



NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA

AZ ELEKTROMOBILITÁSI ESZKÖZÖK KIBERBIZTONSÁGI KOCKÁZATAI, KÜLÖNÖS TEKINTETTEL AZ E-ROLLEREKRE

Információvédelem menedzselése CXIV. Szakmai fórum

2025. január 15.

Harangozó Valentin

Kiberbiztonsági szakértő

SVMRFK,

NKE-RDI Doktorandusz

Tartalom



Témaválasztás indoklása



1 Növekvő népszerűség

Az elektromos járművek, köztük az e-rollerek, egyre népszerűbbé válnak a fenntarthatóság és mobilitás iránti igény növekedése miatt.

1

2

2 Fejlett technológia

Az e-mobilitási eszközök fejlett szoftveres és hálózati funkciókat tartalmaznak, ami kényelmet és élményt nyújt, de sebezhetőséget is jelent.

3 Új kihívások

A kiberbiztonság kulcskérdéssé vált az e-mobilitás térnyerésével, hiszen az adatok és funkciók védelme kritikus fontosságú.

3

Kutatási célkitűzések, hipotézisek

- 1 Az elektromobilitási eszközök számos sebezhetőségi ponttal rendelkeznek.
- 2 Az emberek részéről tapasztalható aggodalom az elektromobilitási eszközök kiberbiztonsági kockázatai miatt.
- 3 Az elektromobilitási eszközökkel rendelkezők optimistábbak és pozitívabbak az elektromos mobilitási technológiákat illetően, mint azok, akik nem rendelkeznek ilyen eszközökkel.
- 4 Az elektromobilitási eszközökkel kapcsolatos kiberbiztonsági tudatosságot befolyásolja a nem és az iskolai végzettség.
- 5 A kiberbiztonság jelentőséggel bír a jármű gyártás, fejlesztés és szabályozás területén.

Kutatás módszertana



Kérdőíves kutatás

Megvizsgáltam, hogy az emberek hogyan viszonyulnak az e-mobilitási eszközök kiberbiztonságához a TAP modell alkalmazásával.

— Optimizmus – 4 állítás

— Jártasság – 4 állítás

— Függőség – 3 állítás

— Sebezhetőség – 3 állítás

**1: Egyáltalán
nem értek egyet**

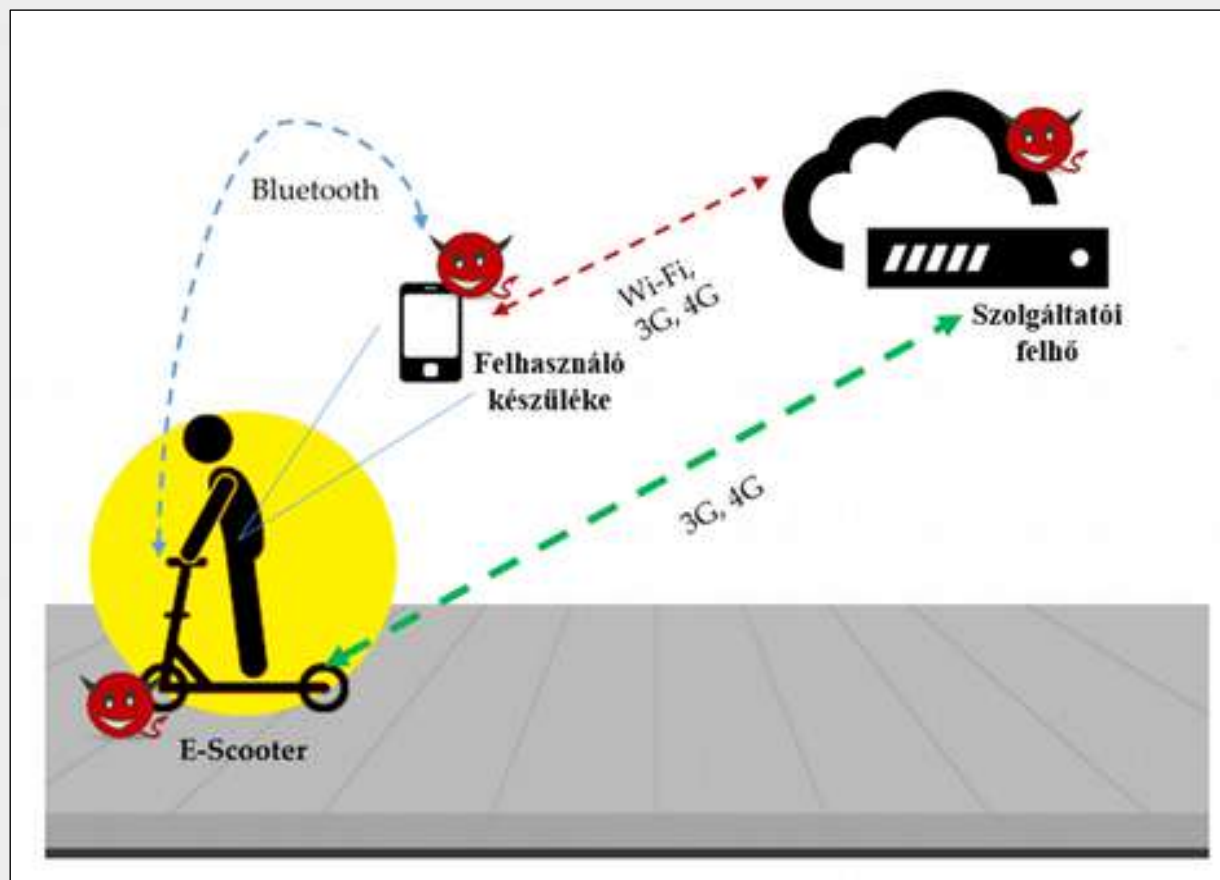
**5: Teljes mértékben
egyetértek**

Biztonsági tesztelés

Megvizsgáltam egy e-roller szoftveres sebezhetőségeit Bluetooth kapcsolaton keresztül a lehetséges módosításokat illetően.



Közösségi e-rollerek veszélyei



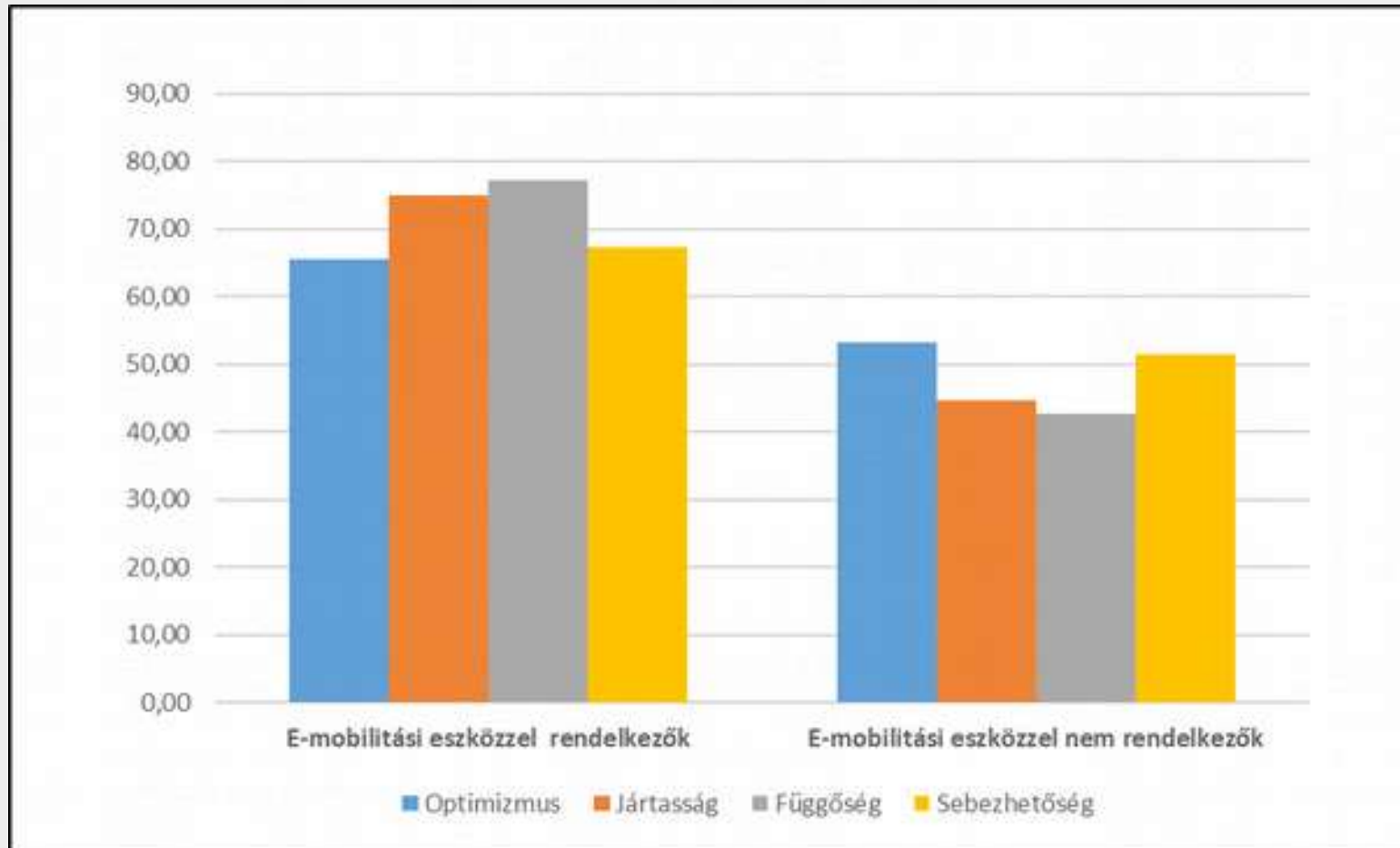
- **Offline (BLE) és Online(felhő) – kommunikáció**
- **GPS támadások – követik a felhasználót**
 - felhasználói szokások megfigyelhetőek
 - spoofing, eltérítés
- **MITM és Replay, DoS támadások**
 - e-roller jogosulatlan lezárása és feloldása, az akku. lemerítése a járműveken (lopás, módosítás, nyomkövetés)
 - a szolgáltatás minőségét rontó támadások

Megoldás lehet:

- más források a helymeghat., GNSS modul figyelje a jelhamisítást
- a valós idejű forgalom szisztematikus megfigyelése és szűrése

Kérdőíves kutatás eredményei

Összefüggések



- **A nem összefüggése a tudatossággal**
 - szignifikáns, férfiak
- **A végzettség összefüggése a tudatossággal**
 - nincsen kapcsolat
- **A TAP-modell faktorainak összefüggései az elektromobilitási eszközök birtoklásával**
 - KW teszt, szignifikáns
 - az elektromobilitási eszközökkel rendelkezők optimistábbak

Biztonsági teszt végrehajtása

DRV



elektromos
motorvezérlő

ESC



elektronikus
sebességszabályzó rendszer

BSM

BLE



akkumulátorkezelő
kommunikációs modul



Bluetooth

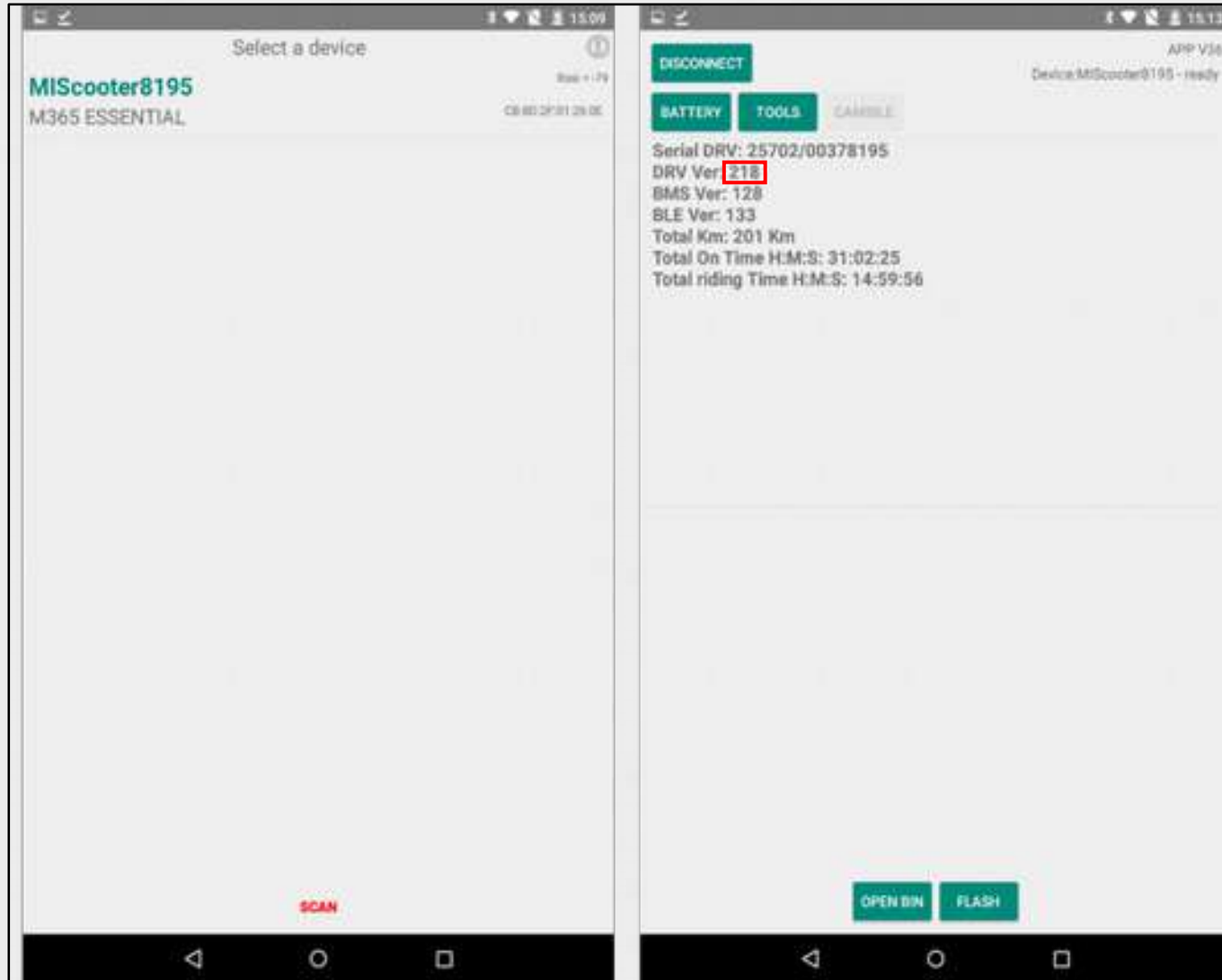
kommunikációs modul

Biztonsági teszt végrehajtása



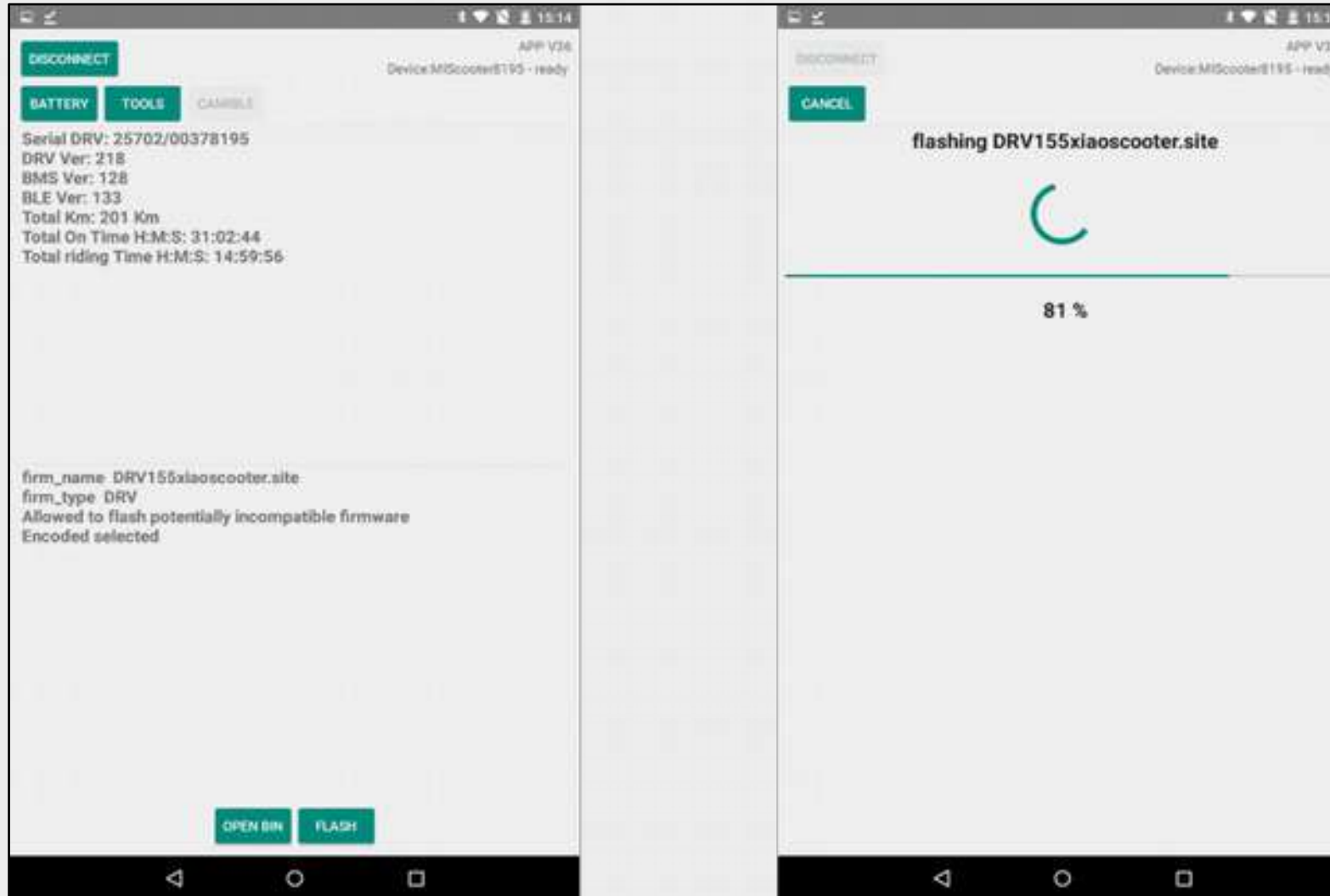
- Saját Xiaomi e-roller
- Gyári FW – CFW
- Különböző módokban (E,D,S) a sebesség limit felülírása
- Motorfék erejének a csökkentése / féklámpa
- BMS kommunikáció kikapcsolása
- Tempomat beállítás

Biztonsági teszt végrehajtása



- Saját Xiaomi e-roller
- DownG app
- Gyári FW – CFW
- BLE hatótávon belül
- BLE hatótávon kívül
- DRV: 2.1.8.

Biztonsági teszt végrehajtása



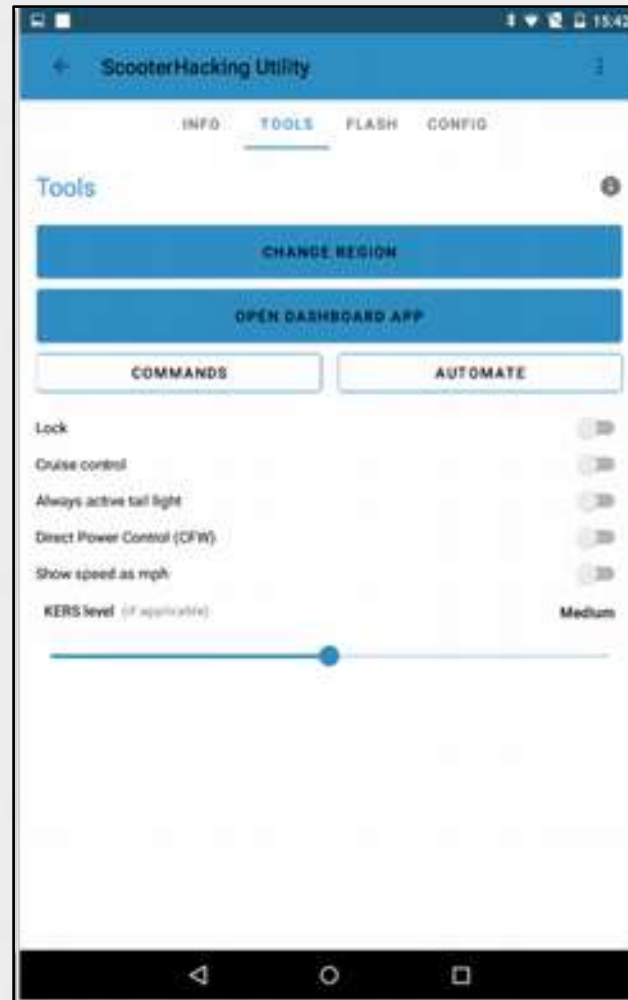
- CFW betöltése
- Flashing folyamat

Biztonsági teszt végrehajtása



- Módosított DRV
- 1.5.5 verzió

Biztonsági teszt végrehajtása

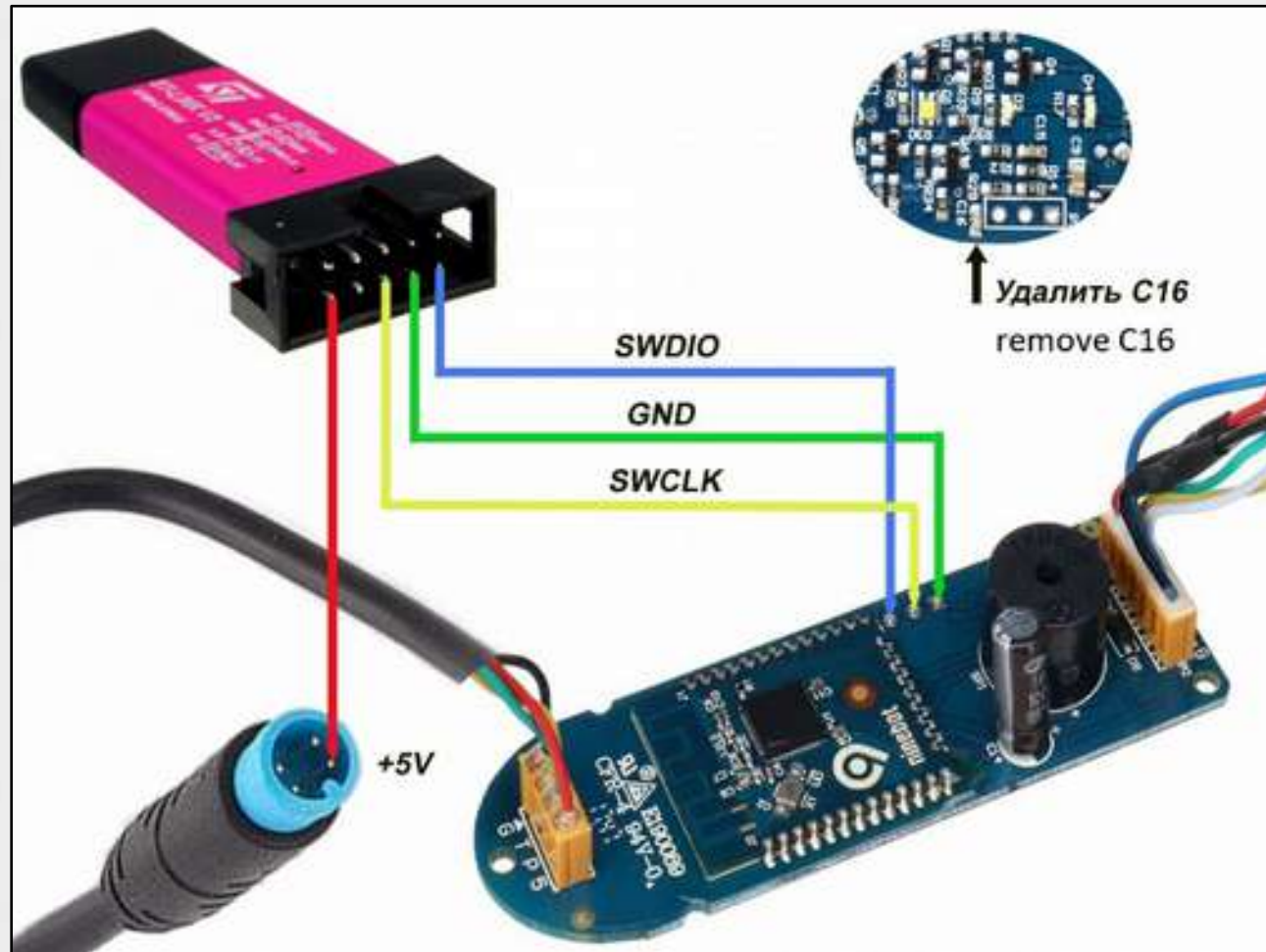


- Third-party appok
- ScooterHacking Utility
- Régió megváltoztatása USA-EU

Újabb teszt:

- MiHome alkalmazással lezárás
- BLE hatótávon belül nem észlelte egyik app sem
- Amíg aktív BLE kapcsolat addig védett
- Bluetooth hatótávon kívül azonban sérülékeny - feloldható

Biztonsági teszt végrehajtása



- Új verzióknál már nem működik
- **Utángyártott alaplapot helyeznek bele**
- **ST-Link V2** programozó eszköz
- BLE modulját lehet programozni

Kutatási eredmények

- 1 Az elemzéssel **igazoltam**, hogy az elektromobilitási eszközök rendszerében **számos sebezhetőségi pont van.**
- 2
- 3 **Igazoltam**, hogy **az emberekben valóban aggodalom van jelen** az elektromobilitási eszközök kiberbiztonsági kockázataival kapcsolatban.
- 4
- 5 **Megállapítottam**, hogy az elektromobilitási eszközökkel rendelkezők körében valóban **optimistább és pozitívabb attitűd tapasztalható** az elektromos

Következtetések



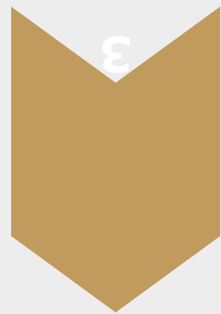
Valós kockázatok

A kockázatok kezelése kiemelkedő fontosságúak a felhasználók és az egész közlekedési infrastruktúra biztonságának szempontjából.



Felelősség

Sebezhetőségek kezelése komoly figyelmet igényelnek mind a felhasználók, mind a gyártók, mind pedig a szabályozó hatóságok részéről.



Felhasználói bizalom

A fenyegetettség csökkentheti a felhasználók bizalmát az elektromos járművek iránt. Ez negatívan befolyásolhatja a döntésüket az ilyen eszközök használatáról vagy vásárlásáról.

Az e-mobilitás terjedése szempontjából ez akadályt jelent, ugyanis lelassulhat az okos városok és az autonóm közlekedés fejlődése is.



NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA



Köszönjük a figyelmüket!

Harangozó Valentin
E-mail: harangozova@somogy.police.hu