

Slabiny v zabezpečení moderních dálkových systémů automobilů

Bc. Samuel Gábor

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Samuel Gábor
Osobní číslo:	A23391
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Slabiny v zabezpečení moderních dálkových systémů automobilů
Téma práce anglicky:	Weaknesses in the Security of Modern Car Remote Systems

Zásady pro vypracování

- Analyzujte současný stav moderních dálkových systémů v automobilech.
- Navrhněte experiment zabezpečení automobilů využívající technologii plovoucího kódu.
- Navrhněte sérii útoků s využitím Flipper Zero, které aplikujete na experiment.
- Proveďte analýzu navrženého experimentu a identifikujte slabiny.
- Prozkoumejte možnosti vzdáleného ovládání automobilu pomocí mobilních aplikací.

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

Seznam doporučené literatury:

1. MONK, Simon. Programming Arduino: getting started with sketches. Third edition. New York: McGraw Hill, [2023]. ISBN 978-1-264-67698-9.
2. KNIGHT, Alissa. Hacking connected cars: tactics, techniques, and procedures. 1st ed. Indianapolis, Indiana: Wiley, [2020]. ISBN 978-1-119-49173-6.
3. SAUTER, Martin. From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband. 4th ed. Wiley, 2021. ISBN 978-1-119-71469-9.
4. SUN, Shao-hui; HU, Jin-ling; PENG, Ying; PAN, Xue-ming; ZHAO, Li et al. Support for vehicle-to-everything services based on LTE. Online. IEEE Wireless Communications. 2016, roč. 23, č. 3, s. 4-8. ISSN 1536-1284.
5. SINGH, Pritpal; SETHI, Tanjot; BALABANTARAY, Bunil Kumar a BISWAL, Bibhuti Bhushan. Advanced vehicle security system. Online. In: 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE, 2015, s. 1-6. ISBN 978-1-4799-6817-6.

Vedoucí diplomové práce: **Ing. Stanislav Kovář, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **29. listopadu 2024**
Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou 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;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne 19.5.2025

.....
podpis autora

ABSTRAKT

Diplomová práca sa venuje analýze bezpečnostných slabín moderných diaľkových ovládačov automobilov využívajúcich technológiu plávajúceho kódu. Teoretická časť rozoberá princípy fungovania tejto technológie, ich vývoj, rozšírenie v automobilovom priemysle a známe typy útokov vrátane ich technickej realizácie. Osobitná pozornosť je venovaná nástrojom ako Arduino a Flipper Zero, ktoré umožňujú praktickú simuláciu útokov. Praktická časť dokumentuje experimenty zamerané na uskutočniteľnosť útoku na ovládače využívajúce technológiu plávajúceho kódu, ktoré boli realizované v laboratórnom prostredí a v reálnych podmienkach na vybraných cieľových systémoch. Práca zároveň hodnotí účinnosť bezpečnostných mechanizmov implementovaných v rôznych generáciách zariadení. V závere práca analyzuje získané výsledky a prináša odporúčania na zvýšenie bezpečnosti bezdrôtových uzamykacích systémov.

Kľúčové slová: diaľkové ovládače, plávajúci kód, slabiny, softvérovo definované rádio, Arduino, Flipper Zero

ABSTRACT

The master's thesis addresses the analysis of security weaknesses in modern automotive remote-control systems that utilize rolling code technology. The theoretical part explores the fundamental operating principles of this technology, its historical development, adoption in the automotive industry, and known categories of attacks, including their technical execution. Special attention is dedicated to tools such as Arduino and Flipper Zero, which facilitate hands-on simulation of security breaches. The practical part presents a series of experiments designed to evaluate the feasibility of attacks on rolling code-based remote systems, carried out under both laboratory conditions and real-world scenarios using selected target platforms. Furthermore, the thesis assesses the effectiveness of security mechanisms implemented across different generations of devices. The final chapter synthesizes the results obtained and proposes recommendations aimed at enhancing the robustness of wireless vehicle locking systems.

Keywords: remote controls, rolling code, vulnerabilities, software-defined radio, Arduino, Flipper Zero

POĎAKOVANIE

Moje poďakovanie patrí školiteľovi diplomovej práce Ing. Stanislavovi Kováňovi, PhD. za jeho odborné vedenie, metodické usmernenia a cenné rady, ktoré významne prispeli k odbornosti a kvalite pri vypracovaní diplomovej práce.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČASŤ	12
1 SÚČASNÝ STAV MODERNÝCH AUTOMOBILOVÝCH DIALKOVÝCH SYSTÉMOV.....	13
1.1 HISTORICKÉ POZADIE A VÝVOJ	13
1.2 VZNIK PKES	14
1.2.1 Neúmyselná aktivácia	14
1.2.2 Integrácia s elektronikou a telematikou vo vozidle.....	15
1.3 TECHNOLOGICKÉ PRINCÍPY A NORMY	15
1.3.1 Komunikačný zásobník a bezpečnostné vrstvy.....	16
1.4 TECHNOLOGIA PLÁVAJÚCEHO KÓDU	17
1.4.1 Synchronizačné okno	18
1.4.2 Kryptografické požiadavky	18
1.5 PREVLÁDAJÚCE ZRANITELNOSTI V SYSTÉMOCH DIALKOVÉHO OVLÁDANIA	19
1.5.1 Útoky s prehratím signálu	19
1.5.2 Reléové útoky.....	20
1.5.3 Rušenie signálu	21
1.5.4 Útok RollJam	21
1.5.5 Klonovanie kľúčov a reverzné inžinierstvo firmvéru	22
2 CONNECTED CARS.....	23
2.1 ARCHITEKTÚRA PREPOJENÝCH VOZIDIEL	24
2.1.1 Hardvérové komponenty	25
2.2 SOFTVÉROVÉ RIEŠENIA A EKOSYSTÉM.....	26
2.3 KOMUNIKAČNÉ PROTOKOLY A TECHNOLOGIE	27
2.3.1 V2X komunikácia	27
2.3.2 Bezdrôtové siete v automobiloch	28
2.4 KYBERNETICKÁ BEZPEČNOSŤ PREPOJENÝCH VOZIDIEL	29
2.5 NORMY KYBERNETICKEJ BEZPEČNOSTI V AUTOMOBILOVOM PRIEMYSLE	31
2.5.1 Odporúčania kybernetických opatrení do budúcnosti.....	32
3 VZDIALENÉ OVLÁDANIE VOZIDIEL PROSTREDNÍCTVOM MOBILNÝCH APLIKÁCIÍ.....	34
3.1 ARCHITEKTÚRA MOBILNÝCH APLIKÁCIÍ PRE SPRÁVU VOZIDIEL.....	34
3.2 FUNKCIE MOBILNÝCH APLIKÁCIÍ PRE SPRÁVU VOZIDIEL.....	35
3.2.1 Integrácia s infotainment systémami.....	37
3.3 BEZPEČNOSTNÉ RIZIKÁ PRI VYUŽÍVANÍ MOBILNÝCH APLIKÁCIÍ.....	37
3.4 MOŽNOSTI ÚTOKOV A ICH SIMULÁCIA	39
II PRAKTICKÁ ČASŤ	41

4	NÁVRH EXPERIMENTU ZABEZPEČENIA AUTOMOBILU S VYUŽITÍM TECHNOLOGIE PLÁVAJÚCEHO KÓDU	42
5	ZOSTROJENIE MODELU BEZDRÔTOVÉHO ZAMYKANIA VOZIDLA S TECHNOLOGIOU PLÁVAJÚCEHO KÓDU	43
5.1	VYSIELAČ	43
5.2	PRIJÍMAČ	44
5.3	PROGRAM PRE ARDUINO	45
5.3.1	Program pre vysielanie signálu	45
5.3.2	Program pre prijatie signálu	49
5.4	KOMPLETIZÁCIA MODELU	54
6	NÁVRH ÚTOKU NA BEZDRÔTOVÝ SYSTÉM S PLÁVAJÚCIM KÓDOM	56
6.1	POUŽITÉ ZARIADENIA A SOFTVÉR	56
6.1.1	Flipper Zero	56
6.1.2	HackRF One PortaPack H4M	56
6.1.3	RTL-SDR	57
6.1.4	Softvérové vybavenie	57
6.1.5	Momentum Firmware	57
6.1.6	SDRSharp	57
6.1.7	Universal Radio Hacker	57
6.2	PRIEBEH ÚTOKU	58
6.2.1	Scenár č. 1: Flipper Zero ako rušič, HackRF One PortaPack ako prijímač	59
6.2.2	Scenár č. 2: HackRF One PortaPack ako rušič, Flipper Zero ako prijímač	59
7	TESTOVANIE ÚTOKU	61
7.1	TESTOVANIE V LABORATÓRNYCH PODMIENKACH	61
7.2	TESTOVANIE V REÁLNYCH PODMIENKACH	63
7.3	VYHODNOTENIE ÚTOKOV	66
7.4	ODPORÚČANIA NA ZVÝŠENIE BEZPEČNOSTI	67
8	BEZPEČNOSTNÁ ANALÝZA MOBILNÝCH APLIKÁCIÍ	69
8.1	ZACHYTÁVANIE SIEŤOVEJ KOMUNIKÁCIE A SSL OCHRANA	69
8.2	STATICKÁ ANALÝZA APLIKÁCIÍ	71
8.3	ÚTOK NA LTE KOMUNIKÁCIU VOZIDLA	74
8.4	BEZPEČNOSTNÉ DOPADY A RIZIKÁ	77
	ZÁVER	79
	ZOZNAM POUŽITEJ LITERATÚRY	81
	ZOZNAM OBRÁZKOV	86
	ZOZNAM TABULIEK	87
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK	88

ÚVOD

História zabezpečenia automobilov je úzko prepojená s vývojom samotného automobilu. Od začiatku, keď boli autá jednoduchými strojmi s minimálnymi bezpečnostnými prvkami, až po dnešné sofistikované vozidlá vybavené pokročilými technológiami, sa evolúcia zabezpečenia áut formovala rastúcou hrozbou krádeží a neoprávneného prístupu. Kým v minulosti boli dostatočné bezpečnostné systémy ako zamykanie volantu, technologický pokrok priniesol nové výzvy a zraniteľnosti, ktoré vyžadujú neustálu inováciu.

V druhej polovici 20. storočia sa stali populárnymi riešeniami autoalarmy, ktoré odrádzali zlodejov zvukovými signálmi a viditeľnými upozorneniami. Koncom 20. storočia znamenali revolúciu v zabezpečení áut systémy bezklúčového prístupu, ktoré vodičom umožnili pohodlne zamykať a odomykať svoje vozidlá na diaľku pomocou rádiových frekvencií. Systémy, chránené technológiou plávajúcich kódov, poskytovali ďalšiu vrstvu bezpečnosti. Napriek týmto pokrokom však moderné diaľkové systémy zostávajú zraniteľné voči rôzne formy útokov od zachytenia signálu, útokov s prehratím signálu a reléovým útokom.

Dnešné vozidlá sú vybavené množstvom sofistikovaných bezpečnostných opatrení, vrátane imobilizérov a systémov GPS sledovania, ktoré významne znížili mieru krádeží áut. Ako sa technológie vyvíjajú, tak sa zdokonaľujú aj metódy útočníkov. So vzostupom bezdrôtových komunikačných technológií, ako sú Bluetooth a LTE, útočníci už nepotrebujú fyzický prístup k vozidlu. Zraniteľnosti diaľkových systémov môžu zneužiť aj na väčšiu vzdialenosť, čím umožnia odcudzenie vozidla.

Cieľom tejto práce je preskúmať a riešiť nové hrozby a slabé miesta v zabezpečení moderných diaľkových systémov áut. Zameraním sa na systémy využívajúce technológiu plávajúcich kódov a testovaním ich náchylnosti na útoky pomocou nástrojov ako Flipper Zero, má táto práca prispieť k hlbšiemu pochopeniu zraniteľností v zabezpečení áut. Práca sa okrem toho zaoberá aj bezpečnostnými rizikami spojenými s mobilnými aplikáciami používanými na diaľkové ovládanie vozidiel a navrhne možné riešenia na zmiernenie týchto rizík.

I TEORETICKÁ ČASŤ

1 SÚČASNÝ STAV MODERNÝCH AUTOMOBILOVÝCH DIAĽKOVÝCH SYSTÉMOV

Automobilové diaľkové systémy zahrnujú funkcie zamykania, odomykania a štartovania motora, ktoré predstavujú základné spojenie medzi vodičom a vozidlom. V posledných desaťročiach prešli tieto systémy výrazným vývojom od jednoduchých mechanických kľúčov až po vysoko sofistikované, často kryptograficky zabezpečené bezdrôtové protokoly. Hlavnou hnacou silou inovácií bolo síce pohodlie používateľov, no ich vývoj formovali neustále preteky v súperení medzi výskumníkmi v oblasti bezpečnosti a potenciálnymi útočníkmi.

1.1 Historické pozadie a vývoj

Historický vývoj zabezpečenia vozidiel predstavuje významný míľnik vo vývoji automobilového priemyslu. Po desaťročia boli mechanické kľúče základným a takmer univerzálnym nástrojom na zamykanie, odomykanie a štartovanie vozidiel. Ich konštrukcia bola relatívne jednoduchá a spoľahlivá a to ich robilo široko využívanými. Mechanické kľúče fungovali na princípe presného usporiadania drážok a zárezov, ktoré zodpovedali špecifickému mechanizmu vo vnútri zámku. Napriek ich účelnosti však tieto kľúče mali významné nedostatky. Hlavným nedostatkom bola náchylnosť na fyzické poškodenie a neoprávnené duplikovanie. Tento nedostatok bol obzvlášť zrejímavý v 80. rokoch 20. storočia, kedy sa významne zvýšil počet krádeží vozidiel. Táto situácia podnietila výrobcov automobilov, aby sa sústredili na bezpečnejšie riešenia zabezpečenia vozidiel.

Rastúca potreba zlepšiť ochranu vozidiel a súčasne zvýšiť komfort užívateľov otvorila dvere novým technológiám. Prvým zásadným prelomom v tejto oblasti bol vznik systémov Remote Keyless Entry (RKE), teda diaľkového bezkľúčového vstupu. Táto technológia umožnila vodičom odomykať a zamykať vozidlo stlačením tlačidla na diaľkovom ovládači. Prvé systémy RKE, ktoré sa objavili v 80. rokoch, fungovali na princípe vysielania nízko-frekvenčného rádiového signálu. Tento signál niesol jednoduchý identifikačný kód, ktorý bol prijatý a overený riadiacou jednotkou vo vozidle. Tieto systémy predstavovali značný pokrok v porovnaní s tradičnými mechanickými zámkami, no ich počiatočné riešenia mali obmedzenia. Prvé generácie RKE systémov sa spoliehali na jednoduché a nešifrované kódy, ktoré boli relatívne ľahko predvídateľné a zraniteľné voči rôznym formám útokov. Útočníci mohli zachytiť signály z diaľkového ovládača pomocou rádiového zariadenia a následne ich použiť na neoprávnený prístup k vozidlu. Tento problém poukázal

na dôležitosť zlepšenia šifrovania a bezpečnostných protokolov v nasledujúcich generáciách systémov RKE. [1], [2]

Bezpečnostné nedostatky prvých bezkľúčových systémov motivovali automobilových výrobcov k hľadaniu efektívnejších spôsobov zabezpečenia. V 90. rokoch sa začali implementovať pokročilejšie technológie, ako napríklad plávajúce kódy (rolling codes), ktoré pri každom použití porovnávali kód uložený v riadiacej jednotke a následne inkrementovali počítadlo. Tento prístup dramaticky znížil riziko zachytenia signálov a možnosti neoprávneného prístupu. Do diaľkových ovládačov začali byť integrované bezpečnejšie protokoly šifrovania, ktoré poskytovali vyššiu úroveň ochrany. Vývoj týchto technológií prispel okrem bezpečnosti aj k zvýšeniu používateľského komfortu. Systémy RKE nielenže eliminovali potrebu manuálnej manipulácie s kľúčom, ale tiež umožnili ďalšie funkcie ako je otváranie kufra alebo vyhľadávanie vozidla na parkovisku. Táto kombinácia bezpečnosti a pohodlia sa stala dominantnou vlastnosťou, ktorú si zákazníci obľúbili a ktorú očakávajú od moderných automobilov. [2]

1.2 Vznik PKES

Systémy pasívneho bezkľúčového vstupu a štartovania (PKES, alebo Passive Keyless Entry and Start) predstavujú významnú technologickú inováciu, ktorá kombinuje pohodlie a pokrokové riešenia v automobilovej bezpečnosti. Tieto systémy eliminovali potrebu manuálneho ovládania kľúčov a umožnili vodičom vstup do vozidla bez použitia tlačidiel a následné naštartovanie stlačením tlačidla v interiéri vozidla. Na princípe rádiových komunikácií na krátku vzdialenosť PKES systém deteguje prítomnosť autorizovaného kľúča v blízkosti vozidla a umožní automatickú interakciu akou je odomknutie dverí a štart motora. Táto technológia sa stala kľúčovou z hľadiska komfortu, priniesla aj nové bezpečnostné výzvy, ktoré si vyžiadali ďalšie inovácie a riešenia.

1.2.1 Neúmyselná aktivácia

Jedným z problémom prvých generácií PKES systémov bola neúmyselná aktivácia, ktorá znižovala celkovú bezpečnosť vozidla. Ak bol kľúč ponechaný vo vnútri vozidla alebo veľmi blízko exteriéru, napríklad v taške položenej blízko dverí, mohol systém vozidlo automaticky odomknúť. Týmto sa zvyšovalo riziko neoprávneného prístupu alebo krádeže vozidla, najmä v preplnených mestských oblastiach či na miestach s vysokou mierou kriminality. Automobilových výrobcov podnietili uvedené nedostatky k vývoju technológií

na zníženie eliminácie uvedených problémov, vrátane implementácie senzorov priblíženia a algoritmov na presnejšie určovanie polohy kľúča. [3]

1.2.2 Integrácia s elektronikou a telematikou vo vozidle

Moderné automobily sa vyznačujú rastúcou komplexnosťou elektronických a softvérových systémov, čo má zásadný vplyv na technológie zabezpečenia a ich zraniteľnosť. Základným stavebným kameňom dnešných vozidiel sú elektronické riadiace jednotky (ECU), ktoré riadia prakticky všetky systémy od motora, brzdového systému a bezpečnostných prvkov až po informačné systémy. Typický moderný automobil obsahuje desiatky, niekedy až stovky ECU, ktoré spolu komunikujú prostredníctvom zberníc, ako je Controller Area Network (CAN) alebo ethernet a ktoré umožňujú vysokorýchlostný prenos údajov medzi systémami. [1]

Integrácia telematiky do vozidiel priniesla novú dimenziu funkčnosti a konektivity. Telematické platformy umožňujú prenos údajov v reálnom čase. To otvára nové možnosti akými sú vzdialená diagnostika, sledovanie polohy a aktualizácie softvéru Over-the-Air (OTA). OTA aktualizácie, ktoré sú bežne využívané na opravu bezpečnostných chýb alebo pridávanie nových funkcií, ale zároveň predstavujú riziko kybernetických útokov. Potencionálni útočníci môžu využiť slabé miesta v softvérovej architektúre vozidla na získanie prístupu k jeho systémom, čo by mohlo viesť k strate kontroly nad hlavnými funkciami. [4], [5]

1.3 Technologické princípy a normy

Technologické princípy automobilových diaľkových systémov odrážajú kombináciu sofistikovaných rádiových technológií, modulácií a bezpečnostných štandardov, ktoré boli vyvinuté na zabezpečenie pohodlia, spoľahlivosti a bezpečnosti. Frekvenčné pásma 315 MHz, 433,92 MHz a 868 MHz sú medzinárodne štandardizované pre priemyselné, vedecké a medicínske účely. Tieto frekvencie boli vybrané najmä pre ich schopnosť pokrývať veľké vzdialenosti a efektívne prenikať cez prekážky, čo je dôležité aj pre automobilové aplikácie. [2]

V oblasti modulácie sa používa ASK (Amplitude Shift Keying) a FSK (Frequency Shift Keying). Tieto metódy umožňujú prenos digitálnych informácií cez analógový rádiový signál. Prvé generácie systémov RKE používali jednoduchšie metódy a nešifrované prenosi. Moderné systémy čelia novým výzvam v oblasti kybernetickej bezpečnosti a vyžadujú

implementáciu pokročilých šifrovacích techník a protokolov na ochranu údajov pred neužitím.

1.3.1 Komunikačný zásobník a bezpečnostné vrstvy

Automobilová bezdrôtová komunikácia je navrhnutá ako viacvrstvový systém, ktorý zahŕňa fyzickú vrstvu, linkovú vrstvu, aplikačnú, prípadne bezpečnostnú vrstvu a kryptografickú vrstvu.

1.3.1.1 Fyzická vrstva

Fyzická vrstva predstavuje základ komunikácie a obsahuje základné rádiové charakteristiky a metódy modulácie. V tejto vrstve sa dáta prenášajú prostredníctvom rádiových vln pomocou modulácií ASK a FSK, ktoré umožňujú efektívne kódovanie digitálnych údajov. Vylepšené rádiové obvody v moderných systémoch umožňujú zlepšený dosah, spoľahlivosť a súčasne minimalizujú spotrebu energie, čo je dôležité pre diaľkové ovládače napájané batériami. [6]

1.3.1.2 Linková vrstva

Úlohou linkovej vrstvy je spravovať synchronizáciu medzi vysielateľom (kľúčom) a prijímačom (vozidlom). Táto vrstva deteguje chyby prenosu a zabezpečuje rámcovanie údajov, aby boli dáta správne interpretované vyššími vrstvami. Synchronizácia je obzvlášť dôležitá pre systémy využívajúce plávajúce kódy, keď každá interakcia medzi kľúčom a vozidlom generuje nový jedinečný kód. Ak sa kód v rámci tejto vrstvy nesynchronizuje správne, systém môže považovať prenos za neplatný. [7]

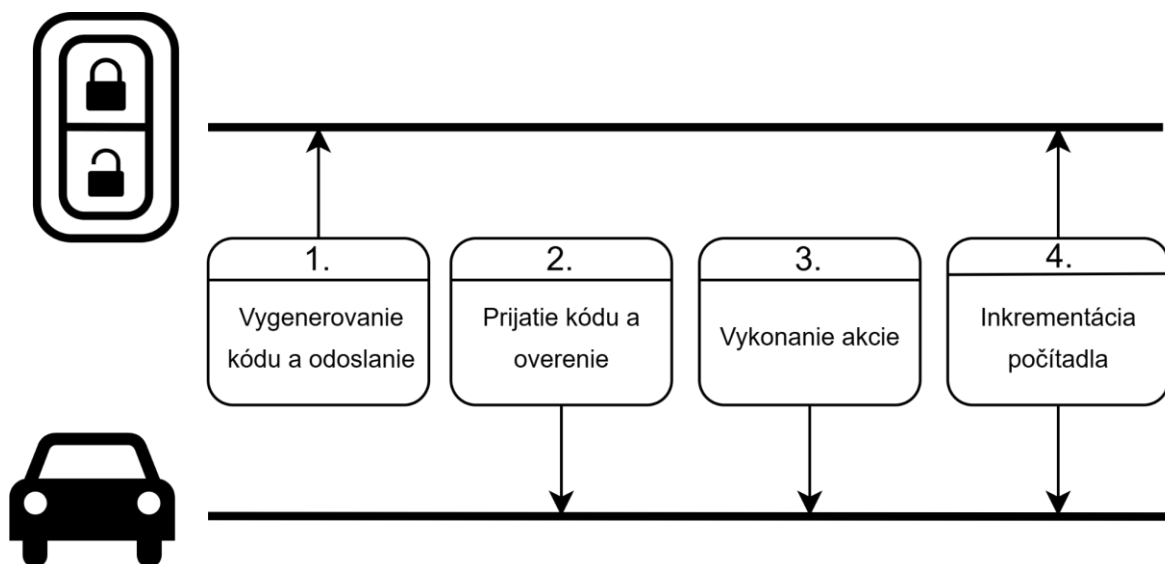
1.3.1.3 Aplikačná a bezpečnostná vrstva

Táto vrstva integruje rozhodovaciu logiku a kryptografické algoritmy, ktoré zabezpečujú autentifikáciu a ochranu pred neoprávneným prístupom. Spracúva šifrovanie a dešifrovanie údajov a implementuje pokročilé šifrovacie protokoly ako sú AES (Advanced Encryption Standard) alebo proprietárne algoritmy. Okrem šifrovania zabezpečuje aj ochranu proti útokom na základe opakovania signálu a reléovým útokom. Efektívnosť bezpečnostných opatrení na tejto úrovni závisí od viacerých faktorov. Schopnosť čipov používaných v diaľkových ovládačoch je rozhodujúca pre bezpečné uchovanie šifrovacích kľúčov, pretože ich kompromitovanie môže vystaviť celý bezpečnostný systém útokom. Rovnako dôležitá je integrita samotných kryptografických algoritmov. Tieto musia byť navrhnuté tak,

aby odolali širokému spektru útokov vrátane brute-force techník a pokročilých matematických analýz. Ďalším dôležitým prvkom je prevencia zneužitia na základe opakovania. Moderné systémy preto implementujú plávajúce kódy, ktoré generujú jedinečný kód pre každú operáciu. V prípade, ak je kód neoprávnene zachytený, nie je možné ho opakovane použiť a tým sa riziko zneužitia výrazne znižuje. Táto vrstva zohráva rozhodujúcu úlohu v zabezpečení komunikácie a ochrane pred rôznymi bezpečnostnými hrozbami, čím výrazne posilňuje celkovú kryptografickú odolnosť systému. [5], [6], [7]

1.4 Technológia plávajúceho kódu

Technológia plávajúceho kódu, po anglicky rolling code, je jedným z najdôležitejších bezpečnostných prvkov moderných automobilových systémov. Tento mechanizmus využíva jednorazové kódy, ktoré sa generujú inkrementáciou počítadla v kombinácii s kryptografickou funkciou. Počítadlo predstavuje vnútornú premennú, ktorá sa pri každom stlačení tlačidla na diaľkovom ovládači zvýši o určitú hodnotu. Zabráňuje sa tým opakovaniu alebo zneužitiu prenosu. Pri každom použití kľúča sa počítadlo zvýši a výsledný kód sa odošle do vozidla, kde sa overí na základe predpovedaného rozsahu počítadiel. Ak sa kód nachádza v preddefinovanom synchronizačnom okne, systém kód akceptuje a vykoná požadovanú operáciu akou je odomknutie alebo štartovanie vozidla. [2]



Obrázok 1 Priebeh komunikácie pomocou plávajúceho kódu

(zdroj: vlastný)

1.4.1 Synchronizačné okno

Synchronizácia medzi kľúčom a prijímačom predstavuje jednu z najväčších technických výziev pri implementácii plávajúcich kódov. Keď používateľ stlačí tlačidlo na kľúči mimo dosahu vozidla, počítaadlo v kľúči sa posunie vpred, ale vozidlo tento prenos nezaznamená. Výrobcovia preto využívajú synchronizačné okná, ktoré umožňujú prijímaču akceptovať kódy v určitom rozsahu predpovedaných hodnôt. Typické synchronizačné okno môže pokrývať desiatky až stovky krokov, čím sa minimalizuje riziko odmietnutia legitímnych prenosov.

Napriek tomu môže dôjsť k desynchronizácii, pri ktorej sa počítaadlo kľúča posunie mimo synchronizačné okno, čo vedie k zamietnutiu legitímnych prenosov. V takom prípade je potrebná manuálna opätovná synchronizácia systému, čo môže byť pre používateľov nepraktické. Okrem prirodzených problémov so synchronizáciou existuje aj riziko desynchronizačných útokov, pri ktorých útočníci zámerne narušia synchronizáciu medzi kľúčom a vozidlom. Takéto narušenie môže viesť k tomu, že systém buď akceptuje neoprávnené prenosy, alebo naopak odmietne legitímne operácie. [2]

1.4.2 Kryptografické požiadavky

Návrh plávajúceho kódu musí byť nielen bezpečný, ale aj praktický, pretože je implementovaný v prostredí s výraznými obmedzeniami hardvéru, energie a dlhodobej odolnosti. Kryptografické algoritmy používané v týchto systémoch musia byť optimalizované na efektivitu bez zníženia úrovne bezpečnosti. Jednou z hlavných výziev je obmedzený spracovateľský výkon, keďže mikrokontroléry automobilovej triedy často disponujú nižším výpočtovým výkonom. To znamená, že zložité šifrovacie algoritmy môžu byť nepraktické, a preto sa uprednostňujú optimalizované algoritmy alebo hardvérové akcelerátory, ktoré umožňujú efektívne spracovanie kryptografických operácií. [8]

Ďalším dôležitým faktorom je energetická efektivita, keďže kľúče sú napájané malými batériami s obmedzenou kapacitou. Použitie výpočtovo náročných algoritmov môže výrazne skrátiť životnosť batérie, preto sa kladie dôraz na návrh šifier s nízkou spotrebou energie. Dlhodobá bezpečnosť je pritom nevyhnutná, keďže životnosť automobilov často presahuje 10 až 15 rokov. Kryptografické algoritmy preto musia byť navrhnuté tak, aby zostali odolné voči vývoju nových útokov a technológií počas celého obdobia ich používania. Prípadná zastaranosť algoritmov by mohla predstavovať vážne bezpečnostné riziko. [1]

Pri návrhu plávajúceho kódu zohrávajú zásadnú úlohu viaceré premenné. Veľkosť počítadla ovplyvňuje generovanie jedinečných kódov. Väčšie počítadlá znižujú pravdepodobnosť náhodnej desynchronizácie, ale zároveň môžu zvýšiť výpočtovú náročnosť a pamäťové nároky systému. Dĺžka kľúča je ďalším z rozhodujúcich faktorov ovplyvňujúcim zraniteľnosť systému, keďže dlhšie kryptografické kľúče poskytujú vyššiu odolnosť voči útokom hrubou silou (brute-force útokom). Bežnou praxou je použitie kľúčov s dĺžkou minimálne 128 bitov. Dĺžka sa môže prispôbiť potrebám systému. Rovnako dôležitý je aj výber algoritmu. Záruku bezpečnosti poskytuje použitie štandardných kryptografických algoritmov ako je AES, keďže tieto algoritmy boli dôkladne testované a validované odbornou komunitou. Proprietárne algoritmy môžu obsahovať skryté slabiny, ktoré sa dajú odhaliť až po ich nasadení do reálneho prostredia. [2] Efektívny návrh plávajúceho kódu musí zabezpečiť rovnováhu medzi bezpečnosťou, výpočtovou náročnosťou a spotrebou energie, aby systém dokázal čeliť aktuálnym aj budúcim bezpečnostným hrozbám.

1.5 Prevládajúce zraniteľnosti v systémoch diaľkového ovládania

Moderné systémy diaľkového ovládania síce priniesli pokrok v oblasti automobilovej bezpečnosti a komfortu, no stále obsahujú slabé miesta, ktoré môžu byť predmetom zneužitia zo strany útočníkov. Tieto zraniteľnosti zahŕňajú techniky na obídenie bezpečnostných mechanizmov akými sú útoky s prehnaním signálu, reléové útoky, rušenie signálu, RollJam útok, klonovanie kľúčov a reverzné inžinierstvo firmvéru. Každá z týchto metód má svoj špecifický spôsob fungovania, dôsledky a možné protiopatrenia.

1.5.1 Útoky s prehratím signálu

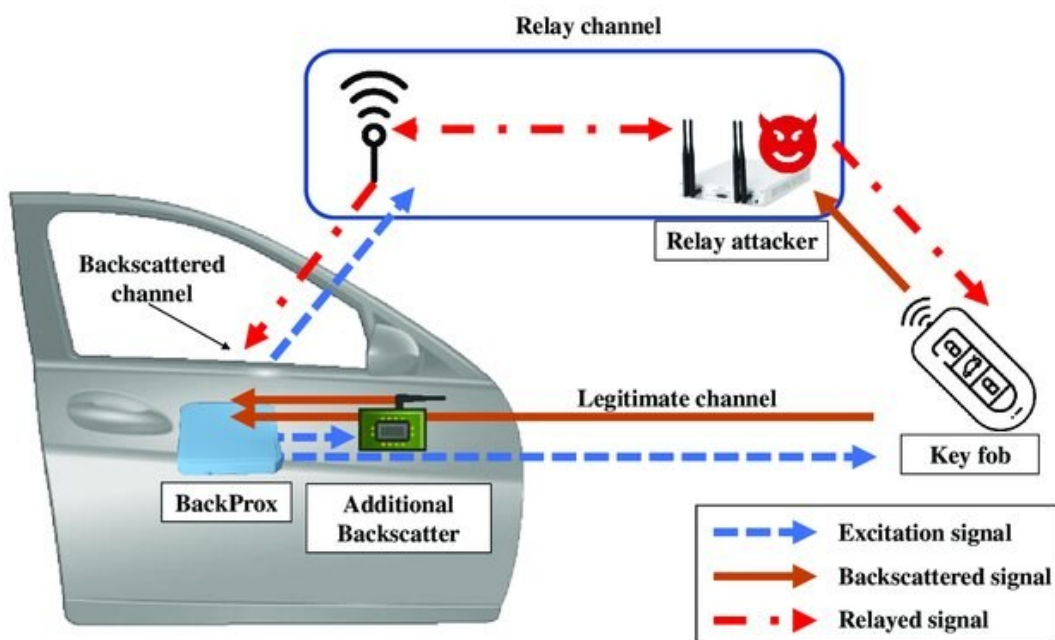
Útoky s prehratím signálu predstavujú závažnú bezpečnostnú hrozbu, pri ktorej útočník zachytí rádiový signál z kľúča a prehrá ho neskôr s cieľom neoprávnene získať prístup k vozidlu. Staršie systémy využívajúce pevný kód sú obzvlášť zraniteľné, pretože neimplementujú jednorazové kódy ani kryptografické ochrany a to ich robí ľahko zneužiteľnými. [1], [2]

V modernejších systémoch technológia plávajúcich kódov síce eliminuje mnohé riziká spojené s týmito útokmi, no nesprávna implementácia alebo chyby v synchronizácii môžu stále vytvárať príležitosti pre útočníkov. Ak je napríklad synchronizačné okno príliš široké, môže dôjsť k zneužitiu bezpečnostných medzier. Na ochranu pred týmito útokmi je

nevyhnutné správne implementovať šifrovanie a jednorazové kódy, ktoré zabezpečia, že každý prenesený signál je unikátny a nemožno ho opakovane použiť. Rovnako dôležité je obmedzenie synchronizačného okna na bezpečný rozsah, čím sa minimalizuje možnosť zneužitia systému neoprávneným prístupom.

1.5.2 Reléové útoky

Reléové útoky, po anglicky nazývané relay attacks, patria medzi najznámejšie a najúspešnejšie metódy krádeže vozidiel vybavených systémami bezklúčového vstupu. Pri tomto type útoku útočník zachytáva signály z kľúča majiteľa vozidla, ktorý sa môže nachádzať vo vrecku, taške alebo v dome a následne ich prenáša do blízkosti vozidla. Tento mechanizmus umožňuje vozidlu detegovať signál a chybné predpokladať, že sa kľúč nachádza v jeho dosahu. Výsledkom je, že sa vozidlo odomkne a umožní sa naštartovanie, čím sa výrazne uľahčí jeho krádež. [3] Tento spôsob útoku je mimoriadne účinný, pretože nevyžaduje kompromitáciu šifrovania ani fyzický prístup ku kľúču.



Obrázok 2 Reléový útok na systém PKES

(zdroj:[9])

Na ochranu pred reléovými útokmi sa využívajú rôzne bezpečnostné opatrenia. Senzory priblíženia umožňujú presnejšie určiť polohu kľúča a zabrániť tým aktivácii vozidla pri detekcii podozrivých signálových prenosov. Časovo obmedzené autentifikačné protokoly dokážu zabrániť neoprávnenému použitiu signálu tým, že overujú jeho platnosť len v krátkom časovom intervale. Okrem toho používanie ochranných puzdier na kľúče, ako

sú faradayové obaly, môže účinne blokovat' rádiové signály a zamedziť ich zachyteniu útočníkmi.

1.5.3 Rušenie signálu

Rušenie signálu je typ útoku, pri ktorom útočník vysiela silné alebo náhodné signály na rovnakých frekvenciách ako systém vozidla a tak naruší komunikáciu medzi kľúčom a vozidlom. Tento útok môže spôsobiť, že používateľ bude musieť opakovane stlačiť tlačidlo na kľúči, čím vznikajú príležitosti na zachytenie signálu a jeho následné zneužitie. Rušenie signálu môže navyše slúžiť ako úvodná fáza sofistikovanejších útokov akými sú RollJam alebo reléové útoky, ktoré umožňujú neoprávnené získanie prístupu k vozidlu.

Na ochranu pred rušením signálu sa využívajú rôzne bezpečnostné opatrenia. Frekvenčné hoppingové technológie dynamicky menia komunikačné frekvencie medzi kľúčom a vozidlom a tým sťažujú útočníkom efektívne rušenie. Ďalším dôležitým opatrením je detekcia anomálií v rádiovom prostredí, ktorá dokáže identifikovať podozrivé rušenie signálu, včas spustiť varovanie a tak minimalizovať riziko útoku. [10]

1.5.4 Útok RollJam

Útok RollJam je sofistikovaná metóda prekonania bezdrôtového zabezpečenia vozidiel využívajúcich plávajúci kód. Tento typ útoku obchádza bezpečnostný princíp tým, že útočník zachytí nový autentifikačný kód ešte pred jeho doručením prijímaču a zároveň ruší prenos, čím prinúti používateľa zopakovať prenos. V dôsledku toho získava dva platné kódy. Prvý okamžite prehrá na získanie prístupu k vozidlu, druhý si ponechá na neskoršie použitie.

Konkrétny útok prebieha v troch krokoch: najskôr útočník ruší komunikáciu medzi ovládačom a vozidlom, aby zabránil prijatiu signálu. Zároveň počas rušenia zachytáva vysielané autentifikačné signály, pričom pri opakovanom stlačení tlačidla získa dve rozdielne, ale platné sekvencie. Následne zruší rušenie a prehrá jeden zo zachytených signálov, ktorý vozidlo akceptuje ako legitímny. Útočník si pritom ponecháva druhý signál, ktorý môže použiť kedykoľvek v budúcnosti aj o niekoľko dní neskôr, pretože ho systém ešte nezaregistroval. [10], [11]

Hlavným nebezpečenstvom RollJam útoku je jeho schopnosť efektívne obísť jednorazovú platnosť plávajúceho kódu bez potreby akéhokoľvek dešifrovania. Útočník iba zachytáva a presne prehráva signál, bez spätnej analýzy či znalosti kryptografickej štruktúry.

Celý proces je pre používateľa neviditeľný. Vozidlo síce nereagovalo hneď na prvý pokus, no po druhom stlačení ovládača (útočník prehral signál) zareagovalo, čo sa dá ľahko pripísať poruche alebo slabej batérii v ovládači. Neexistuje žiadny zvukový, vizuálny ani fyzický náznak toho, že bol jeho signál medzičasom zachytený a zneužitý.

Na ochranu pred týmto typom útoku je nevyhnutné zaviesť dodatočné bezpečnostné opatrenia. Medzi najúčinnšie patria viacfaktorová autentifikácia, biometrické overenie, alebo pokročilé kryptografické techniky, ktoré dynamicky menia počiatočnú hodnotu (seed) pri každom generovaní kódu. Takéto riešenia môžu výrazne sťažiť neoprávnený prístup a eliminovať možnosť zneužitia zachytených kódov.

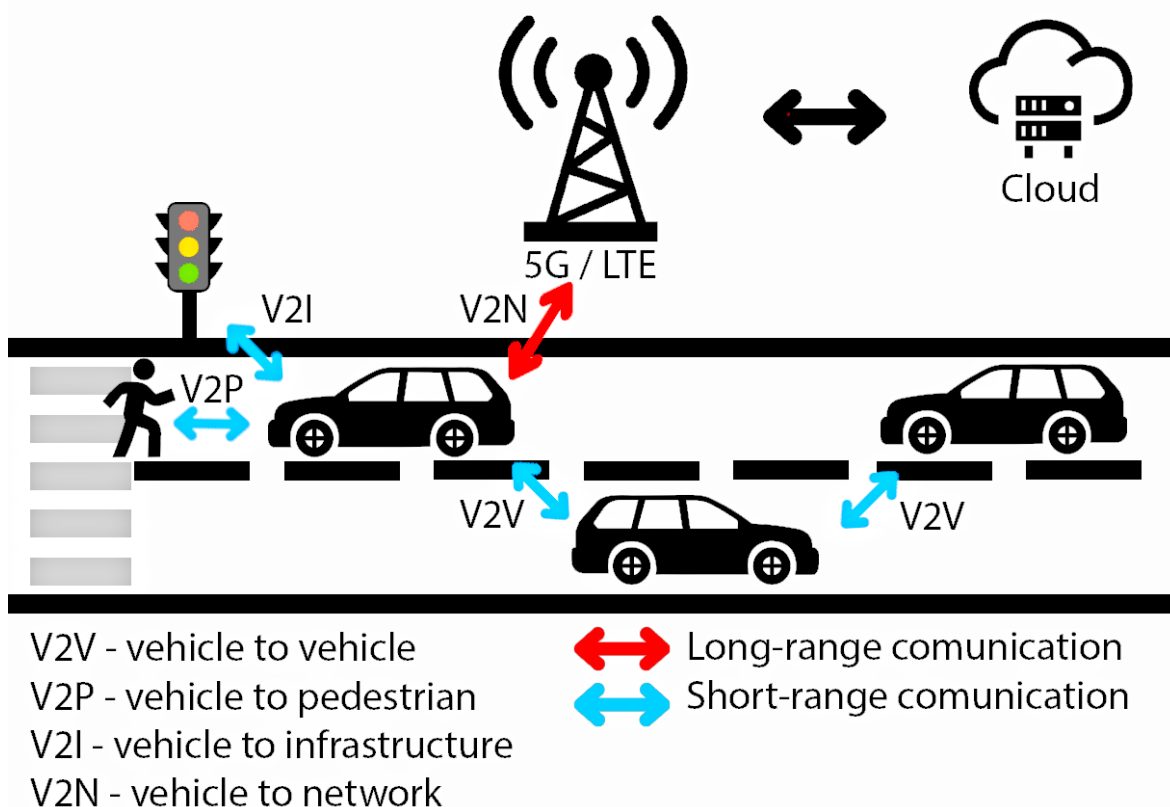
1.5.5 Klonovanie kľúčov a reverzné inžinierstvo firmvéru

Moderné kľúče obsahujú vlastný firmvér, ktorý implementuje kryptografické algoritmy a logiku potrebnú na generovanie a validáciu kódov. Ak sa útočníkom podarí tento firmvér analyzovať alebo napodobniť, môžu vytvoriť klon kľúča a získať neoprávnený prístup k vozidlu. Jednou z hlavných metód klonovania je reverzné inžinierstvo, pri ktorom útočník získa fyzický prístup ku kľúču, prípadne vozidlu a podrobne analyzuje jej firmvér. Tento proces umožňuje odhaliť kryptografické konštanty, seed hodnoty a ďalšie citlivé informácie, ktoré sú rozhodujúce pre autentifikáciu. Ďalšou metódou je analýza prenosov, pri ktorých útočník zachytáva dostatočné množstvo komunikácie medzi kľúčom a vozidlom s cieľom identifikovať vzory a napodobniť autentifikáciu. [12]

2 CONNECTED CARS

Prepojené vozidlá, známe aj ako connected cars, predstavujú jednu z najvýznamnejších inovácií v automobilovom priemysle. Tieto vozidlá disponujú schopnosťou obojsmernej komunikácie s externými systémami, čo im umožňuje interakciu s infraštruktúrou, ostatnými vozidlami i chodcami. Táto konektivita je založená na pokročilých technológiách akými sú 5G siete, Internet of Things (IoT), cloud computing a umelej inteligencii, vďaka čomu môžu prepojené vozidlá poskytovať širokú škálu funkcií zvyšujúcich bezpečnosť, efektivitu a komfort jazdy.

Koncepcia prepojených vozidiel vychádza z myšlienky digitalizácie a inteligentnej mobility, ktorá umožňuje plynulé prepojenie medzi vozidlom a jeho okolím. Vozidlá môžu zdieľať a prijímať údaje prostredníctvom rôznych komunikačných protokolov, čím sa zvyšuje efektivita dopravy a bezpečnosť na cestách. Tento koncept vytvára základ pre rozvoj autonómnych vozidiel a inteligentných dopravných systémov, ktoré budú schopné v reálnom čase analyzovať premávku a optimalizovať jazdu na základe aktuálnych podmienok. [5]



Obrázok 3 V2X komunikácia

(zdroj: vlastný)

Vývoj prepojených vozidiel možno sledovať od konca 20. storočia, v čase, keď sa v automobilovom priemysle začali objavovať prvé formy telematických systémov. V roku 1996 spoločnosť General Motors predstavila systém OnStar, ktorý umožňoval núdzovú komunikáciu a lokalizáciu vozidla. [13] Počas prvej dekády sa do vozidiel začali integrovať technológie ako Bluetooth, Wi-Fi a mobilné dátové pripojenie, rozšírili sa tak možnosti konektivity. S nástupom 4G a 5G sietí sa otvorili nové príležitosti pre rozvoj inteligentných funkcií, ktoré umožňujú pokročilú navigáciu, prediktívnu údržbu, či autonómne jazdné režimy. V súčasnosti sú prepojené vozidlá schopné komunikovať s inteligentnými mestskými infraštruktúrami a využívať umelú inteligenciu na optimalizáciu jazdných parametrov a energetickej účinnosti. Narastajúci rozvoj týchto technológií naznačuje, že bezpečnosť a efektivita autonómnej dopravy budú závisieť od úrovne prepojenosti dopravných a technologických systémov. Jednou z najvýznamnejších výhod konektivity je možnosť vzdialených softvérových aktualizácií, ktoré umožňujú výrobcovi implementovať nové funkcie a bezpečnostné opatrenia bez potreby fyzického zásahu do vozidla. Ďalším dôležitým aspektom je využitie konektivity na zber a analýzu dát o správaní sa vodičov za jazdy, čo umožní lepšie prispôsobenie vozidiel individuálnym potrebám a zároveň môže prispieť k vývoju autonómnych jazdných systémov.

Pre výrobcov automobilov prináša konektivita množstvo nových obchodných príležitostí. Zber údajov o jazdných návykoch a prevádzkových podmienkach umožňuje automobilkám optimalizovať svoje produkty a ponúkať personalizované služby zákazníkom. Výrobcovia môžu taktiež implementovať nové obchodné modely založené na softvérových predplatných a vzdialených aktualizáciách a generovať dodatočné príjmy aj po predaji vozidla. Prepojené vozidlá im umožňujú okrem toho efektívnejšie spravovať servisné a záručné programy a tak znižovať náklady na údržbu a zlepšovať zákaznícku spokojnosť.

2.1 Architektúra prepojených vozidiel

Architektúra prepojených vozidiel je komplexný ekosystém skladajúci sa z hardvérových a softvérových komponentov, ktoré umožňujú vozidlám komunikovať, spracovávať dáta a poskytovať rôzne inteligentné funkcie. Tento systém je založený na integrácii senzorov, výpočtových jednotiek a komunikačných technológií s cloudovými službami a operačnými systémami. Zabezpečuje tým vysokú úroveň konektivity a automatizácie.

2.1.1 Hardvérové komponenty

Hardvérová infraštruktúra prepojených vozidiel pozostáva z viacerých kľúčových komponentov, ktoré zabezpečujú zber, spracovanie a prenos údajov medzi vozidlom, infraštruktúrou a externými systémami.

Jednou z najdôležitejších častí hardvérového riešenia sú senzory a IoT zariadenia, ktoré zohrávajú zásadnú úlohu pri monitorovaní okolia a internej prevádzky vozidla. Medzi tieto zariadenia patria radarové, Light Detection And Ranging (LIDAR), ultrazvukové senzory a kamery, ktoré umožňujú vozidlám detegovať objekty, sledovať jazdné pruhy a predchádzať kolíziám. IoT zariadenia poskytujú dodatočné údaje o stave vozidla akými sú teplota motora, tlak v pneumatikách, spotreba paliva a tak prispievajú k prediktívnej údržbe a optimalizácii výkonu.

Ďalším významným komponentom architektúry prepojených vozidiel sú riadiace jednotky, medzi ktoré patria elektronické riadiace jednotky (ECU) a telekomunikačné riadiace jednotky (TCU). ECU spravujú rôzne aspekty prevádzky vozidla, od riadenia motora po bezpečnostné systémy, zatiaľ čo TCU je primárne zodpovedná za konektivitu vozidla a jeho schopnosť komunikovať s externými sieťami. TCU zabezpečuje dátový prenos medzi vozidlom a cloudovými službami a týmto umožňuje vzdialený prístup k diagnostike a aktualizáciám softvéru.

Dôležitou súčasťou prepojených vozidiel sú komunikačné moduly, ktoré umožňujú prenos údajov prostredníctvom rôznych technológií, ako sú Wi-Fi, 5G, Bluetooth a V2X. Wi-Fi a Bluetooth sa používajú na spojenie medzi vozidlom a mobilnými zariadeniami alebo infotainment systémami, pričom 5G sieť poskytuje vysokorýchlostnú komunikáciu na prenos veľkých objemov dát v reálnom čase. Technológia V2X umožňuje komunikáciu vozidla s inými vozidlami, dopravnými značkami a inteligentnou infraštruktúrou a tým zvyšuje bezpečnosť a efektívnosť dopravy. [14]

Posledným hardvérovým komponentom v rámci architektúry prepojených vozidiel sú infotainment systémy a displeje, ktoré poskytujú vodičom a pasažierom prístup k multimediálnym funkciám, navigácii a komunikačným službám. Moderné infotainment systémy sú vybavené dotykovými obrazovkami, hlasovým ovládaním a umelou inteligenciou, čo im umožňuje intuitívnu interakciu s vozidlom. Tieto systémy sú často prepojené s mobilnými aplikáciami a cloudovými službami. Vodiči tak môžu personalizovať svoje nastavenia a prístup k aktuálnym informáciám o doprave, počasi a stave vozidla.

2.2 Softvérové riešenia a ekosystém

Softvérová infraštruktúra prepojených vozidiel zahŕňa širokú škálu operačných systémov, cloudových platforiem a aplikácií podporujúcich integráciu pokročilých funkcií a služieb. Jadrom softvérovej architektúry prepojených vozidiel sú operačné systémy v automobiloch, ktoré spravujú interakciu medzi hardvérom a aplikáciami. Najrozšírenejšie automobilové operačné systémy sú Linux, QNX a Android Automotive. Linux je open-source platforma, ktorá sa využíva v mnohých moderných vozidlách na riadenie infotainmentu a sieťovej konektivity. QNX, vyvinutý spoločnosťou BlackBerry, sa často používa v automobiloch pre svoju spoľahlivosť a robustnosť najmä v bezpečnostne kritických aplikáciách. Android Automotive je upravená verzia Androidu špeciálne navrhnutá pre vozidlá. Poskytuje vodičom prístup k aplikáciám Google, navigácii a asistentovi Google Assistant. [15]

Dôležitou súčasťou ekosystému prepojených vozidiel sú cloudové platformy a dátové centrá umožňujúce vozidlám ukladať a analyzovať veľké objemy dát. Cloudové technológie zabezpečujú vozidlám možnosť v reálnom čase prijímať aktualizácie softvéru, synchronizovať navigačné údaje a spracovávať informácie o dopravnej situácii. Cloudové riešenia tiež zohrávajú hlavnú úlohu pri zbere a analýze telematických údajov a tým umožňuje výrobcovi automobilov optimalizovať výkonnosť vozidiel a poskytovať nové služby založené na umelej inteligencii a strojovom učení. [16]

V rámci softvérového ekosystému prepojených vozidiel zohrávajú dôležitú úlohu aj aplikácie a služby, ktoré ponúkajú široké spektrum funkcionalít pre vodičov a pasažierov. Medzi najdôležitejšie služby patria navigácia, zábava a vzdialená diagnostika. Navigačné aplikácie, akými sú Google Maps alebo Waze využívajú údaje z cloudu na poskytovanie presných informácií o trase a premávke. Zábavné aplikácie umožňujú streamovanie hudby, videí a podcastov a tým zvyšujú komfort pasažierov počas jazdy. Vzdialená diagnostika umožňuje vodičovi monitorovať stav vozidla cez mobilné aplikácie, prijímať upozornenia na údržbu a kontaktovať servisné strediská v prípade poruchy.

Softvérové riešenia prepojených vozidiel neustále napredujú. Umelá inteligencia a strojové učenie zohrávajú čoraz významnejšiu úlohu pri optimalizácii jazdných návykov, prediktívnej údržbe a autonómnych funkciách vozidiel. Výrobcovia automobilov postupne zvyšujú svoje investície do vývoja bezpečnostných mechanizmov s cieľom ochrániť systém pred kybernetickými hrozbami a zabezpečiť integritu prenášaných dát medzi vozidlami a cloudovými platformami. Architektúra prepojených vozidiel tak kombinuje hardvérové

a softvérové riešenia, ktoré umožňujú vytvárať inteligentnejšie, bezpečnejšie a efektívnejšie vozidlá schopné reagovať na zmeny v dopravnej infraštruktúre a prispôbiť sa potrebám vodičov v reálnom čase. S postupným vývojom autonómnych technológií a rozšírením 5G sietí sa očakáva, že prepojené vozidlá budú zohrávať čoraz dôležitejšiu úlohu v ekosystéme inteligentných miest a udržateľnej dopravy.

2.3 Komunikačné protokoly a technológie

Komunikačné protokoly a technológie sú základným pilierom prepojených vozidiel, pretože umožňujú ich vzájomnú interakciu s infraštruktúrou, cloudovými službami a ostatnými účastníkmi cestnej premávky. Efektívna komunikácia medzi vozidlami a okolitým prostredím zabezpečuje vyššiu úroveň bezpečnosti, lepšie dopravné riadenie a pohodlnejšiu jazdu. Konektivita v moderných vozidlách sa spolieha na rôzne bezdrôtové technológie ako sú 4G LTE, 5G, Wi-Fi, Bluetooth a satelitné systémy, ktoré umožňujú nepretržitý prístup k dátam a službám v reálnom čase.

2.3.1 V2X komunikácia

V2X komunikácia je jednou z najpokročilejších technológií v oblasti prepojených vozidiel. Umožňuje výmenu dát medzi vozidlami a ich okolím. Túto technológiu rozdeľujeme na štyri hlavné kategórie: V2V, V2I, V2P, V2C. Každá z týchto kategórií komunikácie má svoje špecifické využitie a prispieva k zlepšeniu bezpečnosti, efektivity a automatizácie dopravy.

V2V komunikácia umožňuje priamu výmenu informácií medzi vozidlami v reálnom čase. Táto technológia je zásadná pri predchádzaní kolíziám, pretože umožňuje bezpečnostným systémom vozidiel varovať vodičov pred potenciálnymi nebezpečenstvami akými sú náhle brzdenie, nepredvídateľné pohyby ostatných vozidiel. V2V technológia využíva špecializované krátkodosahové komunikačné protokoly, ako je DSRC (Dedicated Short-Range Communication) alebo C-V2X (Cellular Vehicle-to-Everything), ktoré zabezpečujú rýchlu výmenu údajov bez potreby pripojenia na mobilnú sieť. [17], [18]

V2I komunikácia umožňuje vozidlám komunikovať s dopravnou infraštruktúrou ako sú semaforey, dopravné značky a inteligentné cestné senzory. Táto technológia pomáha optimalizovať tok premávky, znižovať dopravné zápchy a zlepšovať ekologickú efektívnosť jazdy. V2I technológie umožňujú vozidlám prijímať informácie o stave vozovky, nehodách alebo dopravných obmedzeniach. Zvyšuje sa tým bezpečnosť a plynulosť premávky. [17], [18]

V2P komunikácia sa zameriava na ochranu chodcov a cyklistov tým, že umožňuje vozidlám detegovať ich prítomnosť prostredníctvom senzorov, kamier alebo pripojenia mobilných zariadení. Inteligentné systémy vo vozidlách môžu rozpoznať chodcov vstupujúcich na cestu a upozorniť vodiča alebo automaticky iniciovať brzdenie a takto minimalizovať riziko nehôd v mestskom prostredí. [17], [18]

V2C komunikácia zabezpečuje nepretržitý prístup vozidla k cloudovým službám. To umožňuje vzdialené aktualizácie softvéru, analýzu dát a poskytovanie personalizovaných služieb vodičom. Cloudové platformy umožňujú výrobcem automobilov zbierať telematické údaje o vozidlách, optimalizovať výkon motorov a ponúkať vodičom pokročilé funkcie akými sú prediktívna údržba a adaptívna navigácia. [17], [18]

V2X technológie tvoria základ pre autonómne vozidlá, ktoré potrebujú nepretržitú výmenu dát na zabezpečenie plynulej a bezpečnej jazdy. Integrácia týchto komunikačných metód do budúcich inteligentných dopravných systémov môže výrazne znížiť počet nehôd a optimalizovať využitie cestnej infraštruktúry.

2.3.2 Bezdrôtové siete v automobiloch

Bezdrôtové technológie sú neoddeliteľnou súčasťou prepojených vozidiel a zabezpečujú efektívnu komunikáciu medzi rôznymi komponentmi vozidla a externými systémami. Medzi najdôležitejšie technológie patria mobilné siete 4G LTE a 5G, krátkodosahové technológie ako Wi-Fi, Bluetooth, NFC a satelitná komunikácia, ktorá zohráva kľúčovú úlohu pri navigácii a autonómnej jazde.

4G LTE a 5G siete predstavujú hlavný pilier konektivity v moderných vozidlách. Technológia 4G LTE umožňuje pripojenie na internet, streamovanie multimédií a cloudové služby. Jej obmedzená rýchlosť a latencia však nie sú ideálne pre pokročilé autonómne funkcie. S nástupom 5G sa otvárajú nové možnosti pre vysokorýchlostnú komunikáciu s nízkou latenciou, ktorá umožňuje okamžitú výmenu dát medzi vozidlami a infraštruktúrou. 5G siete poskytujú lepšiu podporu pre V2X komunikáciu, čo je veľmi dôležité pre bezpečnosť a efektívnosť autonómnych systémov. [14]

Wi-Fi, Bluetooth a NFC sú bezdrôtové technológie, ktoré sa využívajú na komunikáciu medzi vozidlom a mobilnými zariadeniami. Wi-Fi umožňuje bezdrôtové pripojenie infotainment systémov a zdieľanie internetu s pasažiermi. Bluetooth slúži na pripojenie mobilných telefónov s infotainmentom a na ovládanie hlasových asistentov. NFC je

technológia s krátkym dosahom, ktorá sa používa na bezkontaktné platby v palubných systémoch a na bezpečné odomkanie vozidiel prostredníctvom smartfónov. [4], [14]

Satelitná komunikácia zohráva dôležitú úlohu v autonómnych vozidlách a pokročilých navigačných systémoch. Globálne navigačné satelitné systémy GPS, GLONASS, Galileo a Beidou, umožňujú presnú lokalizáciu vozidiel v reálnom čase. V spojení s mapovacími platformami poskytujú autonómnym vozidlám detailné informácie o trase, topografii a dynamických zmenách v dopravnej situácii. Satelitná komunikácia je primárna pre diaľkové monitorovanie a riadenie flotíl vozidiel v oblastiach s obmedzeným pokrytím mobilnými sieťami. [19]

V kombinácii s pokročilými senzorovými systémami a umelou inteligenciou umožňujú bezdrôtové siete v automobiloch vytvorenie bezpečného, efektívneho a inteligentného dopravného ekosystému. Rozvoj 5G a satelitnej konektivity otvára nové možnosti pre autonómne vozidlá a inteligentnú infraštruktúru, ktorá dokáže dynamicky reagovať na meniace sa dopravné podmienky a poskytovať vodičom presné informácie v reálnom čase.

2.4 Kybernetická bezpečnosť prepojených vozidiel

Kybernetická bezpečnosť prepojených vozidiel sa stáva nevyhnutou výzvou s rastúcou úrovňou digitalizácie a konektivity v automobilovom priemysle. Prepojené vozidlá obsahujú množstvo elektronických riadiacich jednotiek, softvérových systémov a komunikačných rozhraní, ktoré môžu byť zraniteľné pri kybernetickom útoku. Bezpečnostné hrozby zahŕňajú neoprávnený prístup, hackerské útoky na systémy vozidla, úniky dát a možné zneužitie osobných informácií. Na ochranu prepojených vozidiel pred týmito rizikami je nevyhnutné implementovať pokročilé bezpečnostné opatrenia ako sú šifrovanie, detekcia anomálií za pomoci umelej inteligencie a bezpečnostné firewally integrované do elektronických riadiacich jednotiek.

Jednou z najväčších hrozieb je neoprávnený prístup do systémov vozidla, ktorý môže útočníkom umožniť manipuláciu s kritickými funkciami ako je brzdenie, riadenie alebo ovládanie motoru. Neautorizovaný prístup môže byť získaný prostredníctvom zraniteľností v softvérových rozhraniach vozidla akými sú Wi-Fi, Bluetooth alebo mobilné siete. Tento typ útoku môže mať fatálne následky, najmä ak je vozidlo v prevádzke a útočník získa možnosť prevziať kontrolu nad riadením. [14], [20]

Ďalším významným rizikom sú hackerské útoky na infotainment systémy a ovládacie prvky vozidla. Infotainment systémy sú často prepojené s externými aplikáciami a cloudovými službami a to ich robí atraktívnym cieľom pre hackerov. Útoky môžu viesť k prevzatiu kontroly nad multimediálnymi funkciami, deaktivácii navigácie, manipulácii s hlasovými asistentmi alebo odpočúvaniu komunikácie medzi pasažiermi a vozidlom. Infotainment systémy môžu byť taktiež zneužitú ako vstupná brána do riadiacich jednotiek vozidla. To im umožňuje sofistikovanejšie útoky na jeho prevádzkové funkcie.

Okrem priameho ovládania vozidla predstavujú významné riziko aj úniky dát a narušenie súkromia používateľov. Prepojené vozidlá neustále generujú a prenášajú veľké množstvo dát, lokalizačných údajov, informácií o jazdnom správaní, biometrických údajov vodiča a osobných informácií prepojených s infotainment systémami. Ak nie sú tieto údaje dostatočne chránené, môžu byť zneužitú na sledovanie pohybu vodiča, krádež identity alebo podvody súvisiace so zneužitím digitálnych služieb spojených s vozidlom. Útočníci môžu tiež manipulovať s telematickými dátami, čo by mohlo mať negatívne dôsledky pre poisťovne alebo flotilové služby, ktoré sa spoliehajú na presnosť týchto údajov. [21]

Proti kybernetickým hrozbám a na zabezpečenie prepojených vozidiel je nevyhnutná implementácia viacerých bezpečnostných opatrení na hardvérovej aj softvérovej úrovni. Výrobcovia automobilov spolu s technologickými spoločnosťami vyvíjajú a nasadzujú pokročilé bezpečnostné riešenia, ktoré pomáhajú chrániť vozidlá pred kybernetickými útokmi a neoprávneným prístupom. Jedným z kľúčových bezpečnostných opatrení je šifrovanie dát a zabezpečené prenosové protokoly. Moderné prepojené vozidlá využívajú šifrovacie algoritmy ako sú AES a RSA (Rivest-Shamir-Adleman) na zabezpečenie citlivých údajov počas ich prenosu medzi vozidlom, cloudom a inými zariadeniami. Šifrovanie chráni osobné údaje vodičov, navigačné informácie a diagnostické dáta pred neoprávneným prístupom. Popri tom sú implementované zabezpečené komunikačné protokoly TLS (Transport Layer Security) a IPSec (Internet Protocol Security), ktoré chránia dátovú výmenu medzi vozidlom a externými sieťami pred odpočúvaním alebo podvrhom údajov. [22] Na detekciu anomálií a kybernetických útokov je využitie umelej inteligencie a strojového učenia ďalším dôležitým bezpečnostným opatrením. Moderné vozidlá sú vybavené bezpečnostnými systémami schopnými analyzovať sieťový prenos a detegovať neobvyklé vzory správania, ktoré môžu naznačovať kybernetický útok. Ak systém deteguje pokus o neoprávnený prístup k elektronickej riadiacej jednotke alebo podozrivú manipuláciu s diagnostickými dátami, môže automaticky zablokovat' komunikáciu s útočníkom

a upozorniť vodiča na potenciálnu hrozbu. Umelá inteligencia sa tiež využíva na identifikáciu podozrivých softvérových aktualizácií, čím pomáhajú predchádzať phishingovým útokom a šíreniu škodlivého kódu. [22] Na ochranu pred škodlivým softvérom a neoprávnenými prístupmi sú prepojené vozidlá vybavené firewallmi a bezpečnostnými modulmi v elektronických riadiacich jednotkách. Tieto bezpečnostné vrstvy kontrolujú všetky prichádzajúce a odchádzajúce dáta a zabezpečujú, že iba autorizované prenosy môžu vstúpiť do sieťového prostredia vozidla. Bezpečnostné moduly v elektronických riadiacich jednotkách obsahujú vstavané mechanizmy na detekciu a elimináciu malvéru. Znižuje sa tým riziko, že útočníci budú môcť zneužiť zraniteľnosti systému na manipuláciu s riadením vozidla. [1]

2.5 Normy kybernetickej bezpečnosti v automobilovom priemysle

Rastúca konektivita vozidiel a pokroky v technológiách priniesli zvýšené požiadavky na kybernetickú bezpečnosť v automobilovom priemysle. Vzhľadom na rastúce kybernetické hrozby a zložitosť moderných vozidiel boli vytvorené medzinárodné predpisy a normy, ktoré stanovujú zásady pre identifikáciu, riadenie a minimalizáciu bezpečnostných rizík počas celého životného cyklu vozidla.

Jedným z najvýznamnejších predpisov je regulačný rámec Európskej hospodárskej komisie Organizácie spojených národov pracovnej skupiny 29 (WP 29) (konkrétne nariadenia R155 a R156), ktorý definuje minimálne požiadavky na kybernetickú bezpečnosť pre vozidlá určené na globálne trhy. Výrobcovia musia preukázať schopnosť ochrany pred kybernetickými hrozbami počas celého životného cyklu vozidla vrátane monitorovania, detekcie a reakcie na bezpečnostné incidenty v reálnom čase. Okrem toho WP.29 vyžaduje implementáciu systémov na vzdialené aktualizácie softvéru, ktoré umožňujú opravy bezpečnostných zraniteľností bez nutnosti fyzického zásahu do vozidla. [23]

Norma ISO/SAE 21434, ktorá nahradila SAE J3061, poskytuje podrobné usmernenia pre riadenie kybernetickej bezpečnosti v automobilovom priemysle. Štandard zavádza systematický prístup k zabezpečeniu vozidiel, pričom zdôrazňuje:

- identifikáciu rizík a zraniteľností v rôznych komponentoch vozidla;
- integráciu bezpečnostných opatrení už vo fáze návrhu, vývoja a testovania systémov;
- nepretržité monitorovanie kybernetických hrozieb, čím sa zabezpečí schopnosť reagovať na nové útoky počas prevádzky vozidla.

ISO/SAE 21434 sa zaoberá všetkými fázami životného cyklu vozidla od konceptu, cez výrobu až po jeho likvidáciu. Zdôrazňuje tiež potrebu úzkej spolupráce medzi automobilovými výrobcami, dodávateľmi a ďalšími zainteresovanými stranami. Jej cieľom vytvoriť odolnejšie bezpečnostné systémy. [24]

Prvým pokusom o vytvorenie usmernenia pre kybernetickú bezpečnosť v automobilových systémoch bola SAE J3061. Položila základy pre ISO/SAE 21434. Norma zdôraznila význam:

- zohľadnenia bezpečnostných hrozieb už vo fáze návrhu vozidla, čím sa minimalizujú riziká ešte pred nasadením systému;
- ochrany komunikačných systémov ako sú technológie V2X, ktoré umožňujú výmenu dát medzi vozidlami a komunikačnou infraštruktúrou;
- rámcov na detekciu, analýzu a zmiernenie kybernetických rizík, ktoré pomáhajú výrobcov pripravovať sa na nové hrozby a reagovať efektívnejšie. [25]

2.5.1 Odporúčania kybernetických opatrení do budúcnosti

Vzhľadom na narastajúcu sofistikovanosť kybernetických hrozieb sa automobilový priemysel spolieha na pokročilé technologické riešenia a spoluprácu medzi výrobcami, dodávateľmi a bezpečnostnými expertmi. Moderné vozidlá sa čoraz viac približujú sieťovým počítačovým platformám. Vyžaduje si to aplikáciu osvedčených bezpečnostných postupov z oblasti informačných technológií. Strategické opatrenia a trendy v oblasti kybernetickej bezpečnosti zahŕňajú bezpečné aktualizácie softvéru, detekciu anomálií pomocou umelej inteligencie, viacfaktorovú autentifikáciu, segmentáciu sietí, kryptografickú agilitu a certifikáciu bezpečnosti. [1]

Bezpečné aktualizácie softvéru umožňujú nasadenie bezpečnostných záplat bez potreby fyzického zásahu do vozidla. Znižuje sa tým riziko kybernetických útokov spôsobených neaktuálnym softvérom. Aby boli tieto aktualizácie spoľahlivé, musia byť chránené robustnými kryptografickými protokolmi, ktoré majú zabrániť ich neoprávnenej manipulácii. Viacfaktorová autentifikácia zvyšuje úroveň ochrany tým, že kombinuje viaceré nezávislé prvky na overenie identity akými sú biometrické údaje, kryptografické kľúče, prípadne doplnkové overovacie metódy. V automobilovom prostredí sa tento princíp uplatňuje napríklad pri digitálnych kľúčoch, kde je potrebné najskôr odomknúť mobilnú aplikáciu biometrickým overením (pomocou odtlačku prsta, alebo rozpoznania tváre)

a následne potvrdiť prístup prostredníctvom kryptografického tokenu uloženého v zabezpečenom hardvéri zariadenia. V prípade zdieľaných vozidiel môže byť vyžadované overenie prostredníctvom RFID karty v kombinácii s rozpoznaním tváre vodiča, alebo v servisných procesoch kombinácia smart karty s jednorazovým prístupovým kódom. Takáto kombinácia faktorov významne znižuje pravdepodobnosť neoprávneného prístupu k citlivým systémom vozidla. Dôležitým opatrením je aj segmentácia sietí, ktorá oddeľuje kritické komponenty od menej dôveryhodných častí systému, čo môže obmedziť dopad prípadného narušenia a zabrániť šíreniu útoku v rámci vozidla. Kryptografická agilita umožňuje rýchlo prispôbovať a aktualizovať kryptografické algoritmy podľa aktuálnych hrozieb, čo je zásadné vzhľadom na neustále meniace sa podmienky v oblasti technológií a kybernetických útokov. K celkovej úrovni bezpečnosti prispieva aj certifikácia podľa medzinárodných noriem, ktorá je zároveň potvrdením, že ochranné mechanizmy vo vozidle spĺňajú požadované štandardy a dokážu odolat' reálnym hrozbám.

3 VZDIALENÉ OVLÁDANIE VOZIDIEL PROSTREDNÍCTVOM MOBILNÝCH APLIKÁCIÍ

Automobilový priemysel prechádza dynamickým vývojom, pričom jedným z hlavných trendov je digitalizácia a automatizácia riadenia vozidiel. Moderné automobily už nie sú odkázané len na mechanické kľúče alebo tradičné diaľkové ovládače, ale čoraz častejšie využívajú mobilné aplikácie na interakciu s vozidlom. Prostredníctvom týchto aplikácií môžu používatelia na diaľku zamykať a odomykať vozidlo, naštartovať alebo vypnúť motor, monitorovať stav batérie a diagnostické údaje, či lokalizovať svoje vozidlo. Výrobcovia automobilov ich integrujú do svojich systémov s cieľom poskytnúť vodičom lepší komfort, možnosť vzdialenej diagnostiky a aktualizácie softvéru vozidla prostredníctvom internetu.

Vzdialené ovládanie vozidiel je umožnené prepojením viacerých technologických prvkov od mobilných aplikácií cez cloudové servery, až po automobilové komunikačné jednotky. Tieto systémy ponúkajú široké možnosti v oblasti používateľskej interakcie. Zároveň predstavujú nové bezpečnostné výzvy. Neadekvátne zabezpečenie môže viesť k neoprávnenému prístupu útočníkov, ktorí môžu manipulovať so systémami vozidla alebo získať citlivé údaje o jeho majiteľovi.

Hoci výrobcovia automobilov neustále pracujú na vylepšovaní bezpečnostných mechanizmov, mobilné aplikácie na ovládanie vozidiel zostávajú atraktívnym cieľom kybernetických útokov. Útočníci môžu zneužiť slabiny v autentifikácii, šifrovaní alebo komunikačných protokoloch a získať tak neoprávnený prístup k vozidlu. Z tohto dôvodu je nevyhnutné analyzovať architektúru týchto aplikácií, identifikovať možné bezpečnostné hrozby a navrhnúť efektívne opatrenia na ich elimináciu.

3.1 Architektúra mobilných aplikácií pre správu vozidiel

Mobilné aplikácie umožňujúce diaľkové ovládanie vozidiel fungujú na princípe centralizovanej architektúry, ktorou hlavnou úlohou je zabezpečiť komunikačný tok medzi používateľom a vozidlom. Tento tok prebieha od používateľa, ktorý zadáva požiadavku prostredníctvom mobilnej aplikácie, cez internetové komunikačné kanály a cloudovú infraštruktúru výrobcu až po samotné vozidlo. Rovnaký komunikačný tok prebieha následne opačným smerom v prípade odpovede alebo spätnej väzby zo strany vozidla. Základný reťazec komunikácie je možné rozdeliť nasledovne:

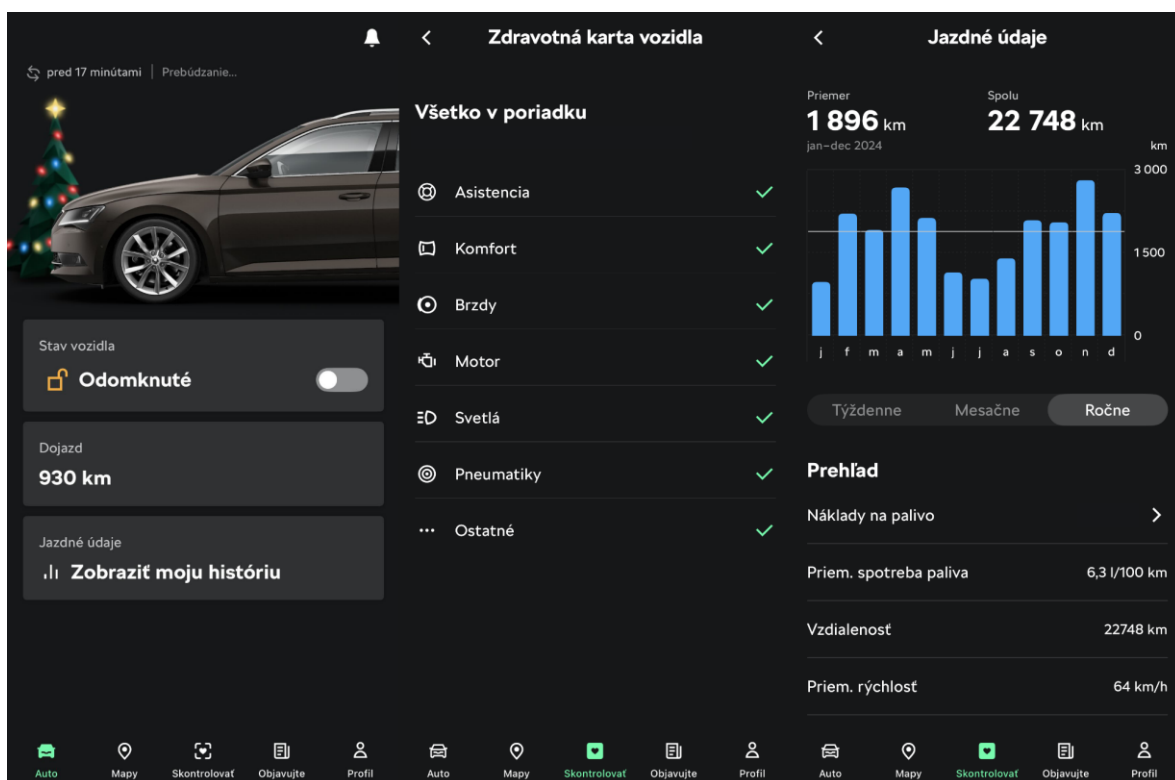
- mobilná aplikácia: interakcia začína na strane používateľa, ktorý cez mobilnú aplikáciu zadáva požiadavky od odomknutie dverí, naštartovania motora, spustenia klimatizácie, alebo lokalizácie vozidla;
- komunikačné médium: požiadavky sú prenášané cez bezpečnostne zabezpečené kanály. Využívajú sa technológie ako Bluetooth, Wi-Fi, LTE alebo 5G, pričom výber závisí od konkrétnej funkcionality, dostupnosti a požiadaviek na bezpečnosť a latenciu;
- cloudový server výrobcu: v cloudovej vrstve dochádza k autentifikácii používateľa, spracovaniu požiadavky a jej odoslaniu do vozidla. Tieto servery zároveň uchovávajú údaje o vozidle, spravujú aktualizácie a umožňujú monitoring systému;
- vozidlo: po prijatí a overení príkazu vykoná vozidlo požadovanú akciu a odošle odpoveď späť do systému - napríklad potvrdenie vykonania úkonu alebo stavové údaje.

Takto navrhnutá centralizovaná architektúra umožňuje efektívne a pružne riadiť bezpečnosť celého systému. Výrobcovia môžu prostredníctvom cloudovej vrstvy realizovať aktualizácie, detegovať podozrivé správanie, obmedziť, alebo zablokovať prístup v prípade kompromitácie. Zároveň však vzniká riziko, že v prípade úspešného útoku na cloudový server môžu útočníci získať prístup k väčšiemu množstvu vozidiel naraz, čo predstavuje významné bezpečnostné ohrozenie v širšom meradle. [26]

3.2 Funkcie mobilných aplikácií pre správu vozidiel

Mobilné aplikácie na ovládanie vozidiel ponúkajú široké spektrum funkcií, ktoré výrazne zvyšujú komfort a pohodlie používateľov. Tieto aplikácie okrem základných operácií akými sú vzdialené odomkanie a zamykanie vozidla, poskytujú aj pokročilé možnosti, napríklad sledovanie diagnostických údajov, geolokácia i aktualizácie softvéru vozidla. Tieto aplikácie fungujú ako rozšírenie palubných systémov automobilov a umožňujú interakciu medzi vodičom a vozidlom aj na veľké vzdialenosti. Mobilné aplikácie pre správu vozidiel sa líšia v závislosti od výrobcu, konkrétneho modelu vozidla a úrovne jeho výbavy, pričom možno rozlíšiť základné funkcie, ktoré ponúka väčšina moderných vozidiel a pokročilé funkcionality, ktoré sú typické najmä pre prémiové značky alebo vozidlá s vyššou mierou konektivity. Medzi najčastejšie sa vyskytujúce funkcie patria:

- vzdialené zamykanie/odomykanie a štartovanie motora: používateľ môže na diaľku zamknúť alebo odomknúť vozidlo a v niektorých prípadoch aj naštartovať motor. Táto funkcia si vyžaduje bezpečné autentifikačné mechanizmy, aby sa zabránilo neoprávnenému prístupu;
- monitorovanie stavu vozidla a diagnostika: aplikácie umožňujú sledovať stav batérie, tlak v pneumatikách, spotrebu paliva a ďalšie dôležité údaje o vozidle. Niektoré modely ponúkajú aj diagnostické upozornenia na blížiacu sa údržbu alebo potrebu servisu;
- geolokácia a plánovanie trasy: používatelia môžu lokalizovať svoje vozidlo na mape, získať navigačné pokyny k jeho aktuálnej polohe alebo si naplánovať cestu. Táto funkcia je užitočná pri hľadaní zaparkovaného vozidla, prípadne pri odcudzení vozidla;
- OTA aktualizácie: niektorí výrobcovia automobilov umožňujú vzdialené aktualizácie softvéru vozidla cez mobilnú aplikáciu. Tieto aktualizácie môžu zahŕňať vylepšenia bezpečnostných mechanizmov, nové funkcie, či opravy chýb. [27], [28], [29]



Obrázok 4 Aplikácia MyŠkoda

(zdroj: vlastný)

3.2.1 Integrácia s infotainment systémami

Niektoré mobilné aplikácie umožňujú priame prepojenie s infotainment systémami automobilov, čo vodičovi poskytuje rozšírené možnosti personalizácie a ovládania multimédií. Aplikácie môžu ponúkať napríklad:

- prednastavenie klimatizácie: možnosť vzdialene aktivovať kúrenie, alebo klimatizáciu pred vstupom do vozidla;
- ovládanie audiosystému: výber skladieb, úprava hlasitosti alebo prístup k streamovacím službám cez mobilnú aplikáciu;
- hlasové ovládanie a integrácia s digitálnymi asistentmi: niektoré aplikácie umožňujú ovládanie vozidla pomocou hlasových príkazov prostredníctvom digitálnych asistentov.

3.3 Bezpečnostné riziká pri využívaní mobilných aplikácií

Mobilné aplikácie na diaľkové ovládanie vozidiel síce prinášajú vyšší komfort a flexibilitu, súčasne otvárajú nové bezpečnostné výzvy. Vzhľadom na to, že tieto aplikácie sú prepojené s cloudovými službami a využívajú rôzne komunikačné protokoly, môžu sa stať cieľom kybernetických útokov. Potenciálne riziká sa týkajú nielen samotných aplikácií, ale aj cloudovej infraštruktúry, prostredníctvom ktorej dochádza k sprostredkovaniu príkazov.

Jedným z najvýznamnejších problémov pri diaľkovom ovládaní vozidiel prostredníctvom mobilných aplikácií je zraniteľnosť použitých komunikačných protokolov. Prenos údajov medzi mobilnou aplikáciou, cloudovým serverom a samotným vozidlom prebieha prostredníctvom technológií Bluetooth, Wi-Fi a mobilnej siete. Bluetooth sa využíva na lokálnu komunikáciu medzi mobilným zariadením používateľa a vozidlom, napríklad pri overovaní prístupu pri príchode k vozidlu. Táto technológia je však náchylná na útoky typu Man-in-the-Middle, pri ktorých sa útočník vstupuje medzi dve komunikujúce strany s cieľom zachytiť a modifikovať prenášané údaje za účelom neoprávneného odomknutia vozidla. Na prenos údajov medzi aplikáciou a cloudovým serverom sa zvyčajne používajú Wi-Fi siete a mobilné dátové pripojenie. Wi-Fi spojenie, najmä v prípade verejných, či nesprávne nakonfigurovaných sietí, predstavuje riziko zachytenia a manipulácie s dátami. LTE siete poskytujú vyššiu mieru zabezpečenia, no ani tie nie sú imúnne voči sofistikovaným útokom, najmä ak sú zamerané na cloudovú infraštruktúru výrobcu vozidiel. Úspešný útok na cloudový server môže viesť k hromadnému narušeniu

systémov u viacerých vozidiel naraz, čo pre jeho možní veľký rozsah predstavuje zásadné bezpečnostné riziko. [30]

Ďalšou významnou bezpečnostnou hrozbou je nedostatočné zabezpečenie API rozhraní, ktoré spracúvajú príkazy na ovládanie vozidiel. Cloudové servery, ktoré spracúvajú požiadavky mobilných aplikácií, môžu byť vystavené útokom zameraným na obchádzanie autentifikácie alebo zneužitie chybne implementovaných autorizačných mechanizmov. Útočník, ktorý by získal prístup k takémuto API, by mohol neoprávnene ovládať akékoľvek vozidlo pripojené k systému. [31]

Značné riziko predstavujú aj útoky s prehratím signálu. Tieto útoky sú najčastejšie spájané s fyzickými kľúčmi, no za určitých okolností môžu byť aplikovateľné aj na mobilné aplikácie. Predstavuje to hrozbu najmä v prípade ak výrobcovia neimplementujú dostatočné bezpečnostné opatrenia akými sú jednorazové tokeny, časové pečiatky alebo end-to-end šifrovanie. V prípade, že aplikácia používa statické alebo opakovane použiteľné príkazy, útočník môže zachytiť legítimnú komunikáciu medzi aplikáciou a vozidlom (prostredníctvom nezabezpečeného Wi-Fi spojenia) a následne túto komunikáciu zneužiť na vykonanie rovnakej akcie - napríklad odomknutie dverí.

Bezpečnostné riziká súvisia aj s uchovávaním citlivých údajov v aplikácii samotnej. Niektoré mobilné aplikácie uchovávajú prihlasovacie údaje, tokeny, šifrovacie kľúče v nezašifrovanej podobe. To môže viesť k ich zneužitiu v prípade kompromitácie smartfónu. Ak útočník získa prístup k takýmto údajom, môže bez prekážok ovládať vozidlo aj bez znalosti pôvodných prihlasovacích údajov. [30]

Významným problémom z pohľadu kybernetickej bezpečnosti sú útoky zamerané na softvér mobilných aplikácií, pri ktorých útočníci využívajú techniky reverzného inžinierstva na odhalenie vnútornej logiky a získanie citlivých údajov obsiahnutých v kóde. Častou chybou vývojárov je zakódovanie šifrovacích kľúčov priamo do zdrojového kódu aplikácie (hardcoded encryption keys). Typickým príkladom je situácia, keď je v aplikácii napevno uvedený AES kľúč používaný na šifrovanie komunikácie s vozidlom alebo serverom. V takom prípade stačí, aby útočník aplikáciu dekompiloval a kľúč následne z kódu extrahoval. Takto získaný kľúč môže zneužiť na dešifrovanie komunikácie, vytváranie falošných príkazov cez vlastnú aplikáciu alebo na neautorizovaný prístup k API. V praxi boli takéto zraniteľnosti odhalené napríklad v aplikáciách niektorých čínskych výrobcov, kde boli šifrovacie kľúče a API tokeny dostupné priamo v kóde. Riziko navyše zvyšujú modifikované verzie aplikácií distribuované mimo oficiálnych obchodov, inštalácia

ktorých môže viesť k získaniu neoprávneného prístupu k vozidlu, prípadne k exfiltrácii citlivých údajov bez vedomia používateľa. [30]

Jedným z ďalších významných rizikových faktorov je nedostatočne zabezpečený proces autentifikácie a autorizácie, ktorý môže viesť k neoprávnenému ovládaniu vozidiel. Ak aplikácia používa iba jednoduché overenie heslom bez viacfaktorovej autentifikácie, útočník, ktorý získa prihlasovacie údaje, môže získať plnú kontrolu nad vozidlom. Rovnako nebezpečné je, ak systém neimplementuje adekvátne obmedzenia oprávnení, čo môže umožniť zmenu úrovne prístupu a vykonávať operácie, ktoré by nemali byť dostupné pre bežného používateľa.

3.4 Možnosti útokov a ich simulácia

Na zabezpečenie ochrany mobilných aplikácií určených na diaľkové ovládanie vozidiel je nevyhnutné pochopiť spôsoby, akými môžu byť tieto systémy napadnuté. Simulácia útokov umožňuje identifikovať zraniteľnosti a vyhodnotiť efektivitu existujúcich bezpečnostných mechanizmov. Pri analýze bezpečnosti mobilných aplikácií sa využívajú rôzne testovacie techniky, ktoré zahŕňajú testovanie komunikácie medzi aplikáciou a cloudovými servermi, analýzu zdrojového kódu a praktické simulácie kybernetických útokov.

Jedným z najbežnejších typov testovania je analýza zraniteľností Bluetooth komunikácie. Keďže niektoré automobilky umožňujú prepojenie mobilnej aplikácie s vozidlom cez Bluetooth, je dôležité overiť, či toto spojenie nie je náchylné na útoky typu Man-in-the-Middle. Simulácia takéhoto útoku môže byť vykonaná pomocou špecializovaných nástrojov ako je GATTacker alebo Bettercap, ktoré umožňujú zachytávať a modifikovať prenosy údajov medzi mobilnou aplikáciou a vozidlom. Ak je spojenie medzi zariadeniami nedostatočne šifrované alebo aplikácia neoveruje autenticitu pripojeného zariadenia, útočník môže manipulovať s prenášanými príkazmi a neoprávnene ovládať vozidlo. [32], [33]

Ďalším dôležitým hľadiskom pri testovaní aplikácií je interceptovanie komunikácie medzi mobilnou aplikáciou a cloudovým serverom výrobcu. Na tento účel sa využívajú nástroje ako je Burp Suite, ktorý umožňuje analyzovať HTTP/S prenosy, odhaliť potenciálne slabé miesta v autentifikácii a zabezpečení údajov. Pri tomto teste sa overuje, či aplikácia správne implementuje ochranu proti útokom typu Man-in-the-Middle a či nedochádza k prenášaní citlivých údajov v nezašifrovanej podobe. Ak aplikácia nedostatočne overuje

platnosť certifikátov alebo umožňuje obísť TLS ochranu, útočník môže odchytiť a modifikovať príkazy odosielané na server. [34]

Pri penetračnom testovaní mobilných aplikácií sa analyzuje aj bezpečnosť zdrojového kódu a spôsob uchovávanía citlivých údajov. Reverzné inžinierstvo aplikácie môže odhaliť slabé miesta v implementácii autentifikačných mechanizmov alebo prítomnosť staticky uložených kryptografických kľúčov. Nástroje akými sú apktool pre Android, class-dump pre iOS, umožňujú dekompiláciu aplikácie a skúmanie jej vnútorných mechanizmov. Ak sa v aplikácii nachádzajú hardcodované prihlasovacie údaje, prípadne šifrovacie kľúče, útočník ich môže extrahovať a použiť na získanie prístupu k vozidlu. [35]

Simulácia útoku s prehratím signálu je ďalšou metódou testovania bezpečnosti mobilných aplikácií. Pri tomto type útoku útočník zachytí autentifikačné údaje a príkazy odoslané z aplikácie do vozidla a následne ich v neskoršom čase opakovane odošle. Ak aplikácia neimplementuje mechanizmy na detekciu a blokovanie opakovane odoslaných príkazov, môže dôjsť k neoprávnenému ovládaniu vozidla. Testovanie tohto scenára sa vykonáva pomocou rádiových nástrojov akými sú HackRF One či Flipper Zero, ktoré umožňujú zachytávanie a prehrávanie signálov v rôznych bezdrôtových komunikačných pásmach.

Okrem uvedených testovacích metód je dôležité analyzovať aj cloudové rozhrania a API služby, ktoré spracúvajú požiadavky na ovládanie vozidiel. Ak rozhranie API nie je dostatočne chránené pred neoprávnenými požiadavkami a nedostatočne obmedzuje počet autentifikačných pokusov, môže byť náchylné na útoky hrubou silou i na podvrhnuté požiadavky. Pri simulácii útokov na API sa testuje, či je možné obísť autentifikáciu, ako systém reaguje na nesprávne formátované požiadavky a či obsahuje dostatočné obmedzenia pre opakované pokusy o prihlásenie. [36]

II PRAKTICKÁ ČASŤ

4 NÁVRH EXPERIMENTU ZABEZPEČENIA AUTOMOBILU S VYUŽITÍM TECHNOLOGIE PLÁVAJÚCEHO KÓDU

Navrhnutý experiment zabezpečenia automobilu je realizovaný prostredníctvom modelu centrálného zamykania s implementáciou ochrany prostredníctvom plávajúceho kódu. Tento systém umožňuje vodičovi bezpečne zamknúť alebo odomknúť vozidlo pomocou diaľkového ovládača, pričom zabezpečuje odolnosť voči bežným útokom akými sú zachytávanie a prehratie signálu.

Implementácia plávajúceho kódu v experimente prebiehala tak, že pri každom stlačení tlačidla na vysielacom je vygenerovaný nový jedinečný kód na základe jednoduchého inkrementálneho algoritmu. Prijímač následne prijme kód a porovná ho s očakávaným kódom, alebo s kódom v definovanom tolerančnom pásme (akceptácia N nasledujúcich kódov). V prípade, že prijatý kód zodpovedá očakávanému, alebo povolenému rozsahu, servomotor sa aktivuje a LCD displej zobrazí aktuálny stav systému (zamknuté alebo odomknuté). Nesprávne alebo opakovane prijaté kódy sú odmietnuté a tým sa zabezpečuje ochrana proti útokom s prehratím signálu. Funkčnosť implementovaného plávajúceho kódu bola overená pomocou praktických testov, pri ktorých sa využijú zariadenia Flipper Zero a HackRF One na simuláciu zachytávania a prehrávania bezdrôtovej komunikácie. Cieľom bolo otestovať odolnosť systému voči bežným pokusom o narušenie bezpečnosti.

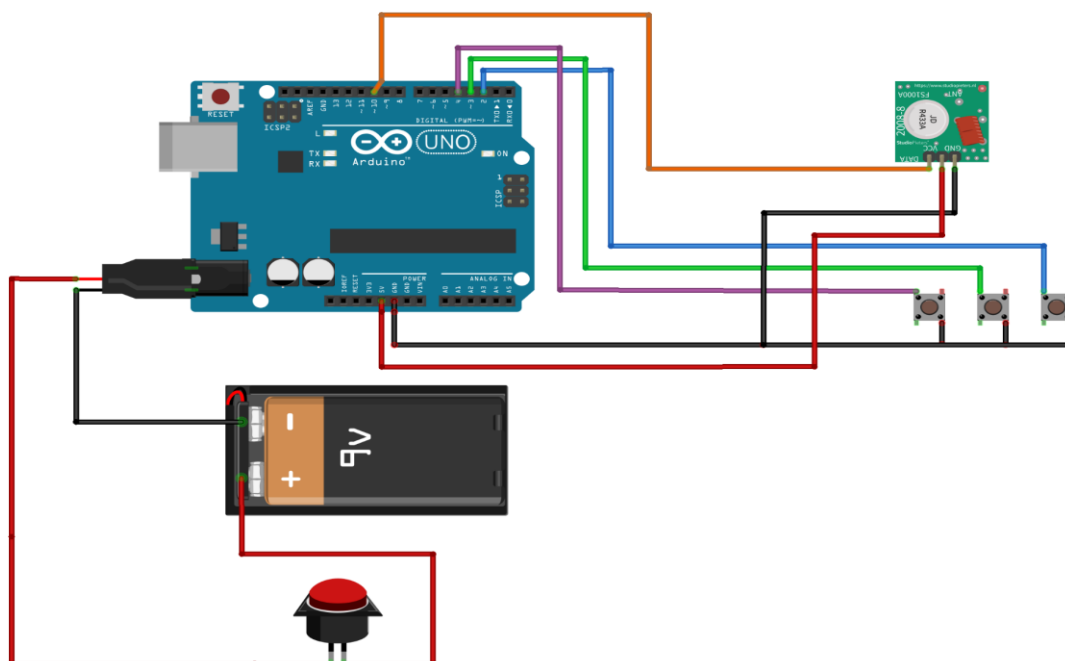
5 ZOSTROJENIE MODELU BEZDRÔTOVÉHO ZAMYKANIA VOZIDLA S TECHNOLOGIOU PLÁVAJÚCEHO KÓDU

Na demonštráciu fungovania bezpečnostného systému bezdrôtového zamykania vozidla bola použitá zostava dvoch platforiem Arduino Uno. Tieto platformy boli rozdelené podľa funkcie na vysielaciu a prijímaciu jednotku. Model simuluje autentický mechanizmus centrálného zamykania vozidla pomocou dynamicky generovaných plávajúcich kódov, čím výrazne zvyšuje odolnosť systému proti útoku s prehratím signálu.

5.1 Vysielač

Vysielacia jednotka plní funkciu diaľkového ovládača. Hlavnou úlohou tejto časti systému je generovať jedinečný plávajúci kód pri každom stlačení tlačidla a následne ho bezdrôtovo odoslať k prijímaču.

Na dosku sú pripojené tri tlačidlá reprezentujúce funkcie uzamknutia, odomknutia a otvorenia kufra. Po stlačení niektorého z tlačidiel Arduino vygeneruje príslušný plávajúci kód a odošle ho cez RF vysielač pracujúci na frekvencii 433 MHz. Napájanie zabezpečuje 9 voltová batéria pripojená cez podsvietený spínač. Tlačidlá sú zapojené na digitálne piny D2, D3 a D4, zatiaľ čo RF vysielač je pripojený na pin D10. Celé zariadenie je napájané výstupom 5 voltov z Arduino dosky.

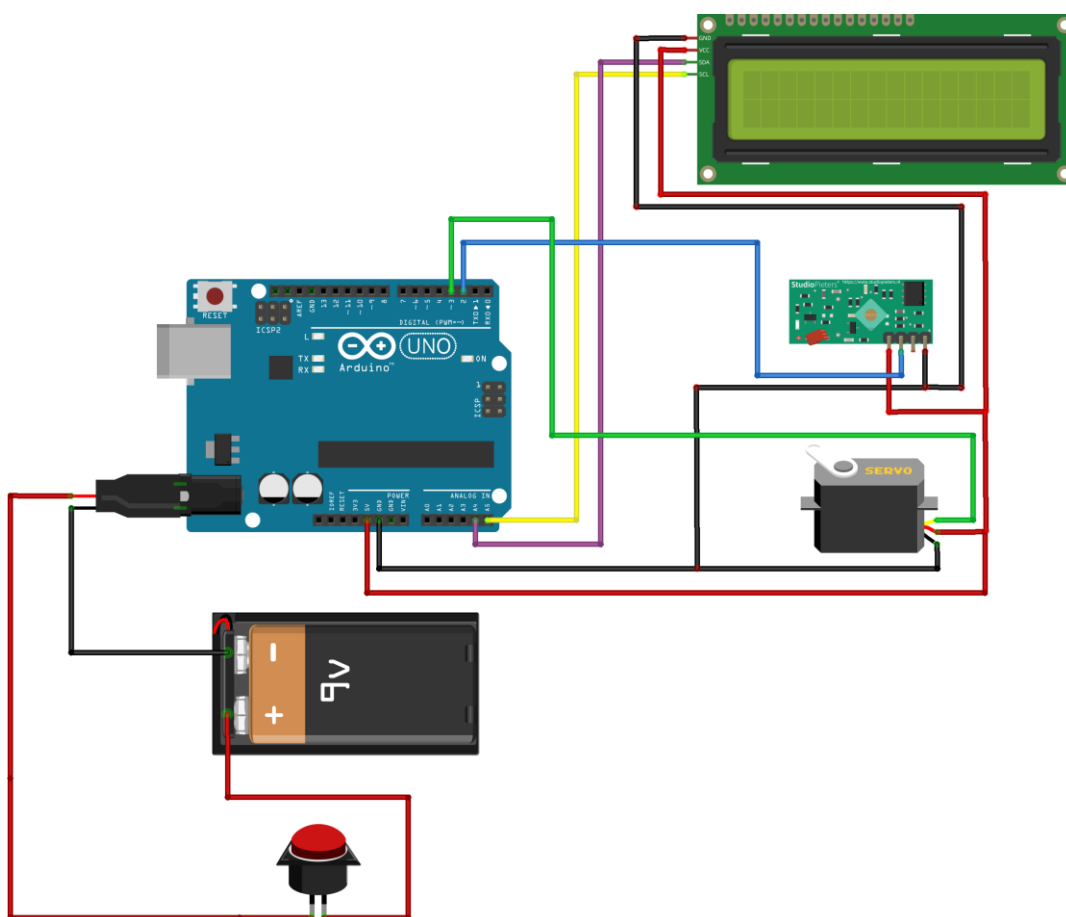


Obrázok 5 Zapojenie vysielača Arduino

(zdroj: vlastný)

5.2 Prijímač

Prijímacia jednotka simuluje riadiacu jednotku automobilu, ktorá prijíma signály z vysieláča a vyhodnocuje ich platnosť. Na základe správneho kódu vykonáva príslušnú akciu, teda zamykanie, odomkykanie alebo otvorenie kufra. Aj táto časť systému je postavená na platforme Arduino Uno, ktorá prijíma údaje cez RF prijímač na frekvencii 433 MHz pripojený k digitálnemu pinu D2. Po prijatí signálu Arduino vyhodnotí jeho platnosť a v prípade korektnosti vydá pokyn na vykonanie príslušnej akcie. Fyzické zamykanie a odomkykanie je simulované servomotorom, ktorý je ovládaný cez digitálny pin D3. Vizualizáciu aktuálneho stavu systému zabezpečuje LCD displej 16x2 s I2C prevodníkom, ktorý je pripojený na piny A4 (SDA) a A5 (SCL). Prijímač je napájaný 9 voltovou batériou a všetky komponenty sú napájané cez 5 voltový výstup Arduino dosky.



Obrázok 6 Zapojenie prijímača Arduino

(zdroj: vlastný)

5.3 Program pre Arduino

Pri tvorbe programového vybavenia modelu bol použitý programovací jazyk pre Arduino a potrebné knižnice pre jednotlivé periférie. Vyvinutý program slúžil na simuláciu systému centrálného zamykania automobilu, pričom každé stlačenie tlačidla generuje unikátny prenosový kód.

Hlavným cieľom implementácie bolo zabezpečiť, aby každá požiadavka zamknutia, odomknutia, alebo otvorenia kufra zo strany používateľa viedla k vytvoreniu vždy nového, jedinečného kódu, ktorý je následne odoslaný prijímacej jednotke.

5.3.1 Program pre vysielanie signálu

Program vysielacej jednotky je založený na práci s knižnicou RCSwitch. V inicializačnej fáze sa vytvára inštancia triedy RCSwitch pod názvom mySwitch, ktorá predstavuje samotný RF vysielateľ a poskytuje základné metódy ako `send()`, `enableTransmit()` a `enableReceive()`.

Konfigurácia systému začína príkazom `mySwitch.enableTransmit(10)`, ktorým je definované, že pin D10 bude použitý na odosielanie rádiových signálov. Príkazom `pinMode` sú piny D2, D3 a D4 nastavené ako vstupy s aktivovanými internými pull-up rezistormi. Tým sa zabezpečí, že v pokojovom stave budú mať tieto piny logickú hodnotu HIGH, a po stlačení tlačidla dôjde k ich prepnutí na hodnotu LOW. [37] Inicializácia sériovej komunikácie prostredníctvom príkazu `Serial.begin(9600)` umožňuje monitorovanie odosielaných správ cez sériový monitor v prostredí Arduino IDE.

Každému tlačidlu je priradený konkrétny digitálny pin. Pin D2 slúži na ovládanie funkcie otvorenia kufra, pin D3 na zamknutie a pin D4 na odomknutie vozidla. Tieto piny sú definované ako konštanty typu `const int`, aby sa predišlo nechceným zmenám počas behu programu.

Pre správnu identifikáciu prenosov a zabezpečenie unikátnosti signálov sa využívajú premenné typu `unsigned long`, ktoré slúžia na sledovanie počtu stlačení jednotlivých tlačidiel. Pri každom stlačení sa hodnota príslušného počítadla zvýši o jednotku, čím sa zabezpečí, že každý vyslaný kód bude jedinečný.

```
// Potrebná knižnica pre RF komunikáciu
// -----
#include <RCSwitch.h>
// -----
// Vytvorenie inštancie objektu pre vysielanie dát
// -----
RCSwitch mySwitch = RCSwitch();
// -----
// Definovanie pinov pre tlačidlá na ovládači
// -----
const int trunkButtonPin = 2;    // Pin tlačidla pre otvorenie kufra
const int lockButtonPin = 3;     // Pin tlačidla pre zamknutie vozidla
const int unlockButtonPin = 4;   // Pin tlačidla pre odomknutie vozidla
// -----
// Inicializácia počítačiel pre simuláciu rolling code
// -----
unsigned long lockCounter = 0;    // Počítadlo pre tlačidlo zamknutia
unsigned long unlockCounter = 0;  // Počítadlo pre tlačidlo odomknutia
unsigned long trunkCounter = 0;   // Počítadlo pre tlačidlo kufra
// -----
// Funkcia setup() - inicializácia systému
// -----
void setup() {
    Serial.begin(9600);            // Spustenie sériovej
    komunikácie pre ladenie (9600 baud)
    mySwitch.enableTransmit(10);   // Nastavenie pinu 10 pre
    vysielanie RF signálu

    // Nastavenie tlačidlových pinov ako vstupy s internými pull-up
    rezistormi
    pinMode(lockButtonPin, INPUT_PULLUP);
    pinMode(unlockButtonPin, INPUT_PULLUP);
    pinMode(trunkButtonPin, INPUT_PULLUP);
}
```

Samotné spracovanie stlačenia tlačidla prebieha podľa nasledovnej logiky:

- pomocou príkazu `digitalRead` sa zisťuje stav konkrétneho tlačidla;
- ak Arduino zistí, že tlačidlo bolo stlačené (pin je v logickom stave LOW), príslušné počítadlo (`lockCounter++`, `unlockCounter++` alebo `trunkCounter++`) sa inkrementuje;
- pomocou funkcie `sprintf` sa vytvorí správa vo formáte reťazca, kde predpona znaku označuje funkciu („L“ pre zamknutie, „U“ pre odomknutie, „T“ pre otvorenie kufra) a za ňou nasleduje aktuálna hodnota počítadla;
- výsledná správa sa odošle prostredníctvom metódy `mySwitch.send`.

Paralelne sa táto správa zobrazí aj na sériovom monitore pomocou príkazov `Serial.print` a `Serial.println`, čo umožňuje diagnostiku a monitorovanie správnosti komunikácie počas testovania. Po odoslaní správy nasleduje krátka časová medzera `delay(500)`, ktorá slúži na elimináciu nechceného viacnásobného zaznamenania stlačenia tlačidla v dôsledku mechanického kmitania kontaktov (tzv. debounce efekt). Spracovanie každej funkcie (zamknutie, odomknutie, otvorenie kufra) je identické, líši sa len použitím príslušnej premennej počítadla a predpony v generovanom kóde.

```

// Funkcia loop() - hlavný cyklus programu
// -----
void loop() {
    // Kontrola stlačenia tlačidla zamknutia
    if (digitalRead(lockButtonPin) == LOW) {
        lockCounter++; // Inkrementácia počítadla pre zamknutie
        char message[10];
        sprintf(message, "L%lu", lockCounter); // Vytvorenie správy v
tvare "L<číslo>"
        mySwitch.send(message); // Odoslanie správy cez
RF vysielateľ
        Serial.print("Odosielam: ");
        Serial.println(message); // Výpis odoslanej správy
na sériový monitor
        delay(500); // Krátka pauza na
zabránenie opakovania
    }

    // Kontrola stlačenia tlačidla odomknutia
    if (digitalRead(unlockButtonPin) == LOW) {
        unlockCounter++; // Inkrementácia počítadla pre odomknutie
        char message[10];
        sprintf(message, "U%lu", unlockCounter); // Vytvorenie správy
v tvare "U<číslo>"
        mySwitch.send(message); // Odoslanie správy
cez RF vysielateľ
        Serial.print("Odosielam: ");
        Serial.println(message);
        delay(500);
    }

    // Kontrola stlačenia tlačidla kufra
    if (digitalRead(trunkButtonPin) == LOW) {
        trunkCounter++; // Inkrementácia počítadla pre otvorenie kufra
        char message[10];
        sprintf(message, "T%lu", trunkCounter); // Vytvorenie správy v
tvare "T<číslo>"
        mySwitch.send(message); // Odoslanie správy cez
RF vysielateľ
        Serial.print("Odosielam: ");
        Serial.println(message);
        delay(500);
    }
}

```

5.3.2 Program pre prijatie signálu

Program prijímacej jednotky je postavený na kombinácii niekoľkých knižníc, ktoré zabezpečujú prácu s rôznymi perifériami. Na začiatku programu sú načítané knižnice Wire.h a LiquidCrystal_I2C.h pre komunikáciu a ovládanie LCD displeja cez I2C zbernicu, Servo.h na riadenie servomotora a RCSwitch.h na prijímanie bezdrôtových signálov z RF prijímača pracujúceho na frekvencii 433 MHz. V inicializačnej časti sú definované dôležité premenné a objekty programu. Pin určený pre ovládanie servomotora je definovaný ako servoPin, zatiaľ čo pin receiverPin slúži na pripojenie RF prijímača. Vytvára sa objekt lcd pre správu LCD displeja s adresou 0x27 a rozmermi 16x2 znakov, objekt servo na ovládanie servomotora a objekt mySwitch na správu prijímania RF signálov. Pre každý typ príkazu zamknutie, odomknutie a otvorenie kufra sa uchováva posledná prijatá hodnota počítadla. Tento mechanizmus slúži na detekciu a ochranu pred útokmi s prehratím signálu, kedy by mohol byť zachytený a opakovane odosielaný starý príkaz. Program inicializuje sériovú komunikáciu príkazom Serial.begin(9600), čo umožňuje výpis informácií do sériového monitora pre účely monitorovania a ladenia. RF prijímač je aktivovaný príkazom mySwitch.enableReceive(digitalPinToInterrupt(receiverPin)), ktorý umožňuje prijímanie signálov prostredníctvom prerušenia. Súčasne sa vykonáva inicializácia servomotora prostredníctvom servo.attach(servoPin), pričom motor sa nastaví do základnej polohy 90 stupňov, čo reprezentuje zamknutý stav. LCD displej sa inicializuje príkazom lcd.begin(16, 2) a podsvietenie sa aktivuje pomocou lcd.backlight(). Následne je na displeji zobrazený počiatočný stav systému prostredníctvom správy "Status: Locked".

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Servo.h>
#include <RCSwitch.h>

// Definovanie pinov pre pripojené komponenty
// -----
const int servoPin = 4;          // Pin pre ovládanie servomotora
const int receiverPin = 3;       // Pin pre príjem RF signálu (433 MHz)

// -----
// Inicializácia objektov LCD displeja, serva a RF prijímača
// -----
LiquidCrystal_I2C lcd(0x27, 16, 2); // LCD displej s I2C adresou 0x27
Servo servo;                      // Objekt servomotora
RCSwitch mySwitch = RCSwitch();  // RF prijímač

// -----
// Počítadlá očakávaných hodnôt pre príkazy
// -----
unsigned long expectedLockCounter = 0;
unsigned long expectedUnlockCounter = 0;
unsigned long expectedTrunkCounter = 0;

void setup() {
    Serial.begin(9600); // Inicializácia sériovej komunikácie

    // Aktivácia RF prijímača (na pine s prerušením)
    mySwitch.enableReceive(digitalPinToInterrupt(receiverPin));

    // Pripojenie servomotora k príslušnému pinu
    servo.attach(servoPin);
    servo.write(90); // Výchozia pozícia (zamknuté)

    // Inicializácia LCD displeja
    lcd.begin(16, 2); // Displej má 16 znakov a 2 riadky
    lcd.backlight(); // Zapnutie podsvietenia
    lcd.setCursor(0, 0);
    lcd.print("Status: Locked"); // Počiatočný stav
}
```

Počas chodu programu Arduino neustále kontroluje dostupnosť nového prijatého RF signálu. Ak je nový signál detegovaný, jeho hodnota sa načíta do premennej `receivedCode`. Takto prijatý kód sa ďalej spracúva tak, že sa rozdelí na dve časti: príkaz a počítadlo. Príkaz je reprezentovaný prvou číslicou kódu (1 pre zamknutie, 2 pre odomknutie, 3 pre otvorenie kufra), zatiaľ čo nasledujúce číslice reprezentujú počet stlačení tlačidla. Ak prijaté počítadlo predstavuje vyššiu hodnotu než predchádzajúca uložená hodnota a zároveň neprekračuje rozdiel troch jednotiek, tak prijatý príkaz je považovaný za legitímny. Na základe rozpoznaného príkazu Arduino vykoná príslušnú akciu. Pri zamknutí sa servo nastaví do polohy zodpovedajúcej zamknutému stavu a LCD displej zobrazí hlásenie "Status: Locked". V prípade odomknutia sa servo nastaví do polohy otvorenia a displej aktualizuje správu na "Status: Unlocked". Ak je prijatý legitímny príkaz na otvorenie kufra, Arduino krátko pohne servomotorom vpred a vzad, čím simuluje mechanizmus otvorenia kufra a zároveň zobrazí na displeji správu "Trunk Opened". V prípade, že prijatý signál s počítadlom nezodpovedá očakávanej hodnote, alebo ide o pokus o opätovné odoslanie starého kódu, systém na displeji vyhlási varovanie o detegovanom útoku. Po spracovaní každého príkazu je prijímač vyčistený, aby bol pripravený na príjem ďalšieho signálu.

```
void loop() {
    // Kontrola dostupnosti prijatého signálu
    if (mySwitch.available()) {
        unsigned long receivedCode = mySwitch.getReceivedValue(); //
        Prijatie signálu

        Serial.print("Received code: ");
        Serial.println(receivedCode);

        // Oddelenie identifikátora príkazu a počítadla
        unsigned long counter = receivedCode % 1000; // Posledné 3 číslice
        = počítadlo
        unsigned long command = receivedCode / 1000; // Prvé číslo =
        identifikátor (1, 2, 3)

        // Spracovanie príkazu podľa typu
        if (command == 1) { // Zamknutie
            if (counter > expectedLockCounter && (counter -
            expectedLockCounter) <= 3) {
                expectedLockCounter = counter; // Aktualizácia očakávaného
                počítadla
                servo.write(180); // Nastavenie serva do
                zamknutej pozície
                lcd.setCursor(0, 0);
                lcd.print("Status: Locked ");
            } else {
                Serial.println("Attack detected on lock button.");
                lcd.setCursor(0, 0);
                lcd.print("Attack detected! ");
            }
        }

        } else if (command == 2) { // Odomknutie
            if (counter > expectedUnlockCounter && (counter -
            expectedUnlockCounter) <= 3) {
                expectedUnlockCounter = counter;
                servo.write(0); // Nastavenie serva do
                odomknutej pozície
                lcd.setCursor(0, 0);
                lcd.print("Status: Unlocked ");
            } else {
                Serial.println("Attack detected on unlock button.");
                lcd.setCursor(0, 0);
                lcd.print("Attack detected! ");
            }
        }
    }
}
```

```
    }

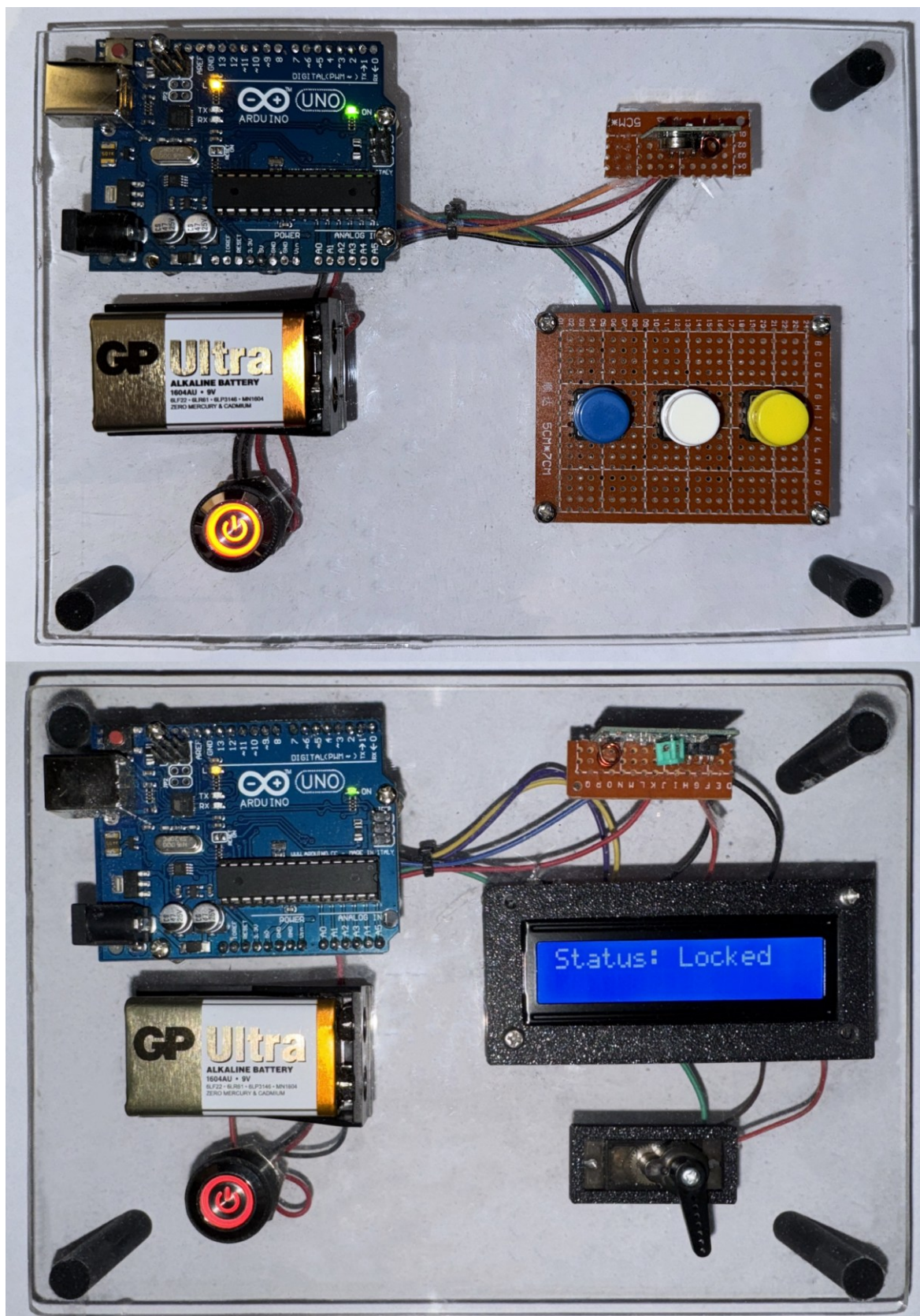
    } else if (command == 3) { // Otvorenie kufra
        if (counter > expectedTrunkCounter && (counter -
expectedTrunkCounter) <= 3) {
            expectedTrunkCounter = counter;
            lcd.setCursor(0, 0);
            lcd.print("Trunk Opened      ");

            // Dvojité otvorenie kufra pomocou pohybu serva
            for (int i = 0; i < 2; i++) {
                servo.write(0);
                delay(500);
                servo.write(180);
                delay(500);
            }
        } else {
            Serial.println("Attack detected on trunk button.");
            lcd.setCursor(0, 0);
            lcd.print("Attack detected! ");
        }
    }
}

// Vymazanie príznaku dostupnosti signálu
mySwitch.resetAvailable();
}}
```

5.4 Kompletizácia modelu

Po kompletnom zostavení hardvérových komponentov a nahratí softvéru bolo možné prakticky demonštrovať funkčnosť systému bezdrôtového zamykania vozidla s použitím plávajúceho kódu. Vysielacia jednotka pozostáva z dosky Arduino Uno, RF vysieláča pracujúceho na frekvencii 433 MHz, troch ovládacích tlačidiel, 9 voltovej batérie a hlavného napájacieho spínača. Každé tlačidlo reprezentuje jednu funkciu: zamknutie, odomknutie a otvorenie kufra. Po stlačení tlačidla Arduino vygeneruje jedinečný plávajúci kód, ktorý je bezdrôtovo prenesený k prijímacej jednotke. Tento proces simuluje fungovanie diaľkového ovládača vozidla, keď sa pri každom príkaze zabezpečuje unikátna autentifikácia signálu. Prijímacia jednotka je tvorená doskou Arduino Uno, RF prijímačom, servomotorom a LCD displejom. Po prijatí signálu Arduino vyhodnotí jeho platnosť pomocou algoritmu plávajúceho kódu. V prípade overenia správnosti kódu sa vykoná príslušná akcia. Servomotor prestaví mechanizmus zamknutia, alebo odomknutia a LCD displej aktualizuje svoj výstup napríklad zobrazením „Status: Locked“ alebo „Status: Unlocked“. Funkcia otvorenia kufra je simulovaná krátkym pohybom servomotora dopredu a dozadu, pričom displej zobrazí príslušnú správu. Model umožňuje simulovať celý proces bezdrôtového zamykania, od zadania príkazu, cez prenos a overenie signálu, až po vykonanie mechanickej akcie a vizualizáciu stavu. Vďaka použitiu plávajúceho kódu tento model efektívne demonštruje princípy moderných zabezpečených systémov centrálneho zamykania automobilov.



Obrázok 7 Kompletizácia modelu

(zdroj: vlastný)

6 NÁVRH ÚTOKU NA BEZDRÔTOVÝ SYSTÉM S PLÁVAJÚCIM KÓDOM

Cieľom tejto časti bolo prakticky demonštrovať možnosti realizácie útoku na model bezdrôtového zamykania automobilu využívajúceho plávajúci kód. Na realizáciu útoku boli použité zariadenia Flipper Zero a HackRF One PortaPack H4M, pričom samotný útok bol založený na princípe RollJam, ktorý kombinuje rušenie komunikácie, zachytávanie a prehrávanie signálu.

6.1 Použité zariadenia a softvér

Na realizáciu útoku RollJam boli použité zariadenia a softvérové nástroje, ktoré sú bežne dostupné na trhu a sú využívané pri výskume bezpečnosti bezdrôtových technológií. Zariadenia boli vybrané tak, aby pokrývali všetky fázy útoku od rušenia signálu, cez jeho zachytávanie, až po spätné prehratie.

6.1.1 Flipper Zero

Flipper Zero je kompaktné multifunkčné zariadenie určené na testovanie rôznych bezpečnostných technológií. Disponuje integrovaným RF modulom založeným na transceiveri Texas Instruments CC1101, ktorý umožňuje vysielanie a prijímanie signálov v pásmach 300-348 MHz, 387-464 MHz a 779-928 MHz. Tento čip podporuje rôzne druhy modulácie vrátane ASK, FSK, 2-FSK a dosahuje prenosovú rýchlosť až 500 kbps. Maximálny výstupný výkon anténneho signálu je 20 dBm. V rámci experimentu bol Flipper Zero použitý na dve kľúčové úlohy: na rušenie komunikácie medzi diaľkovým ovládačom a vozidlom v čase autentifikácie a na následné prehrávanie zachyteného signálu s cieľom simulovať legitímny príkaz od používateľa. Zariadenie je samostatne ovládateľné pomocou vstavaného displeja a tlačidiel bez potreby počítača. [38]

6.1.2 HackRF One PortaPack H4M

PortaPack je rozšírenie pre softvérovo definované rádio zariadenie HackRF One umožňujúce ovládanie bez potreby pripojenia k počítaču. Verzia Mayhem H4M obsahuje upravený firmvér s množstvom funkcií pre testovanie RF bezpečnosti. HackRF One pracuje v širokom frekvenčnom rozsahu od 1 MHz do 6 GHz a využíva 8-bitový analógovo-digitálny prevodník s rýchlosťou vzorkovania 20 MSPS, čo umožňuje zachytávanie a generovanie signálov vo vysokom časovom rozlíšení. Maximálny výstupný výkon vysielania dosahuje

približne 15 dBm. Používa sa na záznam, analýzu, prehrávanie a generovanie rušiacich signálov v rôznych frekvenčných pásmach. V rámci experimentu slúžilo na zachytávanie RF signálov z ovládača, ich spätné prehrávanie a tiež na vytváranie rušiaceho signálu počas fázy narušenia komunikácie. [39]

6.1.3 RTL-SDR

RTL-SDR je lacný SDR prijímač, ktorý bol využitý ako podporný nástroj na pasívne sledovanie frekvenčného spektra. Pracuje v rozsahu od 24 MHz do 1766 MHz a je postavený na čipovej sade RTL2832U. Vzorkovanie prebieha rýchlosťou 2,4 MSPS, čo je postačujúce na analýzu ASK a FSK signálov. Počas experimentov slúžil na vizualizáciu RF prenosov v reálnom čase, overenie vysielania a prijímania signálov, ako aj na kontrolu správneho načasovania rušenia. [40]

6.1.4 Softvérové vybavenie

Na efektívne pracovanie so zachytenými signálmi, ich analýzu a spätné vysielanie, bolo nevyhnutné zabezpečiť funkčné prepojenie hardvérových zariadení so zodpovedajúcim softvérovým vybavením. Každý z použitých nástrojov vyžadoval špecifický softvér, ktorý umožňoval jeho ovládanie, vizualizáciu dát a ich spracovanie. Softvérové nástroje boli vybrané s ohľadom na ich kompatibilitu s použitými zariadeniami, s ohľadom na ich dostupnosť a možnosti analýzy RF prenosov.

6.1.5 Momentum Firmware

Momentum Firmware je alternatívny firmvér pre zariadenie Flipper Zero. Rozširuje jeho možnosti najmä v oblasti práce s RF signálmi. Umožňuje širšiu podporu rôznych formátov, pokročilejšie skriptovanie a lepšiu kontrolu zachytávania a prehrávania RF komunikácie.

6.1.6 SDRSharp

SDRSharp je softvérový nástroj určený na vizualizáciu spektra RF signálov v reálnom čase. V kombinácii s RTL-SDR adaptérom bol používaný na monitoring priebehu útoku, sledovanie frekvenčnej aktivity a overovanie správneho priebehu rušenia a vysielania.

6.1.7 Universal Radio Hacker

Universal Radio Hacker je softvér navrhnutý na detailnú prácu so zachytenými RF signálmi. V experimente slúžil na analýzu dát získaných pomocou zariadení HackRF One

PortaPack a RTL-SDR, dekódovanie prenesených informácií, identifikáciu opakujúcich sa častí signálu a prípravu príkazov na spätné prehrávanie do cieľového zariadenia.

6.2 Priebeh útoku

Praktická realizácia útoku RollJam prebiehala v dvoch samostatných sériách s rôznou konfiguráciou zariadení. Cieľom zmeny konfigurácie bolo overiť účinnosť oboch možných scenárov: v prvom prípade Flipper Zero slúžil ako zariadenie na rušenie, zatiaľ čo HackRF One PortaPack vykonával zachytávanie a prehrávanie signálov. V druhom prípade boli úlohy obrátené. HackRF One PortaPack zabezpečoval rušenie a Flipper Zero zachytával autentifikačné signály. Oba scenáre mali prakticky dokázať, že aj pri rozdielnom hardvéri možno útok úspešne vykonať pokiaľ sú správne nastavené frekvencie, načasovanie a režimy zariadení.

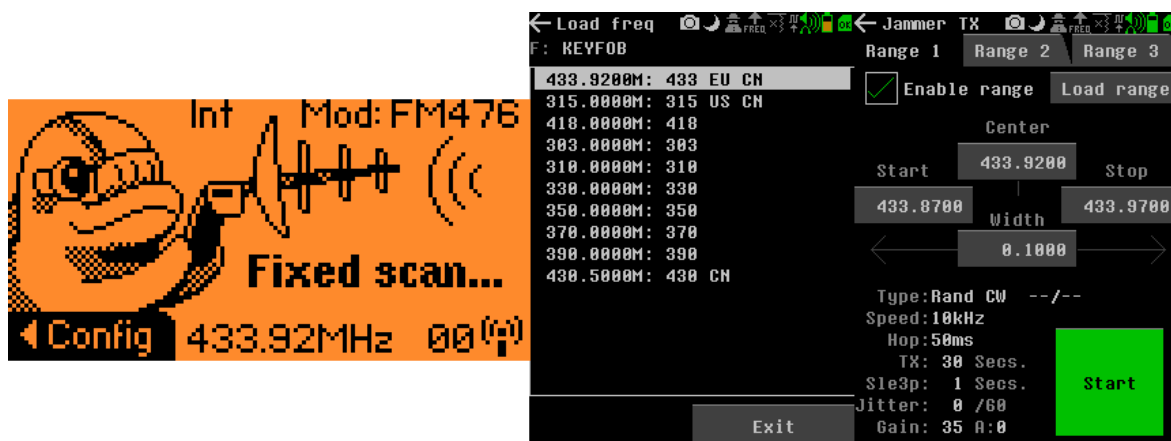


Obrázok 8 Dve konfigurácie zariadení Flipper Zero a Porta Pack

(zdroj: vlastný)

Prvým krokom bolo nakonfigurovanie zariadení do požadovaného stavu. Na Flipper Zero bol nainštalovaný Momentum Firmware, ktorý rozširuje funkčnosť zariadenia o pokročilé RF nástroje vrátane možnosti prehrávania a rušenia signálu. Inštalácia prebiehala jednoducho cez webové rozhranie vývojára systému. Do Flipper Zero boli následne nahraté vzorové súbory s rušiacimi signálmi, ktoré sú verejne dostupné na internete. [41] Alternatívne je možné tieto signály zachytiť priamo prostredníctvom HackRF One PortaPacku, ktorý obsahuje aplikáciu Jammer. Tá umožňuje zadať cieľovú frekvenciu a generovať rušivý signál.

HackRF One PortaPack bol pripravený pomocou vstavaného rozhrania, pričom sa využívali nástroje na záznam signálu, spätné prehrávanie a rušenie signálu. Všetky nastavenia sa vykonávali priamo cez displej zariadenia bez nutnosti pripojenia k počítaču.



Obrázok 9 Príklad nastavení Flipper Zero a PortaPack

(zdroj: vlastný)

6.2.1 Scenár č. 1: Flipper Zero ako rušič, HackRF One PortaPack ako prijímač

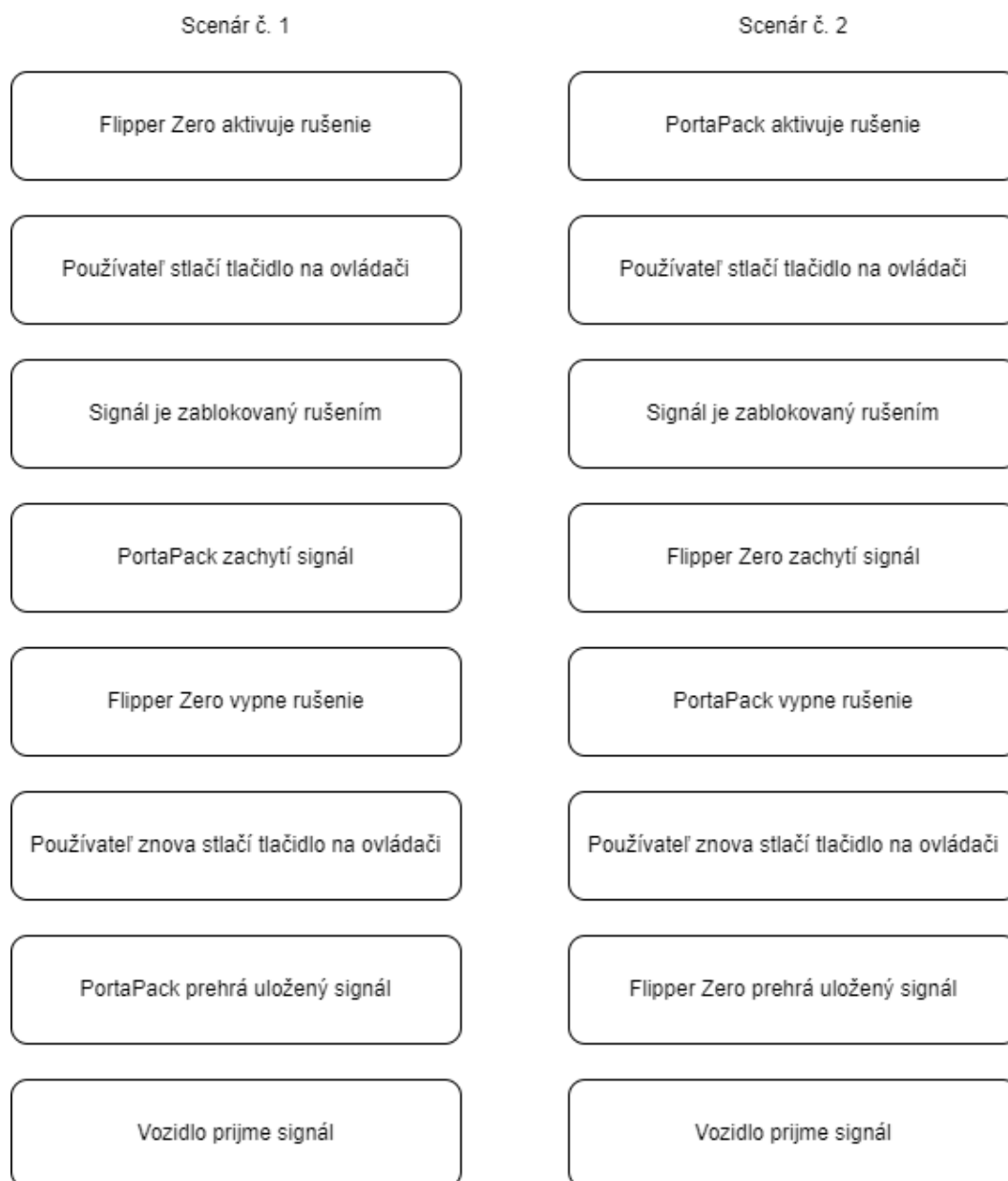
V scenári č. 1 Flipper Zero generoval rušiaci signál na frekvencii 433 MHz, čím sa znemožnilo doručenie autentifikačného kódu z diaľkového ovládača do vozidla. Súčasne HackRF One PortaPack zachytil tento signál, uložil ho a neskôr bol použitý na jeho prehratie. Postup prebiehal nasledovne:

1. Flipper Zero spustil rušenie pomocou uloženého signálu;
2. v momente, keď používateľ stlačil tlačidlo na ovládači, rušenie znemožnilo spracovanie signálu vozidlom;
3. PortaPack v režime „Capture“ zachytil autentifikačný signál, ktorý nebol prijatý;
4. po ukončení rušenia majiteľ vozidla zvyčajne zopakuje príkaz, tentoraz úspešne;
5. zachytený signál zostáva nepoužitý a HackRF One PortaPack ho následne prehrá.

6.2.2 Scenár č. 2: HackRF One PortaPack ako rušič, Flipper Zero ako prijímač

V scenári č. 2 bol na rušenie použitý HackRF One PortaPack, ktorý spustil aplikáciu Jammer. Flipper Zero bol súčasne pripravený na prijímanie signálu. Priebeh bol rovnaký ako v predchádzajúcom scenári, iba so zmenenými úlohami zariadení:

1. HackRF One PortaPack ruší prenos medzi ovládačom a vozidlom na frekvencii 433 MHz;
2. počas rušenia Flipper Zero zaznamenal RF signál vyslaný diaľkovým ovládačom;
3. vozidlo signál neprijalo, no Flipper Zero si ho uložil;
4. po ukončení rušenia používateľ zopakoval príkaz, na ktorý vozidlo zareagovalo;
5. neskôr Flipper Zero prehrá pôvodný zachytený signál a vozidlo ho akceptovalo.



Obrázok 10 Diagram scénárov testovania

(zdroj: vlastný)

7 TESTOVANIE ÚTOKU

Fáza testovania bola rozdelená do dvoch samostatných častí. Testovanie v laboratórne kontrolovanom prostredí a testovanie v reálnych podmienkach. Cieľom tejto dvojfázovej metodiky bolo komplexne posúdiť praktickú uskutočniteľnosť a efektivitu útoku na rôzne systémy využívajúce plávajúci kód, ktorý je v súčasnosti jedným z najrozšírenejších spôsobov zabezpečenia zariadení ovládaných rádiovou komunikáciou.

V prvej fáze sa testovanie realizovalo v izolovanom laboratórnom prostredí na modeli systému centrálného zamykania zostavenom pomocou mikrokontroléra Arduino UNO a bezdrôtového RF modulu s pevne stanovenou frekvenciou 433 MHz. V tomto prostredí boli vytvorené ideálne podmienky pre zachytávanie a prehrávanie signálov bez vonkajšieho elektromagnetického rušenia, bez prekážok a s možnosťou presnej kontroly vzdialeností aj načasovania. Laboratórne testovanie slúžilo predovšetkým na overenie technickej funkčnosti útoku, odladenie zariadení a identifikáciu ich limitov.

V druhej fáze sa testovanie presunulo do reálneho prostredia kde boli útoky simulované na skutočných cieľoch, konkrétne na automatickej bráne a 3 vozidlách vyrobených v rôznych rokoch 2015, 2019, 2024. Tieto testy prebiehali v prostredí s prítomnosťou reálneho rušenia ako napríklad iné bezdrôtové prenosy, kovové a reflektívne predmety v okolí, premenlivé počasie, či blízkosť iných vozidiel vysielajúcich RF signály. Táto fáza testovania slúžila na overenie uskutočniteľnosti útoku v podmienkach, ktoré najviac zodpovedajú reálnemu svetu a každodennému použitiu bezdrôtových uzamykacích systémov.

Testovanie bolo zamerané najmä na zachytenie autentifikačného kódu v čase, keď je komunikácia medzi diaľkovým ovládačom a prijímačom úmyselne rušená, možnosť spätného prehratia zachyteného signálu po odstránení rušenia s cieľom simulovať legitímny príkaz používateľa a reakciu cieľového systému na takto získaný príkaz. Takto rozdelená a štruktúrovaná fáza testovania umožnila objektívne porovnať správanie zabezpečovacích systémov v ideálnych podmienkach oproti reálnym, a tým odhaliť ich praktickú odolnosť voči útoku.

7.1 Testovanie v laboratórnych podmienkach

Testovanie v laboratórnych podmienkach sa uskutočnilo na modeli systému centrálného zamykania vytvorenom pomocou mikrokontroléra Arduino UNO, ktorý komunikoval prostredníctvom RF vysielачa a prijímača na frekvencii 433 MHz. Systém bol

naprogramovaný tak, aby simuloval fungovanie plávajúceho kódu, kde každý nový príkaz generoval iný kód v sekvencii a prijímač akceptoval len tie kódy, ktoré ešte neboli spracované. Vzdialenosť medzi vysielajúcim a prijímacím Arduino bola počas všetkých testov fixne nastavená na 2 metre, aby sa eliminoval vplyv ich vzájomnej vzdialenosti na výsledky. Menila sa iba vzdialenosť medzi útočnými zariadeniami a cieľovým systémom.

Na testovanie boli použité dve rôzne zostavy zariadení, ktoré sa striedali v úlohách rušiaceho a prijímacieho komponentu. Účelom bolo posúdiť, ako rôzne kombinácie ovplyvnia schopnosť útoku a či má zmena rolí vplyv na výsledok. V oboch prípadoch sa použili rovnaké zariadenia Flipper Zero (FZ) a HackRF One PortaPack (PP), pričom v prvom scenári plnil Flipper Zero úlohu rušiaceho zariadenia a HackRF One PortaPack zabezpečoval príjem a opätovné vysielanie (p/v) signálu. V druhom scenári sa úlohy zariadení vymenili. HackRF One PortaPack bol použitý ako rušič a Flipper Zero ako prijímacie/vysielacie zariadenie. Každý scenár obsahoval testy pri troch vzdialenostiach: 1 m, 5 m a 10 m, pričom sa pre každú vzdialenosť realizovalo päť opakovaní.

Tabuľka 1 Prehľad útokov na Arduino Uno

Arduino Uno	Vzdialenosť	Pokus č. 1	Pokus č. 2	Pokus č. 3	Pokus č. 4	Pokus č. 5
Scenár č. 1: FZ - rušenie, PP - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	×	✓	✓
Scenár č. 2: PP - rušenie, FZ - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	✓	✓	×
Legenda	✓	Úspešný pokus		×	Neúspešný pokus	

(zdroj: vlastný)

Testovanie ukázalo, že útok RollJam je v laboratórnych podmienkach veľmi stabilný a opakovateľný, najmä pri vzdialenostiach do 5 metrov. Všetky pokusy boli úspešné pri vzdialenostiach 1 m a 5 m bez ohľadu na použitú konfiguráciu zariadení. Pri vzdialenosti 10 metrov došlo len k dvom zlyhaniam z celkovo 10 pokusov a to v jednom prípade pri prehrávaní signálu HackRF One PortaPackom – Scenár č. 1 a v jednom prípade pri prehrávaní Flipperom Zero – Scenár č. 2. Zlyhanie pri tejto vzdialenosti mohlo byť spôsobené viacerými faktormi. Napríklad dočasnou stratou synchronizácie medzi rušením a záznamom signálu, kolísaním úrovne prijímaného signálu, nepresným časovaním rušenia alebo drobnými elektromagnetickými interferenciami v prostredí, ktoré sa inak považovalo za kontrolované. Z pohľadu praktického nasadenia testy ukázali, že aj vzdialenosť 10 metrov

nepredstavuje zásadnú prekážku pre úspešné vykonanie útoku RollJam, ak sú splnené technické predpoklady.

7.2 Testovanie v reálnych podmienkach

Po úspešnej realizácii útoku v laboratórnom prostredí nasledovala druhá fáza testovania, zameraná na overenie praktickej účinnosti útoku typu RollJam v podmienkach, ktoré viac zodpovedajú reálnemu svetu. Testovanie prebiehalo na vonkajšom parkovisku obchodného centra počas štandardnej prevádzky. Hlavným cieľom tejto časti testovania bolo zistiť ako sa systém správa v prostredí s reálnym RF rušením, fyzickými prekážkami, odrazmi signálu a inými premennými, ktoré nemožno presne kontrolovať. Testovanie bolo realizované na štyroch cieľových systémoch vrátane automatickej posuvnej brány s implementovaným plávajúcim kódom a troch vozidlách z výrobných rokov 2016, 2019 a 2024. Vozidlá z rokov 2019 a 2024 boli vybavené systémom bezkľúčového prístupu a reprezentovali moderné implementácie bezdrôtového zamykania s pravdepodobnou vyššou úrovňou zabezpečenia.

Vo všetkých prípadoch bola počas testovania dodržaná fixná vzdialenosť 2 metre medzi ovládačom (alebo kľúčom) a cieľovým systémom teda medzi používateľom a jeho vozidlom či bránou. Tento model vychádzal z realistického scenára, kde má používateľ ovládač pri sebe (napríklad v ruke, alebo vo vrecku), keď prístupuje k autu alebo k bráne. Vzdialenosť zariadení na útok sa menila na 1, 5, 10 a 20 metrov. Zahrnutie minimálnej vzdialenosti 1 meter slúžilo na porovnanie správania systému v optimálnych podmienkach, zatiaľ čo vzdialenosti 5 až 20 metrov simulovali reálne scenáre, v ktorých by sa útočník nachádzal v dostatočnej vzdialenosti, aby nevzbudzoval podozrenie.

Pri automatickej bráne, ktorá používala ovládač na frekvencii 433,92 MHz s jednoduchým plávajúcim kódom, bol útok úspešný vo všetkých testovaných vzdialenostiach. Signál sa podarilo bez problémov zachytiť a následne prehrať, pričom brána reagovala ako keby išlo o originálny príkaz. Brána nedisponovala žiadnym pokročilým overovaním, ani ochranou proti opakovaniu, čo sa ukázalo ako kritické z hľadiska bezpečnosti.

Tabuľka 2 Prehľad útokov na automatickú bránu

Automatická brána	Vzdialenosť	Pokus č. 1	Pokus č. 2	Pokus č. 3	Pokus č. 4	Pokus č. 5
Scenár č. 1: FZ - rušenie, PP - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	✓	✓	✓
	20 m	✓	✓	✓	✓	✓
Scenár č. 2: PP - rušenie, FZ - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	✓	✓	✓
	20 m	✓	✓	✓	✓	✓
Legenda	✓	Úspešný pokus		×	Neúspešný pokus	

(zdroj: vlastný)

Pri vozidle z roku 2016, ktoré používalo klasický diaľkový ovládač bez funkcie keyless, boli všetky pokusy opäť úspešné bez ohľadu na vzdialenosť útočníka. Signál sa podarilo zachytiť a prehrať aj pri vzdialenosti 20 metrov. To dokazuje, že staršie zabezpečovacie systémy bez pokročilej autentifikácie sú extrémne zraniteľné.

Tabuľka 3 Prehľad útokov na vozidlo z roku 2016

Vozidlo z roku 2016	Vzdialenosť	Pokus č. 1	Pokus č. 2	Pokus č. 3	Pokus č. 4	Pokus č. 5
Scenár č. 1: FZ - rušenie, PP - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	✓	✓	✓
	20 m	✓	✓	✓	✓	✓
Scenár č. 2: PP - rušenie, FZ - p/v	1 m	✓	✓	✓	✓	✓
	5 m	✓	✓	✓	✓	✓
	10 m	✓	✓	✓	✓	✓
	20 m	✓	✓	✓	✓	✓
Legenda	✓	Úspešný pokus		×	Neúspešný pokus	

(zdroj: vlastný)

Vozidlo z roku 2019 už disponovalo keyless technológiou. Pri testovaní, keď sa ovládač nachádzal vo vzdialenosti 2 metre od auta a útočné zariadenia sa nachádzali vo vzdialenostiach 1, 5, 10 a 20 metrov, boli pri nižších vzdialenostiach prvé dva pokusy úspešné. V treťom pokuse došlo k chybe prehratia signálu a následne vozidlo prestalo reagovať aj na originálny kľúč. Vozidlo ho vyhodnotilo ako neplatný a odmietalo jeho použitie. Bolo potrebné opätovne synchronizovať kľúč s vozidlom. To svedčí o tom,

že bezpečnostný mechanizmus je aktívny, nakoľko detegoval narušenie sekvencie alebo podozrivú aktivitu. Pri vzdialenostiach 5, 10 a 20 metrov už nebol ani jeden pokus úspešný z dôvodu účinnejšieho potlačenia neautorizovanej komunikácie a vyradenie kľúča.

Tabuľka 4 Prehľad útokov na vozidlo z roku 2019

Vozidlo z roku 2019	Vzdialenosť	Pokus č. 1	Pokus č. 2	Pokus č. 3	Pokus č. 4	Pokus č. 5
Scenár č. 1: FZ - rušenie, PP - p/v	1 m	✓	✓	×	×	×
	5 m	×	×	×	×	×
	10 m	×	×	×	×	×
	20 m	×	×	×	×	×
Scenár č. 2: PP - rušenie, FZ - p/v	1 m	×	×	×	×	×
	5 m	×	×	×	×	×
	10 m	×	×	×	×	×
	20 m	×	×	×	×	×
Legenda	✓	Úspešný pokus		×	Neúspešný pokus	

(zdroj: vlastný)

Vozidlo z roku 2024 preukázalo úplnú odolnosť voči útoku. Počas testovania, ak bol kľúč opäť umiestnený vo vzdialenosti 2 metre a útočné zariadenie sa pohybovalo vo vzdialenostiach 1 až 20 metrov, sa nepodarilo zachytiť a ani prehrať signál tak, aby ho vozidlo prijalo. Vozidlo nijako nereagovalo, neukázalo známky zachytenia o spracovanie signálu a všetky pokusy zlyhali. Dá sa predpokladať, že ide o moderný systém s viacnásobným overovaním zahŕňajúcim časovú synchronizáciu, kontrolu sekvenčného počítadla, a pravdepodobne aj kryptografickú autentifikáciu medzi kľúčom a vozidlom.

Tabuľka 5 Prehľad útokov na vozidlo z roku 2024

Vozidlo z roku 2024	Vzdialenosť	Pokus č. 1	Pokus č. 2	Pokus č. 3	Pokus č. 4	Pokus č. 5
Scenár č. 1: FZ - rušenie, PP - p/v	1 m	×	×	×	×	×
	5 m	×	×	×	×	×
	10 m	×	×	×	×	×
	20 m	×	×	×	×	×
Scenár č. 2: PP - rušenie, FZ - p/v	1 m	×	×	×	×	×
	5 m	×	×	×	×	×
	10 m	×	×	×	×	×
	20 m	×	×	×	×	×
Legenda	✓	Úspešný pokus		×	Neúspešný pokus	

(zdroj: vlastný)

Výsledky testovania v reálnych podmienkach preukázali, že útok RollJam je plne realizovateľný pri systémoch bez pokročilého zabezpečenia a to aj na vzdialenosti, pri ktorých by bol útočník v bežnej situácii nenápadný. Moderné vozidlá implementujúce viacúrovňovú ochranu sú voči tomuto typu útoku vysoko odolné. Závažným zistením bol prípad vozidla z roku 2019, keď útok spôsobil desynchronizáciu legitímneho kľúča, čím sa vyradil z prevádzky aj originálny používateľ. Tento efekt môže predstavovať bezpečnostné riziko aj z pohľadu používateľskej dostupnosti systému.

7.3 Vyhodnotenie útokov

Testovanie prebiehalo v dvoch etapách. Najprv v kontrolovanom laboratórnom prostredí, následne v podmienkach zodpovedajúcich bežnému používaniu bezdrôtového zamykania. Výsledky týchto dvoch fáz pokusov poskytli komplexný pohľad na praktickú uskutočniteľnosť útoku typu RollJam, jeho limity a účinnosť ochranných opatrení implementovaných v rôznych generáciách zabezpečovacích systémov.

V laboratórnych podmienkach boli výsledky stabilné, s vysokou úspešnosťou najmä pri kratších vzdialenostiach. Ukázalo sa, že útok je plne realizovateľný pri vzdialenostiach do 5 metrov, bez ohľadu na použitú konfiguráciu zariadení Flipper Zero alebo HackRF One PortaPack. K zlyhaniu dochádzalo až pri vzdialenosti od 10 metrov, a aj to len výnimočne. Táto fáza testovania potvrdila, že ak nie sú prítomné rušivé faktory alebo prekážky, technicky nie je problém útok zrealizovať.

Reálne testovanie ukázalo, že prax je omnoho náročnejšia. Zatiaľ čo staršie systémy ako automatická brána a vozidlo z roku 2016 boli napadnuteľné bez ohľadu na vzdialenosť, novšie technológie vykazovali obranné reakcie. Vozidlo z roku 2019, hoci bolo spočiatku zraniteľné, po prehratí signálu aktivovalo ochranný režim, ktorý spôsobil desynchronizáciu legitímneho kľúča. To predstavuje výrazný bezpečnostný prvok, ktorý síce nezabránil útoku úplne, no minimalizoval jeho následky a znemožnil ďalšie opakovanie. Vozidlo z roku 2024 bolo voči útoku úplne odolné. Systém pravdepodobne používal kombináciu kryptografických kontrol, sekvenčnej logiky a časového overenia, vďaka čomu bol schopný detegovať neautorizovaný zásah a ignorovať prehrávané signály. Tento výsledok jasne ukazuje kam smeruje vývoj zabezpečenia a aké riešenia sú v praxi účinné.

Z pohľadu útočníka je zrejmé, že úspešnosť útoku závisí nielen od hardvéru a vzdialenosti, ale predovšetkým od samotnej architektúry zabezpečovacieho systému cieľa. Zariadenia ako Flipper Zero a HackRF One PortaPack ponúkajú dostatočný výkon aj

vo vzdialenostiach nad 10 metrov v prípade, ak im v tom nebráni aktívna ochrana na strane prijímača. Výsledky zároveň ukazujú, že ani výmena rolí medzi zariadeniami nemá zásadný vplyv na úspešnosť. To poukazuje na vysokú flexibilitu útočnej metódy pri práci s týmito zariadeniami.

V prípade novších vozidiel vybavených bezkľúčovým prístupom by bol hľadiska efektivity útoku pravdepodobne vhodnejší reléový útok. Ten nepracuje so zachytením a opakovaním signálu, ale s jeho okamžitým predĺžením medzi kľúčom a vozidlom v reálnom čase. Tento typ útoku je technicky náročnejší a vyžaduje špecializované zariadenia schopné obojsmerného prenosu s nízkou latenciou. Takéto nástroje nie sú bežne dostupné a ich obstaranie predstavuje pre bežného útočníka výraznú prekážku.

Na základe výsledkov testovania možno konštatovať, že pri starších systémoch je nevyhnutné zvyšovať úroveň zabezpečenia, najmä implementáciou ochrany proti prehratiu signálu, časovým obmedzením platnosti autentifikačného kódu a kontrolou sekvenčných skokov. Pre domácnosti, ktoré používajú ovládače brán s jednoduchým plávajúcim kódom, je dôležité zvážiť modernizáciu, alebo dodatočnú ochranu týchto systémov. Pri systémoch keyless je vhodné dbať aj na fyzickú ochranu kľúčov, ich uskladňovanie v tienených puzdách, ktoré znemožnia vzdialené zosilňovanie signálu. Rovnako dôležitá je aj informovanosť používateľov o rizikách, ktoré s bezdrôtovým ovládaním prichádzajú a potrebe správať sa zodpovedne – nenechávať kľúče blízko vstupov do budov či pri oknách.

Výsledky testovania ukazujú, že hoci sú niektoré typy útokov technicky nenáročné a realizovateľné bežne dostupným vybavením, správne implementované bezpečnostné mechanizmy ich dokážu efektívne znefunkčniť. To potvrdzuje význam dôsledného návrhu bezpečnostných protokolov v bezdrôtových systémoch a potrebu neustáleho vývoja ochranných technológií.

7.4 ODPORÚČANIA NA ZVÝŠENIE BEZPEČNOSTI

Na zvýšenie odolnosti bezdrôtových systémov vo vozidlách je nevyhnutné zaviesť prísnejšiu sekvenčnú logiku. Prijímač by mal spracovávať iba kódy nachádzajúce sa v úzko definovanom okne sekvenčných hodnôt. Ak dôjde k prijatiu kódu mimo tohto rozsahu, systém by mal automaticky spustiť dodatočné overenie alebo daný príkaz odmietnuť. Dôležité je tiež sledovať trend inkrementácie sekvencie. Výrazné skoky by mali byť limitované, pričom akékoľvek odchýlky od bežného postupu môžu naznačovať pokus o útok, alebo stratu synchronizácie medzi ovládačom a prijímačom. Ďalším dôležitým

bezpečnostným prvkom je časové obmedzenie platnosti autentifikačných kódov. Každý kód by mal byť platný len niekoľko sekúnd, čím sa výrazne znižuje riziko jeho neskoršieho zneužitia prostredníctvom prehratia. Rovnako dôležité je, aby bol každý autentifikačný kód po úspešnom spracovaní jednoznačne a nenávratne vyradený. Systém by mal byť schopný zaznamenať každý pokus o opätovné použitie rovnakého kódu a vyhodnotiť ho ako incident.

Bezpečnosť možno výrazne posilniť integráciou kryptografických mechanizmov do procesu autentifikácie. Použitie symetrických algoritmov, ako je HMAC (Hash-based Message Authentication Code), alebo AES, by výrazne sťažilo interpretáciu zachytených signálov bez prístupu k zdieľanému kľúču. V ideálnom prípade by mala byť komunikácia medzi kľúčom a vozidlom založená na asymetrickej kryptografii, ktorá využíva páry verejných a súkromných kľúčov, čím sa minimalizuje riziko kompromitácie aj pri zachytení celej výmeny. Systém by mal byť schopný aktívne identifikovať anomálie v prenose a reagovať adekvátnym spôsobom. Ak dôjde k opakovanému rušeniu signálu, zvýšenému počtu neúspešných autentifikácií alebo opakujúcim sa vzorom v prenose, je vhodné bezdrôtové ovládanie dočasne zablokovať. Zároveň by malo byť možné aktivovať výstražné systémy, akými sú akustický alarm alebo vizuálna signalizácia a vyžadovať fyzické overenie používateľa priamo vo vozidle.

Z praktických opatrení je vhodné odporučiť používanie fyzickej ochrany - napríklad tienených puzdier na kľúče (Faradayových obalov), ktoré dokážu účinne blokovat' rádiové vlny. Tým sa eliminuje možnosť neúmyselného zosilnenia alebo predlžovania signálu, čo je obzvlášť dôležité pri bezkľúčových (keyless) systémoch. Okrem toho je rozumné parkovať vozidlá mimo priameho dohľadu potenciálnych útočníkov v uzavretých alebo strážených priestoroch. V každom prípade by mal byť používateľ informovaný o bezpečnostných rizikách spojených s používaním bezdrôtových systémov. Zvýšenie povedomia o správnom používaní týchto technológií (neodomykať vozidlo z veľkej vzdialenosti, pravidelne aktualizovať softvér a byť obozretný v neznámom prostredí) výrazne prispieva k celkovej bezpečnosti systému. Prevencia, školenie a informovanosť zohrávajú kľúčovú úlohu pri znižovaní zraniteľností a posilňovaní dôveryhodnosti moderných vozidiel.

8 BEZPEČNOSTNÁ ANALÝZA MOBILNÝCH APLIKÁCIÍ

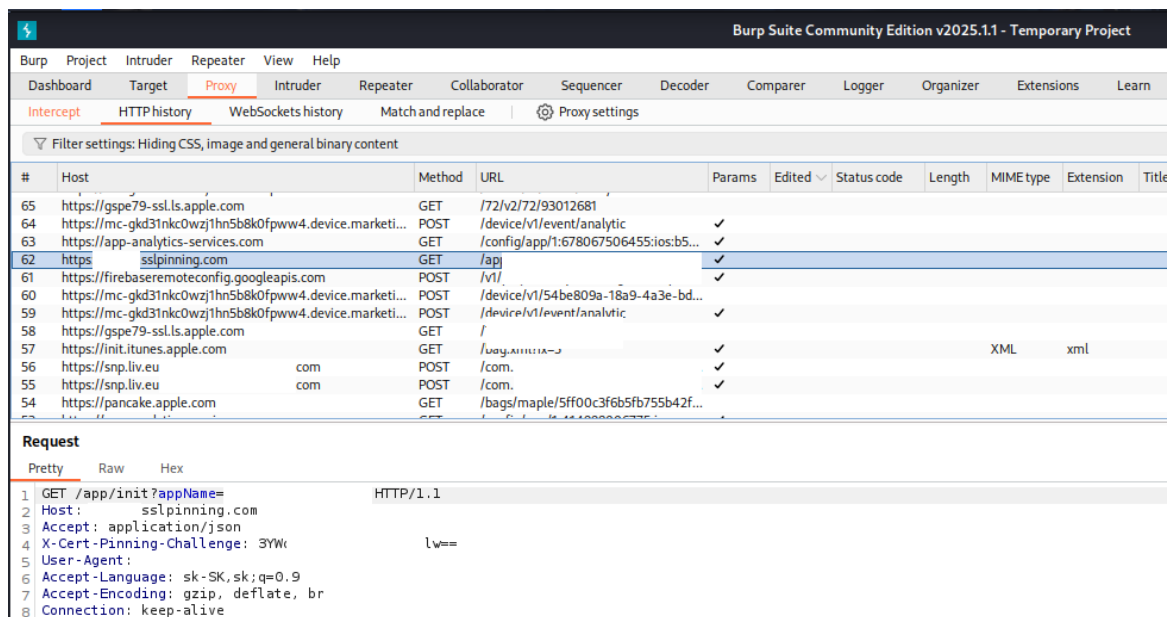
Mobilné aplikácie na správu vozidla umožňujú používateľovi monitorovať a ovládať vozidlo na diaľku prostredníctvom smartfónu alebo tabletu, pričom komunikujú s backend servermi automobilky a následne so samotnou telematickou jednotkou vozidla. Analýza zahŕňala statickú analýzu aplikačných súborov prostredníctvom nástroja MobSF, ako aj dynamické testovanie sieťovej komunikácie zamerané na identifikáciu potenciálnych slabín, ktoré by mohli byť zneužitú útočníkom.

8.1 Zachytávanie sieťovej komunikácie a SSL ochrana

Súčasťou analýzy mobilných aplikácií bola dynamická kontrola bezpečnosti sieťovej komunikácie medzi aplikáciami a vzdialenými backend servermi výrobcov. Pokus o zachytávanie dát prebiehal na zariadení s operačným systémom Android 14, pričom bol využitý nástroj Burp Suite spustený v prostredí Kali Linux. Mobilné zariadenie bolo pripojené do rovnakej Wi-Fi siete ako Burp proxy server a v jeho nastaveniach bola manuálne nakonfigurovaná HTTP proxy adresa. Pre zachytávanie šifrovanej komunikácie bol do Android nainštalovaný vlastný certifikát Burp Suite typu Certificate Authority (CA), ktorému bola explicitne povolená dôvera v systémových nastaveniach.

Po týchto prípravách bolo možné monitorovať a analyzovať komunikáciu medzi zariadením a servermi aplikácií. Všetky tri analyzované aplikácie využívali zabezpečený komunikačný protokol HTTPS, ktorý zodpovedá aktuálnym bezpečnostným štandardom a zabezpečuje dôvernú a integritu prenášaných údajov. Počas analýzy sa však ukázalo, že dve z aplikácií implementovali techniku certificate pinning. Táto bezpečnostná metóda zaisťuje, že aplikácia akceptuje len konkrétne verejné kľúče serverových certifikátov, čím sa znemožňuje zachytávanie a modifikácia šifrovanej komunikácie aj v prípade, že v systéme je nainštalovaný dôveryhodný CA certifikát.

V prípade jednej z analyzovaných aplikácií bol počas zachytávania komunikácie detegovaný priamy dôkaz o použití certificate pinningu a to prostredníctvom spojenia s rôznymi servermi - napríklad pomocou domény sslpinning.com. Táto doména naznačovala nielen aktívnu kontrolu certifikátu, ale aj to, že akékoľvek pokusy o Man-in-the-Middle útok by boli neúspešné. Burp Suite nedokázal dešifrovať prenášané dáta, čím sa potvrdila správna implementácia SSL pinningu a vysoká úroveň zabezpečenia.



Obrázok 11 Overovanie certifikátu aplikácie

(zdroj: vlastný)

Tretia analyzovaná aplikácia certificate pinning neobsahovala. To umožnilo plný prístup k šifrovanej komunikácii prostredníctvom MITM proxy, čo zahŕňalo možnosť čítať, upravovať a analyzovať jednotlivé požiadavky a odpovede smerované na server. Z pohľadu sieťovej bezpečnosti predstavuje absencia certificate pinningu vážnu slabinu, ktorá môže viesť k narušeniu dôvernosti údajov, kompromitácii prístupových tokenov alebo manipulácii s požiadavkami.

Výsledky dynamickej analýzy ukazujú, že používanie štandardného šifrovania cez HTTPS je dnes už očakávaným minimom, no v mnohých prípadoch to nemusí postačovať. Rozdiely v implementácii pokročilých ochranných mechanizmov akým je certificate pinning, priamo ovplyvňujú schopnosť aplikácie odolávať pasívnemu sledovaniu a aktívnym útokom prostredníctvom kompromitovanej siete.

8.2 Statická analýza aplikací

Z důvodu obmedzených možností dynamického testovania, najmä v prípadoch, keď aplikácie implementovali certificate pinning, bola vykonaná doplňujúca statická analýza všetkých troch aplikácií. Použitý bol nástroj Mobile Security Framework (MobSF), ktorý umožňuje spätnú dekompiláciu aplikačných súborov a identifikáciu potenciálnych slabín bez potreby spustenia samotnej aplikácie. Testovanie prebehlo na webovej platforme <https://mobsf.live>, kde boli nahrané inštalačné súbory všetkých aplikácií.

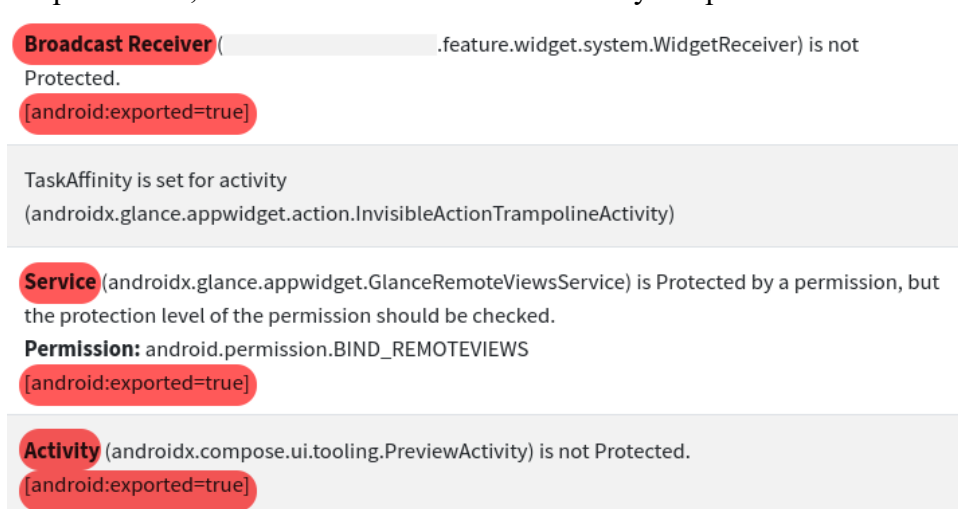
Vo všetkých troch analyzovaných aplikáciách bola detegovaná prítomnosť tvrdokódovaných citlivých údajov priamo v zdrojovom kóde. Išlo najmä o reťazce obsahujúce `client_id`, `client_secret`, šifrovacie kľúče, interné API identifikátory a ďalšie tokeny, ktoré by v produkčnej aplikácii nemali byť verejne prístupné. Takýto prístup predstavuje vážne bezpečnostné riziko, keďže útočník môže po získaní APK súboru tieto hodnoty extrahovať a použiť na vytváranie neautorizovaných požiadaviek voči backend serverom výrobcu. Tento typ zraniteľnosti patrí pod bod M9: Insecure Data Storage podľa OWASP Mobile Top 10 2024. [42] Ide síce o problém na strane klienta, jeho dôsledky môžu byť kritické najmä ak nie sú na serveri implementované dodatočné overenia.

STANDARDS	FILES
CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	Show Files /marketingcloud/registration/Registration.java /api/bff/v1/ParkingAccountDto.java /api/bff/v1/ToDoDto.java /api/bff/v1/infrastructure/ApiClient.java /api/bff_air_conditioning/v2/infrastructure/ApiClient.java /api/bff_car_configurator/v3/infrastructure/ApiClient.java

Obrázok 12 Detekcia tvrdokódovaných API kľúčov aplikácie B

(zdroj: vlastný)

MobSF analýza odhalila, že v jednej z testovaných aplikácií (aplikácia A) sa nachádzali komponenty (Activities, Services, BroadcastReceivers) definované s atribútom `exported="true"` bez špecifikovaného oprávnenia (permission). To znamená, že iná aplikácia nainštalovaná na rovnakom zariadení by mohla tieto komponenty vyvolať a potenciálne zneužiť ich funkcionality bez vedomia používateľa. Tento typ zraniteľnosti je známy ako component hijacking a patrí medzi časté chyby v konfigurácii Android aplikácií. Môže viesť k spúšťaniu vnútorných operácií mimo kontroly vývojára a používateľa, a tým sa zníži integrita celej aplikácie. Ostatné dve testované aplikácie mali komponenty správne nakonfigurované buď neboli exportované (`exported="false"`) alebo boli chránené vhodne zvoleným oprávnením, čím sa zamedzilo ich zneužitie inými aplikáciami.



Obrázok 13 Component hijacking v aplikácii A

(zdroj: vlastný)

Dve z troch analyzovaných aplikácií (A a C) využívali komponentu `WebView` s povoleným vykonávaním JavaScriptu. Pokiaľ aplikácia načítava do `WebView` externý obsah alebo generuje HTML stránky na základe dynamického vstupu, vzniká priestor pre JavaScript Injection, čo môže viesť k vykonaniu škodlivého kódu v prostredí aplikácie. MobSF odhalil, že neexistujú žiadne dodatočné kontroly vstupu pri práci s `WebView`, a ani obmedzenia na úrovni domén, z ktorých sa môžu stránky načítavať. Absencia takýchto kontrol je z pohľadu bezpečnosti vážnym nedostatkom najmä ak `WebView` slúži ako interaktívne rozhranie pre komunikáciu s používateľom. Aplikácia B `WebView` nevyužívala, čo predstavuje z hľadiska bezpečnosti pozitívum.

```

    }
    this.webView.addJavascriptInterface(new AnonymousClass8(str), "android");
}

public void showLoading() {
    this.webView.setVisibility(8);
    this.progressBarView.setVisibility(0);
}

public void clearHiddenElementErrors() {
    getUiHandler().postDelayed(new C(this, 2), 300L);
}

public void continueValidationElement(String str, String str2) {
    getUiHandler().postDelayed(new Runnable() {
        final /* synthetic */ String val$jsSubmitted;
        final /* synthetic */ String val$jsValidationScriptStr;

        public AnonymousClass4(String str3, String str22) {
            r2 = str3;
            r3 = str22;
        }

        @Override // java.lang.Runnable
        public void run() {
            PaymentForm.this.webView.loadUrl(r2);
        }
    }, 300L);
}

```

PaymentForm.4

Obrázok 14 Potencionálne zraniteľný WebView komponent

(zdroj: vlastný)

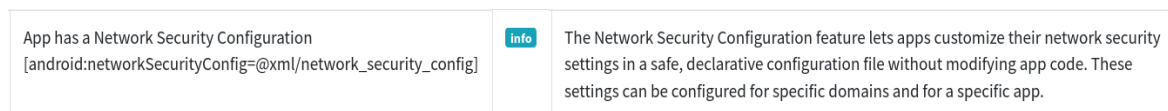
Všetky tri aplikácie trpeli nedostatočnou obfuskáciou kódu. Po spätnom preklade nebolo detegované použitie nástrojov ako ProGuard alebo R8 v plnej konfigurácii. V zdrojových súboroch zostali zachované zrozumiteľné a jednoznačné názvy tried, metód a premenných ako LoginActivity, VehicleService, SendCommand a podobne. Tento fakt výrazne uľahčuje reverzné inžinierstvo a umožňuje útočníkovi rýchle pochopenie vnútornej logiky aplikácie. Obfuskácia pritom nepredstavuje významnú prekážku pre vývoj, no jej absencia výrazne znižuje ochranu aplikácie pred zneužitím. Vhodnou stratégiou je implementácia viacerých ochranných vrstiev, konkrétne kombinácia nástrojov ProGuard, R8 a vlastných mechanizmov na ochranu pred reverzným inžinierstvom, akými sú napríklad techniky anti-debuggingu a kontroly integrity aplikácie.

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check
Compiler	r8 without marker (suspicious)

Obrázok 15 Neúplná obfuskácia detegovaná v aplikácii C

(zdroj: vlastný)

Aplikácia B ako jediná implementovala samostatný súbor `network_security_config.xml`, v ktorom boli špecifikované domény, na ktoré sa aplikácia môže pripájať. Takéto nastavenie zabráňuje spojeniam so škodlivými alebo neautorizovanými servermi aj v prípade, že by útočník získal schopnosť upraviť DNS alebo inak manipulovať sieť. Aplikácie A a C takúto konfiguráciu neobsahovali, čím sa zvyšuje riziko v prípade kompromitovanej siete.

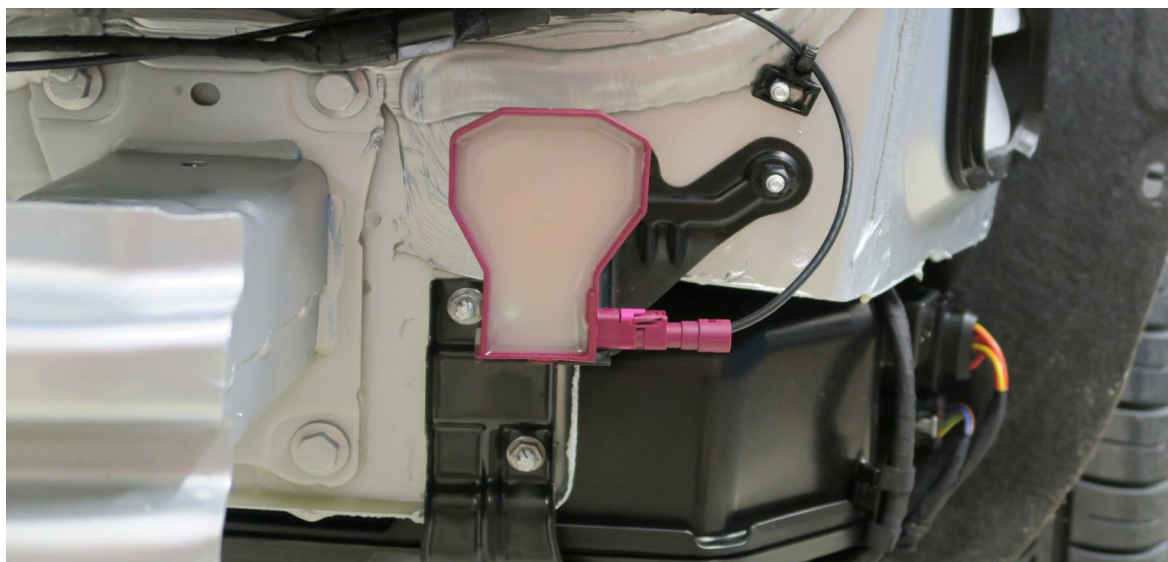


Obrázok 16 Konfigurácia zabezpečenej komunikácie v aplikácii B

(zdroj: vlastný)

8.3 Útok na LTE komunikáciu vozidla

Moderné vozidlá sú čoraz viac závislé na nepretržitej dátovej konektivite. Vďaka zabudovanej telematickej riadiacej jednotke nadväzujú spojenie s cloudovou infraštruktúrou výrobcu prostredníctvom mobilnej siete. Tento kanál umožňuje realizáciu viacerých funkcií: vzdialené ovládanie vozidla cez mobilnú aplikáciu, diagnostiku, OTA aktualizácie alebo lokalizáciu vozidla.



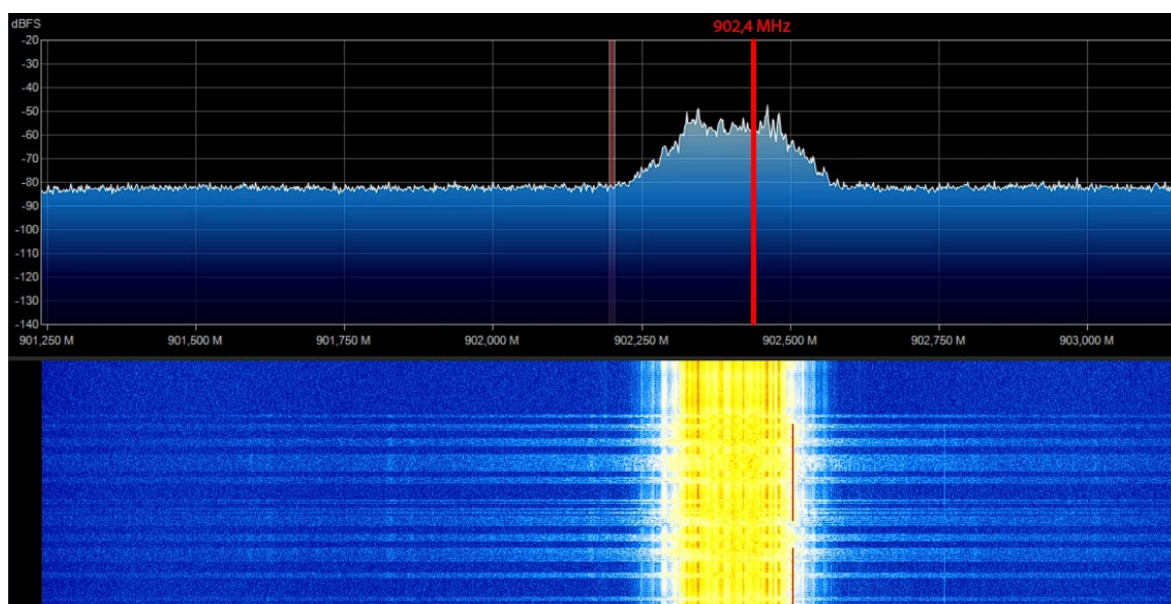
Obrázok 17 LTE anténa v oblasti pod zadným nárazníkom

(zdroj:[43])

V rámci testovania zraniteľnosti mobilných aplikácií bola preto analyzovaná aj samotná komunikácia medzi backend servermi výrobcu a vozidlom, ktorá prebieha práve cez dátové spojenie. Cieľom bolo overiť, do akej miery môže byť táto komunikácia zraniteľná voči

útokom z fyzickej vrstvy a to konkrétne narušením konektivity. Z pohľadu bezpečnosti možno bezdrôtovú komunikáciu označiť ako zraniteľné miesto celého systému. Fyzická vrstva (rádiofrekvenčné pásmo) sa napriek použitiu moderných šifrovacích protokolov a ochranných mechanizmov javí ako slabina, ktorú možno zneužiť útokmi typu Denial-of-Service (DoS).

V prvej fáze experimentu bola vykonaná pasívna analýza rádiovkej komunikácie medzi vozidlom a vzdialeným serverom výrobcu, pričom pozornosť bola zameraná na správanie telematickej riadiacej jednotky počas bežného používania mobilnej aplikácie. Cieľom bolo zistiť, v akých frekvenčných pásmach prebieha dátová komunikácia, a overiť, či je spojenie medzi vozidlom a backend infraštruktúrou aktívne nepretržité alebo sa aktivuje len na požiadanie. Na zachytávanie a analýzu signálu bolo použité zariadenie HackRF One PortaPack. Merania prebiehali pomocou softvérového nástroja SDRSharp v kombinácii s externou anténou naladenou na rozsah frekvencií zodpovedajúcich pásmu GSM/LTE. Experimentálny postup pozostával z opakovaného vykonávania akcií používateľom prostredníctvom mobilnej aplikácie výrobcu napr. odomknutie vozidla, načítanie polohy vozidla a súčasného monitorovania rádiového spektra. Počas analýzy boli na frekvencii 902,4 MHz detegované krátke a opakované pulzy modulovaného signálu, ktoré boli časovo zhodné s okamihmi, kedy bola zadaná požiadavka v aplikácii, čo indikovalo, že ide o dátové prenosy súvisiace s komunikáciou medzi vozidlom a backend serverom.



Obrázok 18 Komunikácia vozidla so serverom

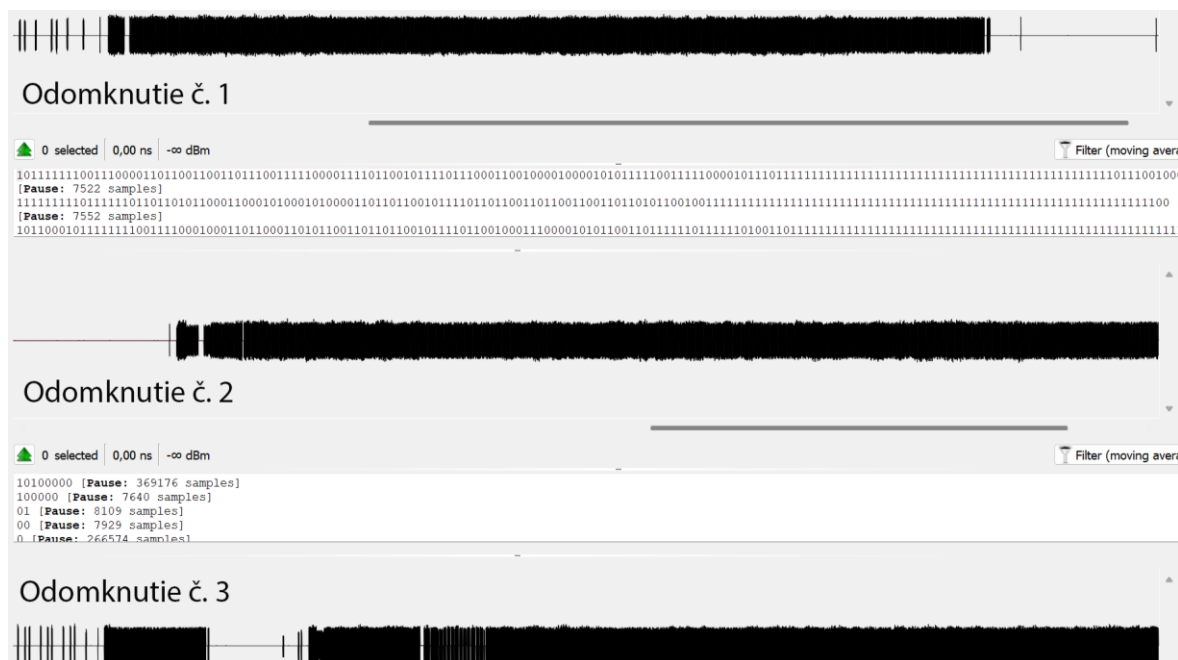
(zdroj: vlastný)

Na základe spektrálnej analýzy bolo zistené, že telematická jednotka nevyužíva výhradne LTE sieť, ako by sa dalo predpokladať na základe deklarovanej výbavy vozidla, ale v testovanej lokalite prešla na spojenie prostredníctvom technológie EDGE v pásme 900 MHz. Táto zmena poukazuje na adaptívne správanie modemu TCU jednotky, ktorý sa v prípade nedostupnosti LTE automaticky prepína na nižšiu úroveň konektivity. Zaznamenané správanie dokazuje, že spojenie medzi vozidlom a serverom sa neudržiava nepretržite, ale aktivuje sa len pri vyžiadanej akcii zo strany používateľa.

V druhej fáze bol uskutočnený test rušenia signálu. Išlo o simulovaný DoS útok zameraný na fyzické prerušenie spojenia. Vzhľadom na legislatívne obmedzenia bolo rušenie vykonané v kontrolovanom a opustenom prostredí s najmenšou intenzitou rušenia bez zásahu do funkcie iných okolitých zariadení. Rušenie signálu bolo realizované pomocou zariadenia HackRF One PortaPack s využitím jeho vstavaného režimu frekvenčného preladovania v rozsahu od 901 MHz až po 905 MHz. Rýchlosť prechodu rušiaceho signálu bola nastavená na 10 kHz. To znamená, že rušiaci signál sa posúval po frekvenčnej osi v krokoch 10 kHz, čím dochádzalo k postupnému pokrytiu celého spektra. Počas rušenia mobilná aplikácia po zadaní príkazu na akciu vozidla nedokázala nadviazať spojenie a vypísala chybovú hlášku o neúspešnom vykonaní akcie. Vozidlo nereagovalo na žiadne požiadavky. Po ukončení rušenia systém automaticky obnovil spojenie a požiadavky bolo možné opäť odosielať.

Na základe získaných poznatkov bola analyzovaná možnosť útoku s prehraním signálu. Táto komunikácia po vyslaní príkazu na odomknutie a zamknutie vozidla cez aplikáciu bola zachytená pomocou HackRF One PortaPack a softvéru Universal Radio Hacker. Zachytenie samotného signálu prebehlo úspešne. Počas zaznamenávania komunikácie bolo možné jednoznačne identifikovať aktivitu vo frekvenčnom spektre, ktorá korešpondovala s okamihmi odomykania vozidla cez mobilnú aplikáciu. Po zachytení signálu bol v URH aktivovaný modul Signal Analysis, ktorý identifikoval časti s viditeľne modulovaným priebehom. Tieto časti zodpovedali očakávaným okamihom, keď boli z mobilnej aplikácie odoslané príkazy. Pri následnom pokuse o detailné spracovanie a interpretáciu zachyteného signálu však nastali zásadné obmedzenia. Analýzou v nástroji URH sa ukázalo, že prijatý signál pozostáva z dátových sekvencií bez jednoznačnej čitateľnej štruktúry. Opakovanou snahou o dekodovanie a prehratie signálu sa potvrdilo, že samotná komunikácia je zabezpečená kryptografickými mechanizmami, ktoré znemožňujú jej priame spracovanie a interpretáciu prostredníctvom dostupných nástrojov. Na základe získaných výsledkov

možno konštatovať, že hoci zachytenie rádiového prenosu bolo úspešné, dekodovanie a analýza prenášaného obsahu nebola možná z dôvodu aplikovaného šifrovania na úrovni protokolu.



Obrázok 19 Komunikácia LTE medzi vozidlom a základňovou stanicou

(zdroj: vlastný)

8.4 Bezpečnostné dopady a riziká

Vykonaná bezpečnostná analýza mobilných aplikácií a komunikačnej infraštruktúry vozidla potvrdila, že napriek využívaniu moderných šifrovacích technológií existujú viaceré slabiny na strane klientskych aplikácií a fyzickej vrstvy prenosu dát. Dynamická analýza ukázala, že štandardné HTTPS zabezpečenie je nevyhnutné, ale bez správnej implementácie certificate pinningu môže byť komunikácia stále zraniteľná voči útokom typu Man-in-the-Middle. Statická analýza ďalej odhalila nedostatky v správe citlivých údajov, konfigurácii komponentov, ochrane pred reverzným inžinierstvom a sieťovej bezpečnosti. V prípade komunikácie medzi vozidlom a backend servermi sa preukázalo, že fyzická vrstva zostáva slabým článkom celého systému a je náchylná na DoS útoky či pasívne sledovanie aktivity. Aj bez dešifrovania vyšších vrstiev bolo možné identifikovať opakujúce sa dátové vzorce. Naznačuje to potrebu ďalšieho výskumu v oblasti ochrany RF komunikácie. Výsledky analýzy ukazujú, že na dosiahnutie vysokej úrovne bezpečnosti je potrebné kombinovať robustné softvérové opatrenia s ochranou proti fyzickým útokom na úrovni siete.

Tabuľka 6 Prehľad zistených slabín

Oblasť analýzy	Aplikácia A	Aplikácia B	Aplikácia C	Bezpečnostný dopad
Certificate Pinning	Áno	Nie	Áno	Bez pinningu umožňuje MITM útok
Tvrdokódované citlivé údaje	Áno	Áno	Áno	zneužitie API
Component Hijacking	Áno	Nie	Nie	Útoky tretích aplikácií na interné komponenty
WebView s JavaScriptom	Áno	Nie	Áno	Spustenie škodlivého JS vo WebView
Obfuskácia kódu	Nie	Nie	Nie	Jednoduché reverzné inžinierstvo
Sieťová konfigurácia	Nie	Áno	Nie	Možnosť pripojenia k neautorizovaným serverom

(zdroj: vlastný)

ZÁVER

Diplomová práca sa zameriava na analýzu bezpečnostných slabín moderných diaľkových systémov automobilov, najmä systémov využívajúcich technológiu plávajúceho kódu. Kombinuje teoretické spracovanie problematiky s praktickými experimentami a poskytuje komplexný pohľad na aktuálny stav zabezpečenia a jeho nedostatky.

V teoretickej časti je spracovaná evolúcia automobilových diaľkových systémov od mechanických riešení až po súčasné bezkľúčové technológie. Podrobne sú rozobraté technológie RKE, PKES, princípy plávajúceho kódu i známe typy útokov vrátane RollJam a reléových útokov. Zároveň je analyzovaná bezpečnosť komunikácie v prostredí prepojených vozidiel a riziká spojené s mobilnými aplikáciami na diaľkové ovládanie vozidiel.

Praktická časť sa sústreďuje na zostrojenie modelu bezdrôtového zamykania vozidla založeného na platforme Arduino s implementovaným plávajúcim kódom, jeho testovanie voči rôznym typom útokov a následnú analýzu výsledkov. Útok RollJam bol úspešne simulovaný na starších a menej zabezpečených systémoch, zatiaľ čo moderné systémy s viacúrovňovou autentifikáciou a pokročilými obrannými mechanizmami vykazovali výrazne vyššiu odolnosť. Výsledky experimentov ukazujú, že kľúčovými prvkami efektívneho zabezpečenia sú správna implementácia synchronizácie plávajúceho kódu, použitie robustných kryptografických algoritmov a aktívna detekcia anomálií v komunikácii. Významnú úlohu zohráva aj odolnosť mobilných aplikácií voči reverznému inžinierstvu a útokom typu Man-in-the-Middle; statická analýza odhalila viaceré bezpečnostné nedostatky v reálne používaných aplikáciách.

Práca poukazuje na nevyhnutnosť komplexného prístupu k zabezpečeniu vozidiel, ktorý zahŕňa nielen ochranu rádiovkej komunikácie, ale aj dôsledné zabezpečenie softvérových komponentov. Pre prax odporúča implementáciu viacfaktorovej autentifikácie, zavedenie časových obmedzení platnosti autentifikačných kódov, využitie asymetrickej kryptografie a zvyšovanie povedomia používateľov o fyzickej ochrane diaľkových ovládačov. Zistenia prispievajú k lepšiemu pochopeniu bezpečnostných rizík v oblasti automobilovej kybernetickej bezpečnosti a predstavujú základ pre ďalší výskum ochrany prepojených a autonómnych vozidiel.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] KNIGHT, Alissa. Hacking connected cars: tactics, techniques, and procedures. 1st ed. Indianapolis, Indiana: Wiley, [2020]. ISBN 978-1-119-49173-6.
- [2] Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems. Online. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf. [cit. 2025-02-23].
- [3] JOO, Kyungho; JO, Hyo Jin a CHOI, Wonsuk. Securing Passive Keyless Entry and Start System in Modern Vehicles Based on LF-Band Signal Analysis. Online. IEEE Internet of Things Journal. 2024, roč. 11, č. 24, s. 40176-40190. ISSN 2327-4662. Dostupné z: <https://doi.org/10.1109/JIOT.2024.3453920>. [cit. 2025-02-23].
- [4] SAUTER, Martin. From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband. 4th ed. Wiley, 2021. ISBN 978-1-119-71469-9.
- [5] SUN, Shao-hui; HU, Jin-ling; PENG, Ying; PAN, Xue-ming; ZHAO, Li et al. Support for vehicle-to-everything services based on LTE. Online. IEEE Wireless Communications. 2016, roč. 23, č. 3, s. 4-8. ISSN 1536-1284. Dostupné z: <https://doi.org/10.1109/MWC.2016.7498068>. [cit. 2025-02-23].
- [6] SUN, Li a DU, Qinghe. A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. Online. Entropy. 2018, roč. 20, č. 10. ISSN 1099-4300. Dostupné z: <https://doi.org/10.3390/e20100730>. [cit. 2025-02-23].
- [7] ROHOKALE, Vandana Milind; PRASAD, Neeli Rashmi a PRASAD, Ramjee. Cooperative Wireless Communications and Physical Layer Security: State-of-the-Art. Online. Journal of Cyber Security and Mobility. 2012. ISSN 2245-4578. Dostupné z: <https://doi.org/10.13052/jcsm2245-1439.1235>. [cit. 2025-02-23].
- [8] SINGH, Pritpal; SETHI, Tanjot; BALABANTARAY, Bunil Kumar a BISWAL, Bibhuti Bhushan. Advanced vehicle security system. Online. In: 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). IEEE, 2015, s. 1-6. ISBN 978-1-4799-6817-6.

- [9] PARK, Hoorin a HONG, Jeongkyu. BackProx: Secure Backscatter-Assisted Proximity Detection for Passive Keyless Entry and Start Systems. Online. *Sensors*. 2023, roč. 23, č. 4. ISSN 1424-8220. Dostupné z: <https://doi.org/10.3390/s23042330>. [cit. 23.02.2025].
- [10] D., Stabili; F., Valgimigl a T., Bocchi. Implementing and testing RollJam on Software-Defined Radios. Online. *CEUR Workshop Proceedings Vol-3731*. 2024. Dostupné z: <https://ceur-ws.org/Vol-3731/>. [cit. 2025-02-23].
- [11] KAMKAR, S. Drive it like you hacked it [online]. 2015 [cit. 23.02.2025]. Dostupné z: <https://samy.pl/defcon2015/>.
- [12] Automotive firmware extraction and analysis techniques. Online, Thesis, Ph.D. Birmingham: University of Birmingham, College of Engineering and Physical Sciences, 2021. Dostupné z: <https://etheses.bham.ac.uk/id/eprint/11516/>. [cit. 2025-02-23].
- [13] OnStar: 10 Years After: 10 Years After. Online. *Just Auto*. 2006. Dostupné z: <https://www.just-auto.com/features/onstar-10-years-after/>. [cit. 2025-02-23].
- [14] AHANGAR, M. Nadeem; AHMED, Qasim Z.; KHAN, Fahd A. a HAFEEZ, Maryam. A Survey of Autonomous Vehicles: Enabling Communication Technologies and Challenges. Online. *Sensors*. 2021, roč. 21, č. 3. ISSN 1424-8220. Dostupné z: <https://doi.org/10.3390/s21030706>. [cit. 2025-02-23].
- [15] JULIUSSEN, Egil. Perspectives on Automotive Operating Systems. Online. *EE Times*. 2022. Dostupné z: <https://www.eetimes.com/perspectives-on-automotive-operating-systems/>. [cit. 025-02-23].
- [16] MASOOD, Arooj; LAKEW, Demeke Shumeye a CHO, Sungrae. Security and Privacy Challenges in Connected Vehicular Cloud Computing. Online. *IEEE Communications Surveys & Tutorials*. 2020, roč. 22, č. 4, s. 2725-2764. ISSN 1553-877X. Dostupné z: <https://doi.org/10.1109/COMST.2020.3012961>. [cit. 2025-02-23].
- [17] NAEEM, Muhammad Ahtsam; JIA, Xiaolin; SALEEM, Muhammad Asim; AKBAR, Wasif; HUSSAIN, Afzaal et al. Vehicle to Everything (V2X) Communication Protocol by Using Vehicular AD-HOC Network. Online. In: 2020 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP). IEEE, 2020, s. 384-388. ISBN 978-1-6654-0503-4. Dostupné z: <https://doi.org/10.1109/ICCWAMTIP51612.2020.9317386>. [cit. 2025-02-23].

- [18] CHEN, Shanzhi; HU, Jinling; ZHAO, Li; ZHAO, Rui; FANG, Jiayi et al. Cellular Vehicle-to-Everything (C-V2X). Online. Wireless Networks. Singapore: Springer Nature Singapore, 2023. ISBN 978-981-19-5130-5. Dostupné z: <https://doi.org/10.1007/978-981-19-5130-5>. [cit. 2025-02-23].
- [19] GIULIANO, Romeo. From 5G-Advanced to 6G in 2030: New Services, 3GPP Advances, and Enabling Technologies. Online. IEEE Access. 2024, roč. 12, s. 63238-63270. ISSN 2169-3536. Dostupné z: <https://doi.org/10.1109/ACCESS.2024.3396361>. [cit. 2025-02-23].
- [20] SOLON, Olivia. Team of hackers take remote control of Tesla Model S from 12 miles away. Online. The Guardian. Dostupné z: <http://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes>. [cit. 2025-02-23].
- [21] THE WALL STREET JOURNAL. The Wall Street Journal; YouTube. Online. Dostupné z: <https://www.youtube.com/watch?v=CctuP9IIEOs>. [cit. 2025-02-23].
- [22] KIFOR, Claudiu Vasile a POPESCU, Aurelian. Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies. Online. Sensors. 2024, roč. 24, č. 18. ISSN 1424-8220. Dostupné z: <https://doi.org/10.3390/s24186139>. [cit. 2025-02-23].
- [23] ASHKENAZY, Shlomi. Understanding the UNECE WP.29 Automotive Cybersecurity Reg. Online. Cybellum. 2024. Dostupné z: <https://cybellum.com/blog/understanding-unece-wp29-automotive-cybersecurity-regulation/>. [cit. 2025-02-23].
- [24] ISO/SAE 21434 certifikace – Řízení kybernetické bezpečnosti silničních vozidel. Online. SGSCorp. 2022. Dostupné z: </cs-cz/services/iso-sae-21434-certifikace--systemu-kyberneticke-bezpecnosti-silnicnich-vozidel>. [cit. 2025-02-23].
- [25] SCHMITTNER, Christoph; MA, Zhendong; REYES, Carolina; DILLINGER, Oliver a PUSCHNER, Peter. Using SAE J3061 for Automotive Security Requirement Engineering. Online. In: SKAVHAUG, Amund; GUIOCHET, Jérémie; SCHOITSCH, Erwin a BITSCH, Friedemann (ed.). Computer Safety, Reliability, and Security. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016, s. 157-170. ISBN 978-3-319-45479-5. Dostupné z: https://doi.org/10.1007/978-3-319-45480-1_13. [cit. 2025-02-23].

- [26] SALEK, M Sabbir; KHAN, Sakib Mahmud; RAHMAN, Mizanur; DENG, Hsien-Wen; ISLAM, Mhafuzul et al. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. Online. IEEE Internet of Things Journal. 2022, roč. 9, č. 11, s. 8250-8268. ISSN 2327-4662. Dostupné z: <https://doi.org/10.1109/IIOT.2022.3152477>. [cit. 2025-02-23].
- [27] Škoda Connect. Online. Škoda Auto. 2025. Dostupné z: <https://www.skoda-auto.sk/technologie/skoda-connect>. [cit. 2025-02-23].
- [28] Bluelink aplikácia. Online. Hyundai. 2025. Dostupné z: <https://www.hyundai.com/sk/sk/sluzby/dalsie-sluzby/bluelink-konektivita/bluelink-aplikacia.html>. [cit. 2025-03-01].
- [29] BMW ConnectedDrive. Online. BMW AG. 2025. Dostupné z: <https://www.bmw.sk/sk/digital-services/bmw-connecteddrive.html>. [cit. 2025-02-23].
- [30] TAKAHASHI, Junko. An Overview of Cyber Security for Connected Vehicles. Online. Vydavateľ nenájdený. 2018. Dostupné z: https://www.jstage.jst.go.jp/article/transinf/E101.D/11/E101.D_2017ICI0001/_pdf. [cit. 2025-02-23].
- [31] HASHEM EIZA, Mahmoud a NI, Qiang. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. Online. IEEE Vehicular Technology Magazine. 2017, roč. 12, č. 2, s. 45-51. ISSN 1556-6072. Dostupné z: <https://doi.org/10.1109/MVT.2017.2669348>. [cit. 2025-02-23].
- [32] TOULAS, Bill. Hackers can steal your Tesla Model 3, Y using new Bluetooth attack. Online. BleepingComputer. 2022. Dostupné z: <https://www.bleepingcomputer.com/news/security/hackers-can-steal-your-tesla-model-3-y-using-new-bluetooth-attack/>. [cit. 2025-02-23].
- [33] FERNICK, Jennifer, QASIM KHAN, Sultan (ed.). Technical Advisory – BLE Proximity Authentication Vulnerable to Relay Attacks. Online. NCC GROUP. NCC Group. 2022. Dostupné z: <https://www.nccgroup.com/uk/research-blog/technical-advisory-ble-proximity-authentication-vulnerable-to-relay-attacks>. [cit. 2025-02-23].
- [34] HAJ BAKRY, Talal a MYSK, Tommy. Can a Tesla Stop Phishing and Social Engineering Attacks? Online. Mysk Blog – In-Depth Cybersecurity. 2024. Dostupné z: <https://mysk.blog/2024/03/10/tesla-phone-key/>. [cit. 2025-02-23].

- [35] VELU, Vijay Kumar. Mobile application penetration testing: explore real-world threat scenarios, attacks on mobile applications, and ways to counter them. Community experience distilled. Birmingham: Packt Publishing, 2016. ISBN 978-1-78588-337-8.
- [36] CURRY, Sam. Hacking Kia: Remotely Controlling Cars With Just a License Plate: Remotely Controlling Cars With Just a License Plate. Online. Samcurry.net. 2024. Dostupné z: <https://samcurry.net/hacking-kia>. [cit. 2025-02-23]
- [37] MONK, Simon. Programming Arduino: getting started with sketches. Third edition. New York: McGraw Hill, [2023]. ISBN 978-1-264-67698-9.
- [38] Tech specs of Flipper Zero. Online. Documentation. 2025. Dostupné z: <https://docs.flipper.net/development/hardware/tech-specs>. [cit. 2025-02-23].
- [39] HackRF One. Online. Great Scott Gadgets. 2021. Dostupné z: https://hackrf.readthedocs.io/en/latest/hackrf_one.html. [cit. 2025-02-23].
- [40] About RTL-SDR. Online. Rtl-sdr.com. 2024. Dostupné z: <https://www.rtl-sdr.com/about-rtl-sdr/>. [cit. 2025-02-23].
- [41] SHUR1K-N. Flipper-Zero-Sub-GHz-Jamming-Files. Online. GitHub. 2024. Dostupné z: <https://github.com/SHUR1K-N/Flipper-Zero-Sub-GHz-Jamming-Files>. [cit. 2025-02-23].
- [42] THE OPEN WORLDWIDE APPLICATION SECURITY PROJECT (OWASP). OWASP Mobile Top 10. Online. OWASP Foundation. 2024. Dostupné z: <https://owasp.org/www-project-mobile-top-10/>. [cit. 2025-02-23].
- [43] LTE anténa v oblasti pod zadným nárazníkom, ktorá slúži pre mobilné online služby. Online. In: Škoda Storyboard. 2022. Dostupné z: <https://www.skoda-storyboard.com/sk/skoda-svet-sk/inovacie-sk/tu-tvoje-auto-pocujes-ma/>. [cit. 2025-02-23].

ZOZNAM OBRÁZKOV

Obrázok 1 Priebeh komunikácie pomocou plávajúceho kódu.....	17
Obrázok 2 Reléový útok na systém PKES.....	20
Obrázok 3 V2X komunikácia	23
Obrázok 4 Aplikácia MyŠkoda.....	36
Obrázok 5 Zapojenie vysielacza Arduino.....	43
Obrázok 6 Zapojenie prijímača Arduino	44
Obrázok 7 Kompletizácia modelu.....	55
Obrázok 8 Dve konfigurácie zariadení Flipper Zero a Porta Pack	58
Obrázok 9 Príklad nastavení Flipper Zero a PortaPack	59
Obrázok 10 Diagram scenárov testovania	60
Obrázok 11 Overovanie certifikátu aplikácie	70
Obrázok 12 Detekcia tvrdokódovaných API kľúčov aplikácie B.....	71
Obrázok 13 Component hijacking v aplikácii A.....	72
Obrázok 14 Potencionálne zraniteľný WebView komponent.....	73
Obrázok 15 Neúplná obfuskácia detegovaná v aplikácii C	73
Obrázok 16 Konfigurácia zabezpečenej komunikácie v aplikácii B	74
Obrázok 17 LTE anténa v oblasti pod zadným nárazníkom.....	74
Obrázok 18 Komunikácia vozidla so serverom	75
Obrázok 19 Komunikácia LTE medzi vozidlom a základňovou stanicou.....	77

ZOZNAM TABULIEK

Tabuľka 1 Prehľad útokov na Arduino Uno	62
Tabuľka 2 Prehľad útokov na automatickú bránu	64
Tabuľka 3 Prehľad útokov na vozidlo z roku 2016	64
Tabuľka 4 Prehľad útokov na vozidlo z roku 2019	65
Tabuľka 5 Prehľad útokov na vozidlo z roku 2024	65
Tabuľka 6 Prehľad zistených slabín	78

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
ASK	Amplitude Shift Keying
CA	Certificate Authority
CAN	Controller Area Network
C-V2X	Cellular Vehicle-to-Everything
dBm	Decibel-milliwatt
DOS	Denial of Service
DSRC	Dedicated Short-Range Communications
ECU	Electronic Control Unit
EDGE	Enhanced Data Rates for GSM Evolution
FSK	Frequency Shift Keying
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HMAC	Hash-based Message Authentication Code
HTTP/S	Hypertext Transfer Protocol / Secure
IOT	Internet of Things
IPSec	Internet Protocol Security
kbps	Kilobits per second
LIDAR	Light Detection and Ranging
LTE	Long Term Evolution

m	Meter
MHz	Megahertz
MITM	Man-In-The-Middle
MobSF	Mobile Security Framework
MSPS	Mega Samples Per Second
NFC	Near Field Communication
OTA	Over-the-Air
PKES	Passive Keyless Entry System
RF	Radio Frequency
RFID	Radio-Frequency Identification
RKE	Remote Keyless Entry
RSA	Rivest-Shamir-Adleman
SDR	Software-Defined Radio
SSL	Secure Sockets Layer
TCU	Telematics Control Unit
TLS	Transport Layer Security
UHR	Universal Radio Hacker
V2C	Vehicle-to-Cloud
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
Wi-Fi	Wireless Fidelity
WP	Working Party