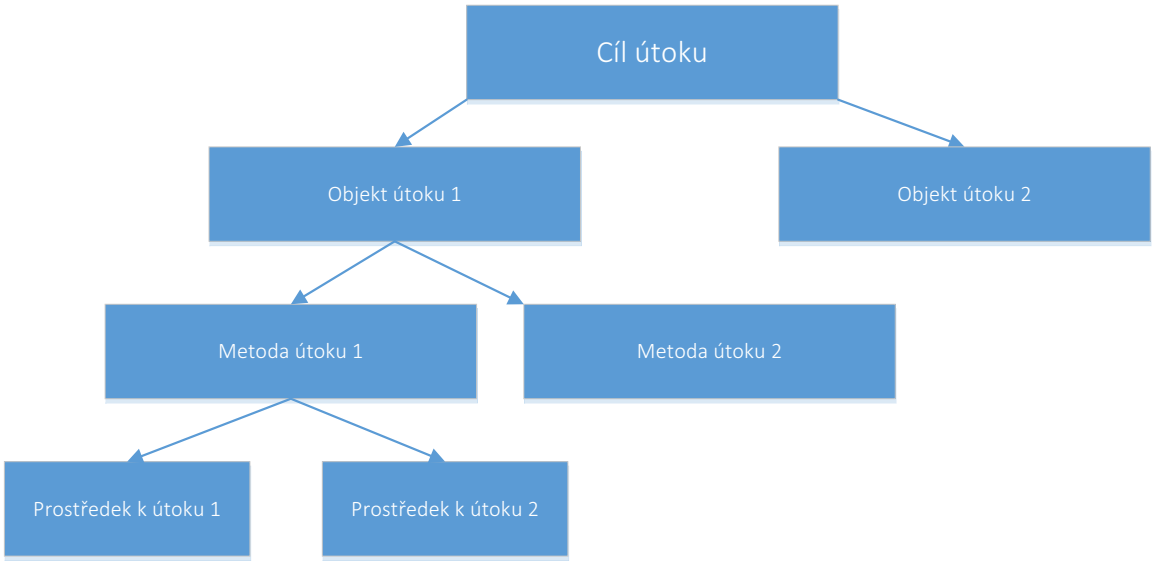
Cílem TARA analýzy je definovat potenciální hrozby pro funkci systému, posouzení rizika spojeného s každou identifikovanou hrozbou, zda je riziko na přijatelné úrovni či jestli je potřeba vytvořit protiopatření.

2.2.1.3 Metoda EVITA

Zkratka EVITA je metoda s názvem „**E**-Safety **V**ehicle **I**ntrusion Pro**t**ectec **A**pplications“. Tato metoda je nástroj, který byl vyvinut Evropskou komisí ve spolupráci s velkou částí známých organizací. K nejznámějším organizacím například patří BMW Group Research and Technology Bosch, Continental nebo Fujitsu. Cílem projektu bylo navrhnout a ověřit architekturu pro sítě uvnitř aut, kde by komponenty, které odpovídají za bezpečnost uvnitř vozidla, byly ochráněny před neoprávněnou manipulací a ochranou před únikem citlivých údajů. Metoda EVITA se soustřeďuje na 4 oblasti: provozní oblast, bezpečnostní oblast, oblast ochrany údajů a finanční oblast.

Úkolem provozní oblasti je udržet zamýšlenou provozní výkonnost a funkce automobilu. Bezpečnostní oblast má za úkol zajistit funkční bezpečnost uživatelů ve voze a účastníků provozu. Oblast ochrany osobních údajů má za úkol ochranu osobních údajů řidičů vozidel a duševní vlastnictví výrobců automobilů a jejich dodavatelů. Ve finanční oblasti má za úkol zabránit obchodním transakcím, které jsou podvodné, a také zajištění ochrany před krádeží vozidla.

Pro každou z těchto oblastí existují dva faktory, které mají určitou vypovídající hodnotu o zabezpečení každé oblasti. Je to identifikace rizika a klasifikace rizika. Faktor identifikace rizika je souhrn nejhorších možných scénářů, jež mohou nastat, a rozdělení každého scénáře do tzv. attack trees, „attack trees“ je podrobný rozpis daného útoku. V takovém to rozpisu je Objekt útoku, metoda útoku a použití komponent. K pochopení tzv. „attack trees“ dojdeme nejlépe diagramem. Na obrázku č. 13je obecný diagram, který zobrazuje rozpis prostředků, které jsou potřeba k útoku na systém.



Obrázek 13 - Obecný rozpis útoku v podobě EVITA metody
Zdroj: SAE J3061

Takový diagram představuje souhrn komponent a metod, které v celku tvoří nástroj, který je schopen docílit k plánovanému útoku. K převedení tohoto diagramu na skutečnost použijeme příklad, ve kterém chce útočník přebrat kontrolu nad brzdovou soustavou vozidla. Cílem útoku je brzdová soustava. Objekty útoku 1 a 2 jsou komponenty způsobující to, že se útočník dostane k brzdové soustavě. Takovými objekty může být například ECU řídící jednotka, která má na starost právě řídící soustavu. Metodami útoku je poté činnost, která způsobila, že se dotyčný dostal k objektu útoku. Příkladem toho může být například odposlouchávání vozidla a poté připojení k autu, z toho vyplývá další část s názvem Prostředek k útoku, což je prostředek, který musel útočník použít, aby daná metoda byla

uskutečnitelná. V tomto případě to je například odposlouchávání ECU jednotky pomocí OBD diagnostiky.

Výstupem tohoto diagramu je identifikace rizik a spolu s testovacími scénáři tvoří faktor, který kompletně identifikuje riziko pro následnou klasifikaci. Následná klasifikace vychází z metody **TARA**, která se vyskytuje v předešlé kapitole.

Po zhodnocení každé oblasti a faktorů v ní obsažených přichází na řadu tabulka na obrázku č. 14, který určuje třídu daného systému.

Třída	Bezpečnost	Soukromí	Finance	Provoz
S0	Žádná zranění	Žádný neautorizovaný přístup k datům	Bez finančních ztrát	Žádný vliv na provozní výkon
S1	Lehká zranění	Přístup pouze k anonymním datům	Nízké ztráty (~$10)	Nerozeznatelný dopad na řidiče
S2	Těžká zranění	Přístup k datům, která identifikují auto či	Průměrné ztráty (~$100)	Řidič si je vědom nižšího výkonu
S3	Život ohrožující	Sledování řidiče či auta	Vážné finanční ztráty (~$1000)	Značný vliv na výkon
S4	Život ohrožující nebo s fatálními následky pro více lidí	Sledování více řidičů či aut	Vážné finanční ztráty pro více aut	Značný vliv na výkon u více aut

Obrázek 14 - Rozdělení tříd závažnosti
Zdroj: SAE J3061

S třídou daného systému přichází na řadu tzv. potenciál útoku. Potenciál útoku je pravděpodobnost úspěšného útoku. Definuje ho útočník spolu se systémem a faktory této veličiny jsou uplynulý čas, úroveň znalostí útočníka, potřebná znalost systému, příležitost k útoku a potřebné vybavení. Každému z těchto faktorů se přiřadí číslo, které hodnotí jeho obtížnost. Např. u úrovně znalosti útočníka to může být laik s hodnotou 0, odborník s hodnotou 3, expert s hodnotou 6 a více expertů s hodnotou 8. Součet hodnot těchto faktorů poté vypovídá tabulka, na obrázku č. 15, o výši pravděpodobnosti, čím vyšší součet hodnot tím větší pravděpodobnost.

Hodnoty	Potenciál útoku potřebný k identifikaci a úspěšnému provedení útoku	Pravděpodobnost útoku
0-9	Základní	5
11-13	Rozšířený základ	4
14-19	Mírný	3
20-24	Velký	2
>=25	Nad očekávání	1

Obrázek 15 - Rozdělení potenciálu útoku
Zdroj: SAE J3061

Ve finální fázi nastává proces, který porovnává hodnotu pravděpodobnosti útoku a třídu závažnosti, a podle toho určuje výši rizika v následujícím obrázku. Je to stupnice od R0 do R6, kdy R0 je riziko nejnižší a R6 riziko nejvyšší.

Bezpečnostní úroveň rizika		Kombinovaná pravděpodobnost útoku				
		A=1	A=2	A=3	A=4	A=5
Závažnost	1	R0	R0	R1	R2	R3
	2	R0	R1	R2	R3	R4
	3	R1	R2	R3	R4	R5
	4	R2	R3	R4	R5	R6

Obrázek 16 - Rozdělení úrovně rizik
Zdroj: SAE J3061

Metoda EVITA je metoda, která srovnává úroveň rizika podle stanovených tabulek a v podstatě tím standardizuje úrovně rizik. Společnost, která tuto metodu použije, tak získá podrobný přehled o rizikách, které zjistila, a může tak pokračovat dál v řešení těchto rizik.

2.2.1.4 Pohled na bezpečnost z pohledu vozidla

Tato kapitola se bude věnovat otázkám bezpečnosti vozidla. Při pohledu na vozidlo nastává několik základních otázek, které souvisejí s bezpečností, a je nutné na ně odpovědět:

- Jakou elektronickou architekturu vozidlo používá?

- Definování počtu a typů interních komunikačních sítí ve vozidle.
- Identifikace počtu ECU jednotek ve vozidle.
- Jaká síť bude obsažena v každé ECU jednotce?
- Jak bude každá ECU jednotka identifikovaná?
- Které ECU by měly, vzhledem k jejím funkcím, být zabezpečeny? A jak to bude provedeno?
- Jak a s čím bude každá ECU komunikovat?
- Potřebná HW specifikace každé ECU jednotky.
- Potřebný software každé ECU.

Tyto otázky slouží k základnímu shrnutí a obeznámení, s čím vlastně společnost pracuje, a slouží jako úvodní informace pro další fáze při zabezpečování vozidla.

Standard J3061 nabízí několik bezpečnostních mechanizmů sloužící jako přibližný návod a postup, na jaké části vozidla se zaměřit:

- Izolování/oddělení systémů, které mají externí přístup od systémů, jež jsou kritické pro bezpečnostní systémy vozu a provozní funkčnost vozu. Také odizolování/oddělení systémů, které mají vliv na provozní funkčnost vozu.
- Mechanizmus definování přístupu ke kritickým ECU, k jejich diagnostickým módům a jejich datům.
- Mechanizmus, který zamítne přístup k informacím o provozním stavu vozidla, k osobním datům, k finančním datům, atp.
- Komunikační mechanismy mezi zařízeními, které způsobí to, že při výměně informací mezi přijímači nemůže dojít k záměně informací.

- Mechanismy, které efektivně zabezpečí diagnostické a aktualizační procesy.

- Kroky, které zabezpečí vozidlo proti metodám reverzního inženýrství, jakožto efektivního nástroje k útokům.

Tyto body spolu s otázkami slouží jako základ k zabezpečení vozidel, nicméně je na každé automobilce, jak si zabezpečí svůj model, neboť každá automobilka používá svůj hardware. V tomto standardu se totiž nevyskytuje přesnější informace o hardwarových prostředcích a jejich zabezpečení.

2.2.1.5 Integrace a testování

Integrace a následné testování systémů jsou kritickým procesem ve vývoji bezpečnosti pro vozidla. Proces testování slouží k potvrzení, že jednotlivé integrované systémy jsou schopné komunikace a při tom jsou schopni dodržet bezpečnostní zásady. Testování se dělí na dvě skupiny: penetrační testy a tzv. fuzz testing.

Penetrační testy simulují útoky na systém pomocí jedinců, kteří se snaží chovat jako hacker. Tito testeři se snaží infiltrovat do systému za použití všech prvků, které systém nabízí. Toto testování se nachází v pozdější fázi životního cyklu, neboť k penetračním testům je potřeba funkční zařízení, tudíž toto testování probíhá až v závěru vývoje, a zároveň je také méně času k odstranění chyb.

Fuzz testování může být použito v testování funkce. Je to testování, které na vstupech systému poskytuje chybná, neočekávaná či náhodná data. Úkolem je zjistit, jak daný systém funguje a je schopný se při těchto nečekaných situacích chovat, popřípadě zaznamenávat chyby způsobené nečekanými vstupy, a předat je vývoji, který je schopen tyto chyby opravit.

2.2.1.6 Shrnutí SAE J3061

V předešlých kapitolách bylo shrnuto několik témat ze standardu J3061 od SAE. Práce se věnovala dvěma druhům analýz rizik, která jsou primárním procesem k určování rizik a následnému vývoji. Další kapitolou byl úvod do bezpečnostních otázek automobilových systémů. Tato problematika představuje úvod do problematiky v kapitole č. 3, která je analýzou bezpečnostních rizik spojených s Connected Car. Další kapitolou byla integrace

a testování, kde se kapitola věnovala jen stručnému úvodu. Testování je jeden z hlavních prvků při vývoji systému, nicméně pro účel naší práce je úvod do této problematiky dostačující.

Hlavním prvkem této normy je životní cyklus bezpečnosti, v této kapitole je cyklus zmíněn, neboť byl vysvětlen v kapitole předchozí v normě IEC 61508 a v podstatě z tohoto životního cyklu vychází a je si velmi podobný.

Tato norma je detailnějším průvodcem k tomu, jak zabezpečit automobilový systém, nicméně nevyskytuje se zde nic, co by vypovídalo o technické stránce věci. Jsou zde popsány podrobněji fáze životního cyklu a způsoby, které se v každé fázi vykonávají. Jsou zde popsány také metody analýz a hodnocení rizik, které jsou pro vývoj nezbytné.[16] [18]

2.3 Srovnání norem IEC a SAE

Závěrem této kapitoly je porovnání norem a jejich částí představených v této práci. První normou, která se zde objevila, byla norma IEC 61508. Tento soubor slouží jako obecný předpoklad bezpečnosti v elektronických systémech a sleduje otázky životního cyklu bezpečnosti. Bezpečnost musí být řešena od počátku vývoje a hrozby, které nemůžou být tolerovány, musejí být sníženy použitím ALARP principu. Celkově norma hodnotí obecnou bezpečnost, tudíž se zde nevyskytují žádné informace o autě či jak tato pravidla užít u vývoje bezpečnosti vozidla. V případě životního cyklu bezpečnosti se tato pravidla dají reflektovat, a tak mohou sloužit jako podpůrný prostředek u vývoje. Každopádně se nejedná o prostředek, který tento vývoj nahradí.

V případě normy SAE J3061 se jedná o soubor, který poskytuje detailnější popis základních principů při řešení tématu bezpečnosti automobilových systémů. Stejně jako IEC 61508 obsahuje životní cyklus bezpečnosti, v této práci byl použit cyklus z normy IEC 61508, v každém případě SAE J3061 obsahuje cyklus detailnější a pro použití v automobilovém průmyslu, ale svojí podstatou vychází z cyklu z normy IEC 61508. Pro účel této práce, která se snaží normy porovnat a provést čtenáře základními principy, je tento cyklus dostačující. Norma SAE J3061 mimo jiné obsahuje detailní popis každé fáze z cyklu

a vysvětluje postupy a principy v dané fázi. Pro účel této práce a nahlédnutí do některých z fází bylo vybráno několik kapitol z této normy. První kapitolou byl popis a úvod do problematiky bezpečnosti systému obecně. Další kapitolou byl popis analytického nástroje s názvem **TARA.** Navazující kapitolou byl popis metody **EVITA** a průvodce určení úrovně rizika a jeho podrobného popisu. Aby se nejednalo pouze o teoretické věci ohledně vývoje bezpečnosti, v práci se také vyskytuje pohled na bezpečnost z perspektivy vozidla. Kapitola vysvětluje prostředky vozidla a otázky, které je třeba si zodpovědět při práci na bezpečnosti, bezpečnostní mechanismy, které slouží jako úvodní manuál při zabezpečení. Závěrečnou kapitolou byla fáze životního cyklu bezpečnosti a to je integrace a testování. K účelu této práce posloužila pouze teorie, která rozděluje testování do kategorií, a podtrhává fakt, že testování je nedílnou součástí každého vývoje.

Úkolem stávající kapitoly je mimo jiné určitým způsobem porovnat tyto dvě normy. Nicméně je to nelehký úkol, protože se jedná o normy, které jsou jedinečné svého druhu. IEC 61508 v pohledu obecné bezpečnosti a SAE J3061 v pohledu bezpečnosti automobilových vozidel. Dá se říci, že SAE J3061 vychází z IEC 61508 s tím rozdílem, že se SAE J3061 má nastavený exaktní směr. V obou normách se nacházejí životní cykly bezpečnosti a ve většině případů se neliší, jen v případě SAE J3061 se jedná o cyklus podrobnější a se zaměřením na bezpečnostní vývoj automobilů.

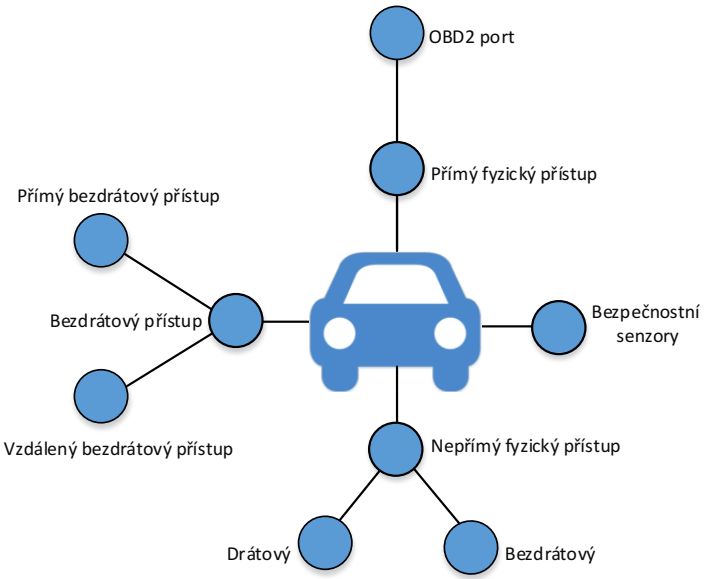
V obou normách chybí techničtější popis dané problematiky a určité schéma automobilové sítě a případy jejího zabezpečení. Na závěr by bylo jistě na místě dané normy ohodnotit, bohužel ohodnocení těchto norem je spíše otázkou na vybrané automobilky, které jistě dané normy používají, nicméně vzhledem k utajení a uzavřenosti automobilových vývojových center pro veřejnost, je ohodnocení těchto norem nemožné a laikem bezvýznamné.

3 Analýza potenciálních rizik spojených s připojením vozidla k internetu

Nadcházející kapitola, která nese název Analýza potenciálních rizik spojených s připojením vozidla k internetu, se dotkne analýzy rizik a bude přitom vycházet z diagramu Connected Car řešení. Kapitola standardizačních norem byla spíše teoretickým úvodem do problematiky bezpečnosti s pohledem na vývoj automobilu se službami Connected Car. V této kapitole bude přiblížení technické stránky věci a nastínění možnosti rizik, které nezpůsobuje jen špatný návrh výrobce, ale například nevhodné použití uživatelem. Autorem vytvořená analýza podtrhne přístup k Connected Car z technického pohledu a nastíní možná rizika.

3.1 Analýza technických prostředků automobilu

Následující kapitolou bude technického rozpisu možností, jak se zaměřit na automobil jako potenciální předmět útoku. K tomuto popisu poslouží obrázek č. 17, který zobrazuje vůz, a jeho možnosti přístupu v high-level zobrazení.



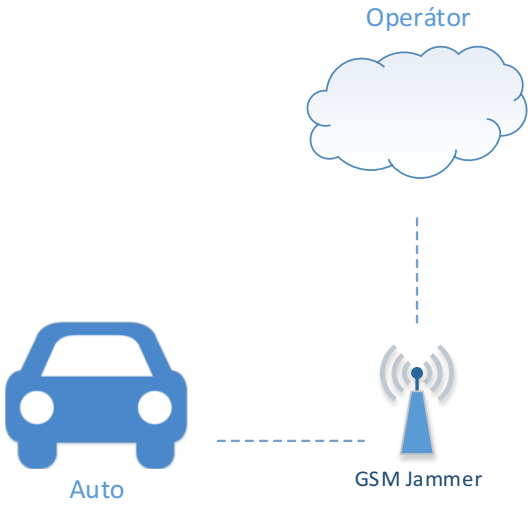
Obrázek 17 - Connected car a jeho možnosti přístupu
Zdroj: Vlastní

V tomto zobrazení můžeme automobil dělit na 4 skupiny, přičemž každá skupina zprostředkovává potenciálnímu útočníkovi prostředky k přístupu. První skupinou je přímý fyzický přístup. Tímto přístupem se rozumí přístup do odemčeného vozidla a přístup ke všem jeho prostředkům. V tomto případě je zde pouze OBD2 port, neboť za pomocí tohoto portu je možnost se připojit přímo do sítě CANBus, na kterou je tento port připojen. V teoretickém uvažování by se jednalo o přístup do sítě, která zajišťuje v podstatě kompletní komunikaci v autě a i komunikaci mezi řídícími mechanismy automobilu. Samotný OBD2 port s Connected Car službami nesouvisí, nicméně ve spojení s OBD2 donglem, který byl představený v první kapitole a zpřístupňuje Connected Car služby pro vozy, které těmito službami od výroby nedisponují, je to možnost pro útočníka dostat se k síti automobilu. Přístup k těmto donglům je za pomoci Wi-Fi a nebo pomocí bluetooth, v obou případech je pravděpodobné, že budou zařízení zabezpečená, nicméně v teoretické rovině zde vzniká riziko připojení se útočníka k síti OBD2 portu a následné zneužití této situace. Reálné použití by mohlo být například, když daný automobil čeká pravidelný servis. Je zde možnost zpřístupnění OBD2 donglu pomocí servisových pracovníků a následné dohledání OBD2 donglu a jeho zneužití.[9]

Další skupinou je nepřímý fyzický přístup, který se dále dělí na přístup drátový a bezdrátový. Drátovým přístupem se rozumí přístup pomocí dostupných prostředků uvnitř automobilu např. USB port, SD port nebo přehrávač CD. Tyto prostředky jsou oproti OBD2 donglu nepřímým přístupem, protože nejsou přímo napojené na síť CANBus. Za pomocí těchto prostředků je možnost potenciální změny softwaru v autě a následnému převedení vlivu těchto změn na Connected Car služby. V praktickém použití to může být například přehrání systému multimediální jednotky s upraveným OS. Tento systém poté může obsahovat různé malwary či přímo přístup pro daného útočníka. Automobilka Fiat Chrysler Automobiles (FCA) učí zákazníky, jak si stáhnout jejich software a následně ho přehrát v autě v případě, že FCA vydá bezpečnostní záplatu. Známé zneužití automobilu a jeho řídících mechanismů bylo představeno v první kapitole, toto převzetí kontroly nad automobilem bylo způsobeno právě za pomocí přehrání OS a následného vzdáleného připojení. Tento problém byl vyřešen právě ze strany automobilky FCA, kdy rozesílali USB Flash Disk zákazníkům. Daný flash disk obsahoval novější verzi systému, v níž byla opravena bezpečnostní chyba.[14]

Druhou podkategorií je bezdrátový přístup. Je to přístup za využití prostředků jako např. Wi-Fi a BT. U těchto prostředků platí stejná rizika jako v případě drátových, ale je zde navíc možnost ovlivnění připojených zařízení. V případě Wi-Fi je to možnost připojení se na danou síť, odposlouchávat ji a následně zasílat zpětně na síť data hodící se ke zneužití daného vozidla. S tímto faktem také souvisí možnost připojení se útočníka za pomocí zařízení nepřímo připojeného k autu. V případě smartphonů to může být připojení daného uživatele k Wi-Fi síti, které vozidlo vytváří, a následné připojení útočníka přes daného uživatele, který má nezabezpečený telefon. Nezabezpečený telefon může vzniknout například z důvodu nepravidelných instalací bezpečnostních aktualizací a tím vzniklých bezpečnostních problémů.

Třetí kategorií je přístup pomocí bezdrátového přístupu. V této kategorii se jedná především o přístup do vozidla za pomoci mobilní datové sítě. Příklad útoku je za užití tzv. GSM Jammeru, což je zařízení tvářící se jako vysílač signálu mobilního operátora a slouží jako most k připojení se k síti.[9] V praxi to znamená, že se vozidlo připojí k „vaší“ síti, ale i přes to jsou funkční jeho Connected Car služby, neboť je schopen se přes vás připojit k mobilnímu operátorovi. Daný útočník může komunikaci odposlouchávat a využít tak daných prostředků k ovlivnění vozidla. Pro lepší představení tohoto zařízení slouží obrázek č. 18.



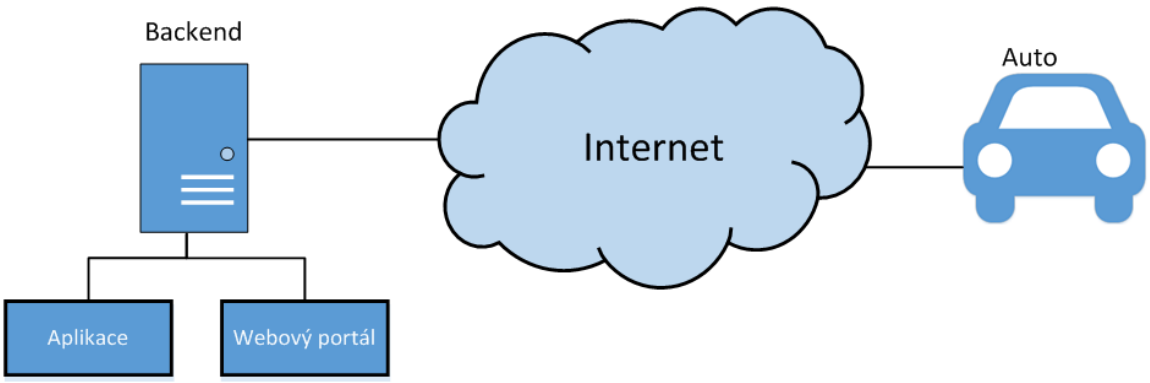
Obrázek 18 - GSM Jammer a jeho funkce
Zdroj: Vlastní

Poslední kategorií jsou specifické vlastnosti bezpečnostních senzorů aut. V této kategorii se jedná o teoretičtější případ více než v kategoriích předešlých, neboť nejsou známa žádná zařízení a případy, ve kterých by došlo k ovlivnění vozidla za pomocí bezpečnostních senzorů. Jsou to bezpečnostní senzory, které přímo ovlivňují další funkcionalitu vozidla, jeho řídící mechanismy a dokážou tak vážně zasáhnout do jeho prostředků a je vhodné je zde zmínit.

3.2 Analýza technických prostředků zprostředkovatele služeb

Další součástí Connected Car služeb je tzv. zprostředkovatel služeb. V této práci bude dále zmiňován jako tzv. back-end. V první kapitole při seznámení s celkovým řešením Connected Car služeb byla tato komponenta představena. Je to však mnohem komplexnější systém než se zdá. Komplexnost v backendu spočívá v tom, že je to systém, který odpovídá za všechny služby v řešení Connected Car. Nicméně žádná automobilka neodkryje své řešení backendu, ať už z bezpečnostního či konkurenčního důvodu, proto se v této kapitole objeví jen hrubá analýza, jak by nejspíše mohl celý systém fungovat, popř. jeho potenciální rizika.

Podobně jako v předchozí kapitole je vhodné začít s high-level zobrazením dané komunikace, viz Obrázek č. 19.



Obrázek 19 - High-level schéma komunikace backendu
Zdroj: Vlastní

Za příklad, jak tento koncept funguje, použijeme dotaz z webového portálu. Po užití služby, která zjistí, kde se dané vozidlo nachází, se vyšle dotaz směrem od portálu k backendu, ten rozliší, od koho daný požadavek směřuje a s jakým vozidlem je daný účet provázán, poté pomocí internetu naváže kontakt s automobilem a požádá o potřebné údaje. Vozidlo pošle zprávu s polohou, směrem k backendu. Back-end poté pošle zprávu zpět webovému portálu. Prvním bodem k diskuzi je samotné zabezpečení počítače uživatele. S tím souvisí druhý bod, a to je zabezpečení backendu směrem k uživateli, např. kvůli odposlouchávání komunikace mezi back-endem a uživatelem. Třetím bodem je zabezpečení samotného backendu směrem k internetu, jelikož se zde zachází s citlivými údaji uživatele. Posledním bodem je poté samotná komunikace mezi back-endem a vozidlem.

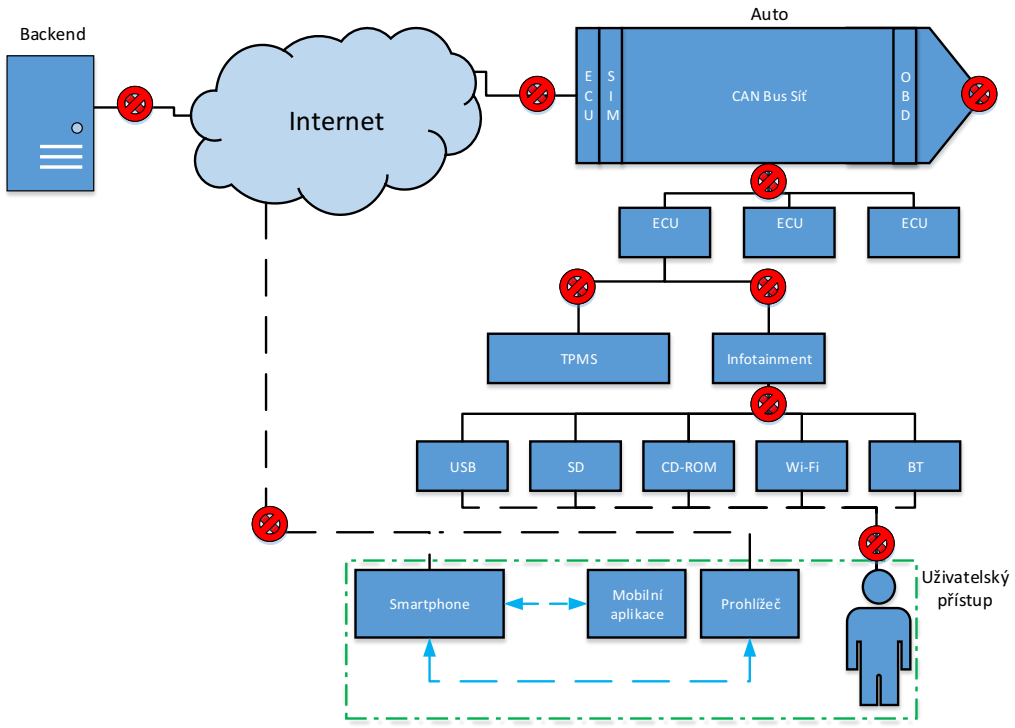
Z backendu jako takového neplynou žádná životu ohrožující rizika, neboť pomocí portálu není možné ovlivňovat chování vozidla. Nicméně je na místě se zmínit o této části řešení Connected Car, neboť přístup pomocí portálu či webové aplikace je možný po zadání uživatelského jména a hesla a samotný účet je riziko v tom, že obsahuje citlivá data. Může obsahovat i údaje o kreditních kartách, neboť některé automobilky mají i zakomponovaný e-shop, kde je možnost zakoupit či prodloužit předplatné služeb.

3.3 Analýza celkového Connected Car řešení

V předešlých kapitolách bylo představeno high-level zobrazení komunikace Connected Car. Tato schémata byla rozdělena na komunikaci zprostředkovatele služeb Connected Car a na samotný vůz a jeho celkovou konektivitu, přičemž kapitola obsahovala i potenciální rizika spojená s Connected Car službami. Tato kapitola se bude snažit o spojení předešlých dvou schémat a shrnutí rizik, která vyplývají pro uživatele Connected Car. V tomto oddíle se také pokusíme shrnout rizika pro samotného výrobce. Na obrázku č. 20 je bližší pohled na danou problematiku spolu s červenými body, které signalizují potenciální body zranitelnosti, a body, kterým je třeba se věnovat.

Z první kapitoly, kde se na schématu vyskytuje pouze vozidlo s možnostmi konektivity, se v této kapitole promítá vozidlo jako CANBus síť a konektivita této sítě je zde vyobrazena

jako síťová topologie. Z druhé kapitoly zde vstupuje zprostředkovatel služeb a jako poslední článek je zde zobrazen samotný uživatelský přístup.



Obrázek 20 - Schéma celkového Connected Car řešení
Zdroj: Vlastní

Samotná část vozidla se skládá z komponent ECU/SIM a OBD. ECU/SIM je jednotka, která podporuje vložení SIM karty a zpřístupnění datového připojení, červený bod u této jednotky je proto, že zde probíhá komunikace mezi internetem a vozidlem. Rizikem je využití zmíněného tzv. GSM Jammeru, odposlouchávání sítě a následné využití informací z odposlechu. OBD jednotka, jak už bylo v předešlých kapitolách řečeno, je port diagnostiky, který je volně přístupný, a díky tomuto portu je možnost získání služeb Connected Car i v autě, které to přímo nepodporuje. Existují dva typy rizik, jeden typ, kdy vozidlo využívá externí dongle, a riziko, kdy teoretický útočník může za využití servisního pracovníka zneužít OBD port k získání některých citlivých dat. Dalším bodem potenciální zranitelnosti je samotné zabezpečení mezi CANBus sítí a ECU jednotek. V schématu se vyskytuje několik ECU jednotek, je to proto, že v autě neexistuje pouze jedna ECU jednotka, která se stará o vše, těchto jednotek existuje v autě několik. Riziko spočívá v tom, že jednotka, která má na

starost kritické funkce automobilu, např. řízení, by měla být odizolována od jednotek, které by podléhaly útokům ze třetích stran. Taktéž se body nacházejí u komponent TPMS a infotainment. Komponenta TPMS je v autě komponenta sloužící pro kontrolu tlaku v pneumatikách z angličtiny „Tyre Pressure Monitoring System“.[5] Tento systém totiž vysílá nízkofrekvenční signály, které se dají teoreticky odposlouchávat, a navázat díky nim komunikaci s vozidlem. Dalším bodem je samotný infotainment, kde je vidět bod zranitelnosti ze strany ECU a bod zranitelnosti ze strany uživatele. Bod zranitelnosti ze strany ECU jednotek je ze stejného důvodu jako bod mezi ECU a CANBus sítí. Je totiž potřeba, aby infotainment byl také odizolován od ostatních jednotek. Bod zranitelnosti ze strany multimediálních stupů zastupuje zabezpečení všech vstupů a ochranu proti vloženým mediím. Ze strany uživatelského přístupu je bod také kvůli ochraně mobilního zařízení a jeho případného zneužití.[9]

Dalším okruhem zranitelností je část zprostředkovatele služeb. Kvůli tomu, že si každá automobilka chrání své know-how, není zde mnoho věcí, které by se daly popsat. Komunikace back-endu probíhá s vozidlem oběma směry. Komunikace, která mezi těmito dvěma komponentami probíhá, je bodem zranitelnosti, protože zde může být opět riziko odposlouchávání a podvrhu informací. Pro tento případ je zde na místě důkladné zabezpečení od výrobce. V každém případě je důležité se také zaměřit na uživatelské zařízení, tj. prostředky, kterými se uživatel připojuje. Na jedné straně je to samotné vozidlo, nicméně na druhé straně to jsou koncoví zákazníci a jejich nezabezpečená zařízení. Automobilky jsou proto v nelehké situaci, v níž musejí počítat s různými scénáři, a vytvořit přístup tak, aby byl odolný i vůči některým situacím, které jsou způsobeny nejen jejich řešením. Praktický příklad může být, když se uživatel připojuje pomocí aplikace, zadá zde své přihlašovací údaje, díky kterým má přístup do portálu, a poté zkouší funkce Connected Car. Na druhé straně stojí potenciální útočník, který se ani nepokoušel o jeho údaje do portálu, ale pouze získal přístup do jeho smatphonu, přes bezpečnostní mezeru, kterou zákazníkův smartphone obsahoval. Poté potenciální útočník dostane možnost přihlášení do portálu a s tím spojené funkce. Jak už bylo řečeno, funkce spojené s portálem nejsou nikterak životu ohrožující, nicméně je možné zde sledovat vozidlo, a také v některých případech obsahují uživatelské účty informace kreditní karty.

Na straně uživatelského přístupu obrázek ukazuje, že uživatel má tři možnosti, jak přistupovat k službám Connected Car. První možností je přístup přímo k vozidlu vybavenému službami a druhou možností je prohlížeč. Na schématu je zobrazeno propojení mezi prohlížečem a smartphonem, je to z toho důvodu, že lze přistupovat i pomocí prohlížeče na smartphone, i když na smartphone existuje aplikace.

Na obrázku č. 20 je zobrazeno kompletní technické řešení Connected Car a červenými obrazci zobrazeny jeho potenciální zranitelnosti. Tento digram je platný pro Connected Car řešení od výrobce a i pro řešení od externích výrobců pomocí OBD donglu. Tento obrázek dále slouží jako podklad pro tvorbu pravidel pro bezpečné využití služeb, kterým se věnuje následující kapitola.[19][20][21]

4 Vytvoření pravidel pro bezpečné využití Connected Car

Kapitola pod názvem Vytvoření pravidel pro bezpečné využití Connected Car se zabývá vytvořením postupů, které by bylo možné použít při tvorbě a použití Connected Car služeb. Při tvorbě těchto pravidel využije práce obsahu předešlých kapitol, což znamená obecnější pohled na Connected Car řešení a užití bezpečnostních norem.

4.1 Pravidla pro zákazníka

Pravidly pro zákazníka máme na mysli pravidla, která by zákazník měl dodržet, pokud chce bezpečně pracovat s řešením Connected Car. Nicméně na začátku koupě každého vozu si zákazník vždy položí několik otázek, které ho zajímají ohledně vlastností vozu. Při koupi vozu s řešením Connected Car by tak zákazník mohl a měl obohatit svůj zájem o několik otázek, které by prodejce měl zodpovědět, a přesvědčit tak zákazníka o bezpečnosti řešení. Otázky, které by byly vhodné k zodpovězení:

1. Jestliže se jedná o uživatele více technicky směrovaného, bylo by na místě tázat se, jak jsou řešeny bezpečnostní záplaty a celkově možnosti aktualizace.

2. Výsledky bezpečnostních testů daného výrobce.

3. Jestli výrobce vydal souhrnný manuál a bezpečnostní pravidla pro použití Connected Car služby.

Z těchto otázek by tak vyplynula pravidla, která by měl zákazník dodržet. Jestliže daný výrobce vydal manuál k použití, tak tento manuál je samotným návodem k bezpečnému použití Connected Car a výrobce se tak vlastně odvolává k tomu, že pokud vznikne škoda způsobená nevhodným užitím tohoto řešení, daný výrobce nenese žádnou odpovědnost.

V následujícím odstavci jsou pokyny, které platí pro všechna Connected Car řešení, a každá automobilka by takové pokyny měla vydat. Ať už pro ochranu zákazníka, tak především pro ochranu jména společnosti.

Pravidla pro uživatele:

1. Chránit své mobilní zařízení před zneužitím, krádeží či ztrátou, mj. chránit své mobilní zařízení dle obecných zásad bezpečnosti při používání internetu. Chránit mobilní zařízení vhodným antivirovým programem, pravidelně ho aktualizovat, atp.

2. Neupravovat software u zařízení, která přistupují ke službám Connected Car. U vozidel je to úprava multimediálních jednotek a u mobilního telefonu je to úprava systému (např. u OS Android, úprava zvaná „root“, u iOS zařízení tzv. „jailbreak“).

3. Neinstalovat neověřené aplikace třetích stran do mobilu či vozidla.

4. Dbát na pravidla týkající se zacházení s počítači a mobilními zařízeními, což např. znamená vytvoření bezpečného hesla.

5. Zakoupené zařízení OBD2, které zpřístupňuje Connected Car služby, musí být v souladu s HW požadavky a HW podporou vozidla.

6. Je potřeba respektovat kontrolní hlášení vozidla a v případě některé poruchy, vyhledat ihned autorizovaný servis.

7. Vždy aktualizovat veškerá mobilní zařízení a automobil, pokud to výrobce umožní.

8. Zákazník by měl vždy zamykat své vozidlo ve veřejně přístupných oblastech.

9. Nikomu nesdělovat své osobní a přihlašovací údaje.

10. Jestliže se zákazník domnívá, že se jeho vozidlo stalo terčem útoku, měl by urychleně navštívit autorizovaný servis.

4.2 Pravidla pro výrobce

Pravidly pro výrobce rozumíme pravidla, která by výrobci měli dodržovat při vývoji daného řešení. Bezpečností se zabývají všechny společnosti, které vytvářejí služby Connected Car, neboť jsou si vědomi následků, které by mohly v případě nedostatečného zabezpečení nastat. Při vytváření těchto pravidel se bralo v úvahu obecné přesvědčení o bezpečnosti a také byly brány v potaz předešlé kapitoly. Vznikla tak pravidla pro výrobce:

1. Návrh Connected Car architektury, kde řídící jednotky automobilu, které řídí veškerou řídící komunikaci, jsou separátně odděleny od ostatních jednotek, zejména od jednotky ECU/SIM, která je zprostředkovatelem internetu v automobilu.

2. Při návrhu systému je potřeba zvážit zapouzdření jednotlivých komponent. Ve výsledku by byly komponenty rozděleny na několik bezpečnostních vrstev a pro potenciálního útočníka by to znamenalo více bariér k prolomení.

3. Využití tzv. redundance systému, v praxi by to znamenalo využití komponent „na vícekrát“. Použití více komponent, které by vykonávaly tu samou činnost. Zamezilo by se výpadkům služeb, neboť když jedna komponenta vypoví činnost, nahradí ji komponenta druhá, zároveň to pro útočníka přináší další obtíž v podobě překonání další komponenty navíc, protože by zde bylo na místě použití pravidla z předešlého bodu, což by znamenalo, že by tato každá komponenta byla jinak zabezpečená.

4. Při návrhu řešení zakomponovat takovou funkcionalitu, která by vyhodnocovala bezpečnost v síti vozu. Např. funkcionalitu, která ověří, že zapojený USB disk není pro dané vozidlo hrozbou.

5. Obeznámit se s bezpečnostními normami a případné využití od raného vývoje daného řešení.

6. Během fáze, kdy se dané řešení testuje výrobcem, je na místě, aby byly v testování zakomponovány testovací scénáře, které prověřují bezpečnostní otázky Connected Car.

7. Při vývojové fázi je nutno provést důslednou kontrolu zdrojového kódu a případnou opravu bezpečnostních zranitelností přímo v kódu.

8. Při vývojové fázi zakomponovat funkcionalitu OTA aktualizací.

9. Ze strany výrobce ověřit zaměstnance, kteří se podílejí na vývoji tohoto řešení. Omezit přístup k datům, která odhalují celý koncept řešení a uživatelská data, zaměstnancům a především třetím stranám.

10. Definování procesů pro koncového uživatele, tzn. zákaznickou podporu, jasné definování terminologie řešení a kompletní dokumentace pro zákazníky, kde by bylo vysvětlení všech Connected Car služeb, a především jak se dané služby používají.

4.3 Shrnutí pravidel

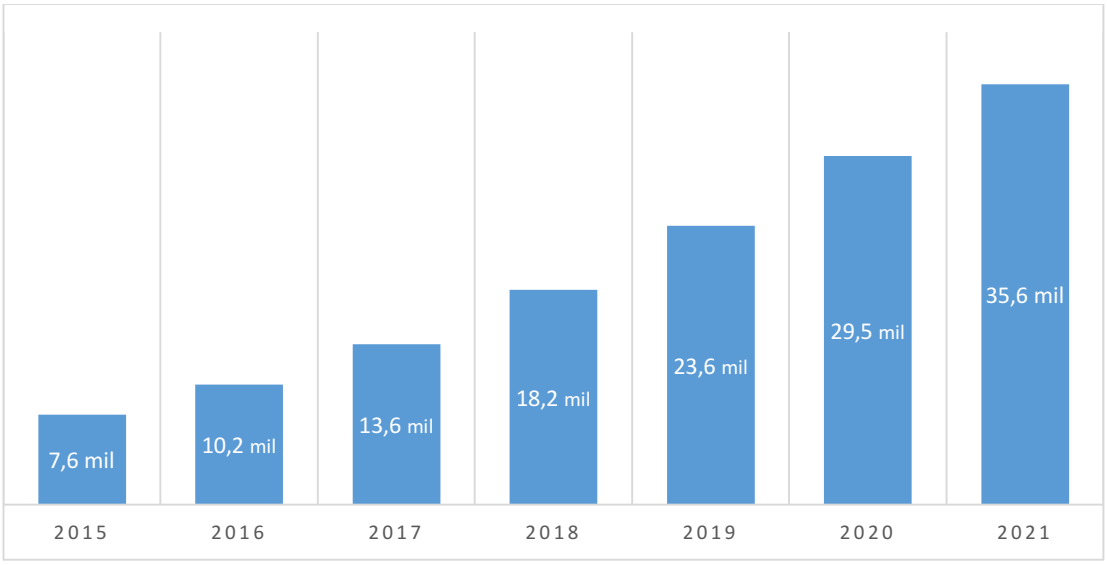
Výsledkem této práce jsou pravidla, která jsou určitými opatřeními vůči vlivům okolí. Jsou to pravidla, která říkají, jak zacházet se službami Connected Car. Nicméně v měřítku práce není úkolem vytvořit pravidla, která budou „neprůstřelnou zdí“ proti útočníkům, kteří chtějí tyto služby zneužít. Jsou to pravidla, kterými se dá proaktivním způsobem přitížit potenciálním útočníkům a zabránit, alespoň typům útoků, kdy uživatel nastavuje jednoduché heslo a útočník ho pouze uhádne. Tato pravidla jsou zaměřena na obě strany, kterých se tato služba týká. Strana zákazníka, který tyto služby využívá, a strana výrobce, který tyto služby zprostředkovává. V případě zákazníka jsou v pravidlech zahrnuta i zařízení, kterými zákazník služby využívá, tzn. mobilní telefon a osobní počítač. V případě výrobce jsou zde doporučení hlavně na období raného vývoje, kdy je důležité už při fázi konceptu zahrnout prvky zabezpečení a zvažovat tak potenciální rizika.

5 Vyhodnocení praktického přínosu v dané oblasti

Vyhodnocení praktického přínosu pro oblast Connected Car je poslední kapitolou této práce a zhodnocuje celkovou přidanou hodnotu v oblasti bezpečnosti Connected Car. Ze strany uživatele to je přínos, který uživateli přináší užitek. V tomto případě to bude užitek z pocitu proaktivního bezpečí, tzn. pocit, kdy daný uživatel udělal vše, čeho byl schopen, aby předešel útokům.

Ze strany výrobce je největším ukazatelem samozřejmě prodej daného vozidla či řešení. V uvedení příkladu na rovinu Connected Caru, to je prodej vozidla na základě vhodného zabezpečení, tím míněno v porovnání dvou automobilek by si teoretický zákazník vybral to řešení, které je lépe zabezpečeno. V praxi spíše vozidlo, které prodejce dokáže lépe „prodat“ jako bezpečné.

Obrázek č. 21 nám ukazuje počet vozidel, která obsahují služby Connected Car. Graf také zobrazuje předpověď do roku 2021 a je z něj patrné, že počet vozidel vybavených službami Connected Car roste, tím lze říci, že každým rokem roste i počet potenciálních cílů.



Obrázek 21 - Počet vozidel vybavených službami Connected Car v letech 2015-2021
Zdroj: STATISTA (2016, https://www.statista.com/outlook/320/109/connected-car/united-states#market-revenue)

Počet cílů, či počet životů, které se každým rokem mohou stát terčem útoku. V roce 2017 je to 13,6 miliónů vozidel, což představuje milióny lidí, kteří jsou v potenciálním ohrožení. Proto je důležité pozastavit se nad tématem bezpečnosti řešení Connected Car. Tato práce netvrdí, že když výrobce dodrží všechna pravidla obsažená v kapitole pravidel pro výrobce, tak není možné vozidlo zneužít. Nicméně říká, kterých oblastí je potřeba se držet, a že je nesmírně důležité se zabývat bezpečností už od počátku vývoje, a ne nejdříve řešení vyvinout a až poté ho zabezpečit. Tato pravidla by především měla sloužit jako úvod do dané problematiky a další rozvoj hlubších znalostí by měl být pod dohledem specializovaných pracovníků.

Odpověď na otázku praktického přínosu je v případě pravidel pro zákazníka, jejich proaktivní ochrany proti nejběžnějším útokům a zkomplikování podmínek útočníkům, kteří se snaží pomocí těchto nejběžnějších podmínek vozidlo zneužít.

V případě pravidel pro výrobce je odpovědí, že tato práce slouží jako podpůrný prostředek při vývoji řešení Connected Car a úvod do problematiky bezpečnosti.

Závěr

V této práci bylo možno se setkat s problematikou bezpečnosti Connected Car služeb. Bezpečnost tohoto trendu je nesmírně důležitá část komplexní bezpečnosti vozidla, neboť přímo ovlivňuje vozidlo a účastníky v něm.

Cílem této bakalářské práce bylo vytvoření úvodu do dané problematiky a vytvoření pravidel pro bezpečné využití Connected Car služeb. První kapitola sloužila jako úvod do Connected Car služeb a podstatné informace o těchto službách. Daný oddíl čtenáře seznámil s možnostmi realizace Connected Car služeb a její spojitosti s IoT. Dále kapitola kategorizovala nabídku služeb a čtenář se zde mohl dočíst příklad automobilek, které vlastní Connected Car řešení a příklad společností, které tyto řešení dodávají externě.

Druhá kapitola se zabývala problematikou, která přímo souvisí s bezpečností, a to byla problematika standardizačních norem, které mají souvislost s Connected Car řešením. V této kapitole byly popsány dvě standardizační normy a byly zde vysvětleny základní principy těchto norem. První standard byl základní standard obecné bezpečnosti a druhý standard byl provázán přímo s Connected Car řešením. Závěrem kapitoly bylo porovnání těchto norem a stručný popis každé z nich.

Obsahem třetí kapitoly byla praktická analýza, vytvořená autrem práce, dané problematiky, která řešila technické prostředky automobilu, služeb a poté tato dvě odvětví „spojila“ v jedno. Výstupem této analýzy je celkové schéma Connected Caru, určení potenciálních rizik, které z tohoto schématu vyplynuly a jejich následné detailní odůvodnění.

Vytvoření pravidel pro bezpečné využití Connected Car je názvem čtvrté kapitoly, kde se daná pravidla kategorizovala na pravidla pro výrobce a pravidla pro uživatele/zákazníka. Výstupem této kapitoly je soubor pravidel, v případě pravidel pro výrobce jsou body, které slouží jako podpůrný prostředek pří vývoji Connected Car služeb. V případě pravidel pro uživatele jsou to pravidla, která slouží jako „manuál“ pro zacházení s Connected Car službami a jejich bezpečnějším použitím.

Závěrečná kapitola podtrhuje praktický přínos práce a říká, že práce jako taková není schopna pokrýt téma bezpečnosti Connected Caru ze všech možných pohledů. Práce je „vstupní branou“ do problematiky Connected Car bezpečnosti a slouží jako podklad pro rozsáhlejší práci v tomto odvětví.

Seznam použité literatury

[1] Internet *of Things to overtake mobile phones by 2018: Ericsson Mobility Report* [online]. Stockholm, Sweden: Press Releases, 2016 [cit. 2017-03-21]. Dostupné z: http://hugin.info/1061/R/2016987/748418.pdf

[2] Hacked home devices caused massive Internet outage. *USATODAY* [online]. USA: USATODAY, 2016 [cit. 2017-05-03]. Dostupné z: https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/

[3] DHANJANI, Nitesh. *Abusing the internet of things: blackouts, freakouts, and stakeouts*. O'Reilly Media, 2015. ISBN 1491902337.

[4] HU, Fei. *Security and privacy in internet of things (IoTs): models, algorithms, and implementations*. 1. CRC Press, 2016. ISBN 978-149-8723-183.

[5] KHURRAM, Muzaffar, Hemanth KUMAR, Adi CHANDAK, Varun SARWADE, Nitu ARORA a Tony QUACH. Enhancing Connected Car adoption: Security framework. In: *2016 International Conference on Connected Vehicles and Expo (ICCVE)* [online]. IEEE, 2016, s. 27-28 [cit. 2017-03-09]. DOI: 10.1109/ICCVE.2016.5. ISBN 978-1-5090-4524-2. Dostupné z: http://ieeexplore.ieee.org/document/7800179/ [6]

[6] BÉCSI Tamás, ARADI Szilárd a GÁSPÁR Peter. Security issues and vulnerabilities in Connected Car systems. In: *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)* [online]. IEEE, 2015, s. 477-482 [cit. 2017-03-09]. DOI: 10.1109/MTITS.2015.7223297. ISBN 978-9-6331-3140-4. Dostupné z: http://ieeexplore.ieee.org/document/7223297/

[7] *Connectivity - ŠKODA* [online]. ŠKODA Auto, 2016 [cit. 2017-03-14]. Dostupné z: http://www.skoda-auto.com/en/experience/product-features/connectivity/

[8] *Open Platform - Mojio* [online]. Mojio [cit. 2017-03-14]. Dostupné z: https://www.moj.io/connected-car-platform/

[9] SMITH, Craig. *The car hacker's handbook: a guide for the penetration tester*. San Francisco: No Starch Press, 2016. ISBN 1593277032.

[10] *Volkswagen Car-Net* [online]. T-Mobile [cit. 2017-03-14]. Dostupné z: http://volkswagen-carnet.com/int/en/start/app-overview.html

[11] *Software 8.0 | Tesla* [online]. Tesla, 2016 [cit. 2017-03-14]. Dostupné z: https://www.tesla.com/software

[12] *Chytré auto – T-mobile.cz* [online]. T-Mobile [cit. 2017-03-14]. Dostupné z: https://www.t-mobile.cz/chytre-auto

[13] *Zubie: We Make Driving Safer and Worry Free* [online]. Zubie [cit. 2017-03-14]. Dostupné z: http://zubie.com/

[14] The *Weak Spot Under the Hood* [online]. New York: The New York Times, 2015 [cit. 2017-03-21]. Dostupné z: https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html

[15] MILLER, Michael. *The Internet of things: how smart TVs, smart cars, smart homes, and smart cities are changing the world*. Indianapolis, Indiana: Que, 2015. ISBN 0789754002.

[16] UHER, Jaromír. Úvod do funkční bezpečnosti I: norma ČSN EN 61508. *Automa* [online]. 2004, **2004**(08), 1 [cit. 2017-03-09]. Dostupné z: http://automa.cz/cz/casopis-clanky/uvod-do-funkcni-bezpecnosti-i-norma-csn-en-61508-2004_08_32520_3609/

[17] ČSN EN 61508. *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností*. 2 ed. Český normalizační institut, 2011.

[18] SAE J3061. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. SAE International, 2016.

[19] HSU, Ching-Hsien, Feng XIA, Xingang LIU a Shangguang WANG. *Internet of Vehicles - Safe and Intelligent Mobility: Second International Conference, IOV 2015, Chengdu, China, December 19-21, 2015, Proceedings*. 1. China: Springer, 2015. ISBN 978-3-319-27292-4.

[20] *Security challenges and approaches in internet of things*. New York, NY: Springer Berlin Heidelberg, 2016. ISBN 9783319442297.

[21] HU, Fei. *Internet of vehicles - technologies and services: First International Conference, IOV, Beijing, China, September 1-3, 2014. Proceedings*. CRC Press, 2016. ISBN 3319111663.