Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging

Sebastian Köhler††, Richard Baker††, Martin Strohmeier*, Ivan Martinovic†

†University of Oxford, ‡armasuisse Science + Technology

† Both authors contributed equally to this paper.
https://www.ingenieur.de/technik/fachbereiche/mobilitaet/neue-initiative-fuer-den-aufbau-einer-ladeinfrastruktur-fuer-e-lkw/
https://www.cleanelectric.de/mehr-baguettes-als-ladesaeulen/
HomePlug Green PHY

https://cdn.motor1.com/images/mgl/g3Wjm/s2/efacec-s-first-350-kw-ccs-combo-dc-fast-chargers-already-up-and-running.jpg
Combined Charging System (CCS)

CCS Combo 1 (US)

CCS Combo 2 (EU)
CCS Power-Line Communication
Previous Work on EV Security

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
Previous Work on EV Security

“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, \textit{unintentional wireless channel}.” \cite{Baker2019}

\cite{Baker2019} Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
Previous Work on EV Security

“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, *unintentional wireless channel.*” [1]
Threat Model: Goals
Threat Model: Goals
Threat Model: Goals

Individual Vehicle

Fleet Denial
Threat Model: Goals

- **Individual Vehicle**
- **Fleet Denial**
- **Unspecific Disruption**
Threat Model: Capabilities
Threat Model: Capabilities

Access to off-the-shelf equipment
Threat Model: Capabilities

Access to off-the-shelf equipment

Little to no DSP knowledge
Brokenwire Attack: Wireless Exploitation of CSMA/CA

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.
Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to detect the presence of Preamble Symbols [...]: When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a total SNR of 2 dB at the receiver terminal.” [2]

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.
Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to detect the presence of Preamble Symbols [...] when the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a total SNR of 2 dB at the receiver terminal.” [2]

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.
Brokenwire Attack: Wireless Exploitation of CSMA/CA

“The receiver shall be able to detect the presence of Preamble Symbols [...] When the desired Preamble Symbol waveform present at the receiver has a signal power of -35 dBm and is corrupted by Gaussian noise producing a total SNR of 2 dB at the receiver terminal.“ [2]

+ 

“[The] use of PLC in EV charging and the design of the CCS standard lead to a uniquely high-quality, unintentional wireless channel.“ [1]

[1] Baker R. and Martinovic I. Losing the Car Keys: Wireless PHY-Layer Insecurity in EV Charging. In 28th USENIX Security Symposium, Santa Clara, CA, 2019.
[2] HomePlug Powerline Alliance. Homeplug Green PHY Specification. 2013.
Brokenwire Attack: A closer look

- HP1.0 FC
- Preamble
- AV FC + Payload
- Noise
Brokenwire Attack: A closer look
Lab Testing: Experimental Setup

Charging Cable

HPGP PLC Modem

Raspberry Pi (EVCC)

HPGP PLC Modem

Raspberry Pi (SECC)

Antenna Balun

Amplifier (Mini-Circuits ZX80-100VH+)
Lab Testing: Experimental Setup

- HPGP PLC Modem
- Raspberry Pi (EVCC)
- Raspberry Pi (SECC)
- Electric Vehicle
- Charging Cable
- Antenna Balun
- Amplifier (Mini-Circuits ZX60-100VH+)
Lab Testing: Experimental Setup

- HPGP PLC Modem
- Raspberry Pi (EVCC)
- Raspberry Pi (SECC)
- Charging Cable
- Electric Vehicle
- Charging Station
- Antenna Balun
- Amplifier (Mini-Circuits ZX60-100VH+)
Lab Testing: Power vs. Distance
Lab Testing: Power vs. Distance

![Graph 1: Output Power $P_{\text{out}}$ (dBm) vs. Distance $d$ (m)]

![Graph 2: Output Power $P_{\text{out}}$ (mW) vs. Distance $d$ (m)]
Real-World Testing: Equipment

- LimeSDR
- Amplifier
- Bench Power Supply
- UPS
- Antenna
Real-World Testing

Scenario 1  Scenario 2  Scenario 3  Scenario 4  Scenario 5
## Real-World Testing: Vehicle Overview

| Vehicle | Class             | Price ($) | Charging Capacity |
|---------|-------------------|-----------|-------------------|
| A       | Subcompact        | 50,000    | 50 kW             |
| B       | Compact SUV       | 85,000    | 150 kW            |
| C       | Shooting Brake    | 150,000   | 270 kW            |
| D       | Subcompact        | 20,000    | 50 kW             |
| E       | Mid-size Sedan    | 50,000    | 120 kW            |
| F       | Mid-size SUV      | 70,000    | 150 kW            |
| G       | Compact           | 45,000    | 125 kW            |
| H       | Compact           | 32,000    | 50 kW             |
Real-World Testing: Distance

47.39m
Countermeasures
Countermeasures

Shielding
Countermeasures

Shielding

Firmware Upgrade
Countermeasures

- Shielding
- Firmware Upgrade
- Re-authentication
Conclusion
Conclusion

CCS is vulnerable to wireless attacks
Conclusion

CCS is vulnerable to wireless attacks

Large number of vehicles is affected

~12M
Conclusion

CCS is vulnerable to wireless attacks

Large number of vehicles is affected

PLC is not suitable for the charging loop

~12M
Questions?

✉️ info@brokenwire.fail  or  sebastian.kohler@cs.ox.ac.uk
🌐 https://brokenwire.fail
🐱 https://github.com/ssloxford/brokenwire
 CVE https://nvd.nist.gov/vuln/detail/CVE-2022-0878