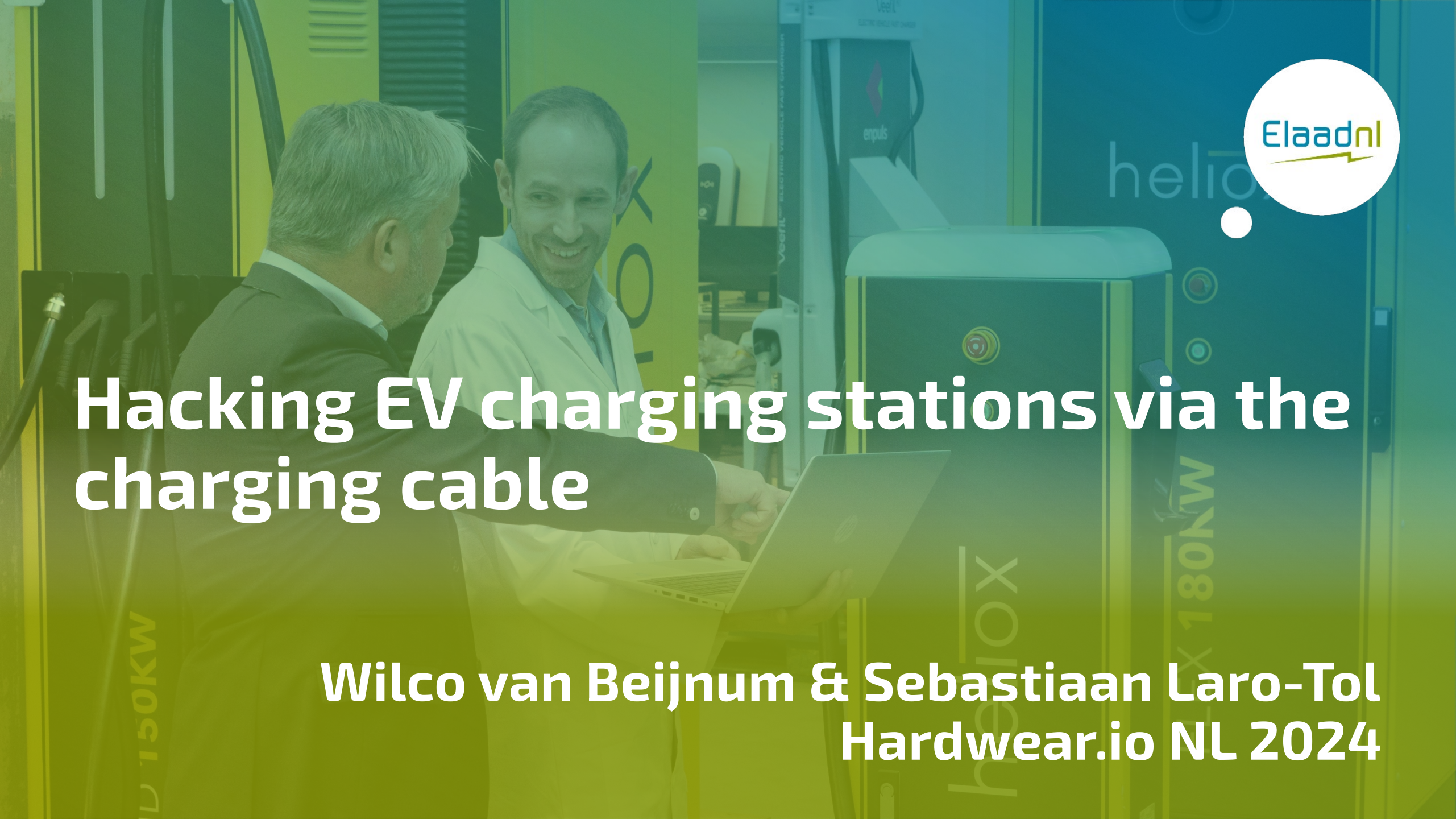


Hacking EV charging stations via the charging cable

Wilco van Beijnum & Sebastiaan Laro-Tol

Hardwear.io NL 2024

Us and ElaadNL

Wilco van Beijnum

- Researching cyber security of charging infrastructure at ElaadNL via Scyon

Sebastiaan Laro-Tol

- Test automation engineer at ElaadNL via Capgemini Engineering
- Testing Power Quality and Immunity of EV Infrastructure, with a background in red teaming

ElaadNL

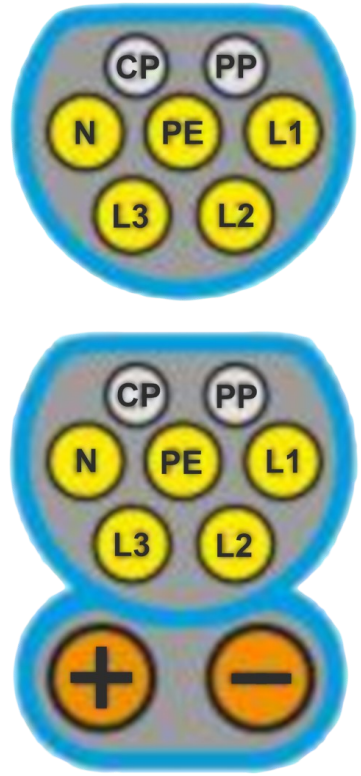
- Knowledge and innovation center for smart and sustainable charging of EVs

Approach

1. Charging cable communication specification
2. Research hardware and software setup
3. Demo
4. Results and impact
5. What's next?

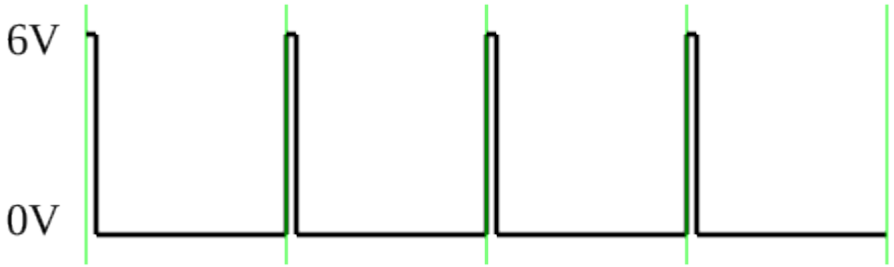
Communication – IEC 61851

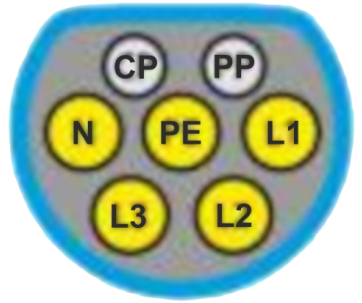
- IEC 61851 (Mode 3/4) – PWM over CP pin
- Voltage controlled by EV: state
- PWM duty cycle controlled by EVSE (charging station): max. current

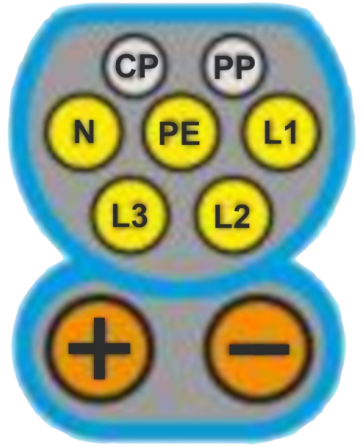


Communication – IEC 61851

- IEC 61851 (Mode 3/4) – PWM over CP pin
- Voltage controlled by EV: state
- PWM duty cycle controlled by EVSE (charging station): max. current
- 5% PWM







Communication - SLAC

- Signal Level Attenuation Characterisation (SLAC) initiates High Level Communication (HLC)
- Uses Power Line Communication (PLC)
- Signal strength measurement
- Used by DC CS (fast charger), and AC CS with HLC (PnC or V2G) support

Protocol	Direction	Info
HomePlug AV	EV -> Broadcast	CM_SLAC_PARM.REQ
HomePlug AV	EVSE -> EV	CM_SLAC_PARM.CNF
HomePlug AV	EV -> Broadcast	CM_SLAC_PARM.REQ
HomePlug AV	EV -> Broadcast	CM_START_ATTEN_CHAR.IND
HomePlug AV	EV -> Broadcast	CM_MNBC_SOUND.IND
HomePlug AV	EVSE -> EV	CM_ATTEN_CHAR.IND (Groups = 58, Avg. Attenuation = 32,66 dB)
HomePlug AV	EV -> EVSE	CM_ATTEN_CHAR.RSP
HomePlug AV	EV -> EVSE	CM_SLAC_MATCH.REQ
HomePlug AV	EVSE -> EV	CM_SLAC_MATCH.CNF
HomePlug AV	EV -> ?	CM_SET_KEY.REQ (Set Key Request)
HomePlug AV	? -> ?	CM_SET_KEY.CNF (Set Key Confirmation)
HomePlug AV	EV -> ?	Qualcomm Atheros, LINK_STATUS.REQ
HomePlug AV	? -> ?	Qualcomm Atheros, LINK_STATUS.CNF

Communication - 70121/15118

- Get EVSE IP address and port using SDP

Protocol	Direction	Info
V2GMSG (SDP)	EV -> Broadcast	SDP request message, No transport layer security
V2GMSG (SDP)	EVSE -> EV	SDP response message, No transport layer security

```
▾ V2G SECC Discovery Protocol Response
    SECC IP Address: fe80::201:87ff:fe08:1e79
    SECC Port: 49152
    Security: 0x10 (No transport layer security)
    Transport Protocol: 0x00 (TCP)
```

Communication - 70121/15118

- EV sends supported protocols
- EVSE chooses protocol (DIN-SPEC-70121 / ISO-15118-2 / ISO-15118-20)
- Messages encoded using EXI

```
V2G Message
▾ Metadata
    EXI: 8000EBAB9371D34B9B79D189A98989C1D191D191818999D26B9B3A232B30020000040001B75726E3A64696E3A37303132313A323031323A4D7367446566004000010088
    Message: supportedAppProtocolReq
    Decoded XML [truncated]: <?xml version="1.0" encoding="UTF-8"?><ns1:supportedAppProtocolReq xmlns:ns1="urn:iso:15118:2:2010:AppProtocol"><AppPr
    Message Validation: Successful
    Schema: urn:iso:15118:2:2010:AppProtocol
▾ supportedAppProtocolReq
    [XML Attributes:  xmlns:ns1="urn:iso:15118:2:2010:AppProtocol"]
  ▾ AppProtocol
      ProtocolNamespace: urn:iso:15118:2:2013:MsgDef
      VersionNumberMajor: 2
      VersionNumberMinor: 0
      SchemaID: 1
      Priority: 1
  ▾ AppProtocol
      ProtocolNamespace: urn:din:70121:2012:MsgDef
```

Protocol	Direction	Info
V2GMSG (SAP)	EV -> EVSE	supportedAppProtocolReq
V2GMSG (SAP)	EVSE -> EV	supportedAppProtocolRes

Communication - 70121/15118

- Continuous communication during charging
- Payment, charging parameters, etc. exchanged

Protocol	Direction	Info
V2GMSG (ISO-2)	EV -> EVSE	SessionSetupReq
V2GMSG (ISO-2)	EVSE -> EV	SessionSetupRes
V2GMSG (ISO-2)	EV -> EVSE	ServiceDiscoveryReq
V2GMSG (ISO-2)	EVSE -> EV	ServiceDiscoveryRes
V2GMSG (ISO-2)	EV -> EVSE	PaymentServiceSelectionReq
V2GMSG (ISO-2)	EVSE -> EV	PaymentServiceSelectionRes
V2GMSG (ISO-2)	EV -> EVSE	AuthorizationReq
V2GMSG (ISO-2)	EVSE -> EV	AuthorizationRes
V2GMSG (ISO-2)	EV -> EVSE	ChargeParameterDiscoveryReq
V2GMSG (ISO-2)	EVSE -> EV	ChargeParameterDiscoveryRes
V2GMSG (ISO-2)	EV -> EVSE	PowerDeliveryReq
V2GMSG (ISO-2)	EVSE -> EV	PowerDeliveryRes
V2GMSG (ISO-2)	EV -> EVSE	ChargingStatusReq
V2GMSG (ISO-2)	EVSE -> EV	ChargingStatusRes
V2GMSG (ISO-2)	EV -> EVSE	PowerDeliveryReq
V2GMSG (ISO-2)	EVSE -> EV	PowerDeliveryRes
V2GMSG (ISO-2)	EV -> EVSE	SessionStopReq
V2GMSG (ISO-2)	EVSE -> EV	SessionStopRes

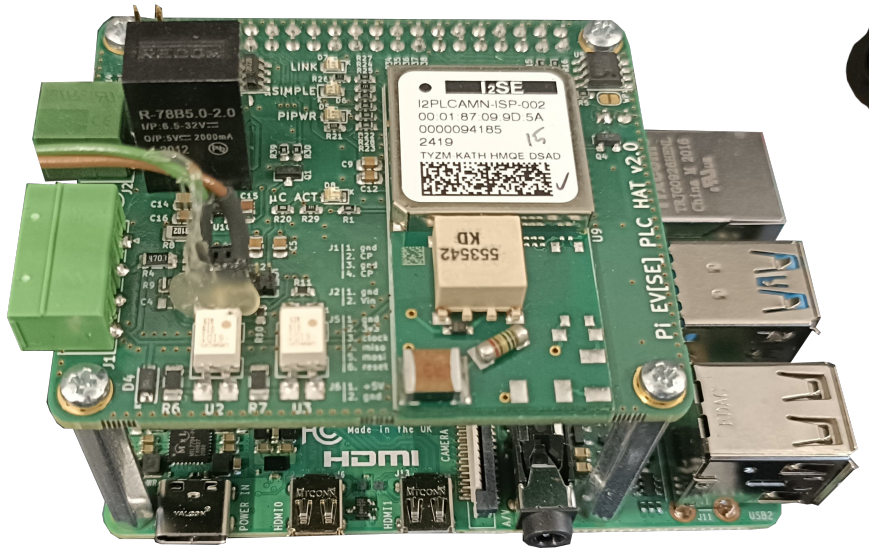
PLC modem

- Modem available in Linux as ethernet interface
- Service listening on all interfaces available via PLC

```
pi@evcc02:~ $ ifconfig
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::10dc:d0ff:fe45:fb72  prefixlen 64  scopeid 0x20<link>
        ether 12:dc:d0:45:fb:72  txqueuelen 100  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 816 (816.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Testing hardware

- Raspberry Pi with HAT in Pelican Case
- Uses I2SE PLC Stamp Mini 2 modem
- HAT connected to relevant pins of charging socket



Testing software

- IEC 61851: self-developed script
- SLAC: self-developed script
- DIN-SPEC-70121 / ISO-15118: altered SwitchEV Josev[1]

[1] https://github.com/SwitchEV/iso15118

Methodology

- Access to many charging stations

- Connect testbox to charging station


```
▾ EVSEMinimumCurrentLimit: 0h
    Multiplier: 0
    Unit: h
    Value: 0
▾ EVSEMinimumVoltageLimit: 0h
    Multiplier: 0
    Unit: h
    Value: 0
▾ EVSEPeakCurrentRipple: 0h
    Multiplier: 0
    Unit: h
    Value: 0
```

Testlab picture for reference, displayed chargers are not specifically part of research, or vulnerable

Demo


Charging Station Login
Elaadnl
ISO 15118
Charger out
L1
L2
L3
Charger in
ISO 15118
charging station
Elaadnl

Recap

- Capture IPv6 address, run *Nmap* scan
- Limit scan speed
- Forward using *socat*

```
pi@evcc02:~ $ nmap -Pn -n --scan-delay 10ms -p 8008 -r fe80::201:87ff:fe05:ef86%eth1 -6
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-15 14:59 CEST
Nmap scan report for fe80::201:87ff:fe05:ef86
Host is up (0.0056s latency).

PORT     STATE SERVICE
8008/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
pi@evcc02:~ $ socat -dd tcp4-listen:8008,reuseaddr,fork tcp6:[fe80::201:87ff:fe05:ef86%eth1]:8008
2024/10/15 14:59:44 socat[1166] W ioctl(5, IOCTL_VM_SOCKETS_GET_LOCAL_CID, ...): Inappropriate ioctl for device
2024/10/15 14:59:44 socat[1166] N listening on AF=2 0.0.0.0:8008
```

Results

- 18 DC + 1 AC charging stations, 13 manufacturers
- 10 charging stations (53%) exposed some service
  - Eight chargers with SSH exposed
  - One charger with MQTT exposed
  - Two chargers with HTTP exposed
  - Some other (proprietary) services exposed

Results – MQTT server

outlet/1/dc-metering {"actualCurrent":0.061523438,"actualVoltage":199.70001,
"accumulatedEnergy":1272.699}
outlet/1/dc-metering/meterdata {"publicKey":"","meterId":""}
outlet/1/diagnostics/eea {"controlPilotPositiveVoltage":5.684,"controlPilotNegativeVoltage":
-11.223,"controlPilotDutyCycle":4,"controlPilotFrequency":1000,"averageAttenuation":7.5689654}
outlet/1/module {"state":"Operational","errors":[],"climateMeasurements":{"measurements":
[{"name":"DCPositive","property":"Temperature","value":21.31},{"name":"DCNegative","property":
"Temperature","value":21.1},{"name":"Cabinet","property":"Temperature","value":26.119999}]},
"ip":"192.168.1.2"}

- Unsuccessful in manipulating functioning

Results – HTTP servers

- Access gives control over CS configuration
- Brute-forceable default password
- Vulnerabilities in backup/restore functionality leads to RCE

Impact

- Network services attacked from charging cable
  - Pivot into internal network
  - Impact on mobility
  - Power grid stability, blackouts
- Malicious cars

Conclusion

- Large ethernet attack surface
- Misconfiguration is common
- Increased attention to cyber security needed

What's next?

- Report findings
- Test charging station at ElaadNL, conduct external pentests
- Continued testing of charging stations, planned testing for EVs
- ElaadNL advices public tenders and legislators
  - Network and Information Systems directive (NIS2)
  - Radio Equipment Directive (RED)
  - Cyber Resilience Act (CRA)

Thank you!

Questions?

Wilco van Beijnum – wilco.van.beijnum@elaad.nl
Sebastiaan Laro-Tol – sebastiaan.laro.tol@elaad.nl


Elaadnl