VicOne
Driving Automotive Cybersecurity Forward

EVSE Cybersecurity Landscape: Threats, Vulnerabilities and Key Considerations

Michael Fulgencio

Solution Engineer, VicOne North America

EVSE Expansion Outpaces Cybersecurity

1 Expanding Exposure

The rapid deployment of 192,000 U.S. charging ports has broadened the attack surface across connected EVSE networks and backend systems.

2 Lagging Cybersecurity Maturity

Despite this growth, most EVSE operators rely on traditional IT tools that protect networks, not embedded firmware or controllers. This mismatch creates unseen vulnerabilities in the charging network.

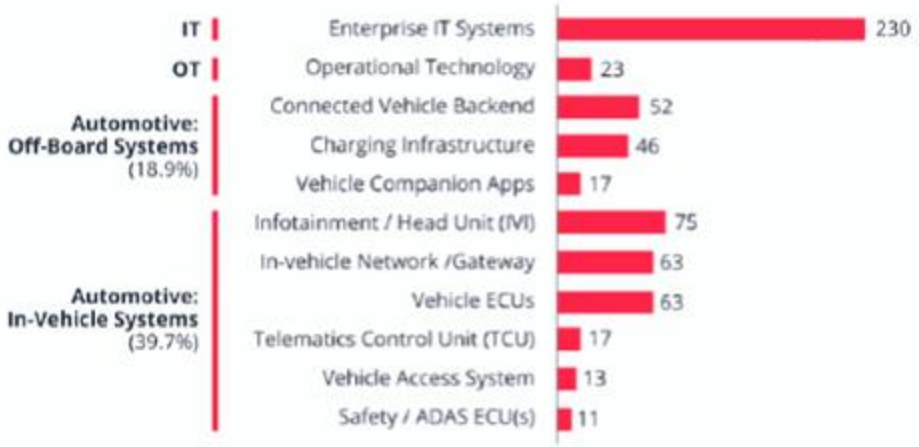
3 Evolving Threat Activity

While no Advanced Persistent Threats (APT) or state-sponsored campaigns are evident, data and PII breaches, fraud, and vulnerabilities show that cybercriminals are increasingly probing the EV ecosystem.

2025 Automotive Threat Landscape – Why It Matters for EV Charging?

610
Total Incidents
(2024 total: 215)

Where Attackers Focus



1,384
Vulnerabilities
(2024 total: 954)

Where Vulnerabilities Impact Vehicle Domains

FROM ISOLATED SYSTEMS TO OVERLAPPING RISK DOMAINS

VicOne

EVSE in the News

New Flaws Expose EVlink Electric Vehicle Charging Stations to Remote Hacking

Schneider Electric has patched several new vulnerabilities that expose its EVlink electric vehicle charging stations to remote hacker attacks.

Watch Out Electric Vehicle Owners – Brokenwire Attack Remotely Disrupts Charging

https://www.hackread.com/brokenwire-attack-electric-vehicle-charging-remotely-disrupt/

Hackers Are Targeting EV Charging Stations

by Becca Hopkins | More Articles: News
Published on May 6, 2022 | Comments (0)

SHARE:

The growing number of EV charging stations in the U.S. and worldwide allows more drivers to easily access the convenience and eco-friendliness of driving an electric vehicle. However, there's a major downside to these rapidly appearing EV charging stations: they are surprisingly vulnerable to cyberattacks from hackers.

EV charging station attacks are becoming more common

EV CHARGERS COULD BE A SERIOUS TARGET FOR HACKERS

by: Lewin Day

56 Comments

November 28, 2022

Computers! They're in everything these days. Everything from thermostats to fridges and even window blinds are now on the Internet, and that makes them all ripe for hacking.

Electric vehicle chargers are becoming a part of regular life. They too are connected devices, and thus pose a security risk if not designed and maintained properly. As with so many other devices on the Internet of Things, the truth is anything but.

COMPROMISED!

Pranksters hack electric vehicle charging station screens to display porn website

Motorists at electric vehicle charging stations in UK's Isle of Wight got a bit of a shock recently after seeing pornographic visuals on display screens. How did that happen? Well, the display screens at the electric vehicle charging points were reportedly hacked and started displaying a porn website. Many signs at the stations were hacked and some customers found themselves directed to a graphic porn site.

TN Viral Desk | Updated Apr 27, 2022 | 05:51 PM IST

Share This Article

UP NEXT

1 Pranksters hack electric vehicle charging station screens to display porn...

2 Madame Tussaud was forced to practice her waxwork and sculpting skill...

Representative image

Photo : iStock

Ad closed by Google

https://www.timesnownews.com/viral/pranksters-hack-electric-vehicle-charging-station-screens-to-display-porn-website-article-91127012

Vulnerabilities could let hackers remotely shut down EV chargers, steal electricity

The emerging market's uneven response to fix the flaws suggests cybersecurity could be a growing concern in electric car charging networks.

BY CHRISTIAN VASQUEZ • FEBRUARY 1, 2023

https://www.motorbiscuit.com/hackers-targeting-ev-charging-stations/

VicOne

The Current EVSE Threat Landscape

Cybercriminal activities

Ransomware and data breaches

Phishing and scams

Physical threats and vandalism

Research-identified vulnerabilities

Denial of service (DoS) and communication disruptions

Insider threats

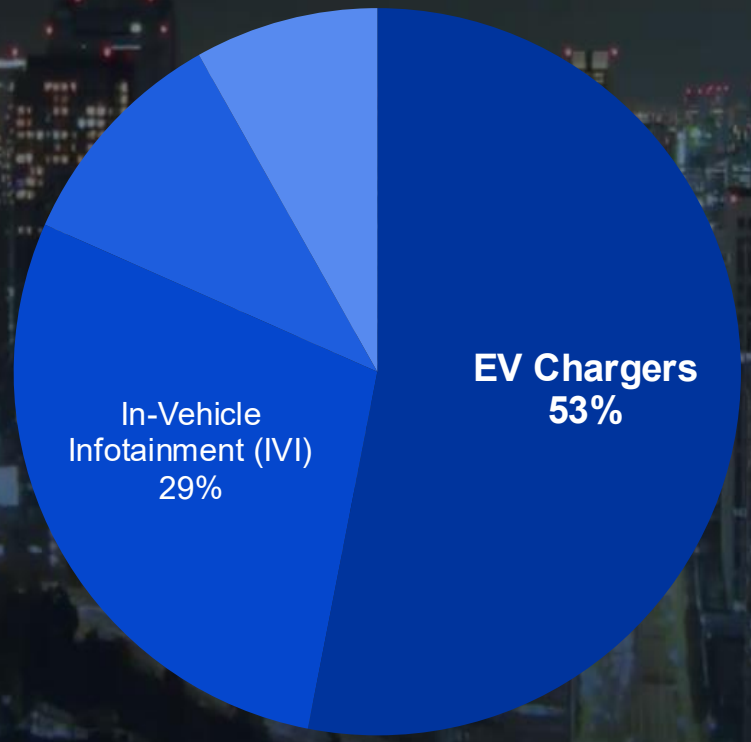
Grid manipulation

VicOne | ZERO DAY INITIATIVE

PWN2OWN AUTOMOTIVE

Pwn2Own Automotive Exploits:

- Pwn2Own Automotive 2024 & 2025: **50+ Zero-Day** vulnerabilities across EVSE brands
- Exploits: Buffer overflows, RCE, auth bypass
- Devices: ChargePoint, Tesla, Phoenix Contact, Autel, Ubiquiti, WolfBox



Zero-Day Vulnerabilities by Category

EV Chargers | In-Vehicle Infotainment (IVI) | Tesla | Operating System

Pwn2Own Automotive 2026: 76 Zero-Day Vulnerabilities

VicOne

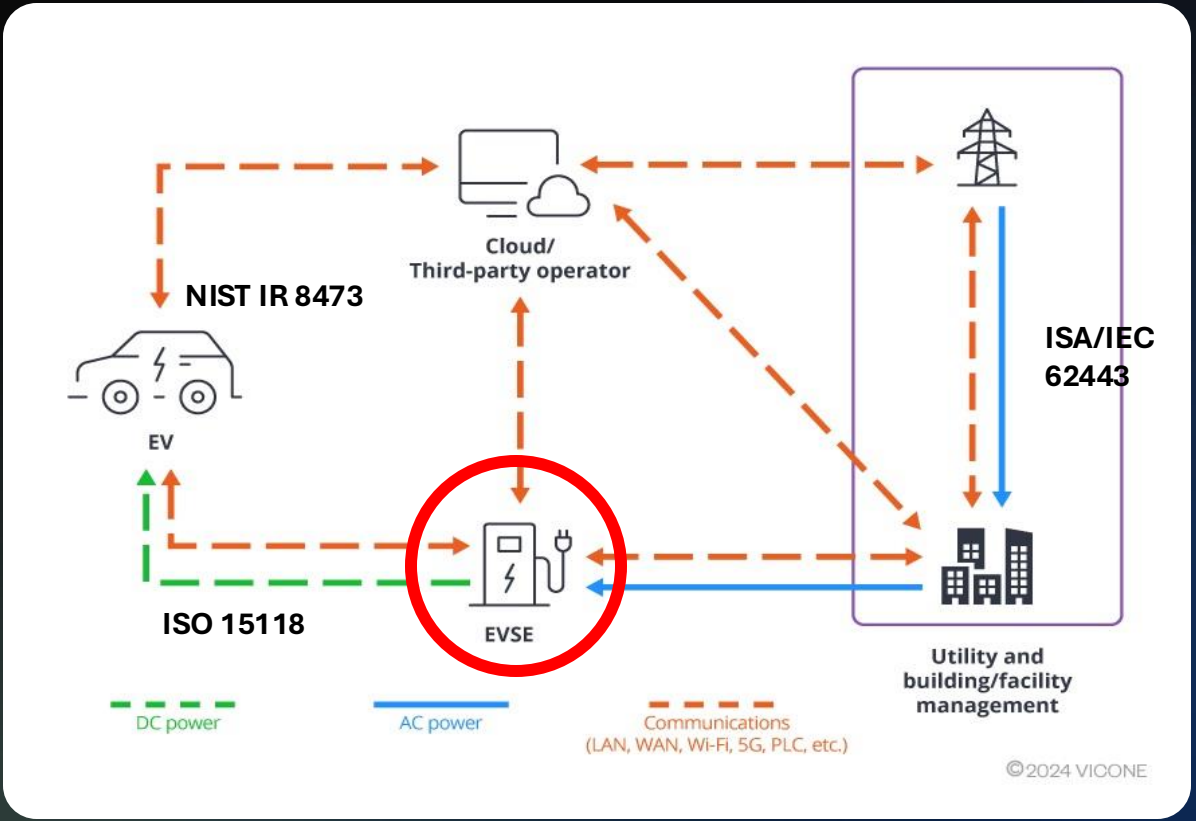
VicOne | ZERO DAY INITIATIVE

PWN2OWN AUTOMOTIVE

Key Finding from Pwn2Own:

- Vulnerabilities were discovered despite standards compliance (e.g. ISO 15118, IEC 62443)
- Security gaps appear due to:
  - Differences in scope between standards
  - Voluntary implementation of controls
  - Inconsistent integration across systems

IT Security Alone Isn't Enough



Compliance with frameworks such as NIST IR 8473, IEC 62443, and ISO 15118 requires a

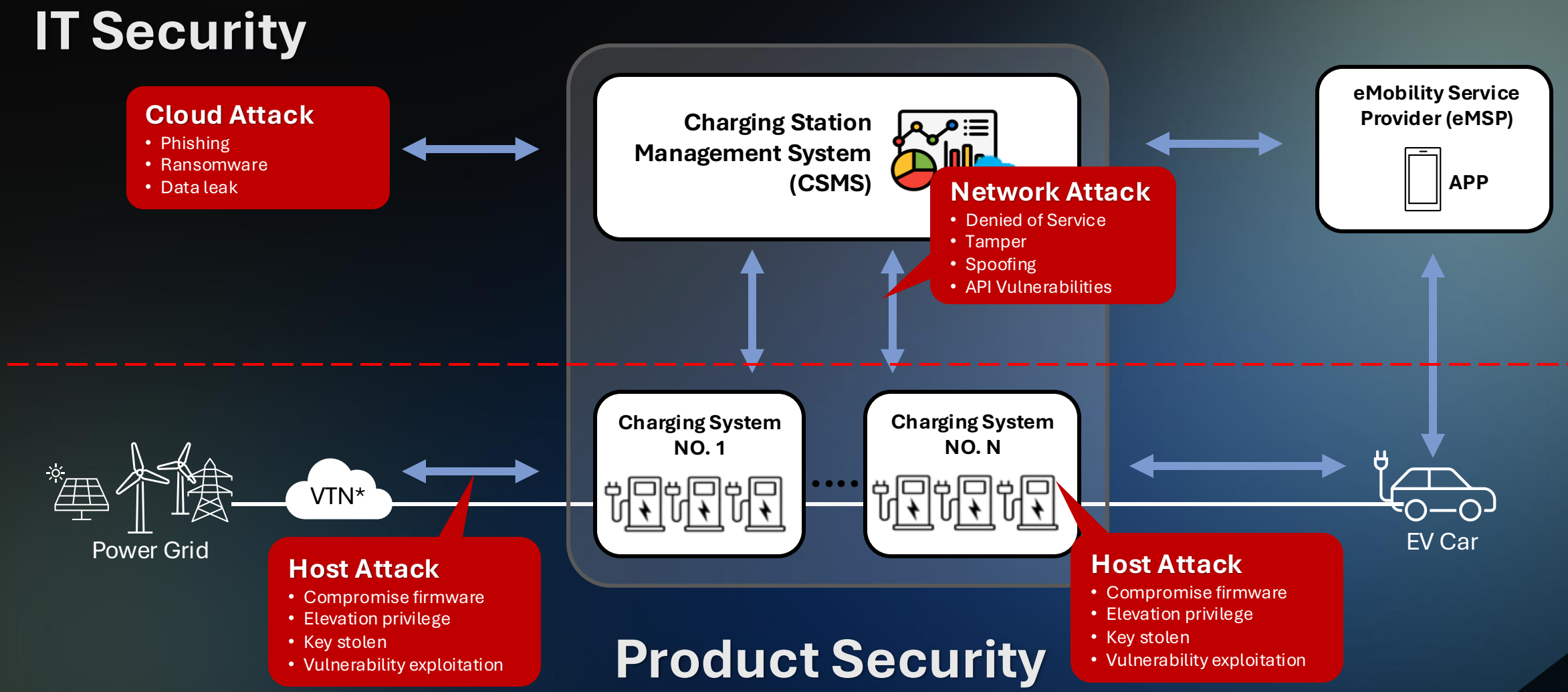
Product-Level Cybersecurity

(SBOMs, vulnerability management, threat intelligence) that IT-only approaches were never designed to deliver.

- **ISA/IEC 62443**: Ensures system-level cyber resilience
- **ISO 15118-20**: Core communication and security standard
- **NIST IR 8473**: Cybersecurity risk management

VicOne

Attack Surface in EVSE



IT Security ≠ Product Security

Traditional IT tools like Rapid7 cannot identify or mitigate EVSE-specific risks (i.e., insecure firmware, EVSE-related protocol vulnerabilities, EV charger firmware vulnerabilities, supply chain risks), leaving critical gaps in compliance and safety.

IT Security

focuses on protecting networks, endpoints, and user access.

IT Security Examples:

- Firewalls, SIEM alerts, and VPNs
- Protecting cloud infra and backend servers

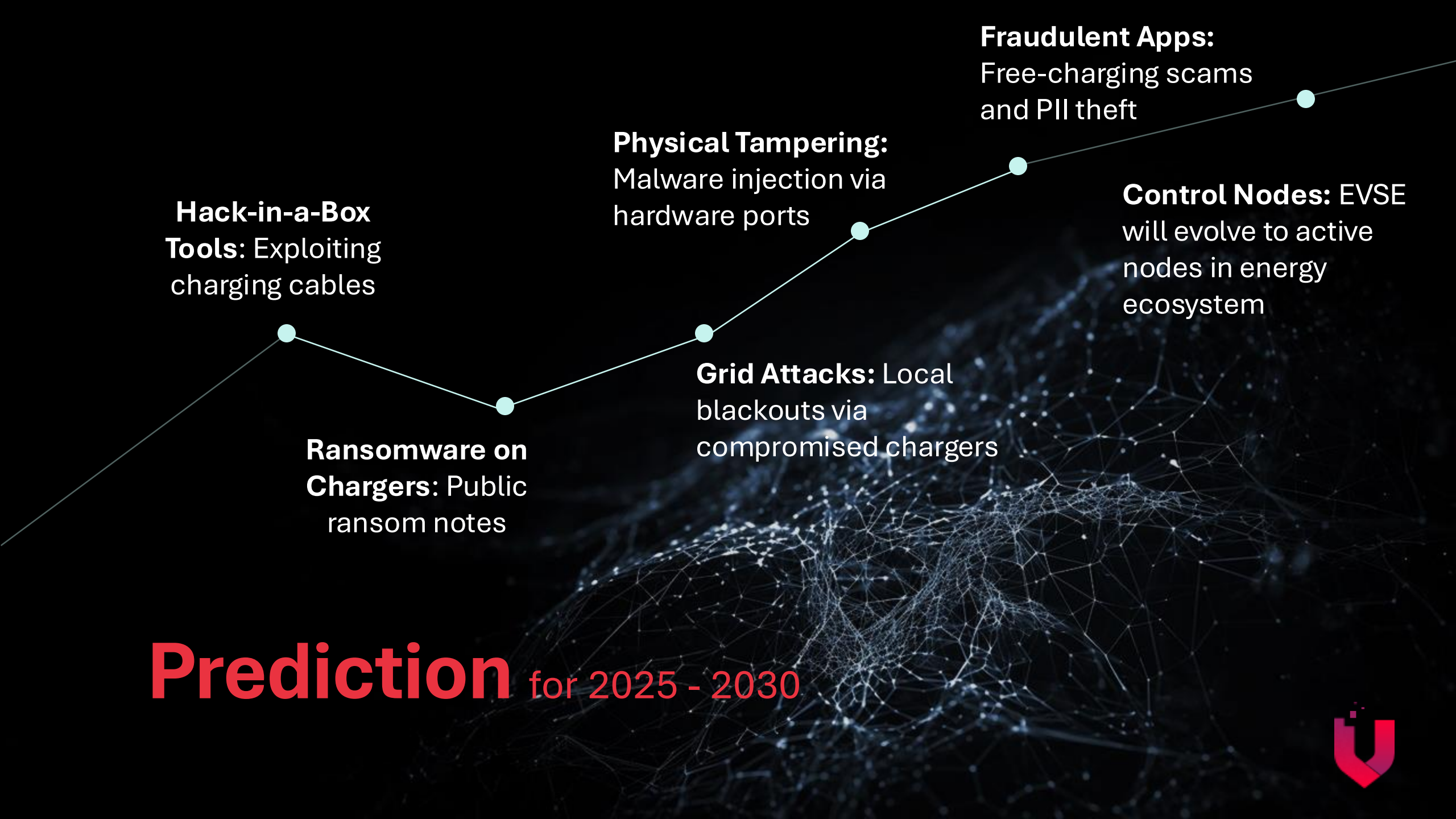
Product Security

ensures that physical systems remain secure throughout their lifecycle.

Product Security Examples:

- Firmware vulnerability discovery and triage
- 3rd party supply chain SBOM/HBOM correlation
- OCPP security event correction
- Host-based IDPS

VicOne


Hack-in-a-Box Tools: Exploiting charging cables
Ransomware on Chargers: Public ransom notes
Physical Tampering: Malware injection via hardware ports
Grid Attacks: Local blackouts via compromised chargers
Fraudulent Apps: Free-charging scams and PII theft
Control Nodes: EVSE will evolve to active nodes in energy ecosystem
Prediction for 2025 - 2030


VicOne
Thank You
Learn more about VicOne
by visiting VicOne.com or
scanning this QR code.
Email: michael_fulgencio@vicone.com