Elaadnl

CYBER SECURITY IN THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Paul Broos
23 April 2024

About ElaadNL

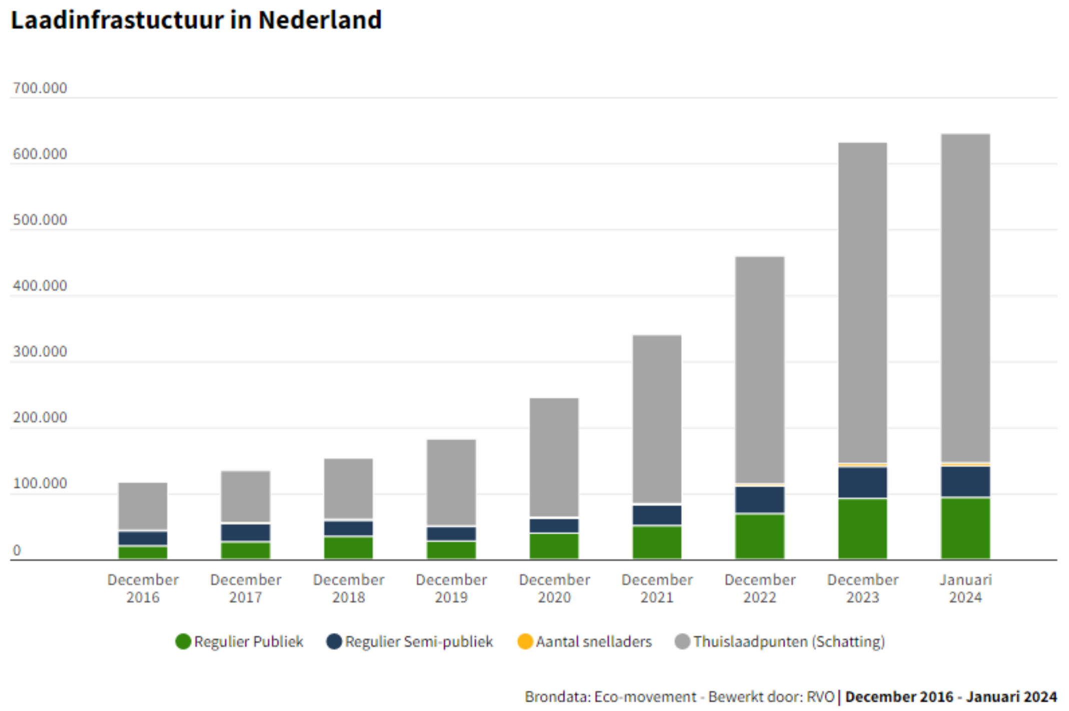
- Initiative of Dutch grid operators, founded 2009
- Forecasts of market developments electric mobility
- Smart charging
- Fast charging stations for trucks
- Process improvement roll out of charge points
- Testlab:
  - Interoperability
  - Power quality
  - Smart charging
- Innovation e.g. Grid Shield
- Cyber security

Risks and grid impact

- 300.000 cars charging equals 3GW of *collective* power
- 3GW is the European incident reserve capacity (frequency containment reserves)

A large hack, could potentially disturb the entire European grid.

Vehicle to grid only adds to this challenge.



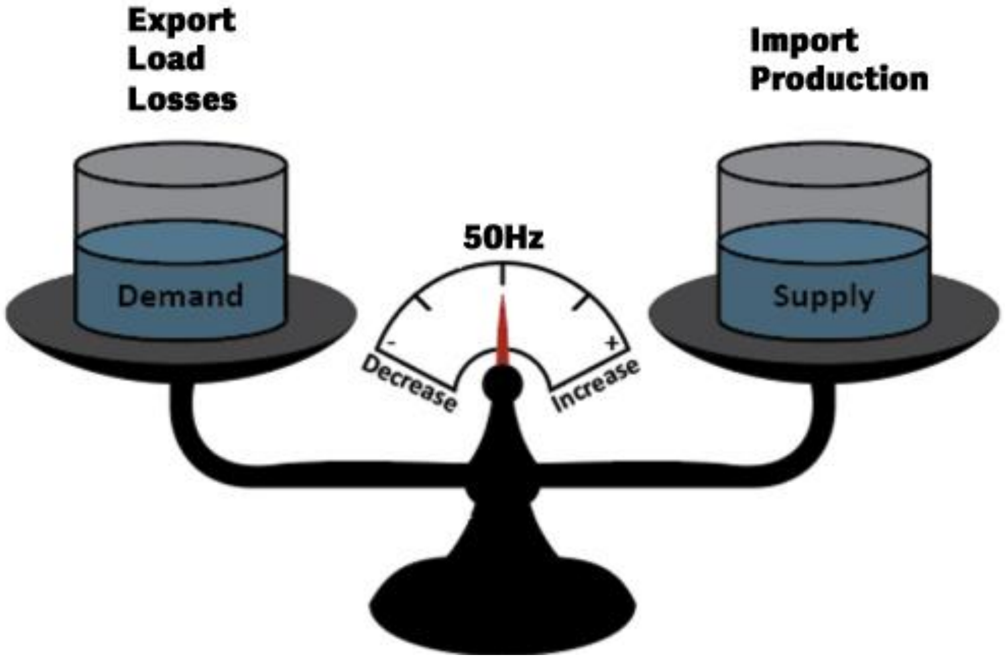
Laadinfrastuctuur in Nederland

Brondata: Eco-movement - Bewerkt door: RVO | **December 2016 - Januari 2024**

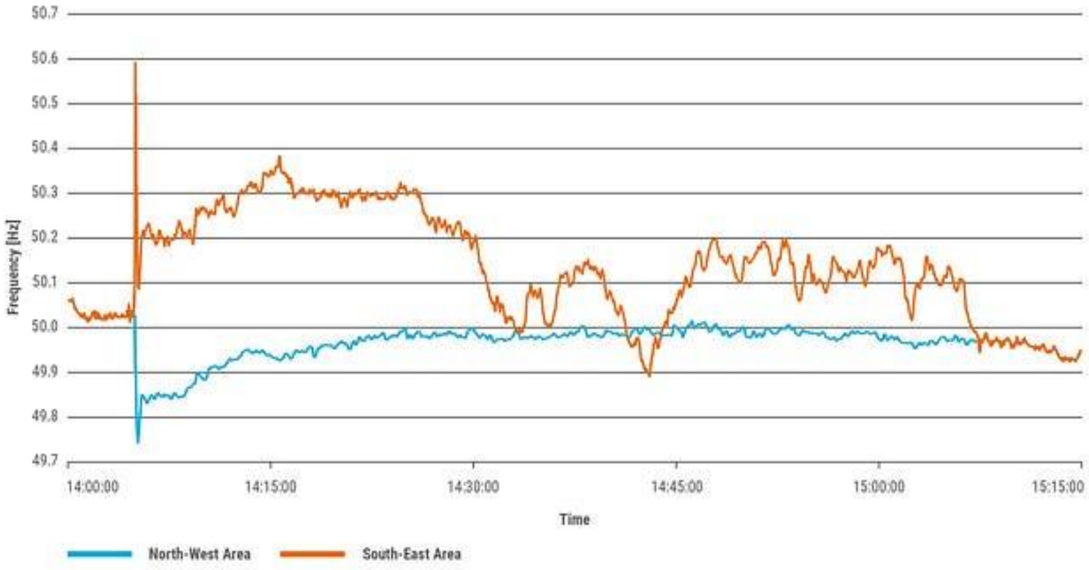
498801	*private/home chargers*
93974	*public chargers*
48012	*semi-public public chargers*

https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2017%3A220%3ATOC&uri=uriserv%3AOJ.L_.2017.220.01.0001.01.ENG

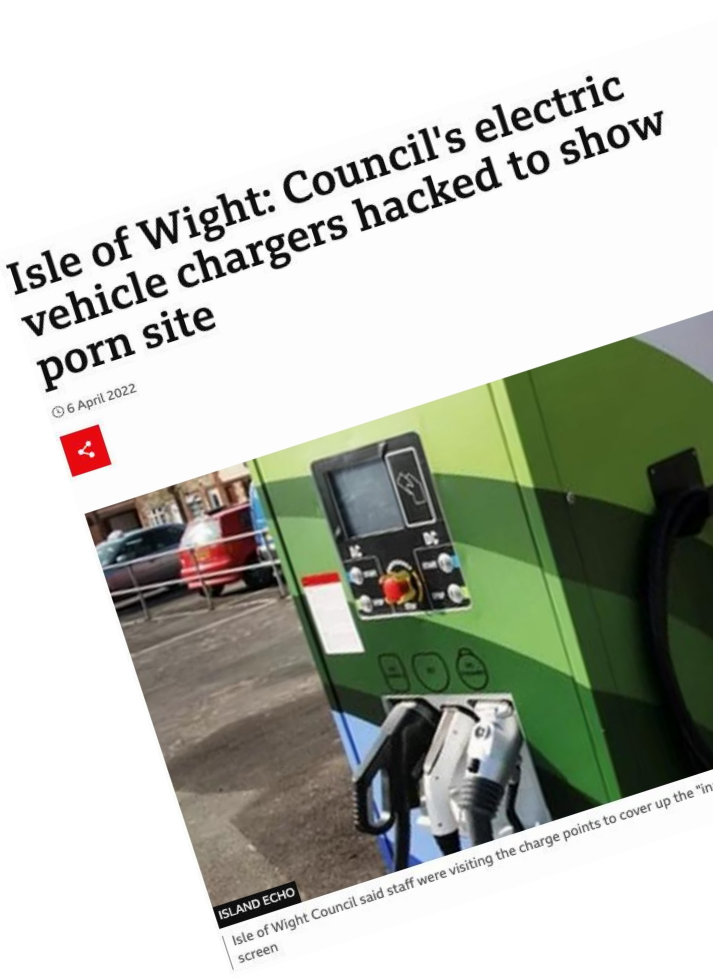
Mismatch in demand and supply



8th of January 2021



The need for Cyber Security

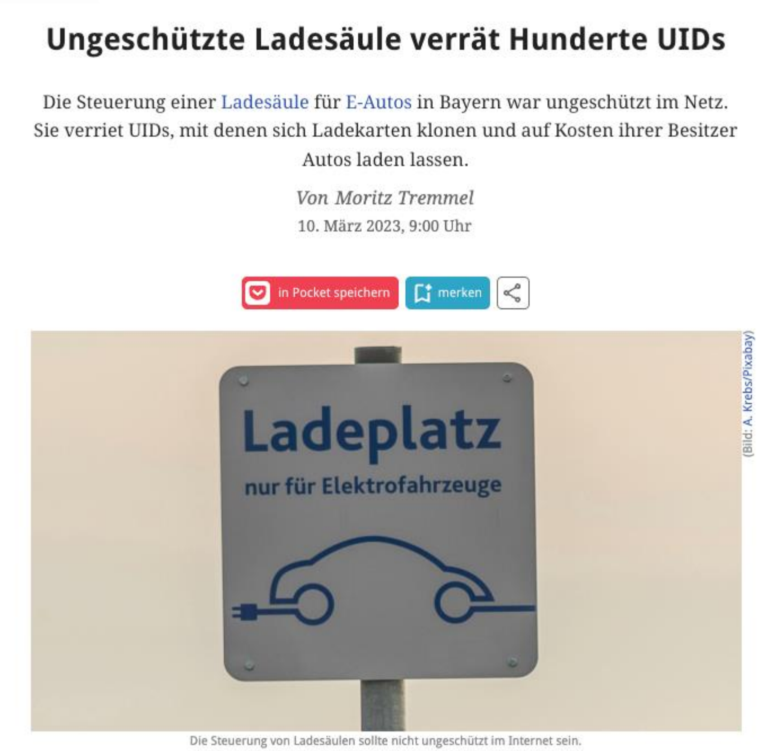


Isle of Wight: Council's electric vehicle chargers hacked to show porn site

6 April 2022

ISLAND ECHO

Isle of Wight Council said staff were visiting the charge points to cover up the "in
screen



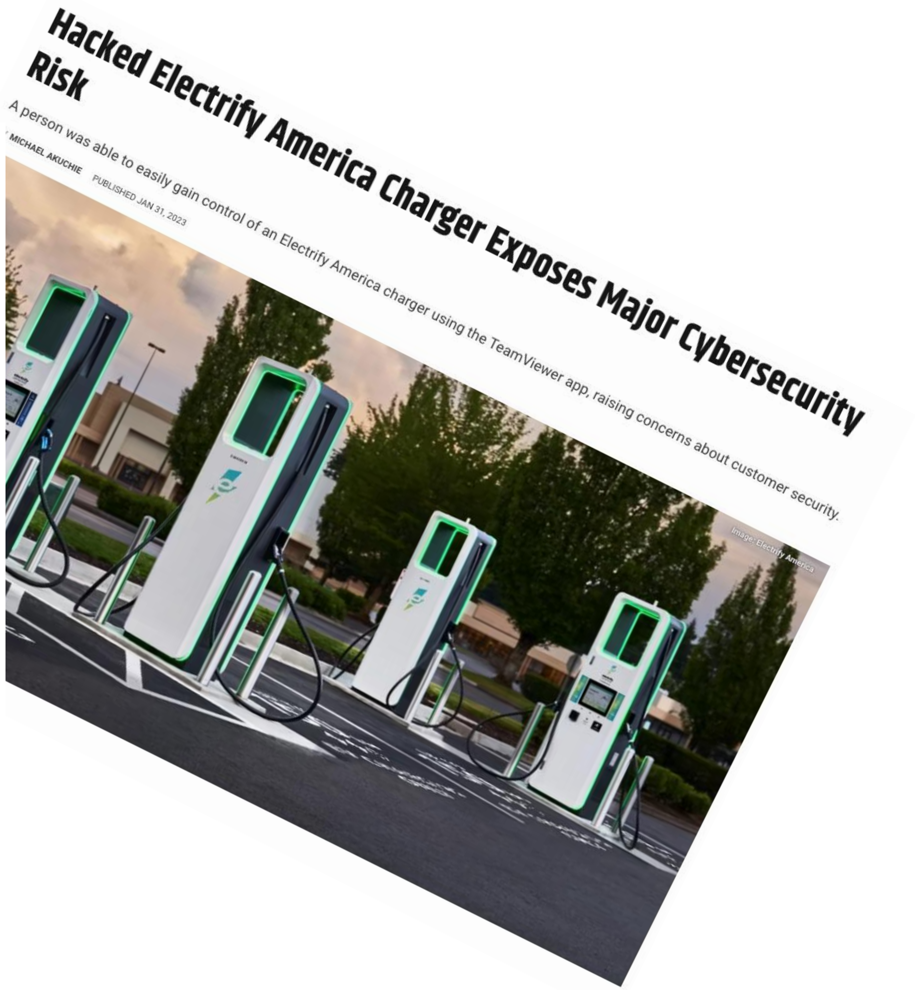
Ungeschützte Ladesäule verrät Hunderte UIDs

Die Steuerung einer Ladesäule für E-Autos in Bayern war ungeschützt im Netz. Sie verriet UIDs, mit denen sich Ladekarten klonen und auf Kosten ihrer Besitzer Autos laden lassen.

Von Moritz Tremmel
10. März 2023, 9:00 Uhr

(Bild: A. Krebs/Pixabay)

Die Steuerung von Ladesäulen sollte nicht ungeschützt im Internet sein.



Hacked Electrify America Charger Exposes Major Cybersecurity Risk

A person was able to easily gain control of an Electrify America charger using the TeamViewer app, raising concerns about customer security.

MICHAEL AKUCHIE PUBLISHED JAN 31, 2023

Image: Electrify America

Risks

EV driver

- Car not charged
- Private information leaked
- Manipulation of financial details of transaction

Grid

- Local grid overload (if smart charging is overruled)
- Black-out (inter)national grid

Risks and grid impact

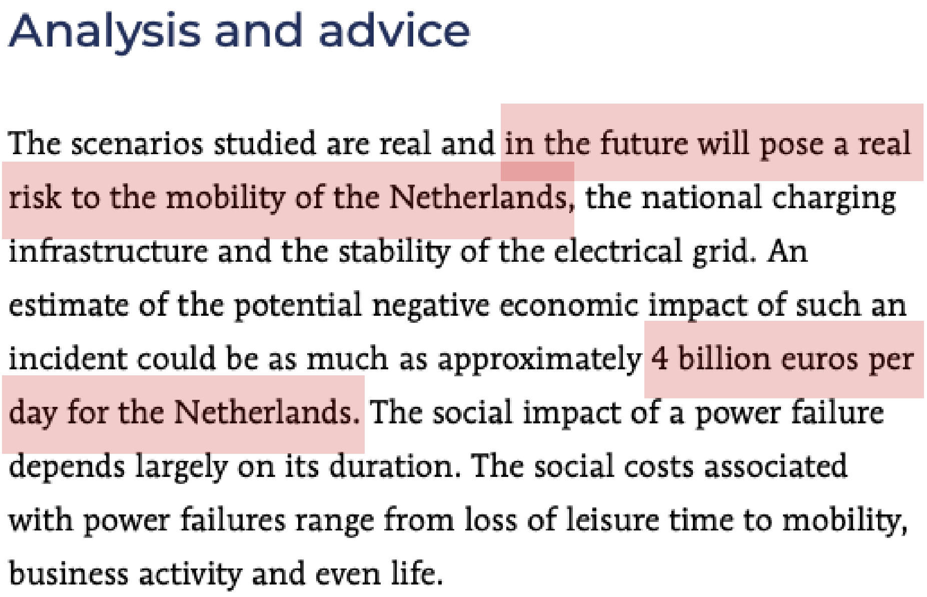
Berenschot

REPORT

Impact of cyber-security risks on the Dutch national charge point infrastructure

National charging infrastructure

30 november 2021 | 65719 | Public



Analysis and advice

The scenarios studied are real and in the future will pose a real risk to the mobility of the Netherlands, the national charging infrastructure and the stability of the electrical grid. An estimate of the potential negative economic impact of such an incident could be as much as approximately 4 billion euros per day for the Netherlands. The social impact of a power failure depends largely on its duration. The social costs associated with power failures range from loss of leisure time to mobility, business activity and even life.

Report by Berenschot

https://www.agendalaadinfrastructuur.nl/PageByID.aspx?sectionID=208529&contentPageID=2135552

Hack the charge station through the car

In Europe, the vehicle-to-grid (V2G) system is already available. This system allows stored energy in car batteries to be redistributed over the grid to help balance demand vis-à-vis production level.

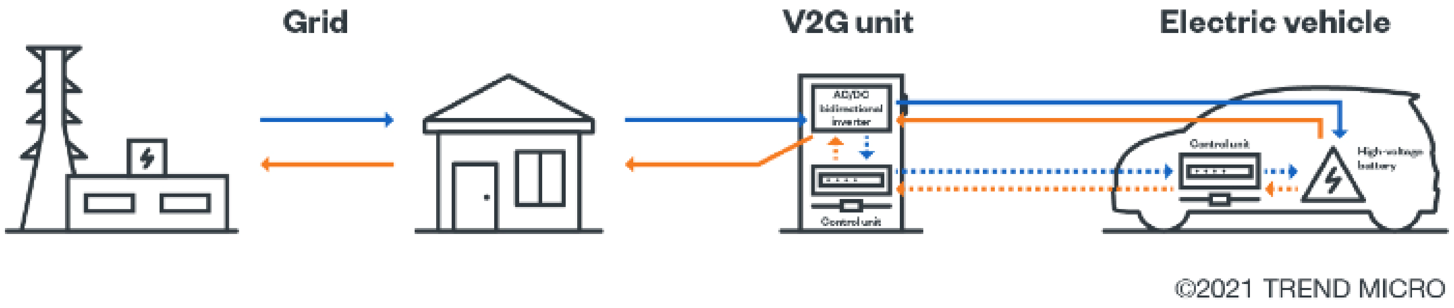


Figure 1. A simple V2G infrastructure

Image reference: Automobile Propre

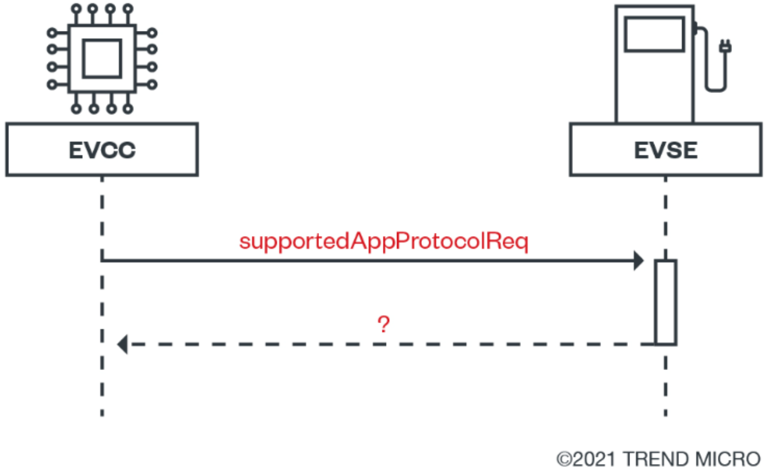
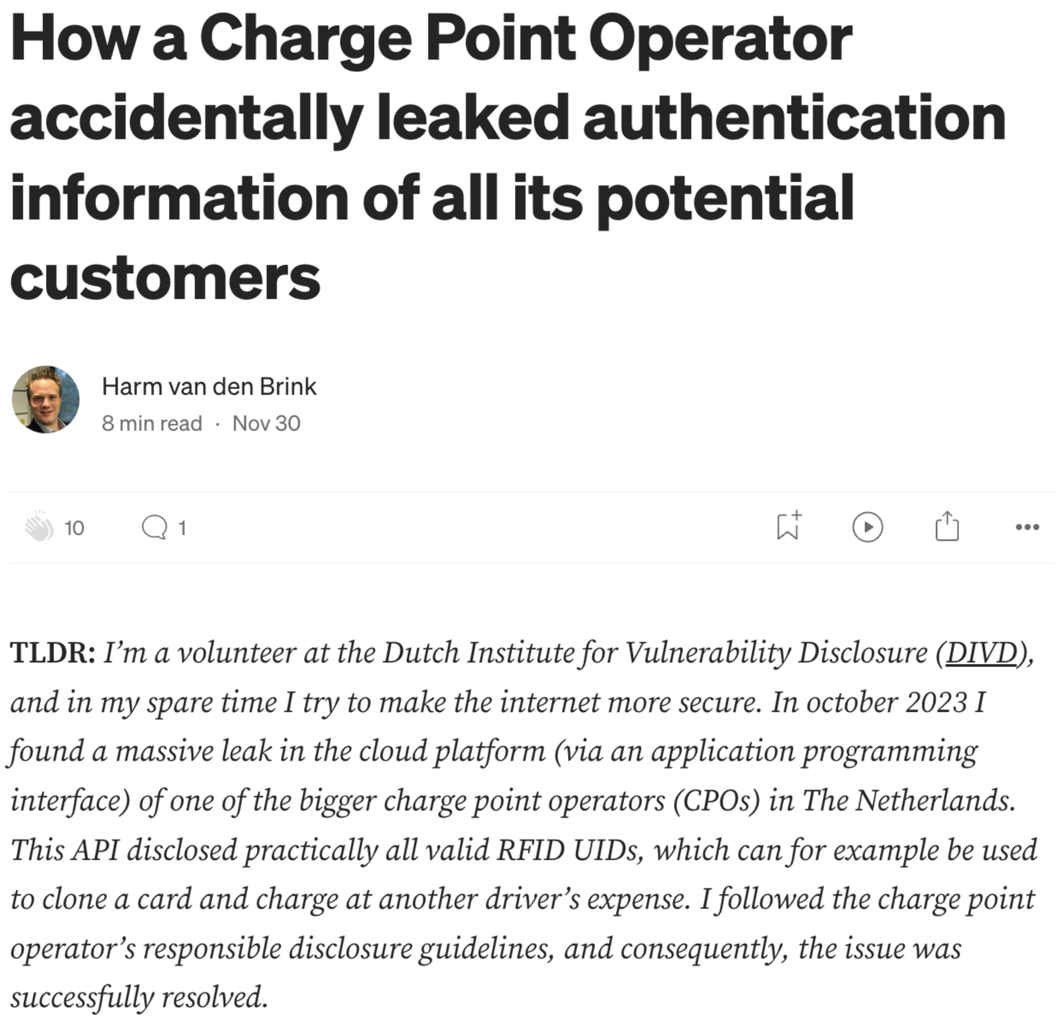


Figure 3. Attacking the first state with V2GInjector

https://www.trendmicro.com/en_us/research/21/l/examining-log4j-vulnerabilities-in-connected-cars.html

Leaking RFID UIDs



How a Charge Point Operator accidentally leaked authentication information of all its potential customers

Harm van den Brink
8 min read · Nov 30

TLDR: *I'm a volunteer at the Dutch Institute for Vulnerability Disclosure (DIVD), and in my spare time I try to make the internet more secure. In october 2023 I found a massive leak in the cloud platform (via an application programming interface) of one of the bigger charge point operators (CPOs) in The Netherlands. This API disclosed practically all valid RFID UIDs, which can for example be used to clone a card and charge at another driver's expense. I followed the charge point operator's responsible disclosure guidelines, and consequently, the issue was successfully resolved.*

How to improve the cyber security of EV-charging

Issue: Dutch grid-operators have no legal means to demand sufficient security controls by Charge Point Operators.

Solution:

1. Develop a standardized set of security requirements
   a. Simplifies better procurement of charge points
   b. Eases the product management task for suppliers
   c. Simplifies products and reduces cost of products
2. Convincing lawmakers that CPOs should be added to energy sector in NIS2.
3. Convincing lawmakers that the CRA should also address the risks of charge points.

Requirements

ElaadNL & ENCS (European Network for Cyber Security) requirements

European Network for Cyber Security

Commissioned by ElaadNL

EV Charging Systems

Security Requirements

Elaadnl

Version 1.0 - April 2016

https://encs.eu/resource/ev-301-2019-security-requirements-for-procuring-ev-charging-stations/

Requirements

- Part of most public tenders in the Netherlands since 2017
- Thousands of charge stations already compliant
- Multiple chargers tested and pen-tested

Requirements

In the UK for home chargers it states:

Cybersecurity statements

Manufacturers must either comply with the cybersecurity requirements in The Electric Vehicles (Smart Charge Points) Regulations 2021 or provide answers to the following questions:

1. How does the chargepoint ensure an appropriate level of encryption of the communications between the chargepoint and the chargepoint operator?
2. How does the chargepoint operator ensure its communications and functions are appropriately encrypted?

Manufacturers must provide a detailed description of the features that ensure communications between the chargepoint and chargepoint operator are secure, preferably referring to any relevant standards in their response.

Compliance with the **European Network for Cyber Security EV Charging Systems Security Requirements** is considered an appropriate level of cybersecurity.

Requirements

ElaadNL & ENCS requirements since 2017

- EV-301-2019 Security requirements for procuring EV charging stations
  - Access control
  - Cryptography
  - Physical and environmental security
  - Operations security
  - Communication security
  - System aquisition, development and maintenance
  - Supplier relationships
  - Information security aspects of business continuity management

Operations security

Future-Proof design (OP1-CS):

Charging stations need enough memory and computational power for future security updates. This prevents obsolescence and maintains security over the product's lifespan. Implement by choosing hardware capable of handling anticipated future updates and expansions.

Tamper detection (PH3-CS):

The charging station must detect physical tampering, such as when the cover is opened. This mitigates the risk of physical tampering with the device which could compromise system integrity. Implementation can be through physical locks, tamper-evident seals, and logging access.

Use of strong cryptographic keys and algorithms (CR1-CS):

This ensures that the charging station employs robust cryptographic practices. The risk of decryption of sensitive data by unauthorized entities is mitigated. Implement strong encryption standards as per guidelines such as those recommended by the ECRYPT* report.

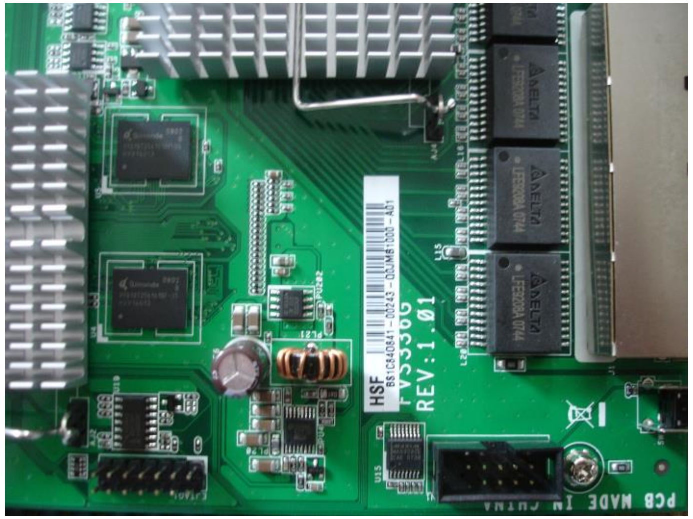
OP4-CS: Security events

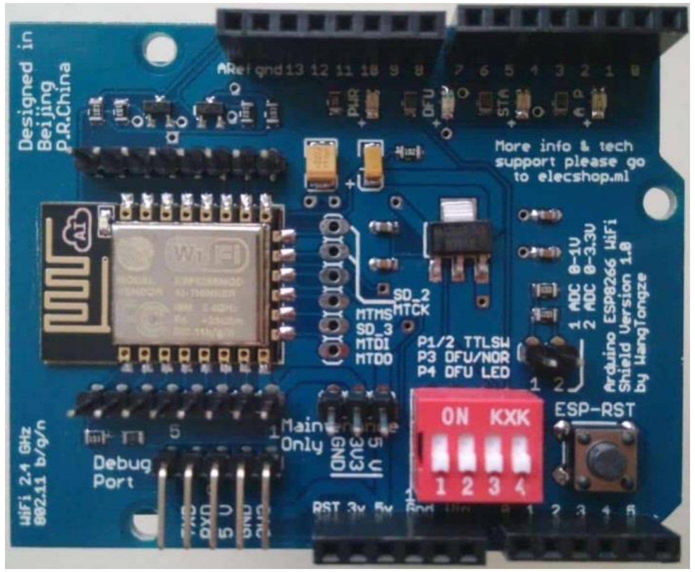
The charging station shall be able to log security events for the following in a local log:

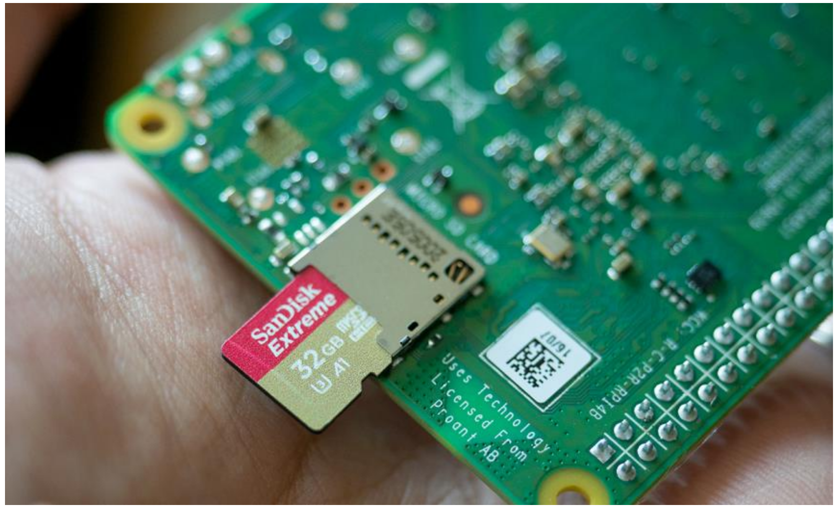
1. Firmware updates
2. Failed authentication attempts
3. Changes to the system time
4. Booting the device
5. Changes to the security log
6. Changes to security parameters
7. Memory exhaustion
8. Attempts to physically tamper with the device
9. Invalid firmware signatures
10. Invalid certificates
11. Invalid settings for cryptographic protocols such as TLS

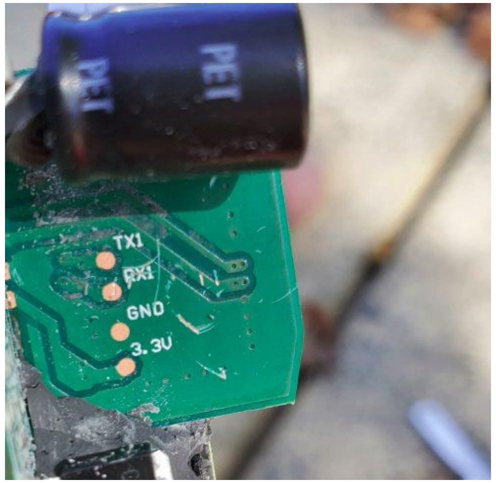
The log entries for security events shall include a timestamp, an event description and the user, role or process causing the event.

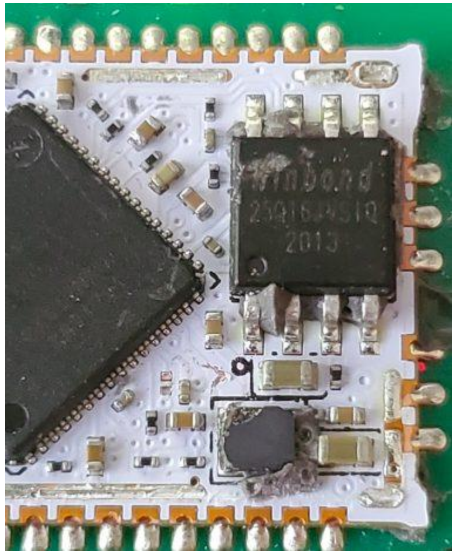
Physical and environmental security




Designed in Beijing P.R.China
More info & tech support please go to elecshop.ml
Arduino ESP8266 WiFi Shield Version 1.0 by WangTongze
P1/2 TTLSW
P3 DFU/NOR
P4 DFU LED
ESP-RST
ON KXK
Debug Port
Main Only
WiFi 2.4 GHz 802.11 b/g/n

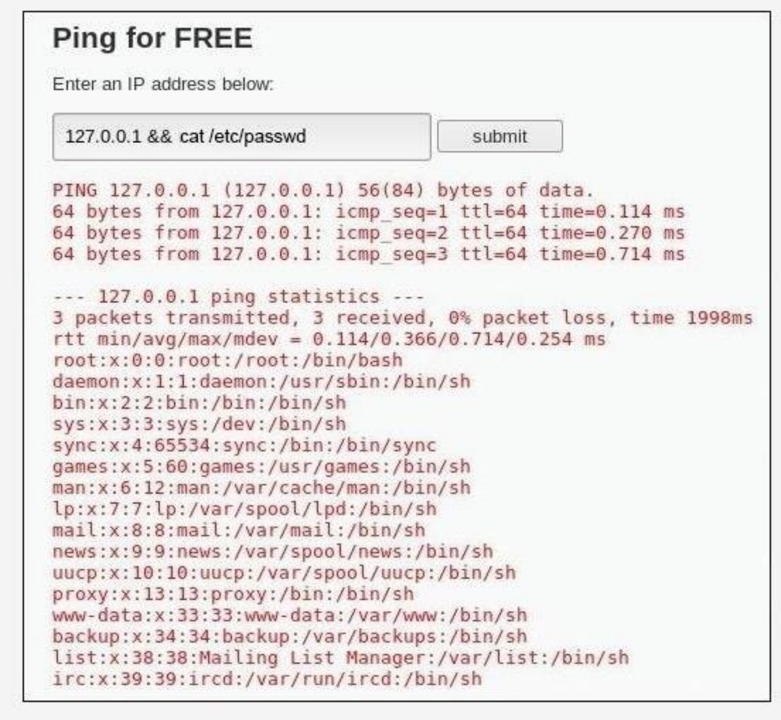






Some vulnerabilities we saw

- Remote code execution
- Command injection
- Debug ports on hardware
- Unencrypted flash
- DoS via OCPP
- ...



Ping for FREE

Enter an IP address below:

127.0.0.1 && cat /etc/passwd

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.270 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.714 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.114/0.366/0.714/0.254 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
```

What’s next?

Requirements to norm

IEC 62443: *a framework for ensuring the security of Industrial Control Systems (ICS) and Operational Technology (OT) networks*

- Mapping ENCS/ElaadNL requirements to IEC 62443 (62443-4-1 & 62443-4-2)
- Pre-qualify and gap analysis for IEC 62443
- Testing & Certification via IEC 62443 scheme

NIS2

In Annex I (Sectors **of High Criticality**)

we find that "Distribution system operators", "Transmission system operators", "Producers", "Nominated electricity market operators", "Market participants providing aggregation, demand response or energy storage services", and

"**Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider**"

are in the scope of the NIS 2 Directive.

Elaadnl