THE POTENTIAL USE OF PASSENGER CAR DATA TRAFFIC FOR RECONNAISSANCE PURPOSES

SZEMÉLYGÉPJÁRMŰVEK ADATFORGALMÁNAK MEGFIGYELÉSI CÉLÚ FELHASZNÁLÁSI LEHETŐSÉGEI

HEGYI Henrietta[1] – ERDŐDI László[2]

Abstract

As a by-product of the fourth industrial revolution, smart devices are also gaining ground in the home. As well as simple IoT devices, advanced passenger vehicles can be considered as such smart devices. As network communication functions become commonplace in vehicles, the opportunities for targeting them are also expanding. This paper will briefly describe the infocommunication systems of vehicles, illustrate through case studies its vulnerabilities and some of the ways in which the data can be exploited, and then attempt to sketch a situation that adequately exemplifies the possible consequences by means of a theoretical scenario.

Keywords

IoT, passenger vehicle, information security, botnet, reconnaissance

Absztrakt

A negyedik ipari forradalom egyik mellékhatásaként az okoseszközök egyre nagyobb teret nyernek a lakossági felhasználás terén is. Az egyszerű IoT eszközök mellett a fejlett személygépjárművek is ilyen okoseszközöknek tekinthetők. Ahogyan a járművek esetén a hálózati kommunikációs funkciók mindennapossá válnak, az őket célzó támadási lehetőségek is kiszélesednek. Jelen tanulmány röviden bemutatja a járművek infokommunikációs rendszereit, esettanulmányokon keresztül szemlélteti annak sérülékenységeit, illetve az adatok felhasználásának néhány módját, majd kísérletet tesz rá, hogy egy elméleti szituáció segítségével felvázoljon egy olyan szituációt, mely megfelelően példázza a lehetséges következményeket.

Kulcsszavak

IoT, személygépjármű, információbiztonság, botnet, megfigyelés

[1] hegyi.henrietta@uni-obuda.hu | ORCID: 0000-0002-7731-840X | Doctoratal Student, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University | Doktorandusz, ÓE Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem

[2] erdodi.laszlo@nik.uni-obuda.hu | ORCID: 0000-0002-4910-4228 | Senior Lecturer, John von Neumann Faculty of Informatics, Óbuda University | Adjunktus, Neumann János Informatikai Kar, Óbudai Egyetem

IOT ESZKÖZÖK ELTERJEDÉSE ÉS ADATGYŰJTÉSI TENDENCIÁK

A 4. ipari forradalom folyományaként az egész világon egyre elterjedtebbé válnak az okoseszközök. A negyedik ipari forradalom kifejezés Klaus Schwab nevéhez köthető, aki így foglalta össze:

„Mint ahogy az első ipari forradalom gőzzel működtetett gyárai, a másodiknál a tömeggyártás tudományának alkalmazása, továbbá a harmadik ipari forradalom során a digitalizáció elkezdése, addig a negyedik ipari forradalom olyan technológiái, mint a mesterséges intelligencia, a genomszerkesztés, a kiterjesztett valóság, a robotika és a 3D nyomtatás, gyorsan megváltoztatják azokat a folyamatokat és módszereket, ahogy az emberiség az értékeket létrehozza, cseréli és elosztja. Ahogy az az előző forradalmak során is történt, ez a változás is mélyen átalakítja az intézményeket, iparágakat és a magánszemélyeket is. Ennél is fontosabb azt észrevenni, hogy ezt a forradalmat az emberek ma meghozott döntései vezérlik. A világ 50–100 év múlva nagymértékben függ majd attól, hogy hogyan gondolkodunk ma ezekről a befektetésekről, és hogyan vezetjük be ezeket a nagy teljesítményű új technológiákat."

A negyedik ipari forradalom magával hozta az olyan újításokat is, amik mindannyiunk életét meghatározzák: az okostelefonok által irányítható okos lakberendezési tárgyakon át az okosórákig. Ahogyan Krasznay Csaba rámutat [1], akár már egy egyszerű kábel is tartalmazhat mikroprocesszorokat, melyekről nem feltétlenül tudjuk, hogy konkrétan milyen adatforgalmat bonyolítanak. A „digitális társadalom" létéhez ma már elengedhetetlenül hozzátartozik az, hogy egyre több internetre csatlakozó eszközzel vesszük körül magunkat. [1] Az IoT-eszközökkel, rendszerekkel és szolgáltatásokkal kapcsolatos veszélyek és kockázatok sokrétűek, és gyorsan fejlődnek, ráadásul rendkívül széles területet ölelnek fel. Ezért fontos megérteni, hogy pontosan milyen elméleti keretekkel, szabályozási környezettel lehetséges az ilyen eszközöket biztosítani és milyen operatív intézkedéseket kell kidolgozni, amelyek segítenek megvédeni őket a különböző fenyegetésektől. Ahogyan ezt az Európai Uniós Kiberbiztonsági Ügynökség, az ENISA is kiemeli, az IoT eszközök esetében éppen a komplexitás miatt jelent kihívást. [2]

Az egyre több tiszta, szenzorok általi adatot gyűjtő okoseszköz elterjedésével párhuzamosan a XXI. században kibontakozó másik fontos tendencia az egyes állami és nemállami szervezetek egyre nagyobb mértékű adatgyűjtési folyamatai. Világszinten az Egyesült Államok ellen indított 2001. szeptember 11-i terrortámadás jelentett olyan fordulópontot, melynek köszönhetően a kibertérből származó információk szerepe felértékelődött. Miután a globális szempontból is sokkoló terrortámadás körülményeit sikerült tisztázni, az Egyesült Államok lassan megkezdte a tömeges adatgyűjtési programjának elindítását, amelyről az Edward Snowden által nyilvánosságra hozott adatokból értesült a világ. Snowden és más, kevésbé ismert aktivisták és hackerek csoportjai rámutattak az átfogó programmal kapcsolatos szabályozási hiányosságokra. [3], [4]

2017-ben a CIA által kiszivárgott hacker eszközökről készült egy „Vault 7" nevű, a Wikileaks dokumentum. A leírás rávilágított, hogy a szervezet aktívan keresi a sebezhetőségeket olyan okoseszközökben, mint például az okostelefonok, okostelevíziók, vagy éppen a személygépjárművek. [1], [5]

PÉLDA AZ IOT ESZKÖZÖKKEL VALÓ VISSZAÉLÉSRE: A MIRAI BOTNET BEMUTATÁSA

Annak ellenére, hogy az IoT eszközök nem tekinthetnek vissza hosszú múltra, a több kompromittált eszközből álló hálózatok, melyeket szinkronizált támadásokhoz használnak, már ma sem számítanak újdonságnak. Az elsősorban beágyazott és IoT-eszközökből, főként webkamerákból álló Mirai botnet 2016 végén jelent meg az interneten, amikor több nagynevű célpontot hatalmas elosztott szolgáltatásmegtagadási (DDoS) támadásokkal sújtott.

M. Antonakakis et al. [6] *„Understanding the mirai botnet”* című tanulmányban hét hónapos visszatekintő elemzésben mutatja be a Mirai 600 ezer fertőzött eszköz csúcsra történő növekedéséről szóló, és a DDoS áldozatainak történetét. A 2016 szeptemberétől kezdődően tömeges elosztott szolgáltatásmegtagadási (DDoS) támadások sorozata ideiglenesen megbénította a Krebs on Security [7], az OVH[3] és a Dyn [6] működését. A Krebs elleni kezdeti támadás volumene meghaladta a 600 Gbps-ot [7] - ez az eddigi legnagyobbak közé tartozik. Figyelemreméltó, hogy ez az elsöprő forgalom az internet néhány százezer, az összes lehetséges host közül a legkevésbé „erősekről” – IoT eszközökről - származott, amelyek a Mirai nevű új botnet irányítása alatt álltak. A kutatók megállapították, hogy a botnet az első 20 órában közel 65 000 IoT-eszközt fertőzött meg, mielőtt elérte volna a 200 000-300 000 fertőzéssel járó stabil állapotot. [6] Ezek a botok a földrajzi régiók és autonóm rendszerek egy szűk sávjába estek, Brazília, Kolumbia és Vietnám aránytalanul nagy arányban jelentek meg a fertőzések forrásának helyszíneként, 41,5%-ot téve ki az összes lokációból.

A Mirai működése a következőképpen foglalható össze: a command and control szerver két socket listenert futtatott: egyet a Telnet-kapcsolatokhoz, egyet pedig egy programozott API-hoz. A Telnet socket a 23-as portot figyelte, és minden érvényes kapcsolatot a megfelelő bot vagy admin kezelőhöz irányított. Az API socket a 101-es portot figyelte, és a hozzá küldött érvényes támadási parancsokat továbbította a csatlakoztatott botokhoz. Továbbá, minden egyes csatlakoztatott bot új sebezhető eszközök után kutatott az interneten. Amint felfedeztek egyet, a hitelesítő adatait, IP-címét, és a hozzáféréshez használt portot elküldték a loader szervernek. Ez lehetővé tette az adatok fájlban történő eltárolását, majd rosszindulatú szoftver futtatását az eszközön. [8]

Bár Mirai a DVR-ektől kezdve az IP-kamerákon és routereken át a nyomtatókig számos eszközt megcélzott, a kutatók felfedezték, hogy végső eszközösszetételét erősen befolyásolta egy maroknyi fogyasztói elektronikai gyártó piaci részesedése és tervezési döntései. [8] Ennek egyik mutatója, hogy miközben a megfertőzött eszközök folyamatosan szkennelték az internetet, újabb és újabb gyenge eszközöket keresve találták meg például a beépített gyenge jelszavakat. Az ehhez hasonló sérülékenységeket kihasználva birtokba vették az új eszközt, majd a központtól érkező utasításokat alapján szinkronban hajtottak végre olyan támadásokat, amelyek többek között globális digitális szolgáltatásokat céloztak. [1]

A személygépjárművek adattovábbítási mechanizmusaik miatt szintén alkalmasak lehetnek a botnetek kialakítására, amennyiben a támadóknak többféle sérülékenységet egy-

[3] https://twitter.com/olesovhcom/status/778830571677978624

idejűleg sikerül kiaknázniuk. Az ehhez hasonló lehetőségekről már jelenleg is több tanulmány olvasható – ilyen például egy elektromos személygépjárművekből létrehozott botnetnek a villamos hálózatra gyakorolt lehetséges hatásairól szóló 2021-es tanulmány. [9]

SZEMÉLYGÉPJÁRMŰVEK ADATTOVÁBBÍTÁSI MECHANIZMUSAI ÉS SÉRÜLÉKENYSÉGEI

A modern járművek olyan összekapcsolt elektronikai rendszereket tartalmaznak, amelyek a kibertérben jelenlévő különböző fenyegető szereplők potenciális célpontjai lehetnek. Az személyautók ma már képesek interakcióba lépni környezetükkel azáltal, hogy adatokat cserélnek az városok lakosságának nyújtott szolgáltatások széles skáláját biztosító vezérlőállomásokkal. Ez ráadásul nem csak okosvárosokra vonatkozik – gondoljunk csak a telekommunikációs hálózattal való összeköttetésre. A járművek ezenkívül kifinomult vezérlőket tartalmaznak, amelyek valós időben kezelik az érzékelők hálózatán keresztül gyűjtött adatokat. Ennek köszönhetően hasonló szerephez jutnak a kibertérben, mint a mobiltelefonok vagy a számítógépek. Amennyiben a gyártó, azaz az úgynevezett OEM (original equipment manufacturer) és alvállalkozói nem gondoskodnak a megfelelő védelemről a hackerek átvehetik a jármű irányítását azáltal, hogy a CAN-buszon nagyszámú vezérlőhálózati csomagot (normál és diagnosztikai csomagokat egyaránt) küldenek a belső alkatrészeknek. Ha a rosszindulatú csomagok a jogos csomagok előtt érkeznek az ECU-khoz (engine control unit), az alkatrészek érvényesnek tekintik azokat.

A normál csomagokat a támadók többféle komponens manipulálásának céljából küldhetik, beleértve az autó sebességmérőjét, kilométer-számlálóját, a fedélzeti navigációs rendszert, a kormányzást, a kamerarendszert, a fékeket és a gyorsítást. A diagnosztikai csomagokkal a jármű néhány komponensének viselkedésének megváltoztatása idézhető el, mint például a fékek kezelése, a motor leállítása, a lámpák villogása, az ajtók zárása/kioldása és az üzemanyagszint-mérő módosítása. A normál csomagokkal ellentétben az ECU-nak küldött diagnosztikai tevékenységeket hitelesíteni kell. A hitelesítési folyamat gyenge végrehajtása azonban komoly kockázatot jelent a felhasználók számára.

Támadás formája	Leírás
Telematikai rendszerek elleni támadások	A telematikai rendszerek lehetővé teszik, hogy a járművek egy távoli központtal kommunikáljanak, telemetriai adatokat és egyéb információkat cseréljenek vele. Egyes autógyártók már most is kínálnak ügyfeleiknek telemetriai szolgáltatásokat távdiagnosztikai célokkal, amelyekkel megelőzhetők a véletlen balesetek és az elektronikai hibák. A támadók kihasználhatják e rendszerek sebezhetőségeit, hogy potenciálisan beavatkozzanak a fedélzeti alkatrészekbe és módosítsák azok paramétereit, megváltoztassák a jármű reakcióját a vezető utasításaira.
Rosszindulatú programok kihasználása	Egy támadó személyre szabott rosszindulatú szoftvereket juttathat be egyes autóalkatrészekbe, módosítva azok viselkedését, vagy szolgáltatásmegtagadási állapotot idézhet elő. Egy rosszindulatú programot kü-

Támadás formája	Leírás
	lönböző módokon lehet bejuttatni a rendszerbe. Például egy MP3-olvasóba dugott USB-stick segítségével vagy vezeték nélküli technológián (Wifi, Bluetooth, mobilkommunikáció) keresztül.
Jogosulatlan alkalmazások	A fedélzeti számítógépek alkalmazásokat és a kapcsolódó frissítéseket tölthetnek le és hajthatnak végre. Egy fenyegető szereplő saját céljai elérése érdekében módosíthatja ezeket az alkalmazásokat. Egy klasszikus ellátási lánc elleni támadás során a hackerek olyan hamisított frissítést juttathatnak be az autóba, amely a járműre telepítve és végrehajtva lehetővé teszi a támadók számára, hogy további rosszindulatú tevékenységeket hajtsanak végre.
OBD porton keresztüli hozzáférés	A testreszabott szoftverek kihasználhatják az OBD-II (fedélzeti diagnosztikai) portot a telepítéshez. Ha a csatlakozóhoz a CAN-buszon keresztül hozzáférnek, lehetőség nyílik a csatlakozóhoz csatlakoztatott minden alkatrész megfigyelésére.
Ajtózárak és kulcstartók	Egy támadó utánozhatja a kulcscsomók és ajtózárak által a zárak vezérlésére és az autómotorok indítására/leállítására használt hozzáférési kódot.

1. Táblázat - Gyakori személygépjárműveket érő támadástípusok, saját szerkesztés.

Jelen tanulmány szempontjából az első három támadástípus bír relevanciával, mivel ezekhez van szükség internetcsatlakozásra. Ahhoz azonban, hogy a lehetséges veszélyeket jobban megértsük, érdemes áttekinteni a személygépjárművek belső hálózatának sajátosságait is. A következő generációs elektromos architektúráinak, azaz EEA (Electrical/Electronic Architecture) egyik legjelentősebb kihívása a jármű elektronikus alkatrészei közötti nagysebességű kommunikáció kezelése a költségek szinten tartása mellett. Az alábbi táblázat a főbb belső hálózati protokolltípusokat foglalja össze:

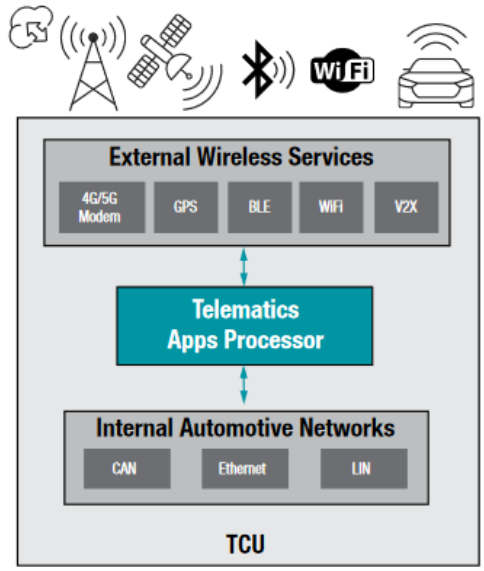
Protokoll neve	Leírás
CAN (Controller Area Network)	A jelenlegi autóipar legsikeresebb kommunikációs hálózata a CAN protokoll. A CAN protokollt a Bosch vállalat fejlesztette ki, és 1986-os megjelenése óta a legszélesebb körben használt szabvány a járműhardverek kommunikációjának területén. [10] Más hálózati technológiákhoz képest a CAN kiemelkedő előnyökkel rendelkezik a költséghatékonyság és a rugalmasság terén. A CAN egyik változata a rugalmas adatátviteli sebességű (CAN-FD) [11], [12] amely akár 8 Mb/s sávszélességű [13]. A CAN egy többmesteres hálózat, amelyben min-

Protokoll neve	Leírás
	den csomópont egyformán és egymástól függetlenül fogadhat és sugározhat információt. Ezzel a tulajdonságával a CAN szinte „plug-and-play" módon működik: új ECU-k vagy diagnosztikai eszközök könnyen csatlakoztathatók a hálózathoz a hálózat külön módosítása nélkül. Ez azonban a kommunikációs rendszert is sebezhetővé teszi a támadásokkal szemben. [13]
LIN (Local Interconnect Network)	A helyi összekötő hálózat (LIN) lehetővé teszi az alacsony költségű és rugalmas vezetékkötegek kialakítását, és könnyen megvalósítható speciális támogatási követelmények nélkül. A LIN sávszélességi kapacitása azonban csak 20 kb/s. Általában az ablakok tekerését és az ülések vezérlését végző kapcsolókban és motorokban használják.
FlexRay	A FlexRay protokollt úgy tervezték, hogy támogassa a jármű biztonságkritikus funkcióinak ellátására szolgáló elektromos/elektronikus rendszerek használatát, beleértve a "brake-by-wire", "suspension-by-wire", "steer-by-wire" és általában az "x-by-wire" elven működő kapcsolatokat. [14] A beépített időszinkronizációs mechanizmusnak köszönhetően a FlexRay kis időbeli késleltetés mellett is képes biztosítani a biztonságkritikus komponensek közötti valós idejű kommunikációt.
MOST (Media Oriented Systems Transport)	A MOST (Media Oriented Serial Transport) egy másik járműfedélzeti hálózat. A MOST-ot a járművekben található infotainment eszközök és kapcsolódó alkalmazások támogatására fejlesztették ki. [15], [16], [17] Fizikai rétegként műanyag optikai szálakat használ, így a hálózat el van szigetelve az elektromágneses interferenciától (EMI), ami megakadályozza az olyan problémákat, mint a zúgó hangok az infotainment rendszerben. [17]
Ethernet – TCP/IP	Ahogy az autók egyre inkább összekapcsolódnak, egyre több adatra van szükségük, ami miatt az Ethernet egyre elterjedtebbé vált az autókban – az átjárók ennek az igénynek a kielégítésére fejlődtek ki. Míg a régebbi átjárók kisebb, egyszerűbb mikrokontrollereket (MCU-kat) használtak vezérlőként, az újabb átjárók processzorokat használnak, néha egy kiegészítő MCU-val kiegészítve. A processzor és az MCU közötti különbség a memóriában rejlik - a processzorok külső memóriával rendelkeznek, míg az MCU-k mindent a chipen tárolnak. A processzorokra való áttérés oka részben a támogatási szempontokban keresendő. Sok processzorban az Ethernet és az azt támogató szoftver is integrálva van. A több memóriával rendelkező processzorok népszerű

Protokoll neve	Leírás
	operációs rendszereket, például Linuxot futtatnak, ami nagyobb hordozhatóságot tesz lehetővé, és csökkenti a fejlesztési időt. [18], [19]

2. Táblázat - Személygépjárművek belső hálózatának jellemző protokollja, saját szerkesztés.

A fent felsorolt belső hálózatokat egyre több jelenleg is forgalmazott személygépjármű esetében egy beépített „router", a TCU (Telematics Control Unit) [20] köti össze a telekommunikációs hálózattal – a TCU tehát tulajdonképpen egy olyan ECU, amely kapcsolatot biztosít az internethez. Az internethez és a felhőhöz csatlakozó autók egyre inkább mindenütt jelen vannak, mivel az autógyártók a járműveket Wifi, Bluetooth és mobil adatátviteli lehetőségekkel szerelik fel. Az ilyen csatlakoztathatóság lehetővé teszi a segélyhívást (eCall). valamint a szórakoztató és egyéb tartalmak elérését online hozzáféréshez utazás közben, valamint az OTA-szolgáltatás mellett szoftverfrissítéseket biztosít az autóban lévő digitális tartalomhoz. [20] Hogy a jármű szórakoztatóelektronikai eszközeire a gyártó „over-the-air", azaz OTA frissítéseket küldhessen, azért van szükség, mert így anélkül teszi lehetővé a szoftverek naprakészen tartását, hogy a tulajdonosnak fel kéne keresnie egy szervizt. Ez természetesen nem csak kényelmi funkció, hanem olyan szempontból is hasznos lehet, ha éppen biztonsági rések kijavítását kell minél gyorsabban megoldani. Mivel azonban a járművek a mobiltelefonokhoz hasonlóan egyszerű HTTPS protokollon keresztül kommunikálnak, így ezekhez hasonlóan kitettek a különböző sérülékenységeknek.



1. ábra - Egy telematikai rendszer sematikus rajza, Subbu Venkat 2020. [20]

Az 1-ábra egy telematikai rendszer sematikus rajzát mutatja. A TCU-k a csatlakoztathatóság biztosításához mobil vagy Wifi modemmel, a modemtől kapott adatok feldolgozásához pedig alkalmazásprocesszorral rendelkeznek. A feldolgozás magába foglalja az adatok dekódolását, az adatok érvényesítését és továbbítását az átjáróhoz vagy egy másik

tartományi ECU-hoz. A jelenlegi architektúrákban a modem és a processzor egyetlen félvezető eszközbe van integrálva. Mivel azonban a modemszabványok folyamatosan fejlődnek, az autógyártók egyre inkább olyan architektúra felé fordulnak, amely elválasztja a modemet a processzortól. Ezenkívül mind az autóipari átjárók és a TCU-k is egyre inkább Ethernet-alapúvá válnak. A modemnek a processzortól való elválasztásának előnye, hogy az ECU gyorsan átállítható egy új modemszabványra mindössze a modem cseréjével, megőrizve a processzort és az összes kapcsolódó és rajta futó szoftvert. [20] Bár a biztonság és a védelem ebben a tekintetben is egyre fontosabbá válik, sajnos gyakran még mindig a költségek döntenek. Egy dedikált beágyazott biztonsági processzor vagy alrendszer segíthet megvédeni a jármű biztonsági kulcsaihoz való hozzáférést, a kommunikációs csatornák biztonságának fokozását. A biztonsági funkciók jellemzően diszkrét MCU-kban valósulnak meg, amelyek tanúsítvánnyal rendelkeznek. Az alkalmazásprocesszorokat és a biztonsági MCU-t is integráló SoC (system-on-chip) azonban alacsonyabb anyagköltséget kínál az autóipari OEM-eknek. [20]

2016-ban a Keen Security Lab, kínai biztonsági kutatók egy csoportja felfedezett egy módszert a Tesla modellekben található CAN-busz feltörésére, amely a kijelzőket és a fékeket vezérli. [21] A kutatók képesek voltak távolról hozzáférni a központi vezérlőegységhez, és beállítani a tükröket, bezárni az ajtókat, manipulálni a műszerfalat, sőt még a fékeket is be tudták kapcsolni. Ezt jelentették a Teslának, a cég pedig egy újonnan kiadott frissítéssel reagált a bejelentésre. Ez az esemény azonban egyértelműen rávilágított arra, hogy az alkalmazott elavult szoftverrel valóban probléma van. Néhány évvel később szintén a Keen Security Lab egy másik csapata 14 sebezhetőséget fedezett fel a BMW által gyártott járművekben. [22] Felfedezték, hogy egy hiba kihasználásával hozzáférhetővé válik a telematikai vezérlőegység, valamint a CAN-busz. A Teslához hasonlóan a BMW válasza az volt, hogy frissítéseket vezetett be az érintett modellekhez. Ezeket OTA (over-the-air) megoldással, az interneten kapcsolaton keresztül vagy a BMW márkakereskedésekben tették elérhetővé az ügyfelek számára. Hasonlóan, holland kutatók felfedeztek egy módszert, amellyel meg lehet kerülni a rádiófrekvenciás azonosításon (RFID) alapuló kulcsos indításgátlókat, [23] amelyeket 1996 óta számos autógyártó elsődleges biztonsági funkcióként használ. A szerzők egy olyan módszert alkalmaztak, amely megkerüli a kriptográfiai hitelesítést, miközben kevesebb mint 6 perc alatt, speciális hardver nélkül elvégezhető.

Egy másik példa a személygépjárművek feletti irányítás megszerzéséhez Sam Curry webalkalmazások biztonságával foglalkozó kutató 2023 január 3-i esettanulmánya [24], melyben részletes leírást ad több ismert márka rendszereihez való távoli hozzáférésének lehetőségeiről. A teszt során Curry és csapata a következő adatokhoz fért hozzá a teljesség igénye nélkül: a tulajdonos elérhetőségei, email címe, telefonszáma (pusztán az alvázszám ismeretében) és a következő rendszereket volt képes távolról irányítani: elektromos zár, motor (indítás is), precíziós lokáció, fényszórók, duda, a felhasználói fiók lecserélése (azaz a felhasználó kizárása az autóból), hozzáférés a 360 fokos kamerához élő felvételek készítésével, távoli kódok futtatása, hozzáférés a memóriák tartalmához, illetve egyes márkák esetében hozzáférés a vállalat dolgozóinak adataihoz.

A támadás kiindulópontja lehet maga a személygépjármű is, de jellemzőbben az OEM (gyártó) vagy forgalmazó központi szerver webes felületeinek valamelyike számít alkalmas célpontnak, ahonnan egyidejűleg több jármű felé is továbbíthatóak az utasítások. Tekintettel arra, hogy az adattovábbítás nem feltétlenül csak a gyártó felé folyhat, hanem

más telematikai vállalatok is részt vehetnek annak valamelyik szakaszában, így a potenciális támadási felület is kiterjedt. A sérülékenységek eredhetnek félrekonfigurált webalkalmazásokból, hozzáférhető API végpontokból (különösen figyelemreméltó példa erre a leírásban szereplő TOTP generálást lehetővé tevő végpontra vonatkozó rész). [24] Amennyiben a támadó hozzáfér a vállalaton belüli kommunikációs csatornákhoz és/vagy a vállalat forráskód repository-jaihoz, olyan információk megszerzésére lesz képes, melyekkel könnyen megértheti a fedélzeti rendszer biztonsági funkcióinak működését és megtalálhatja a további sérülékenységeket, melyek az egyes járművekkel való közvetlen kommunikációt lehetővé teszik számára.

További példa a Tesla Kínai Népköztársaság egyes területeiről való kitiltásának története. Az Állampárt a Tesla sanghaji gyárának megnyitását követően aggodalmát fejezte ki azzal kapcsolatban, hogy a járművek korlátlanul készíthetnek felvételeket még az olyan magas biztonsági besorolású helyekről is, mint például a katonai bázisok – amennyiben bejutnak egy ilyen területre. [25] Figyelemreméltó az a tény, hogy a párt egy magasszintű, zárt, éves megbeszélésének időpontjával kapcsolatban a márka járművei teljesen kitiltásra kerültek „legalább két hónapos időtartamra" a teljes helyszínül szolgáló pekingi városrészből. [26] Ez az információ abban a tekintetben is különlegesnek számított, mert a rendszeresen megtartott találkozó dátumát hagyományosan nem szokták nyilvánosságra hozni. Hasonló helyzet alakult ki Csengduban is, ahol a kitiltás tényéről sem látott napvilágot hivatalos információ, egyszerűen a Tesla tulajdonosok figyeltek fel rá, hogy bizonyos városrészekre nem engedik be őket a rendőrök. A kínai esetekkel kapcsolatban Elon Musk úgy nyilatkozott, hogy a Tesla autói nem kémkednek sem Kínában, sem máshol, és hogy a céget bezárnák, ha ez megtörténne. [27] Hónapokkal később a vállalat közölte, hogy az általa Kínában értékesített autók által generált összes adatot az országban tárolják. Az iparág és a szabályozó hatóságok számára világszerte egyre nagyobb kihívást jelent annak ellenőrzése, hogy ezeket a képeket hogyan használják fel, hová küldik és hol tárolják. 2021-ben a Tesla sanghaji üzemében készült az amerikai autógyártó által világszerte leszállított 936 000 jármű mintegy fele.[4], [26] Kína ráadásul hatalmas piac is a Tesla és az elektromos járművek számára.

EGY MEGFIGYELÉST CÉLZÓ TÁMADÁS LEHETSÉGES FORGATÓKÖNYVÉNEK BEMUTATÁSA

Az fejlett személygépjárműveket különböző fenyegető szereplők vehetik célba, például olyan személyek, akik megpróbálnak megtámadni egy adott autót, hogy annak rendszereit valamilyen célból a saját szolgálatukba állítják vagy éppen magánadatokat szerezzenek a jármű rendszereiből. Jelen tanulmányban a kifinomultabb támadástípusokra összpontosítunk, amelyek az intelligens járművek hálózatát és adatfolyamát használják. Az általunk elemzett forgatókönyvben feltételezzük, hogy a fenyegető szereplőnek több autóhoz is hozzáférése van, és a rendszeres adatkommunikációt használja titkos csatornaként a rosszindulatú tevékenység végrehajtására. Megközelítésünk az személygépjárművet a korábbi fejezetekben bemutatott információkra építve speciális IoT eszköznek tekinti, amely rendszeres hálózati kommunikációval rendelkezik.

[4] https://carsalesbase.com/china-tesla/

A több járműhöz és azok adataihoz való hozzáférés egyedülálló lehetőséget biztosít a fenyegetést okozó szereplők számára. Vélelmezzük, hogy a fenyegető szereplő hozzáférhet az összes szükséges intelligens járműadathoz, mint például a következőkhöz:

- a jármű GPS-koordinátái az időbélyegzőkkel együtt;
- a jármű által belülről és kívülről készített kameraképek, azok időbélyegzőjével együtt;
- a jármű belsejében zajló hangkommunikáció, szintén az időadatokkal együtt.

Azt is figyelembe vesszük, hogy a jármű rendelkezik a következőkkel:

- rendszeres kommunikáció az akkumulátorra vonatkozó naprakész adatok szolgáltatása érdekében;
- rendszeres kommunikáció a szoftverfrissítések ellenőrzésére;
- rendszeres kommunikáció az önvezető adatok megszerzésére és jelentésére;
- rendszeres kommunikáció a gépjármű-biztosítóval.

Feltételezésünk szerint a fenyegető szereplő képes ezen adatcsatornák egyikét használatba venni és a kommunikációt rejtett csatornaként használni a rosszindulatú tevékenység elrejtésére. Az alábbiakban tehát azt feltételezzük, hogy a járművek egy jelentősebb csoportjához egy külső szereplő hozzáfér, ezáltal lehetősége van egy előre meghatározott algoritmus alapján adatokat lekérni. Ilyen adat lehet pl. az autó külső kameráinak felvételei. Ezek alapján néhány elméleti lehetőséget vizsgálunk. A különböző lehetőségek vizsgálatánál két alapvető jellemzőt figyelembe kell vennünk:

- az algoritmus komplexitása, amit a személygépjárműnek végre kell hajtania a megfigyelő művelet során;
- a többletadatok mennyisége, amit a személygépjárműnek továbbítania kell a támadó (megfigyelő) felé.

Mivel a fenti körülményeket vizsgáló, az itt bemutatott elméleti modellhez hasonló leírás a tanulmány írásának időpontjában nem állt rendelkezésre, így a továbbiakban ismertetett információk során a szerzők által kikalkulált értékek bemutatására kerül sor.

Kijelölt területek megfigyelése

Egy elméleti lehetőség a kijelölt objektumok környezetének megfigyelése. Egy ilyen jellegű támadásnál a jármű GPS koordináták alapján aktiválja a megfigyelést. Az algoritmus tehát annak aktuális pozícióját figyeli és abban az esetben, ha egy meghatározott pozícióba kerül, fényképeket készít a külső kamerák segítségével. Ezen fényképeket a telekommunikációs hálózaton keresztül képes továbbítani a támadó felé. A támadó algoritmus komplexitása ebben az esetben alacsony. A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos helypozíció figyelés, adott pozíciókban az extra funkciók aktiválása és deaktiválása;
- aktivált állapotban fényképek készítése;
- az elkészített képek azonnali vagy késleltetett rejtett továbbítása.

Az általunk alkalmazott modell a kontrollált autók számából mint bemenő adat és a forgalom nagyságából kiindulva vizsgálja a támadó lehetőségeit. Vizsgálatunkhoz egy Budapest nagyságú várost feltételeztünk 500.000 autóval. Az autók eloszlása a városban

nem egyenletes, illetve a gépjármű tulajdonosának lakhelye, munkahelye és egyéb életvitelszerű mozgása befolyásolja az autó lehetőségeit. Mindezektől függetlenül egyszerűsített módon azt feltételeztük, a városban lévő autók egyenletesen járják a várost. További feltételezéseink a megfigyelt épülettel kapcsolatosak. Az elkészített vizsgálatunkban azt feltételezzük hogy a megfigyelt épületben emberek dolgoznak vagy laknak. Egy ember legalább napi 4 percet az épületen kívül, de az épület környezetében van, az okos autók által vizuálisan elérhető területen (2 perc érkezéskor, 2 perc távozáskor).

A forgalom nagyságát percenkénti áthaladó autószámmal vesszük figyelembe. Egy egysávos úton 50-es tempóval 10 autó halad át percenként egy sávban. Az autók száma természetesen függ a napszaktól, a sávok számától és az esetleges közlekedési dugóktól, lámpáktól és a megengedett sebességtől. A vizsgálatunk másik bemenő paramétere a kontrollált autók száma. Megvizsgáltuk a lehetőséget azokban az esetekben ha a támadó 1, 100, 1000, 10.000 illetve 100.000 gépjármű adataihoz fér hozzá:

autók száma melyekhez a támadó hozzáfér	**5 gépjármű percenként / napi 5000**	**10 gépjármű percenként / napi 10000**	**20 gépjármű percenként / napi 20000**	**40 gépjármű percenként / napi 40000**
1 gépjármű	kb. évente 2 fotó	kb. 3 havonta egy fotó	kb. havonta egy fotó	kb. 2 hetente 1 fotó
100 gépjármű	kb. naponta egy fotó	kb. naponta 2 fotó	kb. 4 óránként egy fotó	kb. 2 óránként egy fotó
1000 gépjármű	kb. 2 óránként egy fotó	kb. óránként egy fotó	kb. fél óránként egy fotó	kb. 15 percenként egy fotó
10.000 gépjármű	10 percenként egy fotó	5 percenként 1 fotó	2-3 percenként egy fotó	1-2 percenként egy fotó/teljes megfigyelés
100.000 gépjármű	percenként egy fotó / teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés

3. Táblázat - Kijelölt területek megfigyelése, saját szerkesztés.

Kijelölt személyek megfigyelése

A kijelölt személy megfigyeléshez tartozó algoritmus komplexitása ebben az esetben lényegesen magasabb. Ebben az esetben a gépjárműnek folyamatos arcfelismerést kell végeznie a kamerák képeiből. A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos arcfelismerés a vizuálisan elérhető személyekre, adott személy beazonosítása esetén a további szükséges funkciók aktiválása;
- aktivált állapotban fényképek tárolása és a GPS adatok lementése;
- az elkészített képek és GPS adatok azonnali vagy késleltetett rejtett továbbítása.

A kijelölt személy megfigyeléséhez azt feltételezzük hogy a célszemély napi 20 perc és 2 óra közötti időtartományt tartózkodik az utcán, az okos gépjárművek által vizuálisan elérhető területen:

autók száma amihez a támadó hozzáfér	**napi 20 perc az utcán**	**napi 40 perc az utcán**	**napi 1 óra az utcán**	**napi 2 óra az utcán**
1 gépjármű	kb. 100 naponta egy detektált pozíció	kb. 50 naponta egy detektált pozíció	kb. 20-30 naponta egy detektált pozíció	kb. 10-20 naponta egy detektált pozíció
100 gépjármű	kb. naponta 1 detektált pozíció	kb. naponta 2 detektált pozíció	kb. naponta 3 detektált pozíció	kb. naponta 6-8 detektált pozíció
1000 gépjármű	naponta 10 detektált pozíció	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés
10.000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés
100.000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés

4. Táblázat - Kijelölt személyek megfigyelése, saját szerkesztés.

ÖSSZEGZÉS

Jelen tanulmányban a személygépjárművekhez kapcsolódó megfigyeléssel kapcsolatos kibertámadások lehetőségeit vizsgáltuk. Elemeztük a rendelkezésre álló információkat, az egyes autótípusok sajátosságait, az eddig publikált támadásokat és egyéb ezzel kapcsolatos kiszivárgott információkat. Megvizsgáltunk néhány elméleti lehetőséget feltételezve hogy a támadó hozzáfér egy vagy több okos személygépjármű erőforrásaihoz.

A vizsgáltaok alapján arra jutottunk, hogy egy (vagy főként több) személygépjármű belső rendszereihez való hozzáférés természetesen nagyobb feladat, mint a korábbiakban bemutatott IoT botnetek létrehozása. Azonban a megfelelő erőforrások birtokában egyáltalán nem tűnik lehetetlennek. Egy az általunk kidolgozott forgatókönyvhöz hasonló eset megvalósulása komoly személyi biztonsági, vagy adott esetben nemzetbiztonsági kockáza-

tot is jelenthet. Míg a tanulmányok túlnyomó része kifejezetten az automata járművek, illetve a V2x technológiák biztonságának kérdésköreit járja körül, fontos, hogy a már jelenleg is elterjedt és használatban lévő rendszerek biztonságára is megfelelő figyelem irányuljon.

Az adatokhoz való hozzáférés révén okozott károk nagysága és típusa nagyban függ a támadó kapacitásaitól és céljaitól is, így további kutatás alapját képezheti ezeknek a céloknak az ismertetése. Amennyiben a támadó olyan nagy erőforrásokkal rendelkező szervezet, mint például egy állami támogatást élvező hacker csoport, abban az esetben a támadás akár szofisztikáltabb módon, annak napvilágrakerülése nélkül is véghezvihető.

További kutatási lehetőséget ad a potenciális célpontok szerinti vizsgálat is. Az OEM-en és a kereskedőkön túl célponttá válhatnak a különböző flották adatainak kezelésére specializálódott telematikai vállalatok. Az ilyen szolgáltatók különböző eszközöket biztosítanak ügyfeleik számára, hogy azok pontosan nyomon követhessék a gépjárműflottájuk egyes elemeinek mozgását, helyzetét vagy bármilyen más, az igényeknek megfelelő információt, akár kameraképekkel is. Amennyiben egy flotta esetében alkalmazott fejlett telematikai rendszerhez fér hozzá a támadó, akkor az hasonló aggodalmakra adhat okot, hiszen ezek az eszközök kifejezetten nyomkövetési célt, illetve az autóról és környezetéről folyó adatgyűjtést szolgálják. A flotta alatt ráadásul nem csak logisztikai vállalatokat érthetünk, hanem például a rendőrség vagy egyéb hatóságok, mentők, tűzoltók járműveit is, akik esetlegesen szenzitív helyekre is beléphetnek.

Az okosgépjárművek robbanásszerű elterjedése a közeljövőben bekövetkezik. Amellett, hogy a kényelmi szolgáltatások egy élvezhetőbb, biztonságosabb és környezetbarátabb jövőt hoznak az emberiségnek, számos olyan elméleti lehetőség rejlik a technológiában, amely nemzetbiztonsági kockázatot jelent. A megfelelő szabályozás, átláthatóság kierőltetése jelentősen mérsékelni tudja ezen veszélyforrásokat.

FELHASZNÁLT IRODALOM

[1] C. Dr. Krasznay, *Kiberbiztonság a XXI. században*, Budapest: Katonai Nemzetbiztonsági Szolgálat, 2022.

[2] ENISA, „IoT," 2020. [Online]. Elérhető: https://www.enisa.europa.eu/topics/iot-and-smartinfrastructures/iot. [Hozzáférés dátuma: 28 02 2023].

[3] R. Deibert, „The Geopolitics of Cyberspace after Snowden," *Current History*, vol.: 114, szám:768, pp. 9-15., 2015.

[4] E. Snowden, *Rendszerhiba*, Budapest: XXI. Század, 2019.

[5] Wikileaks, „Vault 7: CIA Hacking Tools Revealed," Wikileaks, 2017. [Online]. Elérhető: https://wikileaks.org/ciav7p1/. [Hozzáférés dátuma: 28 02 2023].

[6] M. Antonakakis, T. April, Bailey Michael, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, A. J. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, C. Seaman, N. Sullivan, K. Thomas és Y. Zhou, „Understanding the Mirai Botnet," in *Usenix*, Vancouver, BC, Canada, 2017.

[7] C. B. Krebs, „Krebs On Security Hit With Record DDoS," KrebsOnSecurity, 2017. [Online]. Elérhető: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Hozzáférés dátuma: 28 02 2023].

[8] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim és J. N. Kim, „An In-Depth Analysis of the Mirai Botnet," in *2017 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, IEEE, 2017, pp. 6-12.

[9] O. G. M. Khan, E. El-Saadany, A. Youssef és M. Shaaban, „Impact of electric Vehicles Botnets on the Power Grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*, Montreal, QC, Canada, IEEE, 2019, pp. 1-5.

[10] A. Fodor, D. Fodor, K. Dr. Bíró és L. Dr. Szabó, „A CAN mint ipari kommunikációs protokoll," Kolozsvár: Kolozsvári Műszaki Egyetem, 2007.

[11] M. Afsin, K. W. Schmidt és E. G. Schmidt, „C3: configurable CAN FB Controller: Architecture, design and hardware implementation Industrial Embedded Systems (SIES)," in *2017 12th IEEE International Symposium On*, IEEE, 2017, pp. 1-9.

[12] F. Hartwich és et al., „CAN with flexible data-rate," in *iCC*, 2012, pp. 1-9.

[13] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang és S. Yu, „Attacks and defences on intelligent connected vehicles: a survey," *Digital Communications and Networks*, vol.: 6, szám: 4, pp. 399-421, 2020.

[14] F. Consortium, Flexray Communication System Protocol Specification 3.0.1, 2010.

[15] S. Khurshid, C. Păsăreanu és W. Visser, „MOST 150 development and production launch from an OEM's perspective," in *11th MOST Intercon-Nectivity Conference*, Dél-Korea, 2010, pp. 553-568.

[16] A. Grzemba, „Most Book from Most 25 to Most 150," in *MOST Cooperation FRANZIS*, 2011.

[17] E. Zeeb, „Optical data bus systems in cars: current status and future challenges," in *27th European Conference on Optical Communication (ECOC)*, IEEE, 2001, pp. 70-71.

[18] H. Lothamer, „Automotive gateways: the bridge between communication domains," Texas Instruments, 2017.

[19] J. Taube, F. Hartwich és H. Beikirch, „Comparison of CAN Gateway Modules for Automotive Industrial Control Applications," iCC, 2005.

[20] S. Venkat, „Evolving Automotive Gateways for Next-Generation Vehicles," Texas Instruments, 2020.

[21] A. Perring, R. Canetti, J. D. Tygar és D. Song, „The Tesla Broadcast Authentication Protovol vol. 5," *CryptoBytes*, vol.: 5, szám: 2, pp. 2-13, 2002.

[22] Z. Zorz, „Researchers hack BMW cars, discover 14 vulnerabilities," Helo Net Security, 2018. [Online]. Elérhető: https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.

[23] R. Verdult, F. Garcia és J. Balasch, „Gone in 360 Seconds: Hijacking with Hitag2," Usenix, 2012.

[24] S. Curry, „Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More," Samcurry.net, 2023. [Online]. Elérhető: https://samcurry.net/web-hackers-vs-the-auto-industry/. [Hozzáférés dátuma: 28 02 2023].

[25] S. Loveday, „China Resort Town Bans Tesla's EVs Over Spying Concerns,” InsideEVs, 2022. [Online]. Elérhető: https://insideevs.com/news/593257/tesla-cars-banned-china-spying-concerns/. [Hozzáférés dátuma: 38 02 2023].

[26] Reuters, „Tesla cars barred for 2 months in Beidaihe, site of China leadership meet,” Reuters, 2022. [Online]. Elérhető: https://www.reuters.com/business/autos-transportation/chinas-beidaihe-district-bar-tesla-cars-driving-july-local-police-2022-06-20/. [Hozzáférés dátuma: 28 02 2023].

[27] K. Lyons, „Elon Musk says Tesla would be 'shut down' if its cars were used for spying in China,” The Verge, 2021. [Online]. Elérhető: https://www.theverge.com/2021/3/21/22343018/elon-musk-tesla-shut-down-cars-spying-china. [Hozzáférés dátuma: 28 02 2023].

[28] H. Mukundhan, „Anatomy of an IoT DDoS Attach and Potential Policy Responses,” *ISACA JOURNAL,* vol.: 5, 2017.