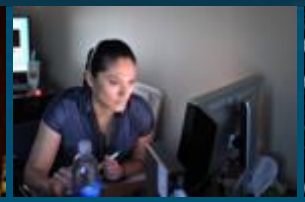
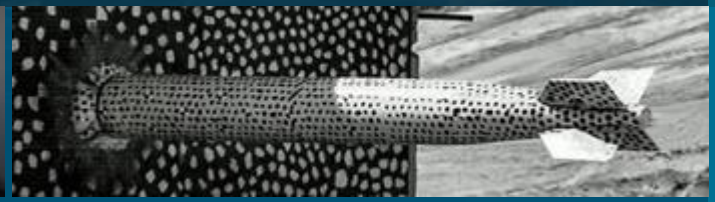
Securing Vehicle Charging Infrastructure





2020 DOE Vehicle Technologies Office Annual Merit Review

Arlington, VA
June 1-4, 2020

Jay Johnson, Sandia National Laboratories

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

Project ID: ELT198

SAND2020-4324 C

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Overview

$3M Project (Oct 2018–Sept 2021) (60% complete)

- Team: Sandia, PNNL, ANL
- Partners: DOT Volpe Center, NMFTA, 2 DCFC Vendors, 1 Utility

Project objective: Quantify cybersecurity risks to electric vehicle supply equipment (EVSE) and establish actionable recommendations to protect charging infrastructure so automotive, charging, and utility stakeholders can better protect customers, vehicles, and power systems in the face of new threats.

Technical Barriers/Gaps:

- Poorly implemented EVSE cybersecurity is a major barrier to electric vehicle (EV) adoption
- No comprehensive cybersecurity approach and limited best practices have been adopted by the EV industry
- Incomplete industry understanding of the attack surface, interconnected assets, and unsecured interfaces

Relevance

Primary goal: protect US critical infrastructure and improve energy security through technical analysis of the risk landscape presented by massive deployment of interoperable electric vehicle chargers.

- As the US transitions to transportation electrification, **cyber attacks on vehicle charging could impact nearly all US critical infrastructure.**

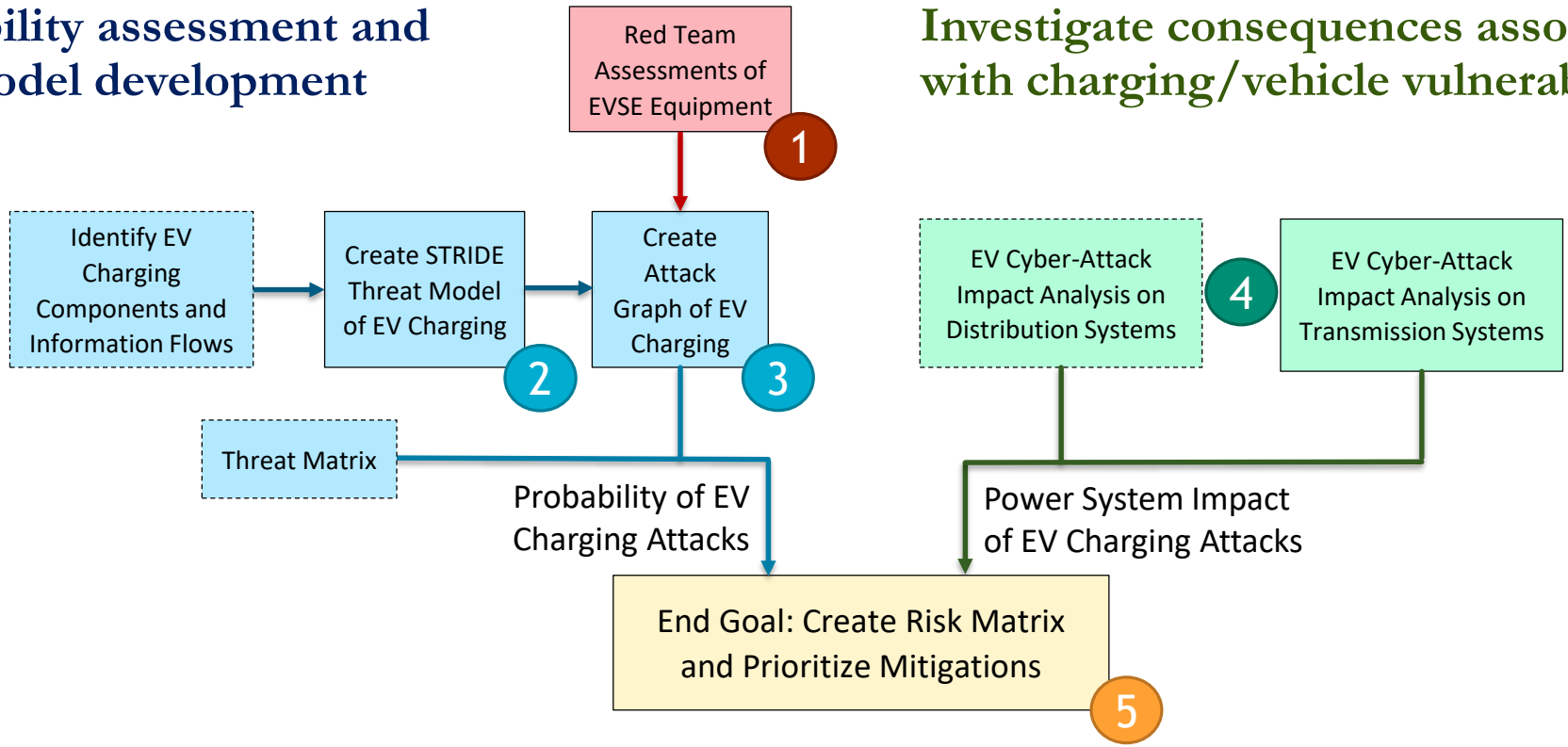
This project is **laying a foundation for securing critical infrastructure** by:

- Conducting adversary-based assessments of charging equipment
- Creating a threat model and attack graphs of EV charging
- Analyzing power system impact for different attack scenarios
- Providing a risk-based recommendations and hardening suggestions to the EVSE industry

Milestones

- Publish **attack graphs** and present initial **hardening recommendations** (FY20)
- Complete draft **threat model** for vehicles/charging infrastructure with prioritized vulnerabilities and enumerated communication entities/interfaces (FY21)
- Complete **consequence study** mapping EV/charging potential vulnerabilities to power system and other critical infrastructure impact (FY21)
- Draft **hardening guide** for EVSE vendors and networked associates (FY21)
- Complete **PKI recommendations** to standards development organizations (FY21)

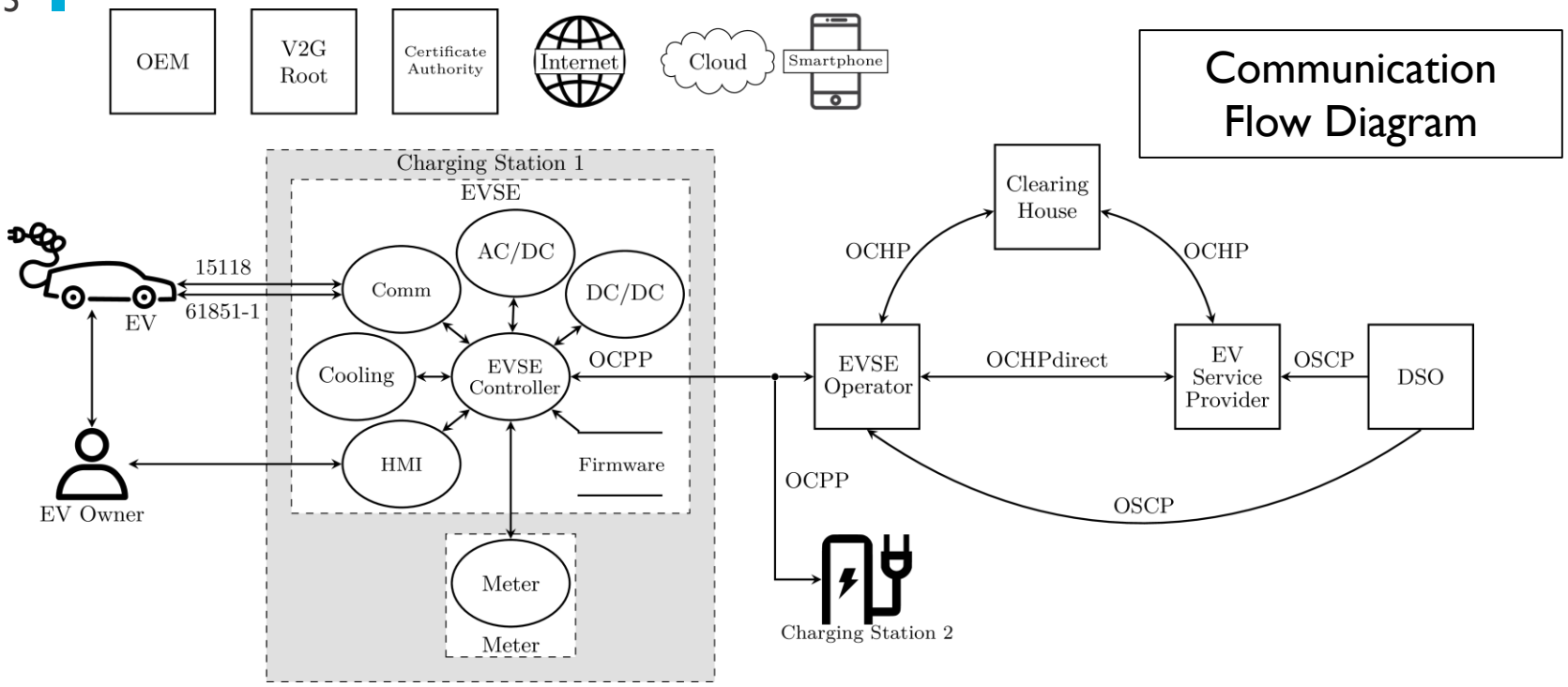
Approach



Project Deliverables

1. Anonymized **red team results** with brownfield EVSE hardening guide, recommendations, and best practices.
2. Report on the **threat model** with stakeholder entities, potential vulnerabilities, and risks to EV/EVSE infrastructure.
3. Published **attack graph** indicating how different attack vectors could be exploited to enact impacts to critical infrastructure.
4. Conference paper which quantifies cyber consequences associated with vehicle/charging vulnerabilities on the power system.
5. Final report of EVSE **cyber risks assessment**, suggested **mitigations**, and approaches for EV charging **cyber-resilience**.

Threat Model of EV Charging – Grid Impacts



STRIDE Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Developing first of its kind EV Threat Analysis:

1. Identify consequences to energy and transportation sectors
2. Define XFC security objectives: privacy, power system, transportation system, financial transactions, etc.
3. Revise communication and energy flow diagrams
4. Identify vulnerabilities using STRIDE
5. Identify controls and mitigations to address threats

Also, investigated the Public Key Infrastructure (PKI) security defined in ISO/IEC 15118-2

Findings:

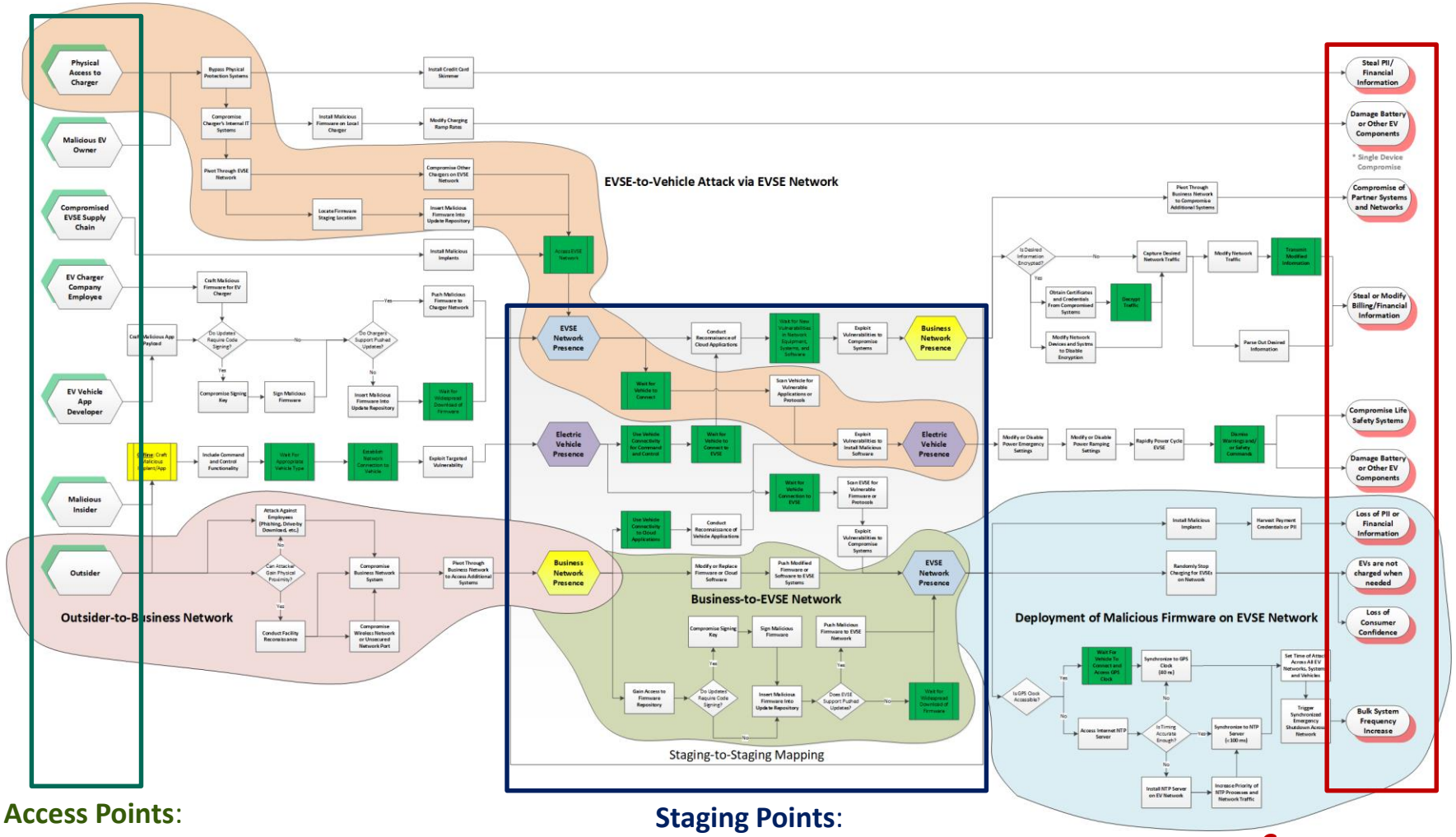
- STRIDE's narrow focus limits understanding of significant consequences.
- Understanding consequences helped us identify relevant threats.
- Energy sector cannot mitigate every XFC threats on their own.
- All XFC parties need strong coordinated cyber practices.

Deliverable:

- Threat consequence report publication target date: 9/2020

EV Charging Attack Graphs

- Attack graphs show attacker actions to achieve an objective
  - Illustrates access points, staging areas, and consequences of concern
  - Graphically illustrates the steps an attacker must take to move from system/network access to the consequences of concern
  - Complex steps are displayed as images
  - Public vulnerabilities and red team results advise attack graph



Access Points: attacker starting locations

Staging Points: network presence/pivoting

Consequences of Concern: impacts

Details in B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

EV Charging Attack Graphs

The team created attack graphs for the following use cases:

1. **Outsider to Business Network Presence**
   - Access Point: Attacker does not have authorized physical access to facility, network, or computing infrastructure.
   - Staging Point: Attacker gains presence in the EVSE Manufacturer's business network to use for follow-on activity.

2. **Deployment of Malicious Firmware**
   - Access Point: (A) Insider with physical facility access and has credentials to access the business network or (B) attacker with business network presence.
   - Consequences of Concern: (A) Bulk system frequency increase, (B) EVs not charged when needed, (C) loss of consumer confidence.

3. **Physical Compromise of EVSE**
   - Access Point: Attacker has physical access to EVSE
   - Consequences of Concern: (A) Loss of PII or financial information, (B) Compromise of partner systems and networks.
   - Staging Point: Attacker gains presence in EVSE Network

4. **EVSE to Vehicle**
   - Access Point: Attacker has malicious implant in EVSE.
   - Consequences of Concern: Compromise Vehicle Information System leading to consequences in #3
   - Staging Point: Attacker gains presence in Electric Vehicle

- Two major concerns in large-scale attack:
  - **Can the attacker "pivot"** between the components/networks to compromise information flows?
  - **Can an attacker synchronize their attack** to affect large portions of the grid simultaneously?

Details in B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

Red Teaming is…

Authorized

Assessments performed with permission of the system owner

Adversary-Based

Account for attackers' motivations and goals, knowledge and skills, tools and means

Defensive

We seek to improve the security posture of the system, network, or organization

Answers the question: ***Secure from whom and with what goals, skills, means, and tools?***

Red teaming is useful when:

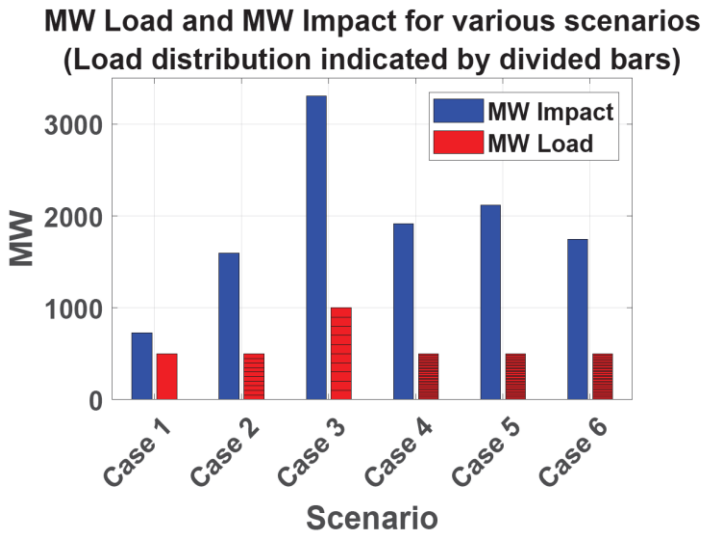
- Developer focus is on function rather than security
- System is deployed in a hostile environment
- Complex systems or systems of systems
- System is attractive to dynamic, adaptable adversaries
- Security choices must be made
- New use or new application of an existing system that may have unknown consequences
- System history shows previously discovered vulnerabilities
- A qualitative measure of system security is desired
- Need to establish or evaluate training and doctrine

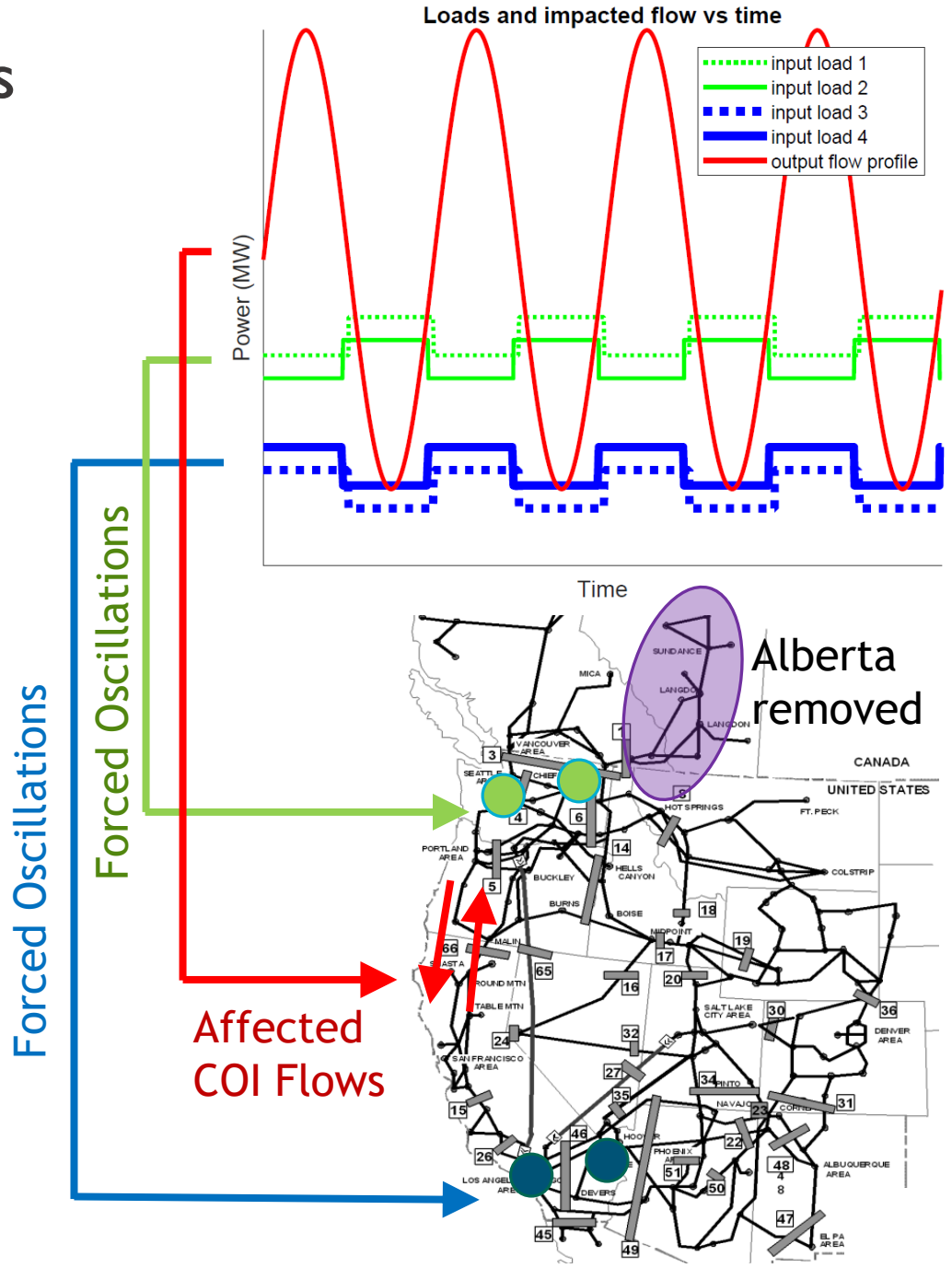
Red Team Assessments

- Access to equipment requires:
  - Extensive conversations with EV charger vendors/owners
  - Building trust with these organizations
  - Non-disclosure agreements
  - Concurrence on rules of engagement
- To date, the red team has investigated:
  - 4 DCFCs
  - 2 Level-2 chargers
  - ISO 15118-2 PKI requirements
- Plan to assess additional DCFCs and L2s in the final project year.
- Team has already found many areas for improvement, e.g.,
  - Failure to physically secure EVSE enclosures
  - Default passwords for internal systems, or credentials posted inside enclosure
  - Data is not encrypted at rest and only financial data is encrypted in transit
  - Unnecessary ports and services are enabled
- End goal: create a fully-anonymized set of findings and collection of recommendations for the EV charging community based on red team results.

Update on Power System Consequences

- In PY1:
  - Conducted distribution simulations and showed voltage excursions above ANSI C84.1 Range A with V2G functions when EVSEs were at end of feeder.
  - On the Western Electricity Coordinating Council (WECC), a simultaneous "digital emergency stop" of 10 GW of load (e.g., 22,000 EVSEs @ 450 kW), did not exceed NERC PRC-024-2 voltage or frequency relay trip limits.
- This year:
  - Full WECC planning model used in determining whether manipulating load due to EVSEs can induce interarea forced-oscillations
  - Used modal/eigen analysis to determine resonant frequencies
  - Conducted frequency response to select most affected locations
  - Results: Loads of 500 MW intelligently distributed across WECC cause >1500 MW of power fluctuations in California-Oregon Intertie (COI)
  - Full impact details are sensitive and cannot be provided here





WECC image from "Western Interconnection Transmission Path Flow Study, 1998 thru 2005,"
URL: https://www.wecc.org/Reliability/2007_WI_TransPath_UtilizationStudy.pdf

Risk Matrix and Remediation Prioritization

- For each attack scenario, likelihood of success and potential power system impact will be used to estimate risk.
  - Risk = Probability * Impact
  - Probability: estimated from threat model and vulnerability assessments
  - Impact: determined from power system simulations
- Identifying highest risk scenarios will inform DOE and industry of mitigation priorities

Likelihood (Threats + Vulnerabilities)	Consequence (Power System Impact)				
	Insignificant No Observable Impact to Power System	**Minor** Local Power System Impacts	**Moderate** Regional (Distribution) Blackout	**Major** Widespread (Transmission) Blackout	**Severe** Widespread Outage for Extended Period
Almost Certain Vulnerability Exploitable By Attacker: Script Kiddie Funding: None Time: Days	Medium	High	High	Extreme	Extreme
Likely Vulnerability Exploitable By Attacker: Skilled Actor Funding: Little Time: Weeks	Medium	Medium	High	Extreme	Extreme
Possible Vulnerability Exploitable By Attackers: Moderately-Skilled Team Funding: Some Time: Months	Low	Medium	Medium	High	Extreme
Unlikely Vulnerability Exploitable By Attackers: Skilled Team Funding: Substantial Time: Years	Low	Low	Medium	High	High
Rare Vulnerability Exploitable By Attackers: Nation State Funding: Substantial Time: Decades	Low	Low	Low	Medium	High

Likelihood axis advised by:
[1] M. Mateski, et al. “Cyber Threat Metrics” SAND2012-2427.
[2] D.P. Duggan, S.R. Thomas, C.K.K. Veitch, L. Woodard. “Categorizing Threat: Building and Using a Generic Threat Matrix.” SAND2007-5791.

Consequence axis advised by:
[3] J. Johnson, et al., “Power System Effects and Mitigation Recommendations for DER Cyber Attacks,” IET Cyber-Physical Systems: Theory & Applications, Jan 2019.

Responses to Reviewers' Comments

Consider incorporating a commercial cybersecurity firm as consultant.

- The sensitive nature of the red team assessments doesn't permit bringing on outside partners for the assessments.

Need fleet partners and telematics manufacturers to bring in real-world application views.

- Agreed. This team is working with industry to better understand the real-world implementations of telematics systems for the threat models and has share initial results with the industry to get feedback and identify areas of improvement.

Need specifics in the risk matrix, e.g., specifics on the axes.

- These details have been added, albeit at a notional level.

Good analytics on power system impacts, but additional work is needed beyond current scope (e.g., supplying wrong voltage, high current leading to a vehicle fire) to develop remediation methods for other attacks

- This project is scoped to focus on impacts to the power system because many of the other VTO-funded projects are taking a broader view of attack consequences. We're working hard to coordinate our efforts with the other cybersecurity projects.

Unclear which labs were responsible for each of the project activities.

Lab	Red Team Assessments	Threat Modelling	Attack Graphs	Power System Modelling
Sandia	Lead	Support	Lead	Distribution
PNNL		Lead		Transmission
ANL	Support		Support	

Partnerships/Collaborations

National Lab Team: SNL, PNNL, ANL
Government Partners: DOT Volpe Center
Industry Partners:

- National Motor Freight Traffic Association, Inc. (NMFTA)
- Multiple leading DC Fast Charging (DCFC) vendors
- Large utility partner

External Collaborators: The team continues to work closely with DOE VTO-funded cybersecurity projects and government agencies, including:

- DHS
- DOT
- Navy
- Army
- DOE FEMP
- DOE CESER

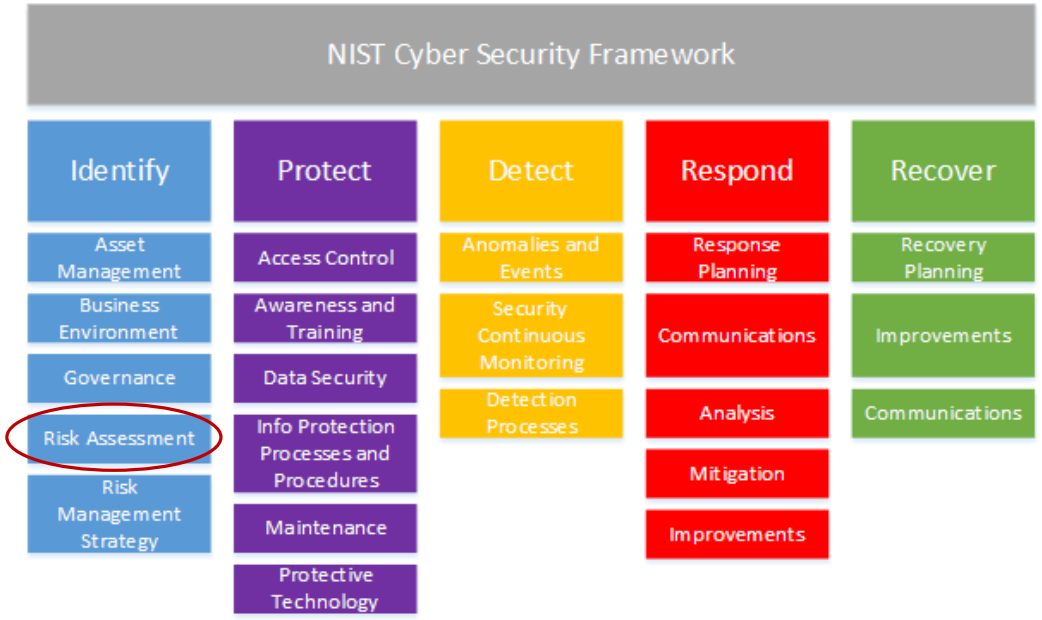
Remaining Challenges and Barriers / Future Research

This project is helping **identify potential EV charger vulnerabilities and quantify the risk to critical infrastructure** when vehicle charging infrastructure is maliciously controlled.

- First step in continuous process of hardening charging infrastructure against cyber-attacks.

Risk assessments are the beginning of a comprehensive approach to cybersecurity. Additional work must include:

- Developing **standardized policies** for managing chargers and other assets in the charging ecosystem
- Designing effective **perimeter defenses** to protect the assets including: firewalls, access control lists, data-in-flight requirements (encryption, node authentication), etc.
- Creating **situational awareness** systems, **intrusion detection/prevention systems**, and anomaly detection.
- Researching **response mechanisms** to prevent further adversary actions on the system, nonrepudiation technologies, and dynamic responses.
- Creating hardware- and software-based fallback and **contingency operating modes**.



Summary

- **The goal of the project is to provide DOE and automotive, charging, and utility stakeholders with a strong technological basis for securing critical infrastructure**.

- By **collaborating closely with other government agencies and industry stakeholders**, we hope to generate a consensus threat model for EV charging and quantify the risk to the power system.

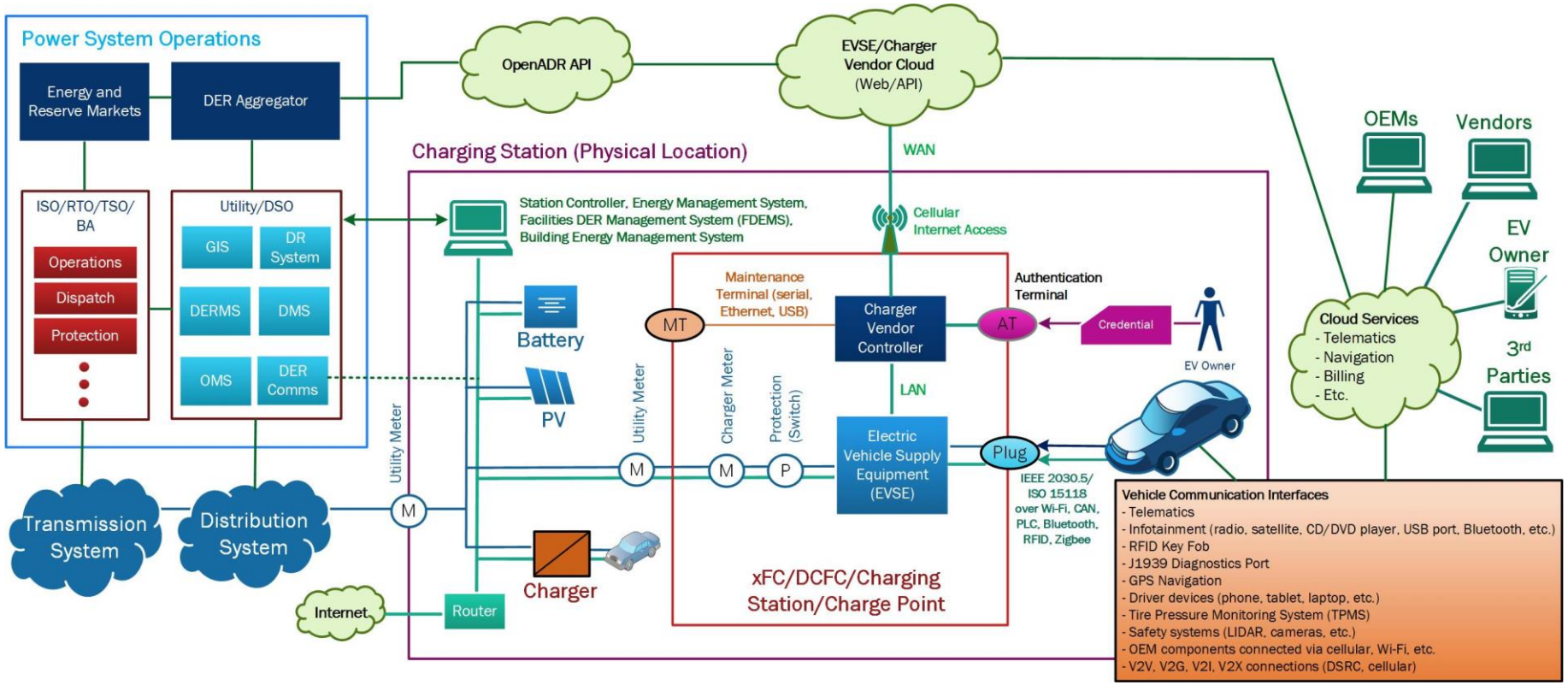
- To accomplish this, the team is:
  - Conducting adversary-based assessments of charging equipment
  - Creating threat models and attack graphs of the EV ecosystem to estimate the probability of different attacks
  - Analyzing power system impact for different attack scenarios

- This is **only the beginning of a long process to secure charging infrastructure from cyber attacks**.

Technical Backup Slides

EV Charging Components and Information Flows

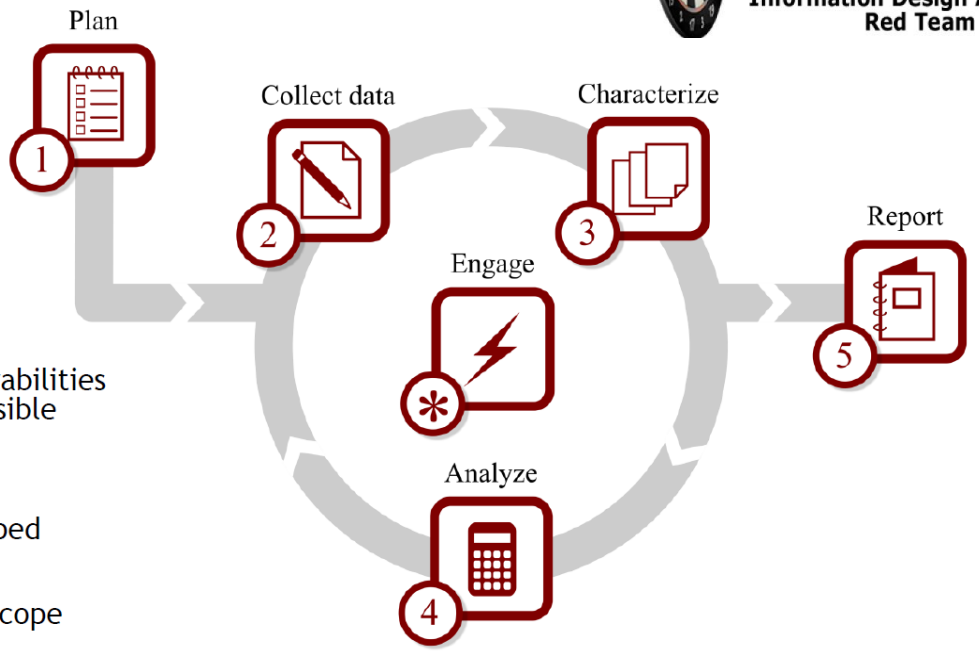
Created common nomenclature and enumerate assets and interfaces.



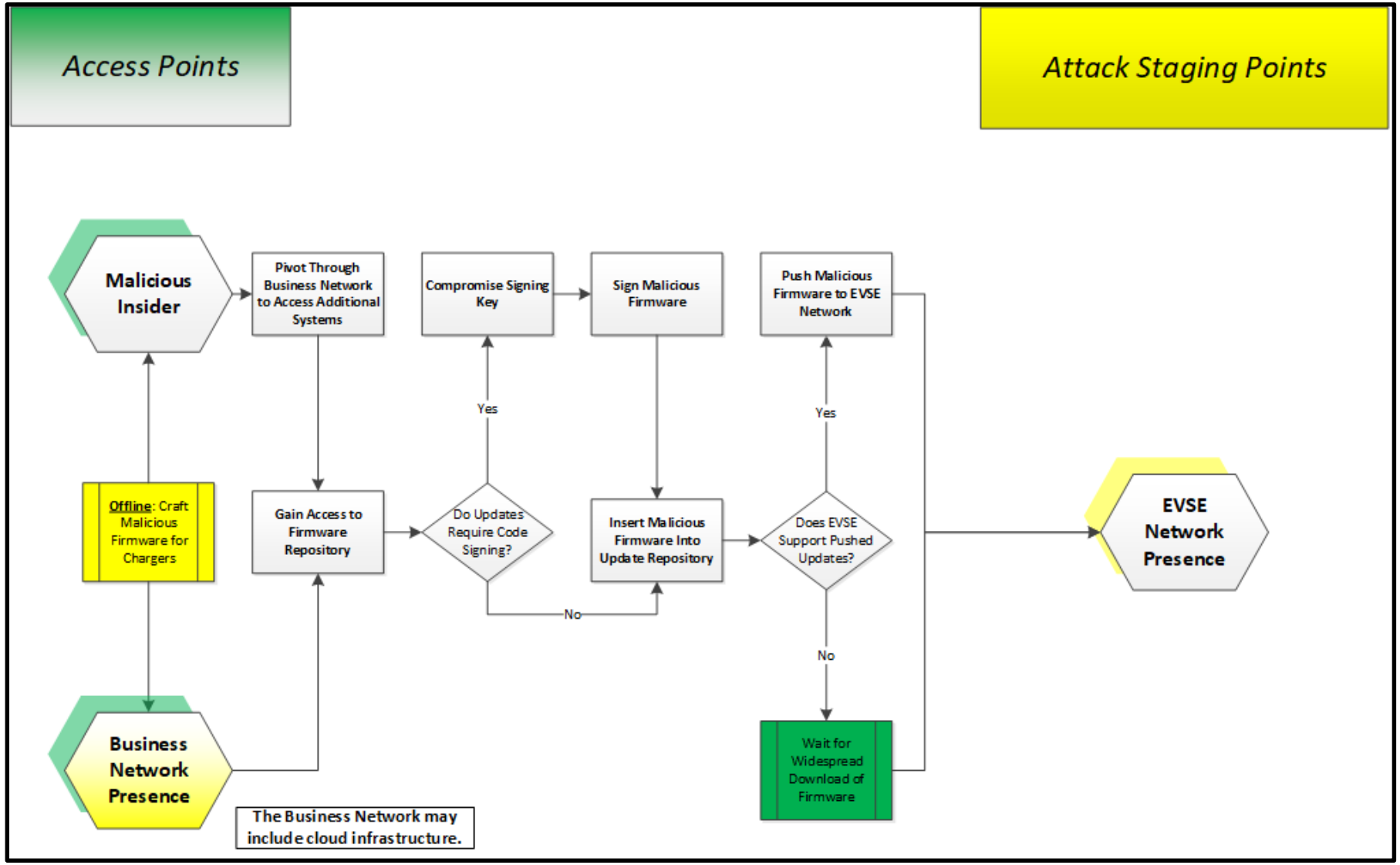
Red Teaming

Provides hands-on input to threat model/attack graph

- **Planning**
  - Negotiate work
  - Identify and procure resources
- **Data Collection**
  - Scoping visit activities and information requests
  - Open source information gathering
- **Characterization**
  - Refine understanding of system given data collected
  - Generate/refine views to facilitate discussion
- **Analysis**
  - If needed, collect more data and re-characterize
  - Otherwise, determine where vulnerabilities may exist and what attacks are possible
- **Reporting & Closeout**
  - Compile final report
  - Complete other deliverables as scoped
- **Demos & Experiments**
  - These are optional and depend on scope
  - Obtain special authorization
  - Formulate risk management plan
  - Test the exploitability of identified vulnerabilities

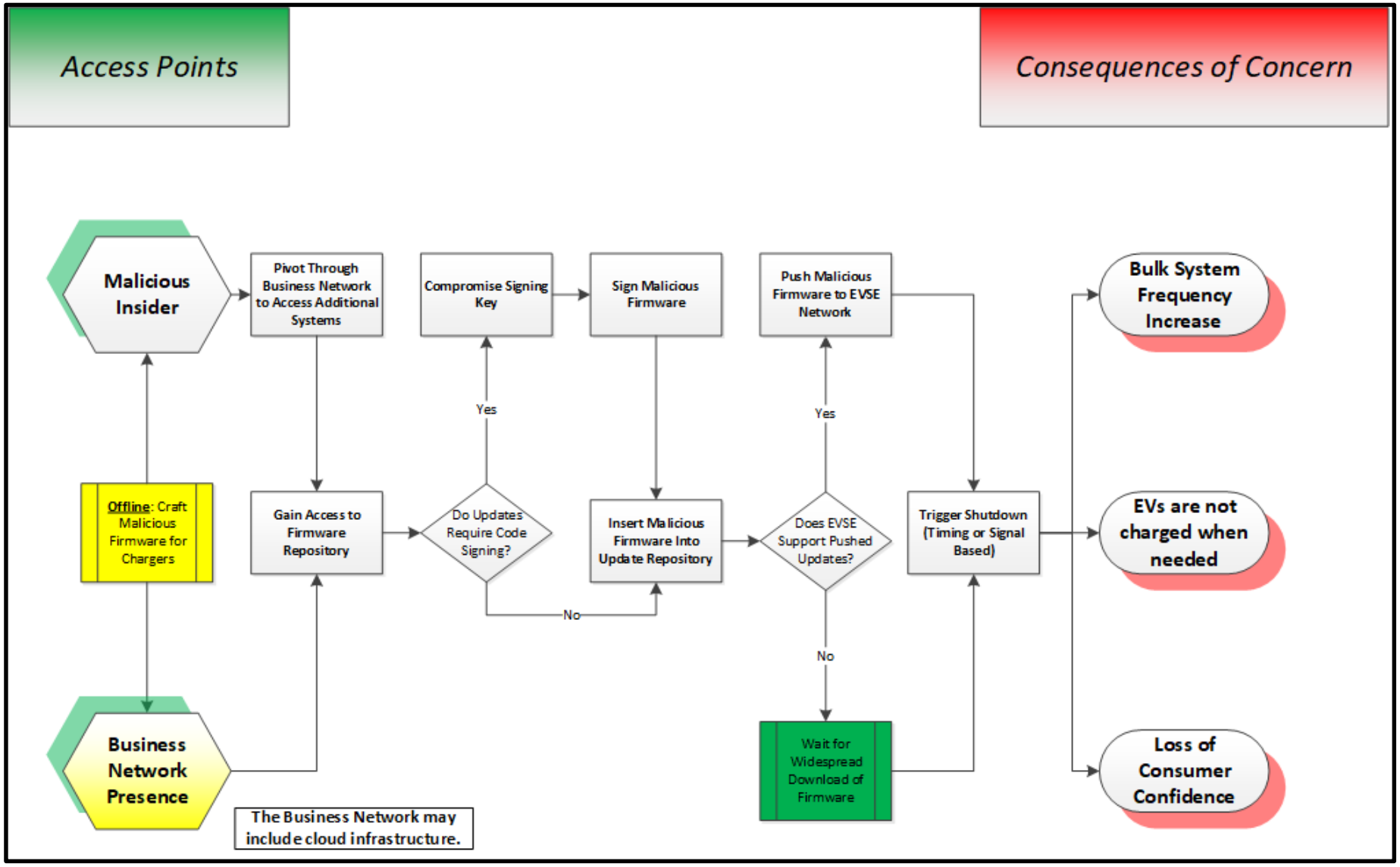


Example Attack Graph: Pivoting From Business Network to EVSE Network



Details in B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

Deployment of Malicious Firmware



Details in B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

Initial EVSE Hardening Recommendations

Implementation of industry best practices across all networks

- Critical business systems should be well protected and accessible only to essential personnel
- Limit connections between different networks
- Log and monitor events within the various networks
- Require digital signatures for all software and firmware
- Utilize multi-factor authentication and separation of duty principles for critical activities

Physically secure EVSE to prevent tampering

- Ensure the supply chain is secure and spot check hardware before deployment
- Monitor EVSE systems for unscheduled physical access