

**VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH
STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE**

BAKALÁŘSKÁ PRÁCE

**Elektronické zabezpečení vozidel a jeho
využití v kriminalistické praxi**

Autor práce: por. Martin Rychetský, DiS

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.

Katedra: Katedra právních oborů a bezpečnostních studií

2025

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Martin Rychetský

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Místo studia: Příbram

**Název bakalářské práce: Elektronické zabezpečení vozidel a jeho využití v
kriminalistické praxi**

**Název bakalářské práce v anglickém jazyce: Electronic Vehicle Security and its
Use in Criminalistics Practice**

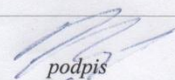
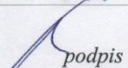
Katedra: Katedra právních oborů a bezpečnostních studií

Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

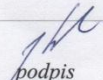
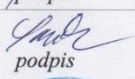
Datum zadání bakalářské práce: říjen, 2024 – listopad, 2024

Cíl bakalářské práce:

Cílem této práce je zhodnocení jednotlivých druhů elektronického zabezpečení vozidel, jejich možnosti, slabiny a volba nejvhodnějšího typu zabezpečení jako prevence před krádežemi vozidel a věcí z vozidel.

Student: Martin Rychetský	3.11.2024 datum	 podpis
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.	9.11.2024 datum	 podpis

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	2.12.2024 datum	 podpis
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9.12.2024 datum	 podpis
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10.12.2024 datum	 podpis



Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucímu bakalářské práce JUDr. Milanovi Kocíkovi, MBA, LL.M.
za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

RYCHETSKÝ, M. *Elektronické zabezpečení vozidel a jeho využití v kriminalistické praxi: bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 65 s.

Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Klíčová slova: elektronické zabezpečení, krádeže vozidel, eCall, vyhledávání

Tématem této bakalářské práce je elektronické zabezpečení vozidel, rozebírá jednotlivé druhy, zjišťuje jejich slabiny a možnosti překonání a zobrazuje jejich využití v kriminalistické praxi

V úvodní části je vysvětlen pojem krádeže motorových vozidel, je zde zmíněna také jejich statistika, způsoby, ale také jaká byla historie krádeží vozidel od té historicky první až po současnost. Dále jsou popisovány příklady elektronického zabezpečení. V návaznosti na tuto kapitolu budou představeny také možnosti a prostředky k překonání zabezpečení vozidel a také dva příklady z praxe, kdy byly zabezpečovací systémy využity v kriminalistické praxi.

Hlavní náplní práce je seznámení s možnými riziky v souvislosti s krádeží motorového vozidla a poskytnutí možných řešení k jeho zabezpečení.

ABSTRACT

RYCHETSKÝ, M. Electronic Vehicle Security an its Use in Criminalistics Practice: Bachelor Thesis. České Budějovice: The College of European an Regional Studies, 2025. 65 pgs.

Supervisor: JUDr. Milan Kocík, MBA, LL.M.

Key words: electronic security, vehicle theft, eCall, search

The topic of this bachelor's work is electronic vehicle security, analyzes the different types, identifies their weaknesses and possibilities of overcoming them, and shows their use in criminalistic practice.

In the introductory part, the concept of motor vehicle theft is explained, statistics, methods, as well as the history of vehicle theft from the historical first to the present are also mentioned. Examples of electronic security are described below. Following this charter, it will be also introduce the ways and means of overcoming vehicle security and two practical examples where security systems have been used in criminal practice.

The main focus of the work is to familiarize with possible risks related to vehicle theft and provide possible solutions to secure it.

Obsah

Úvod.....	9
1 Cíl a metodika bakalářské práce	10
2 Historie krádeží motorových vozidel	11
3 Krádeže motorových vozidel	13
3.1 Stručná charakteristika krádeží motorových vozidel	13
3.2 Statistika krádeží motorových vozidel	14
3.3 Způsoby krádeží motorových vozidel	17
4 Legislativa k pátrání po vozidlech	20
5 Elektronické zabezpečení vozidel	22
5.1 Elektronické zabezpečení vozidel instalované výrobcí vozidel	22
5.1.1 Centrální zamykání	22
5.1.2 Imobilizér	27
5.1.3 Alarm.....	29
5.1.4 GPS sledovací systémy	30
5.1.5 Systém eCall.....	31
5.1.6 Bezpečnostní kamery	34
5.2 Dodatečně instalované elektronické zabezpečení vozidla.....	35
5.2.1 Systém Sherlog security	35
5.2.2 Tajný spínač	36
5.2.3 eCall	37
5.2.4 Air Tag	38
6 Příklady nálezu odcizených vozidel v praxi.....	40
6.1 Za použití systému eCall	40
6.2 Za použití systému Sherlog	42
7 Zařízení užívané k překonání elektronického zabezpečení.....	43
7.1 Flipper Zero	43

7.2	Pandora	45
7.3	Radiostanice Baofeng.....	46
7.4	Výkonná rušička signálu	48
8	Rušičky a legislativa	49
9	Zjištění informovanosti veřejnosti v oblasti zabezpečení vozidel	50
9.1	Cíl zkoumání	50
9.2	Stanovení otázek dotazníku.....	50
9.3	Vyhodnocení odpovědí na jednotlivé otázky	52
9.4	Vyhodnocení hypotéz.....	56
9.5	Výsledek zkoumání	56
	Závěr	57
	Seznam použitých zdrojů	59
	Seznam zkratk	63
	Seznam obrázků	64
	Seznam grafů.....	65

Úvod

Vzhledem ke služebnímu zařazení autora na 8. oddělení obecné kriminality služby kriminální policie a vyšetřování obvodního ředitelství policie Praha I, které se zabývá primárně kriminalitou na úseku krádeží motorových vozidel, je tématem bakalářské práce právě elektronické zabezpečení vozidel proti krádeži a jeho využití v kriminalistické praxi. Volba tématu práce je úzce spjata s praxeologickými zkušenostmi autora, jenž se touto problematikou zabývá již řadu let v rámci prověřování krádeží automobilů. Přínosem této práce bude prohloubení znalostí v oblasti zabezpečení motorových vozidel, zhodnocení jednotlivých druhů elektronického zabezpečení, zjištění možností, nedostatků a způsobů jejich překonání a následná aplikace v kriminalistické praxi.

Cílem této bakalářské práce rozhodně není poskytnutí návodu, jak se zmocnit motorového vozidla, ani zřízení si neoprávněného vstupu do něj nebo obdobné trestné činnosti. Jejím cílem je zmínění statistiky a historie krádeží motorových vozidel, způsobů zabezpečení, jejich rozdělení, funkce a principy, zhodnocení slabin a případná prevence před krádeží motorových vozidel. Snahou autora je také doporučení nejvhodnějšího druhu zabezpečení, případně jeho kombinace. Práce je doplněna o rozbor ukázkových případů z praxe, kdy za použití různého elektronického zabezpečení došlo k nálezu a následnému zajištění odcizeného vozidla. Práce se také věnuje legislativním normám, na základě nichž lze provádět pátrání po vozidlech. Na závěr je uvedeno doposud nejspolehlivější zabezpečení vozidla.

1 Cíl a metodika bakalářské práce

Hlavním cílem této bakalářské práce je analýza jednotlivých druhů elektronického zabezpečení vozidel, jejich možnosti, slabiny, způsoby překonání a volba nejvhodnějšího typu zabezpečení jako prevence před krádežemi vozidel a věcí z vozidel.

První kapitola teoretické části práce, která byla zpracována výzkumnou metodou popisnou, obsahuje cíl a metodiku bakalářské práce, ve druhé kapitole je vysvětlení základního pojmu krádeže, způsoby jejího provedení, statistický vývoj krádeží motorových vozidel na území České republiky a pohled do historie krádeží vozidel. Další kapitola je věnována elektronickému zabezpečení vozidel, ta je následně rozdělena na dvě podkapitoly, v nichž jsou uvedeny jednotlivé druhy elektronického zabezpečení vozidel rozdělené dle instalace výrobcem vozidel nebo dodatečné instalace. Čtvrtá kapitola je věnována kazuistice, kdy jsou zmíněny dva případy z praxe, kdy došlo k nálezů odcizeného vozidla za využití různých druhů elektronického zabezpečení. V páté kapitole teoretické části jsou představena zařízení, která slouží k překonání elektronického zabezpečení vozidel, je zde zmíněn princip, na kterém tato zařízení pracují. Šestá kapitola je věnována legislativě ve vztahu k zařízením fungujícím na principu rušení signálu. Následná kapitola se věnuje legislativě, na jejímž základě lze provádět pátrání po vozidlech.

V praktické části je použita výzkumná metoda kvantitativního průzkumného dotazníkového šetření, je zde provedena analýza informovanosti v oblasti zabezpečení vozidel, kde je autor toho názoru, že většina respondentů nemá dostatečné znalosti v oblasti zabezpečení vozidel. Součástí této praktické části je i shrnutí a vyhodnocení tohoto průzkumu, čímž bude naplněn vedlejší cíl této bakalářské práce.

2 Historie krádeží motorových vozidel

Ve světě je historicky první nahlášená krádež automobilu datována k červnu roku 1896, ta se odehrála ve Francouzském hlavním městě Paříži. Vozidlo značky Peugeot tehdy odcizil mechanik, ke kterému si své vozidlo dal opravit holandsko-belgický bankéř, zakládajícím členem Automobile Club de France, později známý jako FIA (Federation Internationale de l'Automobile), pan Baron Étienne van Zuylen van Nyevelt. K jeho velkému štěstí byl vůz nalezen v nedaleké vesnici Asnieres a zloděj chycen. Tento čin přinesl řadu inovací, díky nimž se auta stávala odolnější proti krádeži¹. Tehdy i díky velmi nízkému počtu vyrobených kusů aut a celkové koncepci vozů připomínající spíše kočár neměly vozy ani dveře. Automobily byly navíc příliš ojedinělé a byly výsadou uživatelů z nejvyšších vrstev společnosti.

Jako první technologii proti krádeži automobilu vyvinula společnost Leach Automobile v roce 1900 a byl jí odnímatelný volant. Hlavní myšlenkou bylo, že řidič po jízdě volant sundá a vezme si ho s sebou. V dnešní době už je to celkem úsměvná představa, nicméně toto zabezpečení bylo poplatné tehdejší době.

Počátkem 20. let 20. století byly automobily opatřovány dveřmi, ve kterých byly zámky. Bohužel byly vyráběny jen ve velmi malé sérii a bylo jednoduché je překonat, protože jedním klíčem bylo možné odemknout více zámků. Změna přišla až v 70. letech dvacátého století, kdy byly představeny sofistikovanější zámky².

Největším rozvojem automobilové kriminality bylo zavedení pásové výroby vozidel Henry Fordem v roce 1913. Docházelo k orientaci na široké vrstvy zákazníků a výrobě unifikovaných vozů. Tehdy vyjížděl z výrobní linky každých 10 vteřin nový Ford T v jediném odstínu laku a to černém. Zavedením pásové výroby a průmyslovou expanzí do celého světa došlo k revoluci v oblasti krádeží motorových vozidel. V roce 1925 klesla cena modelu Ford T z původních 825 dolarů na pouhých 300 dolarů. Ta byla pro veřejnost náhle dostupnější, poptávka po nich rostla, stejně jako po dílech, které byly z velké části snadno zaměnitelné³. Tehdy také rostla obliba, zejména na americkém kontinentu, krádeží vozidel za účelem jízdy pro potěšení, tzv. „Joyriding“,

¹ *A Brief History of Car Security Systems*. Online. Dostupné z: <https://www.blackknighttracking.com>. [cit. 2024-08-17]

² *Leach (automobile)*. Online, 2023-09-27. Dostupné z: <https://en.wikipedia.org>. [cit. 2024-08-24]

³ *Ford Model T: Revoluce na čtyřech kolech*. Online. 2024-05-16. Dostupné z: <https://www.venclikovi.cz>. [cit. 2024-08-27]

který byl výsadou dospívajících chlapců za účelem dělání dojmu na děvčata. Vozidla bývala často nalezena nabouraná, bez benzínu nebo shořelá za účelem zahlazení stop. To vedlo ke snaze uvádět na trh první systémy, tehdy pouze mechanického blokování ovládacích prvků. K roku 1913 lze datovat také první vynález alarmu, který vynalezl nejmenovaný denverský vězeň. Princip spočíval v tom, že se alarm spustil, když se někdo pokusil pomocí startovací kliky ručně protočit motor⁴.

⁴ *A Brief History of Car Security Systems*. Online. Dostupné z: <https://www.blackknighttracking.com>. [cit. 2024-08-17]

3 Krádeže motorových vozidel

3.1 Stručná charakteristika krádeží motorových vozidel

Krádeže jsou v dějinách lidstva od nepaměti, hlavním motivem pachatele je zmocnit se hodnotné věci někoho jiného bez vynaložení vlastních prostředků nebo jen s minimem takových prostředků. To je i v dnešní době pro nejednoho člověka lákavé. Automobil nikdy nebyl a není ani dnes úplně levnou záležitostí, což je jedním z hlavních důvodů, proč jsou velmi často terčem trestné činnosti. I přes veškerou snahu vývojářů samotných automobilek v oblasti zabezpečení vozidel, tak i samotných majitelů, kteří svá vozidla opatřují různými druhy jak mechanického, tak elektronického zabezpečení, stávají se motorová vozidla stále oblíbeným terčem zlodějů, ti totiž drží souběžně krok s vývojem zabezpečovacích systémů. Mezi základní preventivní opatření v boji proti krádežím motorových vozidel je jejich zabezpečení a to ve dvou úrovních, jednak proti odcizení a dále pak existence zařízení sloužící k dohledání odcizeného vozidla. Zabezpečovací zařízení lze dělit z několika pohledů. Obecně jsou dělena na pasivní a aktivní zabezpečovací zařízení, která se dále člení na mechanická a elektronická⁵.

Krádež motorového vozidla je považována za závažný trestný čin a je postihována podle zákona. Zákon č. 40/2009 Sb. trestní zákoník⁶ (dále jen trestní zákoník), uvádí v §205, že krádež motorového vozidla je prostou krádeží. Řadí jí mezi majetkové trestné činy a stanoví trestní sazby, které se liší dle různých atributů. Těmi jsou např. hodnota odcizeného vozidla, dle jejíž výše lze skutek kvalifikovat jako přečin nebo zločin. Zda je pachatel trestán za obdobnou trestnou činnost opakovaně nebo zda se jedná o organizovanou skupinu pachatelů. Organizovaná skupina není striktně definována trestním zákoníkem, přestože s ní operuje v mnoha svých ustanoveních, mimo jiné jakožto kvalifikovanou skutkovou podstatu trestného činu krádeže dle § 205/4 písm. a) trestního zákoníku. Obecně se za organizovanou skupinu považuje skupina více (minimálně však tří) osob, páchající závažnou trestnou činnost, které mají jasně rozdělené role, ve kterých se podílejí svým dílem k úspěšnému dosažení

⁵ PORADA, Viktor. *Kriminalistika*. Brno: CERM, 2001. s. 721. ISBN 80-7204-194-0

⁶ JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou : podle stavu k 1.1.2010*. Glosátor. Praha: Leges, 2009. s. 258. ISBN 978-80-87212-22-6.

stanoveného cíle za účelem zisku⁷. Toto se vyznačuje vzájemnou koordinací a plánovitostí, jež zvyšují pravděpodobnost úspěšného dokonání trestného činu⁸. Samotná podstata krádeže spočívá v úmyslném jednání pachatele, kdy si neoprávněně přisvojí cizí věc tím, že se jí zmocní a způsobí tak tímto činem škodu nikoliv nepatrnou⁹. Co je to vlastně autokriminalita a kdo se jí dopouští? Stejně jako ostatní druhy majetkové a jiné kriminality jde o sociálně patologický jev, který vede k narušování pravidel chodu společnosti a způsobuje obětem trestných činů majetkovou škodu, fyzickou a jinou újmu¹⁰.

V případě, kdy ke krádeži již dojde, je nezbytné v co nejkratší době zjistit od oznamovatele co nejpřesnější ucelení informace a základní popis vozidla se všemi identifikátory a identifikačními znaky. Dále zda je vozidlo vybaveno nějakým zabezpečením, zjistit o jaký druh zabezpečení se jedná a zjistit, zda jej lze využít k vypátrání¹¹.

3.2 Statistika krádeží motorových vozidel

Statisticky největší nárůst této trestné činnosti v České republice je datován k počátku devadesátých let. Vliv na to zcela jistě má hromadný rozvoj vozidlového parku co se četnosti, tak i jeho rozmanitosti týká. Došlo také k zásadní změně společenského a politického uspořádání. K expanzi kriminality zcela jistě přispělo také otevření státních hranic a zvýšení pohybu kriminálně závadových osob zejména z oblasti východní Evropy. Počátkem devadesátých let se také zvýšila životní úroveň obyvatel České republiky a otevřela se pomyslná brána zahraničního trhu s automobily. Počet krádeží vozidel měl tak stoupající tendenci až to až do roku 1997, kdy bylo dosaženo nejvyššího množství odcizených vozidel.

⁷ NOŽINA, Miroslav. *Mezinárodní organizovaný zločin v České republice*. Praha: Themis, 2003. s. 16. ISBN 80-731-2018-6

⁸ CHMELÍK, Jan a kolektiv. *Rukověť kriminalistiky*. Plzeň: Aleš Čeněk, 2005. s. 369. ISBN 80-86898-36-9

⁹ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 45. ISBN 978-80-7488-424-5

¹⁰ IBL, Petr. *Kriminologie*. Karlovy Vary: Vysoká škola Karlovy Vary, 2014. s. 12. ISBN 978-80-87236-22-2

¹¹ MUSIL, Jan a kolektiv. *Kriminalistika: vybrané problémy teorie a metodologie*. Praha: Policejní akademie České republiky, 2001. s. 204. ISBN 80-7251-080-0

Jak zobrazuje graf č. 1, v roce 2020 bylo na území České republiky spácháno 3201 krádeží dvoustopých motorových vozidel. V roce 2021 to bylo 2989 krádeží, v roce 2022 vzrostl počet krádeží vozidel na hodnotu 3343, v roce 2023 byl opět zaznamenán pokles na 2976 vozidel a v roce 2024 bylo dosaženo historicky nejnižšího počtu odcizených vozidel na celém našem území od vzniku samostatné České republiky s hodnotou 2793 vozidel¹² a míra objasněnosti překročila velmi slibných 50%, oproti tomu, na počátku milénia se objasněnost pohybovala kolem 15%. Pro zajímavost v roce 1997 bylo na území České republiky odcizeno 29422 dvoustopých vozidel, což je nejvyšší počet v novodobé historii ČR.

Graf 1 Statistika krádeží motorových vozidel na území ČR



Zdroj: vlastní, zpracováno dle mapy kriminality¹¹

Oproti předešlým rokům jde dnes o velmi výrazný pokles zapříčiněný mimo jiné i značným vývojem na úseku zabezpečení motorových vozidel. Svou nezanedbatelnou roli také hraje povinnost každého nového majitele zajistit na STK (Stanice Technické Kontroly) evidenční kontrolu před každou registrací nového vlastníka, v případě dovozu ze zahraničí, též dovozovou technickou kontrolu. Vozidlo tak prochází několika kontrolními mechanismy, kdy je podrobena důkladné kontrole jeho identifikátorů a skrytých znaků, zda nefigurují v mezinárodním registru odcizených vozidel, či zda nedošlo k pozměnění identifikátorů např. přeražením čísla VIN (Vehicle Identification Number)¹³ nebo přenos vevařením části vozu s nepříslušným číslem. Kód VIN je v podstatě rodné číslo vozidla, které si s sebou nese od výroby po celou dobu existence.

¹² POLICIE ČR. *Mapa kriminality*. Online. Dostupné z: <https://kriminalita.policie.cz/>. [cit. 2024-07-01]

¹³ VLK, František. *Anglicko-český technický automobilový slovník*. Auto-moto-profi. Praha: Computer Press, 2001. s. 194. ISBN 80-722-6522-9

Není to však jen číslo, které je vyraženo na nosné části karoserie nebo je s touto pevně a neoddělitelně spojeno, je to důmyslný kód složený ze sedmnácti znaků, obsahující číslíce i písmena. Ukryvá v sobě zemi původu, výrobce, typ vozidla a další informace, díky kterým jsou vyjádřeny individuální vlastnosti vozidla¹⁴. Dále se kontroluje také originalita výrobního štítku, zda je příslušný k danému vozu, zda nejde o falzum nebo nedošlo k jeho tzv. přenesení. Toto opatření v minulosti také přispělo k následnému odhalení kradených vozidel. Většina vozidel je dnes opatřena množstvím skrytých znaků, které poté usnadňují identifikaci daného vozu.

Prověření ojetého vozu nabízí také společnost Cebia, s.r.o., která spolupracuje s pojišťovnami, autorizovanými servisy, leasingovými společnostmi, Policií ČR a dalšími důvěryhodnými zdroji. Svou činností se významně podílí na kultivaci trhu s ojetými vozy. Společnost Cebia je výhradním představitelem systému OCIS (Open Car Information System) v ČR a SR. Tento systém používají partneři Cebia po celém světě jako nástroj pro evidenci a výměnu dat o vozidlech. Zde jsou evidována data o počtu ujetých kilometrů v určitých časových horizontech, týkajících se například provedení evidenční kontroly, technické kontroly včetně měření emisí, dopravní nehoda, škodní událost nahlášená pojišťovně atd. K dispozici jsou i fotografie z těchto událostí, čímž v kombinaci vývojem počtu ujetých kilometrů také eliminuje možnost pořízení odcizeného vozidla¹⁵.

V neposlední řadě je třeba zmínit také aktivnější přístup ze strany Policie ČR, která v rámci bezpečnostních opatření velmi aktivně vyhledává odcizená vozidla, využívá k tomu množství technických prostředků a vybraní pracovníci jsou pravidelně proškolení v otázkách zabezpečení motorových vozidel, zejména v automobilce Škoda Mladá Boleslav a.s. – sekce bezpečnosti. Je zde velký předpoklad, že klesající tendence na úseku krádeží motorových vozidel bude i nadále pokračovat, což je jistě dobrá zpráva pro všechny motoristy. Avšak krádeže v našem světě vždy byly, jsou a jistě i vždy budou.

S rozvojem elektromobility v současné době se ovšem zároveň nabízí opačný předpoklad, a sice nárůst krádeží automobilových součástek, konkrétně elektrobaterií.

¹⁴ RAK, Roman a kol. *Krádeže vozidel: odhalování, vyšetřování a prevence*. Brno: CERM, 2001. s. 88. ISBN 80-7204-218-1

¹⁵ SAIDL, Jan. *Cebia: ověřená historie*. Online. 2024-05-16. Dostupné z: <https://www.autolexicon.net/cs/articles/cebia/>. [cit. 2025-03-04]

S tím je spojena časová náročnost krádeže, neboť taková demontáž elektrických článků není jednoduchou záležitostí. Proto lze předvídat, že pro samotné zloděje bude snazší odcizit celé vozidlo a následnou demontáž provést později ve vlastním zázemí. Tento trend je však z hlediska posuzování kriminality příliš mladý, proto až čas ukáže, jak se bude v budoucnu vyvíjet.

Dle statistik velmi často bývají rizikové konkrétní značky vozidel, což je dáno zejména poptávkou a zastoupením konkrétní značky na trhu. Velká poptávka a silné zastoupení ve vozovém parku, určuje snadný výběr vhodného vozu k odcizení a rychlý odbyt celého vozu nebo jeho částí, u nichž je velmi často znemožněna pozdější identifikace. Statistikám kralují zejména vozy koncernu VW (Volkswagen, Škoda, Audi, Seat). Na území České republiky této statistice neblaze vládne již několik let vůz značky Škoda Octavia. V poslední době je na vzestupu i obliba korejské značky Hyundai, pramenící z nízké pořizovací ceny, rozvoje výrobních závodů na našem území, rostoucí oblibou české motoristické veřejnosti a tedy vysokým zastoupením ve vozovém parku.

Nutno podotknout, že statistiku krádeží motorových vozidel také značně ovlivňují pojistné a leasingové podvody, které se nyní stávají stále častějším jevem. Pro pachatele takového podvodu jde o velmi snadný a rychlý zdroj zisku, který mu vyplatí pojišťovna v rámci pojistného plnění a to s minimem vynaloženého úsilí a bez obav z odhalení. Taková vozidla nejčastěji končí v zahraničí, kde doje k registraci na nového majitele a až poté je nahlášeno odcizení vozidla v původní zemi¹⁶. Další možností je, že automobily skončí rozřezány a prodány na náhradní díly. V obou případech tak pachatel podvodu inkasuje hned dvakrát.

3.3 Způsoby krádeží motorových vozidel

Krádeže motorových vozidel jsou páčány různými způsoby a prostředky, od použití hrubého násilí až po nejdokonalejší technické přípravky k překonání technického zabezpečení vozidel a to jak mechanického, tak elektronického. Předmětem útoku jsou vždy motorová vozidla a jednání pachatele musí vždy směřovat k zmocnění

¹⁶ CHMELÍK, Jan a kolektiv. *Rukověť kriminalistiky*. Plzeň: Aleš Čeněk, 2005. s. 377. ISBN 80-86898-36-9

se motorového vozidla a to ať za účelem krátkodobého využití, případně jeho tzv. legalizace nebo snaha toto motorové vozidlo zpeněžit¹⁷.

Podle složitosti způsobu páchání lze krádeže rozdělit na ty jednoduché a krádeže kvalifikované. Mezi jednoduché řadíme zejména krádeže starších motorových vozidel, která nejsou výrobcí proti odcizení dostatečně zajištěna. Do těchto vozidel pachatelé vnikají převážně za použití násilí, například rozbitím skleněné výplně okna motorového vozidla, následně dochází k tzv. rozlomení spínací skříňky a s tímto vozidlem zpravidla bez větších problémů odjíždějí. K odcizení těchto vozidel dochází nejčastěji kvůli krátkodobému užívání nebo poptávce po náhradních dílech.

Páchání složitých krádeží vyžaduje od pachatelů přípravu, jejíž úroveň se řídí zejména typem motorového vozidla a stupněm jeho zabezpečení a tedy i předpokládanou náročností spáchání trestného činu, zajištění odbytu odcizeného vozidla, zajištění krycích dokladů a pozměnění identifikačních znaků¹⁸.

Z hlediska způsobu provedení krádeží motorových vozidel můžeme krádeže rozdělit na:

- překonání mechanického zabezpečení vozidla spočívající v destrukci nějakého zařízení tvořící jistící překážku nebo jeho zámku. Pokud je volant zabezpečen bezpečnostní tyčí, její přestípnutí, podchlazení a následná destrukce, nebo přeríznutí samotného volantu a sundání zabezpečovací tyče, rozlomení zámku spínací skříňky či zámku převodovky. Tomu zpravidla vždy předchází násilné vniknutí do vozidla ať už rozbitím skleněné výplně dveří nebo rozlomením zámku dveří za užití nejrůznějších nástrojů, jako jsou rozlamováky, planžety nebo mechanické dekodéry zámků dveří. Široký sortiment těchto, ale i jiných prostředků lze zcela legálně zakoupit na webových stránkách.¹⁹
- překonání elektronického zabezpečení vozidla (výměna řídicí jednotky za vlastní upravenou, přemostění nebo reset imobilizéru prostřednictvím OBD

¹⁷ Kolektiv autorů HSVB za redakce pplk. Dr. Bohuslava Němce, *Kriminalistická příručka*. 1. svazek, Druhé vydání. Brno: Kriminalistický ústav VB, 1967. s. 112. ČÚKK 791/66-EÚ EK 3594/66

¹⁸ CHMELÍK, Jan a, kolektiv. *Rukověť kriminalistiky*. Plzeň: Aleš Čeněk, 2005. s. 357. ISBN 80-86898-36-9

¹⁹ *Locksmith.cz Professional Unlocking Tools*. Online. Dostupné z: <https://www.locksmith.cz/cs/automobily-26>. [cit. 2025-03-18]

zástrčky, rušení GSM, GPS signálu nebo rušení nebo přenos signálu vysílaného originálním autoklíčem, který je v držení majitele vozidla). V poslední době jsou hojně využívána, na trhu volně dostupná, elektronická zařízení, která dokážou blokovat, nahrát, dekodovat a uložit signál klíče pro pozdější využití. Pro pachatele pak není problém vozidlo odemknout a následně uzamknout. OBD (On Board Diagnostic) je mechanické rozhraní pro připojení konektoru diagnostického kabelu pro navázání komunikace mezi diagnostickým přístrojem a řídicími jednotkami ve vozidle. Od roku 2001 jí musejí mít všechny zážehové a od roku 2003 všechny vznětové motory²⁰. „GSM (Groupe Spécial Mobile) – z původního názvu francouzské skupiny, která navrhla první verze standardu GSM, což je celosvětově nejrozšířenější standard pro mobilní telefony, ale i pro datové přenosy“²¹.

- kombinací obou předešlých způsobů – zde obecně platí, že čím více zabezpečení na vozidle je, tím se pro zloděje stává tato „kořist“ méně atraktivní.
- odtažením pomocí odtahového vozidla – v našich končinách nepříliš častý jev, objevuje se zpravidla u krádeží na objednávku. Předmětem bývají převážně historická vozidla, běžně nepojízdná nebo déle stojící vozidla, tvářící se jako opuštěná. Ke krádeži dochází bez odemčení a nastartování a překoná tak hned několik druhů zabezpečení. Takový způsob je ale dosti hlučný, časově náročný a jistě i láká pozornost případných svědků, nicméně fantazii samotných zlodějů se meze nekladou je tak možné odcizit vozidlo pod smyšlenou legendou, např. že se jedná o odtah z důvodu neplacení leasingu apod.

²⁰ ŠVAMBERK, Jiří. *Diagnostická zásuvka OBD: Víte, k čemu slouží a co vše z ní můžete zjistit?* Online. 2019. Dostupné z: <https://www.tipcars.com>. [cit. 2024-05-14]

²¹ PC-IN PLZEŇ. *GSM - Slovník ICT pojmů*. Online, 12.09.2015. Dostupné z: <https://www.pcinplzen.cz>. [cit. 2024-08-22]

4 Legislativa k pátrání po vozidlech

Jedním ze základních úkolů policie je mimo jiné chránit bezpečnost majetku a další úkoly na úseku vnitřního pořádku. Z toho lze vyvodit, že Policie ČR chrání majetek občanů, pátrá po odcizených věcech a věcech pocházejících z trestné činnosti nebo k takové činnosti sloužících. Takové pátrání je legislativně ukotveno v zákoně č. 273/2008 Sb. O Policii České republiky, konkrétně v §68 odst. 1, který uvádí: *Policie provádí jakou součást plnění svých úkolů pátrání po osobách a věcech s cílem zjistit, kde se tyto osoby nebo věci nacházejí, nebo identifikovat osoby, mrtvol, části lidského těla anebo kosterního nálezu neznámé totožnosti.* Pátrání po osobách a věcech je zákonem o policii koncipováno jako součást jednotlivých úkolů plněných policií²². Tentýž zákon v § 42 dává policii oprávnění k zastavení a prohlídce dopravního prostředku mimo jiné z důvodu pátrání po věcech pocházejících z trestné činnosti nebo s takovou činností související nebo má-li důvodné podezření, že používáním dopravního prostředku, na dopravním prostředku nebo v souvislosti s dopravním prostředkem byl spáchán trestný čin²³.

Takovému pátrání zpravidla předchází oznámení o krádeži vozidla oznamovatelem a jako jedním z prvních úkonů je vyhlášení pátrání po vozidle v informačním systému PatrMV. Do systému se zadají základní identifikační znaky jako je VIN vozidla a registrační značka. Po vozidle je tímto krokem vyhlášeno pátrání nejen na území České republiky, ale i na území členských států Schengenského prostoru.

V případě odcizeného vozidla, které je opatřeno systémem eCall, má policejní orgán možnost po splnění zákonných podmínek vyžádat záznam telekomunikačního provozu dle ust. § 88a trestního řádu²⁴. Před tím si však musí na základě ust. § 8 odst. 1 trestního řádu²⁵ dožádat od automobilky nebo jejího oprávněného servisního střediska údaje nezbytné pro získání lokalizačních údajů, v tomto případě IMEI. V přípravném řízení vydává příkaz k zjištění údajů telekomunikačního provozu soudce na základě

²² ŠKODA, Jindřich; VAVERA, František a ŠMERDA, Radek. *Zákon o policii s komentářem*. Plzeň: Aleš Čeněk, 2009. s. 231. ISBN 978-80-7380-160-1

²³ ŠKODA, Jindřich; VAVERA, František a ŠMERDA, Radek. *Zákon o policii s komentářem*. Plzeň: Aleš Čeněk, 2009. s. 149. ISBN 978-80-7380-160-1

²⁴ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 166. ISBN 978-80-7488-424-5

²⁵ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 128. ISBN 978-80-7488-424-5

návrhu státního zástupce a to státnímu zástupci nebo policejnímu orgánu. Příkaz musí být vydán písemně včetně řádného odůvodnění. Dle odstavce 4 téhož zákona není příkazu třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat²⁶. V tomto případě majitel či provozovatel již odcizeného vozidla. Následně servisní policejní pracoviště zajistí od poskytovatele telekomunikačních služeb záznam provozních a lokalizačních údajů vozidla, které následně předá policejnímu orgánu pro účely pátrání po odcizeném vozidle.

²⁶ *Trestní předpisy [ÚZ 2020 č. 1389]. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 167.*
ISBN 978-80-7488-424-5

5 Elektronické zabezpečení vozidel

Mimo mechanického existuje několik druhů elektronického zabezpečení vozidel, které slouží k ochraně proti krádeži a neoprávněnému přístupu. Dělí se na elektronické zabezpečení instalované výrobcem automobilů a na dodatečně instalované zabezpečení vozidla uživatelem. Jak bylo již uvedeno výše, elektronické zabezpečení si prošlo obrovským vývojem a nyní je na trhu nepřehledné množství různých zabezpečení, které lze pořídit od pár stokorun až řádově po desetitisíce a záleží jen na samotném majiteli, pro jaký druh zabezpečení se rozhodne. Bohužel stejně jako se neustále vyvíjí nové a nové druhy zabezpečení, stejně se vyvíjí i znalosti zlodějů a jsou tak vždy o krok napřed. Je ale důležité uvědomit si, že každý zabezpečovací systém, a to bez ohledu na jeho pořizovací hodnotu, má mnohem větší význam než zabezpečení žádné. Jakékoliv zabezpečení může zloděje odradit, protože jeho překonání je pro něj jednoduše překážkou a to z důvodu absence vhodných nástrojů nebo časové prodlevy samotné krádeže. Na elektronické zabezpečení vozidel myslí i pojišťovny, které při uzavírání smluv o pojištění vozidla proti krádeži v případě nainstalovaného zabezpečení nabízejí mnohdy i velmi zajímavé slevy na pojistném. Tím motivují majitele automobilů k jejich zabezpečení a na oplátku nabízejí výhodnější cenu hrazené pojistné částky. Výše slevy se zpravidla liší na druhu pořízeného zabezpečení²⁷.

5.1 Elektronické zabezpečení vozidel instalované výrobcí vozidel

5.1.1 Centrální zamykání

„Elektronický systém, který umožňuje synchronizovaně odemykat a zamykat dveře vozidla na dálku centrálně pomocí dálkového ovladače, který je součástí originálního autoklíče. Tento systém může být ovládán mechanicky zámkem dveří nebo elektronicky pomocí dálkového ovladače. Dokáže zamezit otevření dveří neautorizovanými osobami“²⁸. Centrální zamykání funguje díky elektromotoru, který

²⁷ PAJER, M. Zabezpečení vozidel. *Security magazín Časopis pro vaši bezpečnost*. Praha: FAMily media, 1999, roč. 5-6, č. 4, s. 7-19. ISSN 1210-8723.

²⁸ *Centrální zamykání vozidel*. Online. 2024. Dostupné z: <https://www.autoprofi.cz>. [cit. 2024-06-03]

svým pohybem pomocí mechanického táhla zajišťuje odemčení nebo uzamčení zámku dveří, ale i víčka palivové nádrže nebo dveří zavazadlového prostoru a to vše pouhým stisknutím jednoho tlačítka na dálkovém ovladači²⁹. V současné době je klasické centrální zamykání vylepšeno systémem keyless, což je tzv. bezklíčové centrální zamykání, které umožňuje odemčení a uzamčení vozidla bez manipulace s autoklíčem, kdy postačí jeho přítomnost v blízkosti vozidla. U luxusních vozidel nabízí výrobci ovládání vozidla pomocí mobilní aplikace, která umožňuje odemykání nebo zamykání dveří, startování motoru nebo dokonce nastavení různých funkcí vozidla. Keyless systémy se stávají stále více běžnou součástí moderních vozidel a nabízejí větší pohodlí a bezpečnost pro jejich uživatele, ale zároveň jsou také velkou slabinou při zabezpečení vozidel.

Většina elektronických automobilových zámků pracuje na frekvenci 315 nebo 433 MHz a používají tzv. plovoucí kód, který se mění při každém stisku tlačítka. Řídící jednotka je nastavena tak, aby nepřijala dvakrát stejný kód. Protože tyto systémy často neřeší časovou platnost kódu, lze aplikovat tzv. Replay útok. *Jedná se o útok, který zahrnuje zachycení přenášených informací o autentizaci nebo řízení přístupu a jeho následné opětovné přenosy s úmyslem vytvořit neoprávněný účinek nebo získat neoprávněný přístup*³⁰. Laicky řečeno spočívá v tom, že útočník použije zařízení k dočasnému zarušení vozidla a po přijetí platného kódu jej vypne. Uživatel bude muset vyslat minimálně dva signály k uzamčení vozidla a vůbec ho nenapadne, že se právě stal obětí útoku. Hacker dostává do vlastnictví jeden platný kód pro pozdější otevření vozidla. Obrovskou slabinou tohoto systému je fakt, že řídící jednotka centrálního zamykání je schopna přijmout jen jeden signál klíče na dané frekvenci, takže jako rušičku tohoto signálu lze použít i klíč od jiného vozidla pracující na stejné frekvenci, kdy při jeho stisku a tedy vysílání signálu na konkrétní frekvenci, není možné příslušným originálním klíčem uzamknout vozidlo³¹. Stejným způsobem lze použít i různé dálkové ovladače, například od garážových vrat, posuvných bran nebo i radiostanice. Podmínkou je opět pracovní frekvence totožná s tou, na které pracuje napadené vozidlo. Proti tomuto útoku v podstatě neexistuje prevence, pouze po uzamčení fyzická kontrola, zda skutečně došlo k uzamčení dveří vozidla.

²⁹ VLK, František. *Lexikon moderní automobilové techniky*. Brno: Prof. Ing. František Vlk, DrSc., nakladatelství a vydavatelství, 2005. s. 60. ISBN 80-239-5416-4

³⁰ TAYLORCOXX. *Replay útoky*. Online. 2017. Dostupné z: <https://www.tx.cz>. [cit. 2024-07-23]

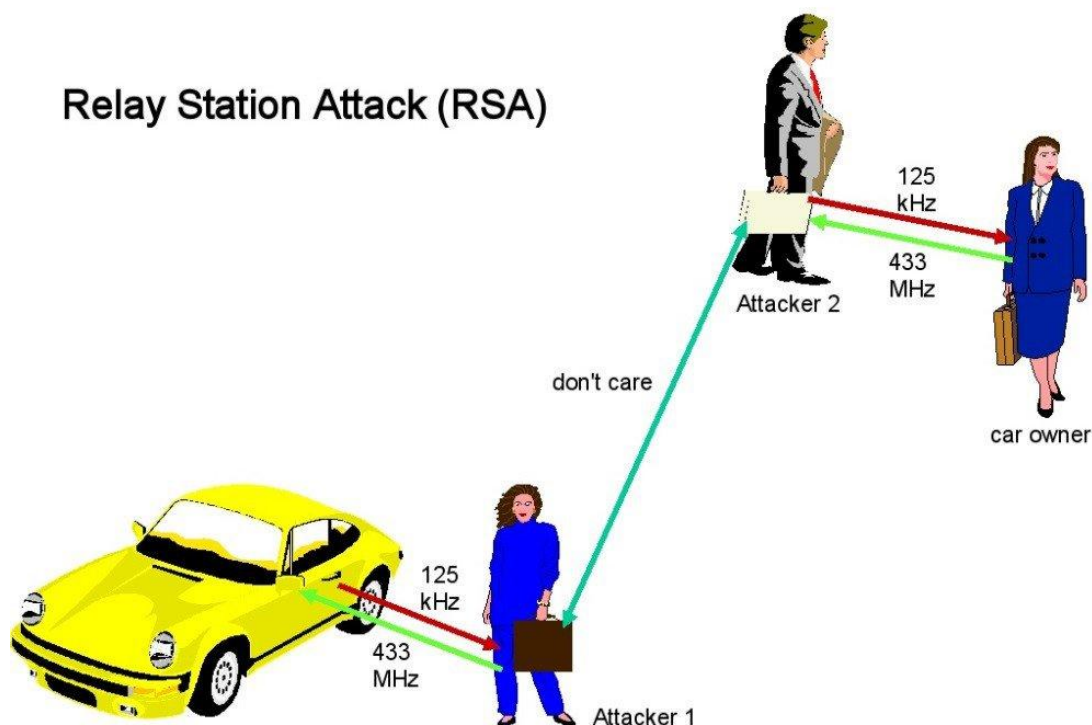
³¹ ZVAŘIČ, Filip. *Úvod do hackování aut - Car hacking - Hacking lab*. Online. 2020-09-22. Dostupné z: <https://hackinglab.cz>. [cit. 2024-06-18]

S centrálním zamykáním také velmi úzce souvisí tzv. keyless systém, nebo také KESSY (Keyless Entry, Start and exit System – elektronický zamykací systém, umožňující řidiči bezklíčové otevírání a startování vozu) – *je založen na principu, že originální klíč od vozidla stále vysílá signál a hledá vozidlo. Pokud se majitel s klíčem přiblíží na krátkou vzdálenost, přibližně na jeden až dva metry k vozidlu a dotykem kliky dveří nebo zadních dveří zavazadlového prostoru se vozidlo samo odemkne a poté je možnost pomoci tohoto signálu i nastartovat*³². Komunikace mezi klíčem a vozidlem probíhá šifrovanou rádiovou komunikací, vozidlo si rozumí pouze s vlastním klíčem, s žádným jiným. Tyto systémy se stávají stále více běžnou součástí moderních vozidel, přestože byly vyvinuty již v 80. letech minulého století a nabízejí větší pohodlí a bezpečnost pro jejich uživatele, ale zároveň jsou také velkou slabinou při zabezpečení vozidel a jedná se aktuálně o nejčastější způsob jejich napadení. Princip spočívá v tom, že vozidlo vysílá pasivně na nízkých frekvencích rádiový dotaz, zda se v jeho blízkosti nachází autorizovaný klíč a to právě na vzdálenost do 2 metrů. Oproti tomu klíč vysílá odpověď na mnohem větší vzdálenost, kdy se rádiovým signálem dotazuje na přítomnost vozidla, ke kterému je autorizován, tato vzdálenost je cca 100 metrů. Protože ale na velkou vzdálenost klíč tzv. neslyší volání auta, nereaguje dál než 1 až 2 metry od vozidla. Na delší vzdálenost Keyless standardně fungovat nebude. Ač se jeví tento systém jakkoliv bezpečný, na jeho překonání stačí vložení dalšího mezičláčku mezi klíč a vozidlo. Tímto mezičláčkem je pouhý zesilovač signálu – extender, který nedělá nic jiného, než zopakuje volání auta na klíč a zpět a tím výrazně prodlouží vzdálenost, na kterou klíč reaguje. V praxi to funguje tak, že zloději využívají prodlužovák signálu, extender, zesilovač. Skládá se ze dvou zařízení, které spolu komunikují bezdrátově. Pro obsluhu těchto zařízení jsou potřeba dvě osoby. První z nich se s prvním zařízením postaví k autu a dotýká se kliky nebo mačká tlačítko pro otevření dveří, v tom okamžiku se snaží auto zavolat na svůj klíč, ale ten leží doma na skřínce za zamčenými dveřmi nebo jej má majitel při sobě ve vzdálenosti vyšší než několik stovek metrů a volání auta neslyší, auto se neotevře. Pokud ale zloději aktivují extendery, volání auta na klíč zesílí ten u vozidla, přenesení ho bezdrátově k druhé jednotce, kde je druhý zloděj, ten má k extenderu připojenou výkonnou anténu, kterou namíří na objekt, kde se klíč nachází a volání auta na klíč zesílí tak, že ho klíč uslyší a odpoví. Pokud vozidlo uslyší odpověď z klíče, obvykle do 100 metrů od auta, odemkne se. To samé se opakuje s nastartováním vozidla. Kromě zesílení volání z auta na klíč mohou extendery zesilovat i odpověď

³² Keyless Block - zařízení proti krádeži auta s bezklíčovým zamykáním. Online. Dostupné z: <https://authoralarm.cz>. [cit. 2024-07-23]

z klíče do auta, pak může být vozidlo napadeno i třeba na vzdálenost tisíců kilometrů³³. V praxi se však krade na vzdálenost několika desítek až stovek metrů. Tento typ napadení se nazývá relay station attack.

Obrázek 1: schéma provedení útoku Relay Station Attack³⁴



Možnosti prevence před tímto druhem útoku jsou dvě. Ta první je omezení komfortu volných rukou diagnostickým zablokováním možnosti bezklíčového ovládání vozidla, čímž se dokonale zamezí tomuto útoku a to ať už je klíč na pohybu nebo leží nehnutě někde doma, ale uživatel musí běžným způsobem odemknout vozidlo stiskem tlačítka na klíči. Druhou možností je patentovaný vynález pana Ing. Stanislava Čechráka ze společnosti ESSAtech s. r. o., kterou je elektronický čip, tzv. Keyless Defender, který je zobrazený na obrázku č. 3. Tento čip se velmi jednoduše nainstaluje do klíče od vozidla a tvoří vlastně jakýsi obal baterie, která se nachází v elektronickém klíči. Jeho funkcí je odpojit elektroniku klíče od baterie v okamžiku, kdy se klíč nepohybuje. Tím zajistí, že doma odložený klíč bude zcela nefunkční a není možné jej

³³ SECURITY MAGAZÍN. *Keyless systém - příliš vysoká cena za komfort?* Online. 2019. Dostupné z: <https://www.securitymagazin.cz>. [cit. 2024-07-23]

³⁴ ZVAŘIČ, Filip. *Úvod do hackování aut - Car hacking - Hacking lab*. Online. 2020-09-22. Dostupné z: <https://hackinglab.cz>. [cit. 2024-06-18]

zneužit pro otevření a nastartování vozidla. Jakmile se klíč pohne, opět je baterie pomocí čipu připojena a klíč funguje zcela standardně. Keyless Defender však funguje pouze v případě, že se klíč nachází bez pohybu, ne na ten, který má uživatel u sebe a je tak stále v pohybu. Čip je možné kdykoliv z klíče vyjmout a uvést jej tak do původního stavu³⁵. Cena Keyless Defenderu se pohybuje okolo čtyř tisíc korun českých. Jednou z dalších možností, jak zabránit vysílání signálu klíče směrem k vozidlu je pořízení různých stínících obalů nebo Faraday boxů, kam je vždy třeba takový klíč uložit, v tomto případě je klíč zcela odstíněn vždy, pokud je v takovém obalu uložen. Cena tohoto typu obalů se pohybuje v řádech stokorun, zhruba do dvou tisíc korun českých.

Při jednom z pokusů byla provedena simulace krádeže 13 vozidel s keyless systémem, toto se podařilo během 6 minut a to za použití extenderu³⁶.

Obrázek 2: Keyless deffender³⁷



³⁵ ESSATECH, S.R.O. *Produkty ESSAtech, s.r.o.* Online. Dostupné z: <https://www.essatech.cz>. [cit. 2024-07-23]

³⁶ ZLODEJ, Tonda. *Theft of 13 keyless cars in 6 minutes!*. YouTube. 2019. Dostupné z: https://www.youtube.com/watch?v=02CLcw_Gt24. [cit. 2025-03-18]

³⁷ ESSATECH, S.R.O. *Produkty ESSAtech, s.r.o.* Online. Dostupné z: <https://www.essatech.cz>. [cit. 2024-07-23]

5.1.2 Imobilizér

Tato technologie zabráňuje nastartování motoru bez příslušného autentizačního kódu, který je uložen v čipu, který je v současné době součástí každého autoklíče. Jeho funkce spočívá v tom, že po vypnutí motoru přerušuje jeden nebo několik okruhů nezbytných k nastartování motoru, nejčastěji se jedná o signál do palivového čerpadla, startéru a zapalování. Podle počtu přerušovaných okruhů se imobilizér rozděluje na jednookruhový nebo víceokruhový. Následným startováním autorizovaným klíčem s přítomným čipem dojde k propojení imobilizérem přerušovaných okruhů a motor lze nastartovat. Po vypnutí zapalování opět dojde k rozpojení elektrických obvodů dle továrního nastavení.

Imobilizér se začal používat v automobilech přibližně od 90. let, ale jeho použití se postupně rozšířilo a dnes je standardní součástí mnoha moderních vozidel³⁸. Ne vždy však byla jeho podoba jako dnes, kdy je v originálním autoklíči umístěn čip cca o velikosti jednoho centimetru, který tak automaticky komunikuje s vozidlem při manipulaci ve spínací skřínce. Dříve měl imobilizér podobu např. čipové karty nebo konektoru, které bylo třeba před nastartováním vložit do příslušného slotu.

Od roku 1993 se stal CAN protokol mezinárodním standardem pro všechna běžná vozidla a od roku 2001 všechna auta vyrobená v Evropě mají povinně CAN sběrnici. Controlled Area Network, nebo zkráceně CAN sběrnice pro výměnu dat, umožňuje vzájemnou komunikaci mezi elektronickými moduly na palubě vozidla, ale slouží taky ke komunikaci s diagnostickým softwarem prostřednictvím diagnostické zástrčky. Umožňuje přenos dat rychlostí až 1Mb/s a jedná se o dvoudrátovou poloduplexní síť³⁹.

Každý výrobce aut může používat lehce odlišné protokoly na CAN sběrnici a frekvence použité při komunikaci. Jednotky hodnotí relevanci zprávy podle tzv. Arbitration ID, které specifikuje ID jednotky, pro kterou je zpráva určena. Toto ID také určuje prioritu zprávy – nižší ID znamená vyšší prioritu. 6 nul po sobě znamenají high priority error. Slabinou takového zabezpečení je tzv. DoS (Denial of Service) útok což v podstatě znamená odepření služby a jeho principem je zaslání 32 takovýchto

³⁸ AUTOKLICECZ.CZ. *Co je to imobilizér?* Online. 2021. Dostupné z: <https://www.autoklicecz.cz>. [cit. 2024-07-23]

³⁹ ZABEZPEČ AUTO. *Sběrnice CAN - co to je a jak to funguje?* Online. ZABEZPEC-AUTO.CZ. Dostupné z: <https://zabezpec-auto.cz>. [cit. 2024-07-23]

chybových zpráv po sobě, kdy tímto útokem dojde k zahlcení vnitřního systému, čímž dojde k odepření funkčnosti a jednotka ECU (Electronic Control Unit – vestavěný počítač pro řízení automobilových systémů) přejde do stavu OFF. Hacker, který se dostane k OBD-II portu a provede výše zmíněné kroky, získá kontrolu nad CAN sběrnici a tudíž nad důležitými funkcemi vozidla⁴⁰. Ukázka OBD-II portu ve vozidle je na obrázku č. 3, téměř vždy se nachází v dosažitelné vzdálenosti z místa řidiče a nejčastěji bývá ve spodní části palubní desky a jeho konektor je zpravidla opatřen výraznou barvou. Jedná se tak o velmi výraznou slabinu tohoto typu zabezpečení, přesto výrobci automobilů doposud nezpracovali na jeho inovaci. Na trhu je dostupné mechanické zabezpečení OBD-II portu, čímž lze zamezit neoprávněnému přístupu ke sběrnici vozidla a tím k vyřazení funkce imobilizéru.

Obrázek 3: OBD-II port ve vozidle⁴¹



Další možností jak obejít imobilizér je použití vlastní řídicí jednotky s deaktivovanou činností imobilizéru, která spočívá v přemostění spoje a výstupní signál fakticky toto zabezpečení obejde. Zde je vyžadována příprava a nutnost použít řídicí jednotku shodného typu a motorizace. Nevýhodou u tohoto typu krádeže je pohyb pachatele u vozidla, kdy je nutné manipulovat v motorovém prostoru za účelem výměny

⁴⁰ ZVAŘIČ, Filip. *Úvod do hackování aut - Car hacking - Hacking lab*. Online. 2020-09-22. Dostupné z: <https://hackinglab.cz>. [cit. 2024-06-18]

⁴¹ Mtaplus - *Problematika diagnostiky starších vozidel*. Online. Dostupné z: <https://www.mtaplus.cz>. [cit. 2024-07-23]

řídící jednotky, toto jednání nejen, že významně poutá pozornost, ale také prodlužuje dobu nezbytnou k odcizení vozu.

5.1.3 Alarm

Elektronický zabezpečovací systém, který slouží k detekci neautorizovaného vstupu do vozidla. Jedná se o aktivní prvek elektronického zabezpečení vozidla, který je v případě montáže z výroby napojen na řídící jednotku vozidla. V případě podnětu se spustí hlasitý akustický alarm za účelem upozornění majitele a okolí na neoprávněnou manipulaci s vozidlem⁴². Některé systémy mohou také zablokovat některé funkce vozidla nebo informovat majitele vozidla pomocí notifikace na mobilní telefon či pager⁴³. Existuje několik druhů alarmů od jednoduchých, až po ty složité, které uživateli umožňují připojovat další zařízení či čidla. Alarm má několik druhů senzorů, nejčastěji jde o otřesový senzor, dále pohybový, akustický, či senzor náklonu. O přítomnosti alarmu ve vozidle většinou informuje indikátor v podobě blikající LED (Light Emitting Diode – elektroluminiscenční dioda) diody na viditelném místě, zejména v prostoru čelního nebo bočního skla a to z toho důvodu, aby bylo na první pohled zřejmé, že vozidlo je právě tímto zabezpečovacím zařízením opatřeno, mnohdy jsou také boční okna vozidel vybavena samolepícím štítkem oznamující přítomnost alarmu, aby tak došlo k co možná největšímu odrazení potenciálního zloděje k neoprávněnému vniknutí do vozidla. Alarm tak působí spíše preventivně, než aby přímo zamezil krádeži vozidla. Nevýhodou alarmu instalovaného výrobcem automobilu přímo při jeho výrobě je shodné schéma zapojení všech vyrobených kusů daného modelu a není tak problém i pro méně zdatného zloděje si takové schéma opatřit a alarm v případě krádeže vyřadit z provozu. Další nevýhodou je případ použití zařízení, které umí číst a kopírovat na dané frekvenci plovoucí kód originálního klíče. V takovém případě zloděj odemkne vozidlo standardním způsobem a alarm napojený na centrální zamykání vozu se domnívá, že jde o autorizovaný vstup pomocí originálního klíče a alarm se neaktivuje. V nedávných dobách také mnohokrát docházelo k situaci, kdy bylo novým majitelem vozidla zjištěno, že předešlý majitel si někde na vozidle, tak aby místo bylo volně přístupné, ukryl originální klíč. Adresu nového majitele měl uvedenou v kupní smlouvě, nic tedy nebránilo předešlému majiteli, aby si na uvedenou adresu dojel, vyndal svůj, na voze ukrytý, klíč a vozidlo běžně odemkl, nastartoval a odjel. Stejně tak mohl mít

⁴² PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. s. 885. ISBN 978-80-7380-589-0

⁴³ WEIGEL, Ondřej. *Jak zabránit krádeži vašeho automobilu: mechanické a elektronické zabezpečení*. Praha: Computer Press, 2000. ISBN 80-7226-349-8

k dispozici i duplikát originálního klíče, aniž by o tom nový majitel věděl. V takovém případě alarm vyhodnocuje situaci jako autorizovaný vstup, imobilizér má správné informace a umožní řádné nastartování vozidla. Na obrázku č. 4 je reálný příklad ukrytého klíče za krytkou ve spodní části nárazníku vozidla Škoda Superb II, nalezeného novým majitelem po koupi vozidla.

Obrázek 4: Klíč od vozidla Škoda Superb, ukrytý v nárazníku⁴⁴



5.1.4 GPS sledovací systémy

Tyto systémy používají satelitní navigaci a mobilní síť pro určení a sledování polohy vozidla v reálném čase. Mohou také poskytovat další informace, jako je stav motoru, rychlost, stav paliva v nádrži, úroveň nabití baterie a další. GPS (Global Positioning System – satelitní navigační systém americké vlády spuštěný v roce 1997, který v současné době využívá soustavu 31 družic poháněných solární energií, GPS funguje nepřetržitě, za každého počasí a všude na světě)⁴⁵ systém umožňuje majiteli vozidla rychle lokalizovat a nalézt vozidlo v případě krádeže. Přichází tedy na řadu, pokud všechny předešlé zabezpečovací systémy, ať mechanické nebo elektronické, nedokážou samotné krádeži zabránit a vozidlo je odcizeno. Spočívá tedy v lokalizaci

⁴⁴ AUTANET. *Jednoduchá finta, jak vám ukradnou auto*. Online. 2016. Dostupné z: <https://www.autanet.cz>. [cit. 2024-07-23]

⁴⁵ TOPGIS. *GPS: globální satelitní navigační systém*. Online. Dostupné z: <https://www.gisonline.cz>. [cit. 2024-09-14]

polohy odcizeného vozidla. Mnohdy se však jedná o nadstandardní službu hrazenou uživatelem, aby mohla být využívána v plném rozsahu. Často si ani samotní uživatelé nejsou vědomi, že mohou této službě využívat a tuto službu, která je zpravidla zahrnuta v balíčku dalších služeb, z pocitu nadbytečnosti ani nepožijí nebo neprodlužují.

GPS modul disponuje informacemi o datu, času, pozici, kurzu a rychlosti a tato data formou signálu přeposílá dále za pomoci antény⁴⁶. Tento vysílaný GPS signál lze prostřednictvím speciální rušičky vyrušit a znemožnit tak funkci takového zabezpečovacího systému.

5.1.5 Systém eCall

Myšlenka eCallu (Emergency Call – nouzové volání) je poměrně stará, již v minulosti se jí zabývala řada jednotlivých zemí a výrobců vozidel již ve 20. století, bohužel často jen na národní, lokální nebo uzavřené technologické úrovni jednotlivých výrobců vozidel. Jakýmsi předchůdcem byly tzv. „SOS hlásky“⁴⁷ umístěné zejména na dálničních sítích. Měly v dobách, kdy mobilní telekomunikační služby nebyly tak rozšířené, jako je tomu dosud, svou nezastupitelnou roli. Jedná se o jakési boxy oranžové barvy s logem telefonního sluchátka a nápisem SOS. Uvnitř se nacházelo fixní komunikační zařízení. Dalo se jimi obdobným způsobem jako u eCallu přivolat pomoc, kdy kromě spojení příslušného tísňového volání byla předána i pozice příslušné hlásky a tím došlo k jednoznačnějšímu určení polohy dopravní nehody. Avšak je zcela závislá na vůli volajícího.

První impuls jednotného vývoje učinila až Evropská komise, která vydala v roce 2001 tzv. Bílou knihu (Evropská dopravní politika pro rok 2010: čas rozhodnout, vedená pod označením COM (2001) 0370 z 12.9.2001) definující strategii rozvoje a řízení dopravní problematiky. Jedním z hlavních strategických cílů celoevropské úrovně bylo snížit úmrtnost na silnicích do roku 2010 o 50%⁴⁸.

⁴⁶ ŠVÁBENSKÝ, Otakar. *Základy GPS a jeho praktické aplikace*. 1. vydání. Brno: CERM, 1995. ISBN 80-214-0620-8

⁴⁷ WIKIWAND. *SOS hláska* - Wikiwand. Online. Dostupné z: <https://www.wikiwand.com>. [cit. 2024-06-27]

⁴⁸ MATOUŠKOVÁ, I.; MORAVČÍK, L., RAK, R. a kol. *ECall - Inteligentný dopravný systém (aspekty právne, technické, informačné a psychologické)*. Bratislava: Magnet Press, Slovakia, 2015. s. 219. ISBN 978-80-89169-31-3

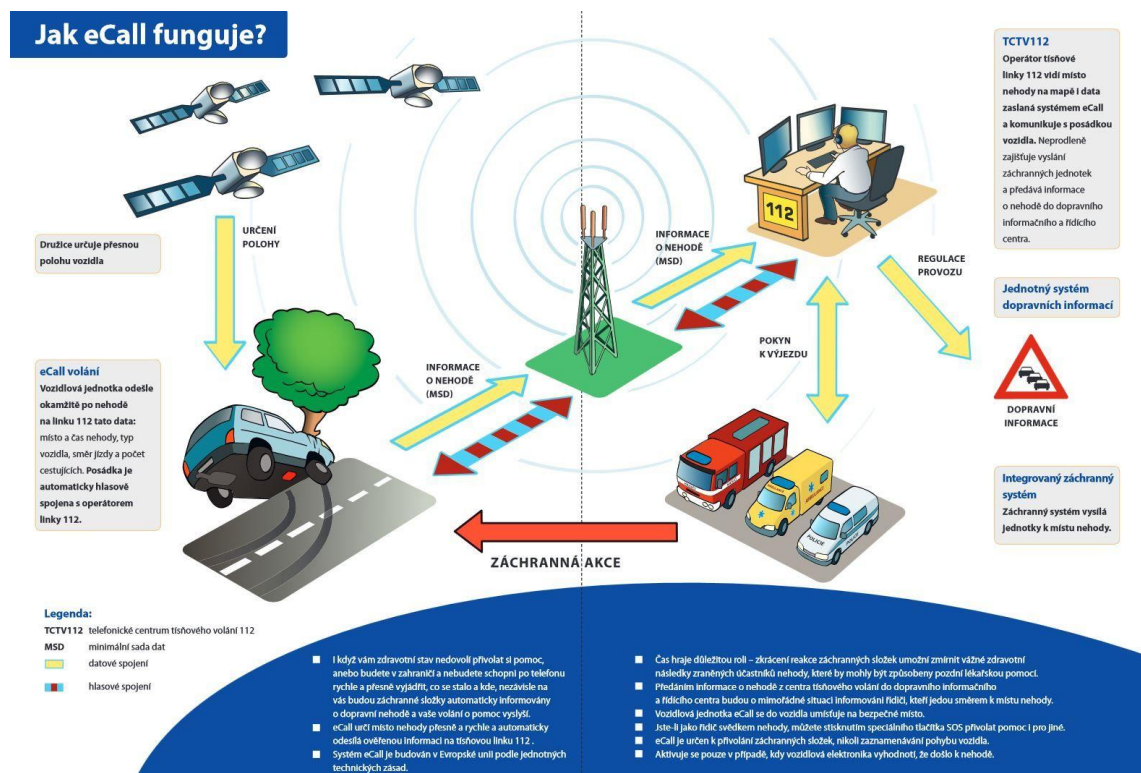
ECall je systém hojně používaný zejména u vozidel vyrobených v EU. V minulosti byl podobný systém instalován výrobcí vozidel prémiových značek již od devadesátých let minulého století, byl tehdy závislý na činnosti osádky vozidla a byla zde podmínka přítomnosti zabudovaného telefonu ve vozidle, nešlo tedy o automatický systém, jako nyní. Jedná se vlastně o jakousi černou skříňku vozidla a základem tohoto systému je vozidlová jednotka obsahující virtuální kartu SIM (Subscriber Identity Module – obsahující údaje o uživateli mobilních služeb, v tomto případě o vozidle, slouží k identifikaci účastníka v mobilní síti), která je v závislosti na konkrétním modelu vozidla zabudována na různém místě. Tato jednotka monitoruje množství kritických veličin pomocí vlastních senzorů či napojením na CAN sběrnici vozidla. Musí být schopna vyhodnotit nouzovou situaci, kdy je posádka ohrožena na životě či zdraví a aktivovat funkci eCall. Systém v případě vážné dopravní nehody na základě obdrženého signálu nárazových čidel, iniciací airbagů či pyrotechnických patron bezpečnostních pásů bez asistence posádky automaticky naváže hlasovou komunikaci vozidla s nejbližším operačním střediskem linky tísňového volání 112 a zároveň bude vytvořen telekomunikační bezdrátový most pro přenos nezbytných dat. Tímto umožní získat další údaje o nehodě, čímž optimalizuje složení záchranných složek a snižuje tak reakční čas a zvyšuje se pravděpodobnost rychlé záchrany zraněných osob. Systém eCall také poskytuje základní informace o nehodě, jako je VIN (Vehicle Identification Number) vozidla z toho plyne informace, zda se jedná o motocykl, osobní automobil a jaký typ nebo například autobus, geografické souřadnice místa nehody, čas nehody, rychlost vozidla a směr jízdy, aktivace airbagů, případně počet pasažérů (tato informace se získává ze senzorů zapnutí bezpečnostních pásů ve vozidle). Kromě automatické aktivace je umožněno posádce vozidla přivolat pomoc i ručně stisknutím „SOS“ tlačítka a to i posádce vozidla, která je svědkem takové události, vyžadující si zásah složek IZS. Tento bezpečnostní systém je povinný v nových vozidlech vyrobených v Evropské unii od roku 2018.

Data odesílaná na operační středisko tísňové linky 112 se v terminologii pall označují jako MSD (Minimum Set of Data – minimální soubor údajů)⁴⁹.

Na obrázku č. 5 je principiálně zobrazené, jak celý systém eCall funguje.

⁴⁹ MATOUŠKOVÁ, I.; MORAVČÍK, L., RAK, R. a kol. *ECall - Inteligentný dopravný systém (aspekty právne, technické, informačné a psychologické)*. Bratislava: Magnet Press, Slovakia, 2015. s.223. ISBN 978-80-89169-31-3

Obrázek 5: Schéma funkce systému eCall⁵⁰



Přestože se systém eCall jeví jen jako jeden z prvků pasivní bezpečnosti při provozování motorového vozidla má i obrovský benefit pro policii z hlediska jeho vyhledání. Navíc znemožnění provozuschopnosti či odstranění eCallu bude postihováno a kontrolu správné funkce bude provádět stanice technické kontroly při zákonných pravidelných prohlídkách vozidel.

Jak již bylo zmíněno součástí je virtuální karta SIM umístěná v elektronickém zařízení kdesi ve vozidle a tato karta je neustále připojena k mobilní síti. Mobilní operátoři jsou dle zákona o elektronických komunikacích⁵¹ dále jen ZEK, povinni po dobu 6 měsíců uchovávat provozní a lokalizační údaje všech uživatelů mobilních sítí. § 97 odst. 4 ZEK uvádí, že provozní a lokalizační údaje podle odstavce 3 § 97 tohoto zákona jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a době trvání komunikace. Rozsah uchovávání provozních a lokalizačních údajů uchovávaných podle

⁵⁰ SAJDL, Jan. *ECall - autolexicon.net*. Online. Dostupné z: <https://www.autolexicon.net>. [cit. 2024-09-14]

⁵¹ ČESKO. Zákon č. 273 ze dne 22. srpna 2012 o elektronických komunikacích. In *Sbírka zákonů České republiky*. Online. 2012. Částka 94. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-273/zneni-20121001>. [cit. 2025-03-18]

*odstavce 3 § 97 tohoto zákona, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis*⁵². Policejní orgán si následně cestou oprávněného útvaru vyžádá dle §88a odst. 1 zák. č. 141/1961 Trestní řád zjištění údajů o uskutečněném telekomunikačním provozu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce⁵³. Musí však být splněny zákonné podmínky tohoto úkonu, jinak jej nelze provést.

5.1.6 Bezpečnostní kamery

Jsou čím dál častěji součástí vozidel vyšších tříd. Tyto kamery mohou ukládat záznam okolí vozidla a tento záznam může být užitečný při identifikaci pachatele a poskytnutí důkazů o krádeži. Samostatnou kapitolou v tomto směru jsou vozidla výrobce TESLA, jejichž četnost ve vozovém parku je stále vyšší a vyšší. Palubní kamery na těchto vozech pořizují videozáznam okolí vozu během jízdy. Pomocí kamery lze zaznamenávat incidenty během jízdy nebo jiné významné události stejně jako v případě externích palubních kamer u jiných vozidel. Záznamy se ukládají do paměti naformátovaného USB flash disku. To zda palubní kamera automaticky uloží videozáznam nebezpečné situace, určuje několik faktorů, například velikost působící síly, zda došlo k aktivaci airbagů nebo například stlačením klaksonu⁵⁴.

Vozidla Tesla, se součástí výbavy označenou Sentry mode mají kamery s rozsahem 360°, ty snímají okolí i zaparkovaného a uzamčeného vozidla. Aktivují se pohybem, nárazem, otřesem nebo otevřením dveří. Takže v případě násilného vniknutí do vozidla je toto schopné zcela autonomně spustit kamery a zadokumentovat tak pachatele vloupání do vozidla, tento záznam následně uloží ve své paměti a lze ho tak přehrát přímo na obrazovce ve vozidle nebo v počítači. Policii tímto způsobem poskytne zcela samostatně důkaz v podobě obrazových záznamů spáchaného trestného činu. Tuto funkci lze pochopitelně také vypnout, což se bohužel mnohdy děje z důvodu velkého

⁵² ČESKO. Zákon č. 273 ze dne 22. srpna 2012 o elektronických komunikacích. In *Sbírka zákonů České republiky*. Online. 2012. Částka 94. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-273/zneni-20121001>. [cit. 2025-03-18]

⁵³ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 166. ISBN 978-80-7488-424-5

⁵⁴ TESLA. *Palubní kamera, režim Sentry a zabezpečení*. Online. 2024. Dostupné z: <https://www.tesla.com>. [cit. 2024-08-08]

pohybu osob kolem vozidla zejména v centrech velkých měst a dochází k ukládání velkého objemu dat, ale hlavně k vybíjení baterií, což děsí velkou většinu uživatelů elektromobilů. Kromě aktivního kamerového systému vozy značky TESLA ukládají údaje o otevření a zavření dveří, oken, kapoty, otřesu a náklonu, všechny tyto údaje jsou schopny zasílat uživateli formou notifikace na mobilní telefon.

5.2 Dodatečně instalované elektronické zabezpečení vozidla

5.2.1 Systém Sherlog security

Společnost Sherlog je na trhu v oblasti zabezpečení vozidel již přes 30 let a čítá již přes 65.000 tisíc zabezpečených vozidel. Mezi největší výhody tohoto způsobu zabezpečení patří zejména unikátní nezarušitelná rádiová síť, Non-stop operační centrum a vlastní vyhledávací technika, mezi které spadá i letadlo. Díky těmto atributům má společnost Sherlog 98% úspěšnost dohledání s průměrným dohledáním do 2 hodin. Vozidla lze dohledat v ČR i v EU. V závislosti na zakoupeném druhu služby nabízí společnost i vícestupňové zabezpečení, což znamená kromě aktivní rádiové jednotky také přítomnost další jednotky pracující na jiném principu, např. GPS modul a v případě rušení signálu získá operační středisko výstražné hlášení o rušení jedné z jednotek, což znamená okamžitou aktivaci výjezdového vyhledávacího týmu, který se neprodleně snaží vozidlo dohledat a to i ve spolupráci s Policií ČR⁵⁵.

Technologie

Rádiová technologie SHERLOG se provozuje na neveřejných frekvencích a na vlastní infrastrukturu vysílačů po celé ČR, oproti konkurenčnímu řešení, které využívá veřejné frekvence určené pro GPS/GSM včetně vysílačů daného mobilního operátora.

Infrastruktura

Vlastní infrastruktura vysílačů, včetně vyhledávacích aut je strategicky rozmístěná pro pokrytí celé České republiky. Konkurenční společnosti využívají

⁵⁵ SHERLOG. *O vozidla se staráme již 30 let*. Online. Dostupné z: <https://www.sherlog.cz>. [cit. 2024-06-06]

infrastrukturu vysílačů mobilních operátorů, od kterých nakupují datové služby do SIM karet.

Rušení jednotek

Zloději často využívají v případě krádeže vozidla mobilní rušičky, které se dají na internetových stránkách sehnat od pár stovek korun do několika jednotek tisíc až desetitísiců. Díky unikátnosti vlastní technologie SHERLOG není tato ovlivněna a bez starosti lze vozidlo dohledat. Konkurencí využívané typy GPS/GSM jednotek si s mobilními rušičkami neporadí. Jednotky nedokážou přes rušení odeslat polohu vozidla a tím majiteli nebo dohledávacímu týmu znemožní lokalizovat odcizené vozidlo. Z důvodu využívání sítí mobilních operátorů, kteří mají nespočetné množství zařízení, obsahující SIM karty, není možné detekovat jedno rušené zařízení.

Cena služby

Pořizovací cena základního balíčku 15730,-Kč včetně DPH a roční provozní poplatek je ve výši 7865,-Kč včetně DPH. S tímto základním balíčkem lze vozidlo dohledat pouze na území ČR. V případě vícestupňového zabezpečení a možnosti vyhledání vozidla v zahraničí je jednorázová cena prémiového balíčku 39930,-Kč a roční poplatek ve výši 11979,-Kč.

5.2.2 Tajný spínač

Tajný neboli skrytý vypínač slouží ke zvýšení ochrany vozidla před odcizením. Jeho účelem je zamezení neoprávněnému nastartování tak že je přerušen konkrétní elektrický obvod a tím je znemožněna například dodávka paliva do motoru nebo znemožněna funkce jeho zapalování. Umístění tajného vypínače je ve většině případů konzultováno s uživatelem vozu a proto je vždy velmi těžké tento vypínač najít a umožnit tak nastartování vozidla. Pokud je vypínač umístěn na nepředpokládaném místě, jde o velmi účinné zabezpečení proti krádeži, vzhledem k zanedbatelné pořizovací ceně v řádu stokorun je tak i velmi vhodné k zabezpečení. Poměrně snadným a cenově velmi dostupným zařízením je také elektronický odpojovač baterie pomocí dálkového ovládání, ten s sebou však nese nevýhodu odpojení řídících jednotek vozu a jeho infotainmentu a tím i vymazání jeho paměti. To v případě moderních vozidel,

kde se ukládá mimo jiné i nastavení komfortních jednotek ve vozidle, paměti autorádia, času a dalších veličin, není až tak atraktivní řešení zabezpečení a je tedy vhodnější spíše pro starší automobily.

5.2.3 eCall

Přestože do nových vozidel je v rámci evropského společenství nyní tento bezpečnostní systém montován povinně už při výrobě, uživatelé starších vozidel, které tímto systémem nedisponují, mají taktéž možnost nechat si dodatečně eCall do vozidla namontovat. Není to tolik běžné vzhledem k neustálé obnově vozového parku, kdy starších vozidel ubývá. Navíc tento systém není zaryt do povědomí veřejnosti a spoustu lidí o něm vůbec neví. Jedná se však o finančně výhodné řešení u staršího vozidla, neboť jediná investice je jen do pořízení jednotky eCall a následný provoz už nevyžaduje žádné další náklady. Částka dodatečné montáže se pohybuje okolo čtyř tisíc korun českých.

O přítomnosti systému eCall ve vozidle zpravidla napovídá přítomnost tří tlačítek většinou v prostoru vnitřního osvětlení na stropnici. Jedná se o tlačítka se symbolem „i“, symbolem servisního klíče a třetí tlačítko s nápisem SOS, to bývá mnohdy červené nebo oranžové barvy.

Obrázek 6: Tlačítka systému eCall k manuálnímu užití⁵⁶



5.2.4 Air Tag

AirTag je v současné době velmi oblíbené sledovací zařízení velmi malých rozměrů vyvinuté společností Apple. Jedná se o nenápadný lokalizační přívěšek, který byl stvořen za účelem lokalizace drobných předmětů, které jejich uživatelé často ztrácejí, ať už jsou to klíče, peněženky či batohy. Tento přívěšek slouží vybranému okruhu uživatelů mající přístup do služby „Najít“ od společnosti Apple. Díky AirTagům tak lze tyto předměty nalézt, i když jsou vzdálené kilometry daleko. Jak vlastně tyto miniaturní přívěšky fungují? Princip je jednoduchý. AirTag v sobě nemá žádný GPS modul, ale komunikuje s iPhonem prostřednictvím Bluetooth a je také schopen předat polohu do aplikace Najít i přes ostatní iPhony kdekoli na světě. Uvnitř přívěšku se nachází knoflíková baterie CR2032, která zaručuje nabitý stav zařízení po dobu delší než jeden rok, o vybití baterie automaticky uživatele upozorní jeho iPhone. Po jejím vybití jí lze snadno vyměnit za novou. Zařízení je navrženo tak, aby odolávalo vodě i prachu⁵⁷. Nejen z těchto důvodů se těší velké oblibě a čím dál více uživatelů ho užívá k ochraně svého majetku, mimo výše zmíněného jej také instalují do jízdních kol, elektrokoloběžek, ale také právě do automobilů, případně do jejich součástí, které

⁵⁶ Skoda-Kodiaq-2017-GER. Online. In: . 2017. Dostupné z: <https://autocatalogarchive.com/wp-content/uploads/2017/07/Skoda-Kodiaq-2017-GER.pdf>. [cit. 2024-08-04]

⁵⁷ FILIP, Jiří. *Pro začátečníky: Jak využít AirTag na maximum*. Online. 2022. Dostupné z: <https://www.letemsvetemapple.eu/2022/12/26/pro-zacatecniky-jak-vyuzit-airtag-na-maximum/all/#comments>. [cit. 2025-03-05]

bývají často předmětem krádeží, těmi jsou například přední světlomety, jejichž cena se neřídka pohybuje v částkách převyšujících sto tisíc korun českých. Z hlediska praxe je známo mnoho případů, kdy právě AirTag přispěl k nalezení odcizených věcí. Obrovskou výhodou jsou jeho velmi malé rozměry a lze jej tak ukrýt či nalepit prakticky kamkoliv, dále pořizovací cena od 890 korun českých, což je cena více než přijatelná vzhledem k tomu, jaké možnosti nám nabízí.

Nevýhodou však je, že lze jeho správnou funkci využívat jen za podmínky, že se v jeho okolí pohybují mobilní telefony iPhone, což může například v nějaké odlehlé lokalitě bez pohybu osob znemožnit jeho správnou funkci. Nicméně v současnosti už je na trhu několik podobných zařízení pracujících i pod operačním systémem Android a lze jejich funkci využívat obdobně jako AirTag za využití jakýchkoliv jiných mobilních telefonů kromě iPhonů.

6 Příklady nálezu odcizených vozidel v praxi

6.1 Za použití systému eCall

Dne 22. 7. 2022 byly na základě oznámení ze strany poškozeného místním oddělením Vokovice zahájeny úkony trestního řízení pro přečin krádeže dle § 205 odst. 1, písm. b), odst. 3 trestního zákoníku⁵⁸. Dle oznamovatele se měl neznámý pachatel dne 22. 7. 2024 v průběhu noci v Praze 6 dopustit krádeže motorového vozidla LAND ROVER RANGE ROVER SPORT 3.0 SDV6 a odjet s ním neznámo kam. Vyhodnocením kamerových záznamů z místa události bylo zjištěno, že dne 22. 7. 2022 v čase 04:46 hod. s vozidlem odjíždí dva neznámí muži. K případu bylo zajištěno množství dalších kamerových záznamů, na kterých byl zjištěn výskyt doprovodného vozidla a trasa odjezdu odcizeného vozidla, jehož pohyb byl zadokumentován z Prahy 6 až do Kralup nad Vltavou, kde jeho cesta končí. Pátrání v místě posledního výskytu nepřineslo kladných poznatků k jeho výskytu ani nálezu. Policejní orgán od distributora vozidel Land Rover vyžádal IMEI vozidla navázané na systém eCall, po jehož zjištění vyžádal ve smyslu § 88a odst. 4 Trestního řádu⁵⁹ jeho lokalizaci cestou servisního útvaru. „Zkratka IMEI znamená International Mobile Equipment Identity, což je jedinečný identifikátor složený z 15 číslic pro mobilní zařízení. Každému zařízení je přiděleno jedinečné číslo, aby jej bylo možné jednoznačně identifikovat“⁶⁰. Vyhodnocením telekomunikačního provozu došli kriminalisté ke zjištění, že trasa jízdy odcizeného vozidla se shoduje s kamerovými záznamy a dne 22. 7. 2022 a vozidlo skutečně dojelo do Kralup nad Vltavou. Dne 23. 7. 2022 však bylo vozidlo lokalizováno v jedné z ulic v Praze 9, kde se nacházelo až do dne 14. 8. 2022. Po vozidle bylo kriminalisty prováděno pátrání v lokalitě, kde se dle eCall mělo nacházet, využito bylo i speciálně upravené služební vozidlo určené k vyhledávání, avšak ani tentokrát nedošlo k nálezu. V dané lokalitě se nacházelo několik uzavřených a oplocených objektů a domů s podzemními garážemi, kde mohlo být vozidlo ukryto a bylo tak nezbytné provést přesnou lokalizaci vozidla. Ke spolupráci tedy bylo dne 15. 9. 2022 přizváno

⁵⁸ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 60. ISBN 978-80-7488-424-5

⁵⁹ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 166. ISBN 978-80-7488-424-5

⁶⁰ MARCINM. *IMEI vs. IMSI - Zprávy - IMEI.info*. Online. 2023. Dostupné z: <https://www.imei.info>. [cit. 2024-08-22]

specializované pracoviště zaměřující se na vyhledávání telekomunikačních zařízení za použití tzv. IMSI catcheru. „IMSI odkazuje na *International Mobile Subscriber Identity*, často zkráceně *IMSI*. Číslo má také délku 15 číslic. Je však možné, že v některých případech může být pouze 14 číslic. Je to jedinečné číslo uložené v 64bitovém poli na SIM kartě, které identifikuje zákazníka telefonní sítě“⁶¹.

Specialisty byl potvrzen předpoklad, že se vozidlo nachází v uváděné lokalitě a byl označen konkrétní bytový dům s podzemní garáží, kde bylo odcizené vozidlo po chvíli skutečně nalezeno, avšak s nepřislušnými registračními značkami, které byly několik dní před krádeží také odcizeny. Při následném ohledání vozidla⁶² došlo k zajištění velkého množství stop, jako jsou pachové, daktyloskopické a genetické, v neposlední řadě byly nalezeny příslušné registrační značky, které byly pachateli sejmuty a ukryty pod gumovými koberečky za předními sedadly. Pozdějším šetřením zjistili policisté překvapující informace o pachateli, který si se zneužitou identitou opatřil padělané doklady, zajistil si pronájem parkovacího místa za využití několika prostředníků a je tak zřejmé, že se na krádež vozidla důkladně připravil. Operativní cestou byla zjištěna skutečná identita pachatele, který je zkušeným zlodějem a v době krádeže tohoto vozidla byl prověřován a vyšetřován v souvislosti s krádežemi několika dalších, kdy má na kontě i obecné ohrožení a násilí proti úřední osobě způsobené ujížděním před policejními vozidly a najížděním na samotné policisty. Toho času se však od 28. 7. 2022 nacházel ve výkonu trestu odnětí svobody za několik předešlých krádeží. Z výsledků osob užívajících uvedené podzemní garáže vyplynulo, že toto místo sloužilo delší dobu jako skrýš odcizených vozidel, mimo jiné i totožného vozidla bílé barvy, který byl zajištěn s ukrajinskými registračními značkami, padělanými ukrajinskými doklady a změněnými identifikátory. Dosud tak není jasné, kolik jich bylo tímto pachatelem odcizeno, ale je zřejmé, že se tímto podařilo rozkrýt alespoň část organizované skupiny dopouštějící se krádeží motorových vozidel sofistikovaným způsobem včetně padělání dokladů. Hlavní pachatel této skupiny je osobou velmi nebezpečnou s bohatou trestní minulostí. Obvodní soud pro Prahu 6 jej dne 16. 4. 2024 uznal vinným z výše uvedeného skutku a uložil mu nepodmíněný trest odnětí svobody v délce trvání 69 měsíců a dále trest propadnutí věci, tedy zajištěné finanční hotovosti převyšující částku 120.000,-Kč.

⁶¹ MARCINM. *IMEI vs. IMSI - Zprávy - IMEI.info*. Online. 2023. Dostupné z: <https://www.imei.info>. [cit. 2024-08-22].

⁶² *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 187. ISBN 978-80-7488-424-5

Toto je jeden z mnoha případů, kdy bylo zabezpečovacího systému eCall využito v kriminalistické praxi za účelem úspěšného vyhledání odcizeného vozidla a dopomohlo tak k rozkrytí zločinecké struktury v oblasti autokriminality. Byť se jedná o systém vyvinutý za účelem ochrany života a zdraví uživatelů motorových vozidel, je také významným pomocníkem v boji proti trestné činnosti.

6.2 Za použití systému Sherlog

V čase 02:45 hod. byl bez vědomí nic netušícího majitele automaticky aktivován systém ochrany SHERLOG u vozidla BMW X5, který byl volně zaparkován v jedné z ulic na Praze 6 a odtud odcizen neznámým pachatelem. Operačním střediskem byl majitel telefonicky vyrozuměn o aktivaci systému ochrany Sherlog s dotazem, zda je poplach oprávněný a zda opravdu došlo k odcizení. Ten operačnímu středisku potvrdil, že vozidlo skutečně nestojí na místě, kde ho zaparkoval a oba klíče se nachází doma. Poškozený byl tedy požádán, aby odcizení neprodleně oznámil na tísňovou linku 158, aby bylo vozidlo ihned vyhlášeno do celostátního pátrání a následně byly ve věci místním oddělením Policie ČR Vokovice zahájeny úkony trestního řízení pro trestný čin krádež. Operační centrum Sherlog do místa pohybu odcizeného BMW vyslalo několik vyhledávacích vozidel a o pohybu informovalo také operačního důstojníka PČR, který následně informoval hlídky v terénu, které tak měly k dispozici aktuální pohyb vozidla. Ve spolupráci s PČR bylo vozidlo dohledáno v ulici Sokolovská v Praze 8. Na místě byl zadržen pachatel s rušičkou signálu GPS a GSM. Doba od aktivace systému ochrany do zadržení byla pouhá jedna hodina a pachatel byl následně obvodním soudem pro Prahu 6 za tento trestný čin pravomocně odsouzen. Díky pořízení elektronického zabezpečení vozidla, které sice není úplně levnou položkou, tak došlo k ušetření majetkové hodnoty ve výši více než 1 milion korun českých a vozidlo se tak vrátilo v rekordním čase zpět majiteli v nepoškozeném stavu.

7 Zařízení užívané k překonání elektronického zabezpečení

Jsou to taková zařízení, která nebyla jejich výrobce primárně vyrobena k takovému účelu, aby sloužila k nelegální trestné činnosti, ale jejich funkce byla kriminálně závadovými osobami k takové činnosti zneužita. Původním záměrem výrobců bylo spíše usnadnění a rozšíření možností uživatelů nejrůznějších elektronických zařízení. Většinu z těchto zařízení lze naprosto legálně pořídit na trhu a my si představíme ty nejoblíbenější a nejhojněji užívané právě pro vloupání do vozidel. Níže je výčet nejhojněji užívaných zařízení pachatelů krádeží, který vychází z kriminalistické praxe autora.

7.1 Flipper Zero

Jedná se o v současnosti nejoblíbenější zařízení k překonání elektronického zabezpečení vozidel, mezi kriminálně závadovými osobami páchající trestnou činnost na úseku autokriminality. Flipper Zero lze zcela legálně pořídit v základním provedení za částku kolem šesti tisíc korun českých a výdrž zařízení je až 28 dní na jedno nabití. Jde o přenosný multifunkční nástroj, který se na první pohled tváří jako hračka, proto nebudí ani mezi většinou kontrolujících policistů přílišnou pozornost. O to víc dokáže překvapit tím, že hravě zvládne hackování „(*hackování = nestandardní použití aplikace nebo počítačového systému, kdy se jedná o ilegální průnik pomocí prolomení digitální ochrany*)“⁶³) digitálních věcí, jako jsou rádiové protokoly, systémy řízení přístupu, hardware a další. Je plně open source (open source = software s otevřeným zdrojovým kódem⁶⁴) a přizpůsobitelný, takže jej lze rozšířit o další funkce. Flipper zero je plně autonomní a lze jej ovládat pomocí pětítlačítkové směrové šipky bez potřeby užití dalších zařízení jakou jsou počítače nebo smartphony a hlavní funkce jsou tak k dispozici z hlavní nabídky zobrazované na 1,4 palcovém monochromatickém LCD displeji. Nicméně lze ho ovládat i pomocí například smartphonu nebo tabletu, avšak vždy musí být zařízení přítomno například v kapse a ovládání mobilním telefonem je tak ještě mnohem nenápadnější. Flipper má integrovanou vícepásmovou anténu, což

⁶³ Computer hacking - Wikisofia. Online. Dostupné z: <https://wikisofia.cz>. [cit. 2024-08-09]

⁶⁴ IT SLOVNÍK. Co je to Open source? - Slovník cizích slov. Online. Dostupné z: <https://it-slovník.cz>. [cit. 2024-08-08]

z něj dělá výkonný transceiver s dosahem až 50 metrů. Transceiver nazýváme zařízení, které v telekomunikačním prostředí dokáže vysílat i přijímat. Tento název je odvozen z anglických slov TRANSmitter (vysílač) a reCEIVER (přijímač). Jeho pracovní rozsah je pod 1 GHz (Gigahertz – jednotka frekvence, používá se pro udávání frekvence signálu), což je provozní rozsah pro širokou škálu bezdrátových zařízení a systémů kontroly přístupů, jako jsou dálková ovládání garážových vrat, závory, dálkové bezklíčové systémy a vzhledem k tomu, že pracuje mimo jiné i na frekvencích 433 MHz a 868 MHz, které využívá většina automobilek pro bezklíčové ovládání vozidel, lze za určitých podmínek načítat a ukládat pro další použití i signály těchto klíčů. Uživatelem lze rozšířit jeho možnosti instalací dalších aplikací pro čtení dat z dalších zařízení a lze tak ovládat např. meteostanice, chytré zásuvky či žárovky nebo třeba domovní zvonky. Zařízením Flipper lze také klonovat nízkofrekvenční bezkontaktní karty, které jsou hojně používány ve starých systémech kontroly přístupu po celém světě. Byť je tento systém zastaralý a hloupý, používá se dodnes, nemá žádný ověřovací mechanismus, což umožňuje, aby jej kdokoliv četl, klonoval a emuloval (Emulace = napodobení činnosti jednoho zařízení pomocí jiného zařízení, které k tomuto účelu není původně určeno). Pomocí integrovaného čipu NFC („NFC je zkratka pro anglický výraz *Near Field Communication*, jedná se o bezdrátovou technologii umožňující rychlou a zabezpečenou výměnu dat na krátkou vzdálenost“⁶⁵) dokáže klonovat například i platební karty. Kromě načtení je schopen ukládat je do paměti pro pozdější emulaci. Majitelé přístroje Flipper Zero si mohou na dálku sdílet ID načtených karet s ostatními uživateli Flipper Zero. Firmware (Firmware = data uložená v paměti zařízení, na základě kterých je schopno fungovat) tohoto zařízení lze samozřejmě i následně updatovat v různých stupních ať už ve verzích zdarma nebo v těch placených, tím se možnosti této „hračky“ velmi výrazně rozšiřují a lze pak i dešifrovat různé signály, které v základním nastavení firmawaru Flippera dešifrovat nejdou. Od toho se odvíjí velikost potřebné SD karty⁶⁶. Na obrázku č. 7 je zobrazeno zařízení Flipper zero.

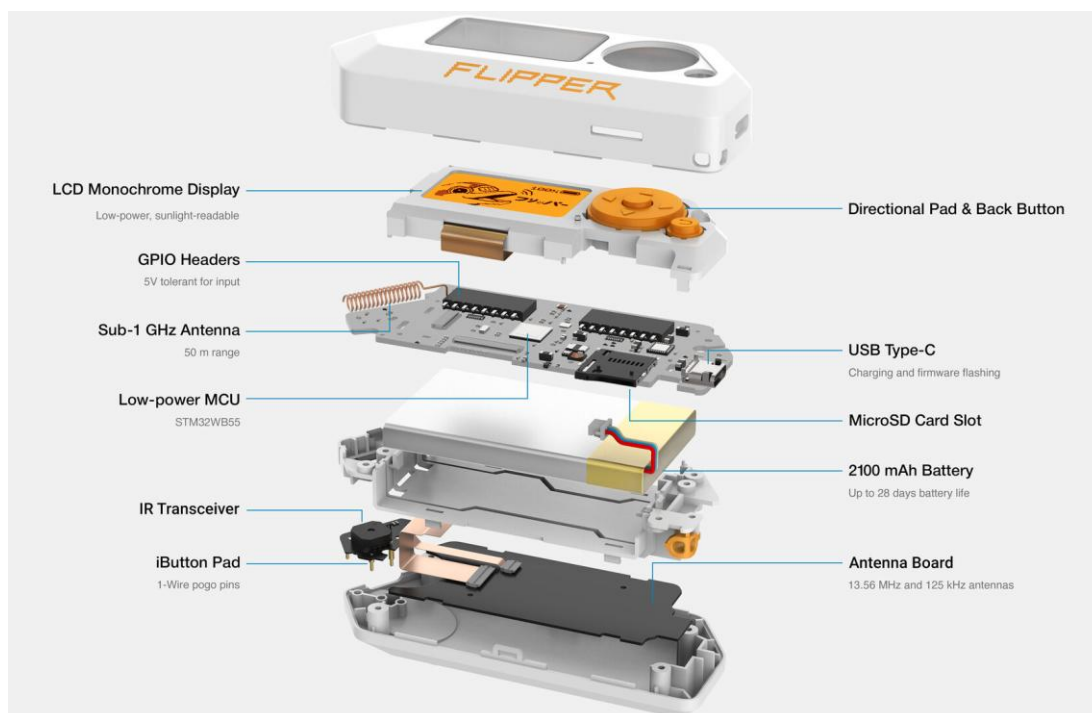
Příklad použití Flipper zero při krádeži vozidla Honda Civic.⁶⁷

⁶⁵ PATRON-PRO. *Co je to NFC?* Online. Dostupné z: <https://www.patronpro.cz>. [cit. 2024-08-08]

⁶⁶ FLIPPER ZERO. *Portable Multi-tool Device for Geeks*. Online. Dostupné z: <https://flipperzero.one/>. [cit. 2024-08-08]

⁶⁷ ISTROSEC. *Stealing Honda Civic using Flipper Zero CVE-2022-27254*. YouTube. 2022. Dostupné z: <https://www.youtube.com/watch?v=2bb45r2Cbh4&t=83s>. [cit. 2025-03-18]

Obrázek 7: Zařízení Flipper zero⁶⁸



7.2 Pandora

Jde o zařízení fungující na vzdáleném rádiovém kódování a dá se říci, že to je jakýsi jednodušší předek zařízení Flipper zero, který proti němu dokáže minimum věcí. Jedná se o velmi malé zařízení, které lze schovat do dlaně. Má malý displej a lze jej propojit s mobilním telefonem, kde je ovládání mnohem jednodušší. Toto zařízení umí kopírovat signál klíče starších vozidel a ukládá jej pro další použití. Teoretický dosah zařízení se liší podle jednotlivých modelů, ale v ideálních podmínkách je udáváno až do vzdálenosti 2 kilometrů. V městské zástavbě a existenci značného množství různých rádiových signálů je dosah logicky mnohem menší. Přístroj lze využít k vloupání a krádeži vozidel bez jejich poškození a to za užití lsti, tedy překonání uzamčení pomocí načtení kódu originálního autoklíče a následnému užití, vozidlo tak jde jak odemknout, tak i uzamknout⁶⁹. V některých případech byla zadokumentována i možnost nastartování, což se u novějších vozidel řeší vyšší mírou šifrování a tento přístroj si tak

⁶⁸ FLIPPER ZERO. *Portable Multi-tool Device for Geeks*. Online. Dostupné z: <https://flipperzero.one/>. [cit. 2024-08-08]

⁶⁹ CODEGRABBER. *Codegrabber Pandora DXL open Mazda*. YouTube. 2021. Dostupné z: <https://www.youtube.com/watch?v=6KTXmx68uM0>. [cit. 2025-03-18]

s novějšími vozidly neporadí. Z tohoto důvodu už je nyní znatelný úbytek užívání zařízení Pandora, neboť už je prostě zastaralé a technologický vývoj přinesl na trh mnohem zdačnější nástupce.

Dalšími zařízeními s obdobnou funkcí jsou např. MagicCar, Alligator apod.

Na obrázku č. 8 je zobrazeno zařízení Pandora DXL v prodejní ceně 5.500,-Euro.

Obrázek 8: Zařízení Pandora DXL⁷⁰



7.3 Radiostanice Baofeng

V současnosti absolutně nejrozšířenější zařízení využívané k vloupání do vozidel, které nefunguje na jiném principu, než je blokování signálu originálního autoklíče vysílaného příslušnému vozidlu. Vysoká obliba pramení z velmi příznivé pořizovací ceny, která začíná na částce kolem 500 korun českých a naprosto jednoduchého ovládání, spočívající pouze v navolení požadované frekvence a následně ke stisknutí tzv. klíčovacího tlačítka, čímž dojde při pokusu o autorizované uzamčení vozidla k blokaci signálu a vozidlo tak zůstane neuzamčeno a pachatel má volný přístup do vozu. Zde je potřeba minimálně znalosti, na jaké rádiové frekvenci pracuje daná automobilka. Dalšími výhodami je možnost radiostanici při samotném užívání ukrýt např. do kapsy nebo pořízení větší antény, která zvýší dosah radiostanice, který byl vyšetřovacím pokusem zjištěn na vzdálenosti 25 metrů a to i za předpokladu, že radiostanice je od vozidla ve větší vzdálenosti než originální autoklíč. I toto zařízení

⁷⁰ Pandora Code Grabber DXL Model - Turbodecoder. Online. Dostupné z: <https://turbodecoder.com>. [cit. 2024-09-14]

prochází neustálým vývojem a na trhu je možné narazit na několik generací. Obrázek č. 9 z vlastního zdroje zachycuje jednu z mnoha zajištěných radiostanic i s předvolenými frekvencemi a tato rušička byla pachatelem použita v praxi při blokování uzamčení vozidla pomocí centrálního zamykání.

Obrázek 9: Radiostanice Baofeng



Zdroj: Vlastní, zajištěno v rámci trestního řízení

7.4 Výkonná rušička signálu

Několikrát došlo v praxi k setkání s vícepásmovými rušičkami signálu, které dokážou rušit signály typu GSM, GPS, 5G, 4G, 3G, 2G, WIFI, apod. Pořizovací cena takové rušičky se pohybuje v rozmezí od 15 tisíc korun českých, klidně až do výše 40 tisíc korun českých. Přes její velkou spotřebu díky vysokému výkonu má výhodu v napájení z 12ti voltové zástrčky ve vozidle. Velmi oblíbené jsou zejména mezi cizojazyčnými gangy, které na území České republiky dělali organizované nájezdy za krádežemi luxusních vozidel prémiových značek. Nevýhodou proti tomu bylo to, že tato rušička vyrušila nejen signál zabezpečovacího zařízení, pokud fungoval na bázi GPS/GSM, ale také mobilní telefon samotného zloděje, který tak nemohl uskutečnit hovor, ani používat navigaci. Vzhledem k neznalosti trasy mnohdy jednoduše zabloudili a byli tak dopadeni ještě dříve, než přejeli hranice naší republiky.

Na obrázku č. 10, opět z vlastního zdroje, je zajištěná taková rušička.

Obrázek 10: Výkonná rušička signálu



Zdroj: Vlastní, zajištěno v rámci trestního řízení

8 Rušičky a legislativa

Vzhledem k neustálému vývoji technických zařízení a změně postupu pachatelů trestné činnosti a jejich stále častějšího využívání speciálních technických prostředků ve vztahu k vloupání do vozidel a krádežím vozidel za užití těchto speciálních prostředků se podezřelí dopouštějí kromě trestného činu krádeže dle § 205/1 a) Trestního zákoníku⁷¹ také jiných trestných činů. Jedním z nich je trestný čin Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat dle § 231/1 a) trestního zákoníku⁷². Tedy si opatří nebo přechovává speciální prostředek vytvořený nebo přizpůsobený k neoprávněnému přístupu k počítačovému systému nebo k jeho části nebo k neoprávněnému zásahu do počítačového systému nebo nosiče informací neoprávněným užitím dat uložených v počítačovém systému nebo na nosiči informací, v úmyslu, aby jej bylo užito ke spáchání výše uvedeného trestného činu. Naplnění skutkové podstaty trestného činu je v tomto případě odůvodněno skutečností, že v současné době je téměř každé vozidlo z výroby vybaveno elektronikou (počítačový systém, nosič informací), řídicími jednotkami, čipy a komunikátory a pachateli zde hrozí trest odnětí svobody až na dvě léta.

Dalším trestným činem při použití některého ze speciálních zařízení je také neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací dle § 230 Trestního zákoníku⁷³. Zde je trestní sazba v případě úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě či jinému neoprávněný prospěch, ve výši až tří let.

⁷¹ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 60. ISBN 978-80-7488-424-5

⁷² *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 67. ISBN 978-80-7488-424-5

⁷³ *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. s. 66. ISBN 978-80-7488-424-5

9 Zjištění informovanosti veřejnosti v oblasti zabezpečení vozidel

Praktická část této práce se zabývá zjištěním, zda je veřejnost vlastníci nebo užívající motorové vozidlo má nějaké povědomí o zabezpečení vozidel a jakým způsobem si vlastní majetek zabezpečují. Dotazník o sedmi uzavřených a dvou otevřených otázkách byl vytvořen na webových stránkách společnosti Survio⁷⁴ a mezi laickou veřejnost distribuován prostřednictvím sociálních sítí. Platnost dotazníku byla dva kalendářní měsíce.

9.1 Cíl zkoumání

Cílem této části je oslovení laické veřejnosti, která vlastní nebo užívá automobil. Vzhledem k tomu, že respondenti s policejní praxí budou mít podstatně větší znalosti v oblasti zabezpečení vozidel a jeho překonání, byla pro oblast respondentů záměrně zvolena spíše laická veřejnost, aby výsledky byly co nejvěrohodnějším odrazem společnosti. Cílem zkoumání je také zjištění, jestli vůbec a jakým způsobem si majitelé svá vozidla zabezpečují, či tuto starost úplně vypustí díky sjednanému pojištění vozu proti krádeži. Byly tedy stanoveny dvě hypotézy. První hypotéza spočívá v tom, že většina dotazovaných má své vozidlo nějakým způsobem zabezpečeno proti krádeži. Druhá hypotéza je domněnka autora, že laické veřejnosti není znám systém eCall, ani jeho funkce.

9.2 Stanovení otázek dotazníku

Otázky byly v dotazníku položeny takové, aby bylo dosaženo stanoveného cíle zkoumání.

⁷⁴ *Dotazník informovanosti v oblasti zabezpečení automobilů a znalos systému eCall*. Online. Dostupné z: <https://my.survio.com/N5A6S7T2V6M9F1G4C8J3/results>. [cit. 2025-03-18]

1) Jaké jste pohlaví?

Tato otázka byla položena z toho důvodu, aby byla zřejmá skladba respondentů

2) Vlastníte nebo užíváte vozidlo?

Tato otázka byla nezbytná pro další pokračování v dotazníku, pouze v kladném případě, v tom opačném by nebyl dotazovaný vhodným adeptem k dotazníkovému šetření.

3) Je vaše vozidlo vyrobeno od roku 2018 do současnosti?

Zde je otázka cílena na to, zda je vozidlo užívané dotazovaným opatřeno z výroby systémem eCall

4) Je vaše vozidlo pojištěno proti krádeži?

Tato otázka byla cílena v kombinaci s následující otázkou ke zjištění, zda dávají dotazované osoby přednost před vlastní iniciativou v oblasti zabezpečení svého vozidla nebo tuto zodpovědnost zcela vypouští a sjednají si pojištění proti krádeži a nemusí tak nic dalšího řešit.

5) Má vaše vozidlo nějaké zabezpečení proti krádeži?

Viz předešlá otázka.

6) Slyšel/a jste někdy o systému eCall ve vozidlech?

Tato otázka je jednou z klíčových ke zjištění informovanosti motoristické veřejnosti o tomto systému.

7) Víte k čemu eCall slouží?

Podpurná otázka k té předešlé, kde se podaří zjistit, zda respondenti znají funkci tohoto bezpečnostního systému.

8) Máte povědomí o možnostech hackingu elektronického zabezpečení automobilů? Pokud ano, jak se chráníte?

Tato otázka cílí na vědomí majitelů vozidel, zda tuší, jak je snadné překonat elektronické zabezpečení jejich vozu, zda jsou obezřetní a jakým způsobem se proti tomu chrání.

9) Víte, jak systém eCall funguje v případě nehody? Popište ho stručně

Tato otázka má potvrdit odpověď otázky č. 7, že dotazovaný skutečně ví, k čemu tento systém slouží.

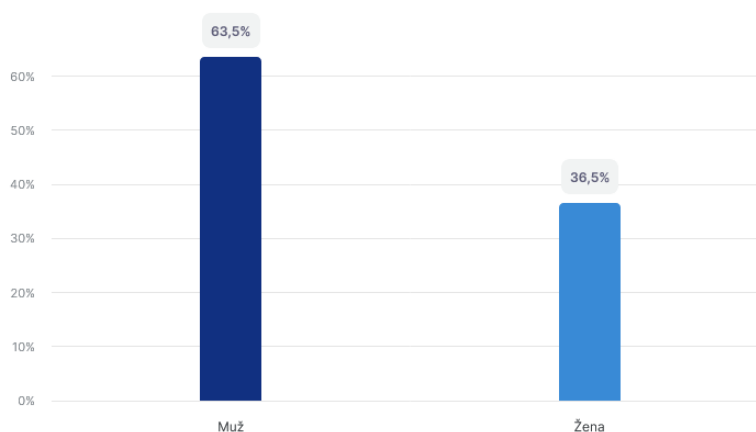
9.3 Vyhodnocení odpovědí na jednotlivé otázky

Vyhodnocení proběhlo formou analýzy respondentů, na základě které byly konstatovány závěry zjištěné z těchto odpovědí. Grafy jednotlivých odpovědí jsou přílohou pod čísly 1 až 7.

Otázka č. 1) zde je zastoupen větší podíl mužů s hodnotou 63,5%, oproti ženám, kterých bylo dotázáno 36.5%.

Graf 2: Pohlaví respondentů

1. Jaké jste pohlaví?

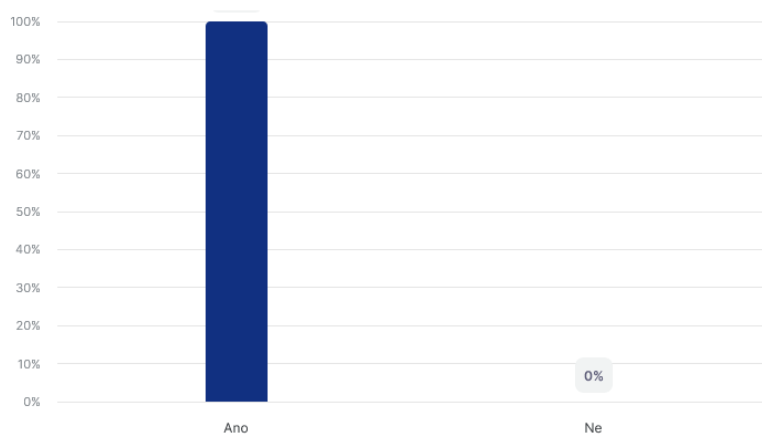


Zdroj: vlastní zpracování

Otázka č. 2) vzhledem k podmínce kladné odpovědi k pokračování v dotazníku je odpověď ano zastoupena 100%.

Graf 3: Vlastníte nebo užíváte vozidlo?

2. Vlastníte nebo užíváte vozidlo?

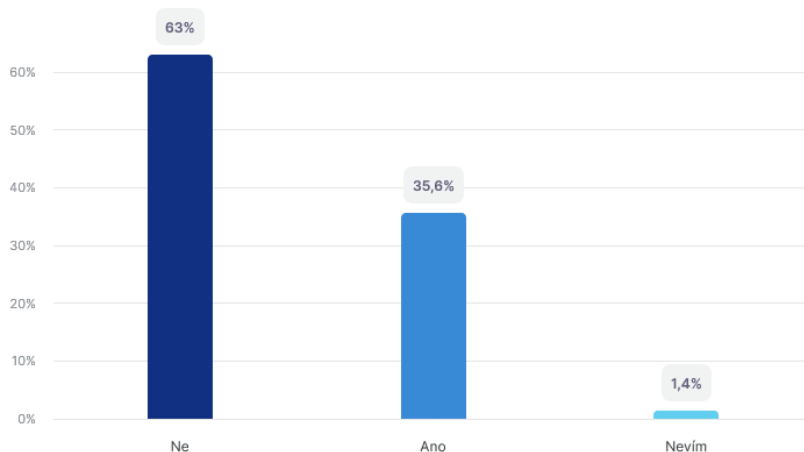


Zdroj: vlastní zpracování

Otázka č. 3) zde je 35,6% odpovědí kladných, tedy více než třetina dotazovaných s největší pravděpodobností vlastní vozidlo disponující systémem eCall již z výroby, 63% vlastní vozidlo starší a 1,4% netuší jaké je stáří jeho vozu.

Graf 4: Stáří užívaného vozidla

3. Je vaše vozidlo vyrobeno od roku 2018 do současnosti?

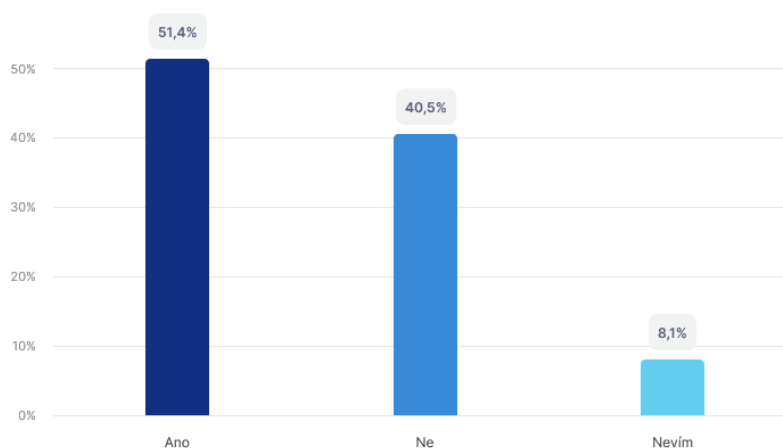


Zdroj: vlastní zpracování

Otázka č. 4) u této otázky je velmi překvapující výsledek s nadpoloviční většinou, kdy je vozidlo dotazovaného pojištěno proti krádeži a to celých 51,4%, přestože dle předchozí odpovědi vlastní 63% dotazovaných vozidlo starší sedmi let. 40,5% nemá vozidlo proti krádeži pojištěno a 8,1% netuší, jestli takové pojištění má sjednáno.

Graf 5: Dotaz na pojištění vozidla

4. Je vaše vozidlo pojištěno proti krádeži?

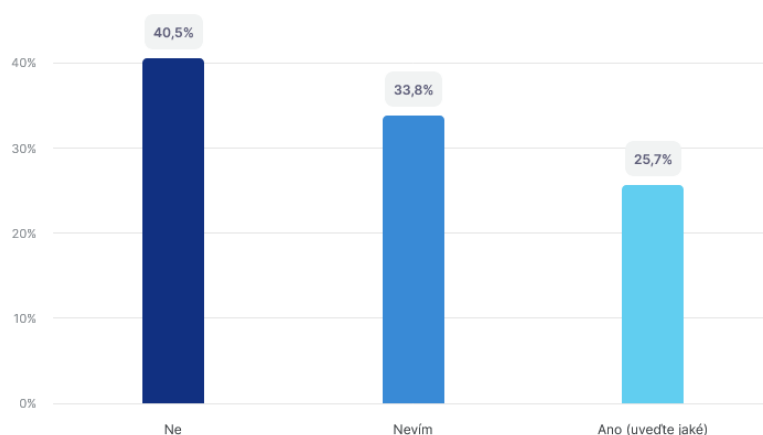


Zdroj: vlastní zpracování

Otázka č. 5) v návaznosti na předešlou otázku se jeví logické, že 40,5% dotazovaných nemá žádné zabezpečení vozidla proti krádeži. Pouhých 25,7% uvedlo, že jejich vozidlo nějaké zabezpečení má a trochu zarážející je fakt, že 33,8% dotazovaných vůbec neví, zda je jejich vozidlo zabezpečeno.

Graf 6: Dotaz na zabezpečení vozidla proti krádeži

5. Má vaše vozidlo nějaké zabezpečení proti krádeži?

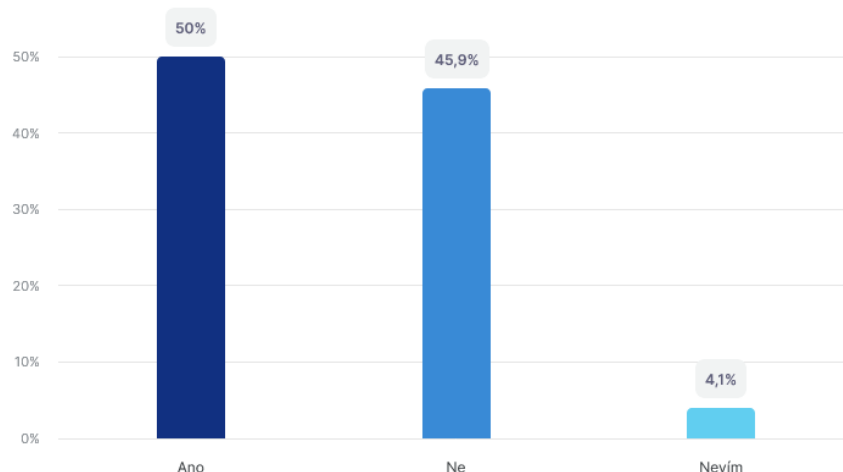


Zdroj: vlastní zpracování

Otázka č. 6) tato otázka přinesla překvapivé zjištění, že rovných 50% respondentů už o systému eCall slyšelo. Oproti tomu 45,9% o něm neslyšelo a 4,1% neví.

Graf 7: Dotaz na systém eCall

6. Slyšel/a jste někdy o systému eCall ve vozidlech?

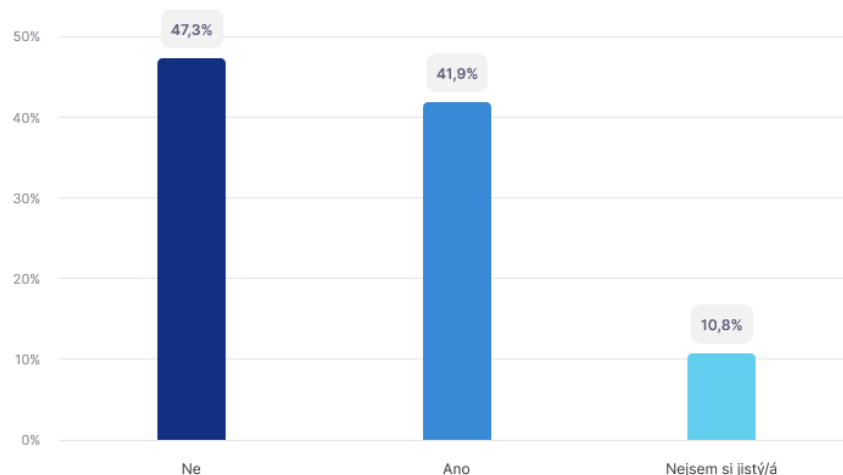


Zdroj: vlastní zpracování

Otázka č. 7) přestože dle předešlé otázky polovina dotazovaných o systému eCall slyšela, tak jen 41,9% ví, k čemu tento systém slouží. 47,3% to neví a 10,8% si není jistá.

Graf 8: Dotaz na funkci eCall

7. Víte k čemu systém eCall slouží?



Zdroj: vlastní zpracování

Otázka č. 8) zde byla možnost volných odpovědí, takže nelze vyvodit jednoznačný závěr, avšak drtivá většina uvedla, že o hackingu nemá tušení a nijak se proti němu nechrání. Ti co povědomí mají tak se proti němu nijak nechrání, důvěřují plovoucímu kódu klíče, nebo spoléhají na pojištění. Objevilo se i několik odpovědí, ve kterých se dotazovaní mylně domnívají, že s ohledem na stáří jejich vozidla se jich tato možnost netýká a vzhledem k minimálnímu množství elektroniky tak automobiloví hackeři nemají co překonávat. Jen malá část dotazovaných si je vědoma této možnosti překonání zabezpečení a podnikají základní kroky k manuální kontrole funkčnosti například centrálního zamykání.

Otázka č. 9) tato otázka potvrdila odpovědi otázky č. 6, ve které 50% dotazovaných uvedlo, že o systému eCall slyšelo, zde taktéž rovných 50% dotazovaných správně popsalo funkci tohoto systému. Někteří ho mylně považují za zabezpečovací systém, který v případě krádeže vyrozumí majitele.

9.4 Vyhodnocení hypotéz

K vyhodnocení hypotéz byly použity odpovědi z dotazníku, které byly podrobeny analýze. Autorem byly formulovány dvě hypotézy. První spočívala v předpokladu, že většina dotazovaných má své vozidlo nějakým způsobem zabezpečeno proti krádeži. Vyhodnocením otázek 4 a 5 byl vyhodnocen závěr, že pouhých 25,7 % respondentů uvedlo, že je jejich vozidlo opatřeno nějakým zabezpečením. Oproti tomu 40,5 % uvedlo, že jejich vůz žádné zabezpečení nemá. Přibližně třetina dotazovaných nemá tušení o zabezpečení jejich vozu, nelze tak vyloučit, že jej má, ale ani potvrdit. S tímto faktem koreluje i výsledek otázky č. 4, kdy nadpoloviční většina respondentů uvedla, že mají vozidlo proti krádeži pojištěno. Hypotéza č. 1 se tak nepotvrdila. Druhá hypotéza, jejíž podstata spočívala v erudici motoristické veřejnosti systému eCall, předpokládala, že bude podstatně nižší než u poloviny dotazovaných. Velmi překvapivým výsledkem otázky č. 6 tak bylo, že rovným 50ti % dotazovaných je tento systém znám, což bylo potvrzeno i následujícími otázkami č. 7 a volnou otázkou č. 9. Tato hypotéza se tak ani nepotvrdila, ani nevyvrátila.

9.5 Výsledek zkoumání

Výsledkem zkoumání bylo zjištěno, že většina dotazovaných vlastní starší vozidlo sedmi let, tedy s rokem výroby nižším než 2018 a nemá tedy z výroby instalovaný systém eCall. Většina má vozidlo pojištěno proti krádeži, což koresponduje s tím, že jen zhruba čtvrtina respondentů jej má nějak zabezpečeno. Z toho plyne, že o zabezpečení motorových vozidel není příliš velký zájem a to buď z důvodu klesajícího počtu krádeží vozidel, nebo je pro majitele snazší sjednat si pojištění proti krádeži. O systému eCall má povědomí polovina dotazovaných.

Závěr

Závěrem lze konstatovat, že zabezpečení majetku, v tomto případě vozidla, není v dnešní době vůbec jednoduché. A to navzdory tomu, že nabídka na trhu doslova překypuje různými prostředky a firmami, které nabízí nejrozličnější elektronické zabezpečení vozidel. Výrobci automobilů každoročně investují do vývoje v oblasti zabezpečení obrovské finanční prostředky, aby právě jejich vozidla byla co nejvíce zabezpečena a ochráněna proti krádeži. Dotazníkovým šetřením mezi motoristickou veřejností bylo zjištěno, že převážná část respondentů nepoužívá, kromě zabezpečení od výrobce, žádné dodatečné zabezpečení a spoléhá se na uzavřené pojištění proti krádeži vozidla.

Autor se osobně účastnil, coby policista služby kriminální policie a vyšetřování, školení v automobilce Škoda auto a.s. v Mladé Boleslavi, kde byly prezentovány nejnovější trendy a možnosti v oblasti zabezpečení vozidel. Jenže bohužel, stejně jako vývojáři technického zabezpečení automobilek i zloději se neustále zdokonalují, nahrává jim v tom i vývoj neustále nových a nových technologií, takže tento boj, jak se zdá, nemůže být nikdy vítězný. Velmi kladně lze hodnotit rozšíření systému eCall, který byť samotné krádeži nezamezí, tak je skvělým želízkem v ohni pro Policii v následném dohledání vozidla a tedy uchránění majetkové hodnoty. V praxi tak bylo tímto způsobem nalezeno velké množství vozidel a systém také dopomohl v několika případech k odhalení tzv. pojistného podvodu, kdy vozidlo fakticky odcizeno nebylo a jeho odcizení bylo jen fiktivní. Osobní domněnkou autora je, že značný úbytek odcizených vozidel a nárůst objasněnosti spojené s nálezy odcizených motorových vozidel lze přičítat právě tomuto systému a rozhodně kvituje rozšíření jeho užívání a povinnou instalaci.

Jaká je tedy ideální volba? Oblast zabezpečení motorového vozidla proti krádeži není vůbec jednoduchou otázkou. Ideálním stavem je vlastnit vozidlo, které je již z výroby osazeno systémem eCall, které by bylo vhodné opatřit ještě sekundárním zabezpečením v podobě např. zařízení AirTag, jehož pořizovací hodnota je minimální a to i přes zdařilou možnost lokalizace. V takovém případě jde o investici pouhých pár stokorun a vozidlo je v podstatě ochráněno, byť se tedy jedná pouze o zařízení, díky kterým lze vozidlo po krádeži lokalizovat a neplní funkci prevence proti krádeži. Doporučením je použít elektronické zabezpečení v kombinaci s tím mechanickým, ať už

se jedná o zámek převodové skříně, bezpečnostní fólie na oknech, vyleptané VIN na všech oknech. Dalším doporučením je deaktivace Keyless systému, který se nyní jeví jako největší slabina v oblasti zabezpečení vozidla a zlodějům tak velmi usnadňuje práci. Ochrana majetku by tak měla být na žebříčku hodnot výše než vlastní komfort. Jak již bylo zmíněno v úvodní části, vždy je lepší nějaké zabezpečení než žádné a čím více ho bude, tím je vyšší pravděpodobnost, že odradí pachatele od krádeže takového vozidla.

V této práci bylo probráno několik druhů elektronického zabezpečení vozidel, stejně tak i výčet jejich slabin a škála možností na jejich překonání. Nyní je na vlastním uvážení každého čitatele, který druh zabezpečení on sám považuje za nejvhodnější. Autor si rozšířil obzor jednak v možnostech elektronického zabezpečení vozidel, ale ještě více v oblasti jeho překonání, kdy tyto poznatky budou zcela jistě využívány v jeho kriminalistické praxi a budou zcela jistě předávány i jeho kolegům. Toto lze považovat za dosažení cíle této bakalářské práce.

Vzhledem k citlivosti zvoleného tématu nelze vypsát veškeré zjištěné skutečnosti, neboť velká většina jich podléhá přísnému utajení, ať už z hlediska autorských práv, tak z důvodu podepsané mlčenlivosti, proto jsou zde vykresleny jen ve velmi obecné rovině.

Na úplný závěr si autor dovoluje citovat pana Ing. Stanislava Čechráka ze společnosti ESSAtech s. r. o. - vynálezce Keyless defenderu a velkého odborníka na elektrotechniku, který říká: „existuje jedno jediné a stoprocentně spolehlivé zabezpečení automobilu, a to žádný automobil nemít.“

Seznam použitých zdrojů

Literární zdroje

1. CHMELÍK, Jan a kolektiv. *Rukověť kriminalistiky*. Plzeň: Aleš Čeněk, 2005. 532 s. ISBN 80-86898-36-9
2. IBL, Petr. *Kriminologie*. Karlovy Vary: Vysoká škola Karlovy Vary, 2014. 257 s. ISBN 978-80-87236-22-2
3. JELÍNEK, Jiří. *Trestní zákoník a trestní řád: s poznámkami a judikaturou: podle stavu k 1. 1. 2010*. Glosátor. Praha: Leges, 2009. 1216 s. ISBN 978-80-87212-22-6
4. Kolektiv autorů HSVB za redakce pplk. Dr. Bohuslava Němce. *Kriminalistická příručka*. 1. svazek, Druhé vydání. Brno: Kriminalistický ústav VB, 1967. 527 s. ČÚKK 791/66-EÚ EK 3594/66
5. MATOUŠKOVÁ, Ingrid; MORAVČÍK, L'ubomír, RAK, Roman a kol. *ECall - Inteligentný dopravný systém (aspekty právne, technické, informačné a psychologické)*. Bratislava: Magnet Press, Slovakia, 2015. 684 s. ISBN 978-80-89169-31-3
6. MUSIL, Jan a kolektiv. *Kriminalistika: vybrané problémy teorie a metodologie*. Praha: Policejní akademie České republiky, 2001. 309 s. ISBN 80-7251-080-0
7. NOŽINA, Miroslav. *Mezinárodní organizovaný zločin v České republice*. Praha: Themis. 2003. 407 s. ISBN 80-731-2018-6
8. PAJER, M. Zabezpečení vozidel. *Security magazín Časopis pro vaši bezpečnost*. Praha: FAMily media, 1999, roč. 5-6, č. 4, s. 7-19. ISSN 1210-8723
9. PORADA, Viktor. *Kriminalistika*. Brno: CERM, 2001. 746 s. ISBN 80-7204-194-0
10. PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. 1024 s. ISBN 978-80-7380-589-0
11. RAK, Roman a kol. *Krádeže vozidel: odhalování, vyšetřování a prevence*. Brno: CERM, 2001. 252 s. ISBN 80-7204-218-1
12. ŠKODA, Jindřich; VAVERA, František a ŠMERDA, Radek. *Zákon o policii s komentářem*. Plzeň: Aleš Čeněk, 2009. 397 s. ISBN 978-80-7380-160-1
13. ŠVÁBENSKÝ, Otakar. *Základy GPS a jeho praktické aplikace*. 1. vydání. Brno: CERM, 1995. 123 s. ISBN 80-214-0620-8

14. *Trestní předpisy [ÚZ 2020 č. 1389]*. ÚZ: úplné znění. Ostrava: Sagit, 2020. 480 s. ISBN 978-80-7488-424-5
15. VLK, František. *Anglicko-český technický automobilový slovník*. Auto-moto-profi. Praha: Computer Press, 2001. 201 s. ISBN 80-722-6522-9
16. VLK, František. *Lexikon moderní automobilové techniky*. Brno: Prof. Ing. František Vlk, DrSc., nakladatelství a vydavatelství, 2005. 344 s. ISBN 80-239-5416-4
17. WEIGEL, Ondřej. *Jak zabránit krádeži vašeho automobilu: mechanické a elektronické zabezpečení*. Praha: Computer Press, 2000. 78 s. ISBN 80-7226-349-8

Elektronické zdroje

1. *A Brief History of Car Security Systems*. Online. Dostupné z: <https://www.blackknighttracking.com/post/2019/07/10/a-brief-history-of-car-security-systems>. [cit. 2024-08-17]
2. AUTANET. *Jednoduchá finta, jak vám ukradnou auto*. Online. 2016. Dostupné z: <https://www.autanet.cz/autonews-jednoducha-finta-jak-vam-ukradnou-auto-3140>. [cit. 2024-07-23]
3. AUTOKLICECZ.CZ. *Co je to imobilizér?* Online. 2021. Dostupné z: https://www.autoklice.cz/clanek/co-je-to-imobilizer_100. [cit. 2024-07-23]
4. *Centrální zamykání vozidel*. Online. 2024. Dostupné z: https://www.autoprofi.cz/centralni-zamykani/?srsltid=AfmBOooCJ5_3XvZYT39DlBJWSlvE7BX3nlhWckZeXoOE-ogMQoEnWpIy. [cit. 2024-06-03]
5. *Computer hacking - Wikisofia*. Online. Dostupné z: https://wikisofia.cz/wiki/Computer_hacking. [cit. 2024-08-09]
6. ČESKO. *Zákon č. 273 ze dne 22. srpna 2012 o elektronických komunikacích. In Sbírka zákonů České republiky*. Online. 2012. Částka 94. Dostupné z: <https://www.zakonyprolidi.cz/cs/2012-273/zneni-20121001>. [cit. 2025-03-18]
7. ESSATECH, S.R.O. *Produkty ESSAtech, s.r.o.* Online. Dostupné z: <https://www.essatech.cz/wp/produkty/>. [cit. 2024-07-23]
8. FILIP, Jiří. *Pro začátečníky: Jak využít AirTag na maximum*. Online. 2022. Dostupné z: <https://www.letemsvetemapple.eu/2022/12/26/pro-zacatecniky-jak-vyuzit-airtag-na-maximum/all/#comments>. [cit. 2025-03-05]
9. FLIPPER ZERO. *Portable Multi-tool Device for Geeks*. Online. Dostupné z: <https://flipperzero.one/>. [cit. 2024-08-08]

10. *Ford Model T: Revoluce na čtyřech kolech*. Online. 2024-05-16. Dostupné z: <https://www.venclikovi.cz/ford-model-t-revoluce-na-ctyrech-kolech/>. [cit. 2024-08-27]
11. IT SLOVNÍK. *Co je to Open source? - Slovník cizích slov*. Online. Dostupné z: <https://it-slovník.cz/pojem/open-source#:~:text=Jako%20open%20source%20se%20ozna%C4%8Duj%C3%AD,kvalitativn%C4%9B%20srovnateln%C3%BD%20s%20placen%C3%BDmi%20alternativami>. [cit. 2024-08-08]
12. *Keyless Block - zařízení proti krádeži auta s bezklíčovým zamykáním*. Online. Dostupné z: <https://authoralarm.cz/produkty/keyless-block/>. [cit. 2024-07-23]
13. *Leach (automobile)*. Online. 2023-09-27. Dostupné z: [https://en.wikipedia.org/wiki/Leach_\(automobile\)](https://en.wikipedia.org/wiki/Leach_(automobile)). [cit. 2024-08-24]
14. MARCINM. *IMEI vs. IMSI - Zprávy - IMEI.info*. Online. 2023. Dostupné z: <https://www.imei.info/cs/news/imei-vs-imsi/>. [cit. 2024-08-22]
15. *Mtaplus - Problematika diagnostiky starších vozidel*. Online. Dostupné z: <https://www.mtaplus.cz/content/101-problematika-diagnostiky-starsich-vozidel>. [cit. 2024-07-23]
16. *Pandora Code Grabber DXL Model - Turbodecoder*. Online. Dostupné z: <https://turbodecoder.com/product/pandora-code-grabber-dxl-model/>. [cit. 2024-09-14]
17. PATRON-PRO. *Co je to NFC?* Online. Dostupné z: <https://www.patronpro.cz/co-je-nfc/>. [cit. 2024-08-08]
18. PC-IN PLZEŇ. *GSM - Slovník ICT pojmů*. Online, 12.09.2015. Dostupné z: <https://www.pcinplzen.cz>. [cit. 2024-08-22]
19. POLICIE ČR. *Mapa kriminality*. Online. Dostupné z: <https://kriminalita.policie.cz/>. [cit. 2024-07-01]
20. SAIDL, Jan. *Cebia: ověřená historie*. Online. B.r., 2024-05-16. Dostupné z: <https://www.autolexicon.net/cs/articles/cebia/>. [cit. 2025-03-04]
21. SAJDL, Jan. *ECall - autolexicon.net*. Online. Dostupné z: <https://www.autolexicon.net/cs/articles/ecall/>. [cit. 2024-09-14]
22. SECURITY MAGAZÍN. *Keyless systém - příliš vysoká cena za komfort?* Online. 2019. Dostupné z: <https://www.securitymagazin.cz/security/keyless-system-prilis-vysoka-cena-za-komfort-1404064481.html>. [cit. 2024-07-23]
23. SHERLOG. *O vozidla se staráme již 30 let*. Online. Dostupné z: https://www.sherlog.cz/?utm_source=seznam&utm_medium=cpc&utm_campaign=Search+%7c+brand&utm_content=sherlog&utm_term=sherlog. [cit. 2024-06-06]

24. Skoda-Kodiaq-2017-GER. Online. In: . 2017. Dostupné z: <https://autocatalogarchive.com/wp-content/uploads/2017/07/Skoda-Kodiaq-2017-GER.pdf>. [cit. 2024-08-04]
25. ŠVAMBERK, Jiří. *Diagnostická zásuvka OBD: Víte, k čemu slouží a co vše z ní můžete zjistit?* Online. 2019. Dostupné z: <https://www.tipcars.com/magazin/nase-tema/diagnosticka-zasuvka-obd-vite-k-cemu-slouzi-a-co-vse-z-ni-muzete-zjistit-20190227.html>. [cit. 2024-05-14]
26. TAYLORCOXX. *Replay útoky*. Online. 2017. Dostupné z: <https://www.tx.cz/slovník/isms/replay-utoky>. [cit. 2024-07-23]
27. TESLA. *Palubní kamera, režim Sentry a zabezpečení*. Online. 2024. Dostupné z: https://www.tesla.com/ownersmanual/model3/cs_cz/GUID-49096E34-97D2-4182-9414-2F7F4E88EE79.html. [cit. 2024-08-08]
28. TOPGIS. *GPS: globální satelitní navigační systém*. Online. Př. n. l. Dostupné z: <https://www.gisonline.cz/slovník/gps/>. [cit. 2024-09-14]
29. WIKIWAND. *SOS hláska - Wikiwand*. Online. Dostupné z: https://www.wikiwand.com/cs/articles/SOS_hl%C3%A1ska. [cit. 2024-06-27]
30. ZABEZPEČ AUTO. *Sběrnice CAN - co to je a jak to funguje?* Online. ZABEZPEC-AUTO.CZ. Dostupné z: <https://zabezpec-auto.cz/sbornice-can-co-to-je-a-jak-to-funguje/>. [cit. 2024-07-23]
31. ZVAŘIČ, Filip. *Úvod do hackování aut - Car hacking - Hacking lab*. Online. 2020-09-22. Dostupné z: <https://hackinglab.cz/cs/blog/uvod-do-hackovani-autcar-hacking/>. [cit. 2024-06-18]

Legislativní dokumenty

1. Zákon č. 40/2009 Sb., trestní zákoník
2. Zákon č. 141/1961 Sb., trestní řád
3. Zákon č. 273/2000 Sb., o Policii České republiky
4. Zákon č. 273/2012 Sb., o elektronických komunikacích

Seznam zkratek

CAN - Controled Area Network

DoS - Denial of Service

eCall - Emergency Call

ECU - Electronic Control Unit

GPS - Global Positioning System

GSM - Groupe Spécial Mobile

IMEI - International Mobile Equipment Identity

IMSI - International Mobile Subscriber Identity

KESY - Keyless Entry, Start and exit System

LED - Light Emitting Diode

MSD - Minimum Set of Data

NFC - Near Field Communication

OBD - On Board Diagnostic

OCIS - Open Car Information System

SIM - Subscriber Identity Module

VIN - Vehicle Identification Number

Seznam obrázků

Obrázek 1: schéma provedení útoku Relay Station Attack.....	25
Obrázek 2: Keyless deffender	26
Obrázek 3: OBD-II port ve vozidle.....	28
Obrázek 4: Klíč od vozidla Škoda Superb, ukrytý v nárazníku.....	30
Obrázek 5: Schéma funkce systému eCall	33
Obrázek 6: Tlačítka systému eCall k manuálnímu užití	38
Obrázek 7: Zařízení Flipper zero	45
Obrázek 8: Zařízení Pandora DXL	46
Obrázek 9: Radiostanice Baofeng.....	47
Obrázek 10: Výkonná rušička signálu	48

Seznam grafů

Graf 1 Statistika krádeží motorových vozidel na území ČR.....	15
Graf 2: Pohlaví respondentů.....	52
Graf 3: Vlastníte nebo užíváte vozidlo?.....	52
Graf 4: Stáří užívaného vozidla.....	53
Graf 5: Dotaz na pojištění vozidla	53
Graf 6: Dotaz na zabezpečení vozidla proti krádeži	54
Graf 7: Dotaz na systém eCall	54
Graf 8: Dotaz na funkci eCall	55