HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 121–137.
DOI: 10.32567/hm.2025.1.7

Harangozó Valentin[1]

Kiberbiztonság a városi mobilitásban, fókuszban az e-rollerek, 2. rész

Cybersecurity in Urban Mobility, Focus on E-Scooters, Part 2

Absztrakt

A kutatás célja az volt, hogy alaposan megvizsgálja az elektromobilitási eszközök sebezhetőségeit, azonosítva a lehetséges kockázatokat és veszélyforrásokat, valamint felmérje a gyártók által alkalmazott biztonsági intézkedések hatékonyságait. A szerző bemutatja a közvetlen tapasztalatait egy elektromos roller sebezhetőségeiről az általa elvégzett biztonsági tesztelés alapján. A kutatás eredményei rávilágítanak arra, hogy az elektromobilitási eszközök megfelelő védelme érdekében elengedhetetlen a kiberbiztonsági kockázatok és az elektromobilitási járművek közötti összefüggés vizsgálata, továbbá a kutatás eredményei kulcsfontosságúak a jövőbiztos mobilitás szempontjából.

Kulcsszavak: elektromobilitás, kiberbiztonság, elektromos járművek, adatbiztonság

Abstract

The purpose of the research was to thoroughly examine the vulnerabilities of electromobility devices, identify potential risks and threats, and assess the effectiveness of security measures implemented by manufacturers. The author presents his direct experiences with the vulnerabilities of an electric scooter based on the security testing he conducted. The results of the research highlight that to adequately protect electromobility devices, it is essential

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem, Rendészettudományi Doktori Iskola, e-mail: harangozovalentin1986@gmail.com

to investigate the connection between cybersecurity risks and electromobility vehicles. Furthermore, the findings of the research are crucial for future-proof mobility.

Keywords: electromobility, cybersecurity, electric vehicles, data security

Bevezetés

A téma helye, jelentősége, aktualitása

Ebben a részben az elektromobilitási eszközök sebezhetőségei kerülnek fókuszba. Az elektromos járművek térnyerése a modern közlekedés egyik legfontosabb innovációja, azonban az eszközök kiberbiztonsági fenyegetettségei és sebezhetőségei jelentős kihívásokkal járnak. Az elektromos járművek és a hozzájuk kapcsolódó infrastruktúra sebezhetőségei nemcsak az adatbiztonságot, hanem a fizikai biztonságot is veszélyeztethetik. A hardveres és szoftveres biztonsági rések kihasználása lehetőséget ad a kiberbűnözők számára, hogy távoli hozzáféréssel manipulálják az eszközöket vagy azok rendszereit. Ez különösen aggasztó, mivel az ilyen sebezhetőségek kihasználása kiberbiztonsági és közlekedésbiztonsági incidensekhez is vezethet.

A kiberbiztonság jelentősége a járműgyártás, fejlesztés és szabályozás területén egyre inkább előtérbe kerül. Az elektromos járművek és a kapcsolódó rendszerek védelme érdekében elengedhetetlen a folyamatos fejlesztés. A kutatás célja az volt, hogy hozzájáruljon egy olyan szabályozási keret kialakításához, amely biztosítja az elektromobilitási járművek biztonságos használatát. Az elektromobilitási eszközök digitalizációja és a hozzájuk kapcsolódó hálózati funkciók új kiberbiztonsági fenyegetéseket hoznak létre, amelyekre eddig kevés figyelem irányult. Éppen ezek az új kihívások és a belőlük fakadó kiberbiztonsági problémák ösztönöztek arra, hogy kutatásomat erre a témára összpontosítsam.

A tudományos probléma megfogalmazása

Az elektromobilitás terjedése az utóbbi években jelentős mértékben átalakította a közlekedési szokásokat, új lehetőségeket és kihívásokat teremtve. Az elektromobilitási eszközök, mint például az e-rollerek, elektromos kerékpárok és elektromos autók, innovatív és környezetbarát alternatívákat kínálnak a hagyományos közlekedési eszközökkel szemben. Ezen eszközök elterjedésével azonban a használatukhoz szükséges digitális infrastruktúra és az ezeken keresztül átvitt vagy tárolt adatok védelme is kiemelt figyelmet igényel.

A modern elektromobilitási rendszerek számos érzékeny adatot kezelnek, például GPS-koordinátákat, személyes profilokat, valamint fizetési információkat, amelyek védelme elengedhetetlen a felhasználók biztonságának és bizalmának megőrzéséhez.

A nem megfelelő adatvédelem súlyos következményekkel járhat, beleértve az adatlopást, az adatokkal való visszaélést, illetve a felhasználók bizalmának elvesztését. Az elektromobilitási eszközök és a kapcsolódó alkalmazások használata során fellépő kiberbiztonsági kockázatok tovább bonyolítják a helyzetet, hiszen a hardveres

és szoftveres sebezhetőségek kihasználása révén a támadók távoli hozzáférést szerezhetnek az eszközökhöz, adatokat lophatnak vagy akár az eszközök működését is befolyásolhatják.

A vizsgálat tárgya és a célkitűzések

Kutatási célkitűzések, fontosabb kérdések

A kutatásom célja az volt, hogy feltárja a mindennapi közlekedésben megjelenő elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat. Kiemelt figyelmet kapnak az adatbiztonságot érintő kérdések, például az eszközön tárolt vagy átvitt személyes információk védelme, a távoli hozzáférés lehetőségei és az esetleges adatlopás veszélyei. Fontos kérdés továbbá az eszközök fizikai biztonsága, a vezérlőrendszer sebezhetőségei és az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben.

A lényegesebb témaköröket vizsgálva két részre volt bontható a kutatás: ebben a részben bemutatom a vizsgált elektromos eszközöknek a kiberbiztonsági fenyegetettségeit, míg az előző részben ismertettem és elemeztem ezen közlekedési eszközök felhasználóinak biztonságtudatossági szintjét és technológiaelfogadási hajlandóságát. A kutatás céljával összhangban annak érdekében, hogy az elektromos járművek sebezhetőségi pontjait feltárhassam és megvizsgálhassam, az alábbi kérdéseket fogalmaztam meg:

- Hol vannak az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben?
- Milyen intézkedéseket és technikai megoldásokat alkalmaznak a gyártók a kiberbiztonsági fenyegetettségek csökkentése érdekében, és ezek mennyire hatékonyak?

Kutatási módszerek

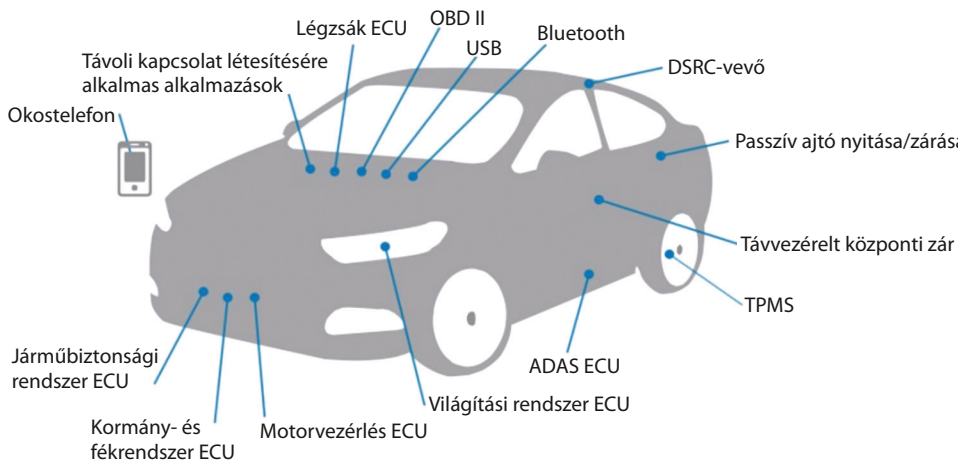
A kutatásom során többféle módszert alkalmaztam az elektromobilitási eszközök kiberbiztonsági kockázatainak feltárására és értékelésére. Elvégeztem egy biztonsági tesztelést egy elektromos rolleren, hogy közvetlen tapasztalatokat szerezhessek az eszköz kiberbiztonsági sebezhetőségeiről. A biztonsági tesztelés olyan elemeket tartalmazott, mint a rendszeres frissítések telepítése során felmerülő kockázatok azonosítása, az eszközön található alkalmazások biztonságának értékelése és a potenciális kockázati tényezők azonosítása.

Az összes adat begyűjtése után részletesen elemeztem és összevetettem az információkat, hogy teljes képet kapjak az elektromobilitási eszközök kiberbiztonsági állapotáról. Ezen elemzés eredményei alapján fogalmaztam meg a kutatás végkövetkeztetéseit és ajánlásait.

Kiberbiztonság a járműiparban

Kiberfenyegetettségek a járművek tekintetében

Fontos megjegyezni, hogy a jövőbeli kiberfenyegetések nemcsak a hétköznapi munkavégzések során lesznek jelen, hanem az elektromos járművek térhódítása miatt a gazdasági szektoron átívelve a mindennapi közlekedésben is meg fognak jelenni. A járműgyártás során egyre több technológiai megoldást vezetnek be mind az utasok, mind a gyalogosok biztonságának javítása érdekében, azonban ezek nem járnak kizárólag pozitív hatásokkal, ugyanis ezekben rejlik a járművek kiberbiztonsági sebezhetősége is (1. ábra).[2]



1. ábra: Lehetséges támadási pontok egy járműben
Forrás: Palkovics 2020: 4

Az egyik ilyen kiberfenyegetettség lehet a jövőben a *vehicle-to-vehicle* kapcsolódás (a továbbiakban: V2V). A korábbi években az autóipari és közlekedési rendszerek fejlesztői óriási erőforrásokat fordítottak arra, hogy kifejlesszék az intelligens közlekedési rendszereket (ITS), valamint a kooperatív intelligens közlekedési rendszereket (C-ITS), továbbá az ezeket a rendszereket összekötő *vehicle-to-everything* (V2X) technológiát.[3] Az elektromos járművek képesek az előttük haladó másik elektromos járművel összekapcsolódni. A járművek közötti kommunikáció természetesen vezeték nélküli hálózat használatával jön létre, ez a funkció hasznos lehet például a haladás során is, mivel lehetővé teszi az autó sebességének csökkentését, ha a másik jármű közelebb kerül. Ilyenkor a kiberfenyegetettség abban rejlik, hogy a támadó visszaélhet a vezeték nélküli hálózat által biztosított kommunikációs technológia hibáival, így könnyedén

[2] Sanguesa et al. 2021: 372–404.
[3] Pethő–Szalay–Török 2022.

átveheti az irányítást, akár csökkentheti is az autó sebességét, és *malware-ekkel* fertőzheti meg ezt a kapcsolatot a járművek között, aminek hatására a V2V-rendszer lehetőséggé válik ahhoz, hogy megfertőzze a többi csatlakoztatott autót is.

A következő kiberfenyegetettség a Controller Area Networkben (a továbbiakban: CAN) rejlik, ugyanis a legtöbb jármű CAN-vezérlőt használ, amely a jármű elektronikus vezérlőegységével (a továbbiakban: ECU) kommunikál. Ahogyan az 1. számú ábrán látható, az ECU számos alrendszert működtet, például az ABS-t, azaz a blokkolásgátló fékeket, légzsákokat, sebességváltót, média- és audiorendszert. Az ECU vezérli továbbá például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zárakat, a légkondicionáló rendszer működését és a fényvezérlés moduljait, illetve több egyéb alkatrész, modul vezérléséért is felelős.[4]

A járműben lévő hálózat összeköti az ECU-kat, és továbbítja az adatokat közöttük. Ez a hálózat magában foglalja többek között a vezérlőterületi hálózatot, a helyi összekötő hálózatot (Local Interconnect Network, a továbbiakban: LIN), az Ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárakhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak.[5] Az ECU könnyedén elérhető egy külső OBD-eszközzel is, amely egy *backdoor* támadásként képes a jármű ECU-jába bejutva parancsokat adni, és vezérelni a különböző rendszereket és szolgáltatásokat. Fontos megemlíteni, hogy a titkosítás hiánya is kiberbiztonsági kockázat, ugyanis a CAN-csomagok nincsenek titkosítva, ezért a támadók könnyen elemezhetik azokat.[6]

Sen Nie és társai egy kísérlet során bemutatták, hogyan irányítható a jármű vezérlőegysége távolról tetszőleges CAN-csomagok küldésével. A kísérlethez egy legújabb *firmware-rel* frissített Tesla járművet használtak, így tesztelték a Tesla S P85 és P75 modellek sebezhetőségét. A teszt során vezeték nélküli technológiával több, a vizsgált járművekben lévő rendszert is meg tudtak károsítani, többek között az integrált áramkört és az átjárókat, ezt kihasználva rosszindulatú CAN-üzeneteket fecskendeztek be a rendszerbe.[7] A felfedezés után a Tesla járműveket már az *over-the-air* (OTA) mechanizmussal frissítették, és kódaláírási védelmet alkalmaztak a sebezhetőség megszüntetésére.[8]

A jelenlegi jármű-technológia lehetővé teszi, hogy az autónkhoz csatlakoztassuk az okostelefonjainkat is, így olyan funkciókat használhatunk a gépkocsinkban, mint a telefonhívás, szöveges üzenet írása vagy zenehallgatás, erre való például az Apple CarPlay vagy az Andorid Auto. Ez azért veszélyes, mert a telefon és a jármű kapcsolata során egy előzetesen összeállított rosszindulatú program (például egy *malware*) azonnal kihasználja a biztonsági réseket a járművekben, ezzel veszélyeztetve a járművezetőt, a járművezető adatait és a közlekedés biztonságát is.

Az okostelefonokkal összekapcsolt járművek kapcsolatából egyéb kiberfenyegetettségek is kialakulhatnak a jövőben, hiszen az összekapcsolt autók képesek rögzíteni a járművezetők fontosabb személyes adatait is a külső eszközökről. Ez az adatbázis „kincsesbánya" lehet egy kiberbűnözőnek akár kémkedés során is.

[4] Tóth 2017.
[5] Katona 2023: 161–176.
[6] Wolf–Weimerskirch–Paar 2004.
[7] Katona 2022.
[8] Kyounggon et al. 2021: 103.

Kiberfenyegetésként említhető a jövőben az elektromos járművek széles elterjedésével az autólopások módszerének megváltozása is. A legtöbb jármű távolról kulccsal nyitható és zárható már most is. Ezt használja ki az a potenciális támadó is, aki képes anélkül ellopni egy autót, hogy ahhoz bármilyen fizikai behatást alkalmazna. Ezt a fajta kibertámadást általában hackerek használják, és nem is kell hozzá sok felszerelés, emellett kifejezetten hatékony. Ebben az esetben a támadó blokkolja a jelet a jármű vezeték nélküli kulcsáról, így nyitva hagyja az autót, mindeközben a jármű válaszol a jelre, amivel megtéveszti a tulajdonosát. A támadás lényege, hogy a kulcs és a jármű kommunikációjához használt elektromágneses hullámokat blokkolja, megakadályozva az autó bezárását. Például egy kutatás során egy VW Grouphoz tartozó jármű távirányító jelét továbbították, majd a járműből küldött jelet lehallgatták, így tetszőlegesen hozzáférhettek a járműhöz.[9]

A fentiek alapján megállapítható, hogy a villamosítás és az automatizált vezetés mellett az elektromos járművek kiberbiztonsága az egyik legfontosabb kihívás a járműipari fejlesztők, a gyártók és az alkatrészgyártók számára. A kiberbiztonsági irányítási rendszerek és szabályozások célja, hogy a jövőben megvédjék a teljes járművet, az infrastruktúrát és a berendezéseket a fenyegetésektől.

Kiberfenyegetettségek az elektromos roller tekintetében

Az elektromos rollerek Magyarországon elég nagy arányban vesznek részt a közúti közlekedésben, és a számuk folyamatosan növekszik. Az elektromos rollereket illetően beszélhetünk saját tulajdonú és közösségi megosztáson alapuló e-rollerekről. A mindennapi közlekedésben Magyarországon 2019-ben az év végén jelent meg a közösségi rollerszolgáltatás. Egy okostelefonokra letölthető applikáció beszerzése után az elektromos rollereket szinte bárki elviheti az utcáról. Mindegyik rollerben található egy globális helymeghatározó rendszer, amely nyomon követi az adott személy használatát. A globális navigációs műholdrendszer egy műholdalapú helymeghatározó, navigációs és időmérő (Position, Navigation and Timing, a továbbiakban: PNT) rendszer. Jelenleg számos Global Navigation Satellite System (a továbbiakban GNSS) van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által használt globális helymeghatározó rendszer a legismertebb. Mindazonáltal az európai vezetésű Galileo, az orosz vezetésű GLONASS, a kínai BeiDou, az India által vezetett IRSS és a japán QZSS mellett áll.[10] Együttes keretrendszerként a GNSS egy világszerte meghatározó és költséghatékony kültéri PNT-technológiává vált. Az egyes GNSS-technológiák alkalmazása elengedhetetlen egy elektromos jármű, például egy e-roller esetében a pontos helymeghatározáshoz. Továbbá a jövőben kialakuló intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges e szenzorok alkalmazása.[11] Azonban ez a helymeghatározó rendszer is rejt magában számos kockázatot, például egy rosszindulatú támadó stratégiailag kiválaszthatja és hamisíthatja

[9] Garcia et al. 2016.
[10] Santra 2019.
[11] Katona 2023.

egy vagy több e-roller helyzetét, átteheti egy eldugott területre vagy olyan területre, ahol minimális az emberi jelenlét, hogy ezzel odacsalja a potenciális áldozatot.[12]

Az elektromos rollerek kiberbiztonsági kockázatai főként a közösségi megosztáson alapuló e-rollereknél jelennek meg, hiszen ezek azok a szolgáltatók, amelyek a felhasználók adatait kezelik, ők felelnek a járművek karbantartásáért és azért is, hogy kiberbiztonsági szempontból sebezhetetlenek legyenek ezek a közlekedési eszközök. Azonban sajnos mégis vannak gyenge pontok, ami aggasztó lehet. Egy fekete kalapos hacker bluetooth-kapcsolaton keresztül a jármű közelében képes az e-rollerek *firmware-jét* letörölni és egy általa módosítottat felölteni arra, így például növelheti az előtte korlátozott sebességet. Erre megoldás lehet, hogy az e-rollerekre kizárólag jóváhagyott firmware-t lehessen telepíteni, valamint hogy a szolgáltatók vagy a gyártók korlátozzák a harmadik féltől származó alkalmazásokat, hogy hozzáférhessenek az e-rollerek *firmware-jéhez*.

Számos szolgáltató kínál mobilalkalmazást az elektromos rollerhez, azonban itt megjelenik egy következő kiberfenyegetettség, az elavult alkalmazásbiztonság. Manapság már a legnépszerűbb elektromos autókhoz is léteznek speciális alkalmazások, amelyekkel a felhasználók rengeteg érdekes és hasznos információhoz juthatnak hozzá a saját autójukkal kapcsolatban. Ez igaz az elektromos rollerekre is, hiszen ezeknek a rollereknek a rendszere főként bluetoothon vagy wifi-kapcsolaton keresztül kommunikál. Azonban minden hálózati kapcsolat megtámadható, és ha nincsen megfelelő védelemmel ellátva, akkor fel is törhető. Ebből következik az elektromos rollerek alkalmazásainak a kiberbiztonsági kockázata is. Ugyanis ezek a felhasználói élményt javító informatikai rendszerek és a hozzájuk kapcsolt okoseszközök, alkalmazások szintén kiberbiztonsági kockázatoknak vannak kitéve, és számos ponton sebezhetők lehetnek. A hackerek olyan szoftvereket hoznak létre, amelyek megkerülhetik az alkalmazások kiberbiztonságát. Ennek eredményeképpen képesek betörni az alkalmazásba és átvenni az irányítást az e-roller felett. A hackerek képesek arra, hogy saját kódot futtassanak az alkalmazásokon, ami azt jelenti, hogy megváltoztathatják vagy teljesen leállíthatják az alkalmazás működését. Az adattitkosítás hiánya szintén kiberfenyegetettség a jövőben. Számos szolgáltató esetében jelenleg az adatok átvitele HTTP használatával történik, ezeket frissíteni kell HTTPS-re. Pontosan azért, hogy a felhasználói adatok, az utazások adatai és a bejelentkezési adatok mind-mind titkosítva legyenek, és ne lehessen hozzáférni ezekhez.

Az elektromos rollerek elterjedésével és fejlődésével együtt járnak a különböző kiberbiztonsági kihívások és kockázatok is. Ahhoz, hogy megértsük és hatékonyan kezeljük ezeket a kockázatokat, fontos áttekinteni és elemző módon megvizsgálni az e-rollerek lehetséges támadási pontjait. Ezért egy táblázatba szedve szemléltetem az e-rollerek legfőbb támadási pontjait, valamint ezek magyarázatát (1. táblázat). Segítségével könnyen azonosíthatjuk az e-rollerek legkritikusabb biztonsági problémáit, és a későbbiekben javaslatok tehetők a megfelelő megelőzési stratégiákra a felhasználók és az eszközök védelme érdekében.

1. táblázat: Az e-rollerek lehetséges támadási pontjai

[12] Vinayaga-Sureshkanth et al. 2020: 31–35.

Támadási pontok	**Magyarázat**
Firmware manipuláció	A hackerek módosíthatják az e-rollerek *firmware-jét,* például növelhetik a sebességet vagy kikapcsolhatják a biztonsági funkciókat, ami veszélyeztetheti az e-rollerek felhasználóit.
Alkalmazásbiztonság megkerülése	Az alkalmazások biztonsági intézkedéseit megkerülve, lehetőség nyílik arra, hogy illetéktelenül hozzáférjenek a felhasználói adatokhoz vagy akár teljesen átvegyék az irányítást az e-rollerek felett.
Adattitkosítás hiánya	Az adatok titkosításának hiánya lehetővé teszi a hackerek számára, hogy illetéktelenül hozzáférjenek az e-rollerek felhasználói adataihoz, például a felhasználók személyes információihoz vagy a közlekedési tevékenységeikhez kapcsolódó adatokhoz. Az adatok átvitele HTTP-n keresztül történik, ami kockázatot jelent. Az adatok titkosítása HTTPS használatával szükséges a biztonságos adatátvitel érdekében.
Bluetooth- és WiFi-kapcsolat	A bluetooth-kapcsolatok kihasználása lehetővé teszi a hackerek számára, hogy távolról kapcsolódjanak az e-rollerekhez, és manipulálják azok működését, vagy akár ellopják azokat. Ha az e-roller alkalmazást használ, és az okostelefon bluetooth- vagy WiFi-kapcsolaton keresztül kommunikál az eszközzel, ezek a csatornák sebezhetővé tehetik a rendszert.
Szoftverfrissítési sebezhetőség	A szoftverfrissítések során felmerülő sebezhetőségek lehetővé tehetik a hackerek számára, hogy kártékony szoftvereket telepítsenek az e-rollerekre, vagy akár illetéktelen hozzáférést szerezzenek azokhoz a frissítési folyamatok során.
Felhasználói hitelesítési problémák	Gyenge felhasználói hitelesítési mechanizmusok vagy hiányos bejelentkezési eljárások lehetőséget adnak a hackereknek arra, hogy illetéktelenül hozzáférjenek az e-rollerekhez.
Adatvédelmi problémák	Az e-rollerekről gyűjtött és tárolt felhasználói adatok védelmének hiánya komoly kockázatot jelent a felhasználók személyes információinak illetéktelen hozzáférése és felhasználása szempontjából, ami súlyos következményekkel járhat az érintettek számára.
Rendszerhiba és sérülékenység	Az e-rollerekben és azok működéséhez szükséges rendszerekben lévő hardver- és szoftverkomponensek sérülékenységei és rendszerhibái lehetővé tehetik a hackerek számára, hogy különféle támadásokat hajtsanak végre az e-rollerek ellen, beleértve a fizikai károkozást és a távoli irányítást.
Felhasználói adatlopás	A hackerek az alkalmazásokon keresztül hozzáférhetnek a felhasználói adatokhoz, például a személyes információkhoz vagy a banki adataikhoz, és ezeket illetéktelenül felhasználhatják vagy értékesíthetik, ami súlyos következményekkel járhat az érintettek számára.
Fizikiai hozzáférés kockázata	A fizikai hozzáférés megszerzése az e-rollerekhez lehetővé teszi a hackerek számára, hogy fizikai károkat okozzanak az eszközökön, például azok megsemmítésével vagy manipulálásával, ami veszélyzeteti az e-rollerek felhasználóinak biztonságát és magánéletét.

Forrás: a szerző szerkesztése Argyropoulos *et al. 2021 és* Vaidya–Mouftah *2020 alapján*

Következtetések

A kiberbiztonsági kockázatok áttekintése során megállapítható, hogy számos potenciális támadási pont létezik az elektromobilitási eszközöknél, amelyek veszélyeztethetik akár az e-rollerek, akár más e-mobilitási eszköz felhasználóinak biztonságát és adataik védelmét.

Fontos hangsúlyozni, hogy ezeket a kockázatokat lehet és kell is kezelni a megfelelő védelmi intézkedésekkel és gyakorlatokkal. Az e-rollerek tervezése és üzemeltetése során kiemelt fontosságú az adatvédelem és a felhasználók bizalmának megőrzése, ezért folyamatos figyelemmel kell kísérni a kiberbiztonsági kockázatokat, és azokra hatékony válaszokat kell kidolgozni a felhasználók védelme érdekében. A biztonságos és kényelmes közlekedés érdekében a gyártók, a szolgáltatók és a felhasználók közös felelőssége, hogy az e-rollerek világa folyamatosan fejlődjön.

Vizsgálat és tesztelés

A vizsgálat módszertana

A vizsgálati módszer ebben a fejezetben egy gyakorlati biztonsági tesztelést foglal magában, amely során valós környezetben teszteltem egy elektromos roller biztonsági mechanizmusait. A vizsgálat során a célom az volt, hogy megállapítsam, hogy egy bluetoothos adatkapcsolati rendszeren keresztül hozzá lehet-e férni az e-rollerek rendszeréhez, és módosíthatók-e egyes gyárilag beállított biztonsági intézkedések. Az elektromos roller rendszerének biztonsági tesztelése lehetővé teszi számomra, hogy a valós életben megvizsgáljam a biztonsági intézkedések hatékonyságát és a rendszer esetleges sebezhetőségeit. Az ilyen tesztek által nyert eredmények segíthetnek bemutatni, hogy az általam megfogalmazott kiberbiztonsági fenyegetettségek valósak, illetve hogy az esetleges hiányosságokat azonosítaniuk kell a szolgáltatóknak és a gyártóknak, továbbá hogy szükséges az elektromobilitási eszközök rendszerének és a hozzájuk társított applikációknak a továbbfejlesztése a felhasználók biztonságának javítása érdekében.

Biztonsági tesztelés a gyakorlatban

Ahogy korábban kifejtettem, a biztonsági tesztelésem célja annak megállapítása volt, hogy vezeték nélküli adatkapcsolati kommunikáción keresztül hozzá lehet-e férni egy elektromos roller rendszeréhez, és módosíthatók-e bizonyos gyárilag beállított biztonsági intézkedések, adatok.

A tesztelés laboratóriumi környezeten kívül, valóságos környezetben történik, ahol valódi elektromos rollert használok. A teszteléshez egy Xiaomi gyártmányú Mi Essential típusú eszközt választottam. Ennek az elektromos rollernek a főbb jellemzői: 20 km-es hatótávval rendelkezik, maximum 20 km/h sebességgel képes haladni. A roller súlya: 12 kg, kerékmérete 8,5 col, és dupla fékrendszerrel (E-ABS és nagy hátsó

tárcsafék) felszerelt. Az akkumulátor típusa lítium-ion, 3 sebességmóddal használható (gyalogos, normál és sport), a töltési ideje körülbelül 3,5 óra. A hozzárendelt gyártói applikáció a Mi Home, amellyel kezelhető a roller rendszere.

Ebben az alkalmazásban látható minden információ a saját rollerünkkel kapcsolatban, többek között a sorozatszám, a szoftver- és hardverinformációk, illetve a megtett kilométer, az akkumulátor töltöttsége. Az applikáció bluetooth-kapcsolaton keresztül kommunikál az elektromos roller vezérlőegységével. Amit még fontos tudni, hogy ebben az alkalmazásban történik – amennyiben rendelkezésre áll újabb – az e-roller szoftverfrissítése, illetve fontos megjegyezni, hogy az adott e-roller-típusoknak mind-mind sajátos funkcióik vannak. Ez a konkrét típus egy belépő szériának minősül a legalapvetőbb funkciókkal, így például nincsen rajta gyárilag elektronikus sebességtartó funkció *(tempomat)*. A gyártói alkalmazás Android-rendszerű eszközökre a Play Áruházból, iOS-rendszerű eszközökre pedig az App Store-ból tölthető le, és az alkalmazáson belül csak az adott e-roller-típusra vonatkozó beállítások szerkeszthetők vele, ezért például korábbi szoftverek nem telepíthetők, pluszbeállítások nem végezhetők el, tehát ez alapján zárt rendszerűnek mondható az alkalmazás.

A tesztelés során mindenképpen Android-rendszerű eszközt fogok használni, ugyanis azok az alkalmazások, amelyekkel megkerülhetők a gyári beállítások, kizárólag a Play Áruházból érhetők el. Ezek úgynevezett *third-party app-ok,* ami azt jelenti, hogy olyan, egy harmadik féltől származó alkalmazások, amelyeket nem az e-roller gyártója készített. Nevezetesen van két ilyen alkalmazás, amelyet szeretnék bemutatni és használni ennek a folyamatnak a végrehajtására, az egyik a ScooterHacking Utility, a másik pedig az m365 DownG.

Minden elektromos rollernek saját vezérlő elektronikája van, és ezzel együtt úgynevezett firmware-je (FW). Röviden ez mondja meg a rollernek, hogyan viselkedjen, milyen teljesítményt adjon le a motor, milyen gyorsan menjen az elektromos roller. Ha ezt az FW-t módosítják, azt nevezzük CFW-nek *(custom firmware)*. A biztonsági tesztelés során használt elektromos rollerre gyári firmware van telepítve. A használt DownG alkalmazás verziószáma 36, a ScooterHacking Utility verziószáma pedig 2.3.2.

Fontos megjegyezni, hogy minden e-rollernek van négy olyan rendszere, amelyet érintenek ezek az alkalmazások az egyes szoftvermódosítások során.

Az e-rollerek esetében ez a négy rendszer a DRV, az ESC, a BSM és a BLE. A DRV az elektromos motor vezérlőjére utal, amely felelős az elektromos motor sebességének és irányának szabályozásáért a rollerben. A motorvezérlő szabályozza a motorhoz szállított energiát a roller vezérléseitől származó bemeneti jelek alapján. Az ESC az elektronikus sebességvezérlő rövidítése. Azzal befolyásolja az elektromos motor sebességét, hogy szabályozza az ahhoz szállított energia mennyiségét. Értelmezi a roller vezérléseitől származó jeleket, és ennek megfelelően szabályozza a motor sebességét. A BSM az akkumulátorkezelő rendszer rövidítése, ami felelős a roller akkumulátorának kezeléséért, ideértve állapotának figyelését, a cellák kiegyenlítését és a túltöltés vagy túlmerülés elleni védelmet. A BMS szinte minden elektronikus eszközben megtalálható, sokféle szerepet játszik az e-rollereken belül. Ez egy beépített rendszer, amely figyeli az akkumulátort és annak egyes akkumulátorcelláit, hogy diagnosztizálja, korrigálja és optimalizálja a járművet. Ezeket az adatokat a BMS folyamatosan gyűjti a zökkenőmentes működés és az optimalizált energiafogyasztás biztosítása érdekében. A BLE

az angol Bluetooth Low Energy rövidítése. Az elektromos roller esetében ez a roller bluetooth-kapcsolatára utal, ami lehetővé teszi annak kommunikációját egy mobilalkalmazással vagy más eszközökkel. A BLE funkciói közé tartozhatnak a roller zárásának/nyitásának vezérlése, beállítások módosítása, a roller helyzetének nyomon követése és a diagnosztikai adatok biztosítása. Ennek a segítségével működik a gyártó által biztosított dedikált alkalmazás is, továbbá ez az a rendszer, amelyre elsődlegesen hatnak a Play Áruházból letölthető, már említett alkalmazások.

Az elektromos rollerek, ahogy korábban volt róla szó, bluetooth-kapcsolaton keresztül kommunikálnak a külső eszközökön lévő applikációkkal. A biztonsági tesztben érintett Xiaomi elektromos roller is a gyártó által fejlesztett Mi Home alkalmazáson keresztül vezérelhető.

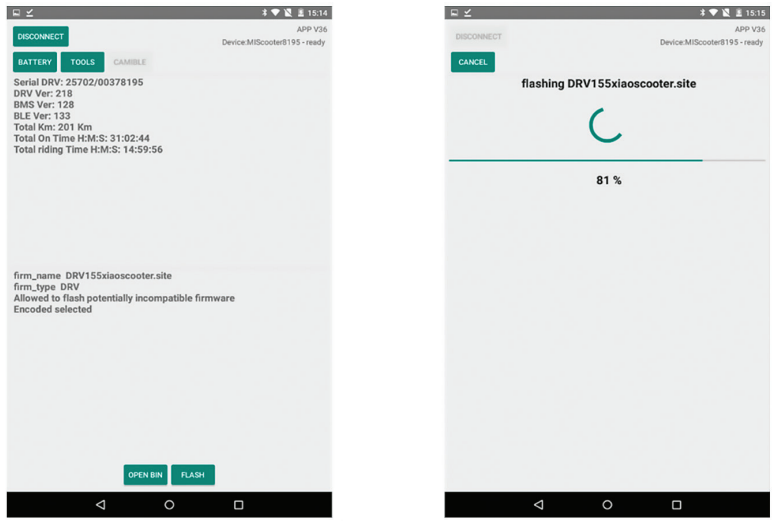
Fontos megjegyezni, hogy ezen a gyári applikáción van egy olyan lehetőség, hogy a saját e-rollerünket, amikor összekapcsoljuk bluetoothon keresztül, elektronikusan le lehet zárni, majd fel lehet oldani a további használat érdekében. Amikor a roller elektronikusan zárolva van, az egyetlen rajta található funkciógombbal kizárólag a lámpát lehet be- és kikapcsolni, minden más funkció ilyenkor le van tiltva, a roller kijelzőjén kizárólag egy lakatszimbólum, és amíg a bluetooth eszközzel kapcsolatban van, egy bluetooth-szimbólum látható. Továbbá fontos, hogy az elektronikus lezárás után a roller további mozgásra képes, azonban az elektromotor folyamatosan fékezi annak első kerekét. Az e-roller nyitásának és zárásának jelentősége lesz a teszt során.

A teszt végrehajtása

Mindenekelőtt szeretném megjegyezni, hogy a téma etikai érzékenysége miatt a jelen fejezetben teljes, részletes kifejtésre nem kerül sor, mivel nem közölnék olyan információkat, amelyek esetlegesen nem kívánt irányú alkalmazásra ösztönözhetnek másokat.

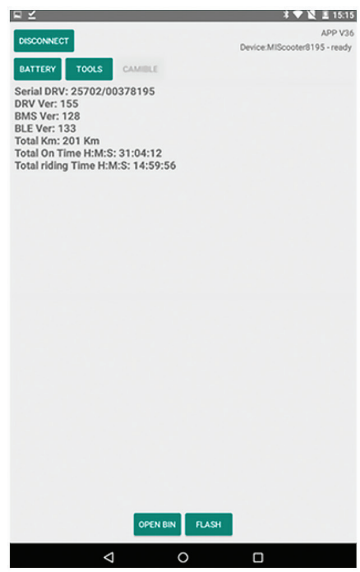
Az első teszt során azt az élethelyzetet szeretném bemutatni, amikor nem használom a Mi Home alkalmazást, és ezáltal nem is zárom le az elektromos rollert elektronikusan. Ebben az esetben a teszt célja a rollerre telepített firmware felülírásra egy olyan *custom firmware-rel,* amelyen a gyári biztonsági intézkedések már felül lettek írva, így például a maximális sebesség beállítása 30 km/h; előtte nem rendelkezett elektronikus sebességtartó funkcióval, ez is be lett állítva a CFW-ben, illetve az elektromotor indítási sebessége is csökkentve lett. Ennek a CFW-nek az e-rollerre történő telepítésére a DownG alkalmazást fogom használni. Itt minden olyan e-roller megjelenik, amely be van kapcsolva, és amelynek a bluetooth-hatótávjában az androidos eszközöm észlelhető.

Miután a módosítani kívánt e-roller megjelenik a listában és kiválasztjuk, egy új felületre kerülünk. Itt már láthatunk minden fontos információt a saját e-rollerünkről: többek között az e-rollerünk szériaszámát és a rajta található DRV, BMS, BLE verziószámokat, illetve az összes megtett utat kilométerben és időben is, azonban ez nem releváns a teszt szempontjából. Ami a teszt szempontjából fontos, az az e-rolleren található DRV verziószám, amely jelen esetben 2.1.8. Ez fog vélhetően módosulni az általam generált CFW verziószámára, ha sikeres lesz a teszt.



2. ábra: A CFW felülírásának folyamata
Forrás: a szerző felvételei a DownG alkalmazásból

Ha a CFW-t betöltjük a programba, elindul a felülírási folyamat, amint az a 2. ábrán is látható. Ez nagyjából 1-2 percet vesz igénybe, és egy százalékos folyamatjelző időközben az aktuális állapotról tájékoztat. A folyamat végén, amennyiben sikeres a felülírás, látható, hogy az általam használt e-roller DRV verziószáma módosult 1.5.5.-re (3. ábra).



3. ábra: A módosult DRV számmal rendelkező e-roller
Forrás: a szerző felvétele a DownG alkalmazásból

A felülírás után megállapítottam, hogy az e-roller az általam generált CFW-vel hibakód nélkül működött tovább, és az eddig tempomattal nem rendelkező e-roller már ilyen funkcióval is bővült, a maximális sebessége módosult 30 km/h-ra, és az elektromotor indító sebessége is módosult a felülírással, amely összesen két percig tartott a DownG alkalmazás használatával.

A ScooterHacking Utility alkalmazás már sokkal több lehetőséget kínál az e-rollerrel kapcsolatos módosítások végrehajtásához. Fontos megjegyezni, hogy ez az alkalmazás már nem kizárólag Xiaomi márkájú e-rollerekkel kompatibilis, hanem más gyártó több típusú e-rollerével is összekapcsolható (például Segway-Ninebot E, F, T, D szériái).

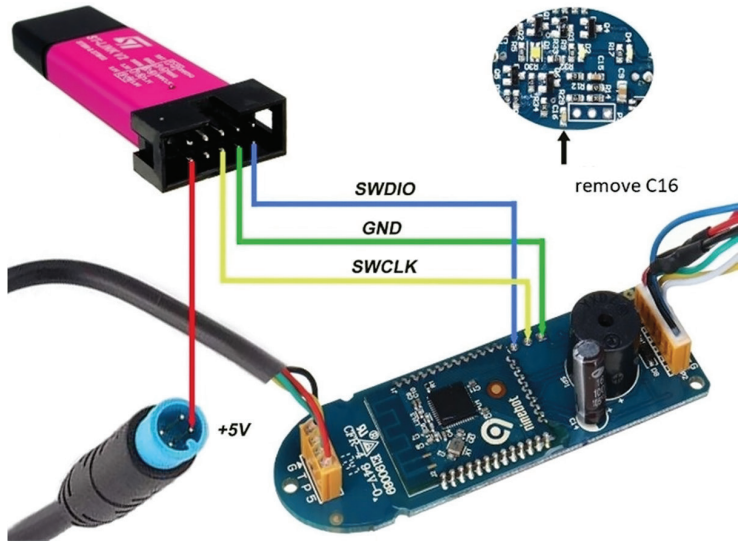
További tesztek végrehajtása

Az első teszt után azt vizsgáltam meg, hogy amennyiben egy e-rollert a korábban ismertetett módon bluetoothszal lezárunk – a valóságban egy gyakran előforduló élethelyzet, hogy valaki elektromosan lezárja az e-rollerét, és amíg nem használja, elmegy annak közvetlen környezetéből –, akkor hogyan reagál egy ilyen alkalmazásra.

Az első esetben úgy hajtottam végre, hogy az az eszköz, amelyről lezártam az e-rollert a Mi Home alkalmazással, ott maradt a roller bluetooth-hatótávolságán belül, és így folyamatos kapcsolat volt az eszköz és az e-roller között. Ebben az esetben az androidos eszközre telepített alkalmazások egyikével sem lehetett észlelni az e-rollert. Tehát az e-roller gyakorlatilag védett maradt, és ez alatt az idő alatt, amíg egy másik bluetooth-kapcsolat aktív volt, nem lehetett rajta végrehajtani változtatásokat.

A második esetben azonban a tesztet úgy hajtottam végre, hogy az az eszköz, amelyről a rollert lezártam a Mi Home alkalmazással, már a bluetooth-hatótávolságon kívül volt, és ebben az esetben az e-roller kijelzőjén kizárólag egy lakatszimbólum jelenik meg. Ekkor az andoridos készülékre telepített alkalmazással azonnal észlelhetővé vált az e-roller, pedig az elektromos zárolás még mindig aktív volt. Azonfelül, hogy az e-roller észlelhető volt, sikerült is bejutni annak vezérlőrendszerébe és a zárolást feloldani az alkalmazással, és lehetőségem nyílt módosításokat végrehajtani az e-rolleren: tudtam csökkenteni az elektromotor fékhatását, az indítási sebességet, a maximális sebességet, az elektromotor-rendszer feszültségét, másik régióba regisztrálhattam az e-rollert stb. Tehát megállapítható, hogy amint nincsen élő bluetooth-kapcsolat az e-roller és egy másik eszköz között, akkor annak rendszerébe könnyedén be lehet jutni, és azon belül változtatások hajthatók végre.

További kutatásokat végeztem különböző internetes forrásokon. Megállapítható, hogy a gyártó ezt a problémát már felismerte, ezért az újabb e-roller-szériákat már egy frissített BLE-verzióval adja ki, és az 1.5.7. verziószámban már blokkolja a vezérlőegység a feloldási lehetőségeket, azonban további kutatásokkal megállapítottam, hogy ennek a védelmi intézkedésnek a megkerülésére két módszer is létezik. Az egyik módszer alapja, hogy már árulnak külön megvásárolható utángyártott e-roller-alaplapokat, amelyeket beleépítve az e-rollerbe lehetőség nyílik annak szoftveres módosítására. A másik módszer lényege pedig az úgynevezett ST-Link V2 használata, amely egy programozó eszköz, USB-modul az STM32 és STM8 processzorcsalád programozásához, és ennek használatával az elektromos roller BLE modulját tudják programozni (4. ábra).



4. ábra: ST-Link V2 összekötése a Xiaomi e-roller vezérlőegységével
Forrás: Instructables 2024

Következtetések

Összegezve: az elvégzett kutatás célja az volt, hogy feltárja az elektromos rollerek bluetooth-kapcsolaton keresztüli hozzáférhetőségének és manipulálhatóságának kiberbiztonsági fenyegetettségeit. A kutatás során a végrehajtott biztonsági vizsgálattal igyekeztem szemléletesen bemutatni, hogy mennyire egyszerű belépni az elektromos rollerek rendszerébe és ott módosításokat végrehajtani.

Az eredmények alapján megállapítható, hogy a könnyű hozzáférhetőség súlyos kockázatokat jelent mind a kiberbiztonság, mind a közlekedésbiztonság, mind pedig az adatvédelem terén. Kiberbiztonsági szempontból az elektromos rollerek rendszereinek sérülékenysége lehetővé teszi a távoli vezérlést és a rendszerben tárolt adatokhoz történő hozzáférést, azok módosítását. Ez pedig potenciálisan komoly veszélyeket rejthet magában a felhasználók és a közlekedés résztvevői számára. Közlekedésbiztonsági aspektusból nézve az e-roller rendszerének manipulálhatósága könnyedén vezethet balesetekhez mind az e-roller vezetője, mind pedig más közlekedők szempontjából. Ezáltal az ilyen típusú járművek veszélyessé válhatnak a közutakon és a gyalogos területeken egyaránt.

Végül úgy gondolom, hogy adatvédelmi szempontból is kiemelt figyelmet kell fordítani az elektromos rollerek rendszerére. Az elektromos rollerek vezérlőegységének manipulálása lehetővé teszi a rendszerfájlokhoz, a rendszerben tárolt adatokhoz való egyszerű hozzáférést. Így például lehetőség nyílik személyes adatok, geolokációs adatok, útvonalak vagy akár az eszköz használatára vonatkozó információk megismerésére, illetéktelen felhasználására.

Kutatási eredmények

Az elektromobilitási eszközök, különösen az e-rollerek kiberbiztonsági fenyegetettségei egyre nagyobb figyelmet kapnak, ahogy ezek az eszközök mind szélesebb körben elterjednek. A kutatás során feltett kérdésekre adott alábbi válaszok egyben a kutatás legfontosabb eredményeit is tükrözik.

A kutatás első kérdésének vizsgálata során megállapítottam, hogy ezek az eszközök és a hozzájuk kapcsolódó szoftverek sebezhetőségei több helyen is megjelenhetnek. Az elsődleges támadási pontok közé tartozik a firmware manipuláció, amely során a hackerek módosíthatják az eszköz szoftverét, például növelhetik az e-roller maximális sebességét, vagy kikapcsolhatják a biztonsági funkciókat. Ez nemcsak az eszköz fizikai biztonságát veszélyezteti, hanem a felhasználók épségét is, hiszen a módosításokkal az e-roller balesetveszélyessé válhat.

A másik jelentős kockázat az alkalmazásbiztonsági rések kihasználása. Az e-rollerek és más elektromobilitási eszközök irányításához használt mobilalkalmazások biztonsági intézkedéseinek megkerülése révén a támadók hozzáférhetnek a felhasználók adataihoz, vagy akár teljesen átvehetik az irányítást az eszköz felett. Ez különösen veszélyes lehet közösségi megosztású eszközök, például e-rollerek esetében, ahol a támadók hozzáférhetnek a rendszerhez, és jelentős károkat okozhatnak. Emellett az adatok titkosításának hiánya is további kockázatot jelent. Sok esetben az eszközök kommunikációja még mindig HTTP-protokollon keresztül történik, amely nem nyújt megfelelő védelmet a támadások ellen. A titkosítatlan adatátvitel során a támadók könnyen megszerezhetik a felhasználók személyes adatait, például GPS-koordinátákat vagy fizetési információkat.

További potenciális támadási pontot jelent a bluetooth- és wifi-kapcsolatok sebezhetősége. Az e-rollerek gyakran kommunikálnak okostelefonokkal, ezeket a kapcsolatokat kihasználva a támadók távolról átvehetik az irányítást az eszközök felett, módosíthatják a működésüket, vagy akár el is lophatják azokat. A szoftverfrissítések sebezhetőségei szintén kihasználhatók. Ha a frissítések során nem megfelelően van biztosítva a folyamat, a támadók rosszindulatú szoftvereket telepíthetnek, amelyekkel hozzáférhetnek az eszköz rendszeréhez.

A második kutatási kérdésre vonatkozóan megállapítottam, hogy a gyártók különböző technikai megoldásokat alkalmaznak a kiberbiztonsági fenyegetettségek csökkentése érdekében. Az egyik legfontosabb intézkedés a firmware védelme. A gyártók sok esetben csak jóváhagyott firmware-t engednek telepíteni az eszközökre, ezzel igyekeznek megakadályozni a külső, nem hivatalos szoftverek telepítését. Noha ez egy hatékony megoldás, a hackerek idővel képesek kijátszani ezeket a védelmi mechanizmusokat, például utángyártott alkatrészek telepítésével vagy speciális programozó eszközök, mint például az ST-Link V2 használatával.

Emellett a gyártók egyre inkább alkalmazzák az adattitkosítást az adatok védelme érdekében. A HTTPS-protokoll használata biztosítja, hogy az adatátvitel során az adatok titkosítva legyenek, ezáltal megnehezítve a támadók dolgát. Azonban még mindig sok eszköz nem használja ezt a megoldást, ami jelentős kockázatot jelent az adatvédelem szempontjából. A rendszeres szoftverfrissítések és a szigorúbb ellenőrzési mechanizmusok szintén hozzájárulnak a kiberbiztonság javításához.

Összességében elmondható, hogy noha a gyártók által alkalmazott védelmi intézkedések hatékonynak bizonyulnak a kiberbiztonsági fenyegetések mérséklésében, a támadók folyamatosan fejlesztik módszereiket, így a védelemnek is állandó fejlesztést és figyelmet kell kapnia.

Összegzett következtetések és ajánlások

Az eredmények alapján számos ajánlás adható mind a felhasználók, mind a gyártók, mind a fejlesztők számára. Úgy gondolom, hogy a felhasználók részére szükséges lenne további oktatási és tájékoztató kampányokat szervezni az eszközök szoftver- és hardver-illesztőprogramjainak fontosságáról és a rendszeres frissítések szükségességéről.

Azonban ezen eredmények alapján hangsúlyozni kell a gyártók, a fejlesztők és a szabályozók felelősségét is a rendszerek biztonságának növelése és a kockázatok minimalizálása érdekében. A rendszeres biztonsági frissítések és a szigorúbb ellenőrzési mechanizmusok bevezetése elengedhetetlen az elektromobilitási eszközök biztonságának szavatolásához. Lehetséges megoldási javaslatként merül fel, hogy a gyártók tegyék lehetővé a felhasználók számára a kétlépcsős azonosítás alkalmazását az e-rollerekhez történő hozzáférés során. Ez azt jelentené, hogy a felhasználóknak nemcsak a jelszavukkal kellene bejelentkezniük az alkalmazásba vagy az e-rollerek vezérlőfelületére, hanem egy második, például SMS-ben küldött vagy autentikációs alkalmazáson keresztül generált kód megadásával is meg kellene erősíteniük az azonosításukat. Ezáltal még nehezebbé válna az illetéktelen hozzáférés, még akkor is, ha az egyik azonosítási tényezőt valakinek sikerülne megszerezni.

Összességében a kiberbiztonsági kockázatok és az elektromobilitási járművek közötti összefüggés vizsgálata kiemelten fontos lépés volt a jövőbiztos mobilitás felé vezető úton. A kutatás során az általam megfogalmazott javaslatok és a jövőben egy megfelelő szabályozási keret kialakítása, továbbá a kiberbiztonsági szakemberek bevonása a gyártók, a fejlesztők, illetve a szolgáltatók körébe nagymértékben segíthet abban, hogy az elektromobilitási járművek és azok felhasználói biztonságosabb környezetben vehessék igénybe ezeket az innovatív közlekedési eszközöket, ezzel hozzájárulva egy fenntartható, biztonságos és technológiailag fejlett közlekedési jövőhöz.

Felhasznált irodalom

Argyropoulos, Nikolaos et al. (2021): Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL. *Transportation Research Procedia,* 52, 307–314. Online: https://doi.org/10.1016/j.trpro.2021.01.036

Garcia, Flavio D. et al. (2016): Lock It and Still Lose It – on the (In)Security of Automotive Remote Keyless Entry Systems. In Holz, Thorsten – Savage, Stefan (szerk.): *SEC'16: Proceedings of the 25th USENIX Conference on Security Symposium.* Berkeley: USENIX Association, 929–944. Online: www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

Instructables (2024): Firmware Downgrade M365. Online: www.instructables.com/Firmware-Downgrade-M365/

Katona Gergő (2022): Autonóm járművek kiberbiztonsági kihívásai (2. rész). *Ludovika.hu,* 2022. január 20. Online: www.ludovika.hu/blogok/cyberblog/2022/01/20/autonom-jarmuvek-kiberbiztonsagi-kihivasai-2-resz/

Katona Gergő (2023): Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész. *Hadmérnök,* 18(3), 161–176. Online: https://doi.org/10.32567/hm.2023.3.11

Kim, Kyounggon et al. (2021): Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Computers & Security,* 103, 102150. Online: https://doi.org/10.1016/j.cose.2020.102150

Palkovics László (2020): Kiberbiztonság a járműiparban. *Scientia et Securitas,* 1(1), 2–6. Online: https://doi.org/10.1556/112.2020.00001

Pethő Zsombor – Szalay Zsolt – Török Árpád (2022): Safety Risk Focused Analysis of V2V Communication Especially Considering Cyberattack Sensitive Network Performance and Vehicle Dynamics Factors. *Vehicular Communications,* 37, 100514. Online: https://doi.org/10.1016/j.vehcom.2022.100514

Sanguesa, Julio A. et al. (2021): A Review on Electric Vehicles: Technologies and Challenges. *Smart Cities,* 4(1), 372–404. Online: https://doi.org/10.3390/smartcities4010022

Santra, Atanu (2019): Augmentation of GNSS Utility by IRNSS/NavIC Constellation Over the Indian Region. *Advances in Space Research,* 63(9), 2995–3008. Online: https://doi.org/10.1016/j.asr.2018.04.020

Tóth, András (2017): Information Security for Electric Cars in Accordance with Nist Critical Infrastructure Cybersecurity Framework. *Hadmérnök,* 12(4), 195–206. Online: http://hadmernok.hu/174_19_toth.pdf

Vaidya, Binod – Mouftah, Hussein T. (2020): Cyber Security Considerations for Automated Electro-Mobility Services in Smart Cities. In Mouftah, Hussein T. – Erol-Kantarci, Melike – Sorour, Sameh (szerk.): *Connected and Autonomous Vehicles in Smart Cities.* Boca Raton: CRC Press, 457–473 Online: https://doi.org/10.1201/9780429329401-17

Vinayaga-Sureshkanth, Nisha et al. (2020): Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems. In *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security.* New York: Association for Computing Machinery, 31–35. Online: https://doi.org/10.1145/3375706.3380559

Wolf, Marko – Weimerskirch, André – Paar, Christof (2004): *Security in Automotive Bus Systems.* Workshop on Embedded IT-Security in Cars (escar), 1–13. Online: www.weimerskirch.org/files/WolfEtAl_SecureBus.pdf