Slabiny v zabezpečení dálkových ovládačů automobilů

Samuel Gábor

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Samuel Gábor**
Osobní číslo:	**A20047**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Slabiny v zabezpečení dálkových ovladačů automobilů**
Téma práce anglicky:	**Security Vulnerabilities of Car Remote Controls**

Zásady pro vypracování

1. Vypracujte rešerši na téma současného stavu bezdrátových technologií v automobilech a softwarově definovaného rádia.
2. Navrhněte experiment zabezpečení automobilů využívající bezdrátový způsob komunikace.
3. Navrhněte sérii útoků s SDR, které aplikujete na experiment.
4. Proveďte analýzu navrženého experimentu a identifikujte slabiny.
5. Identifikujte typ vozidla podle vysílaného signálu.

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

Seznam doporučené literatury:

1. VODA, Zbyšek. Průvodce světem Arduina. Vydání druhé. Bučovice: Martin Stříž, 2017. ISBN 978-80-87106-93-8.
2. KENGO OKA, Dennis. Building Secure Cars. 1. UK: John Wiley & Sons, 2021. ISBN 9781119710745.
3. COLLINS, Travis F., Robin GETZ, Di PU a Alexander M. WYGLINSKI. Software-Defined Radio for Engineers. USA. Artech House Publishers, 2018. ISBN 9781630814571.
4. ALRABADY, A.I. a S.M. MAHMUD. Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. IEEE Transactions on Vehicular Technology [online]. 2005, 54(1), 41-50 [cit. 2022--11-28]. ISSN 0018-9545. Dostupné z: doi:10.1109/TVT.2004.838829.
5. GARCIA, Flavio D., David OSWALD, Timo KASPER a Pierre PAVLIDÈS. Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems. In: Proceedings of the 25th USENIX Security Symposium. Austin, TX: USENIX Association, 2016, s. 929-944. ISBN 978-1-931971-32-4.

Vedoucí bakalářské práce: **Ing. Stanislav Kovář, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **13. prosince 2022**
Termín odevzdání bakalářské práce: **5. června 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

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

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 13. prosince 2022

Samuel Gábor

Slabiny v zabezpečení dálkových ovládačů automobilů

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 19.5.2023 Samuel Gábor v.r.

ABSTRAKT

Bakalárska práca popisuje nedostatky zabezpečenia diaľkových ovládačov automobilov. V úvode sa práca venuje historickým aj aktuálnym trendom v elektronickom zabezpečení automobilov a tiež budúcim možnostiam v tejto oblasti. Práca odhaľuje slabiny diaľkových ovládačov v podobe jednoduchej replikácie signálu bežne dostupných bezdrôtových technológií. Tieto možnosti útokov a spôsoby ich realizácie sú detailne popísané v teoretickej časti práce. Praktická časť demonštruje spomínané typy útokov pomocou softvérového definovaného rádia na modeli zabezpečenia automobilu realizovaného na platforme Arduina v laboratórnych aj reálnych podmienkach. Záver práce analyzuje výsledky ziskané počas experimentov a prináša odporúčania ochrany pred potencionálnymi útokmi.

Kľúčové slová: slabiny, diaľkové ovládače, softvérové definované rádio, Arduino

ABSTRACT

The bachelor's thesis describes the shortcomings of the security of remote car controls. In the introduction, the work deals with historical and current trends in electronic car security and an outline of future directions in the field. The result reveals the weaknesses of remote controls in the form of simple signal replication of commonly available wireless technologies. These attack options and their implementation methods are described in detail in the theoretical part of the thesis. The practical part demonstrates the mentioned attacks using a software-defined radio on a car security model implemented on the Arduino platform in the laboratory and natural conditions. The conclusion of the work analyzes the results discovered during the experiments and provides recommendations for protection against potential attacks.

Keywords: weaknesses, remotes, software defined radio, Arduino

POĎAKOVANIE

Moje poďakovanie patrí školiteľovi bakalárskej práce Ing. Stanislavovi Kovářovi, PhD. za jeho odborné vedenie, metodickú pomoc a cenné rady, ktoré mi poskytol pri jej vypracovaní.

Prehlasujem, že odovzdaná verzia bakalárskej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

História zabezpečenia automobilov je úzko spätá s vývojom samotných automobilov. Vývoj bezpečnostných systémov sprevádza automobilizmus od jeho počiatkov - od času, keď boli automobily základnými strojmi bez rozsiahlych bezpečnostných prvkov, až po modernú éru sofistikovaných vozidiel. Cieľom bezpečnostných systémov je čeliť (zabrániť) rastúcim hrozbám krádeží a neoprávneným prístupom. S technologickým pokrokom však vznikajú nové výzvy a zraniteľnosti, ktoré si vyžadujú neustálu inováciu a zlepšovanie zabezpečenia automobilov. Snahy o riešenie problému krádeží automobilov sa objavujú už na začiatku 20. storočia. Prvým bezpečnostným zariadením, ktoré malo zabrániť neoprávnenej jazde, prípadne krádeži, bol zámok volantu. Ako sa autá stávali zložitejšími a cennejšími, ukázala sa potreba pokročilejších bezpečnostných opatrení. V 50. a 60. rokoch 20. storočia si získali popularitu autoalarmy ako účinný odstrašujúci prostriedok proti zlodejom. Tieto alarmy využívali zvukové sirény a viditeľné blikajúce svetlá, ktoré upozorňovali na potenciálnu manipuláciu s vozidlom a varovali majiteľa aj okoloidúcich. S ďalším technologickým pokrokom v 80. a 90. rokoch 20. storočia bezpečnostné systémy automobilov prešli výraznejšími zmenami. Zavedenie systémov diaľkového bezkľúčového vstupu spôsobilo revolúciu v zabezpečení automobilov. Táto bezdrôtová technológia umožnila vodičom odomykať svoje vozidlá na diaľku, čím sa zabezpečilo pohodlie a zvýšila bezpečnosť. Pomocou rádiofrekvenčných signálov diaľkové ovládanie komunikovalo s uzamykacím systémom vozidla a umožňovalo plynulé prepínanie medzi zamknutým a odomknutým stavom. V súčasnosti dosiahla technológia zabezpečenia automobilov vysokú úroveň dokonalosti. Moderné vozidlá sú vybavené celým radom pokročilých bezpečnostných prvkov vrátane najmodernejších poplašných systémov a imobilizérov, ktoré zabraňujú neoprávnenému zapaľovaniu bez správneho kľúča, i vrátane systémov sledovania polohy, ktoré pomáhajú lokalizovať ukradnuté vozidlá. Tieto pokroky nepochybne prispeli k zníženiu počtu krádeží áut a zvýšeniu celkovej bezpečnosti. Napriek tomuto pokroku zostávajú bezpečnostné systémy automobilov zraniteľné voči rôznym vonkajším vplyvom a útokom. Rušenie, či útoky s prehraním signálu predstavujú významné výzvy pre odolnosť a účinnosť súčasných bezpečnostných systémov. Je dôležité uvedomiť si, že útočníci už nepotrebujú fyzický prístup do vozidla, ale môžu zneužiť zraniteľnosti systému zabezpečenia odkiaľkoľvek v dosahu signálu. Cieľom tejto bakalárskej práce je preskúmať a riešiť vznikajúce hrozby a zraniteľnosti, ktorým čelia moderné bezpečnostné systémy automobilov.

I. TEORETICKÁ ČASŤ

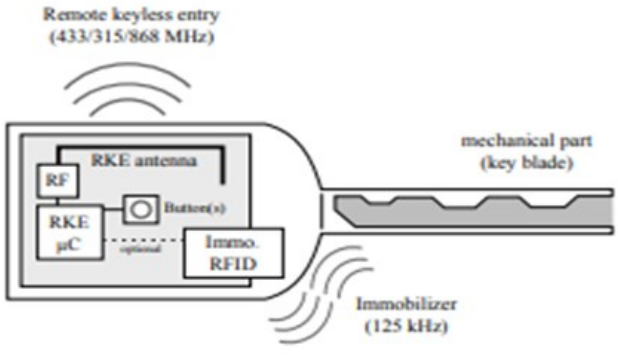
1 AUTOMOBILOVÉ DIAĽKOVÉ OVLÁDAČE

Už niekoľko desaťročí sa využívajú mechanické kľúče na zabezpečenie vozidiel. Mechanické kľúče spočiatku slúžili na jednoduché operácie ako uzamknutie, odomknutie vozidla a naštartovanie motora. Nevýhodou týchto mechanických systémov bola ich pomerne jednoduchá prelomiteľnosť. U skúsenejšieho zlodeja nepredstavovalo problém vytvoriť mechanickú kópiu kľúča, prípadne využiť rôzne zámočnícke techniky na prelomenie zabezpečenia. S postupným vývojom v technologickej oblasti a rastúcimi nárokmi zákazníkov na moderné systémy vo vozidlách prišli sa zvyšovali nároky na bezpečnosť automobilov.

1.1 Imobilizačné čipy

S vývojom technológii vo všetkých smeroch a odvetviach prišiel prelom aj v zabezpečení vozidiel, ktorý využívajú automobily do dnešného dňa. K mechanickým zábranným systémom pribudli tiež elektronické. Vývoj imobilizačných transpondérových čipov a ich následná inštalácia do automobilových kľúčov prispela k zníženiu počtu odcudzených vozidiel. Imobilizér je pasívne zariadenie, ktorého úlohou je zamedziť naštartovaniu motora.

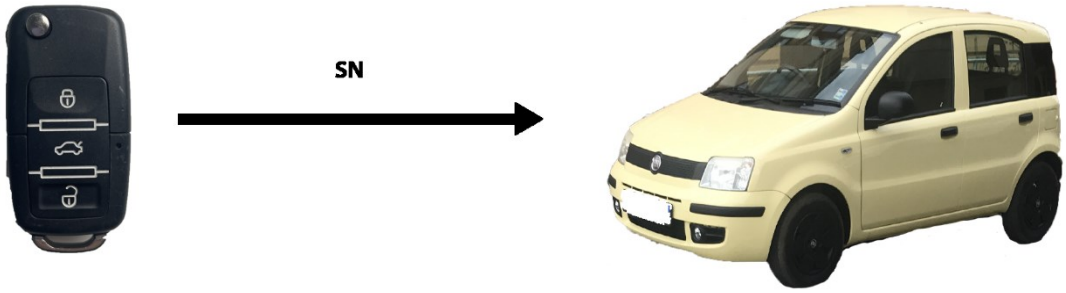
Tieto zariadenia pracujú na princípe rádiofrekvenčnej identifikácii (RFID) s nosnou frekvenciou 125 kHz. K aktivácii imobilizačných jednotiek dochádza do 30 sekúnd po vypnutí zapaľovania motora. K deaktivácii dochádza automaticky pri vložení kľúča od vozidla do spínacej skrinky. V prípadoch, keď vozidlo disponuje bezkľúčovým štartovaním, dochádza k deaktivácií čipu po overení, či sa naprogramovaný kľúč nachádza vo vnútrom priestore vozidla. [1]



Obrázok 1 Nákres kľúču od vozidla [1]

Imobilizačné čipy sa nachádzajú separátne umiestnené v kľúči od vozidla. V zámku zapaľovania sa nachádza anténna cievka, ktorá prijíma signál vysielaný imobilzačným čipom. Pri použití tohto nastavenia imobilizéra je dosah niekoľko desiatok centimetrov.

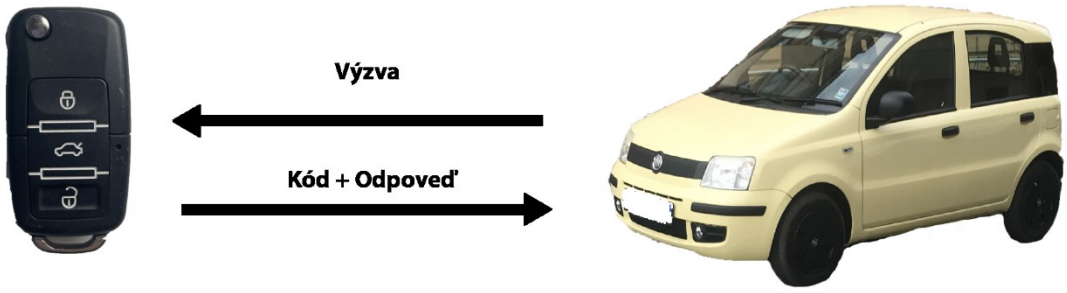
Kryptografia imobilizérov bola dlhé roky na jednoduchej úrovni [1]. Automobiloví výrobcovia využívali jednoduchý systém, keď pri vložení kľúča do zámkového cylindra došlo čipom k vyslaniu kódu, resp. sériového čísla, ktoré bolo unikátne pre každé vozidlo. Tento kód bol následne zachytený anténou a overený riadiacou jednotkou. V prípade, že sa kód zhodoval s požadovaným kódom, bolo umožnené naštartovanie. [2]



Obrázok 2 Jednoduchá komunikácia imobilizéra [zdroj: vlastný]

Nevýhodou tohto systému bolo, že vysielaný kód bol nemenný. Netrvalo dlho a táto slabina bola odhalená útočníkmi, ktorí vedeli zachytiť tento kód a následne ho pomocou iného zariadenia alebo nového naprogramovaného kľúča vygenerovať a odcudziť vozidlo. Dôvodom jednoduchosti týchto systémov mohla byť obmedzená energia RFID technológie, nedostatočný vývoj a taktiež finančné náklady.

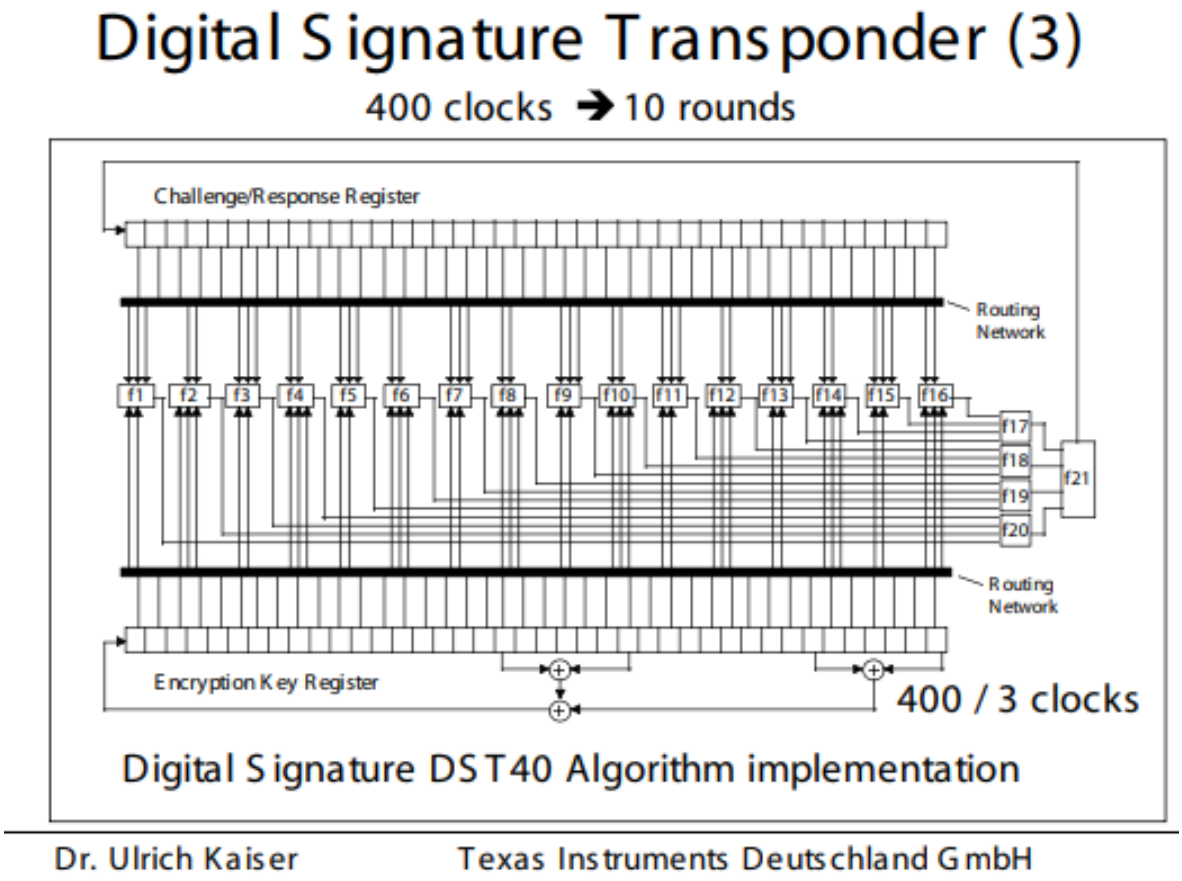
Nasledujúca generácia imobilizérov využíva overovací protokol výzva-odpoveď (Challenge-response). Tento systém využíva zdieľanie šifrovania kryptografického kľúča medzi vozidlom a imobilzačným čipom. Po vložení kľúča do zapaľovania auto vygeneruje náhodné číslo výzvy (challenge). Táto výzva je následne poslaná do kľúča od vozidla, ktorý na základe kryptografického kľúča vygeneruje odpoveď (response). [2]



Obrázok 3 Challenge-response imobilizér [zdroj: vlastný]

Jedným z prvých populárnych imoblizerových transpondérov používaný automobilovými výrobcami po celom svete bol čip nazývaný Digital Siganautre Transponder 40 (DST40) od firmy Texas Instruments. Tento čip využíva 40 bitovú výzvu, ktorá je vyslaná čítacím

zariadením (autom), následne zašifrovaná a skrátená na 24 bitovú odpoveď. Odpoveď je odoslaná do čítacieho zariadenia, kde je overená. [1]



Obrázok 4 Algoritmus šifrovania DST40 [3]

V roku 2005 sa podarilo prelomiť toto zariadenie na konferencií Usenix Security. Problém tohto zariadenia bol v dĺžke bitového kľúču. Nedostatočná 40 bitová dĺžka kľúču mohla byť na základe získania výzvy prelomená reverzným inžinierstvom pomocou softvéru za pár hodín. Útok na toto zariadenie nepatrí k tým najjednoduchším, nakoľko je potrebné byť v blízkosti vozidla na zachytenie výzvy a následne realizovanie procesu nájdenia odpovede zhodnej s výzvou. [1]

V roku 2012 bezpečnostní výskumníci z Usenix Security publikovali dokument poukazujúci na nedostatočnosť nového čipu Hitag2 od spoločnosti NXP Semiconductors, ktorý bol využívaný koncernovými automobilovými výrobcami po celom svete. Tento imobilizačný transpondér využíva 48 bitový kľuč na overenie. V tomto dokumente demonštrovali útok pomocou zariadenia Proxmark III, ktoré je výkonným nástrojom využívaným v oblasti analýzy a testovania bezpečnosti RFID. Proxmark III je populárne a rozsiahlo využívané prenosné zariadenie určené na skúmanie, vyhodnocovanie a využívanie zraniteľností v rôznych

systémoch RFID. Ponúka rozsiahle možnosti pre nízkofrekvenčné aj vysokofrekvenčné technológie RFID a umožňuje emulovať, klonovať a manipulovať s kartami a čítačkami RFID. V publikovanom dokumente výskumníci využili zariadenie Proxmark III na vykonanie útoku, čím demonštrovali jeho účinnosť pri prelomení bezpečnosti cieľového systému. Skutočnosť, že zabezpečenie bolo narušené za menej ako 6 minút, ukazuje silu zariadenia a zdôrazňuje zlepšenia protiopatrení a silnejšej ochrany systémov. [4]

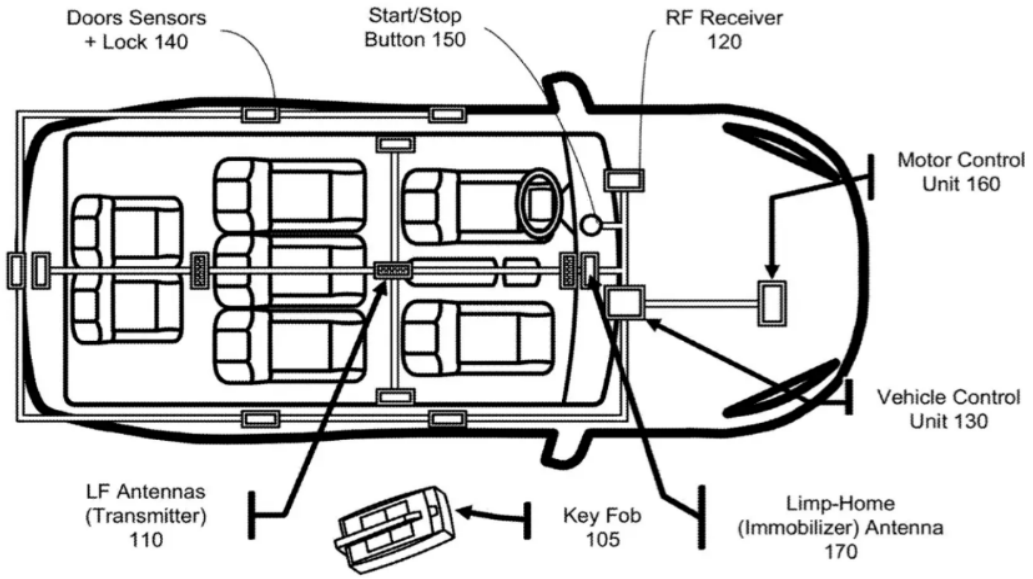
Obrázok 5 Útok pomocou Proxmark III [4]

V roku 2015 bol publikovaný záznam z konferencie [1], v ktorom bolo popísané ďalšie prelomenie zabezpečenia v oblasti imobilizérov. Konkrétne ide o transpondér Megamos Crypto, ktorý prelomili inžinieri Usenix Security a je do dnešného dňa využívaný mnohými automobilovými výrobcami. Slabina tohto čipu využívajúceho 96 bitový kľúč bola v objavení bitov, ktoré boli nastavené na hodnotu 0. Chyba sa objavila v niekoľkých generáciách čipu a umožnila prelomenie do niekoľkých sekúnd.

Postupom rokov síce dochádzalo k vývoju imobilizérov, ale v dnešnej dobe je možné tvrdiť, že klasické imobilizačné čipy nezabezpečujú dostatočnú ochranu, môžu byť jednoducho prelomené a naklonované. Napriek tomu všetky nové vozidlá vyrobené v Európskej únii musia byť od roku 1995 vybavené imobilizérom. [5]

1.2 Passive Keyless Entry and Start

Systémy Passive Keyless Entry and Start, taktiež nazývané PEKS, v preklade pasívny bezkľúčový prístup a štart, pracujú a komunikujú s vozidlom bez interakcie používateľa. Tieto systémy komunikujú s vozidlom na veľmi krátku vzdialenosť, približne jeden meter. Keď sa používateľ priblíži k vozidlu, kľúč vyšle informáciu riadiacej jednotke zabezpečenia vozidla. Ak je táto odpoveď správna, riadiaca jednotka deaktivuje zabezpečovacie systémy a odomkne dvere. Pre možnosť naštartovania motora riadiaca jednotka overuje ďalšiu podmienku – to, či sa kľúč od vozidla nachádza vo vnútornom priestore vozidla na sedenie. [6], [7]



Obrázok 6 Zapojenie PEKS systému vo vozidle [8]

Systémy PEKS sa stali častým cieľom zneužívania pomocou útoku typu man-in-the-middle. Všeobecne je tento typ útoku na vozidlá známejší pod názvom relay attack. Útočníci využívajú najväčšiu slabinu PEKS systémov - to, že tieto systémy nepotrebujú interakciu používateľa na komunikáciu s vozidlom. [1]

1.3 Remote Keyless Entry

Systémy Remote Keyless Entry, v preklade diaľkový bezkľúčový vstup, sú súčasťou výbavy vozidiel už niekoľko rokov. Najviac rozšírené diaľkovo ovládané systémy, na rozdiel od PEKS systémov, vyžadujú interakciu používateľa. V súčasnej dobe sa kombinujú so všetkými systémami, čo znamená, že vozidlo disponuje PEKS technológiou a taktiež má aj možnosť odomknúť vozidlo z väčšej vzdialenosti pomocou stlačenia tlačidla. Samozrejmosťou

je zabudovanie imobilizačného čipu a mechanického kľúča v prípade poruchy a núdzového štartovania.

Po interakcii používateľa diaľkové systémy vyšlú pomocou rádiovej frekvencie signál v určenom frekvenčnom pásme. Frekvencia sa líši na základe lokality, na ktorú je vozidlo dodávané. V Severnej Amerike je táto frekvencia 315 MHz, v Európe je táto frekvencia 433 MHz, prípadne 868 MHz. [1]

1.3.1 Pevný kód

Prvé systémy pre diaľkové odomykanie vozidiel nedisponovali žiadnymi spôsobmi kryptografickej ochrany. Automobily boli odmoknuté na základne prijatia signálnu vyslaného kľúčom od vozidla. Tento kód vyslaný kľúčom sa nemenil a preto dostal pomenovanie statický kód. Na prelomenie tohto systému sa dá použiť jednoduchý typ útoku nazývaný útok prehraním. [9]

1.3.2 Plávajúci kód

Nová generácia diaľkových systémov priniesla zmenu v zabezpečení vozidiel. Automobiloví výrobcovia implementovali systémy s využitím kryptografie - takzvané systémy s plávajúcim kódom. Princíp tohto nového zabezpečenia je v použití počítadla a v uložení istej hodnoty v riadiacej jednotke vozidla a kľúča. Pri odomknutí vozidla stlačením tlačidla dôjde k vyslaniu signálu na odomknutie, ktorý je rozšifrovaný riadiacou jednotkou. Ak je tento proces úspešný, riadiaca jednotka porovnáva hodnotu počítadla vyslanej kľúčom s hodnotou počítadla očakávanej vozidlom. Ak sa zhoduje aj táto hodnota, vozidlo je odomknuté a je inkrementovaná hodnota, ktorá bude očakávaná vozidlom pri ďalšej interakcií. Tento nový systém predstavoval zvýšené zabezpečenie proti útokom s prehraním. [9]

Jednou z najvyužívanejších kryptografických schém je KEELOQ, ale k prelomeniu toho systému došlo v roku 2008. V neskorších rokoch dochádzalo ešte k publikovaniu pokusov o prelomenie automobilových zabezpečení s týmto systémom. K širšiemu prieskumu v oblasti kryptografickej bezpečnosti RKE systémov nedošlo a materiály k tejto oblasti sú veľmi obmedzené. [1]

2 SOFTVÉROVO DEFINOVANÉ RÁDIO

S vývojom technológií vo všetkých oblastiach informačných technológií vyvstáva otázka, či existuje možnosť nahradenia špecializovaných hardvérových zariadení softvérovými. Využívanie softvérových riešení prináša lepšiu flexibilitu a ľahšie možnosti inovácie, nakoľko softvérová aktualizácia je prakticky a aj ekonomicky výhodnejšia ako výmena hardvérových zariadení. Oblasť, kde sa tento prístup osvedčil ako výhodný, je rádiová komunikácia. Nahradenie hardvéru na spracovanie signálu používaného v rádio komunikačných systémoch softvérovými komponentami, nazývaným Softvérovo Definované Rádio (SDR), sa osvedčilo ako flexibilnejšie a univerzálnejšie než klasické rádiové systémy.

Softvérovo definované rádio je typ rádiového komunikačného systému, kde komponenty, ktoré boli tradične implementované v hardvéri, sú namiesto toho implementované v softvéri. Odborná definícia softvérovo definovaného rádia je: „Rádio, v ktorom sú niektoré alebo všetky fyzické vrstvy funkcií definované softvérovo.“ [10] To umožňuje oveľa väčšiu flexibilitu pri navrhovaní rádiového systému, pretože správanie systému možno ľahko upraviť zmenou softvéru. V systéme SDR je rádiový signál najprv prijatý anténou, následne prechádza cez analógovo-digitálny prevodník, ktorý konvertuje analógový rádiový signál na digitálnu reprezentáciu. Tento digitálny signál je potom spracovaný digitálnym signálovým procesorom (DSP), ktorý vykonáva operácie s digitálnymi dátami na extrakciu požadovanej informácie z rádiového signálu. DSP je kľúčovým komponentom v systéme SDR, pretože je zodpovedný za implementáciu rôznych algoritmov a techník používaných na spracovanie digitálneho rádiového signálu. Tieto algoritmy je možné ľahko upraviť alebo aktualizovať zmenou softvéru, čo umožňuje jednoduchú zmenu správania rádia bez potreby výmeny akéhokoľvek hardvéru. Jednou z hlavných výhod SDR je, že umožňuje vytvárať rádiá, ktoré môžu pracovať na viacerých frekvenciách a moduláciách, keďže spracovanie rádiového signálu sa vykonáva softvérovo. To umožňuje vytvoriť jediné rádio, ktoré možno použiť pre širokú škálu rôznych komunikačných štandardov a protokolov. Celkovo technológia SDR umožňuje vytvárať vysoko flexibilné a adaptabilné rádiové systémy, ktoré možno ľahko upravovať a aktualizovať tak, aby vyhovovali meniacim sa potrebám moderných komunikačných systémov. [10]

2.1 Princíp činnosti SDR

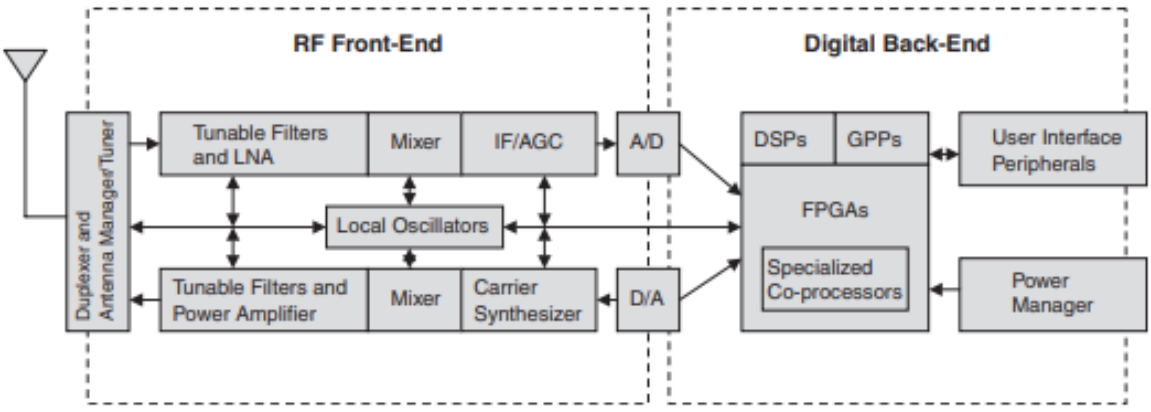
Systém SDR je komplexné zariadenie, ktorého účelom je umožniť neprerušované vysielanie a príjem signálu, pričom vykonáva niekoľko komplikovaných úloh súčasne.

Vo všeobecnosti sa zdigitalizovaný spôsob komunikácie skladá z viacerých vzájomne závislých operácii a krokov zodpovedných za prijímanie určitého typu informácie, pričom na prenášanom type informácie nezáleží. Pri prenose informácie, ktorá je pôvodne analógového typu, napríklad zvuk, musí byť táto informácia digitalizovaná pomocou viacerých krokov. Prvý z nich sa nazýva kvantovanie a slúži na získanie binárnej reprezentácie tejto analógovej informácie. Po vytvorení binárnej formy informácie vysielač spracuje túto informáciu a konvertuje ju na elektromagnetickú vlnu, ktorá je jednoznačne definovaná fyzikálnymi charakteristikami akými sú amplitúda signálu, nosná frekvencia a fáza. Po prijatí tejto vysielanej informácie je úlohou prijímača, aby správne identifikoval fyzikálne charakteristiky prijatého signálu a konvertoval tento signál naspäť do analógovej podoby. [11]

Najjednoduchšia podobizeň SDR by pozostávala iba z antény, dolnej priepuste (po anglicky Low Pass Filter), analógovo - digitálneho prevodníku (A/D prevodník), v prípade vysielača digitálneho - analógového prevodníku (D/A prevodník) a spracovávaným zariadením - napríklad počítačom. Takto konštruované zariadenie by vyžadovalo veľmi drahé komponenty, ktoré nie sú bežne dostupné a nepredstavovali by lepšiu alternatívu k hardvérových špecializovaným zariadeniam. Súčasné bežne dostupné SDR zariadenia sa skladajú väčšieho počtu komponentov, čo zaručuje ich väčšiu univerzálnosť a hlavne nižšiu cenu. [12]

2.2 Komponenty SDR

Komponenty SDR môžeme rozdeliť na dve kategórie, menovite RF Fornt-End a Digital Back-End.



Obrázok 7 Komponenty SDR [10]

2.2.1 RF Front-End

Prvá komunikačná časť SDR sa nazýva Radio Frequency Front End, v preklade predná časť rádiovej frekvencie a predstavuje všeobecný pojem pre obvod medzi vstupom antény prijímača, prípadne vysielača až po analógovo - digitálny prevodník. Táto časť sa skladá z nasledujúcich komponentov: z antény, zosilňovača, filtrov, lokálneho oscilátora, zmiešavača a A/D prevodníka. Vo vysielacej časti SDR sa nachádzajú rovnaké komponenty, ktoré sú usporiadané v opačnom poradí a na miesto A/D prevodníka je použitý D/A prevodník. Úlohou týchto komponentov je zachytenie požadovaného signálu, alebo jeho prenos bez frekvenčného šumu a iných rušivých okolnosti, ktoré by mohli interferovať s ostatnými signálmi v okolí. [12]

2.2.2 A/D prevodník

Analógovo - digitálny prevodník je zariadenie, ktoré konvertuje analógový signál, ako je napríklad zvuková vlna, na digitálny signál. Tento proces je známy ako analógovo - digitálna konverzia. Analógový signál je spojitá fyzikálna veličina, ktorá môže nadobudnúť akúkoľvek hodnotu v určitom rozsahu. Napríklad hlasitosť zvukovej vlny sa môže plynule meniť od veľmi tichej po veľmi hlasnú. Naproti tomu digitálny signál je sekvencia diskrétnych čísel, ktoré môžu nadobudnúť iba konečný súbor hodnôt. [13]

2.2.2.1 Vzorkovanie

Keď sa analógový signál konvertuje na digitálny signál, najprv sa v pravidelných intervaloch vzorkuje spojitá fyzikálna veličina. Vzorkovacia frekvencia je počet vzoriek za sekundu, ktoré A/D prevodník odoberie z analógového signálu. Čím vyššia je vzorkovacia frekvencia, tým detailnejšia a presnejšia bude digitálna reprezentácia analógového signálu. Existuje však kompromis medzi vzorkovacou frekvenciou a rozlíšením A/D prevodníka, čo je počet bitov použitých na reprezentáciu každej vzorky. Zvýšenie vzorkovacej frekvencie zvyčajne vyžaduje zvýšenie rozlíšenia, aby sa zachovala rovnaká úroveň presnosti. Pri výbere vhodnej vzorkovacej frekvencie pre A/D prevodník je potrebné zvážiť niekoľko faktorov. Prvým je Nyquistova - Shannonová teoréma, čo je minimálna vzorkovacia frekvencia, ktorá je potrebná na presné zachytenie všetkých informácií v analógovom signáli. Nyquistova - Shannonová frekvenica sa rovná dvojnásobku najvyššej frekvenčnej zložky v analógovom signáli. Napríklad, ak má analógový signál maximálnu frekvenciu 20 kHz, Nyquistova - Shannonová frekvencia by bola 40 kHz. [13], [14]

Ďalším faktorom, ktorý je potrebné zvážiť, je množstvo aliasingu, ktorý sa môže vyskytnúť. Aliasing je skreslenie, ku ktorému dochádza, keď je vzorkovacia frekvencia príliš nízka a to spôsobuje, že vysokofrekvenčné zložky v analógovom signáli sa javia ako zložky s nižšou frekvenciou v digitálnom signáli. Aby sa predišlo aliasingu, vzorkovacia frekvencia by mala byť aspoň dvojnásobkom Nyquistovej frekvencie. [14]

2.2.2.2 Kvantovanie

Ďalším krokom pri konvertovaní signálu je kvantovanie, kde dochádza k zaokrúhľovaniu na najbližšiu digitálnu hodnotu. Výsledná sekvencia kvantovaných vzoriek je digitálny signál. Presnosť kvantizačného procesu je určená rozlíšením A/D prevodníka, čo je počet bitov použitých na reprezentáciu každej vzorky. Čím vyššie je rozlíšenie, tým viac digitálnych hodnôt je dostupných na reprezentáciu analógového signálu a tým presnejšie budú kvantované vzorky reprezentovať pôvodný analógový signál. [13]

Napríklad, ak je rozlíšenie A/D prevodníka 8 bitov, existuje $2^8 = 256$ možných digitálnych hodnôt, ktoré možno použiť na reprezentáciu každej vzorky. To znamená, že kvantizačná chyba alebo rozdiel medzi pôvodnou analógovou hodnotou a kvantovanou digitálnou hodnotou bude menšia ako 1/256 celého rozsahu analógového signálu. Naopak, ak je rozlíšenie 16 bitov, existuje $2^{16} = 65536$ možných digitálnych hodnôt, takže kvantizačná chyba bude menšia ako 1/65536 celého rozsahu analógového signálu. Vo všeobecnosti je kvantizačná chyba rovnomerne rozložená v celom rozsahu analógového signálu. To znamená, že chyba bude menšia pre hodnoty, ktoré sú bližšie k stredu rozsahu, a väčšia pre hodnoty, ktoré sú bližšie k extrémom. Rozdelenie kvantizačnej chyby je známe ako kvantizačný šum. [13], [14]

Proces kvantovania je dôležitým krokom v analógovo - digitálnej konverzii, pretože umožňuje A/D prevodníku reprezentovať spojitý analógový signál ako diskrétny digitálny signál. Presnosť kvantizačného procesu závisí od rozlíšenia A/D prevodníka a výsledný kvantizačný šum môže ovplyvniť kvalitu konvertovaného digitálneho signálu. Na záver sú tieto hodnoty pretransformované do digitálneho binárneho kódu.

2.2.3 Digital Back-End

Druhá časť softvérovo definovaného rádia sa nazýva Digital Back-End a spracováva digitálne procesy, ktoré sú potrebné pre správne fungovanie. V tejto časti sa spracúva prijatý signál alebo sa syntetizuje prenášaný signál, prípadne oboje pre duplexné rádio. Táto časť

ovláda prvú komunikačnú časť SDR. [11] Po posunutí nosnej frekvencie požadovaného signálu na špecifickú frekvenciu, prechádza tento signál digitálnym filtrom, ktorý poskytuje vysokú úroveň potlačenia a odfiltrovania rušivých signálov, ktoré sa vyskytujú pri príjme. Ďalej tu dochádza k porovnávaniu prijatých symbolov s možnými prijatými symbolmi a dochádza k vytvoreniu záveru, ktoré symboly boli prenesené. V tomto procese sa vyhodnocuje, ktoré symboly mohli byť prijaté chybne z dôvodu slabého signálu alebo prípadného rušenia. [10] Pri vysielaní informácie je tento proces v opačnom poradí ako pri príjme. Digitálna časť pracuje s informáciou, ktorá má byť prenesená a zoskupí ju do paketov, pridáva prípadnú redundanciu bitov na zabezpečenie opravu chýb pri príjme a vyberá vhodný tvar vlny signálu. [11]

2.3 Modulácia signálu

Neoddeliteľnou súčasťou rádiovej komunikácie je modulácia signálu, čo je proces, pri ktorom dochádza k zmene charakteru signálu. Modulácia signálu sa rozdeľuje na analógovú a digitálnu.

2.3.1 Analógová modulácia

Pri analógovej modulácii sa modulácia aplikuje nepretržite v reakcii na analógový informačný signál. Analógovú moduláciu môžeme rozdeliť podľa toho, ktorý parameter sa moduluje. [15]

2.3.1.1 Amplitúdová modulácia

Amplitúdová modulácia, skrátene AM, využíva zmenu amplitúdy signálu. Pri prenášaní informácie dochádza k zmene intenzity signálu, ktorý je následne prijímaný prijímačom. [15]

2.3.1.2 Frekvenčná modulácia

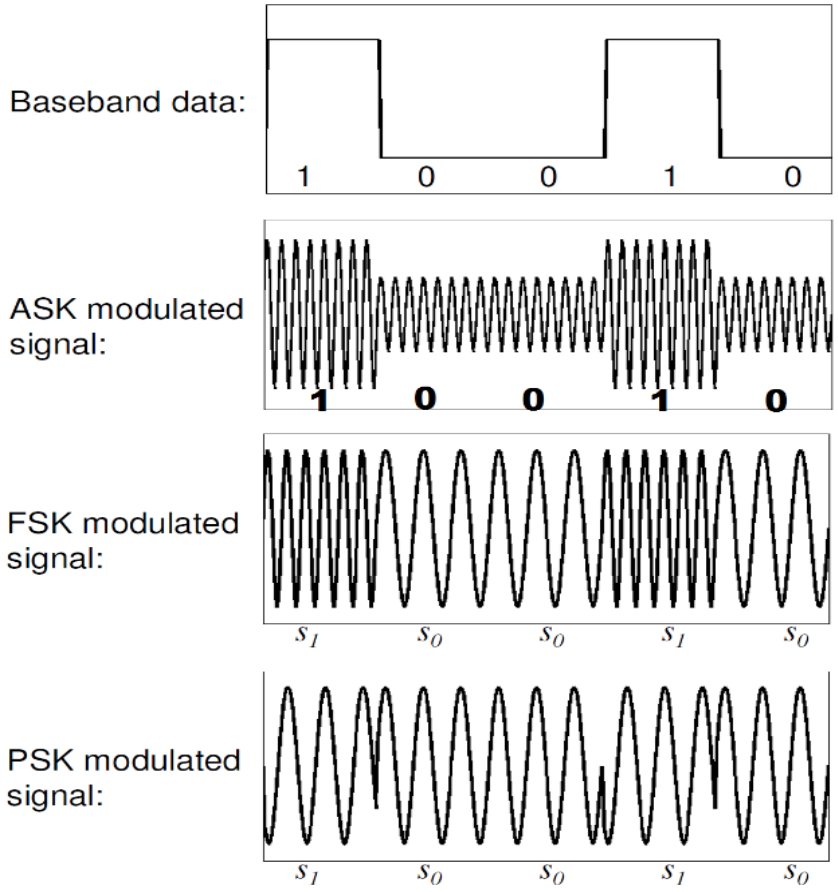
Pri frekvenčnej modulácii, skrátené FM, dochádza k zmene frekvencie nosnej vlny v súlade s okamžitou amplitúdou modulačného signálu, pričom fáza a amplitúda ostávajú konštantné. [15]

2.3.1.3 Fázová modulácia

Fázová modulácia, skrátené PM, vychádza z anglického Phase Modulation, využíva zmenu fázy tvaru nosnej vlny, aby odrážala zmeny vo frekvencií údajov. Vo fázovej modulácii sa nemení frekvencia, no fáza sa vzhľadom na základnú nosnú frekvenciu mení. [15]

2.3.2 Digitálna modulácia

Digitálna modulácia pracuje s prenášanými signálmi, ktoré majú len diskrétne hodnoty a parametre nosného signálu sa menia pri modulácii skokovite. Táto skokovitá zmena parametrov sa nazýva kľúčovanie. [15]



Obrázok 8 Digitálna modulácia signálu [16]

2.3.2.1 Amplitúdové kľúčovanie

V amplitúdovom kľúčovaní, vychádza z anglického Amplitude - Shift Keying (ASK), môže amplitúda prenášaného signálnu naberať jednu z dvoch diskrétnych hodnôt a to 0 a 1. Výhodou tejto modulácie je jej jednoduchosť a nenáročnosť, avšak tento typ modulácie býva náchylný na rušenie okolitými signálmi. [15]

2.3.2.2 Frekvenčné kľúčovanie

Vo frekvenčnom kľúčovaní, vychádza z anglického Frequency - Shift Keying (FSK), dochádza k zmene frekvencie nosnej vlny. [15]

2.3.2.3 Fázové kľúčovanie

Fázové kľúčovanie, vychádza z anglického Phase - Shift Keying (PSK), funguje na princípe zmeny fázy nosnej frekvencie. Túto moduláciu signálu využívajú aj zariadenia, kde je potrebná rýchlejšia odozva, napríklad modemy. [15]

2.4 Komunikačné režimy

Komunikačný režim charakterizuje spôsob a možnosť zariadenia komunikovať s ostatnými zariadeniami, čiže prijímať alebo vysielať dáta. V rámci režimov komunikácie môžeme zariadenia rozdeliť na viacero druhov:

1. simplexná komunikácia,
2. polovičný duplex
3. plný duplex.

V rámci zariadení SDR môžeme komunikačne režimy rozdeliť na prijímače a transceivery.

2.4.1 Simplexná komunikácia

Simplexná komunikácia je definovaná ako komunikácia, ktorá prebieha iba jedným smerom. Príkladom simplexnej komunikácie môže byť rádiové alebo televízne vysielanie, kde vysielacia stanica vysiela signál a koncové zariadenie prijíma jeho vysielanie bez spätnej odpovede. Opakom simplexnej komunikácie je duplexná komunikácia, ktorá prebieha oboma smermi. [17]

2.4.2 Polovičný duplex

Polovičný duplex, po anglicky half - duplex, je režim komunikácie, kde dochádza k obojstrannej komunikácii, ale iba jedným smerom v rovnakom čase. V momente, keď jedna strana začne prijímať signál, musí druhá strana počkať na dokončenie vysielania a až následne môže začať s odpoveďou. Typickým príkladom sú vysielačky, kde pri príjme signálu nemôžeme odpovedať. [17]

2.4.3 Plný duplex

Plný duplex, po anglicky full - duplex, je systém komunikácie, ktorý umožňuje komunikáciu oboma smermi, ale na rozdiel od polovičného duplexu môže táto komunikácia prebiehať súčasne. Príkladom takéhoto typu komunikácie je telefonická komunikácia, kde je možné, aby obe strany hovorili naraz. [18]

2.4.4 Prijímače a transceivery

Pri výbere správneho zariadenia alebo pri všeobecnej práci s SDR je dôležité spomenúť, že na trhu sa vyskytujú dva typy SDR zariadení.

Prvým typom sú zariadenia, ktoré vedia pracovať iba ako prijímače. Tieto zariadenia umožňujú iba simplexnú komunikáciu, čiže vedia iba prijímať signály. Zariadenia väčšinou disponujú podstatne nižšou cenou.

Druhým typom sú transcievery alebo zariadenia, ktoré využívajú duplexnú komunikáciu. Slovo transciever je odvodené z anglických slov transmiter ako vysielač a reciever ako prijímač. Tieto zariadenia vedia dáta nielen prijímať, ale aj vysielať, čo umožňuje širšie využitie ako klasické prijímače. Z ich rozšírenejších funkcií vyplýva aj ich pomerne vyššia cena. [18], [19]

Obľúbenou možnosťou v oblasti SDR je vytvorenie si vlastného transciveru a to kombináciou cenovo dostupenejšieho SDR prijímača akým je napríklad zariadenie RLT (Realtek Limited) – SDR a mikropočítača Raspberry Pi. Po nainštalovaní špecifického softvéru je možné využiť samotný mikropočítač ako vysielacie zariadenie a pomocou kombinácie týchto dvoch zariadení realizovať útoky s prehraním.

2.5 Softvér pre SDR

Na súčasnom trhu existujú mnohé softvérové riešenia pre využívanie SDR. Softvér môžeme rozdeliť na dve kategórie. Prvý z nich je všeobecný softvér. Tento spolupracuje s väčšinou dostupných SDR na trhu a obsahuje mnoho funkcii, ktoré využívajú nielen nadšenci rádio komunikácie, ale aj profesionáli. Druhou kategóriou softvéru je špecifický softvér na konkrétne profesionálne SDR, prípadne softvér na konkrétne aplikácie. Ďalej existujú softvérové riešenia pre rôzne systémy a rôzne operačné systémy. Táto bakalárska práca sa bude zaoberať a využívať prvú kategóriu softvéru.

K najrozšírenejším softvérovým riešeniam využívaným v oblasti SDR patria:

- SDRsharp
- GNU Radio
- Universal Radio Hacker

2.5.1 SDRsharp

SDRsharp je bezplatný softvér, ktorý je veľmi populárny u začiatočníkov v oblasti SDR, ale obsahuje tiež všetky pokročilé funkcie. Výhodou tohto softvéru je jeho grafické rozhranie, ktoré je prehľadné a ľahko sa v ňom orientuje. Tento softvér je kompatibilný s veľkým počtom SDR zariadení. Vo svojej práci budem využívať tento softvér. [19]

2.5.2 GNU Radio

GNU Radio je bezplatný open-source softvér, ktorý využíva bloky, ktoré reprezentujú spracovanie signálu. Môže sa použiť na vývoj aplikácií pre širokú škálu rádiokomunikačných systémov vrátane bezdrôtových komunikácií, radarov a satelitných systémov. Jednou z kľúčových vlastností GNU Radio je jeho modulárny dizajn, ktorý používateľom umožňuje jednoducho vytvárať nové bloky spracovania signálu a vzájomne ich prepájať, aby vytvorili komplexné systémy. Poskytuje tiež grafické užívateľské rozhranie na budovanie a simuláciu rádiových systémov, ako aj nástroje na testovanie a ladenie implementovaného systému. [20]

2.5.3 Universal Radio Hacker

Universal Radio Hacker je bezplatný softvérový nástroj s otvoreným zdrojovým kódom, ktorý možno použiť na analýzu a dekódovanie širokého spektra rádiových signálov. Používajú ho predovšetkým rádioví nadšenci a výskumníci, aby preskúmali možnosti rôznych rádiových systémov a dozvedeli sa viac o tom, ako fungujú. Tento softvér je výkonný a všestranný nástroj, ktorý možno použiť so širokou škálou rádiového hardvéru vrátane softvérovo definovaných rádií a iných typov rádiových prijímačov. Má jednoduché a užívateľsky prívetivé rozhranie, ktoré umožňuje používateľom jednoducho konfigurovať a ovládať svoj rádiový hardvér, ako aj vizualizovať a analyzovať rádiové signály, ktoré prijímajú. Jednou z kľúčových vlastností je jeho schopnosť dekódovať množstvo rôznych rádiových protokolov, vrátane tých, ktoré sa používajú v bezdrôtovej komunikácii, ako je Bluetooth, Wi-Fi a mobilné siete. To umožňuje používateľom nielen počúvať rádiové signály, ale aj porozumieť a interpretovať dáta, ktoré prenášajú. URH obsahuje aj množstvo ďalších funkcií, vďaka ktorým je užitočným nástrojom pre nadšencov rádií a výskumníkov. Ďalšou vstavanou funkciou je generátor signálu, ktorý umožňuje používateľom vytvárať a prenášať svoje vlastné rádiové signály, ako aj sadu nástrojov na spracovanie signálov, ktoré možno použiť na analýzu a manipuláciu so signálmi, ktoré prijímajú. Celkovo je Universal Radio Hacker cenným nástrojom pre každého, kto má záujem dozvedieť sa viac o rádiovej technológii a jej

fungovaní. Je to všestranný a výkonný nástroj, ktorý možno použiť pre širokú škálu aplikácií, od jednoduchého počúvania rádiových signálov až po vykonávanie podrobných analýz a výskumu rôznych rádiových systémov. [21]

2.6 SDR Hardvér

Hardvér SDR je navrhnutý tak, aby bol flexibilný a konfigurovateľný, čo umožňuje jeho použitie pre širokú škálu aplikácií a podporu rôznych rádiových protokolov a frekvenčných pásiem. Špecifické komponenty a dizajn hardvéru SDR sa môžu líšiť v závislosti od konkrétnych požiadaviek a možností systému. Prvým a najdostupnejším typom sú SDR kľúče. Ide o malé prenosné zariadenia, ktoré na pripojenie k počítaču používajú rozhranie USB. Zvyčajne obsahujú rádiový prijímač a DSP a možno ich použiť s množstvom rôznych softvérových aplikácií na príjem a spracovanie rádiových signálov. Ďalšou kategóriou sú väčšie zariadenia, ktoré obsahujú už potrebné komponenty na vysielanie signálu. Tento typ hardvéru obsahuje všetky potrebné komponenty pre kompletný systém SDR vrátane rádiového prijímača, DSP a iného podporného hardvéru. Je zvyčajne väčší a drahší ako kľúče SDR, ale ponúka pokročilejšie možnosti a flexibilitu. Poslednou kategóriou je možnosť zostavenia si vlastného hardvéru.

2.6.1 RTL–SDR

RTL-SDR je typ softvérovo definovaného rádia, ktoré využíva lacný televízny tuner na príjem a spracovanie rádiových signálov. Je to populárny a cenovo dostupný spôsob pre nadšencov rádia a výskumníkov ako preskúmať možnosti technológie SDR. RTL-SDR je malé prenosné zariadenie, čo uľahčuje jeho používanie s prenosným počítačom alebo iným prenosným počítačovým zariadením. Na pripojenie k počítaču používa rozhranie USB a možno ho použiť s množstvom rôznych softvérových aplikácií na príjem a spracovanie rádiových signálov. Jednou z kľúčových výhod RTL-SDR je nízka cena. Zvyčajne sú tieto zariadenia oveľa lacnejšie ako iné typy hardvéru SDR, vďaka čomu sú dostupné širšiemu okruhu používateľov. Majú taktiež široký frekvenčný rozsah, ktorý im umožňuje prijímať signály v rôznych frekvenčných pásmach. Kľúče RTL-SDR sa dajú použiť na rôzne aplikácie, vrátane počúvania rádia FM, dekódovania digitálnych rádiových signálov a dokonca aj sledovania lietadiel. Môžu byť tiež použité v kombinácii s inými softvérovými nástrojmi, ako je Universal Radio Hacker, na vykonávanie pokročilejších analýz a výskumu rádiových signálov. Celkovo sú kľúče RTL-SDR obľúbeným a cenovo dostupným spôsobom pre

nadšencov rádií a výskumníkov, ktorými môžu preskúmať svet softvérovo definovaných rádií. Sú všestranné, ľahko sa používajú a môžu byť použité pre širokú škálu apliká cií. [22]

2.6.2 HackRF One

HackRF One je typ hardvéru softvérovo definovaného rádia SDR, ktorý možno použiť na príjem a prenos rádiových signálov. Je to malé prenosné zariadenie, ktoré sa pripája k počítaču cez rozhranie USB a možno ho použiť s množstvom rôznych softvérových aplikácií na príjem a spracovanie rádiových signálov. HackRF One je navrhnutý ako všestranný a flexibilný nástroj pre rádiových nadšencov a výskumníkov. Má široký frekvenčný rozsah, ktorý mu umožňuje prijímať a vysielať signály v rôznych frekvenčných pásmach. Má tiež vysoký dynamický rozsah, čo mu umožňuje zvládnuť silné signály bez skreslenia. Jednou z kľúčových vlastností HackRF One je jeho schopnosť vysielať aj prijímať rádiové signály. To umožňuje používateľom nielen počúvať rádiové signály, ale aj experimentovať s vytváraním a prenosom vlastných signálov. To môže byť užitočné pre rôzne aplikácie, ako je testovanie bezdrôtových zariadení alebo vytváranie vlastných rádiových protokolov. HackRF One je tiež open-source, čo znamená, že dizajn hardvéru a softvéru sú používateľom voľne k dispozícii na úpravu a prispôsobenie podľa potreby. To umožňuje používateľom vytvárať vlastné verzie hardvéru a softvéru alebo integrovať HackRF One do väčších projektov a systémov. [23]

2.6.3 RPITX a Raspberry Pi

RPITX je softvér, ktorý umožňuje užívateľovi prenášať rádio frekvenčné signály pomocou počítača Raspberry Pi. Raspberry Pi je malý jednodoskový počítač, ktorý je obľúbený medzi elektrotechnickými nadšencami. Ide o nízko nákladovú a flexibilnú platformu, ktorú možno použiť pre širokú škálu projektov - od domácich mediálnych centier a herných konzol až po systémy domácej automatizácie a zariadenia internetu vecí. Raspberry Pi má niekoľko funkcií, vďaka ktorým je vhodný na použitie so softvérom RPITX. Má napríklad výkonný procesor, ktorý zvládne výpočtovú náročnosť prenosu rádio frekvenčných signálov. Po nainštalovaní softvéru je možne nakonfigurovať Raspberry Pi na prenos rádio frekvenčných signálov pomocou príslušných príkazov. Jednou z kľúčových výhod používania softvéru RPITX s Raspberry Pi je, že umožňuje prenášať rádio frekvenčné signály bez potreby ďalšieho hardvéru. Umožňuje tiež väčšiu flexibilitu a experimentovanie, pretože používateľ môže jednoducho upraviť softvér tak, aby vyhovoval jeho špecifickým potrebám. Spojenie Raspberry

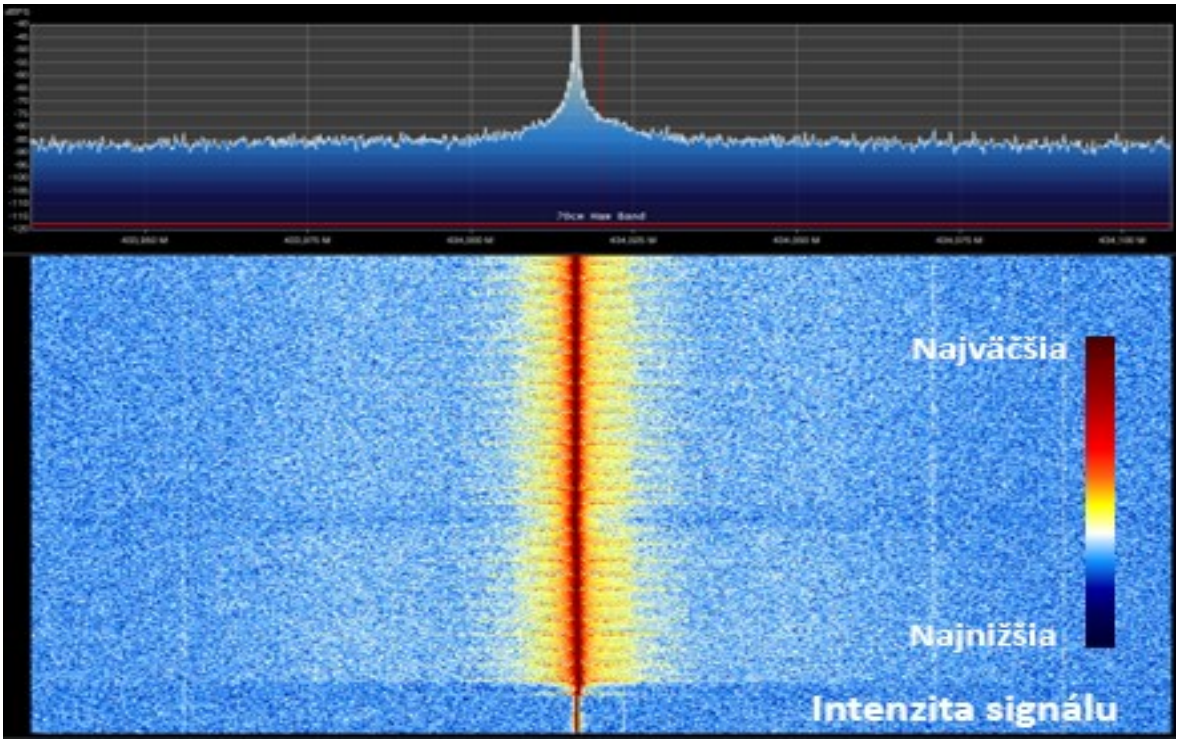
Pi a kľúča RTL-SDR vytvára prenosné a veľmi kompaktné zariadenie na realizáciu rádiových útokov s prehraním v reálnych podmienkach. [24]

3 ANALÝZA BEZDRÔTOVÝCH ÚTOKOV

Nasledujúca kapitola obsahuje analýzu možných typov útokov použitých na prekonanie bezpečnostných systémov automobilov. Uvádza príklady použitia dostupného hardvéru a softvéru.

3.1 Jamming attack

Útok rušením, po anglicky Jamming attack, je typ bezdrôtového útoku, kde dochádza k rušeniu signálu. Útočník vysiela na bezdrôtovom spektre náhodný signál, ktorý väčšinou nepredstavuje nič konkrétne. Cieľom útoku je vysielaním silnejšieho signálu znemožniť správnu komunikáciu medzi zariadeniami. Útok môže narušovať konkrétnu frekvenciu a prípadne aj jej podkanály. [25]



Obrázok 9 Rušenie na frekvencií 434 MHz [zdroj: vlastný]

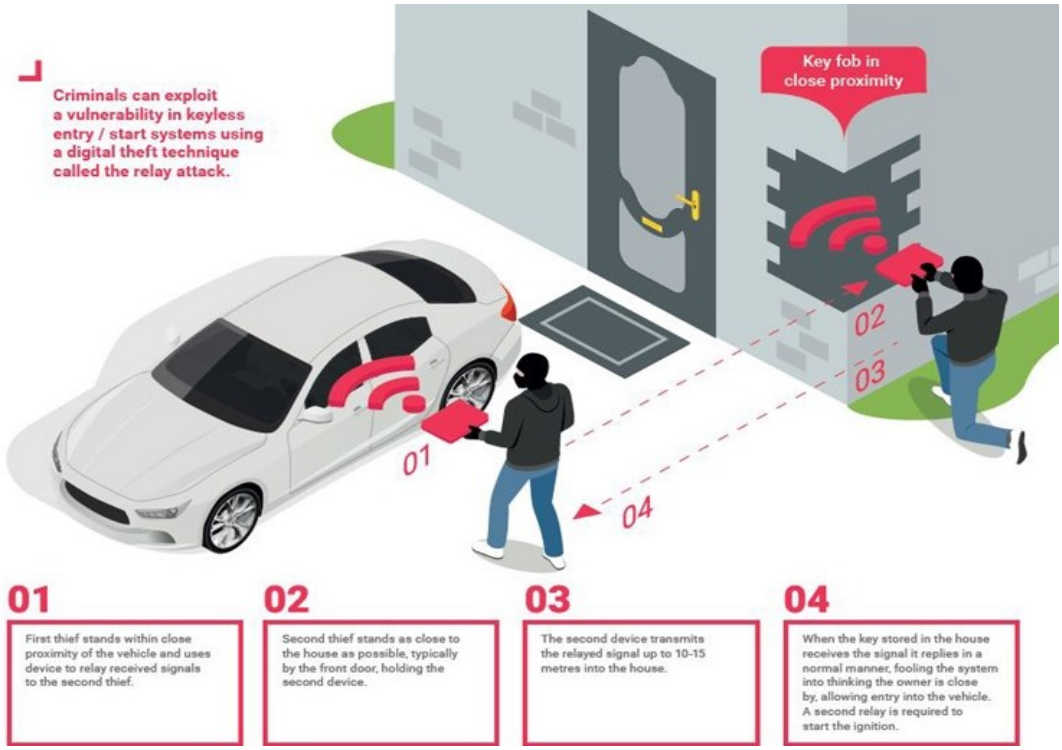
Obrázok 9 zobrazuje rušenie na frekvencií 433 MHz zachytené pomocou SDR. Na grafe v hornej časti obrázku je vykreslený vrchol v reálnom čase, ktorý znázorňuje, že je vysielaný aktívny signál na danej frekvencií. V spodnej časti obrázku sa nachádza rozloženie vysielaného signálu v priebehu času, kde červená farba predstavuje násilnejší vysielaný signál.

3.2 Replay attack

Na prevedenie útoku je útok prehraním, anglicky Replay attack, veľmi jednoduchý. Podstata útoku spočíva v zachytení zašifrovaného signálu a jeho následným prehraním. Pri realizácii útoku útočník odpočúva dané frekvenčné pásmo a následne zachytáva signál. Po jeho úspešnom zachytení je signál možné opätovne prehrávať niekoľkokrát. Slabinou systémov bez odolnosti proti útokom s prehraním je, že útočník nepotrebuje odborné znalosti k prevedeniu útoku. [26]

3.3 Relay attack

Tento typ útoku najčastejšie realizujú dvaja útočníci, ktorí majú prístup k zaparkovanému vozidlu a taktiež ku kľúču od vozidla. Najjednoduchším scenárom je, že vozidlo sa nachádza zaparkované pred domom a kľúč od vozidla je umiestnený v blízkosti dverí alebo okna tak, aby mohli cez tieto materiály ľahko prechádzať rádiové vlny. Jeden útočník sa je v blízkosti kľúča vozidla a druhý pri vozidle. Obaja majú zariadenia, ktoré komunikujú medzi sebou a takto predĺžia vzdialenosť komunikácie s vozidlom, respektíve prinútia vozidlo si myslieť, že kľúč sa nachádza v jeho blízkosti. Následne po odcudzení vozidla dochádza k výmene riadiacich jednotiek, prípadne naprogramovaniu nového kľúča. Tieto systémy sa dajú zaobstarať na čiernom trhu. [27]



Obrázok 10 Príklad relay útoku [28]

3.4 RollJam attack

RollJam útok je špeciálny typ útoku, ktorý je zameraný na zariadenia zabezpečené plávajúcim kódom. Samy Kamar v roku 2015 na konferencií DEF CON demonštroval tento typ útoku. Je považovaný za prvého bezpečnostného výskumníka, ktorý poukázal na nedostatky v týchto zabezpečovacích systémoch. [29] Tento útok je podobný útoku prehraním, ale s pridaným elementom rušenia. Útočník so zariadením sa nachádza v blízkosti automobilu a čaká na užívateľovu interakciu. Po užívateľovej interakcii diaľkové ovládanie vyšle signál, ktorý je zachytený útočníkom a zároveň rušením sa zamedzuje prijatie signálu vozidlom. Užívateľ opätovne použije diaľkové ovládanie, nakoľko podľa neho prvýkrát auto nezareagovalo. Útočník zachytí aj tento signál a následne prehrá prvý zachytený signál bez rušenia a tento signál vozidlo akceptuje. Útočník má následne k dispozícii druhý zachytený signál, ktorý ešte nebol použitý. [29]

II. PRAKTICKÁ ČASŤ

4 NÁVRH MODELU ZABEZPEČENIA

Systém centrálneho zamykania auta je mechanizmus, ktorý umožňuje vodičovi na diaľku zamknúť alebo odomknúť všetky dvere svojho vozidla jediným úkonom - stlačením tlačidla na diaľkovom ovládači. Systém sa zvyčajne skladá z nasledujúcich komponentov:

- riadiaci modul centrálneho zamykania: toto je hlavná riadiaca jednotka systému, ktorá riadi zamykanie a odomykanie dverí vozidla. Riadiaci modul prijíma signály z diaľkového ovládača a posiela príkazy ovládačom zámku dverí na zamknutie alebo odomknutie dverí,
- ovládače zámku dverí: sú to motory, ktoré fyzicky zamykajú alebo odomykajú dvere vozidla. Pohony zámku dverí sú pripojené k riadiacemu modulu centrálneho zamykania pomocou vodičov a sú aktivované riadiacim modulom,
- diaľkové ovládanie: toto je zariadenie, ktoré vysiela bezdrôtové signály do riadiaceho modulu centrálneho zamykania na zamykanie a odomykanie dverí vozidla. Diaľkové ovládanie zvyčajne pracuje na frekvencii 433 MHz,
- káblový zväzok: ide o súbor káblov, ktoré spájajú všetky komponenty centrálneho uzamykacieho systému,
- napájanie: Systém vyžaduje 12 voltové napájanie pre napájanie všetkých komponentov. Je možné použiť autobatériu alebo jednosmerný zdroj.

Keď vodič stlačí tlačidlo uzamknutia alebo odomknutia na diaľkovom ovládači, vykonajú sa tieto kroky:

- diaľkový ovládač vyšle signál do riadiaceho modulu centrálneho zamykania,
- riadiaci modul centrálneho zamykania príjme signál a odošle príkaz ovládačom zámku dverí na zamknutie alebo odomknutie dverí,
- ovládače zámku dverí fyzicky zamykajú alebo odomykajú dvere vozidla,
- stav činnosti uzamknutia/odomknutia je zvyčajne indikovaný blikajúcim svetlom diaľkového ovládača, prípadne vozidla alebo zvukovým upozornením,

Moderné systémy centrálneho zamykania automobilov môžu obsahovať aj ďalšie funkcie, ako je automatické zamykanie dverí, keď je vozidlo v pohybe, poplašné systémy proti krádeži a systémy bezkľúčového vstupu, ktoré umožňujú vodičovi odomknúť vozidlo jednoduchým priblížením sa k nemu.

Pri návrhu systému centrálneho zamykania automobilu založeného na Arduino je nevyhnutné pamätať na integráciu rôznych komponentov, aby sa vytvoril funkčný mechanizmus, ktorý presne reprezentuje činnosť skutočného systému centrálneho zamykania automobilu. V tomto modeli sa používajú dve dosky Arduino Uno: jedna slúži na prijímanie signálov, ich spracovanie a ovládanie činností zamykania/odomykania, zatiaľ čo druhá doska znázorňuje diaľkové ovládanie s tlačidlami na zamykanie a odomykanie spolu s vysielačom. Napájanie dosiek Arduino je možné prostredníctvom sieťového adaptéra, 9 voltovej batérie alebo kábla USB.

Na účely demonštrácie útokov a porovnania sa okrem toho môže použiť komerčne dostupná súprava centrálneho zamykania určená na integráciu do vozidla. Táto súprava zvyčajne obsahuje riadiacu jednotku, kabeláž, dva diaľkové ovládače a malý servomotor, ktorý funguje ako mechanizmus zámku dverí. Systém je napájaný štandardným 12 voltovým elektrickým napájaním, ktoré zodpovedá automobilovým normám. Konkrétne podrobnosti o zapojení a praktickej realizácii systému centrálneho zamykania na báze Arduina sú popísané v praktickej časti bakalárskej práce, ktorá poskytuje komplexný návod na projekt.

5 NÁVRH ÚTOKU

Pri vytváraní stratégie útoku je nevyhnutné zvážiť určité kľúčové vlastnosti, ktoré by mal útok mať. Jednou z týchto vlastností je jednoduchosť z hľadiska vykonania útoku, ako aj celkového času potrebného na jeho vykonanie. Po zvážení všetkých vlastnosti bol na účely testovania vybraný špecifický typ útoku nazývaný replay attack.

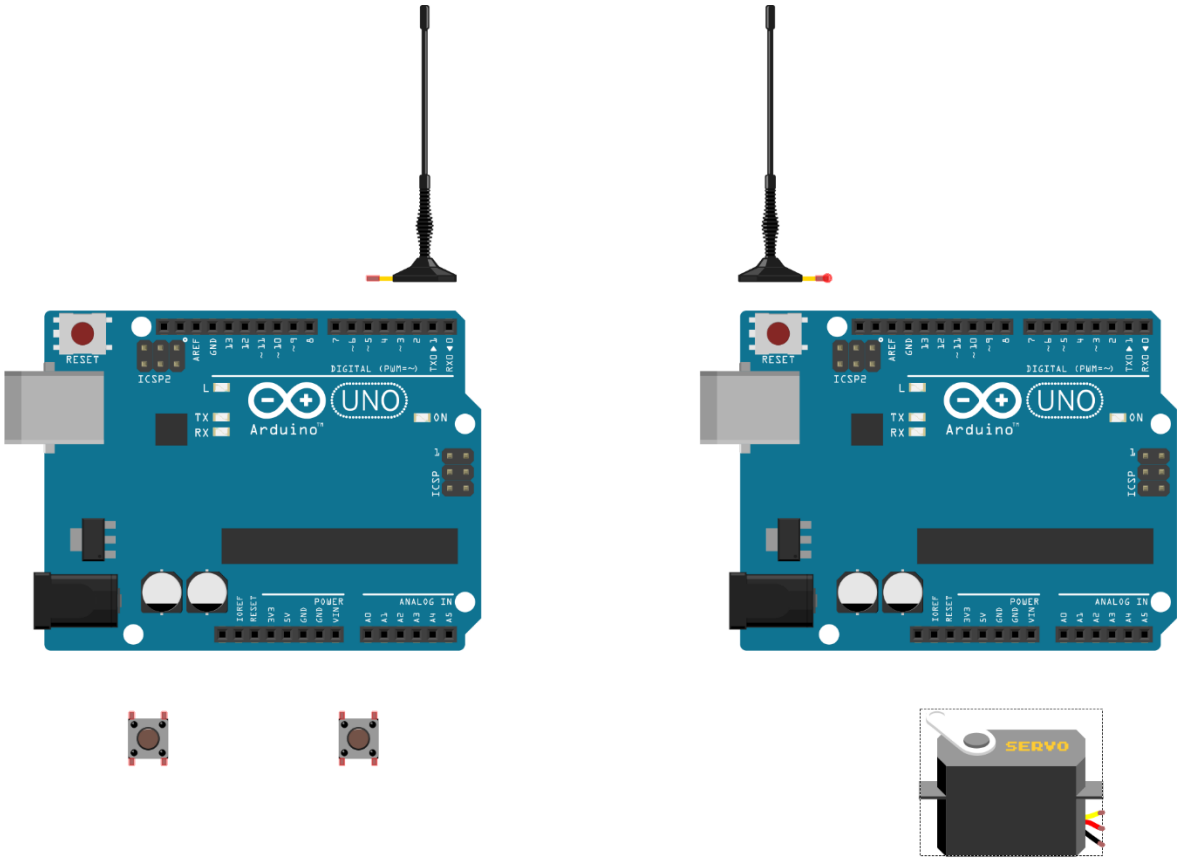
Na efektívne vykonanie útokov boli vybrané dve rôzne metódy. Prvá metóda zahŕňala využitie zariadenia HackRF One, ktoré bolo pripojené k počítaču a ovládané pomocou programu Universal Radio Hacker. Táto konfigurácia poskytovala flexibilitu a presné ovládanie pri vykonávaní útoku a to umožnilo dôkladné posúdenie jeho účinnosti. Pri druhej metóde útoku sa použilo zariadenie vytvorené na mieru na platforme Raspberry Pi. V tejto konfigurácii sa na príjem cieľového signálu použilo cenovo dostupné RTL-SDR. Na zariadení Raspberry Pi bol spustený softvér RPTIX, ktorý umožňoval zachytávanie, ukladanie a následné prehrávanie zachyteného signálu. Na zabezpečenie pohodlia a mobility bolo zariadenie Raspberry Pi vybavené batériou.

Rozhodnutie zvoliť alternatívu založenú na Raspberry Pi bolo podmienené predovšetkým dostupnosťou a cenovou výhodnosťou jednotlivých komponentov. Vzhľadom na celkovú cenu toto riešenie predstavovalo ekonomickejšiu alternatívu v porovnaní so zariadením HackRF One. Tento výber umožnil komplexné vyhodnotenie stratégie útoku pri zohľadnení faktora cenovej dostupnosti.

Použitie dvoch rôznych možností nasadenia zariadení bolo predpokladom na dôkladné posúdenie účinnosti a realizovateľnosti útokov tohto typu. Počas celého procesu bola prvoradá jednoduchosť vykonania a zohľadnenie nákladov. Tento prístup uľahčil komplexnú analýzu vplyvu útoku a poskytol cenné poznatky o jeho potenciálnych dôsledkoch.

6 ZOSTROJENIE MODELU ARDUINA

Na prezentáciu fungovania bezdrôtového systému zamykania auta sa uskutočnila demonštrácia s použitím dvoch platforiem Arduino Uno. Tieto platformy sa použili na vytvorenie systému s rôznymi úlohami: jedna slúžila ako prijímací komponent, druhá ako vysielací komponent.



Obrázok 11 Ilustrácia platforiem Arduino Uno [zdroj: vlastný]

Prvá platforma Arduino Uno bola určená na prijímanie systému. Bola vybavená potrebným hardvérom a softvérom na prijímanie a interpretáciu bezdrôtových signálov. Toto Arduino Uno fungovalo ako centrálna jednotka zodpovedná za detekciu a spracovanie signálov vysielaných vysielacím komponentom.

Druhé Arduino Uno bolo určené ako vysielacia časť systému. Jeho hlavnou funkciou bolo generovať a vysielať bezdrôtové signály do prijímacieho komponentu. Toto Arduino Uno bolo nakonfigurované na interakciu s prijímacím zariadením, čo mu umožnilo vysielať príslušné príkazy na interakciu so servomotorom.

Dve platformy Arduino Uno navzájom spolupracovali, aby demonštrovali princíp bezdrôtového zamykania automobilu. Keď sa spustil príkaz na zamknutie alebo odomknutie vozidla, vysielacia jednotka Arduino Uno generovala príslušný bezdrôtový signál. Tento signál sa

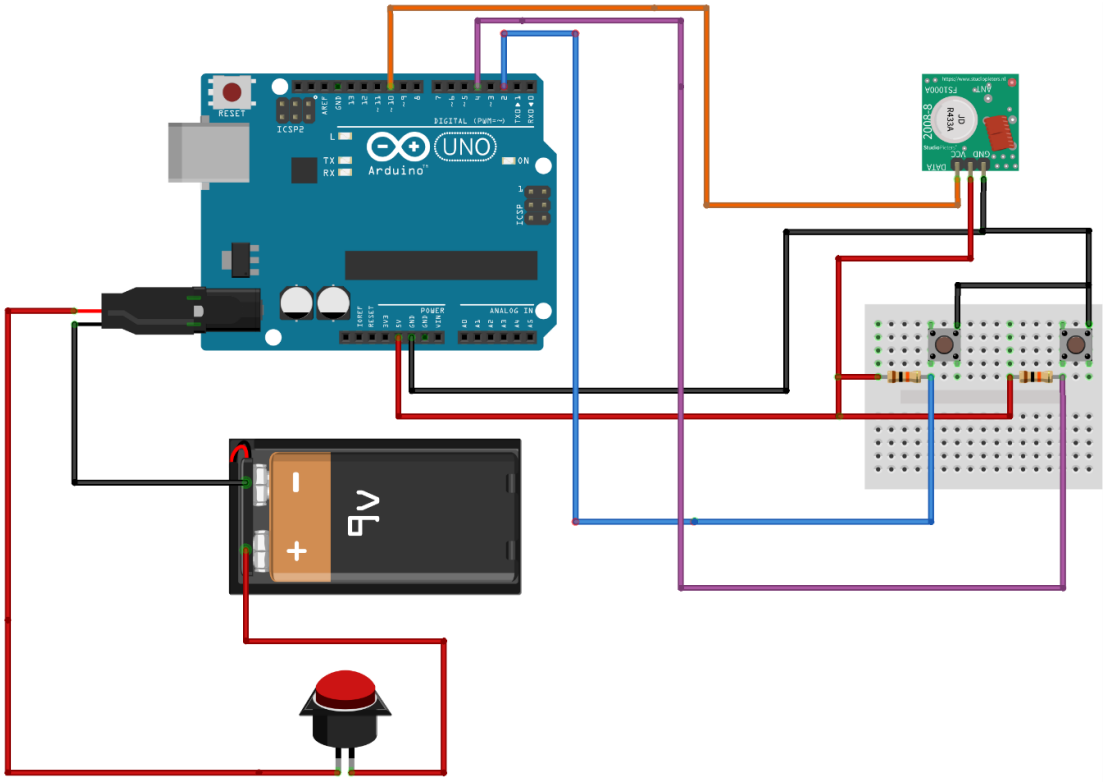
potom preniesol do prijímajúceho zariadenia. Po prijatí signálu ho zariadenie Arduino Uno interpretovalo a príslušne spracovalo. V závislosti od povahy príkazu sa následne spustia potrebné akcie na zamknutie alebo odomknutie vozidla. Táto interaktívna zostava účinne simuluje praktický scenár a poskytuje jasné pochopenie toho, ako môže fungovať bezdrôtový systém zamykania automobilu.

6.1 Vysielač

Vysielacia časť Arduina slúži ako reprezentácia diaľkového ovládania, ktoré sa používa v systéme centrálneho zamykania vozidla. Jej hlavným účelom je posielať príkazy do riadiacej jednotky po prijatí vstupu od používateľa. Táto vysielacia časť sa skladá z niekoľkých prvkov:

- Arduino Uno: Doska Arduino Uno slúži ako hlavný riadiaci prvok, ktorý je zodpovedný za spracovanie a vykonávanie úloh potrebných na prenos príkazov,
- vysielací modul: Modul vysielača sa používa na uľahčenie bezdrôtového prenosu signálov. Tento modul je pripojený k doske Arduino a zohráva dôležitú úlohu pri vysielaní príkazov,
- tlačidlá: Dve tlačidlá, ktoré sú súčasťou vysielacej časti, predstavujú funkcie uzamknutia a odomknutia. Tieto tlačidlá poskytujú používateľovi možnosti na zadanie požadovaného príkazu. Po stlačení iniciujú prenos príslušného signálu do riadiacej jednotky.

Na zabezpečenie prenosnosti a jednoduchého používania sa ako zdroj energie pre vysielaciu časť používa 9 voltová batéria. Táto konfigurácia umožňuje pohodlnú prepravu bezdrôtového systému uzamykania bez potreby pevného zdroja napájania.



Obrázok 12 Nákres Arduino vysielača [zdroj: vlastný]

Na účel prepojenia medzi komponentmi, sú pridelené špecifické digitálne piny na Arduino Uno. V tejto konfigurácii sa využívajú piny D2, D4 a D10. Pin D2 je pripojený k odomykaciemu tlačidlu, zatiaľ čo D4 je pripojený k uzamykaciemu tlačidlu. Tieto pripojenia umožňujú doske Arduino prijímať vstupy z tlačidiel a spracovávať príslušné príkazy. Vysielací modul je pripojený k pinu D10, ktorý umožňuje bezdrôtový prenos príkazov do druhého Arduina. Napájanie tlačidiel a vysielacieho modulu zabezpečené priamo z dosky Arduino, na čo sa využíva výstup 5 voltov. To zjednodušuje nastavenie zapojenia a zabezpečuje konzistentné napájanie týchto komponentov.

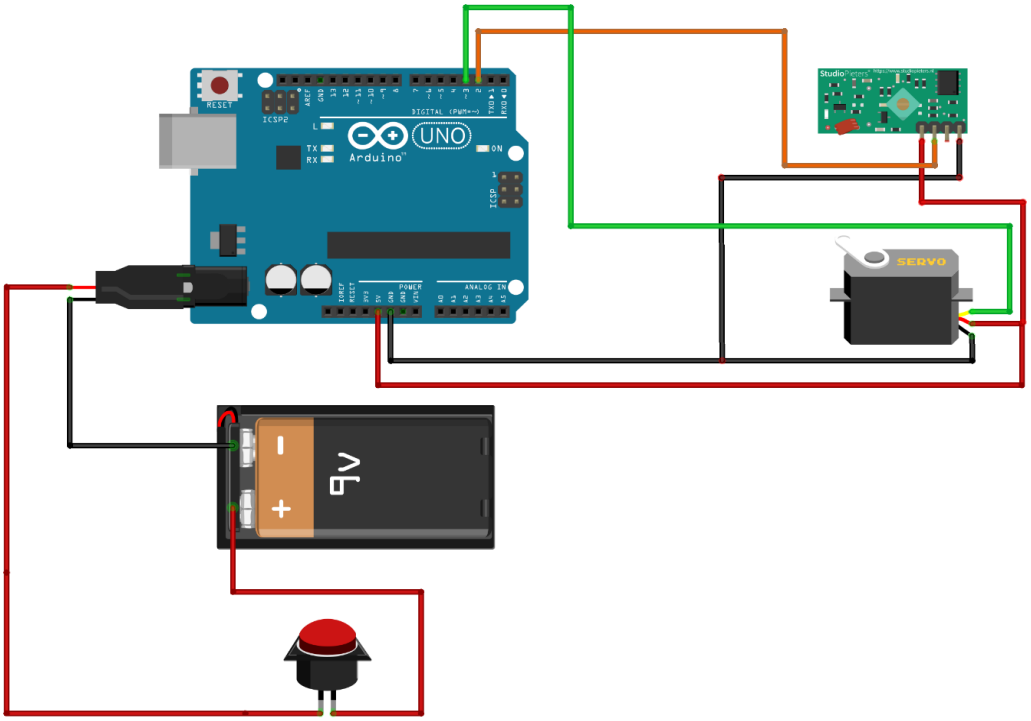
6.2 Prijímač

Prijímacia časť Arduina napodobňuje riadiacu jednotku centrálneho zamykania, ktorá sa nachádza vo vozidle. Jej hlavnou funkciou je prijímať signály vysielané diaľkovým ovládaním a konať podľa nich na základe prijatých pokynov. Prijímacia časť sa skladá z nasledujúcich prvkov:

- Arduino Uno: Podobne ako vo vysielacej časti, aj v prijímacom komponente slúži ako hlavný ovládač doska Arduino Uno. Je zodpovedná za spracovanie prichádzajúcich signálov a vykonávanie potrebných akcií,

- prijímací modul: Modul prijímača sa využíva na zachytávanie bezdrôtových signálov vysielaných diaľkovým ovládaním. Tento modul je pripojený k doske Arduino a umožňuje príjem a interpretáciu príkazov,
- servomotor: Na simuláciu mechanických činností spúšťaných riadiacou jednotkou centrálneho zamykania je použitý malý servomotor. Je zodpovedný za fyzické zamykanie alebo odomykanie dverí vozidla na základe prijatých príkazov.

Na zabezpečenie prenosnosti a pohodlia sa ako zdroj energie pre prijímajúcu časť používa 9 voltová batéria. To umožňuje jednoduchú prepravu systému bez potreby pevného napájania.



Obrázok 13 Nákres Arduino prijímača [zdroj: vlastný]

Na prepojenia medzi komponentmi sa využívajú špecifické digitálne piny na doske Arduino Uno. V tejto konfigurácii sa pin D2 používa na pripojenie prijímacieho modulu, čo mu umožňuje prijímať signály vysielané diaľkovým ovládaním. Pin D3 sa používa na pripojenie servomotora a to uľahčuje jeho ovládanie a umožňuje mu vykonávať požadované činnosti uzamknutia alebo odomknutia. Napájanie servomotora aj prijímacieho modulu zabezpečuje výstup 5 voltov z dosky Arduino. Týmto sa zabezpečuje konzistentný zdroj napájania komponentov, čo zjednodušuje prevádzku.

6.3 Program pre Arduino

Pre správne fungovanie zostavených modulov je potrebné do každej Arduino platformy nahrať správny kód. Pri písaní kódu boli použité knižnice Servo a RCSwitch. Vďaka týmto knižniciam je možné ľahko ovládať servomotor a tiež prijímať a vysielať signály cez rádiokomunikačné moduly. Program slúži ako simulácia systému uzamykania vozidla, ktorý využíva kombináciu rôznych modulov a knižníc na zobrazenie názornej ukážky systému centrálneho zamykania. Na dosiahnutie požadovanej funkcie je nevyhnutné nahrať príslušný kód do každej platformy Arduino zapojenej do systému.

Základná funkčnosť systému uzamykania automobilu spočíva v integrácii dvoch kľúčových knižníc: knižnice Servo a knižnice RCSwitch. Knižnica Servo poskytuje intuitívne a efektívne prostriedky na ovládanie servomotora, ktorý zohráva kľúčovú úlohu v mechanizme zámku auta. Využitím knižnice Servo môže program jednoducho manipulovať s polohou servomotora na zapnutie alebo vypnutie zámku auta, čím sa zabezpečí spoľahlivá a presná prevádzka. Knižnica RCSwitch umožňuje bezproblémovú rádiovú komunikáciu medzi rôznymi modulmi v rámci systému. Táto knižnica umožňuje programu bezdrôtovo vysielať a prijímať signály, čo je nevyhnutné pre efektívnu prevádzku systému zámku auta. Využitím knižnice RCSwitch môže program bezpečne komunikovať s rádiofrekvenčnými modulmi, čím sa uľahčuje prenos signálov zamykania a odomykania. Po prijatí príslušného signálu program prikáže servomotoru, aby sa otáčal, tým sa zapne alebo vypne mechanizmus zámku auta.

6.3.1 Program pre vysielanie signálu

Program pre vysielanie signálu pracuje výlučne s knižnicou RCSwitch a obsahuje dve čiastkové podmienky. Inicializačná časť programu zahŕňa nasledujúce príkazy:

- príkaz "mySwitch.enableTransmit" sa používa na priradenie pinu Arduino zodpovedného za vysielanie signálu,
- príkaz "pinMode" sa používa na konfiguráciu pinov ako vstupov pre tlačidlá,

- príkaz "Serial.begin" sa vykoná na inicializáciu sériovej komunikácie a zobrazenie prenášaného príkazu.

```
#include <RCSwitch.h>
RCSwitch mySwitch = RCSwitch();

void setup() {
  Serial.begin(9600); //zavedenie monitoru
  mySwitch.enableTransmit(10); //pouzitie pinu 10 na vysielanie
  pinMode(2,INPUT); //nastavenie pinu 2 na vstup tlacidla
  pinMode(4,INPUT); //nastavenie pinu 4 na vstup tlacidla

}
```

Obrázok 14 Zavedenie programu pre vysielanie [zdroj: vlastný]

V opakovacej slučke sa nachádzajú dve podmienky, ktoré sa vykonajú pri stlačení tlačidiel.

```
// podmienka ak je stlacene tlacidlo na pine 2
if(digitalRead(2)==LOW){
servo_value=1;  //poloha serva
  mySwitch.send(servo_value, 30); //poslanie hodnoty
  Serial.println(0); //zobrazenie polohy
}

// podmienka ak je stlacene tlacidlo na pine 4
if(digitalRead(4)==LOW){
servo_value=180;  //poloha serva
  mySwitch.send(servo_value, 30); //poslanie hodnoty
  Serial.println(180); //zobrazenie polohy
}}
```

Obrázok 15 Opakovacia časť programu pre vysielanie [zdroj: vlastný]

6.3.2 Program pre príjem signálu

Program pre príjem signálu, na rozdiel od programu pre vysielanie, pracuje s dvoma knižnicami a to konkrétne RCSwitch a Servo. Knižnica Servo je potrebná na ovládanie servomotoru. Spúšťacia časť programu na príjem pozostáva z nasledujúcich príkazov:

- príkaz "Serial.begin" sa vykoná na inicializáciu sériovej komunikácie a zobrazenie prijatého príkazu,
- príkaz "mySwitch.enableReceive" sa použije na priradenie pinu Arduino na príjem signálu,

- príkaz "servo.attach" sa použije na vytvorenie spojenia medzi servomotorom a určeným pinom,
- príkaz " servo.write" sa používa na definovanie polohy servomotora v uhlových stupňoch.

```
#include <Servo.h>
#include <RCSwitch.h>
Servo servo;
RCSwitch mySwitch = RCSwitch();

void setup() {
  Serial.begin(9600); //zavedenie monitoru
  mySwitch.enableReceive(0); //pouzitie pinu 2 na prijem // prerusovac (interrupt) 0 je na pine 2
  servo.attach(3); //pouzitie pinu 3 na pripojenie serva
  servo.write(95);//poloha zapnutia
}
```

Obrázok 16 Zavedenie programu pre príjem [zdroj: vlastný]

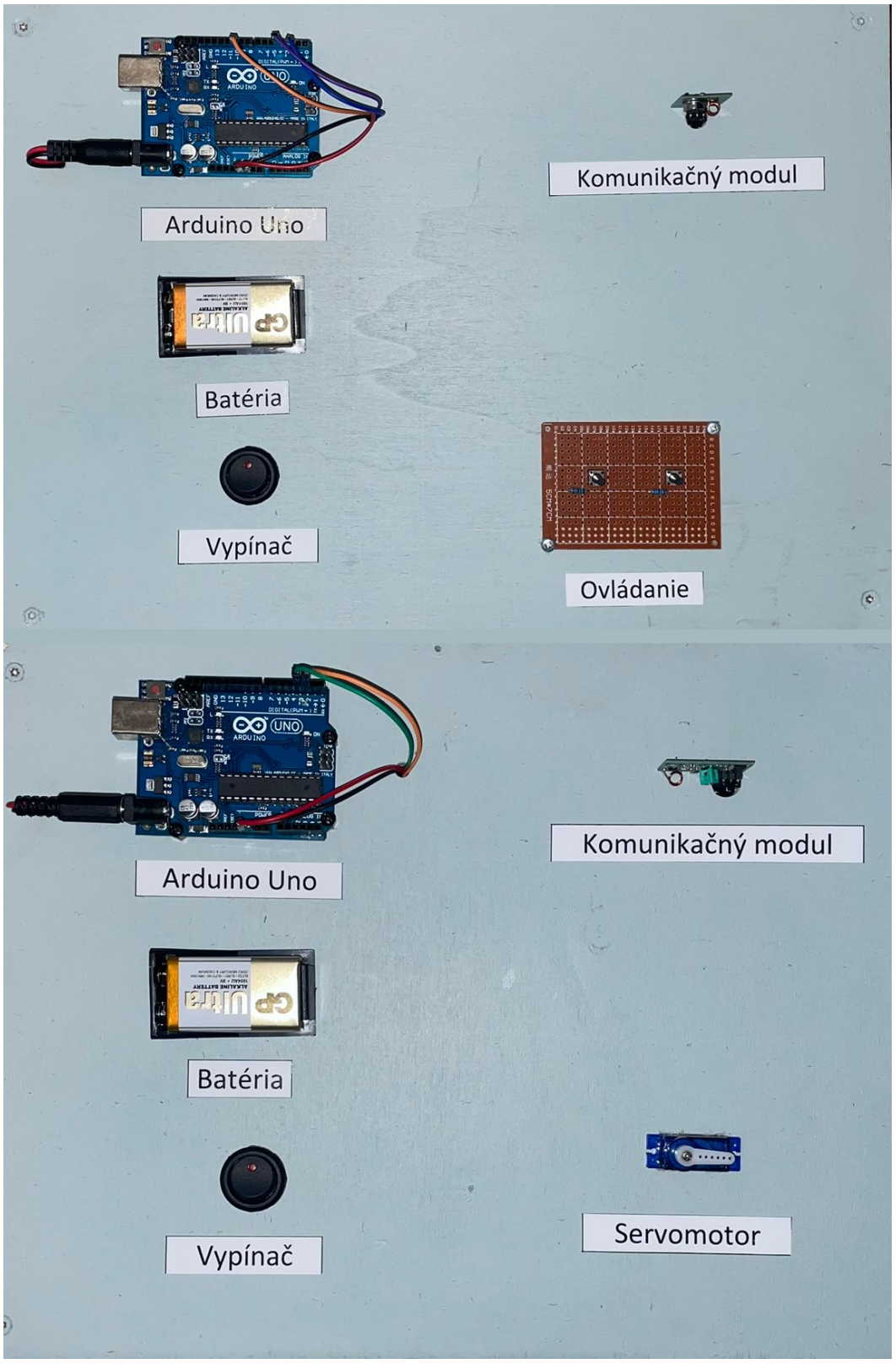
V rámci opakujúcej sa slučky sa implementuje príkaz na vypísanie prijatej hodnoty, po ňom na základe prijatej hodnoty nasleduje príkaz na nastavenie polohy servomotora.

```
void loop() {
  if (mySwitch.available()) {
    Serial.println(mySwitch.getReceivedValue()); //prijatie hodnoty
    servo.write(mySwitch.getReceivedValue()); //posun serva
    mySwitch.resetAvailable();
  }
}
```

Obrázok 17 Opakovacia časť programu pre príjem [zdroj: vlastný]

6.4 Kompletizácia modelu Arduino

Na nasledujúcom obrázku je zobrazená finálna montáž na dvoch samostatných doskách

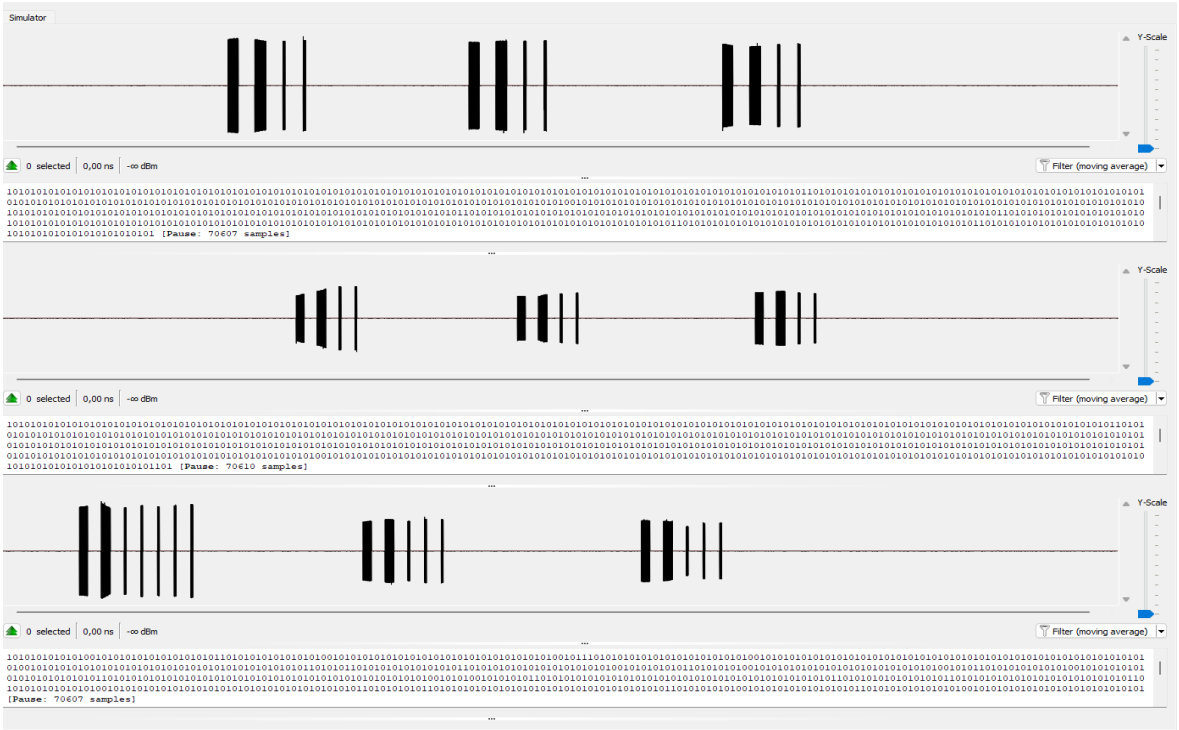


Obrázok 18 Montáž modelu Arduino na doskách [zdroj: vlastný]

7 POUŽITIE HACKRF ONE A UNIVERSAL RADIO HACKER

Vďaka bezproblémovej integrácii zariadenia HackRF One so softvérom Universal Radio Hacker nie je potrebné inštalovať žiadne ďalšie ovládače. Po nainštalovaní softvéru a pripojení zariadenia HackRF One k počítaču pomocou kábla USB je systém pripravený na zachytávanie a vysielanie signálov.

Softvér Universal Radio Hacker poskytuje používateľsky prívetivé rozhranie, v ktorom môžu používatelia vytvárať nové projekty na pohodlnú organizáciu a ukladanie zachytených signálov. Táto funkcia umožňuje používateľom zaznamenávať komplexný zber signálov, čím sa zabezpečí jednoduchý prístup a správa. Okrem toho softvér ponúka flexibilitu interakcie s rôznymi signálmi, čo ďalej zvyšuje jeho možnosti použitia a všestrannosť.

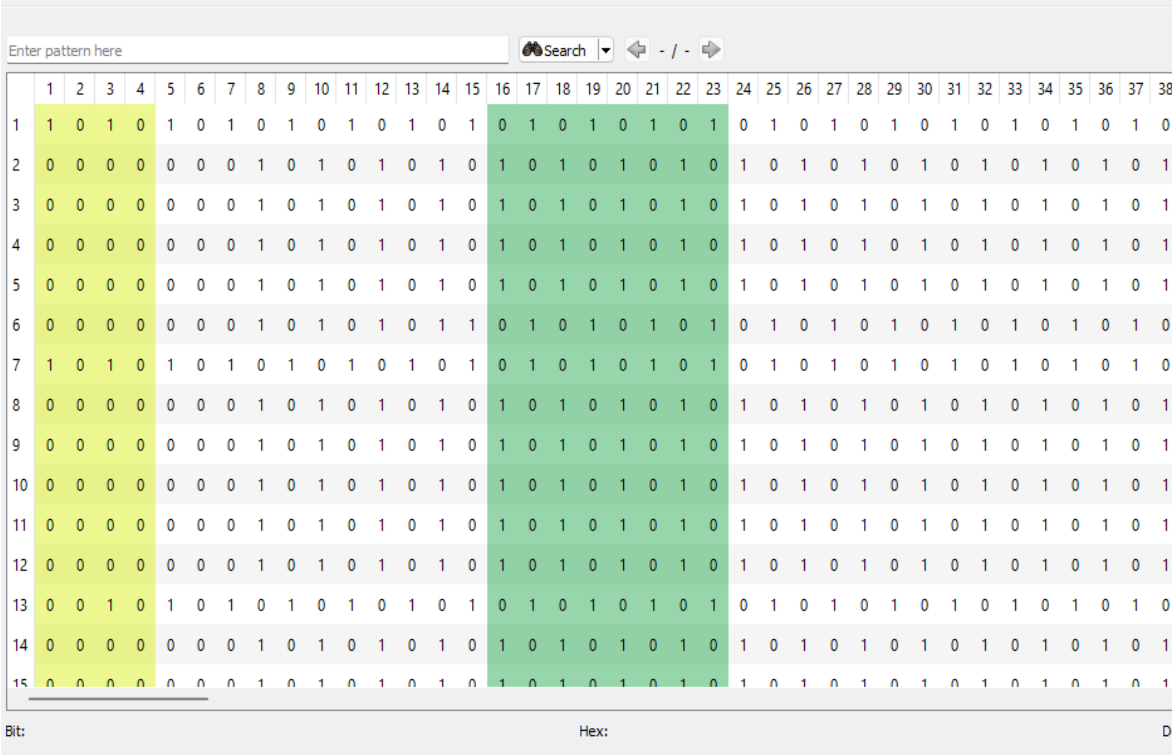


Obrázok 19 Príklad porovnania signálu [zdroj: vlastný]

Obrázok 19 znázorňuje objektívne porovnanie 3 opakovaní odomykacieho signálu 3 rôznych automobilov zachytených z rovnakej vzdialenosti, ktorých časová zvislosť je podobná. Na obrázku je možné vidieť, že najprv dôjde k 2 dlhším vyslaním signálu a následne k niekoľkým opakovaniam s kratším časovým trvaním. Konkrétne 3. signál vysiela 3 až 5 kratších úsekov. U 2. signálu vozidla je možné vidieť, že amplitúda vysielaného signálu je zo začiatku nižšia a postupne sa zvyšuje.

Jednou z unikátnych funkcií softvéru Universal Radio Hacker je jeho schopnosť zobraziť rozloženie zachytených signálov súčasne pre viacero kanálov. Táto funkcia umožňuje používateľom vizualizovať distribúciu signálu a poskytuje prehľad o jeho vlastnostiach a vzoroch. Analýzou distribúcie je možné lepšie pochopiť a interpretovať vysielané signály a podľa toho ich analyzovať. Okrem spomenutého softvér URH poskytuje cenné informácie o rôznych bitoch signálu. Táto funkcia sa ukazuje ako neoceniteľná pri dešifrovaní a interpretácii signálov, pretože pomáha identifikovať a analyzovať jednotlivé zložky tvoriace signál. Pochopením zloženia signálu na úrovni bitov môžeme získať detailné informácie o prenášaných údajoch medzi zariadeniami.

Obrázok 20 zobrazuje zachytený prenos dvoch prvých dlhších amplitúd príkazu odomknutia vozidla diaľkovým ovládaním dvoch rovnakých automobilov. Tieto automobily majú rovnaké parametre ako sú rok výroby a stupeň výbavy. Žltá časť analýzy prenesených údajov zobrazuje rovnaký začiatok prenášaných údajov, kde na riadku číslo 1 až 6 sú zachytené bity 1. vozidla a na riadkoch 7. až 12 druhého vozidla. Zelená časť analýzy zobrazuje 2. dlhšiu amplitúdu prenášaného signálu a vykresľuje, že všetky prenesené údaje sú zhodné.

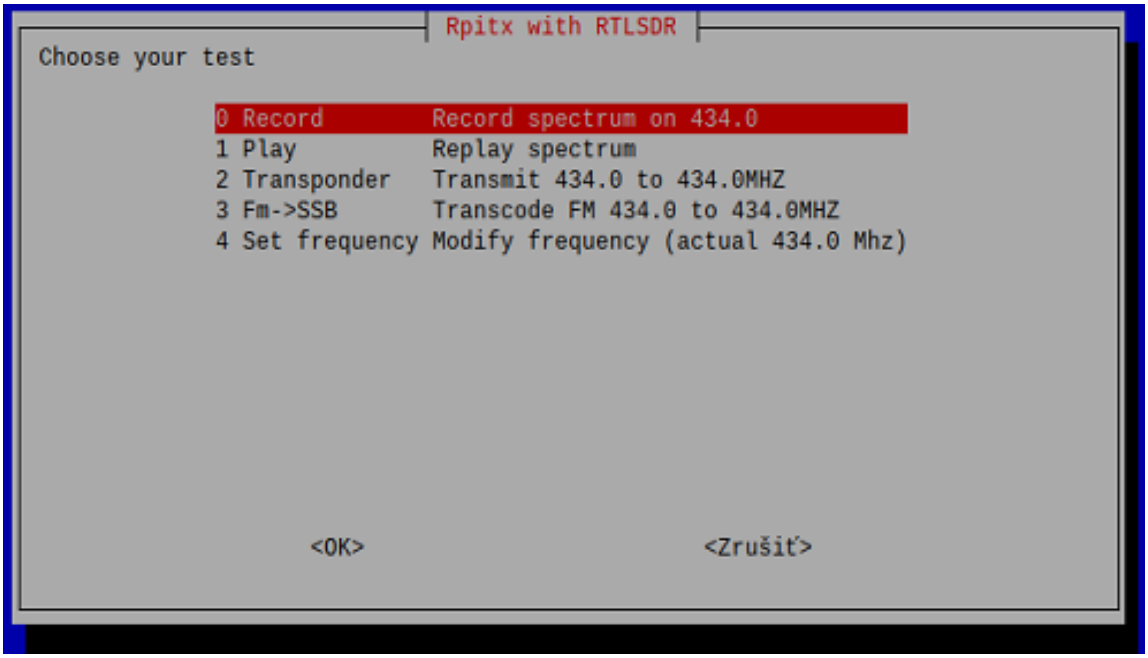


Obrázok 20 Rozdiel zachytených signálov [zdroj: vlastný]

8 INŠTALÁCIA RPITX

Proces inštalácie softvéru RPITX do počítača Raspberry Pi je bezproblémový a nekomplikovaný. Tento softvér je kompatibilný s operačným systémom RaspberryOS, ktorý je známy svojim používateľsky prívetivým rozhraním. Systém poskytuje vizuálne intuitívne a prehľadné prostredie. Po inštalácii operačného systému a zapnutí počítača Raspberry Pi sa inštalácia softvéru RPITX začína zadaním príkazu „git clone https://github.com/F5OEO/rpitx“ do terminálu. Tento softvér bol inštalovaný z tohto zdroja, kvôli tomu, že zabezpečuje inštaláciu najnovšej verzie so všetkými opravami a vylepšeniami priamo od vývojárov.

Po prvom spustení softvéru RPITX sa používateľom okamžite zobrazí výzva, ktorá im umožní prispôsobiť svoje preferencie týkajúce sa zachytávania a prenosu primárnej frekvencie. Je potrebné poznamenať, že v rámci vykonávania meraní je určená primárna frekvencia pre testovacie systémy nastavená na 433 MHz. Táto špecifická frekvencia bola zvolená preto, že zabezpečuje optimálnu kompatibilitu a synchronizáciu medzi všetkými experimentálnymi zariadeniami.



Obrázok 21 Výberové menu softvéru RPITX [zdroj: vlastné]

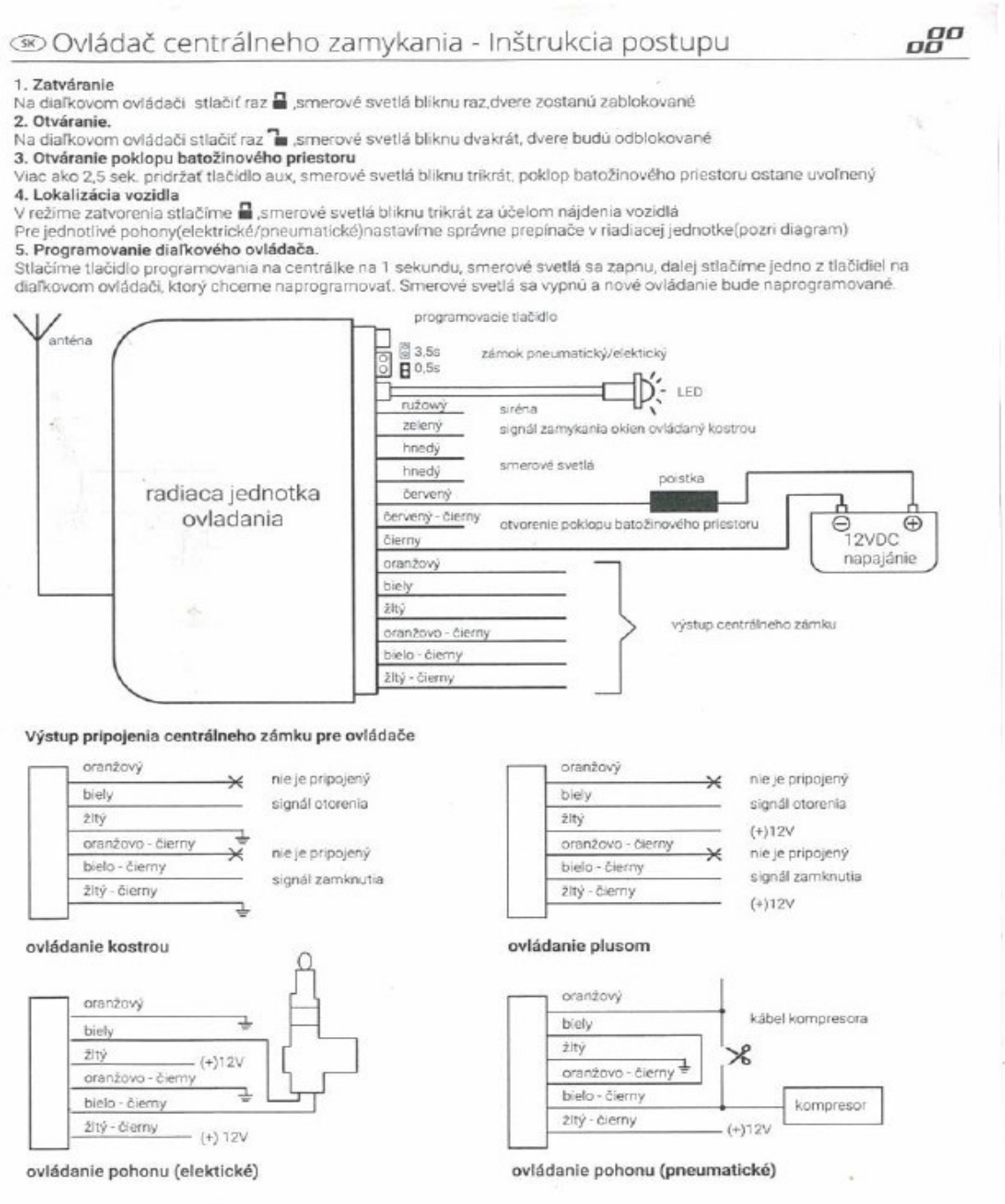
Strategické vylepšenie bolo vykonané s cieľom rozšíriť rozsah zachytávania signálov na čo slúži vybavenia počítača Raspberry Pi so softvérovo definovaným rádiom SDR-RTL dvoma anténami. Táto konfigurácia bola starostlivo zvolená kvôli optimalizácií príjmu a vysielania signálov. Pridanie dvoch antén umožňuje Raspberry Pi efektívne prijímať a vysielať signály v rozšírenom rozsahu, umožňuje tiež systému využiť priestorovú diverzitu a prekonať

potenciálne prekážky alebo rušenia signálu. Vďaka strategicky umiestneným anténam môže Raspberry Pi prijímať signály zo širšieho rozsahu zdrojov a zachytávať slabé alebo vzdialené signály, ktoré by inak boli mimo dosahu. Toto zlepšenie príjmu a prenosu signálov zabezpečuje komplexnejší a robustnejší proces získavania údajov, čo umožňuje hlbšie pochopenie a analýzu signálov v rámci ich analýzy a výskumu.

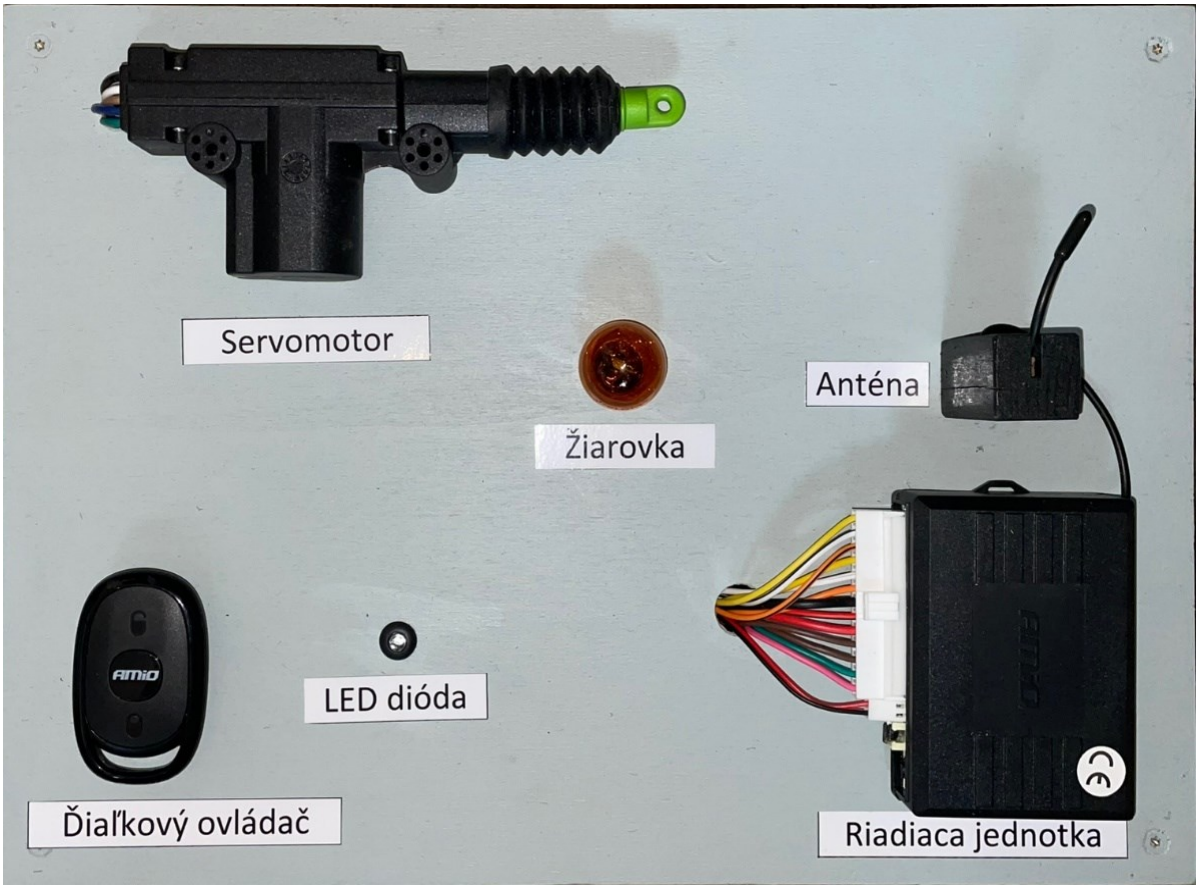
Obrázok 22 Sada na replay attack [zdroj: vlastný]

9 ZAPOJENE CENTRÁLNÉHO ZAMYKACIEHO SYSTÉMU

Systém centrálneho zamykania bol aktivovaný podľa presných pokynov výrobcu, čím sa zabezpečila jeho správna inštalácia vo vozidle. Tento konkrétny model centrálneho zamykania je vybavený jedným elektrickým ťahovým motorom zámku a sprievodnou žltou žiarovkou. Na zabezpečenie správneho fungovania systému je nevyhnutné spoľahlivé napájanie. V tomto prípade sa na zabezpečenie potrebného elektrického napájania systému centrálneho zamykania používa 12 voltový sieťový adaptér. Tento adaptér je špeciálne navrhnutý tak, aby spĺňal požiadavky na napätie systému, čím sa zabezpečí stabilný a stály zdroj energie. Prítomnosť jedného elektrického ťahového motora zámku znamená, že systém centrálneho zamykania funguje prostredníctvom centralizovaného mechanizmu. Po aktivácii tento motor spustí odomykanie alebo zamykanie všetkých dverí súčasne. Jednotný prístup zvyšuje pohodlie a bezpečnosť a umožňuje efektívnu kontrolu prístupu do vozidla. Okrem toho začlenenie žltej žiarovky do systému slúži ako vizuálny indikátor stavu uzamknutia. Keď je systém zapnutý, žiarovka vydáva výrazné oranžové svetlo, ktoré upozorňuje cestujúcich vo vozidle a osoby v okolí na proces zamykania alebo odomykania. Tento vizuálny signál prispieva k bezproblémovému používateľskému zážitku a poskytuje jasnú spätnú väzbu o fungovaní systému. Ak sa pri inštalácii dodržia pokyny výrobcu a ako zdroj napájania sa použije sieťový adaptér s napätím 12 voltov, systém centrálneho zamykania môže spoľahlivo plniť svoj účel. Zabudovanie jedného motora elektrického ťahu zámku a oranžovej žiarovky zvyšuje jeho funkčnosť a užívateľskú prívetivosť. S týmto systémom možno dosiahnuť účinné a bezpečné zamykanie a odomykanie dverí vozidla, čo majiteľovi vozidla môže poskytovať zvýšené pohodlie.



Obrázok 23 Fotokópia návodu [30]



Obrázok 24 Montáž centrálneho zamykania na dosku [zdroj: vlastný]

10 TESTOVANIE ÚTOKU

Fáza testovania zahŕňala nielen laboratórne kontrolované prostredie, aj reálne podmienky, aby sa komplexne posúdili zraniteľnosti a účinnosť systému. V laboratórnych podmienkach sa vykonali hodnotenia s cieľom posúdiť náchylnosť modelov Arduino a centrálneho uzamykacieho systému na potenciálne útoky. Toto prostredie zaručovalo, čo najobjektívnejšie podmienky na zachytávanie signálov, nakoľko nedochádzalo ku rušeniu z okolitých zdrojov, ktoré by mali vplyv na meranie. Reálne podmienky, resp. prostredie mali simulovať miesto, kde dochádza k rušeniu z okolitých vozidiel, iných možných vysielaných signálov a vplyvov počasia. Na dôkladné preskúmanie odolnosti systému sa simulovali rôzne scenáre útokov ako napríklad vzdialenosť zachytávacieho zariadenia, vzdialenosť vozidla od útočníka, vzdialenosť kľúča vozidla od vozidla.

Testovanie bolo rozšírené mimo laboratória na reálne podmienky, pričom zahŕňalo viacerých výrobcov vozidiel. Rovnaké postupy útoku sa zopakovali v rôznych vozidlách, aby sa posúdila výkonnosť systému a identifikovali sa prípadné zraniteľnosti v rôznych modeloch a značkách. Tento prístup zabezpečil komplexné hodnotenie, ktoré zohľadňovalo rozdiely v systémoch vozidiel a implementáciách zabezpečenia.

Počas meraní sa dbalo na to, aby sa čo najpresnejšie replikovali scenáre z reálneho sveta. Na dosiahnutie tohto cieľa sa ako reprezentatívne merania použili vzdialenosti 1, 3, 5 a 10 metrov. Tieto vzdialenosti odrážali typické vzdialenosti medzi hardvérovými zariadeniami a centrálnou jednotkou alebo diaľkovým ovládaním a vozidlom v praktických situáciách, čo uľahčilo presnejšie posúdenie správania a zraniteľnosti systému.

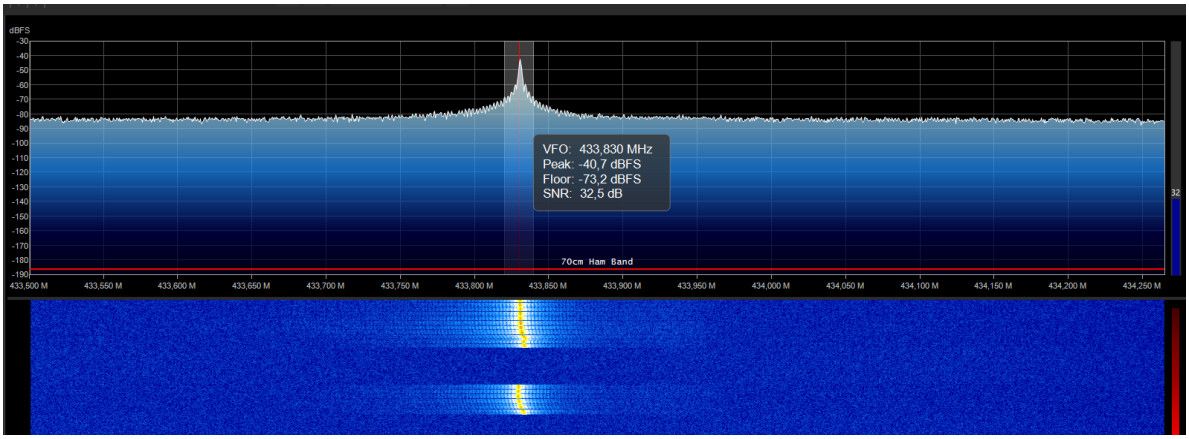
Vykonávaním testov v kontrolovanom laboratórnom prostredí ako aj v reálnych podmienkach bola získaná ucelená predstava o bezpečnosti a správaní systému. Komplexné hodnotenie umožnilo identifikovať potenciálne slabé miesta a náchylnosti v rôznych scenároch a vzdialenostiach.

10.1 Test útoku na Arduino

Zraniteľnosť modelu Arduina bola pôvodne využitá pomocou zariadenia HackRF One, čo umožnilo komplexné posúdenie účinnosti útoku. Uskutočnila sa séria experimentov zahŕňajúcich prehrávanie zachytených signálov na rôzne vzdialenosti. Keď bola vzdialenosť medzi zariadeniami obmedzená na 1 meter, všetky tri pokusy o prehrávanie sa ukázali ako úspešné. S rastúcou vzdialenosťou nad 3 metre však úspešnosť klesala a iba jeden z troch pokusov o

prehrávanie priniesol požadovaný výsledok. Tento pokles účinnosti možno pripísať pozorovanému poklesu intenzity vysielaného signálu počas zachytávania signálu, následkom ktorého bol slabší signál vysielaný počas prehrávania. V dôsledku toho boli útoky na vzdialenosť päť a viac metrov neúčinné, keďže sa nepodarilo zachytiť a prehrať signál s dostatočnou silou. Zariadenie HackRF s obmedzeným dosahom a slabšou konfiguráciou antény preukázalo obmedzenia pri udržiavaní integrity a sily signálu na väčšie vzdialenosti

Okrem uvedeného bola vykonaná porovnávacia analýza pomocou zariadenia Raspberry Pi vybaveného softvérom RPTIX, ktorá poskytla cenné poznatky o vplyve konštrukcie antény na výkon signálu. Zistilo sa, že Raspberry Pi, vybavené samostatnými anténami na príjem a prenos signálu, vykazovalo lepšie výsledky pri zachytávaní a prenose signálu na väčšie vzdialenosti. Tento konštrukčný rozdiel umožnil zvýšenie sily signálu, čo viedlo k vyššej účinnosti a spoľahlivosti prenosu zachyteného signálu z väčších vzdialeností.



Obrázok 25 Zachytenie signálu Arduino [zdroj: vlastný]

Tieto zistenia ako celok zdôrazňujú význam sily signálu a konštrukcie antény pre úspešnosť útokov s prehraním. Zariadenie Raspberry Pi, ktoré využíva dve samostatné všesmerové antény so ziskom 15 dB, čo preukázalo lepšie schopnosti zachytávania a prenosu signálu, čoho výsledkom boli úspešnejšie útoky na väčšie vzdialenosti.

10.2 Test útoku na systém centrálneho zamykania

Útok na uzamykací systém bol navrhnutý tak, aby odrážal predchádzajúci test, ale s kľúčovým rozdielom: nemenila sa len vzdialenosť zachytávacieho zariadenia od vysielaču a prijímaču, ale aj vzdialenosť medzi diaľkovým ovládaním a cieľovým systémom. Tento komplexný experiment zahŕňal celkovo 12 testov po 3 opakovaniach, ktoré boli rovnomerne rozdelené medzi zariadenia HackRF One a Raspberry Pi. Jeho cieľom bolo posúdiť ich účinnosť pri prelomení zabezpečenia uzamykacieho systému.

V rámci každého testu sa uskutočnili tri scenáre, v ktorých vzdialenosť medzi diaľkovým ovládačom a centrálnym uzamykacím systémom ostala konštantná na úrovni 2 metrov, zatiaľ čo vzdialenosťou zachytávacieho hardvéru od systému sa menila v dĺžkach 1, 3 a 5 metrov. Ďalšia séria testov zahŕňala umiestnenie zachytávacieho zariadenia do pevnej vzdialenosti 3 metrov od uzamykacieho systému, zatiaľ čo diaľkové ovládanie bolo umiestnené vo vzdialenosti 3,5 metrov a 10 metrov od systému.

Výsledky týchto experimentov odhalili významné zistenia. Pri použití zariadenia HackRF One v rôznych vzdialenostiach, pri diaľkovom ovládaní v pevnej vzdialenosti 3 metrov, sa všetky testy ukázali ako úspešné a úspešne prelomili vzdialený systém prostredníctvom útokov na opakovanie. Rovnako, keď bolo zariadenie HackRF One fixované v určitej vzdialenosti a diaľkové ovládanie bolo v pohybe, všetky testy priniesli pozitívne výsledky, čo ďalej preukázalo účinnosť zariadenia. Rovnaký prístup sa potom uskutočnil s použitím zariadenia Raspberry Pi, pričom sa uskutočnilo celkovo šesť testov. Je pozoruhodné , že všetkých 6 testov po 3 opakovaniach bolo úspešných pri narušení bezpečnosti uzamykacieho systému, čo ďalej potvrdzuje účinnosť tejto metódy útoku.

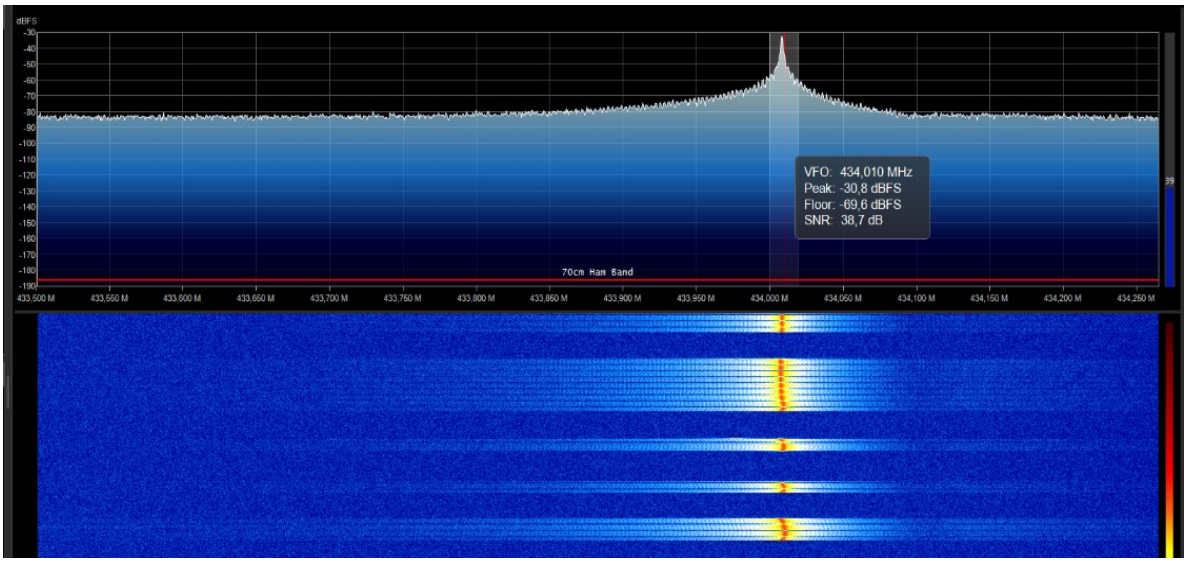
Záverom možno konštatovať, že celkový výsledok tohto komplexného testovania naznačuje dokonalú úspešnosť, pretože všetkých 12 pokusov viedlo k narušeniu uzamykacieho systému. Hoci intenzita signálu vykazovala pri rôznych vzdialenostiach výkyvy, tieto výkyvy nebránili zachyteniu a opakovaniu signálu. Vynikajúci výkon pozorovaný pri týchto testoch možno pravdepodobne pripísať zdokonalenej prijímacej anténe s väčšou dĺžkou na riadiacej jednotke a využitie SAW rezonátoru na diaľkovom ovládači. Tieto faktory významne prispeli k celkovému úspechu testov a zdôraznili význam kvality antény pri zachytávaní a využívaní signálu.

10.3 Útok v reálnych podmienkach

S cieľom kopírovať reálne podmienky sa testovanie uskutočnilo na dvoch rôznych vozidlách patriacich do rovnakej kategórie vozidiel, ktoré boli vyrobené v roku 2009 a 2015. Tieto vozidlá boli vybrané na základe ich približnej nákupnej ceny a boli podrobené testovaniu pomocou zariadení HackRF One a Raspberry Pi. Na vytvorenie realistického prostredia sa experimenty uskutočnili na vnútornom aj vonkajšom parkovisku obchodného centra, konkrétne pri vchode, kde sa maximalizovalo rušenie od okolitých vozidiel a vysielajúcich kľúčov.

Aby sa simulovali reálne scenáre zachytávacie zariadenie bolo umiestnene 5 metrov od vozidla, pričom sa vzdialenosť diaľkového ovládača menila. Počas testov v reálnom prostredí sa dodržiaval špecifický postup, aby sa zabezpečili čo najreálnejšie podmienky. Zachytávacie zariadenie bolo umiestnené vo vzdialenosti 5 metrov od vozidla, pričom vzdialenosť diaľkového ovládaču od vozidla sa menila, aby sa simulovali reálne scenáre.

Keď bol útok HackRF vykonaný na staršie vozidlo z dvojice, vo vzdialenosti 3 metrov od diaľkového ovládania, tento sa ukázal ako úspešný aj po viacnásobnom opakovaní. Pri vzdialenosti 5 metrov boli 2 z 3 opakovaní úspešné, a dôsledku rušenia signálu blízkeho vozidla iba jeden pokus bol neúspešný. Toto rušenie nemalo vplyv na správne fungovanie uzamykacieho systému vozidla, ale jeho následkom boli chyby pri zachytávaní signálu. Na vzdialenosť 10 metrov bol útok neúspešný. Pri použití zariadenia Raspberry Pi sa úspešné pokusy uskutočnili vo vzdialenosti 3 a 5 metrov, a to aj v prípade, keď dochádzalo ku zamykaniu blízkeho vozidla. Na vzdialenosť 10 metrov sa však napriek niekoľkonásobnému opakovaniu pokusy ukázali ako neúspešné

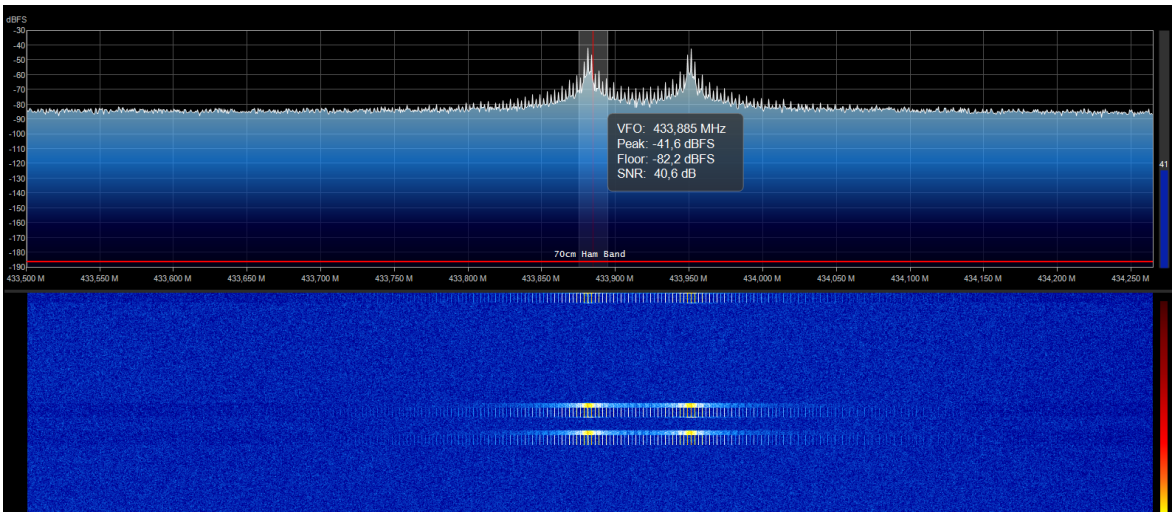


Obrázok 26 Signál staršieho vozidla [zdroj: vlastný]

V prípade vozidla z roku 2015 boli všetky pokusy neúspešné. Toto konkrétne vozidlo využívalo pokročilú technológiu, ktorá sa účinne bránila proti týmto typom útokov pomocou plávajúceho kódu. Obrázok 27 ilustruje, že auto vysiela na jednej hlavnej frekvencií a pod frekvencií súčasne, kde dochádza k prenosu príkazu na odomknutie a taktiež hodnotu počítadla vysielanej kľúčom, ktorá sa porovnáva s hodnotou počítadla očakávanej vozidlom. S ohľadom na toto zistenie sa uskutočnili ďalšie pokusy s použitím techník rušenia signálu,

pri ktorých sa narušilo ovládanie vozidla tým, že sa vynechal jeden kód, po ktorom nasledoval pokus o zachytenie nasledujúceho kódu. Tieto pokusy boli tiež neúspešné.

Na základe testovania vykonaného v reálnych podmienkach bol vyvodený záver, že útoky na prekonanie kódu sú použiteľné na staršie vozidlá vybavené jednoduchšími uzamykacími systémami v dosahu do 5 metrov od kľúča vozidla. Dostupné hardvérové zariadenia použité pri experimentoch však nedokázali prelomiť uzamykacie systémy využívajúce plávajúce kódy, aké sa nachádzajú vo vozidle z roku 2015.



Obrázok 27 Signál novšieho vozidla [zdroj: vlastný]

10.4 Vyhodnotenie všetkých útokov

Všetky výsledky útokov na rôzne systémy boli, kvôli prehľadnosti uvedene v nasledujúcich tabuľkách, kde písmenu U znamená, že útok bol úspešný a naopak písmeno X, že útok bol neúspešný. Tabuľka 1 obsahuje úspešnosť útokov na model centrálneho zamykania zostrojeného pomocou Arduina. Pri útoku na toto zariadene sa ukázala sada na replay attack s Raspberry Pi a RPITX softvérom ako výbornou voľbou, nakoľko všetky útoky boli úspešné. Pri vykonávaní útokov na centrálny zamykací systém, ktoré sú popísané v Tabuľka 2 a Tabuľka 3, boli všetky útoky pomocou HackRF One a Raspberry Pi úspešné bez ohľadu na to, či sa menila vzdialenosť zachytavacích zariadení od centrálneho zamykacieho systému alebo vzdialenosť diaľkového ovládaču. Pokusy o prelomenie zabezpečenia 2 vozidiel v reálnych podmienkach prinieslo dva závery. Zabezpečenie staršieho vozidla sa poradilo odomknúť na vzdialenosť do 5 metrov, čo ukazuje Tabuľka 4. Pri väčších vzdialenostiach boli tieto pokusy neúspešne, rovnako ako prelomenie zabezpečenia modernejšieho vozidla, nakoľko disponovalo obranou proti tomu typu útoku.

Tabuľka 1 Sumarizácia útokov na model Arduino

HackRF One									Raspberry Pi								
1 m			3 m			5 m			1 m			3 m			5 m		
1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
U	U	U	X	U	X	X	X	X	U	U	U	U	U	U	U	U	U

Tabuľka 2 Sumarizácia útokov na centrálne zamykanie v konštantnej vzdialenosti

Diaľkové ovládanie a RJ zamykania vo vzdialenosti 2 metre																	
HackRF One									Raspberry Pi								
1 m			3 m			5 m			1 m			3 m			5 m		
1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Tabuľka 3 Sumarizácia útokov s rôznou vzdialenosťou ovládača

HackRF a Raspberry Pi vzdialenosti 3 metre																	
HackRF One									Raspberry Pi								
3 m			5 m			10 m			3 m			5 m			10 m		
1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Tabuľka 4 Sumarizácia útokov na vozidlo z roku 2009

Vozidlo z roku 2009																		
HackRF One									Raspberry Pi									
3 m			5 m			10 m			3 m			5 m			10 m		
1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
U	U	U	U	X	U	X	X	X	U	U	U	U	U	U	X	X	X

Tabuľka 5 Sumarizácia útokov na vozidlo z roku 2015

Vozidlo z roku 2015																		
HackRF One									Raspberry Pi									
3 m			5 m			10 m			3 m			5 m			10 m		
1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.	1.	2.	3.
X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

11 IDENTIFIKÁCIA VOZIDIEL POMOCOU VYSIELANÉHO SIGNÁLU

Jedným z cieľov tejto bakalárskej práce bolo preskúmať možnosti identifikácie vozidiel prostredníctvom analýzy ich vysielaných signálov. Posledné vykonané meranie sa zameralo najmä na identifikáciu vozidiel na základe ich vysielaného signálu. Na dosiahnutie tohto cieľa bolo starostlivo vybraných 5 vozidiel, aby sa zabezpečilo, že budú mať rovnaké parametre akými sú výrobca, model, rok výroby a úroveň výbavy. Skúmaním získaných meraní sa zistil významný poznatok. Obrázok 28 zobrazuje vyfiltrovanú zhodu signálu 5 vybraných vozidiel, ktorá zobrazuje postupnosť jednotlivých vysielaných bitov. Vozidlá tohto konkrétneho výrobcu inicializujú svoj prenos zreteľnou sekvenciou jednotiek a núl, konkrétne v poradí 1010 vyznačené žltou farbou. Ďalej bolo zistené, že sa zhodujú aj v ďalšej prenášanej postupnosti bitov a to konkrétne v riadkoch začínajúcich 0000 vyznačených zelenou farbou.

Počas fázy zberu údajov boli signály zachytené na verejnom parkovisku, ktoré sa nachádza pred rušným nákupným centrom. Toto prostredie poskytlo príležitosť na vyhodnotenie účinnosti procesu identifikácie. Je zaujímavé, že prostredníctvom vysielaných signálov bolo možné úspešne identifikovať vozidlá toho istého modelu a výrobcu. Tento výsledok ďalej posilnil hypotézu, že analýzou vzorov signálov možno účinne rozlíšiť vozidlá v rámci tej istej kategórie. Následné skúmanie identifikácie podobných znakov u vozidiel iného výrobcu však predstavovalo ďalšie výzvy. Najmä najpopulárnejší český a slovenský výrobca automobilov vykazoval početné varianty výbavy, a to aj v rámci toho istého modelu. Vysielané signály vozidiel sa okrem toho líšili v závislosti od konkrétneho trhu, pre ktorý boli pôvodne určené a neskôr dovezené do krajiny.

Na dosiahnutie presnejšieho a komplexnejšieho systému identifikácie vozidiel sa ukázalo, že jednotný zber údajov zahŕňajúci všetky možné značky a modely automobilov je nevyhnutný. Takýto komplexný súbor údajov by výskumníkom umožnil porovnávať výsledky a identifikovať identické znaky v rôznych vozidlách. Tento jednotný prístup k zberu údajov je potrebný i vzhľadom na prirodzenú zložitosť vyplývajúcu z množstva stupníc výbavy ponúkaných výrobcami a z rozdielov vo vysielaných signáloch na základe rôznych trhových špecifikácií. Pre cieľ presnej identifikácie vozidla je preto nevyhnutné vytvoriť komplexnú databázu, ktorá by zahŕňala rôzne modely vozidiel a s nimi súvisiace vzory signálov.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1												1	0	1	0	1	0	1
2					0	0	0	0	0	0	0	1	0	1	0	1	0	1
3					0	0	0	0	0	0	0	1	0	1	0	1	0	1
4					0	0	0	0	0	0	0	1	0	1	0	1	0	1
5					0	0	0	0	0	0	0	1	0	1	0	1	0	1
6					0	0	0	0	0	0	0	1	0	1	0	1	0	1
7												1	0	1	0	1	0	1
8					0	0	0	0	0	0	0	1	0	1	0	1	0	1
9					0	0	0	0	0	0	0	1	0	1	0	1	0	1
10					0	0	0	0	0	0	0	1	0	1	0	1	0	1
11					0	0	0	0	0	0	0	1	0	1	0	1	0	1
12					0	0	0	0	0	0	0	1	0	1	0	1	0	1
13										0	0	1	0	1	0	1	0	1
14					0	0	0	0	0	0	0	1	0	1	0	1	0	1
15					0	0	0	0	0	0	0	1	0	1	0	1	0	1
16					0	0	0	0	0	0	0	1	0	1	0	1	0	1
17					0	0	0	0	0	0	0	1	0	1	0	1	0	1
18					0	0	0	0	0	0	0	1	0	1	0	1	0	1
19												1	0	1	0	1	0	1
20					0	0	0	0	0	0	0	1	0	1	0	1	1	0
21					0	0	0	0	0	0	0	1	0	1	0	1	0	1
22					0	0	0	0	0	0	0	1	0	1	0	1	0	1
23					0	0	0	0	0	0	0	1	0	1	0	1	0	1
24					0	0	0	0	0	0	0	1	0	1	0	1	0	1
25												1	0	1	0	1	0	1
26					0	0	0	0	0	0	0	1	0	1	0	1	0	0
27					0	0	0	0	0	0	0	1	0	1	0	1	0	1

Obrázok 28 Zhody vo vysielanom signály [zdroj: vlastný]

ZÁVER

Rýchly technologický pokrok spôsobil revolúciu v automobilovom priemysle a priniesol množstvo inovácií, ktoré zlepšujú každodenné používanie automobilov. Jednou z významných oblastí vývoja je elektronické zabezpečenie bezdrôtových systémov motorových vozidiel. Cieľom tejto bakalárskej práce bolo preskúmať a objasniť systémy používané pri zabezpečení vozidiel, poukázať na ich fungovanie, výhody a najmä nevýhody spolu s možnými zlepšeniami, ktoré umožňujú moderné technológie. Práca sa zaoberá vývojom zabezpečenia motorových vozidiel za posledné 3 dekády. Skúmaním rôznych bezpečnostných systémov používaných vo vozidlách sa tento výskum zameriava na objasnenie ich charakteristík a zraniteľností. Je dôležité zdôrazniť, že táto práca nemá slúžiť ako inšpirácia alebo návod na prekonanie bezpečnostných systémov vozidiel. Jej cieľom je skôr poskytnúť prehľad historických a súčasných bezpečnostných systémov, ich nedokonalostí a možností ich zneužitia.

Značná časť práce sa zameriava na analýzu rôznych kategórií zabezpečovacích systémov s dôrazom na ich silné a slabé stránky. Okrem toho výskum poukazuje na rôzne typy útokov, ktorým môžu tieto systémy čeliť. Prezentovaním tohto komplexného chápania bezpečnostných systémov aj potenciálnych útokov má táto práca za cieľ poskytnúť cenné poznatky o celkovom bezpečnostnom prostredí.

Z priebehu štúdie je zrejmé, že neexistuje dokonalý systém zabezpečenia vozidiel. Bez ohľadu na pokrok dosiahnutý v oblasti elektronického zabezpečenia stále existuje možnosť prelomenia týchto systémov. Úspech útoku závisí od rôznych faktorov vrátane vybavenia, prístupu a úrovne zručností narušiteľa. Preto je nevyhnutné preskúmať komplexné bezpečnostné stratégie, ktoré zahŕňajú elektronické aj mechanické prvky. Záverom bakalárskej práce je zdôraznenie komplexnej povahy zabezpečenia bezdrôtových systémov motorových vozidiel. Snaha o dosiahnutie absolútnej bezpečnosti je náročná úloha vzhľadom na neustále sa vyvíjajúcu povahu útokov a vynaliezavosť potenciálnych narušiteľov.

ZOZNAM POUŽITEJ LITERATÚRY

[1] Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems [online]. 1. Austin: USENIX Security, 2016 [cit. 2022-11-19]. ISBN 978-1-931971-32-4. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

[2] Where Things Fall Apart: Protocols (Part 2 of 2). Menu A Few Thoughts on Cryptographic Engineering [online]. Baltimore [cit. 2022-11-19]. Dostupné z: https://blog.cryptographyengineering.com/2011/09/24/where-things-fall-apart-protocols-part/

[3] Security Analysis of a Cryptographically-Enabled RFID Device [online]. 1. Austin: USENIX Security, 2005 [cit. 2022-11-19]. ISBN 978-1-931971-32-4. Dostupné z: https://www.usenix.org/legacy/events/sec05/tech/bono/bono.pdf

[4] Gone in 360 Seconds: Hijacking with Hitag2 [online]. 2015 [cit. 2022-11-19]. Dostupné z: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final95.pdf

[5] Commission Directive 95/56/EC, Euratom of 8 November 1995 adapting to technical progress Council Directive 74/61/EEC relating to devices to prevent the unauthorized use of motor vehicles. EUR-Lex [online]. Štrasburg: Európsky parlament, 1995 [cit. 2022-11-19]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0056

[6] RICHARDSON, Anna. SECURITY OF VEHICLE KEY FOBS AND IMMOBILIZERS [online]. London. [cit. 2022-12-14]. Dostupné z: https://www.cs.tufts.edu/comp/116/archive/fall2015/arichardson.pdf

[7] PASSIVE ENTRY PASSIVE START SYSTEM [online]. Francúzko: Valeo, 2017 [cit. 2022-11-19]. Dostupné z: https://www.valeo.com/en/passive-entry-passive-start-system/

[8] Key Fob patent. In: Apple World Today [online]. 2022 [cit. 2022-11-19]. Dostupné z: https://appleworld.today/wp-content/uploads/2022/06/Key-Fob-patent.jpg

[9] ALRABADY, A.I. a S.M. MAHMUD. Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs. IEEE Transactions on Vehicular Technology [online]. 2005, 54(1), 41-50 [cit. 2022-11-28]. ISSN 0018-9545. Dostupné z: doi:10.1109/TVT.2004.838829.

[10] COLLINS, Travis F., Robin GETZ, Di PU a Alexander M. WYGLINSKI. Software-Defined Radio for Engineers. USA. Artech House Publishers, 2018. ISBN 9781630814571

[11] FETTE, Bruce. Cognitive Radio Technology [online]. 1. USA: Elsevier, 2006 [cit. 2022-12-14]. ISBN 9780750679527. Dostupné z: https://omidi.iut.ac.ir/SDR/2007/WebPages/07_CognitiveRadio/references/ebook/Fette%20B.A.(ed)%20Cognitive%20Radio%20Technology.pdf

[12] INSTALLFEST. Softwarově definované rádio (Jan Hrach) [online] [cit. 2019-04-08]. Dostupné z: https://www.youtube.com/watch?v=i1ZB70nPFg.

[13] PELGROM, Marcel J.M. Analog-to-Digital Conversion. Luxembursko: Springer Science+Business Media, 2010. ISBN 978-90-481-8887-1.

[14] Principles of Data Acquisition and Conversion [online]. USA: Texax Instruments, 2015 [cit. 2022-12-14]. Dostupné z: https://www.ti.com/lit/an/sbaa051a/sbaa051a.pdf

[15] MIHALÍK, Ján a Iveta GLADIŠOVÁ. MODULOVANÉ SIGNÁLY [online]. Košiče: Technická univerzita v Košiciach [cit. 2022-12-14]. ISBN 9788055324425. Dostupné z: https://ldipv.fei.tuke.sk/publications/books/Gladisova_Mihalik_Modulovane%20signaly_LDIPV.pdf

[16] AQUEEL, Atifa. UNIT-4 DIGITAL MODULATION TECHNIQUES [online]. 2020 [cit. 2022-12-14]. Dostupné z: https://old.amu.ac.in/emp/studym/100009218.pdf

[17] Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex). GeeksforGeeks [online]. Uttarpradéš: GeeksforGeeks, 2022 [cit. 2022-12-14]. Dostupné z: https://www.geeksforgeeks.org/transmission-modes-computer-networks/

[18] KOLODZIEJ, Kenneth E. In-Band Full-Duplex Wireless Systems Handbook. Norwood: Artech House, 2021. ISBN 978-1-63081-789-3.

[19] ROMAN, PAOLO. The big book of SDRsharp v5.3 [online]. 5. USA: AIRSPY, 2022. Dostupné také z: https://airspy.com/downloads/SDRSharp_Big_Book_v5.3.pdf Medzera

[20] About GNU Radio. GNU Radio [online]. GNU Radio project, 2022 [cit. 2022-12-14]. Dostupné z: https://www.gnuradio.org/about/

[21] Universal Radio Hacker [online]. 2020, (1.1) [cit. 2022-12-14]. Dostupné z: https://www.oldergeeks.com/downloads/files/userguide.pdf

[22] LAUFER, Carl. The Hobbyist's Guide to the RTL-SDR_ Really Cheap Software Defined Radio. USA, 2015. Dostupné také z: https://www.surviveuk.com/wp-content/uploads/2016/07/The-Hobbyists-Guide-To-RTL-SDR-Carl-Laufer.pdf

[23] Https://hackrf.readthedocs.io/en/latest/index.html. HackRF [online]. USA: Great Scott Gadgets, 2021 [cit. 2022-12-14]. Dostupné z: https://hackrf.readthedocs.io/en/latest/index.html

[24] Rpitx. GitHub [online]. USA: GitHub, 2018 [cit. 2022-12-14]. Dostupné z: https://github.com/F5OEO/rpitx

[25] DUARTE GARCÍA, Jorge. Software Defined Radio for Wi-Fi Jamming [online]. 2016 [cit. 2022-11-19]. Dostupné z DOI: 10.13140/RG.2.2. 23772.90240

[26] Car hacking tutorial: Replay attack /w SDR. Hardware hacking tutorials [online]. Záhreb, 2017 [cit. 2022-11-19]. Dostupné z: https://ivanorsolic.github.io/post/car-hacking/

[27] Keyless car theft: What is a relay attack, how can you prevent it, and will your car insurance cover it?. Leasing.com [online]. Stockport: Leasing.com Group, 2021 [cit. 2022-11-19]. Dostupné z: https://leasing.com/guides/relay-car-theft-what-is-it-and-how-can-you-avoid-it/

[28] Relay car theft. In: Leasing.com [online]. Stockport: Leasing.com Group, 2021 [cit. 2022-11-19]. Dostupné z: https://cdn.leasing.com/cms/relay-car-theft_3.jpg

[29] A hacker made a $30 gadget that can unlock many cars that have keyless entry. Business Insider [online]. 2015, Aug. 6, 2015 [cit. 2022-11-19]. Dostupné z https://www.businessinsider.com/samy-kamkar-keyless-entry-car-hack-2015-8

[30] Keyless entry system KE14 model. AMiO [online]. Poland: AMiO Sp. z o.o., 2023 [cit. 2023-05-21]. Dostupné z: https://amio.pl/en/keyless-entry-system-ke14-model/3-12-910

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

dB	decibel
DST 40	Digital Siganautre Transponder 40
A/D	Analógovo-digitálny
ASK	Amplitude - Shift Keying
D/A	Digitálno-analógový
DSP	Digital Signal Processor
FSK	Frequency - Keying
kHz	Kilohertz
MHz	Megahertz
PEKS	Passive Keyless Entry and Start
PSK	Phase - Shift Keying
RFID	Radio Frequency IDentification
RKE	Remote Keyless Entry
RTL	Realtek Limited
SAW	Surface Acoustic Wave
SDR	Softvérovo Definované Rádio
UHR	Universal Radio Hacker
USB	Universal Serial Bus

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK