Zero Trust, Quantum-Safe, EVCI Network with Reduced Attack Surface

Patero Cybersecurity for Electric Vehicle Charging Infrastructure (EVCI)

By Crick Waters

Key takeaways:

> Up to 1,200,000 U.S. public electric vehicle (EV) charging stations are needed by 2030

> EV charging infrastructure (EVCI) will become a critical component of U.S. infrastructure

> EVCI cybersecurity is weak today and inadequate against future quantum computer attacks.

The Good News & The Bad News

Six short years from now, between 30-42 million light-duty electric vehicles (EVs) will be operating on U.S. roads.[1] A massive public charging station infrastructure deployment is required to accommodate the electrification of America and this transition to EVs. The Infrastructure Investment and Jobs Act provided $7.5B to build an EV charging infrastructure (EVCI) of 500,000 public charging stations...[2]. Still, McKinsey estimates that as much as fifty percent of vehicles sold in America by 2030 will be EVs. In that scenario, an estimated 1.2 million public EV chargers will be required.[3]

While much focus and funding are necessary to fuel the transition to electric vehicles and their respective EVCI, less emphasis is placed on the fact that the infrastructure to deliver energy and store it in 42 million vehicles over a grid of 1.2 million public EV charging stations will become a "National energy storage asset" — a *critical* National asset that will be a lightning rod for cybercriminals and cyberterrorists — that must be protected against cyber terrorists.

[1] "Building the 2030 National Charging Network". Www.Nrel.Gov, 2024, https://www.nrel.gov/news/program/2023/building-the-2030-national-charging-network.html. Accessed 4 Feb 2024.
[2] "Building the electric-vehicle charging infrastructure America needs". Www.Mckinsey.Com, 2024, https://www.mckinsey.com/industries/public-sector/our-insights/building-the-electric-vehicle-charging-infrastructure-america-needs. Accessed 4 Feb 2024.
[3] Ibid.

Numerous government and private studies have been conducted, and much has been written about cybersecurity weaknesses in EVCI. These studies have focused on security flaws without considering that today's cybersecurity encryption technology is at risk from future quantum computer attacks. Kern et al. noted that "no related work focuses on post-quantum cryptography (PQC) in EV charging protocols."[4]

The Executive Branch promulgated specific guidelines and responsibilities for transitioning to post-quantum cryptography (PQC) as a national imperative by issuing a National Security Memorandum (NSM 10) on May 04, 2022. NSM 10 noted that quantum computers could jeopardize civilian communications and undermine supervisory and control systems for critical infrastructure.[5] Subsequently, the National Security Agency issued a timeline for the transition to PQC with Commercial National Security Algorithm Suite 2.0, stating that traditional networking equipment (e.g., virtual private networks, routers - the components used to form the EVCI) support PQC security by 2026 and exclusively PQC security by 2030.[6]

The primary threat of cryptographically relevant quantum computers (CRQC) is from China, which is preparing to "'wreak havoc' on US critical infrastructure," according to FBI Director Christopher Wray on January 31, 2024.[7] China has committed $15.3B to develop quantum computers, eight times that of the U.S. commitment[8] — and it is no secret that Chinese researchers are working to develop methods of cracking classic encryption with quantum computers, as evidenced in a publication by Chinese researchers in December 2022 relating their work to develop techniques for breaking classic RSA-2048 encryption with quantum computers of the size commercially available from IBM today.[9]

---

[4] "QuantumCharge: Post-Quantum Cryptography for Electric Vehicle Charging". Applied Cryptography and Network Security: 21st International Conference, ACNS 2023, Kyoto, Japan, June 19–22, 2023, Proceedings, Part II, Jun 2023, Pages 85–111, https://doi.org/10.1007/978-3-031-33491-7_4

[5] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems". Www.Whitehouse.Gov, 2024, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/. Accessed 4 Feb 2024.

[6] "Commercial National Security Algorithm Suite 2.0". Media.Defense.Gov, 2024, https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF. Accessed 4 Feb 2024.

[7] "Wray warns Chinese hackers are aiming to 'wreak havoc' on U.S. critical infrastructure". Www.Npr.Org, 2024, https://www.npr.org/2024/01/31/1228153857/wray-chinese-hackers-national-security. Accessed 4 Feb 2024.

[8] "Quantum computing funding remains strong, but talent gap raises concern". Www.Mckinsey.Com, 2024, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern. Accessed 4 Feb 2024.

[9] "Factoring integers with sublinear resources on a superconducting quantum processor". Arxiv.Org, 2024, https://arxiv.org/pdf/2212.12372.pdf. Accessed 4 Feb 2024.

The Technical Problem

In July 2022, Sandia, Pacific Northwest, and Argonne National Laboratories published "Cybersecurity for Electric Vehicle Charging Infrastructure," reporting a "technical analysis of the risk landscape presented by the anticipated massive deployment of interoperable EV chargers."[10] The authors identified gaping holes in EVCI security:

- Electric vehicle supply equipment (EVSE) networks (internal and external) do not follow network security best practices.
    - Networks (external to the EVSEs) were not segmented, used VPNs, or did not include protection devices such as intrusion detection systems (IDS) or firewalls.
    - An attacker would gain access to the entire EVSE network without detection by compromising a single EVSE.

- Insecure remote access tools are used to configure and troubleshoot deployed EVSE.
    - Remote access tools for managing EVSEs were communicating on unencrypted networks. Some tools provided complete control of the charging network.

- EVSEs are Internet-connected and discoverable by IP search engines such as Shodan.
    - Discoverability and lack of encryption and protection mean cyber attackers can take complete control of a charging network with existing exploit tools.

- EVSEs use outdated and insecure protocol versions.
    - EVSEs connect to the Internet using insecure and outdated protocols such as Open Charge Point Protocol (OCPP). 1.6 and MQTT.
    - Remote attackers can, therefore, mount assaults on charging networks through known protocol security weaknesses.

Sandia also notes that even the most current EVCI communication protocol promulgates public key cryptography that is obsolete in the face of quantum computers. A sufficiently powerful quantum computer can break traditional public key encryption using Shor's algorithm. For this reason, the U.S. Government has embarked on an effort (a) to identify ciphers resistant to classic and quantum computer attacks (led by the National Institute of Standards and Technologies (NIST)) and (b) to direct U.S. agencies to migrate vulnerable computer systems to quantum-resistant cryptography (via NSM 10).

Current methods used to address the problem

Open Charge Point Protocol (OCPP) specifies the communication protocol between electric vehicle supply equipment (EVSE) and the often cloud-based charging station management system (CSMS). OCCP v1.6 allows transport layer security (TLS) 1.2 or higher. Cristina Alcaraz

[10] "Cybersecurity for Electric Vehicle Charging Infrastructure". Www.Osti.Gov, 2024, https://www.osti.gov/servlets/purl/1877784. Accessed 5 Feb 2024.

et al. note that TLS 1.3, specified in OCCP 2.0.1, includes new security measures at the device and communication level to mitigate the security issues identified in OCCP 1.6.[11]

The use of TLS for securing communication between EVSEs and cloud CSMSs is vulnerable to discovery and attack. As previously noted, attackers, using freely available tools, quickly discover communication network endpoints. Cloud CSMSs using TLS for security are necessarily responsive to search tools like Shodan. Sandia used such an attack in a real-world scenario, quickly identifying and penetrating an EVSE through its Wi-Fi network connection.[12]

The use of TLS, by default, creates an exploitable EVCI attack surface.

A more secure network approach reduces the EVCI attack surface by cloaking network endpoints from discovery and exploitation by attackers.

The use of TLS is also subject to attack by future CRQCs. Because the expected lifespan of EVCI networks is longer than the timeframe before nation-states or cyber terrorists are expected to have access to CRQCs, post-quantum cryptography must be incorporated into EVCIs' security.

Sandia National Labs argues with respect to ISO 15118, *Road Vehicles – Vehicle to Grid Communication* Interface, that "the primary weakness in defining specific hash algorithms, signature algorithms, and protocols for use in the ecosystem is preventing crypto-agility in the future." They further argue that "crypto-agility," the capacity to switch to alternate cryptographic primitives without inducing significant system changes, is seen as an imperative to prepare for the coming quantum computing era."[13]

Patero's Technical Approach

"Attack surface expansion" was the top security risk to organizations named by Gartner in 2022:

> "Enterprise attack surfaces are expanding. Risks associated with using cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media, and more have brought organizations' exposed surfaces outside of a set of controllable assets."[14]

---

[11] "OCPP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0". Link.Springer.Com, 2024, https://link.springer.com/article/10.1007/s10207-023-00698-8. Accessed 6 Feb 2024.

[12] Sandia et al., 29.

[13] "Cybersecurity for Electric Vehicle Charging Infrastructure". 2024. Www.Osti.Gov. https://www.osti.gov/servlets/purl/1877784. 22, 25.

[14] Gartner, Inc. (2022, March 7). *Gartner Identifies Top Security and Risk Management Trends for 2022*. Gartner Newsroom. Retrieved May 22, 2023, from https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

In its March 2023 National Cybersecurity Memorandum, the White House stated:

> "Quantum computing has the potential to break some of the most ubiquitous encryption standards deployed today. We must prioritize and accelerate investments in the widespread replacement of hardware, software, and services that can be easily compromised by quantum computers so that information is protected against future attacks."[15]

As data communication networks have grown, network entry points inside and outside enterprise perimeters have exploded. Data transiting these networks encrypted with classical cryptosystems, including Rivest Shamir-Adleman (RSA), Elliptical Curve Cryptography (ECC), and Diffie-Hellman, are at risk of being compromised by quantum computers.

Patero has developed a network security solution that reduces the exposed attack surface while encrypting data-in-motion with hybrid post-quantum encryption (hybrid-PQC). Patero's hybrid-PQC solution enhances classical cryptosystems with quantum-resistant encryption algorithms selected by the National Institute of Standards and Technology (NIST). The solution reduces the network's exposed attack surface and supplements classical encryption key material with quantum-resistant key material, creating a superior cipher to thwart quantum-enabled attackers.

Distributed Networks

The proliferation of distributed network endpoints, including IoT devices and components of critical infrastructure, has significantly increased the attack surface of data networks across the National Critical Function sectors, making them susceptible to cyber-attacks – providing a point of entry for attackers to gain access to other devices on the network.

Nation-state cyber-attacks are becoming increasingly common and sophisticated. Highly skilled and well-funded teams often carry out these attacks, making them difficult to detect and defend against. The vast increase expected in EVCI charging stations will result in a huge increase in network endpoints, giving these attackers a gigantic attack surface.

Solution Description

Patero reduces the attack surface of distributed networks by collapsing network layers into quantum-safe, trusted channels and moving authentication to network endpoints. This enables zero-trust networking and eliminates the trust broker as an attack vector.

Building a zero trust architecture is a valuable and essential step, but zero trust architectures usually depend on a "trust broker" to moderate network communications through centralized authentication at the initiation of every session. The centralized trust broker must be available to

[15] See National Cybersecurity Strategy, page 25. The White House (March 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

all network endpoints BEFORE authentication and is itself, therefore, exposed to cyber-attacks. A successful attack would expose all connected networks."

The Patero network is a new approach to network security. It shifts the security paradigm from one centered around implementing myriad "access control" methods to one focused on collapsing the network attack surface by cloaking information channels. This shift reduces the network's attack surface while simplifying network management.
Patero implements multiple independent key-validation mechanisms under different protocols for endpoint identity authentication. Each endpoint must be authenticated by other endpoints, which is the first step toward establishing a trusted communication channel.

Endpoint Authentication

Patero establishes initial trust for every endpoint's communication channel to a central communication gateway during deployment by creating a unique classical and a post-quantum public-private key pair and then exchanging the public keys between the endpoints. These keys are required to initiate the communication and to negotiate further endpoint authentication. They are regenerated and replaced upon first contact to invalidate all key material that may become available to 3rd parties during or after deployment.

In addition, Patero uses both a post-quantum and traditional key exchange to create and renew a hybrid quantum-safe session key every 120 seconds with cascading X25519 and Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) secrets through a key derivation function. This session key is then used for message encryption and authentication by symmetric encryption using ChaCha20-Poly1305 with authenticated encryption with associated data (AEAD).

Further continuous endpoint validation based on endpoint characteristics like device serial number and endpoint certificates (e.g. stored on the device's trusted platform module (TPM) chip) can be established to verify and monitor endpoint and prevent attackers from connecting by cloning an endpoint's firmware and encryption keys.

Any requests without correct authentication credentials are ignored, and the incoming packets are dropped. The endpoint behaves like a black hole to an attacker and does not respond to unauthenticated endpoints. Endpoints are effectively unresponsive to attackers.

Post Quantum Encryption

Patero's networking technology uses a hybrid-PQC approach. NIST SP 800-56C REV. 2[16] includes a "hybrid" key generation approach. A hybrid approach provides a low-risk, cost-effective "migration path" path from pre- to post-quantum encryption. A hybrid approach also

[16] National Institute of Standards and Technology (2020, August) *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*. (U.S. Department of Commerce, Washington, DC), NIST Special Publication 800-56C Revision 2.

retains traditional encryption protection, ensuring compliance with Cybersecurity and Infrastructure Security Agency (CISA) best practices and affording industrial control systems (ICS) operators the most robust encryption possible.

A hybrid-PQC approach combines "classical" key encapsulation with "quantum-resistant" key encapsulation from a NIST-selected quantum-resistant algorithm. Patero's hybrid PQC solution is software and requires no new hardware. Patero's solution can also use entropy created by quantum random number generating (QRNG) or quantum key distribution (QKD) technologies.

Attack Surface Reduction

An objective of Patero's solution is to reduce the possible attack vectors that are entry points on network attack surfaces. Detectable entry points create attack vectors. The Patero solution is designed to make network endpoints undetectable, thus reducing the attack surface.

Patero-equipped endpoints will only respond to certified endpoints with known Patero-provided quantum resilient key material. No protocol negotiation mechanism is used, as is frequently seen in networks with TLS and other protocols that can be used as an attack vector.

For edge-to-cloud deployments typical of EVCI networks, the edge endpoint's incoming firewall ports (e.g., at the EV charger) can be closed with the Patero solution. This makes it possible to deploy the edge endpoint so that only outgoing traffic is allowed and allowed only to specific IP addresses. The quantum-safe communication channel is established (and continuously re-established in case of connectivity loss) using only the outgoing traffic to the cloud gateways. Once established, data can flow bi-directionally inside the quantum-safe channel according to the internal firewall, specific routing, and "crypto routing" enforced by the encryption module.

Patero cloud gateways' incoming firewall ports are open to incoming edge gateway connections. Incoming cloud traffic can be filtered and protected more efficiently by cloud-based security measures and denial-of-service (DoS) tools than at the edge. The attack surface is obscured once a quantum-safe channel is created between edge and cloud endpoints. An attacker cannot discern services or protocols used inside the Patero-protected channels.

Cryptographic Agility

Both NIST and the Agence nationale de la sécurité des systèmes d'information (ANSSI) state that the resilience of PQC algorithms against a quantum computer or hybrid quantum-classic computer attack cannot be known a priori. NIST started a competitive standardization process in December 2016 to identify algorithms that are most likely able to resist quantum attacks.

Patero CryptoQoR™ crypto module is crypto agile. It supports multiple NIST candidate PQC algorithms, allowing for selecting user-preferred algorithms (depending on the level of cryptographic security desired) and in situ addition or replacement of quantum-resistant algorithms without product recall, equipment replacement, or network interruption.

Performance

Patero's solution is highly optimized code that leverages kernel space modules of the operating system of physical and virtual gateways with minimal overhead. Patero's CryptoQoR typically operates in the sub-millisecond range using a stream cipher optimized for minimum latency at high throughput rates in challenging network environments.

Resiliency

Patero's CryptoQoR endpoint authentication and retry features provide exceptional resiliency. Real-world data traffic can move various network types from copper to glass, radio satellites, and free space optics. Network conditions, hops, and transit lengths can introduce intermittent latency excursions of hundreds of milliseconds. Patero has been field-proven, employing multiple network types to be resilient to 1-sec latencies - ensuring reliable communication even on degraded networks over long distances. An optional backup connection from EV chargers can be supported for high availability through mobile networks or satellite uplinks to maintain connectivity in case of an external network failure.

Monitoring and Management

Patero's central management system, Qorsight, monitors endpoint performance characteristics and manages endpoint connectivity. Future editions of Qorsight will be enhanced with intrusion detection. Industry protocols and communication characteristics will be reliably distinguished from attack attempts inside the quantum-safe data channels. Further enhancements will detect and mitigate physically compromised edge network endpoints or EV chargers.

Anticipated Public Benefits

Patero's solution substantially benefits applications across the sixteen national critical infrastructure sectors[17] and industrial IoT markets. A variant of the solution is being commercialized now for robotic manufacturing to cloak cloud services from cyber criminals and to secure edge-to-cloud manufacturing data streams with future-safe cryptology.

Technical, Economic, and Social Benefits

As identified by Gartner, "attack surface expansion" was the top security risk to organizations in 2022.[18] The expansion of the national EV charging infrastructure will contribute to the attack surface of the U.S. transportation infrastructure. Patero's proposed solution reduces the attack surface through cloaking, serving the social good and our collective national security mission.

---

[17] "Critical Infrastructure Sectors". 2024. www.Cisa.Gov. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[18] Gartner, Inc. (2022, March 7). *Gartner Identifies Top Security and Risk Management Trends for 2022*. Gartner Newsroom. Retrieved May 22, 2023, from https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

Patero's hybrid post-quantum encryption technology is foundational to the national migration from public key infrastructure to a quantum-safe communication infrastructure. PQC-enabled encryption and endpoint cloaking zero trust architectures in EVCI data architectures will benefit the public by hardening this national infrastructure against cyber-attacks.

The Resulting Product

The solution architecture includes defined technical components of a PQC-hardened, zero trust data communications architecture for EVCIs. As Patero continues its roadmap execution, ICS operators will enjoy a suite of software components and a deployment system that EVCI providers can adopt to reduce the probability of network endpoint detection by remote cyber criminals or terrorists, prevent MiTM attacks, and secure sensitive data from quantum computer attacks.

The Market and Customer

The market opportunity for electric vehicles (EVs) in the United States between now and 2030 is vast, driven by governmental initiatives and market dynamics. The Bipartisan Infrastructure Law and McKinsey's analysis point to a significant surge in EV adoption. With provisions in the infrastructure bill aiming to invest billions in EV infrastructure and consumer incentives, the stage is set for robust growth. McKinsey's estimates suggest that by 2030, EVs could represent nearly half of all vehicle sales in the U.S. Coupled with increasing consumer awareness, technological advancements, and declining battery costs, EVs are poised to revolutionize the automotive industry.

Grand View Research, Inc.[19] projects that the global electric vehicle charging infrastructure market will reach $121.09 billion by 2030, a CAGR of 25.5%. It projects the U.S. EVCI market will reach $24.07 Billion in the same timeframe, a 29.1% CAGR.[20]

This presents immense opportunities for automakers, charging infrastructure providers, and related industries to capitalize on the shift toward electrification while necessitating heightened cybersecurity attention. As the EV market expands, so does the potential for cyber threats targeting vehicles and charging infrastructure. Additionally, the looming threat of quantum computers poses challenges to traditional cybersecurity measures, underscoring the importance of developing robust encryption and security protocols to safeguard against future vulnerabilities.

---

[19] "Electric Vehicle (EV) Charging Infrastructure Market to Reach $121.09 Billion by 2030: Grand View Research, Inc.". 2024. Www.Prnewswire.Com. https://www.prnewswire.com/news-releases/electric-vehicle-ev-charging-infrastructure-market-to-reach-121-09-billion-by-2030-grand-view-research-inc-301805255.html.

[20] "U.S. Electric Vehicle Charging Infrastructure Market Worth $24.07 Billion By 2030". 2024. Www.Grandviewresearch.Com. https://www.grandviewresearch.com/press-release/us-electric-vehicle-charging-infrastructure-evci-market-analysis.

Conclusion

The U.S. is heading toward an electric future—a future of fast, powerful, efficient, and clean transportation. This is great news since transportation is the U.S.'s largest source of greenhouse gas emissions (28% of the total in 2021).[21] So, the transition of transportation to electric vehicles will significantly contribute to slowing global warming.

But with this transition comes a reliance on an electric vehicle charging infrastructure. Like other infrastructure we rely on, such as water and communications, our EVCI will be a "critical" component to our livelihood. This dependence and criticality make the EVCI a target for cybercriminals and terrorists.

Building a new EVCI is not enough; we must also harden this new infrastructure against the future threat of quantum computer attacks planned, coordinated, and executed by sophisticated nation-states — perhaps those same states investing the most in quantum computing.

[21] Sources of Greenhouse Gas Emissions. (2024). Retrieved 26 March 2024, from https://www.epa.gov/ghgemissions/sources-greenhouse-gas-emissions#transportation