black hat
BRIEFINGS

AUGUST 6-7, 2025
MANDALAY BAY / LAS VEGAS

Smart Charging, Smarter Hackers:
The Unseen Risks of ISO 15118

Salvatore Gariuolo

About me

Dr. Salvatore Gariuolo

Senior Threat Researcher

TREND MICRO™

Agenda

1. The ISO 15118 Standard

A strategic response to the EV surge

2. Old Risks, New Risks?

How ISO 15118 changes the threat landscape

3. The Hidden Risks of Compliance

Conclusion and key takeaways

1. The ISO 15118 Standard

A Strategic Response to the EV Surge

EV Surge: What is the problem?

As of today, approx.

27 Million EVs

3% of the global fleet

By 2040, we expect

600 Million EVs

30% of the global fleet

Grid Strain

California implores residents to reduce power use to avoid blackouts.

The New York Times

Power Grids: A Fragile Balance

April 2025, **A lesson from Spain:**

- **Excess electricity can disrupt grid's frequency**
- Renewables supply 50% - but they're intermittent
- Consumption can adjust quickly - generation can't

The entire grid was disconnected to prevent a full collapse

BLACKOUT

Grid Stress: What is the solution?

Upgrade Grid Infrastructure

Global investment needs could exceed **$4.5 billion** per year

Smart charging and V2G communication

- Dynamic charging based on grid conditions and user preferences
- EVs can absorb excess electricity and feed it back when needed

ISO 15118 : Three Key Benefits

Across two versions: **ISO 15118-2** and **ISO 15118-20**

Grid-efficient

- Smart Charging
- **Vehicle-to-Grid**

User-friendly

- Plug & Charge
- Multiple Profiles

Secure

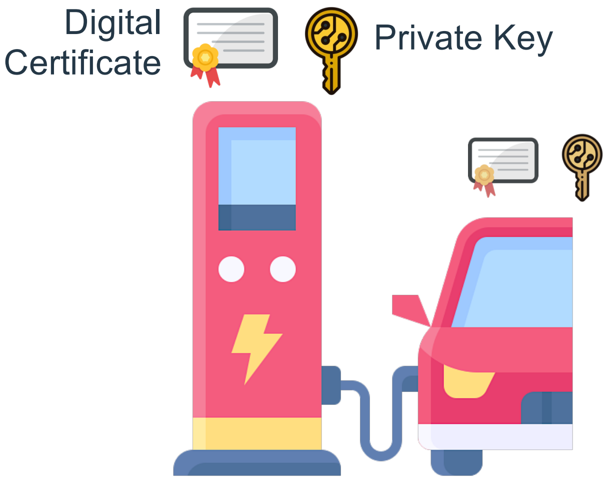
- Public Key Infrastructure
- Transport Layer Security

2. Old Risks, New Risks?

How ISO 15118 changes the threat landscape

A. Mitigated Risks

Securing the Communication between EVs and Charging Stations



How does Plug&Charge work?

- Authentication and Authorization through **PKI**
- Data transmission encrypted via **TLS**

No more RFID cloning or card skimming

No more eavesdropping on session ID and data

A. Mitigated Risks

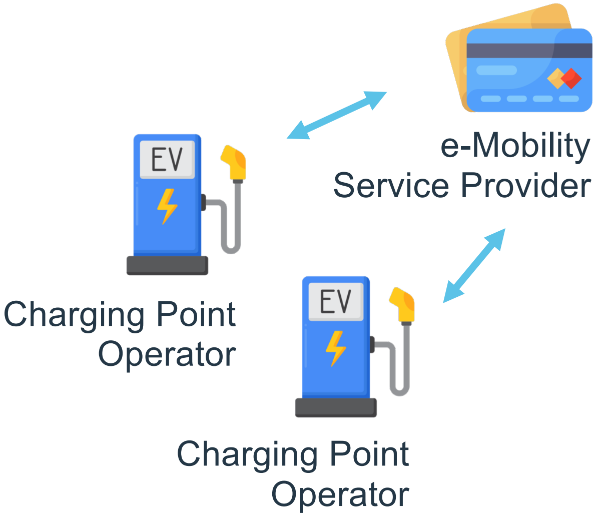
Securing the Communication between EVs and Charging Stations

Threat	Pre - ISO 15118	ISO 15118-2	ISO 15118-20
Unauthorized Charging	🟥	🟩	🟩
Session Hijacking	🟥	🟨	🟩

🟩 Low 🟨 Medium 🟥 High

B. Shifted Risks

Moving Data Security to a Centralized Back-End



How is user data handled?

- **Single entity** managing payments and data
- **More consistency**, lower risk exposure

Charging stations are no longer exploitable

eMSP breaches can expose large pool of data

B. Shifted Risks

Moving Data Security to a Centralized Back-End

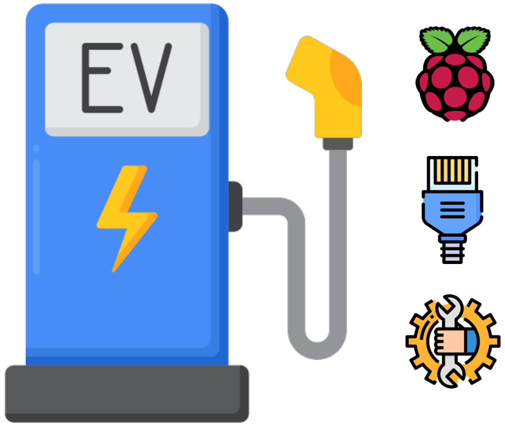
Threat	Pre - ISO 15118	ISO 15118-2	ISO 15118-20
User Data Theft *	🟩	🟨	🟨

* *The risk moves from the* ***charging station*** *to the* ***eMPS***

🟩	🟨	🟥
Low	Medium	High

C. Residual Risks

Charging Stations Remain the Weak Link



Why is this happening?

- **Poor implementation** of charging stations
- **No ISO 15118 guidelines** on physical security

Stations remain vulnerable to compromise

No mechanism to verify charging station integrity

C. Residual Risks

Charging Stations Remain the Weak Link

Threat	Pre - ISO 15118	ISO 15118-2	ISO 15118-20
Denial-of-Service	🟥	🟥	🟥
Unsafe Power Delivery	🟥	🟥	🟥
Unauthorized Charging *	🟥	🟥	🟥

** A threat that ISO 15118 was designed to mitigate*

D. New Risks

How Innovation Opens the Door to New Threats

Where do these risks come from?

- New features like **Smart charging** and **V2G**
- **Vulnerable charging stations** as entry points

Grid signal manipulation to simulate congestion

Synchronized charging / discharging cycles

D. New Risks

How Innovation Opens the Door to New Threats

Threat	Pre - ISO 15118	ISO 15118-2	ISO 15118-20
Charging Manipulation	🟨	🟨	🟥
Battery Degradation *			🟥
Grid Attack *			🟨

** These threats require V2G communication*

3. The Hidden Risks Of Compliance

Conclusion and key takeaways

A Standard can create a false sense of security

True security requires a shift in mindset

Black Hat Sound Bites

- While reducing risks, standards can create blind spots
- When one piece is left out, the whole ecosystem is at risk
- True security requires action beyond compliance