DOCKETED	
Docket Number:	19-AB-2127
Project Title:	Implementation of AB 2127 Electric Vehicle Charging Infrastructure Assessments
TN #:	240901
Document Title:	Michael Bourton Commentson ISO 15118 Charger Communication and Interoperability Workshop on Nov 10, 2021
Description:	Michael Bourton Comments - Comments on ISO 15118 Charger Communication and Interoperability Workshop on Nov 10, 2021, and the Accompanying Staff Proposal
Filer:	System
Organization:	Michael Bourton
Submitter Role:	Public
Submission Date:	12/10/2021 1:43:42 PM
Docketed Date:	12/10/2021

Comment Received From: Michael Bourton
Submitted On: 12/10/2021
Docket Number: 19-AB-2127

Comments on ISO 15118 Charger Communication and Interoperability Workshop on Nov 10, 2021, and the Accompanying Staff Proposal

Additional submitted attachment is included below.

Kitu Systems Inc.
3760 Convoy Street, #230
San Diego CA 92111

December 10, 2021

California Energy Commission
Re: Docket No. 19-AB-2127
1516 Ninth Street
Sacramento, California 95814-5512

Submitted to on-line portal:
https://efiling.energy.ca.gov/EComment/EComment.aspx?docketnumber=19-AB-2127

Re: Comments on ISO 15118 Charger Communication and Interoperability Workshop on Nov 10, 2021, and the Accompanying Staff Proposal

I am founder of Kitu Systems, with more than 40 years' experience in the implementation of communication systems and for the last 12 years specifically related to energy. Kitu Systems designs and supplies both energy related products and service based upon open Smart Grid standards and has participated in the development of these related standards.

At the CEC Workshop on November 10, 2021, I raised a question regarding a Cyber Security issue related to the EVSE and the use of ISO 15118. This concern was initially raised when the standard was reviewed and rejected as a Smart Grid Standard for inclusion in the NIST SGIP Catalog of Smart Grid Standards[1] in 2010 and more recently in the CPUC VGI Communications Protocol Work Group[2] in 2017.

Cyber Security is one of the most important issues in society today and there are already articles posted on the internet on how to hack V2G capable electric vehicles[3]. If these issues are not addressed at conception, they are difficult and very costly to rectify after they have been exploited, in addition to the substantial loss and damage caused to multiple stakeholders by both domestic and foreign cyber-attacks. Both Presidents Obama and Biden have issued Executive orders on cybersecurity.[4]

---

[1] https://www.nist.gov/programs-projects/smart-grid-national-coordination/standards-information-resources-nist-and-sgip

[2] https://www.cpuc.ca.gov/-/media/cpuc-website/files/legacyfiles/d/6442456402-deliverable-1-cpuc-draft-08062017.docx

[3] https://www.slideshare.net/SbastienDudek/article-on-v2g-hacking-v2g-injector-whispering-to-cars-and-charging-stations-through-the-powerline

[4] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity and Executive Order on Improving the Nation's Cybersecurity | The White House

The following sections explain the cybersecurity threat in the context of payment and Vehicle-Grid-integration (VGI) for Electric Vehicle Supply Equipment (EVSE or EV charging stations) and recommends a process for the CEC to move forward urgently on this topic including requiring industry standards for cybersecurity.

The Cyber Security issue relates to the use of a non-Internet compliant based Protocol (ISO-15118) that is used between the EV and the EVSE. Since the Energy Independence and Security Act of 2007[5] US Utilities have been tasked with the development of Internet based standards such as Smart Energy Profile 2 (SEP2) now known as IEEE 2030.5 which replaced Smart Energy Profile 1 (SEP1). In addition, security for payment systems relies on Internet based systems and compliance. The reason is that the investment in the Internet and its underlying standards have evolved quickly to combat new attacks.

The particular cyber security issue that is of great concern and should be urgently addressed before adoption of the proposed system architecture is known as Man-in-the-Middle (MitM) attacks:

> A secure transaction between two parties should not be understood by a third party who may take the opportunity to exploit the information to either cause harm or loss to one of the two parties in the legitimate transaction.

The third party is known as the MitM. We have all been targets of MitM attacks with examples such as receiving emails masquerading as a financial institution or service illegitimately directing their target to click a link to change a password. If the target follows the link, the MitM has now obtained the target's credentials and can use these credentials to cause great harm to their target. This is the most exploited fraud that everyone meets every day, but MitM attacks come in many forms such as the Target Point-Of-Sale credit card system MitM attack in 2013 which netted the attackers 110M Credit card numbers and more recently the Solarwinds software upgrade attack that hit both government and major private companies who are still trying to determine what was stolen or compromised.[6] Neither of these were discovered until after substantial data and financial loss.

There are many pathways in an EV system for payment and VGI signals and if the communication just involves 2 parties, MitM threats do not exist. E.g., EVSP to EVSE.

However, if two different protocols are used then the EVSE can be a host for a MitM attack when it involves two other parties such as when the EV communicates to a payment clearing house or to the Grid, the EVSE has access to the payment information or Grid controls. If malicious code can be inserted by the original manufacturer, the software developer, the EVSE installer, maintenance person or other party that gains accesses to the EVSE via physical access, or an intentional or unintentional back door, then this is a MitM attack. This is because the secured communications protocol from the EV to EVSE must be decrypted by the EVSE and then re-encrypted into another protocol to communicate with the payment system or Grid control. This gives the EVSE access to data-in-the-clear that can compromise the system.

---

[5] https://www.congress.gov/110/plaws/publ140/PLAW-110publ140.pdf
[6] https://www.youtube.com/watch?v=RxGI-l4VxL0

Is the cybersecurity threat solved by a security module in the EVSE?

The purpose of the security module is to encrypt the data downstream to the EV or upstream to the payment system or grid control. This protects the data on the communication path using encryption but does not protect the data inside the EVSE. Specifically, the introduction of a security module is a cyber security risk especially if not initially used, can be leveraged by hackers in the supply chain[7].

How does the cyber attacker get access to the unencrypted information, and can it be prevented?

This is by no means a complete list but here are examples of methods that hackers use and what can be done to prevent these in a two-protocol system.

Hacker Method	Detection	Remedy	Comments
RF Scan the insecured data externally	None	Metal shield	Minor-cost Impact
Physically open EVSE and wire to control board	Open Door alarm and intrusion detection	Resin Pot the assembly to prevent hot-wiring and use a Secure Processor. Take the EVSE out of service on door open until physically inspected.	Door Alarm can be by-passed. High-cost Impact and may not solve the data in transit only data at rest. Unit is not longer repairable.
Infected upgrade images	Use signed images Virus check images before deployment	Development and Operational quality standards	Hard to enforce, especially field upgrades
Unused board components	Nearly impossible to detect, until breached	Do not install unused components	Hard to enforce
Find open communication port to plant malicious code	Penetration Testing for open ports/back doors/system crashes	3-month Penetration Testing regiment	High-cost impact
Insert malicious code during development	Very hard to detect	Rigorous Process and Procedures NIST SP 800-151 SoC-2 Type 2 NIST SP 800-53	Hard to enforce, especially for offshore development
Insert Malicious code during manufacturing	Very hard to detect	Rigorous Process and Procedures NIST SP 800-151 SoC-2 Type 2 NIST SP 800-53	Hard to enforce, especially for offshore manufacturing
Insert Malicious code in the supply or installation phase	Near impossible to detect for field upgrades	Rigorous Process and Procedures NIST SP 800-151 SoC-2 Type 2 NIST SP 800-53	Hard to enforce, as there are many potential actors in the supply and installation chain

[7] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Overall, it is very difficult, costly and a continual process of catch-up to ensure that an EVSE can be designed and made secure as proposed, especially as the hackers see the challenge and continually discover weaknesses to exploit.

Where two protocols are required to be used in a three-party system, this transaction can be done more effectively in the cloud as the system can be physically secured, and extra layers of costly security can be provided. Even so, Cloud systems are still vulnerable as every week, breaches of security are reported by major institutions.

How is this solved in similar situations?

The established and proven method for solving this problem is known as end-to-end authentication authorization and encryption, which is supported by standards-based Internet protocols. There is information that should be passed through the EVSE as encrypted data. For example, if the EV wants to send some information to the payment or grid, then the two parties authenticate each other, authorize the exchange, and encrypt the information known as the payload. Attached to the payload is the routing information and other information such as the source and destination address. The EV then sends this information known as a packet to the EVSE. The EVSE reads the destination address and knows to forward the packet, which is known as bridging, switching, or routing and in this case it's the payment system or grid. Even if there is some malicious code in the EVSE the payload is encrypted and it does not have the security keys to decrypt the information, therefore totally eliminating the MitM. This is the safest and established method for handling this type of situation.

What are the consequences of a cybersecurity attack on the grid, the EV or the payment system?

Cybersecurity is not only a consumer payment fraud issue, but a potential safety issue for the grid and the EV. Examples of threats include:

1. Destabilizing the grid and potentially causing major damage to infrastructure by taking control of a large number of chargers or a few high-power chargers and turning them all on or off at once, or if V2G capable, instructing a large number of EVs to discharge power all at once.
2. Destabilizing the grid by EVSEs requesting a lot of power when it is not actually needed, bringing too much load, or in the case of V2G, generation to a grid area.
3. Over exercise EV batteries, causing battery damage, and creating a fire hazard.
4. Force EVSE out of service or disable the EV by discharging the battery, for example along a major highway. This could be a bigger threat once most transportation transitions to electric and could even be used in conjunction with shutting off charging operations during emergency response events etc.
5. Identity threats and fraud by compromising charging accounts to steal electricity, identity theft, or payment information.

Since most EVSEs are unmonitored and accessible by the public and hackers, malicious code could be present for months or years before being discovered. Cloud based aggregators / server farms spend a lot of money on physical and cybersecurity including frequent penetration testing and constant auditing. While this solution is feasible for a few server farms, it is prohibitively expensive for millions of EVSE.

We strongly recommend that any charging station regulation or funding program by the CEC include requirements for end-to-end system cybersecurity to protect against malicious code, malicious chips and other cybersecurity threats. Specifically, the CEC should require any two-party or three-party architecture to meet:

1. NIST SP-800-161 [8]
2. NIST SP-800-53
3. NISTIR 7628 Revision 1 paragraph 6.5.1 http://dx.doi.org/10.6028/NIST.IR.7628r1
4. Payment Systems Industry Standards[9]
5. Any federal executive orders.[10]

Further we recommend that the CEC should bring in EVSE cybersecurity experts for a workshop and also conduct a systemic cybersecurity review. Specifically, California utilities, EPRI and various private consultants are experts on this topic. EPRI, for example, has a DOE contract on this subject for EVSEs and works with NIST on cybersecurity standards. Utilities such as SCE have or are developing safety and cybersecurity plans for EVSEs. The CEC needs a much deeper review before implementing its proposed workplan on ISO 15118, especially to address the cyber security risks for both payment and VGI systems. Cybersecurity should not be an afterthought. Systems must be designed at the start to be physically and cyber secure. In the public workshop on Nov 10, when these standards and the cybersecurity risk was raised in public comments, at least one expert panelist (Cliff Fietzek at InCharge) agreed that MitM is an issue but only offered a partial remedy using penetration testing.

We greatly appreciate the opportunity to provide feedback on these Workshop and Draft Cybersecurity requirements and thank you for consideration of our comments. Do not hesitate to contact mbourton@kitu.io if you have any questions.

Best regards,

Mike Bourton

Founder, Kitu Systems

[8] The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, was directed to improve cybersecurity for critical infrastructure by a Presidential Executive Order. See here for more information https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics.

[9] PCI standards for chip and contactless readers for credit, debit and cash cards or mobile phones are required by the CARB EVSE payment regulation (per SB 454). For example PCI DSS level 1 standard or PCI standards used by Google, Apple and Samsung payment systems.

[10] The Executive orders from Presidents Obama and Biden referenced earlier and any future orders.