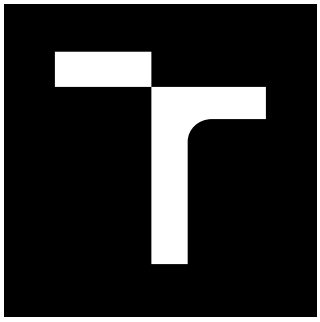
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2021 Bc. Nataliya Golovkova



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

NÁVRH PROTIOPATŘENÍ K ÚTOKŮM NA KONEKTIVITU VOZŮ

PROPOSAL OF CYBER ATTACK COUNTERMEASURES ON THE CONNECTED CARS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Nataliya Golovkova**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Tomáš Gerlich**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Telekomunikační a informační technika**

Ústav telekomunikací

Studentka: Bc. Nataliya Golovkova ***ID:*** 189046
Ročník: 2 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Návrh protiopatření k útokům na konektivitu vozů

POKYNY PRO VYPRACOVÁNÍ:

Diplomová práce bude zaměřena na návrh a implementaci protiopatření známých hrozeb pro napadení konektivních vozů. V teoretické části student nejprve analyzuje známé hrozby, útoky a používané techniky pro napadení konektivních vozů. Následně popíše obecnou architekturu konektivních vozů. V rámci praktické části realizuje návrh a implementaci modelů nejméně tří hrozeb v nástroji Microsoft Threat Modelling Tool nebo IriusRisk. Výběr hrozeb bude vycházet z analýzy v teoretické části práce. Následně student vytvoří návrh protiopatření k definovaným hrozbám.

DOPORUČENÁ LITERATURA:

[1] MACHER, Georg, et al. ISO/SAE DIS 21434 Automotive Cybersecurity Standard-In a Nutshell. In: International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2020. p. 123-135.

[2] SHOSTACK, Adam. Threat modeling: Designing for security. John Wiley & Sons, 2014.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 24.5.2021

Vedoucí práce: Ing. Tomáš Gerlich
Konzultant: Tomáš Trávníček, ŠKODA AUTO a. s.

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Diplomová práce je zaměřena na problematiku konektivních vozů a typy hrozeb které mohou nastat a jak se proti nim chránit. V teoretické části byl popsán obecný model auta. V další části práce byl vytvořen šablon v Microsoft Threat Modeling Tool s hrozbami a protiopatření k nim.

KLÍČOVÁ SLOVA

STDIDE, MS TMT, ECU, TCU, IriusRisk, DFD, Threat model

ABSTRACT

The diploma thesis is focused on the issue of connective cars and the types of threats that can occur and how to protect against them. The general part described the general model of the car. In the next part of the work, templates were created in the Microsoft Threat Modeling Tool with threats and countermeasures to them.

KEYWORDS

STDIDE, MS TMT, ECU, TCU, IriusRisk, DFD, Threat model

GOLOVKOVA, Nataliya. *Návrh protiopatření k útokům na konektivitu vozů*. Brno, 2021, 55 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Tomáš Gerlich,

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Návrh protiopatření k útokům na konektivitu vozů“ jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky

PODĚKOVÁNÍ

Ráda bych poděkovala konzultantovi diplomové práce panu Ing. Tomášovi Trávníčkovi ze společnosti ŠKODA AUTO a.s. za odborné vedení, konzultace, trpělivost, podnětné návrhy k práci a především jeho čas, který mi věnoval při realizaci této práce. Dále děkuji vedoucímu práce Ing. Tomášovi Gerlichovi za pedagogické vedení této práce.

Obsah

Seznam obrázků

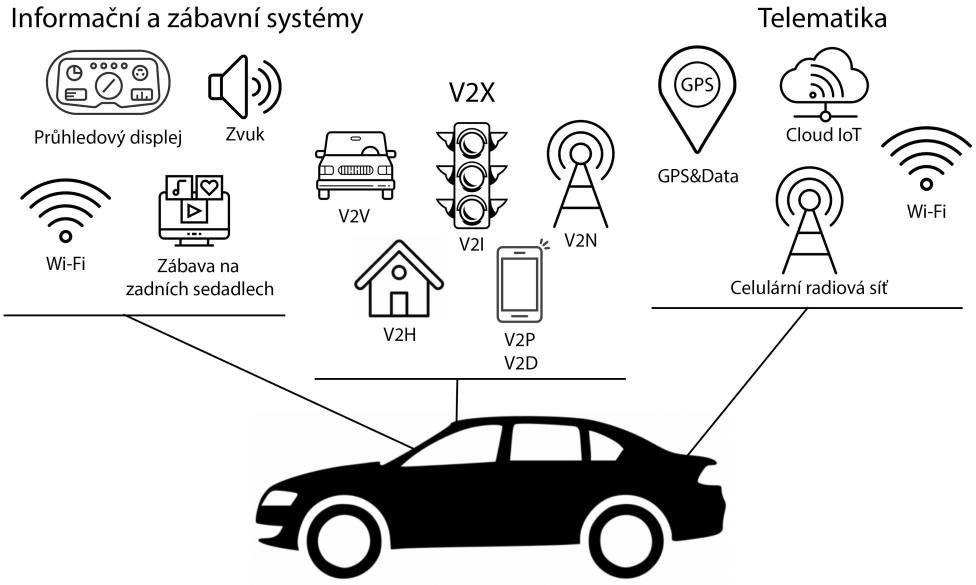
Seznam tabulek

Úvod

Tato diplomová práce se věnuje obecnému popisu konektivního vozu a jeho jednotkám, které lze zneužít pro útočníkovy účely. Následuje popis vybraných typu útoku, rozebraní modelu hrozeb a výběr, jaký nástroj je vhodné použít pro modelovaní v automobilovém průmyslu. Dále se práce zabývá výběrem nástroje vhodného pro modelování. Nástroje jsou srovnané v přehledných tabulkách na základě jejich vlastností. Ve druhé části je obecná implementace automobilového modelu v Microsoft Threat Modeling Tool pomocí existující šablony. Třetí část je zaměřena na vytvoření šablony se setříděnými hrozbami podle STRIDE. V poslední části práce byl vytvořen model s vlastni šablonou.

1 Konektivní vozidlo

Připojené vozy nabízejí širší škálu možností připojení než mnoho jiných připojených zařízení. Kromě toho, že svým uživatelům poskytují v reálném čase přístup ke všem druhům informací, mohou usnadnit kontakt mezi vozidlem a autorizovaným servisem a upozornit pohotovostní služby, pokud jste účastníkem nehody.
Připojené funkce vozidla spadají do několika kategorií viz Obrázek 1.1: **bezpečnost, navigace, infotainment, diagnostika/efektivita a platby.**



Obr. 1.1: Konektivní vozidlo [21]

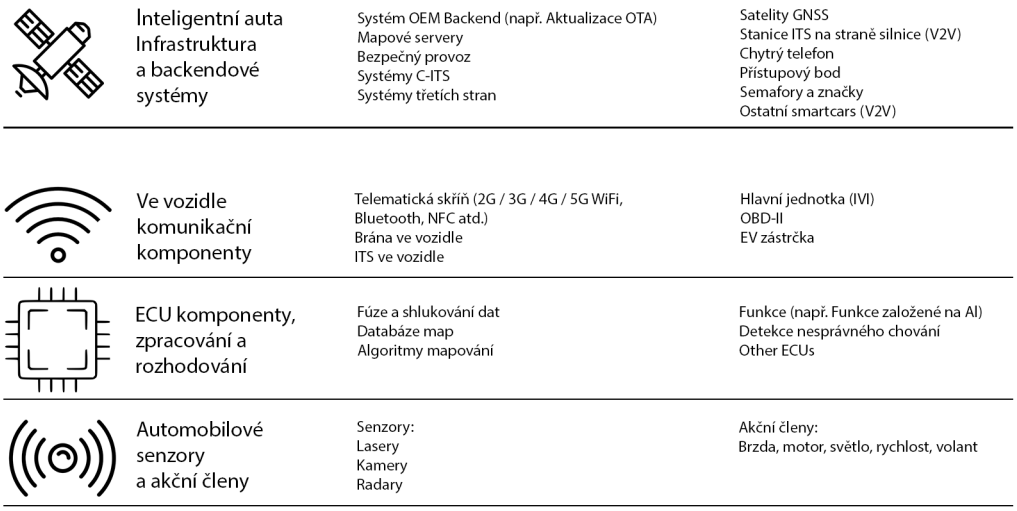
Satelitní navigační systém vašeho vozidla může mít funkci sledování provozu, která vás může upozornit na zpoždění na vaší trase a navrhnout alternativu, jak se jí vyhnout.
Pomocí **aplikace pro chytrý telefon** můžete také na dálku nastartovat auto před tím, než budete chtít nastoupit, aby se okna odmrazila a v kabině bylo teplo, aby bylo připraveno k odjezdu. Může také na dálku odemknout a zamknout auto, zapnout a vypnout blikající světla nebo alarmy, které pomohou najít auto na parkovišti.
Některé automobilové aplikace mohou také zaparkovat auto, pokud je potřeba jej umístit do malého prostoru nebo úzké garáže. Tyto systémy lze také použít k rezervaci vozidla k opravě a v některých případech k dálkové diagnostice poruch vozidla.
Automobily mají systém, který **informuje policii o dopravní nehodě**. Systémy používají data GPS k vyhledání vozidla, aby k němu bylo možné získat co nejrych-

lejší přístup.
Moderní připojená vozidla mohou vytvářet hot-spoty Wi-Fi, což umožňuje těm v autě a v jeho okolí využívat jeho přístup na internet.
Připojená auta se nejen připojují k lidem a službám, ale také k sobě navzájem a infrastruktuře silniční sítě. Autonomní vozidla použijí informace z kamer, laserů a radarů k vytvoření 3D digitální mapy svého okolí. Budou také komunikovat s automobily v jejich okolí, aby získala více informací o tom, zda se chystají zatočit, zrychlit nebo zabrzdit. Schopnost toho ve skutečnosti umožňuje autonomnímu vozidlu vidět skrz a předvídat lidi kolem sebe. Budou také moci přijímat informace ze semaforů, dopravních značek, značení jízdních pruhů a úseků silnic, abych věděli o dopravní zácpě nebo ostré zatáčce na silnici, než je půjde vidět [1].
Mnoho automobilek a technologických společností pracuje na samo-říditelných autech. Některá sériová vozidla již mají některé polo-autonomní prvky, které přispívají k bezpečnosti, například automatické nouzové brzdění, asistent udržování v jízdním pruhu, monitorování mrtvého úhlu, adaptivní tempomat a upozornění na hustý provoz.
K dosažení lepších schopností autonomního řízení se inteligentní automobily spoléhají na celou řadu technologií, včetně:

- **Senzory a akční členy:** zařízení, která mají různé funkce, jako je Detekce objektů a spouštění akcí atd.
- **Umělá inteligence:** Algoritmy, které umožňují elektronickým řídicím jednotkám a počítačům provádět různé úkoly.
- **Strojové učení:** algoritmy, které počítačům umožňují jednat a zvyšují jejich schopnost předvídat události nebo situace.
- **Cloud computing:** řešení, která poskytují přístup k běžným sadám zdrojů, jako jsou servery a aplikace, s minimálním úsilím o správu a interakcí s poskytovateli služeb.
- **Komunikace a sítě:** rádiové technologie a komunikační protokoly, které umožňují výměnu dat mezi různými entitami.

1.1 Referenční model

Inteligentní automobily, a zejména (částečně) autonomní vozy, které obsahují více elektronických řídicích jednotek (ECU) a komponent, se na první pohled mohou zdát příliš komplikované. Ačkoli jsou funkce inteligentních automobilů (jako je brzdění, řízení, zamykání dveří atd.) stejné pro všechna vozidla, každý OEM má ve vozidle svou vlastní architekturu a neexistuje žádná běžná a jedinečná architektura, kterou lze použít jako referenční model. Obrázek 1.2 ukazuje model od ENISA [2]



Obr. 1.2: Referenční model [2]

Popis vrtev referenčního modelu:

- Automobilové senzory a akční členy: Nejnižší úroveň architektury zahrnuje různé inteligentní automobilové senzory používané k monitorování jízdního prostředí shromažďováním údajů o okolí vozidla, jako jsou podmínky na silnici, vzdálenost k jiným objektům a vozidlům, globální navigační satelitní systémy (GNSS).
- ECU vozidla, komponenty pro zpracování a rozhodování: tato úroveň zahrnuje všechny hardwarové a softwarové komponenty, včetně AI, které se používají ke zpracování dat přijatých ze senzorů a akčních členů na úrovni vozidla (tj. Data shromážděná senzory) a Komunikační komponenty ve vozidle (například data přijatá z jiných stanic C-ITS), jakož i provedení příslušného rozhodnutí a jeho přenos do příslušného akčního členu.
- Komponenty komunikace s vozidlem: Tato vrstva obsahuje různé komponenty komunikace s vozidlem používané jak pro komunikaci s vozidlem (například hlavní jednotka, nazývaná také informační a zábavní systém ve vozidle (IVI), nebo brána ve vozidle), a stejně jako komunikace s externími komponentami, jako jsou jiná auta nebo RSU.[2]

1.2 Gateway ECU s telematikou a komunikací

Většina automobilových architektur rozlišuje mezi různými doménami propojenými centrální bránou. Domény odpovídají různým a někdy nezávislým vlastnostem vozidla. Všechny tyto součásti mohou při porušení představovat riziko. Dopad těchto

rizik se může lišit v závislosti na zabezpečení a ochraně soukromí. Z tohoto důvodu jsou komponenty inteligentního automobilu považovány za aktiva a vyžadují odpovídající ochranu. Některá z těchto aktiv jsou uvedena níže.

1.2.1 Řízení převodovky

Automobilová součást, řídicí jednotka používaná v automobilech. Toto je kombinovaný řadič sestávající z řídicí jednotky motoru (ECU) a řídicí jednotky převodovky (TCU). [11].
Moderní automobily se skládají z mnoha zabudovaných elektronických řídicích jednotek (ECU), které ovládají mechanické nebo elektronické systémy vozidla.
Podsíť přenosu je obvykle založena na protokolu CAN (Controller Area Network Network).
CAN, norma ISO od roku 1993, je sběrnicí, ke které je připojena většina ECU vozidel. Vozidlo může mít více sběrnic CAN propojených bránou, aby izolovaly důležitější funkce (např. Řízení přenosu) od méně důležitých (např. Multimédií). Provoz v této interní síti se liší; v některých případech může síť podporovat několik stovek zpráv za sekundu; např. Ethernet. [2].
CAN, stejně jako ostatní protokoly popsané v této zprávě, má problémy týkající se šířky pásma, škálovatelnosti nebo zabezpečení. [9].
Tato oblast zahrnuje fyzické systémy, jako jsou spalovací motory nebo elektromotory, jakož i převodovky, hnací hřídele a kola.

1.2.2 Ovládání podvozku

Tato doména je zodpovědná za ekologickou správu rámu vozidla.
Jedná se obvykle o řízení a brzdy, stejně jako airbagy, řadové kamery, zpětná zrcátka nebo dokonce stěrače.

1.2.3 Ovládání těla

Za tělo je odpovědné ovládání karoserie, to znamená většinu času za prostor pro cestující a kufr.
ECU jsou podobné těm, které se používají v oblasti přenosu. Umožňují cestujícím ovládat různé funkce, jako je sdružený přístroj, ovládání klimatizace nebo zamykání dveří. Podsíť obvykle používá CAN [10].
Typicky se jedná o displej na palubní desce, klimatizaci, stejně jako světla, směrová světla nebo výstražná světla, dveře, okna, bezpečnostní pásy a dokonce i elektrická nebo vyhřívaná sedadla.

1.2.4 Ovládání informačního systému

Tato doména je obvykle oddělená od ovládání karoserie. Patří sem navigační služby, komunikace (telefon atd.) a zábavní služby (audio/video hlavní jednotka).
ECU jsou podobné těm, které se používají v oblasti přenosu. Umožňují cestujícím ovládat různé funkce, jako je hlavní jednotka pro audio/video, navigaci nebo interakci s telefonem uživatele. Služby nabízené prostřednictvím této domény se mohou velmi lišit, například:

- Zábavní služby (audio/video)
- Přístup na internet
- Řidičské služby, jako jsou dopravní informace, mapy.
- Další služby, jako je správa vozového parku, digitální tachograf, geo-oplocení. Tyto služby způsobují, že řídicí jednotky infotainmentu někdy mají konkrétní architektury:
  - U informačních a zábavních systémů lze operační systémy z mobilního průmyslu použít také v ECU (Windows CE (vyřazeno), Android, Tizen nebo WebOS)

Podsíť obvykle používá protokoly jako MOST(Media Oriented Systems Transport) a také sítě ad hoc využívající Bluetooth nebo Wi-Fi. Informační a zábavní systémy se spoléhají na bezdrátovou komunikaci poskytovanou buď vestavěným UICC(Universal Integrated Circuit Card), nebo koncovým zařízením (smartphonem) připojeným přes Bluetooth nebo pomocí kabelu USB. Kromě toho lze k připojení kamerových systémů použít Ethernet [10].

1.2.5 Řízení komunikace

Tato doména, na rozdíl od předchozích, není podsíť, ale častěji sada komunikačních funkcí nabízených telematickou řídicí jednotkou (TCU) fungující jako brána.
Brána poskytuje jak konektivitu, tak většinu zabezpečení určeného pro komunikaci (firewall, ověřovací funkce). Sbírá data z různých ECU pomocí jedné z datových sběrnic vozidla a poskytuje vzdálené připojení k internetu prostřednictvím vestavěného modulu GSM(Global System for Mobile Communications) nebo například pomocí smartphonu řidiče. Tato jednotka je obvykle také spojena s GNSS(Globální Družicový Polohový Systém) za účelem získání informací o poloze vozidla. Řada případů použití, které používají připojení TCU, jsou: [10]

- Vzdálená diagnostika (např. Hlášení poruch, software/aktualizace softwaru ECU nebo parametry ECU)
- Dálkový přenos údajů o vozidle
- Havarijní zprávy a nouzové výstrahy (eCall)

- Sledování ukradeného vozidla nebo geo-oplocení
- Dálkový start motoru
- Správa vozového parku (například pro sledování cesty nebo diagnostiku)
- Informujte řidiče o stavu nabití baterie (SoC) u elektrických vozidel (EV).
- Ekologické řízení

TCU obvykle poskytuje připojení 3G nebo Wi-Fi k poskytování více služeb, jako je komunikace eCall a V2X(Vehicle-to-everything). Na inteligentním stroji jsou možné další protokoly. Tyto typicky zahrnují rozhraní určená pro komunikaci na velké vzdálenosti, stejně jako kabelová nebo bezdrátová rozhraní určená pro místní použití.[2]

1.2.6 Diagnostické a servisní systémy

Diagnostické a servisní systémy jsou externí systémy, které jsou k vozidlu připojeny prostřednictvím vyhrazeného portu. Do této kategorie také zahrnujeme hardwarové klíče pro aftermarket, protože sdílejí stejná rozhraní.
Prostřednictvím portů OBD-II lze k vozidlům připojit různá zařízení pro údržbu a diagnostiku. Mohou být samostatný hardware, například přenosné datové sběrače, nebo se mohou skládat z aplikací běžících na PC nebo tabletu.
Telematické komponenty aftermarketů, jako jsou inteligentní klíče, mají také připojení OBD-II a externí připojení Bluetooth nebo mobilní připojení. Mohou také obsahovat ladicí rozhraní (například přes mini-USB) nakonfigurované k emulaci síťového adaptéru (to znamená, že po připojení se TCU zobrazí jako zařízení v síti). Diagnostika podsítě se obvykle provádí přímo na sběrnici CAN přes port OBD-II. Ethernet se také použije pro diagnostiku DoIP (Diagnostic over IP) [10].

1.3 Příklady napadení inteligentního auta

Byla definována závažnost několika scénářů útoku viz [2]. U každého scénáře útoku byl definován potenciální dopad (tj. Úroveň závažnosti) na vysoký, střední nebo nízký. Rozebrán je útočný scénář s vysokou úrovní závažnosti.

1.3.1 Útoky na servery

Ovlivňují chování automobilu: existuje několik scénářů útoku zahrnujících vzdálené servery. Například, útočník by mohl ohrozit mapová data, které mají vliv na věrohodnost kontroly, nebo dokonce změnit dopravní podmínky, což vede k neefektivní službě.
Vniknutí na servery OEM za účelem zahájení škodlivých aktualizací firmwaru může být katastrofální, protože tento typ útoku je vysoce škálovatelný.

Interní servery používané jako útok na vozidlo nebo extrakce dat

Zneužití oprávnění zaměstnanci (útok zasvěcených osob)
Cíle: Zaměstnanci, BackEnd Server OnPremise a BackEnd Server in Cloud
Kanály: Komunikační kanály, Mobilní síť

Neoprávněný přístup k serveru přes internet (možný například kvůli zadním dveřím, zranitelným místům nezajištěného systémového softwaru, útokům SQL nebo jiným způsobem)
Cíle: Infotainment systém,Externí aplikace, Služby nebo Systémy, Mobilní telefon, Gateway TCU, Bezdrátový systém
Kanály: Mobilní síť

Neoprávněný fyzický přístup k serveru (například prostřednictvím jednotky USB nebo jiného média připojeného k serveru)
Cíle: FD Back End Server,Fyzické zařízení, Zaměstnanci
Kanály: Komunikační kanály, Mobilní síť, Infotaiment networks, CAN bus

Selhání interních serverových služeb ovlivňujících provoz vozidla

Útok na interní server jej například zastaví v práci, zabrání mu v interakci s vozidly a poskytování služeb, na které se spoléhají.
Cíle: FD Back End Server,Externí aplikace, Služby nebo Systémy
Kanály: Infotaiment networks

Data uložená na interních serverech jsou ztracena nebo ohrožena("únik dat")

Ztráta informací v cloudu. Citlivá data mohou být ztracena v důsledku útoků nebo nehod, když jsou data ukládána poskytovateli cloudových služeb třetích stran.
Cíle: Cloud, FD Back End Server, Infotainment systém
Kanály: Komunikační kanály, Mobilní síť

Neoprávněný fyzický přístup k serveru (například přes USB disky nebo jiná média připojená k serveru)
Cíle: Zaměstnanci
Kanály: CAN bus

Porušení informací v důsledku neúmyslné komunikace (například chyby správce, ukládání dat na serverech v garážích)
Cíle: Souborový systém, Mobilní telefon
Kanály: Komunikační kanály

1.3.2 Ohrožení vozidel komunikačními kanály

Internetové připojení vozu je poskytováno buď vysílací/přijímací jednotkou zabudovanou do samotného vozu nebo prostřednictvím systémů třetích stran, jako jsou chytré telefony.
Automobilová síť se dělí na různé technologie systému sběrnice, jako Controller Area Network (CAN), Local Area Network (LIN), Media Oriented System Transport (MOST) a FlexRay. Podsítě jsou navzájem propojeny prostřednictvím řídicích jednotek ECU [12].
Zabezpečení komunikaci je založeno na různých úrovních. Důvěrnost, Dostupnost a Integrita jsou obvykle zabezpečeny kryptografickými algoritmy a bezpečnostními protokoly na fyzické, linkové, sítové nebo aplikační vrstvě.
Pro provoz v reálném čase používají vozidla připojená bezdrátovou technologii, Wi-Fi, Bluetooth, NFC nebo GSM, což vytváří další rizika, která mohou ovlivnit integritu a důvěrnost dat a život lidí; Protože ve vzduchu bude k dispozici obrovské množství dat. To znamená, že někdo např. hacker anebo neoprávněné strany můžou mít způsoby zadávání dat, úpravy záznamů, útočících systémů a každého pohybu vozidla.
Zabezpečení v architektuře Communications access for land mobiles (CALM) chrání kritickou komunikaci ve vozidle pomocí brány firewall ovládané vozidlem. [13]

Nahrazování zpráv nebo dat přijatých vozidlem

Falešné zprávy vydávání se za jinou osobu (např. 802.11p V2X při zapnutí, zprávy GNSS atd.)
Cíle: Gateway TCU, Bezdrátový systém
Kanály: Mobilní síť, V2X komunikace, Komunikační kanály

Útok Sibylly (oklamat ostatní auta, jako by na silnici bylo mnoho aut)
Kanály: Komunikační kanály

Komunikační kanály používané pro neoprávněnou manipulaci, mazání nebo jiné změny kódu/dat vozidla

Komunikační kanály umožňují zadávání kódu, například lze do komunikačního proudu vložit upravený softwarový binární soubor
Komunikační kanály umožňují manipulaci s údaji/kódy vozidla
Komunikační kanály umožňují přepsat data/kód vozidla
Komunikační kanály umožňují mazání dat/kódu vozidla
Komunikační kanály umožňují zadávání dat/kódu do vozidla (zápis datového kódu)
Všem těmto typům útoků jsou přiřazené stejné Aktivy a Kanály

Cíle: Konfigurační soubor, Souborový systém, Bezdrátový systém
Kanály: Komunikační kanály, V2X komunikace, Infotaiment networks, CAN bus

Komunikační kanály umožňují přijímat nespolehlivé zprávy nebo jsou zranitelné vůči útokům odposlechu/přehrávání

Získávání informací z nespolehlivého nebo nespolehlivého zdroje
Cíle:Externí aplikace, Služby nebo Systémy, Externí připojení
Kanály: Komunikační kanály

Člověk uprostřed/mezi
Cíle: Bezdrátový systém, Gateway TCU, ECU
Kanály: Mobilní síť, V2X komunikace, Komunikační kanály, CAN bus

Opakovaný útok, například útok na komunikační bránu, umožňuje útočníkovi downgrade softwaru nebo firmwaru brány ECU
Cíle: ECU, Gateway TCU
Kanály: Komunikační kanály, CAN bus

Informace lze snadno zveřejnit. Například poslechem zpráv nebo poskytnutím neoprávněného přístupu k důvěrným souborům

Monitorování odposlechu/rušení komunikace
Cíle: Bezdrátový systém
Kanály: Komunikační kanály, V2X komunikace, Mobilní síť

Získání neoprávněného přístupu k souborům nebo datům
Cíle: Bezdrátový systém, Konfigurační soubor, Souborový systém
Kanály: Komunikační kanály, V2X komunikace, Mobilní síť

Útoky odepření služby pomoci komunikačních kanálů k narušení funkcí vozidla

Odesílání spousty nevyžádaných dat do informačního systému vozidla, takže nemůže normálně poskytovat služby
Cíle: Bezdrátový systém, Souborový systém, Infotainment systém
Kanály: Mobilní síť, V2X komunikace, Komunikační kanály, CAN bus

Útok "černá díra" vede k narušení komunikace mezi vozidly, útočník může blokovat komunikaci mezi vozidly
Kanály: Komunikační kanály, V2X komunikace

Neoprávněný uživatel může získat privilegovaný přístup k systému vozidla

Neprivilegovaný uživatel může získat privilegovaný přístup, například root práva
Cíle: Zaměstnanci, Vlastník
Kanály: Komunikační kanály

Viry zabudované do komunikace mohou infikovat systémy vozidla

Virus zabudovaný do komunikačních médií infikuje systémy vozidla
Cíle: Infotainment systém, Bezdrátový systém
Kanály: Komunikační kanály

Zprávy přijaté vozidlem (např. X2V nebo diagnostické zprávy) mohou obsahovat škodlivá data

Škodlivé interní zprávy (např. CAN)
Kanály: CAN bus

Škodlivé zprávy V2X, např. Infrastruktura pro vozidla nebo zprávy o vozidle (např. CAM, DENM)
Kanály: V2X komunikace, Komunikační kanály

Škodlivé diagnostické zprávy
Cíle: ECU, Port OBD, Gateway TCU
Kanály: CAN bus

Škodlivé proprietární zprávy (například ty, které obvykle odesílá výrobce OEM nebo dodavatel komponent/systémů/funkcí)
Cíle: ECU, Gateway TCU, Port OBD, Externí připojení
Kanály: Komunikační kanály

Opatření na komunikačních kanálech

Nejprve je nutné chránit komunikační kanály před krádeží dat, například šifrováním dat, například ověřováním zpráv které jsou vyměňovány za účelem ochrany jejich dostupnosti a integrity. Kromě toho musí rozhraní bránit neoprávněnému přístupu. To zahrnuje procesy, jako je například ověřování mezi stroji za účelem zjištění, že komunikuje se známým nebo autorizovaným zařízením. Šifrování lze implementovat pomocí symetrického šifrování i kryptografických algoritmů veřejného klíče. Ověřování lze implementovat pomocí ověřovacích kódů zpráv nebo digitálních podpisů:

první jsou obvykle založeny na symetrických blokových šifrách (CMAC) nebo hašovacích funkcích (HMAC), zatímco digitální podpisy používají šifrování veřejného klíče.
Zabezpečený Gateway v konektivních vozech je ideální platformou pro implementaci specifikovaných opatření na ochranu soukromí a bezpečné ukládání uživatelských dat podporovaných ověřeným přístupem. Brána je jedna z důležitých součástí připojených systémů vozidla, zařízení brány vytváří most mezi systémem Internet of Vehicle (IoV), senzory, vybavením, systémy a cloudem. Napadení brány přeruší komunikaci mezi senzory a internetovou infrastrukturou.Používají se taky Middlewary na zabezpečení. [13]

1.3.3 Hrozby pro vozidla v souvislosti s jejich aktualizačními postupy

Aktualizace jsou pro systém důležité, nebývají však vždy dostatečně zabezpečené. Aktualizace lze použít k přidání nových funkcí do systému vozidla a také k opravě bezpečnostních problémů v systému. Může být nutné aktualizovat různé součásti, například aplikace pro infotainment, mapy, další systémové aplikace nebo dokonce celý operační systém.[2]

Zneužití nebo ohrožení postupů upgradu

Procedury aktualizace po bezdrátové sítí, včetně vytvoření programu aktualizace systému nebo firmwaru.
Cíle: Bezdrátový systém, Gateway TCU, Aktualizační procedury
Kanály: Mobilní síť, CAN bus

Procedury lokální/fyzické aktualizace softwaru. To zahrnuje vytvoření programu pro aktualizaci systému nebo firmwaru.
Cíle:Fyzické zařízení, Aktualizační procedury, Port OBD
Kanály: CAN bus, Komunikační kanály

Software je zpracován před procesem aktualizace (a proto poškozen), i když proces aktualizace zůstává nezměněn.
Cíle: Konfigurační soubor, Zaměstnanci, Souborový systém, Aktualizační procedury
Kanály: Komunikační kanály, CAN bus

Krádež kryptografických klíčů dodavatele softwaru umožňující neplatnou aktualizaci

Cíle: Souborový systém, Aktualizační procedury
Kanály: Komunikační kanály, CAN bus

Odmítnutí legitimní aktualizace

Útok typu odmítnutí služby na aktualizačním serveru nebo v síti, který zabrání nasazení důležitých aktualizací softwaru a nebo odemkne určité funkce klienta.
Cíle: FD Back End Server, Aktualizační procedury
Kanály: Mobilní síť, CAN bus

1.3.4 Ohrožení vozidel neúmyslným lidským jednáním

Nesprávná konfigurace zařízení nebo systémů legitimním subjektem, jako je vlastník nebo servisní komunita

Nesprávná konfigurace zařízení servisním personálem nebo vlastníkem během instalace/opravy/používání, což vede k nepředvídatelným následkům
Cíle: Vlastník, Konfigurační soubor
Kanály: CAN bus

Zneužití nebo správa zařízení a systémů (včetně aktualizací OTA)
Cíle: Port OBD, Zaměstnanci
Kanály: CAN bus

Legitimní subjekty mohou přijmout opatření, která nechtěně přispějí ke kybernetickému útoku.

Nevinná oběť (například vlastník, operátor nebo technik údržby) je podvedena, aby podnikla něco k neúmyslnému stažení malwaru nebo provedení útoku.
Cíle: Vlastník, Zaměstnanci
Kanály: Infotaiment networks, Komunikační kanály

Předepsané bezpečnostní postupy nejsou dodržovány
Cíle: Vlastník, Zaměstnanci
Kanály: Komunikační kanály

1.3.5 Ohrožení vozidel z hlediska jejich externího připojení

Manipulace s konektivitou funkcí vozidla umožňuje kybernetické útoky, včetně telematiky; systémy, které umožňují dálkové ovládání; a systémy využívající bezdrátovou komunikaci na krátkou vzdálenost

Správa funkcí určených pro dálkové ovládání systémů, jako je klíč na dálkové ovládání, imobilizér a nabíječka baterií
Cíle: Mobilní telefon, Klíč vozidla, Externí připojení
Kanály: CAN bus

Manipulace s telematikou vozidla (např. Kontrola měření teploty citlivého zboží, dálkové otevírání dveří nákladového prostoru)
Cíle: Gateway TCU, Externí připojení, Bezdrátový systém, Klíč vozidla
Kanály: CAN bus

Rušení bezdrátových systémů nebo senzorů krátkého dosahu
Cíle: Sensory, Bezdrátový systém, Externí připojení
Kanály: V2X komunikace

Dostupné software třetích stran, například zábavné aplikace, používaný k útoku na systémy vozidel

Poškozené softwarové aplikace s nízkou ochranou používané jako metoda útoku na systémy vozidel.
Cíle: Bezdrátový systém, Externí připojení, Infotainment systém
Kanály: Infotaiment networks

Zařízení připojená k externím rozhraním, například USB porty, OBD port, používaná jako prostředek útoku na systémy vozidla

Externí rozhraní, jako je USB nebo jiné porty používané jako bod útoku, například prostřednictvím vkládání kódu.
Cíle: Externí připojení,Fyzické zařízení, Mobilní telefon, Infotainment systém
Kanály: Infotaiment networks

Média infikovaná virem připojená k systému vozidla
Cíle: Externí připojení, Mobilní telefon, Infotainment systém, Infotaiment networks
Kanály: Infotaiment networks

Diagnostický přístup (například klíče v portu OBD) používaný k usnadnění útoku,

například manipulace s parametry vozidla (přímo nebo nepřímo)
Cíle: Port OBD
Kanály: CAN bus

1.3.6 Možné cíle nebo motivy útoku

Extrahování dat/kódu vozidla

Extrakce softwaru chráněného autorskými právy nebo patentovaného softwaru z automobilových systémů (pirátství)
Cíle: Konfigurační soubor, Souborový systém, Infotainment systém, Mobilní telefon,Externí aplikace, Služby nebo Systémy
Kanály: Infotaiment networks, CAN bus

Neoprávněný přístup k informacím o ochraně osobních údajů vlastníka, jako jsou osobní údaje, fakturační údaje, informace z adresáře, informace o poloze, elektronické ID vozidla atd.
Cíle: FD Back End Server, Cloud, Souborový systém, Mobilní telefon, Infotainment systém,Externí aplikace, Služby nebo Systémy
Kanály: Mobilní síť, V2X komunikace

Načítání kryptografických klíčů
Cíle: Souborový systém, Mobilní telefon, Infotainment systém
Kanály: CAN bus, Infotaiment networks

Manipulace s údaji/kódy vozidla

Neoprávněné změny elektronického ID vozidla
Cíle: ECU, Souborový systém
Kanály: CAN bus

Padělání osobních údajů. Například pokud uživatel chce při placení zobrazit jinou identitu.
Cíle: Souborový systém, Mobilní telefon
Kanály: CAN bus, Infotaiment networks, Komunikační kanály

Akce k překonání monitorovacích systémů (např. Hacking/neoprávněná manipulace/blokování zpráv, jako jsou data ODR Tracker nebo počet spuštění)
Cíle: ECU, Souborový systém, FD Back End Server
Kanály: Mobilní síť

Manipulace s daty za účelem falšování údajů o řízení vozidla (např. Počet kilometrů, rychlost jízdy, směr jízdy atd.)
Cíle: ECU, Souborový systém
Kanály: V2X komunikace, CAN bus

Neoprávněné změny diagnostických dat systému
Cíle: ECU, Port OBD, Gateway TCU
Kanály: CAN bus

Vymazání dat/kódu

Neoprávněné mazání/úpravy protokolů systémových událostí
Cíle: ECU, Gateway TCU
Kanály: CAN bus

Injekce malwaru

Představuje malwarové akce
Cíle: Souborový systém, Cloud, FD Back End Server, Mobilní telefon, Infotainment systém,Externí aplikace, Služby nebo Systémy, Externí připojení
Kanály: Infotaiment networks

Představení nového softwaru nebo přepis stávajícího

Výroba softwaru pro řídicí systém automobilu nebo informační systém
Cíle: Aktualizační procedury, Zaměstnanci
Kanály: CAN bus

Narušení systémů nebo provozu

Například odmítnutí služby může být způsobeno v interní síti přetížením sběrnice CAN nebo spuštěním poruch v ECU prostřednictvím rychlostí zpráv.
Cíle: ECU
Kanály: CAN bus

Manipulace s parametry vozidla

Neoprávněný přístup nebo neoprávněná manipulace s konfiguračními parametry klíčových funkcí vozidla, jako jsou údaje o brzdě, prahová hodnota airbagu atd.
Cíle: Konfigurační soubor
Kanály: CAN bus, Komunikační kanály

Neoprávněný přístup nebo manipulace s parametry nabíjení, jako je nabíjecí napětí, nabíjecí výkon, teplota baterie atd.
Cíle: Souborový systém
Kanály: CAN bus

1.3.7 Potenciální zranitelná místa, která lze zneužít, pokud nejsou dostatečně chráněna nebo vylepšena

Kryptografické technologie mohou být ohroženy nebo nedostatečně použity

Kombinace krátkých šifrovacích klíčů a dlouhých dat vypršení platnosti umožňuje útočníkovi prolomit šifrování.
Cíle: Konfigurační soubor
Kanály: CAN bus

Nedostatečné používání kryptografických algoritmů k ochraně citlivých systémů
Cíle: Konfigurační soubor
Kanály: CAN bus

Použití již nebo brzy zastaralých kryptografických algoritmů
Cíle: Konfigurační soubor
Kanály: CAN bus

Díly nebo spotřební materiál mohou být ohroženy, což umožňuje útok na vozidla.

Hardware nebo software navržený tak, aby umožňoval útok, nebo nesplňuje konstrukční kritéria k zastavení útoku.
Cíle:Fyzické zařízení
Kanály: CAN bus

Vývoj softwaru nebo hardwaru umožňuje chyby zabezpečení

Softwarové chyby. Přítomnost softwarových chyb může být základem potenciálních zranitelností, které lze zneužít. To platí zejména v případě, že software nebyl testován, aby se ověřilo, že není znám špatný kód/chyby, a aby se snížilo riziko vzniku neznámého chybného kódu/chyb.
Cíle:Externí aplikace, Služby nebo Systémy, Infotainment systém
Kanály: Infotaiment networks

Použití zbytků vývoje (např. Ladicí porty, porty JTAG, mikroprocesory, vývojové certifikáty, hesla vývojářů atd.) Může umožnit přístup k ECU nebo umožnit útočníkům získat vyšší oprávnění
Cíle: ECU, Gateway TCU, Port OBD
Kanály: CAN bus

Návrh sítě zavádí zranitelná místa

Nadbytečné internetové porty zůstávají otevřené, aby poskytovaly přístup k síťovým systémům.
Cíle: Port OBD, Infotainment systém, Konfigurační soubor
Kanály: V2X komunikace, Infotaiment networks, CAN bus, Komunikační kanály

Chcete-li získat kontrolu, obejděte oddělení sítě. Specifickým příkladem je použití nezabezpečených bran nebo přístupových bodů (jako jsou brány pro nákladní automobily s přívěsy) k obejití zabezpečení a získání přístupu k dalším síťovým segmentům za účelem provádění škodlivých akcí, jako je odesílání libovolných zpráv sběrnice CAN.
Kanály: CAN bus, Komunikační kanály

Fyzická ztráta dat

Poškození způsobené třetí stranou. Citlivá data mohou být ztracena nebo ohrožena v důsledku fyzického poškození v případě dopravní nehody nebo krádeže.
Kanály: Fyzická hranice vozidla

Ztráta v důsledku konfliktů DRM (správa digitálních práv). Uživatelská data mohou být odstraněna kvůli problémům s DRM
Kanály: Fyzická hranice vozidla

Může dojít ke ztrátě (integrity) citlivých dat v důsledku zhoršení komponent IT, což může způsobit potenciální kaskádové problémy (například v případě klíčové změny)
Kanály: Fyzická hranice vozidla

Neúmyslný přenos dat

Porušení informací. Osobní nebo citlivé údaje mohou uniknout, když vozidlo změní uživatele (například je prodáno nebo použito jako pronajaté auto s novými pronajímateli).
Kanály: Fyzická hranice vozidla

Fyzická manipulace se systémy může vést k útoku

Manipulace s vybavením OEM, jako je neoprávněné vybavení přidané do vozidla, aby byl možný útok typu man-in-the-middle
Kanály: Fyzická hranice vozidla

2 Modelování hrozeb

Modelování hrozeb je proces analýzy rizik, při kterém se složitý systém převádí na jednoduchý model a je zjišťováno, které hrozby mohou ovlivnit provoz systému nebo jeho uživatelů [3]. Tento proces by měl být již zahrnut do fáze návrhu při vývoji nového systému (např. Automobilu). Lze jej však také použít, když je produkt připraven. Při modelování hrozeb se běžně používají následující výrazy:

- **Aktivum(Asset)**: to, co je považováno za cenné, se nazývá aktivum. Může to být systémová součást, data partnerů, použitý software nebo dokonce něco abstraktního, například opuštění společnosti. Útočník chce získat kontrolu nad aktivem ve svůj vlastní prospěch nebo poškodit jeho vlastníka, například úpravou nebo krádeží údajů o zákaznících.
- **Hrozba(Threat)**: Hrozbou se rozumí cokoli, co by mohlo vést ke zlomyslnému nebo neúmyslnému zneužití aktiva. Lidé obvykle myslí na falešného útočníka, který se pokusí kompromitovat bezpečnostní systém využíváním zranitelností systému. Hrozba však může být způsobena také neúmyslným přístupem uživatele nebo přirozenou chybou způsobenou komponentou.
- **Zranitelnost(Vulnerability)**: Zranitelnosti jsou slabosti, které nechávají aktivum otevřené útoku. Každá zranitelnost zůstává vystavena riziku zneužití a poškození majetku.
- **Riziko(Risk)**: Riziko představuje pravděpodobnost poškození aktiva při zneužití zranitelnosti hrozbou.

Softwarový přístup začíná představením struktury systému ve formě architektonických diagramů, jako je diagram toku dat, aby byl zajištěn lepší přehled a pořadí potenciálních problémů. To se ukázalo jako velmi užitečné pro modelování sítě. Stal se ale také standardem pro software, protože Microsoft posunul tento přístup vpřed ve svém Security Development Lifecycle (SDL) a poskytl nástroje jako jeho Threat Modeling Tool (TMT).[8].

U strategie zaměřené na aktiva je nutné nejprve identifikovat aktiva a poté posoudit jejich hodnotu pro útočníka a vlastníka daného aktiva. Podle této priority jsou hrozby řešeny postupně. Útočné stromy se obvykle používají k zobrazení, jak lze zaútočit na každé aktivum, a poté jsou vybrána konkrétní protiopatření.

Metodika zaměřená na útočníka je podobná, ale zde začíná analýzou potenciálního útočníka. Metrika bude zahrnovat různé faktory, jako je motivace, účel, dovednosti nebo financování. Útokové stromy, které ukazují konkrétní požadavky, které musí útočník splnit, pomohou určit možné cesty, kterými se útočník vydá. Na základě těchto výsledků lze použít vhodná řešení zmírnění. Lze například zvýšit velikost šifrovacího klíče, aby se zvýšila prahová hodnota požadovaná pro útočníka, aby sledoval tuto cestu.

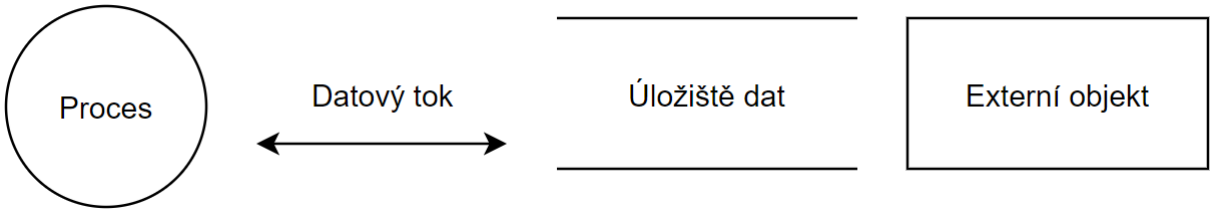
2.1 Metodiky modelování hrozeb

Existuje mnoho metodik modelování hrozeb, stejně jako některé, které kombinují bezpečnost a zabezpečení. Mohou být již použity během fáze návrhu systému, ale mohou být také součástí penetračního testu. Bylo zaměřeno na ty metodologie modelování hrozeb, které lze integrovat a kombinovat zabezpečení a ochranu. Ty, které budou mít největší dopad, budou podrobně popsány, ostatní jsou pouze zmíněny.

2.1.1 Diagramy toku dat

Modely toku dat jsou často ideální pro modelování hrozeb. Modely datových toků existují častěji pro síťové nebo architektonické systémy než pro softwarové produkty, ale lze je vytvořit pro oba. Rozlišuje se několik typů [3] 2.1.1:

- **Proces**
  - Zaoblený obdélník, kruh nebo soustředné kruhy jsou jakýkoli fungující kód. Například kód napsaný v C, C#, Pythonu nebo PHP
- **Datový tok**
  - Šipka - komunikace mezi procesy nebo mezi procesy a datovými sklady. Například síťová připojení, HTTP, RPC, LPC
- **Úložiště dat**
  - Dvě paralelní linie se štítkem mezi nimi jsou věci, ve kterých jsou data uložena. Příklady souborů, databází, registru Windows, segmentů sdílené paměti
- **Externí objekt**
  - Ostrý obdélník - lidé nebo kód mimo vaši kontrolu. Příklad klient



Obr. 2.1: Symboly DFD

2.1.2 STRIDE

Model hrozby STRIDE vyvinutý a používaný společností Microsoft jako součást jejich SDL. STRIDE je zkratka pro Spoofing, Tampering, Repudiation, Information

Disclosure, Denial of service, Elevation of Privelege, což představuje třídy hrozeb pro vlastnosti zabezpečení, které porušují (viz tabulka 2.1.2). Aby se zajistilo, že aplikace je použitelná pro tyto vlastnosti zabezpečení, je potřeba přemýšlet o systému a o tom, zda může útočník k infiltraci použít hrozbu z kterékoli z těchto tříd. [4]

V tomto procesu pomůže nakreslení diagramu. Microsoft nabízí diagram toku dat (DFD), ale fungují i další, jako je diagram UML. U tohoto modelu musí být systém rozložen na malé součásti a poté je každá součást testována, pokud na ni může zaútočit jedna z tříd hrozeb. Ve DFD jsou tyto komponenty jedním z následujících prvků: procesy, úložiště dat, toky dat, interakční prvky a speciální prvek - hranice důvěryhodnosti. Každý z nich je reprezentován svými vlastními symboly a čtyři základní prvky jsou ovlivněny pouze konkrétní sadou tříd hrozeb STRIDE viz. 2.1.2.

Hrozba	Poškození majetku	Popis vlastnosti zabezpečení
Spoofing	Ověření	Potvrzuje se identita uživatele.
Tampering	Integrita	Data lze změnit pouze definovanými způsoby, pověřenými lidmi.
Repudiation	Neodmítnutí	Uživatel nemůže popřít provedení akce.
Information Disclosure	Důvěrnost	Data jsou k dispozici pouze pro pověřené osoby.
Denial of Service	Dostupnost	Systémy jsou v případě potřeby připraveny a fungují dobře.
Elevation of Priviledge	Oprávnění	Uživatelům je výslovně zakázán nebo udělen přístup k prostředkům.

Tab. 2.1: STRIDE Model

Spoofing/Předstírání identity

Spoofing předstírá, že je někdo jiný. V těchto případech útočník předstírá, že je v dané roli. Tyto substituce hrozeb se dělí na [3]:

- Falšovaní procesu na stejném stroji
  - Přejmenovat - pojmenovat svůj proces "sshd"
  - Přejmenovat/propojit - vytvoření trojského koně "su" a změna cesty
  - Vytvoří soubor před skutečným procesem
- Falšovaní souboru

  - Vytvoří soubor v místním adresáři - může to být knihovna, spustitelný soubor nebo konfigurační soubor.
  - Vytvoří odkaz a upraví ho - z pohledu útočníka musí dojít ke změně mezi kontrolovaným odkazem a odkazem, ke kterému se přistupuje.
  - Vytvoří mnoho souborů v očekávaném adresáři - automatizace usnadňuje vytváření 10 000 souborů v /tmp k vyplnění prostoru soubory s názvem /tmp/pid.NNNN nebo podobnými.
- Falešná simulace stroje
  - ARP spoofing
  - Spoofing IP adresy
  - Spoofing DNS
  - Odposlech DNS - hacknutý TLD, registrátor nebo operátor DNS
  - Přesměrování IP - na úrovni přepínače nebo routeru
- Náhrada osoby
  - Nastavuje zobrazovaný název e-mailu
  - Převezme skutečný účet
- Předstíraní rolí
  - Prohlašuje se za tuto roli - někdy se otevře speciální účet s relevantním jménem

Tampering/Neoprávněná modifikace

Tempering mění data(informace), obvykle na disku, v síti nebo v paměti. To může zahrnovat úpravu dat v tabulce (pomocí programu, jako je Excel nebo jiný editor), úprava binárního nebo konfiguračního souboru na disku nebo úprava složitější datové struktury, jako je databáze na disku. V síti lze balíčky přidávat, upravovat nebo odebírat. Někdy je snazší přidávat balíčky, než je upravovat, když je procházíte, a programy velmi špatně zpracovávají další kopie dat. Další příklady [3]:

- Manipulace se souborem
  - Upraví soubor, který vlastní, na který se spoléháte
  - Upraví soubor, který vlastníte
  - Upraví soubor na souborovém serveru, který vlastníte.
  - Upravuje soubor na vašem souborovém serveru - spousta legrace, když přidáte soubory ze vzdálených domén.
  - Upravuje odkazy nebo přesměrování
- Paměť
  - Změní váš kód - je obtížné se chránit, pokud útočník spustí kód jako stejný uživatel
  - Upravuje data, která byla poskytnuta vašemu API - při překročení hra-

nice důvěryhodnosti

- Sítě
  - Přesměruje tok dat na svůj stroj - často první fáze hackingu
  - Změní tok dat po síti. Je to ještě jednodušší, když je síť bezdrátová (WiFi, 3G atd.)
  - Zesiluje spoofingové útoky

Repudiation/Narušení nepopiratelnosti

Odmítnutí tvrdí, že jste něco neudělali nebo nejste zodpovědní za to, co se stalo. Lidé mohou čestně nebo klamavě odmítat. Vzhledem k rostoucím znalostem, které jsou často nutné k pochopení složitého světa, mohou ti, kteří se toho upřímně vzdají, skutečně identifikovat problémy ve vašem uživatelském prostředí nebo architektuře služeb. Hrozby selhání jsou také spojeny se systémem a procesem logovaní. Pokud nemáte logy, neukládáte logy nebo nemůžete logy analyzovat, je těžké zpochybnit hrozby selhání. Existuje také třída útoků, kdy útočníci umisťují data do logu, což ztěžuje jejich analýzu. Pokud například zobrazujete své logy ve formátu HTML a útočník odešle </tr> nebo </html>, zobrazení logu by s nimi mělo zacházet jako s daty, nikoli s kódem. Další hrozby zamítnutí jsou [3]:

- Odmítnutí žaloby
  - Nebyly obdrženy žádné stížnosti - potvrzení může být zvláštní; Znamená e-mail stažený do vašeho telefonu, že jste si jej přečetli? Byly obrázky předem načteny síťovým proxy serverem?
  - Tvrdí, že byl obětí podvodu
  - Používá účet někoho jiného
  - Bez povolení používá platební nástroj někoho jiného
- Útok na logy
  - Upozorní, že nemáte žádné logy
  - Umístí útoky do logů, aby znemožnilo logy, kód pro čtení logů nebo osobu, která čte logy

Information disclosure/Zveřejňování informací

Zveřejnění je poskytování informací někomu, kdo nemá oprávnění. Některé hrozby zveřejnění informací jsou [3]:

- Zveřejnění informací o procesu
  - Načte tajemství z chybových zpráv
  - Přečte chybové zprávy z uživatelského jména/hesla ze všech databázových tabulek

  - Extrahuje strojová tajemství z chybových případů - může učinit ochranu proti poškození paměti jako ASLR
  - Načte obchodní/osobní tajemství z chyb
- Zveřejnění informací o datových úložištích
  - Používá neodpovídající nebo chybějící seznamy ACL
  - Používá špatná oprávnění databáze
  - Vyhledá soubory chráněné neznámem
  - Vyhledá šifrovací klíče na disku (nebo v paměti)
  - Vidí zajímavé informace v názvech souborů
  - Čte soubory při proházení po síti
  - Načte data z logů nebo dočasných souborů
  - Získá data z odkládacího nebo jiného dočasného úložiště
  - Načte data získáním zařízení a změnou operačního systému
- Zveřejnění informací o datovém proudu
  - Čte data ze sítě
  - Přesměruje provoz, aby bylo možné číst data
  - Učí se analýzou provozu
  - Zjistí, kdo s kým komunikuje, vyhledáním DNS
  - Zjistí, kdo s kým komunikuje, zveřejněním informací na sociálních sítích

Denial of Service/Odepření služby

Útoky odmítnutí služby spotřebovávají zdroje potřebné k poskytování služeb. Příklady [3]:

- Odmítnutí služby procesů
  - Využívá paměť (RAM nebo disk)
  - Spotřebuje CPU
  - Používá proces jako zesilovač
- Odmítnutí služby datového úložiště
  - Naplní úložiště dat
  - Vytvoří dostatek požadavků na zpomalení systému
- Odmítnutí služby datového proudu
  - Spotřebuje síťové prostředky

Elevation of Priviledge/Elevace oprávnění

Zvýšení oprávnění umožňuje někomu dělat věci, na které nemá oprávnění, například povolení běžného uživatele spouštět kód jako správce nebo povolení vzdálené osobě spouštět kód bez jakýchkoli práv. Dva důležité způsoby, jak zvýšit oprávnění, zahrnují poškození procesu a získání minulých kontrol autorizace. Příklady [3]:

- Zvýšení oprávnění k procesu jeho poškozením
  - Odesílaní vstupu, který kód nezpracovává podle očekávání - tyto chyby jsou velmi časté a obvykle mají velký dopad.
  - Špatný přístup do paměti pro čtení nebo zápis - zápis do paměti je (doufejme) špatný, ale čtení paměti může umožnit další útoky.
- Zvýšení prostřednictvím zmeškaných kontrol autorizace
- Zvýšení kvůli chybám autorizace - Centralizace takových kontrol usnadňuje správu chyb
- Zvýšení paděláním dat - Změní bity na disku a provede něco jiného, než co zamýšlí autorizovaný uživatel

Prvky	S	T	R	I	D	E
Datový tok		X		X	X	
Datové úložiště		X		X	X	
Procesy	X	X	X	X	X	X
Interakcí	X		X			

Tab. 2.2: Hrozby ovlivňující prvky

Se STRIDE a DFD viz. 2.1.2 se dá systém podrobně modelovat a strukturovaný přístup pomůže najít hrozby ručně. Microsoft také poskytuje nástroj pro vykreslování DFD a automatické vytváření hrozeb na základě předdefinovaných pravidel. Tento model bohužel také neposkytuje hodnocení generovaných hrozeb.[7]

2.2 Shrnutí

Model STRIDE, poskytuje klasifikace hrozeb, které porušují pět vlastností zabezpečení. Chceme-li najít hrozby, je potřeba rozebrat systém na menší součásti a nakreslit diagram datového toku. Poté při pohledu na každou komponentu a přemýšlení o tom, které vlastnosti zabezpečení je třeba chránit, by měly být identifikovány potenciální hrozby. Kromě toho byla tato metoda zvolena, protože společnost Microsoft také vydala svůj nástroj pro modelování hrozeb, který je založen na jejich metodě.

3 Nástroje pro modelování hrozeb

Nástroj pro modelování hrozeb je nástroj, který umožňuje klíčovým zúčastněným stranám navrhovat, vizualizovat, předvídat a plánovat vnější a vnitřní hrozby. Identifikace a náprava hrozeb může organizacím z dlouhodobého hlediska ušetřit miliony a okamžitě jim zabránit. Proto bylo zaměřeno na stávající nástroje, které lze použít k modelování hrozeb v automobilovém průmyslu.

3.1 IriusRisk

Program IriusRisk byl vyvinut společností Continuum Security. IriusRisk nabízí komunitní i komerční verzi nástroje. Tento nástroj je zaměřen na vytváření a udržování platného modelu ohrožení v celém SDLC. Spravuje proces pomocí plně přizpůsobitelných dotazníků a knihoven šablon rizik, s vývojovými diagramy a integrací s DevSecOps (OWASP ZAP, BDD-Security, Threadfix ...), aby vylepšil možnosti automatizace.[5]

3.2 Microsoft Threat Modeling Tool 2016

V rámci navrhovaného Security Development Lifecycle (SDL) společnost Microsoft vydala TMT zdarma. Microsoft Threat Modeling Tool 2016 se skládá ze 2 částí, editoru šablon a tvůrce modelu.[8]
V editoru šablon dá se jednotlivě vytvořit vlastní sadu šablonu (tok, cíl, hranice), která představuje různé prvky DFD (tok dat, proces, úložiště dat, interakce, hranice důvěryhodnosti). Poté dá se přidat nové vlastnosti ohrožení, například Nízké až Střední riziko. Takže nástroj umožňuje automatické vytváření hrozeb. Při provedení je tak potřeba definovat kategorie hrozeb, například STRIDE, a přidat nové typy hrozeb.[8] Například kategorie Spoofing má typ doručování škodlivých aktualizací na vozidlo. Pro každý typ hrozby lze zapsat pravidla, kde se může vyskytovat, například "(Zdroj - [Server aktualizace firmwaru], cíl - [TCU])" . Dále lze nastavit vlastnosti hrozby, například z "Rizika" na "Vysoká" .
Jakmile vytvořena šablona, můžete ji použít k vytvoření nového modelu ohrožení. Ve tvůrci lze vytvořit diagram toku dat pomocí šablon. Každý prvek přidaný do diagramu lze změnit jeho vlastností. Vazby mezi prvky jsou také samotnými prvky, typu "Flow" . Na konci simulace se vytvoří zpráva. Tam systém analyzuje všechny prvky podle pravidel uvedených v šabloně a vygeneruje soubor HTML. Kromě toho jsou hrozby již uvedeny v analytickém zobrazení, kde lze změnit vlastnosti každé hrozby, například "Stav" na "Sníženo" .
Sestava obsahuje pouze jednokanálové hrozby, což znamená, že jsou analyzovány

pouze dvě související položky, takže navrhuje další krok, kdy jsou ručně přidány scénáře hrozeb.
Ve srovnání s jinými bezplatnými nástroji má Microsoft Threat Modeling Tool nejvíce funkcí a schopností. Poskytuje dobré UX prostřednictvím intuitivního a elegantního grafického uživatelského rozhraní (GUI). Schopnost vytvářet zprávy je velkým bonusem tohoto nástroje. Při vytváření obecného modelu byly vygenerovaný stovky hrozeb.

3.3 ThreatModeler

ThreatModeler je komerční balíček dostupný s ročním předplatným s ikonami a šablonami pro přetažení. Nástroj lze použít pro konektivní auto. Mezi další funkce nástroje patří automatické vytvoření stromu útoku.

3.4 Shrnutí

V tabulce 3.4 jsou uvedeny přístroje a jejich hodnocení na základě kritérií. Lepší vizualizace systému vyžaduje schopnost nakreslit diagram datového toku. Vzhledem k tomu, že žádný z nástrojů nemá funkce speciálně navržené pro automobilový průmysl, je třeba jej rozšířit do té míry, aby bylo možné implementovat chybějící komponenty. Nastroj musí automaticky generovat hrozby na základě nakresleného diagramu a předdefinovaných pravidel.

Aplikace	DFD	Rozšiřitelný	Automobilový průmysl	Generování hrozeb
IriusRisk		X		X
Threat MT	X	X	X	X
ThreatModeler		X	X	X

Tab. 3.1: Porovnaní nástrojů pro Modelovaní Hrozeb

4 Realizace

Modelování hrozeb s MS TMT 2016:

1. Přidání šablony
2. Modelování systému
3. Aktuální analýza
4. Vytvoření vlastni šablony
5. Vytváření vlastního modelu

4.1 Modelování hrozeb s MS TMT 2016

Pro tuto práci byl nainstalován Microsoft Threat Modeling Tool 2016 na operační systém Windows 10. Postup modelování hrozeb byl realizován pomocí nástroje Microsoft Threat Modeling Tool 2016.
Hlavním důvodem pro výběr nástroje Microsoft Threat Modeling Tool v automobilovém průmyslu,je to, že umožňuje diagramování toku dat a má vestavěný mechanismus pro automatické generování hrozeb založených na pravidlech. Většina nástrojů pro modelování hrozeb je určena pro počítačové sítě nebo aplikace, a proto je nelze použít k simulaci vozidel. Microsoft poskytuje svobodu vytvářet vlastní šablony, do kterých může uživatel přidávat své komponenty jako "šablony" . S jejich pomocí lze postavit DFD. Kreslení diagramu dává lepší přehled a umožňuje lepší vizualizaci systému, než jen tabulkový pohled na komponenty. Kromě přidání vlastních šablon lze měnit vlastnosti hrozby a vytvořit vlastní pravidla pro generování hrozeb.

4.1.1 Přidání šablony

Nástroj pro modelování hrozeb společnosti Microsoft má ve výchozím nastavení pouze šablony pro malou webovou aplikaci, nikoliv pro oblast automobilů. Byla přidána šablona od skupiny NCC pro automobily na GitHubu [6] pro veřejné použití. Tato šablona pravděpodobně není pro scénář dostatečná. Proto je třeba jej rozšířit přidáním nových vzorů a pravidel. Šablony lze odvodit z komponent architektury systému nebo částí zkopírovaných z existujících šablon.
Šablonu založenou od NCC Group bude nutné rozšířit o další komponenty, zejména pro různé datové proudy sběrnice (CAN, Flexray a LIN) a nové ECU. Každá součást modelu systému má odpovídající šablonu. Kromě toho bude nutné přidat šablonu pro řidiče a mechanika, protože jsou potřebné pro vývoj proudu pro externí zdroj pomocí komponent, jako je například OBD nebo HMI port.

4.1.2 Modelování systému

Po přidání šablon byl nakreslen systémový DFD. Pokud je systém již vizualizován, je snazší přijít s pravidly, která by měla vytvářet očekávané hrozby.
Při návrhu systému pro automobilový průmysl se ve většině případů k připojení některých komponent použije sběrnice.

4.1.3 Aktuální analýza

Nakonec, když se nakreslí diagram a nakonfiguruje se každé pravidlo ohrožení, měla by se vygenerovat zpráva. Musí to být úplná zpráva se všemi vlastnostmi, jinak nelze soubor správně analyzovat.
Typy hrozeb v šabloně jsou tříděny podle kategorií STRIDE. Proto lze toto mapování použít ke klasifikaci typů hrozeb a ke konfiguraci výchozích hodnot dopadu.
Může se stát, že se v sestavě zobrazí zastaralá data. Toto je chyba TMT(Threat Modeling Tool) a lze ji snadno vyřešit přepnutím do zobrazení analýzy, výběrem všech zobrazených hrozeb a jejich odstraněním. Tím se spustí funkce pro opětovné generování všech hrozeb pro model.

Threat List

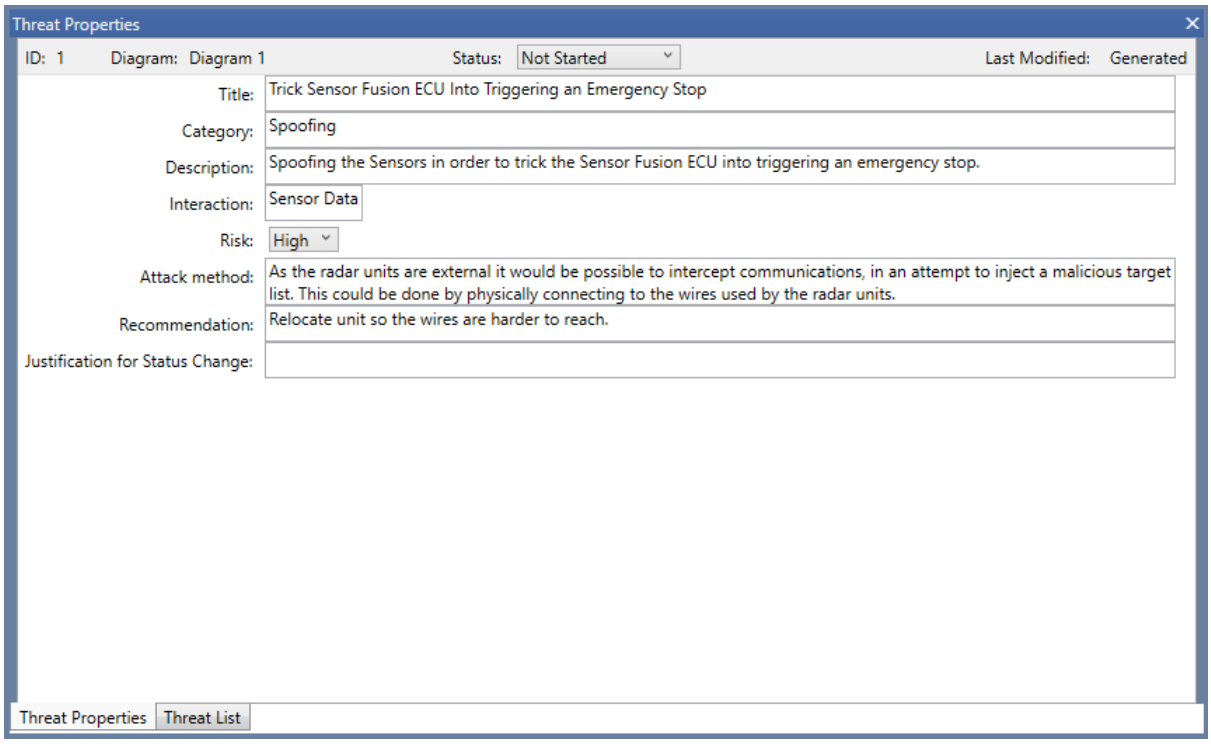
ID	Category	Interaction	Risk	Recommendation
312	Tampering	Ethernet	High	Disable 2G communications, only 3G and 4G should be allowed. Use a secure communication channel between the car and the server.
102	Tampering	GPS Data	High	Disable 2G communications, only 3G and 4G should be allowed. Use a secure communication channel between the car and the server.
281	Spoofing	Commands	High	Relocate unit so the wires are harder to reach.
91	Spoofing	GPS Data	Medium	Combine GPS with other sources of data to provide additional validation.
101	Spoofing	GPS Data	Medium	Combine GPS with other sources of data to provide additional validation.
1	Spoofing	Sensor Data	High	Relocate unit so the wires are harder to reach.
20	Spoofing	Sensor Data	High	Validate Cameras data against data models and additional vehicle data.
21	Spoofing	Sensor Data	High	Implement a gateway module so that the the Cameras and Sensors modules can only send messages relating to themselves.
22	Spoofing	Sensor Data	High	Running vehicle models in parallel to check credibility of path. Have map information on the Sensor Fusion ECU. Introduce redundancy.
23	Spoofing	Sensor Data	High	Relocate unit so the wires are harder to reach.
239	Spoofing	Sensor Data	High	Relocate unit so the wires are harder to reach.
254	Spoofing	Sensor Data	High	Relocate unit so the wires are harder to reach.
36	Information Disclosure	CAN Bus Data Fl	Medium	Consider encrypting the data flow. For web traffic this can be achieved by using HTTPS.
37	Information Disclosure	CAN Bus Data Fl	Medium	Ensure that connections to the delivery server are authenticated and encrypted and access should be limited to only the required files.

Obr. 4.1: Seznam hrozeb

Poté, co bylo vše nastaveno, vygenerovala se zpráva v nástroji Microsoft Threat Modeling Tool. Bylo zjištěno celkem 310 hrozeb souvisejících s různými pravidly hrozeb a způsoby jejich odstranění obrázek 4.1. Další informace o hrozbě se zobrazí v okně vlastnosti hrozby viz. obrázek 4.2.

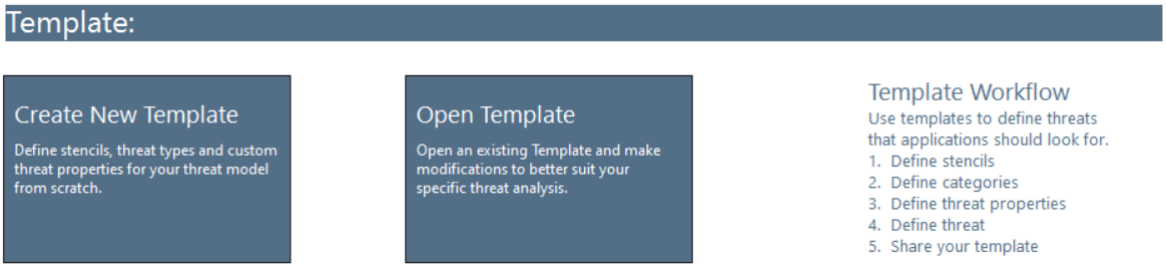
4.1.4 Vytváření vlastní šablony

Šablona pro nový model. Před vytvořením modelu je nutné zvolit, kterou šablonu chceme použít. Nejprve je tedy potřeba vytvořit svoji šablonu viz. Obrázek 4.3.
Otevře se editor pro vytváření šablon, vlastností hrozeb, kategorií hrozeb a typů



Obr. 4.2: Vlastnosti hrozeb

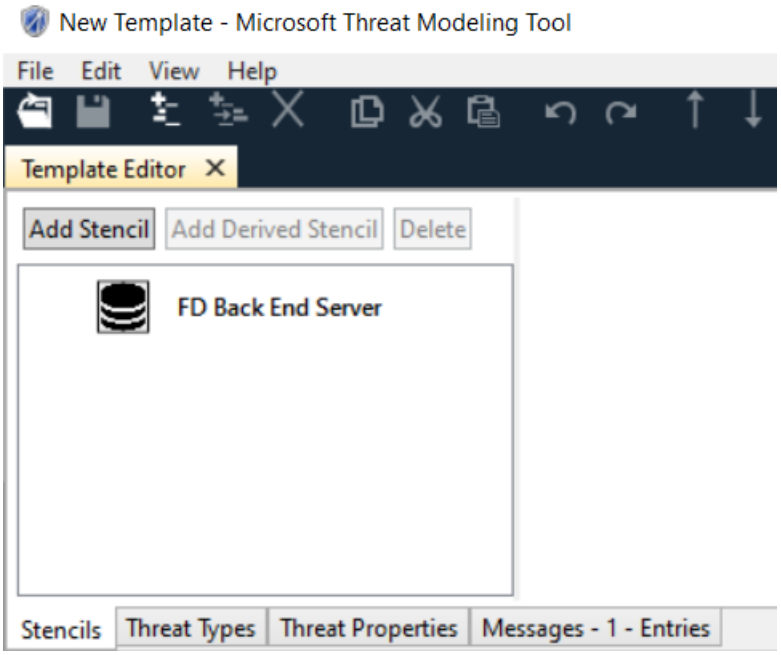
hrozeb. Pokud během vytváření šablony dojde k jakékoli chybě, zobrazí se ve složce "Zpráva" viz. 4.4.



Obr. 4.3: Tvorba šablony

Vzory jsou základní bloky pro vytváření modelů hrozeb. Na kartě Šablony byli vytvořeny vzorníky, ty se zobrazí v okně modelu ohrožení při vytváření modelu viz obrázek 4.4 a příloha.

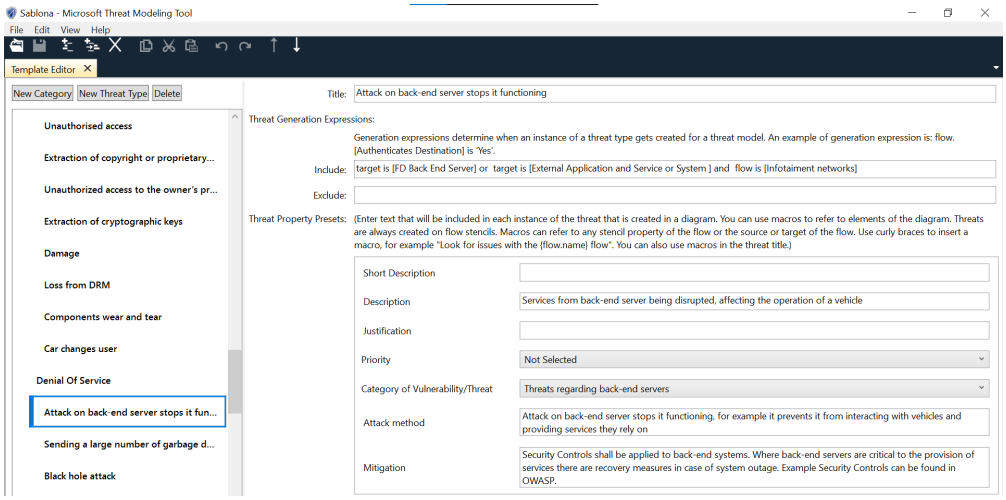
Na kartě "Typy hrozeb" byly na základě STRIDE vytvořeny nové kategorie hrozeb a nové typy hrozeb takže byly popsány způsoby jejich odstranění v položce INCLUDE byli přiraženy každé hrozbě vzorníky u kterých by ty hrozby mohli vyskytnout viz



Obr. 4.4: Záznam vytvářeného vzorníku

obrázek 4.5.

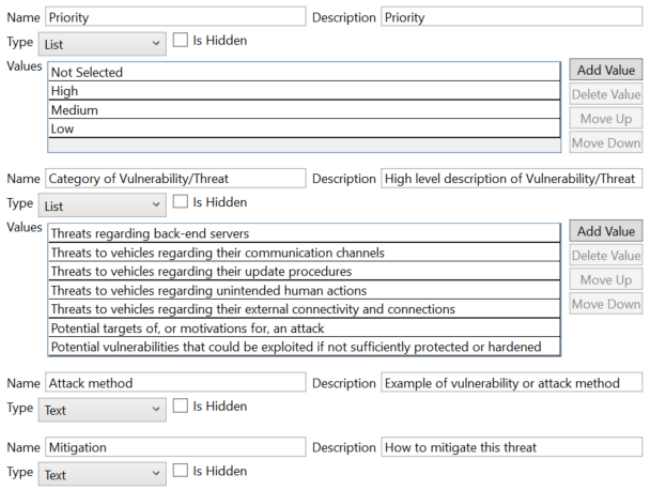
Ve výchozím nastavení mají hrozby sloupce Popis, Stručný popis, Odůvodnění, Interakce a Priorita. Na kartě "Vlastnosti hrozby" jsou tyto řádky šedé, kromě sloupce "Priorita" , protože je nelze změnit.



Obr. 4.5: Návrh odstranění hrozby

Tyto vlastnosti se zobrazí jako sloupce v seznamu hrozeb a panelech vlastností ohrožení v analytickém zobrazení modelu ohrožení, pokud je neoznačíme jako skryté.

Tam bylo vytvořeno více sloupců, které budou v budoucnu potřeba pro analýzu: Kategorie Zranitelnosti/Ohrožení, Metoda útoku, Zmírnění viz obrázek 4.6.



Obr. 4.6: Vlastnosti hrozby

4.2 Vytváření vlastního modelu

4.2.1 Komponenty

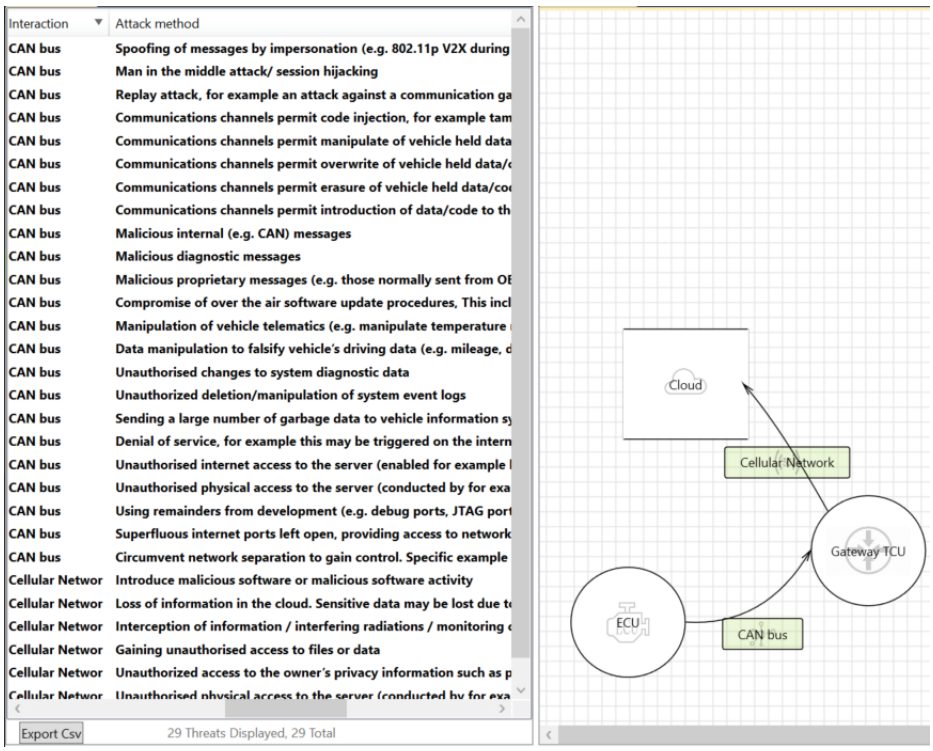
Komponenty pomoci kterých sestavujeme model:
BackEnd Server OnPremise a BackEnd Server in Cloud - přenáší data na back-endové servery patřící k různým entitám. Prvním z nich jsou servery patřící výrobci OEM samotného vozidla, které shromažďují údaje o výkonu a mohou je vzdáleně distribuovat, reprezentace cloudového úložiště.
Konfigurační soubor - soubory používané ke konfiguraci parametrů a počátečního nastavení některých počítačových programů. Používají se pro uživatelské aplikace, procesy serveru a nastavení operačního systému.
Physical device - jakékoliv zařízení, které se připojuje k autu
Komunikační kanály - lze široce definovat jako prostředek, kterým má být zpráva doručena nebo předána cílovému publiku, příjemcům a interakčním osobám. Může se jednat o přímou komunikaci tváří v tvář nebo komunikaci tváří v tvář. Lze jej také kategorizovat jako fyzický nebo mechanický.
Aktualizační procedury - server pro aktualizaci firmwaru/softwaru OTA (bezdrátově)
Zaměstnanci - osoba, která se stará o auto
Souborový systém - souborové systémy spravují data, která přicházejí do různých úložných zařízení uvnitř připojených automobilů. Stejně jako to, co se děje v

počítači, souborové systémy organizují data do souborů, což aplikacím usnadňuje hledání uložených dat.
Vlastník- řidič nebo majitel automobilu, který má fyzický přístup k vozidlu.
ECU - elektronická řídicí jednotka. Tolik komponentů v autě
Gateway TCU - HW modul centrální brány (telematická řídicí jednotka).
Port OBD - An On-Board Diagnostics II Port. Standardní způsob spolupráce vozidel jakéhokoli výrobce s nezávislými opravnami a prodejci za účelem testování emisních norem.
Mobilní telefon - který se připojí k autu a vytváří vnitřní síť
Infotainment systém - informační a zábavní systém ve vozidle.
Bezdrátový systém - komunikace mezi mobilními zařízeními ve vozidlech za účelem vytvoření místního a integrovaného informačního systému.
External Application and Service or System
Externí připojení
CAN bus - CAN je protokol sběrnice, který je vždy podporován, i když mohou existovat i jiné (General Motors také používá například GM-LAN). Samotný CAN je vysokorychlostní, promiskuitní protokol, který vysílá veškerý síťový provoz do všech uzlů na dané sběrnici.
Infotaiment networks - přístup k informačnímu a zábavnímu systému přes Bluetooth, USB nebo Wi-Fi
V2X komunikace - vozidlo ke všemu (infrastruktura, síť, vozidlo, chodec, zařízení, síť)
Mobilní síť - mobilní síť
Fyzická hranice vozidla
In Vehicle trust Boundary - Síť ve vozidle, která spojuje bezpečnostní nebo jiné kritické systémy a funkce. Předpokládá se, že entity v této síti jsou většinou důvěryhodné. Síť nemá žádnou nebo velmi slabou bezpečnostní ochranu.
Klíč vozidla - Znázornění zámku vozidla.
Sensory - radarové nebo ultrazvukové senzory.

4.2.2 Část modelu hrozeb

Na základě vytvořené šablony byl sestaven model auta, pro lepší pochopeni funkčností byl sestaven menší model z několika komponent propojený komunikačními kanály viz. obrázek 4.7 Na obrázku je vidět, že bylo vygenerováno 29 typů útoků působících na komponenty. Mělo by být vygenerováno 28 útoků, ale vzhledem k tomu, že jeden útok působí na dva kanály - CAN bus a Cellural Network, je útoků v součtu celkem 29.
Pro ověření, že model funguje tak jak má, jsem vytvořila tabulku s aktivy a tabulku

hrozbami a přiřadila každé hrozbě několik aktiv které by se to mohlo týkat. Důležité v přiřazení ke každé hrozbě je to, že pokud máme nějaké aktivum (např. ECU), musí k němu být připojen i nějaký kanál(např. CAN bus). Bez toho se pak nevygeneruje hrozba, například u hrozby "Malicious diagnostic messages" viz. níže
target is [ECU] or target is [Port OBD] or target is [Gateway TCU] and flow is [CAN bus]



Obr. 4.7: Část modelu

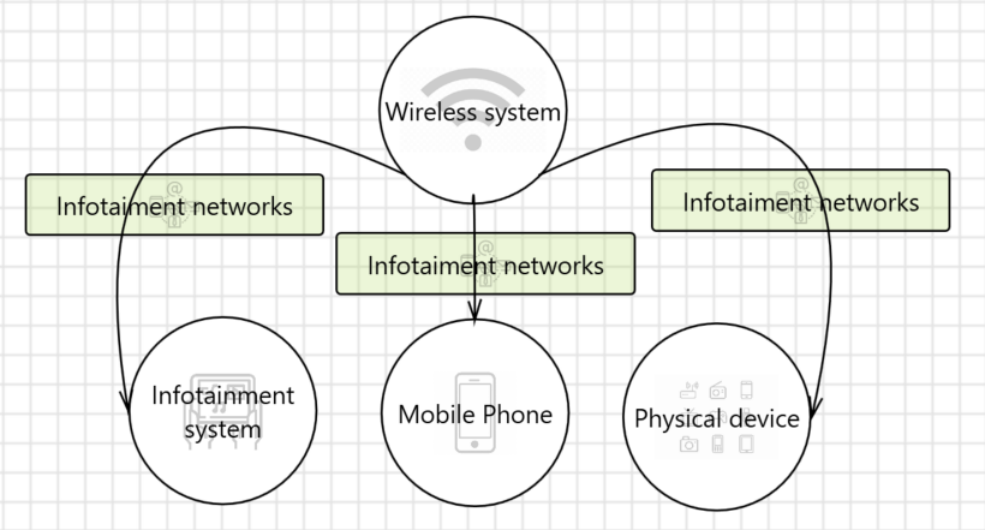
4.2.3 Vytváření infrastruktury auta

Celkový model auta byl sestaven podle mé představy a rozdělen na menši součástky pro průhlednost.

Multimédia

Když uživatel stiskne ovládací tlačítko na smartphonu, řídicí příkazy se odešlou na interní servery výrobce automobilu a tyto příkazy se odešlou do automobilu. Poté jsou prováděny operace dálkového ovládání, jako je odemykání/zamykání dveří, zapnutí klimatizace, blikající světla a dálkové parkování vozidla.[15]
Aby bylo možné provést vzdálené ovládání vozidla, musí útočník zachytit komunikaci mezi klientem a serverem (nebo mezi serverem a vozidlem).[15]

Nejprve se musí extrahovat ověřovací token, což jsou tajné informace potřebné pro dálkové ovládání, pomocí útoku typu man-in-the-middle.[15]
Útočník vytvoří vymyšlený bod Wi-Fi, který použije k připojení zařízení (například počítače s proxy serverem) na parkovišti.[15]
Uživatel (oběť) se připojí k hotovému hotspotu Wi-Fi a věří, že se jedná o skutečný hotspot Wi-Fi. Oběť se poté pokusí provést dálkové ovládání, například odemknout dveře.[15]
Když útočník ví, že se uživatel připojil k vymyšlenému bodu Wi-Fi, útočník zachytí komunikaci mezi smartphonem uživatele a serverem a předá jej přes zařízení útočníka.[15]
Útočník získá ověřovací token a řídicí příkazy, když uživatel zahájí příkaz odemknutí dveří ve smartphonu. Útočník pak může vozidlo volně ovládat, například odemknout dveře, blikat světly a ovládat klimatizaci po stanovenou dobu, během které je platný ověřovací token.[15]
V této situaci je pro útočníka obtížné ovládat jízdní funkce automobilu, když takovéto funkce nejsou pomocí smartphonu umožněny.



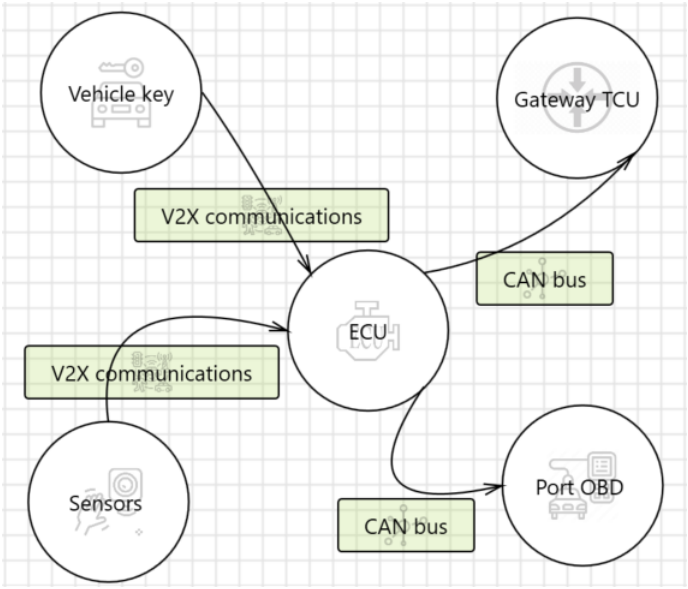
Obr. 4.8: Multimédia

ECU připojení

S ECU lze komunikovat prostřednictvím protokolu Control Area Network.Schéma zapojení ECU s ostatními systémy je zobrazeno na obrázku 4.9. Pomocí programu nebo zařízení pro zachytávání a analýzu CAN protokolu lze určit přenos náhodných nebo specifických paketů CAN do ECU vozidla, aby bylo možno deaktivovat, povolit, různé komponenty, senzory a funkce ve vozidle.[16]

Získaní plného přístupu k elektronické řídicí jednotce vozidla pomocí škodlivého firmwaru může způsobit:

- Zobrazení nesprávných údajů na displeji zařízení
- Zamknutí všech dveří
- Vypnutí veškerých vnitřních a vnějších osvětlení
- Odpojení ABS nebo celého brzdového systému
- Změna paliva a časování ventilů
- Zapnutí kontrolního světla motoru a odeslání nesprávného chybového kódu

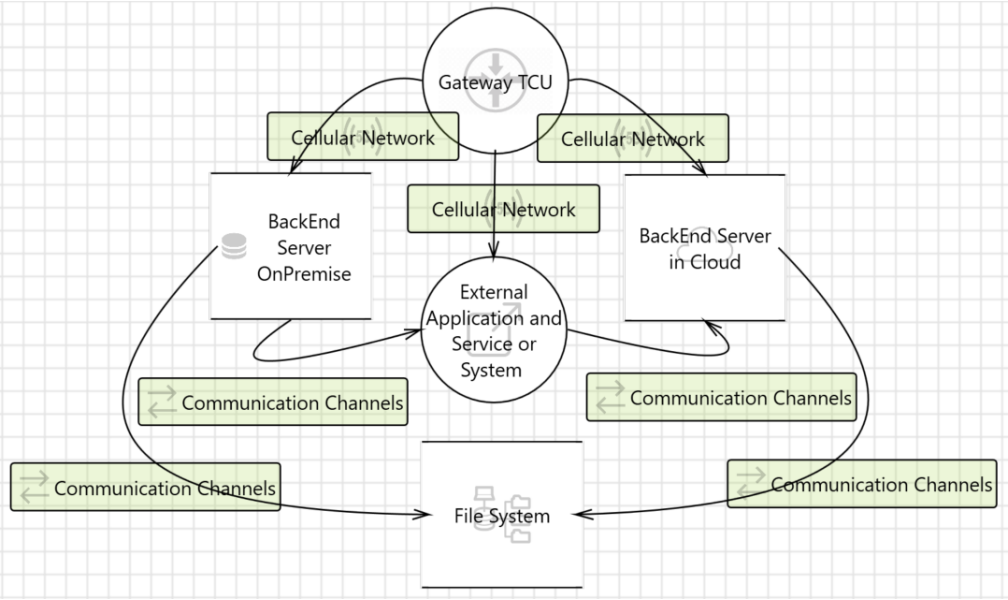


Obr. 4.9: ECU připojení

Gateway TCU připojení

TCU obsahuje mobilní modem, který poskytuje připojení k zařízení s vloženou SIM kartou. SIM karta se konfiguruje pomocí soukromého APN, což znamená soukromou celulární síť, která vyžaduje pro připojení přihlašovací údaje, takže je bezpečnější než veřejný APN. Zapojení TCU a systémů využívající jeho služby jsou zobrazeny na obrázku 4.10. TCU také používá VPN, která spojuje vozidlo se soukromými službami v podnikové síti (telematický server, OTA server atd.)[17]
Když útočník zaútočí na TCU může dostat údaje správce domény ze systémů mimo telematické prostředí. Nejen, že lze přistupovat k jakémukoli jinému serveru (a službám) v podnikové síti, ale pomocí přihlašovacích údajů správce domény je možné provádět libovolný kód na telematických serverech a potenciálně získat přístup ke všem vozidlům.[17]

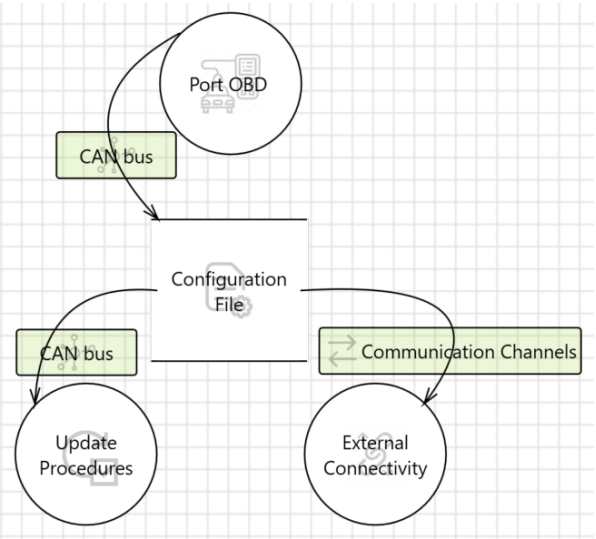
Souborový systém TCU také ukládá citlivá data vozidel, jako jsou hesla a certifikáty. Získáním certifikátů vozidel a jejich hesel se podaří získat přístup k interní síti vozidla.[18]



Obr. 4.10: Gateway TCU

Port OBD

S OBD-II je možné pokusit se naskenovat ECU a získat co nejvíce dat. Ovládání klíčových komponent (jako jsou světla, zámky, brzdy a motor) a zadávat kód do ECU pro přidání trvalých funkcí a připojení více sběrnic CAN.[19]
ECU navíc ukládá důležitá data, jako jsou údaje o nehodách, údaje o pojištění nebo indikátory záruky. Zapojení portu OBD-II je zobrazeno na obrázku 4.11. Taková data jsou také velmi užitečná pro škodlivou manipulaci. Například data, jako je rychlost vozidla, stav bezpečnostního pásu, poloha brzdového pedálu atd., Se obvykle zaznamenávají několik sekund před nehodou.[20]



Obr. 4.11: OBD port

Závěr

Seznámila jsem se s infrastrukturou u připojeného automobilu a s jejich řídícími komponenty (např. ECU), na které mohou útočníci zaútočit. Dozvěděla jsem se, jak se modelují hrozby, pomoci jakých metod a jaké nástroje k tomu lze využít. Podrobněji jsem se seznámila s rozhraním bezplatného nástroje od Microsoft Threat Modeling Tool.

Implementovala jsem vlastní šablonu pro další modelování, popsala v ní typy hrozeb a protiopatření, která se musí použít, aby pak při modelování infrastruktury auta bylo možné využít automatické generování hrozeb a opatření.

V práci jsem se setkala s problémy při přiřarování hrozeb jednotkám - některé se mi nezobrazovaly, protože software generuje útok na základě komunikačních kanálů, např. Pro realizaci modelování útoku na jednotku ECU je nutné vytvořit i komunikační sběrnici CAN bus. Pokud se hrozba týká jenom kanálu, nemusí být nutně přiřazená jednotka. Pro přehlednost byly uvedeny v tištěné podobě jen malé části infrastruktury auta.

Celkový model infrastruktury auto je v příloze, a v práci jsem uvedla ten samý model jenom rozpůlený po částech vztahující na ty hlavní komponenty auta pro přehlednost.

Literatura

[1] *How the connected vehicle offers solutions to today's fleet challenges. Fleetpoint [online]. London: Vehicle Data Powered by CVD & IDS, 2020 [cit. 2020-12-02].* Dostupné z URL: <https://www.fleetpoint.org/autonomous-vehicles/how-the-connected-vehicle-offers-solutions-to-todays-fleet-challenges/>.

[2] *NISA good practices for security of Smart Cars. Greece: European Union Agency for Cybersecurity (ENISA), 2019. ISBN 978-92-9204-317-9. TP-02-19-881-EN-N. Dostupné z: doi:10.2824/17802* Dostupné z URL: <https://www.enisa.europa.eu/publications/smart-cars>.

[3] *SHOSTACK, Adam. Threat Modeling: Designing for Security. USA, Indiana: John Wiley, 2014. ISBN 978-1-118-80999-0.*

[4] *The STRIDE Threat Model [online]. USA: Microsoft, 2009 [cit. 2020-12-02].* Dostupné z URL: <https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN>.

[5] *IriusRisk [online]. USA: IriusRisk, 2016 [cit. 2020-12-02].* Dostupné z URL: <https://iriusrisk.com/>.

[6] *NCC Group Template for the Microsoft Threat Modeling Tool 2016 for Automotive Security [online]. London: NCC Group, 2016 [cit. 2020-12-03].* Dostupné z URL: <https://github.com/nccgroup/The_Automotive_Threat_Modeling_Template>.

[7] *Uncover Security Design Flaws Using The STRIDE Approach [online]. USA: Microsoft, 2019 [cit. 2020-12-06].* Dostupné z URL: <https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach>.

[8] *Microsoft Security Development Lifecycle Threat Modelling [online]. USA: Microsoft, 2017 [cit. 2020-12-06].* Dostupné z URL: <https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>.

[9] *Buttigieg, Robert & Farrugia, Mario & Meli, Clyde. (2017). Security Issues in Controller Area Networks in Automobiles.*
Dostupné z URL:
<https://www.researchgate.net/publication/321124827_Security_Issues_in_Controller_Area_Networks_in_Automobiles>.

[10] *ENISA GOOD PRACTICES FOR SECURITY OF SMART CARS [online]. Europe: European Union Agency for Cybersecurity (ENISA), 2019, 2019 [cit. 2020-12-07]. ISBN 978-92-9204-317-9.*
Dostupné z URL:
<https://www.enisa.europa.eu/publications/smart-cars>.

[11] *Powertrain control module. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2020 [cit. 2020-12-07].*
Dostupné z URL:
<https://en.wikipedia.org/wiki/Powertrain_control_module>.

[12] *KLEBERGER, Pierre, Tomas OLOVSSON a Erland JONSSON. Security aspects of the in-vehicle network in the connected car. In: 2011 IEEE Intelligent Vehicles Symposium (IV) [online]. IEEE, 2011, 2011, s. 528-533 [cit. 2021-02-25]. ISBN 978-1-4577-0890-9. doi:10.1109/IVS.2011.5940525*
Dostupné z URL:
<http://ieeexplore.ieee.org/document/5940525/>.

[13] *TBATOU, S., A. RAMRAMI a Y. TABII. Security of communications in connected cars Modeling and safety assessment. In: Proceedings of the 2nd international Conference on Big Data, Cloud and Applications [online]. New York, NY, USA: ACM, 2017, 2017-03-29, s. 1-7 [cit. 2021-02-25]. ISBN 9781450348522. Dostupné z: doi:10.1145/3090354.3090412*
Dostupné z URL:
<http://dl.acm.org/doi/10.1145/3090354.3090412>.

[14] *Smith, C. (2016). The Car Hacker's Handbook. Nostarch.*
Dostupné z URL:
<https://nostarch.com/>.

[15] *J. Takahashi, M. Iwamura and M. Tanaka, "Security Threat Analysis of Automotive Infotainment Systems,"2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), 2020, pp. 1-7, doi: 10.1109/VTC2020-Fall49728.2020.9348647.*
Dostupné z URL:
<https://ieeexplore.ieee.org/abstract/document/9348647>.

[16] *Malicious ECU Attacks and Security. (2014). Retrieved May 18, 2021*
Dostupné z URL:
<https://sites.google.com/a/g.ucla.edu/malicious-ecu-attacks-and-security>.

[17] *FROM A SINGLE TCU TO FULL CONTROL. (2020). Retrieved May 18, 2021*
Dostupné z URL:
<https://upstream.auto/blog/from-a-single-tcu-to-full-control>.

[18] *Mercedes Benz security bug a sign of connected vehicle security issues?. (2020). Retrieved May 18, 2021, from*
Dostupné z URL:
<https://techhq.com>.

[19] *Ethical Automotive Hacking Simplified. (2020). Retrieved May 18, 2021*
Dostupné z URL:
<https://securitybyescrypt.com>.

[20] *Yadav, A., Bose, G., Bhange, R., Kapoor, K., Iyengar, N. C. S. N., & Caytiles, R. D. (2016). Security, Vulnerability and Protection of Vehicular On-board Diagnostics. International Journal of Security and Its Applications, 10(4), 405-422.*
Dostupné z URL:
<https://doi.org/10.14257/ijsia.2016.10.4.36>.

[21] *V2X in the Connected Car of the Future. (2018). Retrieved May 18, 2021*
Dostupné z URL:
<https://www.qorvo.com>.

Seznam symbolů, veličin a zkratek

STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
GPS	Global Positioning System
ECU	Electronic Control Unit
OEM	Original Equipment Manufacturer
ENISA	The European Union Agency for Cybersecurity
GNSS	Global Navigation Satellite System
AI	Artificial intelligence
C-ITS	Cooperative Intelligent Transport Systems
IVI	In-Vehicle Infotainment
RSU	Remote Concentrator Unit
CAN	Controller Area Network
ISO	International Organization for Standardization
MOST	Media Oriented Systems Transport
UICC	Universal Integrated Circuit Card
USB	Universal Serial Bus
TCU	Telematic control unit
GSM	Global System for Mobile Communications
SoC	State of charge
V2X	Vehicle-to-everything
OBD	On-Board Diagnostics
SQL	Structured Query Language
TMT	Threat Modeling Tool
SDL	Security Development Lifecycle

DFD	Data Flow Diagram
ARP	Address Resolution Protocol
DNS	Domain Name System
IP	Internet Protocol
TLD	Top Level Domain
API	Application Programming Interface
ACL	Access Control List
RAM	Random-access memory
CPU	Central Processing Unit
SDLC	Systems Development Life Cycle
OWASP	Open Web Application Security Project
LIN	Local Interconnect Network
HMI	Human-Machine Interface
ABS	Anti-lock braking system

A Přílohy

Final_Model.tm7
Sablona.tb7
Threat Modeling Full Report.htm