DOE Vehicle Technologies Office
Cyber-Security of On-Road Transportation: ELT206

(Cybersecurity Platform and Certification Framework Development for XFC-Integrated Charging Ecosystem)

PI(s) Tobias Whitney & Sunil Chaya

Presenter: Tobias Whitney, EPRI

6/13/2019

This presentation does not contain any proprietary, confidential, or otherwise restricted information

Overview

Timeline

- October 2018
- December 2020
- 5% complete

Barriers

- Lack of security awareness of standards and requirements
- Limited stakeholder engagement process
- No central location of security risks and requirements

Budget

- $2.2M Total project funding
  - $1.7M DOE Share
  - $.5M Cost share

Partners

- EPRI (Lead)
- Kitu Systems
- Automation Research Group
- GreenLots
- Efacec
- Argonne NL
- NREL
- Other partners

Objectives

- Uniform system-wide requirements
- Active, broad stakeholder team
- Component → System test for requirement verification
- Secure Network Interface Card Open-sourcing of hardware and software design
- Technology transfer through EV Infrastructure Cybersecurity Working Group
- Coordinated effort with wider Federal, State and utility industry coalitions with EPRI as the forum for collaboration

Approach

Milestone	Type	Description	Delivery Date
Risk Matrix Completed	Technical	Risk Matrix for Each Ecosystem Subfunction completed.	Q1 2019 → 3/29/19
Working Group Created	Technical	EV Infrastructure Cybersecurity WG created.	Q1 2019 → 3/29/19
Vulnerabilities and Threats Identified & Secure Network Card Design	Technical	Security vulnerabilities and threats for each subsystem identified.	Q2 2019 → 6/28/19
Subsystem Security Requirement Complete	Technical	Subsystem Security Requirement Complete.	Q3 2019 → 9/30/19
Draft Reference Cybersecurity Architecture Completed	Go/No Go	Draft Reference Cybersecurity Architecture Completed.	Q4 2019 → 12/20/19

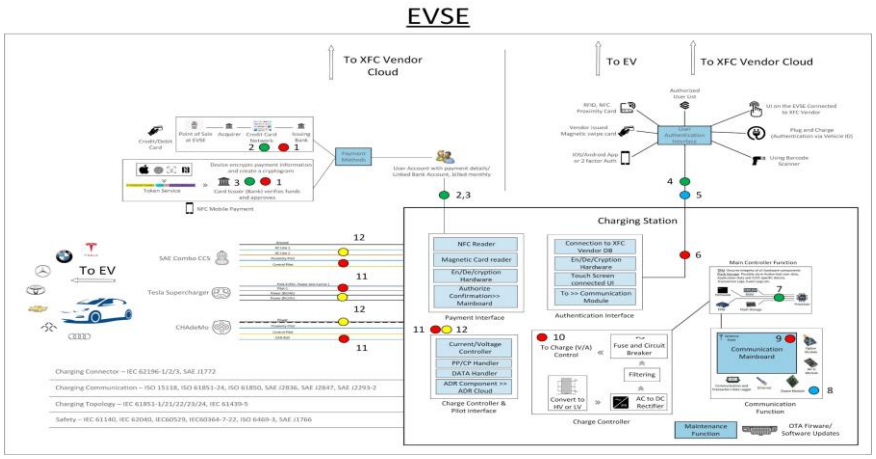
Approach

Milestone	Type	Description	Delivery Date
End-to-End Security Test Plan Complete	Technical	Test plan finalized.	Q1 2020 → 3/31/20
Security Testing Complete	Technical	Testing complete with results documented.	Q2 2020 → 6/30/20
Integrated Grid Security Risk Management Tool Finalized	Technical	Tool developed and updated based on testing results.	Q3 2020 → 9/30/20
Integrated Grid Security Risk Management Tool Published	Technical	Reference architecture is market-ready for implementation through industry deployments and regulatory framework.	Q4 2020 → 12/18/20

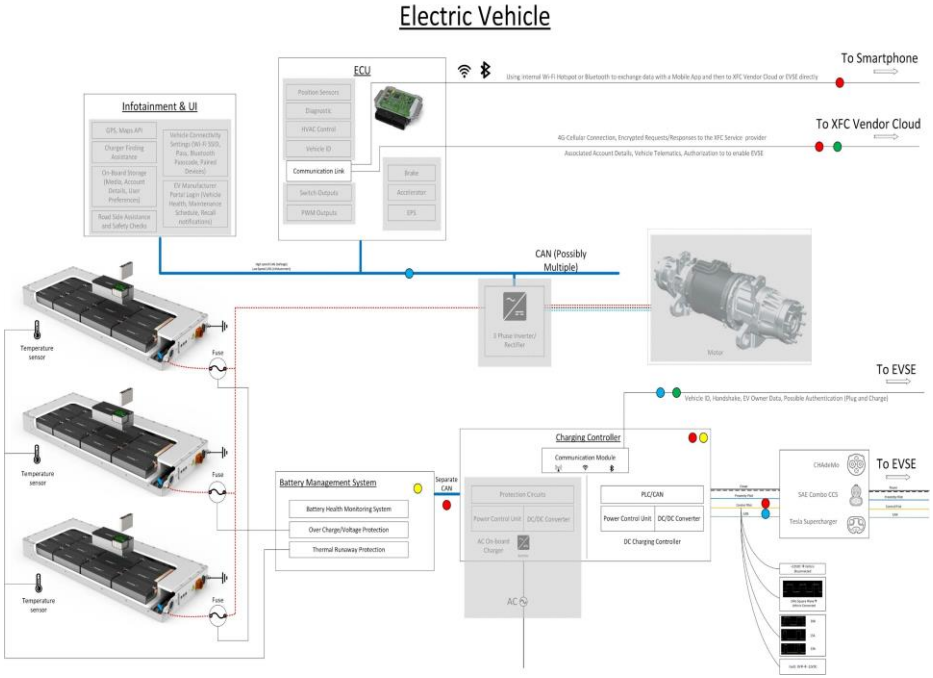
Technical Accomplishments and Progress: Q1 Deliverable and Working Group Formation

Component/Interface Level Risk Assessment

- Each component and system as-is system interface was evaluated for the ecosystem



- A risk type was assigned for each component/interface:
  - Reliability
  - Privacy
  - Financial
  - Safety



Risk Description and Explanation

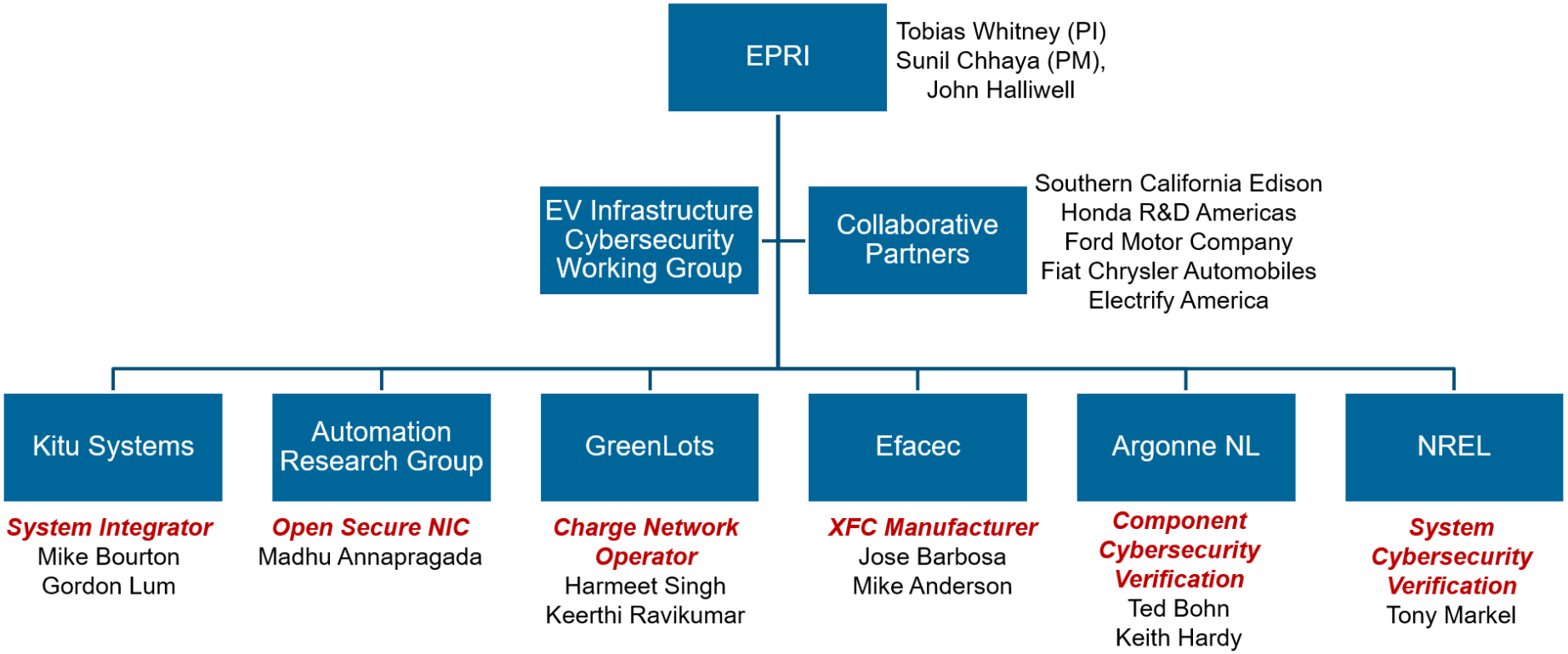
- Each diagram included a risk matrix that elaborated on the risks.
- This will be used to prioritize threats and vulnerabilities
- Controls and requirements language will be derived form risks.

RISK TYPE	SUB-SYSTEM	COMPONENTS INVOLVED	RISK DESCRIPTION	Consequences/Notes
1. Financial Risk	XFC/EVSE Vendor Cloud	Business Logic verifying payment authorization	Gaining root access to the cloud can expose payment details of all consumers who have Auto-Pay setup.	Financial loss due to stolen payment details.
2. Privacy Risk	XFC/EVSE Vendor Cloud	Vehicle Data Table, Customer Data Table	Compromise in security can reveal dynamic location of 100's of EV's	Attacker can track EV's with whatever precision the cloud application gets to know.
3. Reliability Risk	XFC/EVSE Vendor Cloud	EVSE and XFC Vendor Cloud	Modifying/interrupting data between EVSE and cloud to mark a particular EVSE as unavailable or corrupting Data on EVSE Cloud or adding bogus data.	This can trick EV's and the cloud such that all EVSE's appear to be occupied and unavailable; resulting in chaos and loss of business until attack in effect.
4. Privacy Risk	XFC/EVSE Vendor Cloud	Data Blob/Tables/Clusters or any format data is stored.	Once access is achieved, all the dynamic data is now available to spy on thousands of users resulting in massive breach of data and privacy.	Attacker can get all the PII of Users and vehicles like location, address, miles remaining, possible time when user will arrive at the EVSE and other vehicle telematics.
5. Reliability Risk	XFC/EVSE Vendor Cloud	Security Functions	Post unauthorized access to cloud, the security functions are subject to modifications or disabling as per attackers need.	One way is to disable encryption or get the keys so that attacker can later steal all the data without being noticed.
6. Financial Risk	XFC/EVSE Vendor Cloud	Security Functions	Tampering with the security functions creates a huge financial risk, allowing many users to exploit the changes made to the cloud application.	Possibility of getting free charging, theft of payment details, bank account details etc.
7. Reliability Risk	XFC/EVSE Vendor Cloud	OTA/Wired Firmware Update. In-House firmware or outsourced to 3rd party vendor.	The more steps a firmware will take to reach to the final device, the more chances of it being tampered/modified.	Modified firmware can effect entire behavior of the system until fixed.

EV Infrastructure Cybersecurity Working Group

- **30+ members**
- **Utility Companies**
  - Ameren
  - Arizona Public Service
  - Con Edison
  - CPS Energy
  - Great River Energy
  - ITC
  - National Grid
  - NYPA
  - PGE
  - SCE
  - Southern
  - TVA
- **Vehicle Partners**
  - Ford Motor Company
  - Toyota
  - General Motors
- **Other Interested Parties**
  - Vehicle ISAC

Collaboration and Coordination



Overall Impact

- **Link security risks to each component stakeholder in the ecosystem:**
  - Privacy
  - Reliability
  - Safety
  - Physical

- **Security requirements and considerations for each component and interface.**

Summary

Our project will…

- Define and validate uniform cyber-security technologies
- Develop architecture-specific modular security controls
- Publish standards across the EV and electric grid ecosystem to support secure deployment and grid integration of EV charging infrastructure.

Project Coordination

Resources and Capabilities

- What charging equipment or facility capabilities does your project have available?
- What software/hardware tools will your team be using during the project?

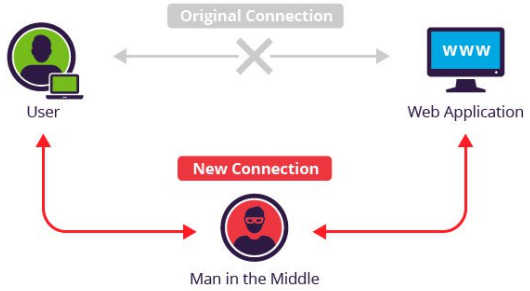
(see the following slides)

Testing Capabilities

- **The CSRL has a library of utility focused cyber security use cases that can be run against test beds to demonstrate the effectiveness of architectural changes or the introduction of new technologies.**

- **Specialized Exploits Available**
  - Advanced MITM attacks utilizing ARP spoofing and IP hijacking
  - IEC/ISO 15118-213 and SAE J2847/2 and other protocols
  - CrashOverride / Industroyer, Havex, Black Energy and DragonFly malware

- **Penetration Testing**
  - Fuzzing
  - Vulnerability Scanning
  - Attack Surface Evaluation

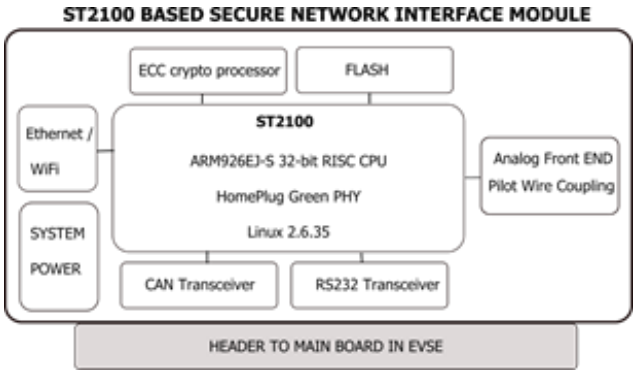


EPRI Open-Sourced Secure Network Interface Module With Secure Open Standards Network Interfaces, for built-in Cybersecurity Compliance

Open Grid Interface API, Local EMS + OCPP, EPRI IEEE 2030.5 server; IEC/ ISO 15118 Server

SAE J1772 PWM Pilot w/ IEEE 2030.5 or IEC/ISO 15118 /PLC

Open-Sourced Secure Network Interface Module for EVSE and XFC



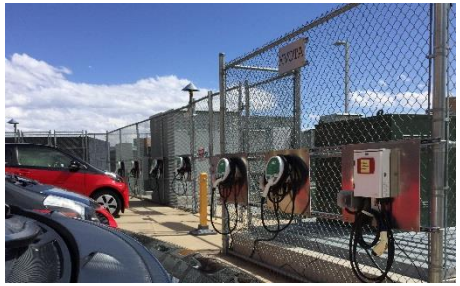
Source: Automation Research Group

Argonne National Lab Test Setup for Component Level Cybersecurity Verification

NREL ESIF Test Setup for EV Infrastructure System Level Cybersecurity Verification

Energy Security and Resilience

Facility Smart Charge Management



Distribution Vehicle to Grid Impacts

DCFC Systems Integration

Assessment Activities

- **What are your project cyber security assessment needs?**
  - Awareness of assessment processes from other projects. Leverage and share results.
- **What information do you need on threat vectors, vulnerabilities, etc. to complete your project?**
  - Any existing work and related publications. Our goal is not re-invent the wheel with regard to coordinated activities.
- **What outcomes or information could your project provide to other teams around the year 1 timeframe?**
  - Component and system level risk assessment and draft security requirements for XFC environment.

Proposed Future Research

Milestone	Type	Description	Delivery Date
Risk Matrix Completed	Technical	Risk Matrix for Each Ecosystem Subfunction completed.	Q1 2019 → 3/29/19
Working Group Created	Technical	EV Infrastructure Cybersecurity WG created.	Q1 2019 → 3/29/19
Vulnerabilities and Threats Identified	Technical	Security vulnerabilities and threats for each subsystem identified.	Q2 2019 → 6/28/19
Subsystem Security Requirement Complete	Technical	Subsystem Security Requirement Complete.	Q3 2019 → 9/30/19
Draft Reference Cybersecurity Architecture Completed	Go/No Go	Draft Reference Cybersecurity Architecture Completed.	Q4 2019 → 12/20/19

Q1 deliverables are complete

Proposed Future Research

Milestone	Type	Description	Delivery Date
End-to-End Security Test Plan Complete	Technical	Test plan finalized.	Q1 2020 → 3/31/20
Security Testing Complete	Technical	Testing complete with results documented.	Q2 2020 → 6/30/20
Integrated Grid Security Risk Management Tool Finalized	Technical	Tool developed and updated based on testing results.	Q3 2020 → 9/30/20
Integrated Grid Security Risk Management Tool Published	Technical	Reference architecture is market-ready for implementation through industry deployments and regulatory framework.	Q4 2020 → 12/18/20