digicert®

POWERING PROGRESS IN EV CHARGING

Addressing Cybersecurity Risks, Ensuring Compliance and Driving Adoption

The global push toward electric vehicles (EVs) is accelerating, driven by the urgent need to reduce carbon emissions and combat climate change. This shift towards electrification underscores the critical role of establishing a secure and reliable EV charging infrastructure to support the growing number of EVs on the road. Stakeholders across the sector, including automotive manufacturers, charge point developers, grid operators, city planners, and policymakers are actively involved in developing a robust electrical infrastructure and charging points to meet the demands of a new generation of electric vehicles. However, as the EV charging ecosystem expands, it becomes a prime target for cyber threats and faces challenges that hinder consumer adoption.

EV CHARGING HAS A RELIABILITY PROBLEM

One of the key challenges faced is range anxiety, which refers to the fear that an EV may not have enough battery range to reach its destination. This concern is exacerbated by the perceived inadequacy of the current charging infrastructure, leading potential EV owners to worry about being stranded without access to a charging station. Moreover, the EV market lacks standardization across different charge point operators (CPOs), leading to confusion among consumers about the interoperability of charging stations with different EV models.

digicert®

HOW CONSUMERS GAUGE EV RISKS

From fear of being marooned without a charge to cybersecurity threats, consumers have considered the security implications of their high-tech electric vehicles. In a study by Deloitte, **53%** of consumers reported their concern about EV security.[1] And it's not just EV skeptics. **64%** of drivers who already own an EV have expressed concern about the security of public charging stations.[2] In the high-visibility industry, consumers have a high awareness of the rewards – and the risks – of electric vehicles. Their fears are not unfounded. Market Scoop reports that the automotive industry has experienced a **225%** increase in cyberattacks over the last **three years**.[3]

To address these challenges, stakeholders must work together to enhance the cybersecurity of the EV charging ecosystem and improve the infrastructure's accessibility and user-friendliness. This includes standardizing charging protocols and connectors, increasing the density and visibility of charging stations, and providing clear, user-friendly

53%

of consumers reported their concern about EV security

64%

of drivers who already own an EV have expressed concern about the security of public charging stations

The automotive industry has experienced a

225%

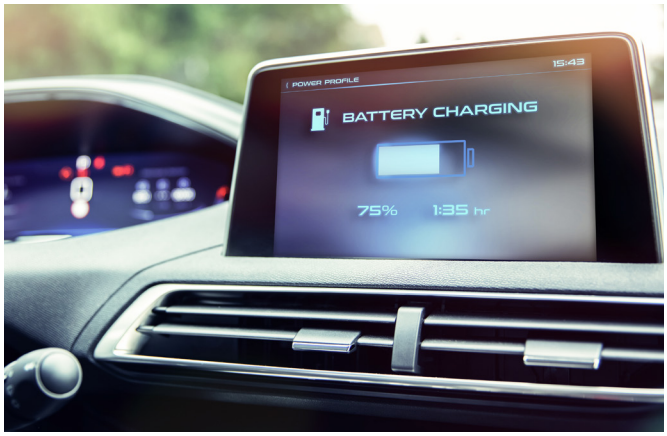
increase in cyberattacks over the last **THREE YEARS**

[1] https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-affordability-concerns-slow-the-road-to-an-electrified-future.html
[2] Ponemon Institute, "Securing the EV Infrastructure: A Survey of Electric Vehicle Drivers in the United States"
[3] https://scoop.market.us/automotive-cyber-security-rises-the-autonomous-driving-technology

information to consumers about how to charge their vehicles at different stations.

To make owning an EV more attractive and accelerate the transition to a sustainable and electrified transportation system, the industry must prioritize addressing these top cybersecurity risks:

1. Unauthorized Access: Cyber attackers could gain unauthorized access to EV charging systems, enabling them to manipulate charging processes or access sensitive data.
2. Data Breaches: Personal and payment information of EV owners could be exposed, leading to privacy violations and financial fraud.
3. Denial of Service (DoS) Attacks: Attackers could disrupt the availability of charging services, causing inconvenience to users and potential damage to the EV charging infrastructure.
4. Firmware Tampering: Malicious firmware updates could compromise the functionality of charging stations or even EVs themselves.
5. Man-in-the-Middle (MitM) Attacks: Attackers could intercept communications between EVs and charging stations to steal data or inject malicious commands.



MEASURES TO MITIGATE RISKS: OCPP 2.0.1. AND ISO 15118-2

Open-source communication standards address the cybersecurity risks that stoke fear in consumers and impede EV adoption.

Secure Communications Across the Charging Network

- OCPP 2.0.1 significantly bolsters the EV charging infrastructure against cyber threats by implementing advanced authentication mechanisms and secure firmware updates, markedly reducing the risk of unauthorized access and data breaches. It introduces new security profiles and functionalities, such as improved authentication mechanisms and secure firmware updates. Additionally, OCPP 2.1 mandates the implementation of TLS 1.3 and mutual authentication with both server-side and client-side certificates.

Secure Communications between EVs and Chargers

- ISO 15118-2 focuses on secure communication between EVs and charging stations. It supports the Plug & Charge feature, enabling automatic and secure authentication and billing without manual user intervention. ISO 15118-2 utilizes Transport Layer Security (TLS) for encrypted communications, protecting against Man in the Middle (MitM) attacks. It also mandates using compliant certificates for authentication, ensuring that only authorized devices and users can access the charging services.

By adhering to these standards, EV and EVSE OEMs, charge point operators, and mobility operators can significantly enhance the security of the EV charging ecosystem. Implementing TLS using ISO 15118-2 compliant certificates ensures that data exchanged between EVs and charging stations is encrypted, safeguarding against eavesdropping and data breaches. Additionally, the advanced security features of OCPP 2.0.1 help prevent unauthorized access and DoS attacks, ensuring the integrity of firmware updates. Adoption OCPP 2.0.1 and ISO 15118-2 standards is essential for mitigating cybersecurity risks in the EV charging ecosystem, providing a robust framework for secure communication, authentication, and data protection. This enhances the overall security posture of EV charging infrastructure and promotes the widespread adoption of electric vehicles.

SECURING THE EV CHARGING ECOSYSTEM: MOVING FORWARD WITH CONFIDENCE

To effectively address the extensive cybersecurity challenges in the EV industry, DigiCert offers critical solutions that enhance device trust and compliance with ISO 15118-2 standards. Our Device Trust Manager in tandem with TrustCore SDK, compliant with FIPS 140-3, is a vital embedded software security development tool. They enable Original Equipment Manufacturers (OEMs) and Charge Point Operators (CPOs) to rapidly enhance the security of their devices and networks.

Device Trust Manager simplifies the management of device identities and credentials, ensuring that each component within the EV charging ecosystem is adequately authenticated and trusted. Meanwhile, TrustCore SDK provides a robust suite of security features that meet the stringent requirements of FIPS 140-3, offering a secure foundation for device software development.

By integrating these tools, OEMs of EVs, EV chargepoints and chargepoint operators (CPOs) can ensure secure communication between EVs and charging stations, encrypted data exchanges, and access control, mitigating risks such as unauthorized access and cyber-attacks. DigiCert's comprehensive solutions address current cybersecurity concerns and support the development of a secure, scalable, and interoperable EV infrastructure. Addressing problems today – with an eye to the challenges of the future - is how we build consumer trust and facilitate the widespread adoption of electric vehicles.

DigiCert secures the digital integrity of 83% of global automotive giants, providing robust cybersecurity solutions that safeguard sensitive data and ensure the reliability of various automotive services. Our expertise ensures that our solutions not only meet the specific needs of EV manufacturers and charging infrastructure providers but also align with the broader automotive security landscape, further enhancing the security and reliability of EV charging systems. Since 2018, DigiCert has been actively working with SAE ITC and the EV PKI (Public Key Infrastructure) community to develop the certificate policy (CP) to realize and robustly implement the ISO 15118-2 standard. In collaboration with ChargePoint and Eonti, DigiCert jointly produced a whitepaper outlining areas where the standard didn't fully address security, interoperability, scalability, and lacked appropriate governance policies and controls This pivotal research led to the SAE's decision to convene the latest EV PKI consortium, which ultimately awarded DigiCert the contract to develop the Certificate Trust List (CTL). This CTL aims to instantiate a comprehensive certificate policy (CP), directly addressing some of the critical challenges previously unmet by the standard. DigiCert's leadership and insight have thus become instrumental in driving the enhancements necessary for a secure, interoperable, and scalable EV charging ecosystem, marking a major stride towards establishing digital trust in the real world of electric vehicle infrastructure.

CHARGING THE FUTURE: SUMMARY AND PATH FORWARD

The electric vehicle (EV) industry stands at a critical juncture: while it offers a transformative solution proven to mitigate global carbon emissions and combat climate change, its widespread adoption is hindered by consumer apprehensions, many of which stem from existing cybersecurity vulnerabilities. These risks not only threaten the integrity of the EV ecosystem but also fuel the concerns that challenge the industry's growth. Addressing these vulnerabilities with a reliable and comprehensive cybersecurity solution is therefore not just imperative for safeguarding the digital infrastructure of EVs; it's a critical step towards building consumer trust, ensuring the seamless integration of electric vehicles into our daily lives, and ultimately, securing the future of sustainable transportation.

A multifaceted approach that combines technological innovation with strategic policy and infrastructure development is required to push EV transformation forward. Industry adoption of standards like OCPP 2.1 and ISO 15118-2, along with the integration of DigiCert's Device Trust Manager and TrustCore SDK, can secure the EV charging ecosystem against cyber threats. These measures not only enhance the security and reliability of EV charging but also bolster consumer confidence in electric vehicles as a viable and sustainable mode of transportation.

To accelerate the transition to electric vehicles, a strategic alliance among automakers, charge point developers, and technology firms is crucial, paving the way for a secure, efficient, and universally accessible EV charging network. This collaborative effort will result in a secure, accessible, and user-friendly charging infrastructure that meets the needs of current and future EV owners.

500 MILLION

EVs by 2030

By 2030, with an anticipated surge to over 500 million electric vehicles on our roads,[4] the imperative for a vast and fortified charging infrastructure is clear. As the industry continues to evolve and innovate, our vision for a fully electrified transportation ecosystem draws closer to reality. Addressing cybersecurity risks and alleviating consumer concerns are pivotal steps in this journey, enabling us to expedite the shift towards electric vehicles. This transition holds the promise of a significant reduction in global carbon emissions, positioning the EV industry at the forefront of a sustainable, electrified future. By embedding digital trust into the very fabric of our infrastructure, we not only secure the path to electrification but also anchor our commitment to the planet. That's digital trust for the real world, powering our drive towards a greener, more secure future.

THE DIGICERT DIFFERENCE

Partner with DigiCert for a security foundation that enhances your device initiatives. Contact us at digicert.com/contact-us to learn how our security not only ensures compliance but also leads to innovation in EV charging.

[4] https://www.iea.org/reports/by-2030-evs-represent-more-than-60-of-vehicles-sold-globally-and-require-an-adequate-surge-in-chargers-installed-in-buildings