Upstream

LEADING THE CHARGE

Securing EV Charging Stations

Will Cybersecurity Risks Stunt EV Growth?

Electric vehicles (EVs) are a critical pillar of the global automotive revolution we're experiencing today. The precondition for bringing this pipe dream to reality relies on securing charging stations that allow consumers to rapidly charge and go.

Whether found outside homes, shopping centers, or along busy corridors, the 2022 $5 billion investment by the US government[1] in charging capabilities will usher in an era of new EV capabilities, along with long-distance travel, V2X, V2G, and a more sustainable future.

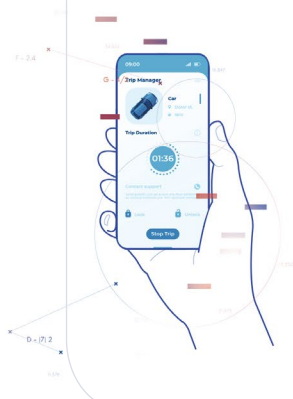
Charging network's wide attack surface

Thousands of charging stations, scattered across the landscape, simultaneously rely on communication between themselves, charging vehicle, local communication networks, electrical infrastructure, and a vehicle owner's mobile device. But, these end points are, at times, lacking the cybersecurity needed to avoid a catastrophic breach.

Charging stations have already been hacked to display lude images[2] and messages[3], showing the capabilities of hackers to penetrate these weakly defended networks. In addition, mobile phone APIs which will be used to verify vehicle to station pairings are a commonly used attack vector, accounting for 7.3% of all automotive cybersecurity incidents since 2010.

7.3%

OF ALL INCIDENTS BETWEEN 2010-2021 INVOLVED A MOBILE APP



Without close and effective monitoring by an OEM's vehicle security operations center (VSOC) of both vehicles and charging stations, the momentum of EV adoption may put hundreds of thousands of users at risk of having personal data and assets compromised.

Glaring cybersecurity gaps

A leading organization showed[4] widespread vulnerabilities in all major charging station brands.

What they found was disregard for best cybersecurity practices. All displayed some level of API authorization override capabilities, allowing for account hijacking, while some did not require any level of authorization upon updating firmware- giving a clear entryway for black-hat actors to install rogue firmware without requiring network approval.

Should this attack be carried out, hackers may be able to inject messages directly into vehicles with no security barriers in place to stop them.

Finally, some charging stations rely on standard off-the-shelf compute modules, making hacking by researchers or black-hat actors feasible without advanced targeted research or knowledge, as a result of online resources that layout known vulnerabilities.

The poor oversight during development has led to dangerous gaps in the global charging stations' cybersecurity posture. Corrupt charging stations across countries or continents can easily infect entire fleets leading to unfathomable dangers.

1 https://highways.dot.gov/newsroom/president-biden-usdot-and-usdoe-announce-5-billion-over-five-years-national-ev-charging
2 https://upstream.auto/research/automotive-cybersecurity/?id=10530
3 https://upstream.auto/research/automotive-cybersecurity/?id=10590
4 https://upstream.auto/research/automotive-cybersecurity/?id=10550

Cyber Risks to Charging Station Adoption

As charging stations continue to roll out across the country, whole industries are relying on their capabilities to drive forward the adoption of an electrified mobility future. OEMs are partnering with charging station suppliers, exposing themselves to third-party vulnerabilities[5], yet putting their own brand reputation on the line.

Beyond risks to OEMs, gaining access to vehicle information exposes users' personal data. Once penetrated, a vehicle can expose location, behavior, and even infotainment system data, giving hackers full access to an individual's personal life.

Ultimately, a hacked device that impacts fleets of vehicles may sew distrust in the EV movement, potentially damaging reputations and electrification adoption.

Fraudulent activity and exposed personal data

One of the biggest draws of EV adoption is the low-cost charging capabilities that owners can utilize while the car is parked at home. At times bundled with the vehicle purchase, these chargers are connected to the home Wi-Fi network, optimizing charging capabilities and giving insights to owners via their mobile devices.

But these same connected features were found to be vulnerable in a leading brand. By exploiting a vulnerability, hackers were able to disconnect a charger from a vehicle, charge their own vehicle, and even remove the owners as authorized users[6], despite it being connected to the owner's home internet network.

In another incident, hackers were able to access a charging station and tamper with data to undercharge or overcharge a vehicle, potentially damaging its battery[7].

Cybersecurity gaps lead to V2G dangers

Some places around the world have begun deploying V2G capabilities, allowing for a bidirectional flow of energy between charging vehicles and power grids. During times of high demand, connected charged vehicles are called upon to put power back into the grid and manage peak surges.

In one incident, a shared Open Chargepoint Protocol (OCPP) was used by a java-based backend server to communicate between charging stations and electric vehicles. The potential risk was revealed upon the discovery of a significant Log4Shell vulnerability, opening the door for a widespread attack that could hit the brakes on the momentum and billions of dollars being invested into vehicle electrification[8].

If these were to be hacked, an attack similar to a DoS attack can occur where thousands of vehicles can either pull or push power into the grid at the same time. Such misuse or manipulation of the protocol would overwhelm the system's hardware, resulting in widespread damage to critical infrastructure.

5 https://upstream.auto/research/automotive-cybersecurity/?id=10600
6 https://upstream.auto/research/automotive-cybersecurity/?id=8780
7 https://upstream.auto/research/automotive-cybersecurity/?id=7570
8 https://energyinformatics.springeropen.com/articles/10.1186/s42162-020-0103-1

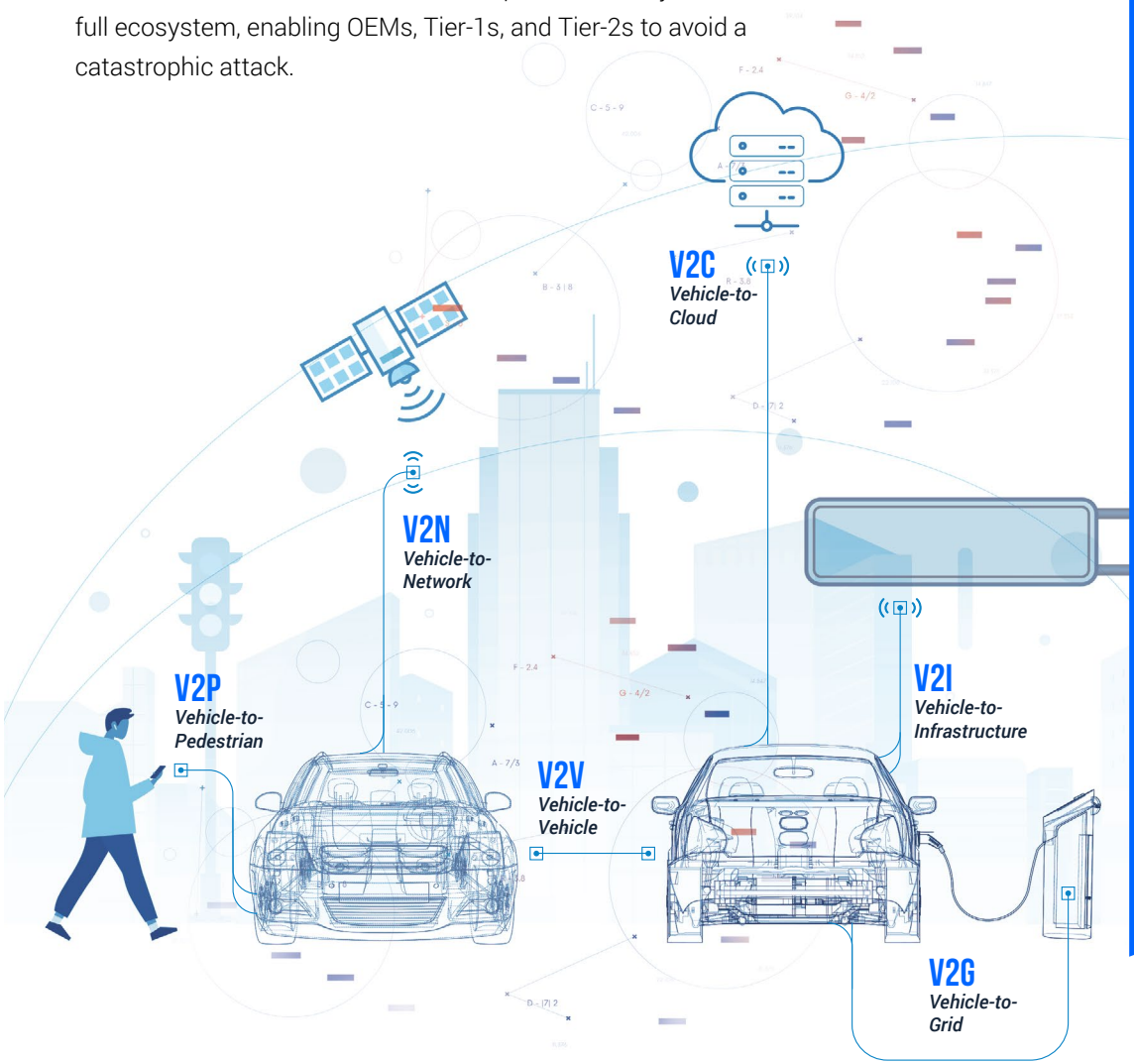
Each charging station provides potential network access to all affiliated stations, making their exposed nature in parking lots or next to homes an easy target for black-hat operators to conduct a close range or physical attack.

Securing them relies on cloud-based monitoring from a central vehicle-specific security operations center (VSOC) that can contextualize data to identify individual, regional, or widespread anomalies.

Unifying cybersecurity standards for V2X adoption

As we increasingly connect our in-vehicle data with charging stations, and smart traffic infrastructure, a vulnerability in one protocol, such as OCPP, can create major problems across a city or nation's transportation grid. This becomes alarming when considering the deployment of autonomous vehicles, which are designed to operate with little or no intervention by an in-vehicle driver. Once an attack spreads from one part of the network to another, it will be the responsibility of OEMs to secure vehicles, charging stations, and any other assets in the impacted sector.

Relying on cybersecurity interoperability through cloud-based communication will allow for better response times by the full ecosystem, enabling OEMs, Tier-1s, and Tier-2s to avoid a catastrophic attack.



Charging Stations and the Demand for 24/7 Holistic Protection

Upstream delivers unparalleled cloud-based cybersecurity with automotive expertise across the rapidly expanding charging station domain.

This holistic asset-first approach protects charging stations by:

- **Securing charging station assets**
  Upstream's agentless and cost-effective solution provides the most comprehensive cybersecurity protection across the entire connected charging station ecosystem, protecting vehicles with zero disruption to charging cycles.
- **Mitigating against known and unknown cyber threats**
  Analyzing both charging station and vehicle data, Upstream's AI-powered cyber threat detection capabilities recognize anomalous behaviors based on contextualized data and a cloud-based virtual representation of each charging station as well as the full network (digital twins).
- **Immediate and effective response**
  Seamless integration to third-party SOC and VSOC solutions such as SIEM, SOAR, and others means your team can execute the best response upon the first signs of a breach.
- **Protecting your brand**
  Maintain brand reputation against potentially damaging current and future cyber attacks.

  As the EV and charging stations are going through a rapid evolution, The Upstream Platform provides the most advanced threat detection, based on first and third-party data.

Upstream VSOC services

Real-time 24/7 monitoring of vehicles and charging stations for complete fraud and security protection throughout their full lifecycle.

- **Domain oversight** to incorporate new threats from AutoThreat® PRO, The Upstream Platform, and emerging insights from the field.
- **AI-based risk detection** with automated workflows, triaging, and incident auto-escalation, reducing false positives and allowing teams to secure chargers around the clock.
- **Machine Learning** profiling for early detection and rapid response.

AutoThreat® PRO

The first and only threat intelligence service, purpose-built for the automotive ecosystem to secure both vehicles and the charging stations they engage with.

- **Supply chain insights and regulatory compliance**
  Component-level mapping to vehicle models and customized tracking based on a product's bill of materials. Remain compliant while ensuring the use of only secure components.
- **Deep and dark web monitoring and threat hunting**
  Beyond publicly reported incidents, AutoThreat® PRO also monitors sentiments to detect early signs of intended exploits and tracks incidents found throughout the deep and dark web, including private forums, marketplaces, and social network channels.
- **Custom reporting**
  Create customized threat reports that can be used for organizational threat awareness or internal risk funding proposals.

About Upstream

Upstream Security offers a cloud-based automotive cybersecurity and data analytics platform purpose-built for connected vehicles and smart mobility services. Upstream's platform fuses machine learning, data normalization, and digital twin profiling technologies to detect anomalies in real-time using existing automotive data feeds. Coupled with AutoThreat® Intelligence, the first automotive cybersecurity threat intelligence feed, Upstream provides unparalleled cybersecurity and data-driven insights, seamlessly integrated into the customer's environment.

Upstream is privately funded by Alliance Ventures (Renault, Nissan, Mitsubishi), Volvo Group, BMW, Hyundai, MSI Insurance, Nationwide Insurance, Salesforce Ventures, CRV, Glilot Capital Partners, and Maniv Mobility.

For more information

Visit us at:
www.upstream.auto

Contact us:
hello@upstream.auto

Follow us: