This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2021-9939C

Special Session: Cybersecurity for Power Electronics

DER Cybersecurity Stakeholder Engagement, Standards Development, and EV Charger Penetration Testing

Jay Johnson

Renewable and Distributed Systems Integration

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

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.

Contents

- Distributed Energy Resource (DER) Cybersecurity Stakeholder Engagement
  - SunSpec/Sandia DER Cybersecurity Workgroup Webinars
- DER Cybersecurity Standards Development
  - DER Cybersecurity Workgroup Recommendations
  - IEEE 1547.3
  - CA Rule 21
- Penetration Testing of Electric Vehicle Supply Equipment (EVSEs)
  - Red Team Research
  - Attack Graphs
  - Hardening Recommendations

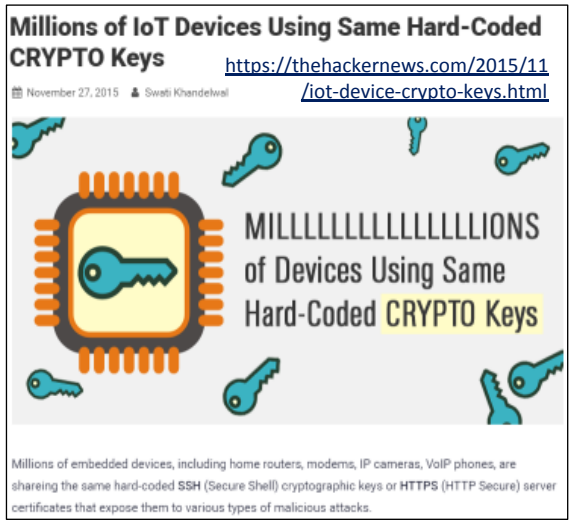
Motivation for Improving Cybersecurity of Energy Conversion Devices

- DER, EV chargers, buildings, microgrids, and other control systems are increasingly **networked** and **internet-connected**.
- An **expanded cyber attack surface** is the price for advanced control, remote access, and convenience.
- **Cybersecurity is rarely a priority** in highly competitive, unregulated markets.

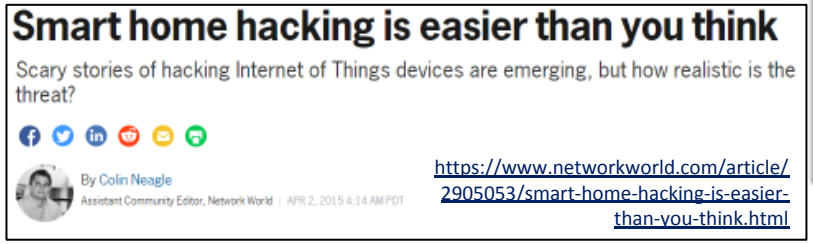
https://thehackernews.com/2016/10/ddos-attack-mirai-iot.html

http://www.bbc.com/news/amp/technology-40861976

http://buildingautomationmonthly.com/guess-who-just-hacked-a-building-automation-system/



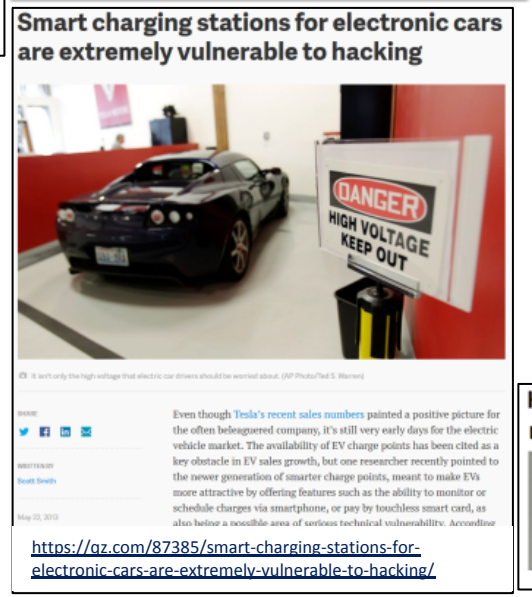
https://thehackernews.com/2015/11/iot-device-crypto-keys.html



https://www.networkworld.com/article/2905053/smart-home-hacking-is-easier-than-you-think.html

https://www.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat

https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/



https://qz.com/87385/smart-charging-stations-for-electronic-cars-are-extremely-vulnerable-to-hacking/

https://www.technologyreview.com/the-download/608464/hackers-could-hold-entire-wind-farms-hostage/

DER Cybersecurity Educational Webinar Series

IEEE ENERGY CONVERSION CONGRESS & EXPO
2021
Vancouver, Canada Oct. 10-14

Engagement activities bring together individuals across industry, academia, and government to exchange ideas and learn

Monthly Educational Webinar Series

- 4th Thursday of Each Month
- Blend of research, implementation recommendations, general cybersecurity education, etc.
- Email support@sunspec.org to participate!

Watch them on SunSpec TV:
https://www.youtube.com/watch?v=vBtYkboJGd0&list=PLFHov2_eYmehGvz2SjlXkLNOfd2Ldk0z_

2021 Webinars

- **1/21/21 – Cybersecurity Advisory Group for State Solar (CATSS) Brief**
  - Campbell Delahoyde, National Association of State Energy Officials (NASEO)
- **2/25/21 – Overview of IEEE 1547.3: A Guide for Cybersecurity of DER Interconnected with Electric Power Systems**
  - Ryan Davidson, MPR Associates
  - Frances Cleveland, Xanthus Consulting International
- **3/25/21 – Conceptualizing Systems Cybersecurity Challenges for Rooftop Solar**
  - Jeremiah Miller, DOE Solar Energy Technologies Office
- **4/22/21 – Securing the Industrial Internet of Things: Cybersecurity for DER**
  - Jim McCarthy, *NIST National Cybersecurity Center of Excellence (NCCoE)*
- **5/27/21 – An Industrial Cybersecurity Perspective**
  - *Ben Miller, Dragos*
- **6/24/21 – Centralized vs Decentralized DER Role-Based Access Control Implementation**
  - *George Fragkos, University of New Mexico*
- **7/22/21 – Software Vulnerabilities (Software Bill of Materials – Transparency in the Software Supply Chain; Longclaw – Firmware Analysis Framework; Next Generation Firmware Analysis for Energy Systems)**
  - *Allan Friedman, US Department of Commerce, NTIA*
  - *Jovana Helms, Lawrence Livermore National Laboratory*
  - *Chris Lamb, Sandia National Laboratories*
- **8/26/21 – Cyber-Physical Intrusion Detection/Mitigation System**
  - *Shamina Hossain-McKenzie, Sandia National Laboratories*
- **9/14/21 – Zero Trust Security for Distributed Energy Resources**
  - *Kip Gering, Xage*
- **9/23/21 – DER Incident Response**
  - *Rob Caldwell, FireEye/Madiant*
- **10/28/21 – Historical Public Key Infrastructure Failures**
  - *Josephine Wolff, Tufts University*

Pre-standardization Activities

SunSpec/Sandia DER Cybersecurity Workgroup

DER Cybersecurity Certification Procedure — Complete

- **Defined standardized procedure for DER vulnerability assessments.**
- Leads: Danish Saleem (NREL) and Cedric Carter (MITRE)
- Publication: "Certification Procedures for Data and Communications Security of Distributed Energy Resources"
- Future work: Expected development within UL 2900-2-4 STP

Secure Network Architecture — Complete

- **Created DER reference architecture best practice.**
- Lead: Candace Suh-Lee (EPRI)
- Publication: "EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design"
- Future work: Risk-based approach adopted in IEEE 1547.3

Data-in-Flight Requirements — Complete

- **Encryption, authentication, and key management requirements.**
- Lead: Ifeoma Onunkwo (Sandia)
- Publication: "Recommendations for Trust and Encryption in DER Interoperability Standards", "Recommendations for Data-in-Transit Requirements for Securing DER Communications".
- Future work: IEEE 1547.3 update, IEEE 2030.5 revisions.

Access Control — Complete

- **DER Role-Based Access Control recommendations.**
- Lead: Jay Johnson (Sandia)
- Topics: Access control taxonomy and security models
- Publication: "Recommendations for Distributed Energy Resource Access Controls"
- Follow-on: Added recommendations to IEEE 1547.3 Guide

Patching Requirements — Complete

- **Establishing patching guidelines for DER devices.**
- Lead: Jay Johnson (Sandia), Ingo Hanke (SMA)
- Publication: "Recommendations for Distributed Energy Resource Patching"
- Follow-on: Added recommendations to IEEE 1547.3 Guide

Utility/Aggregator Auditing Procedure — Starting

- **Creating recommended auditing practices for DER networks.**
- Planned for Oct 2021. Lead: TBD
- Topics: Step-by-step auditing procedure for internal or external compliance review. Recommend data for attack forensics.

Related Activity: Blockchain Workgroup

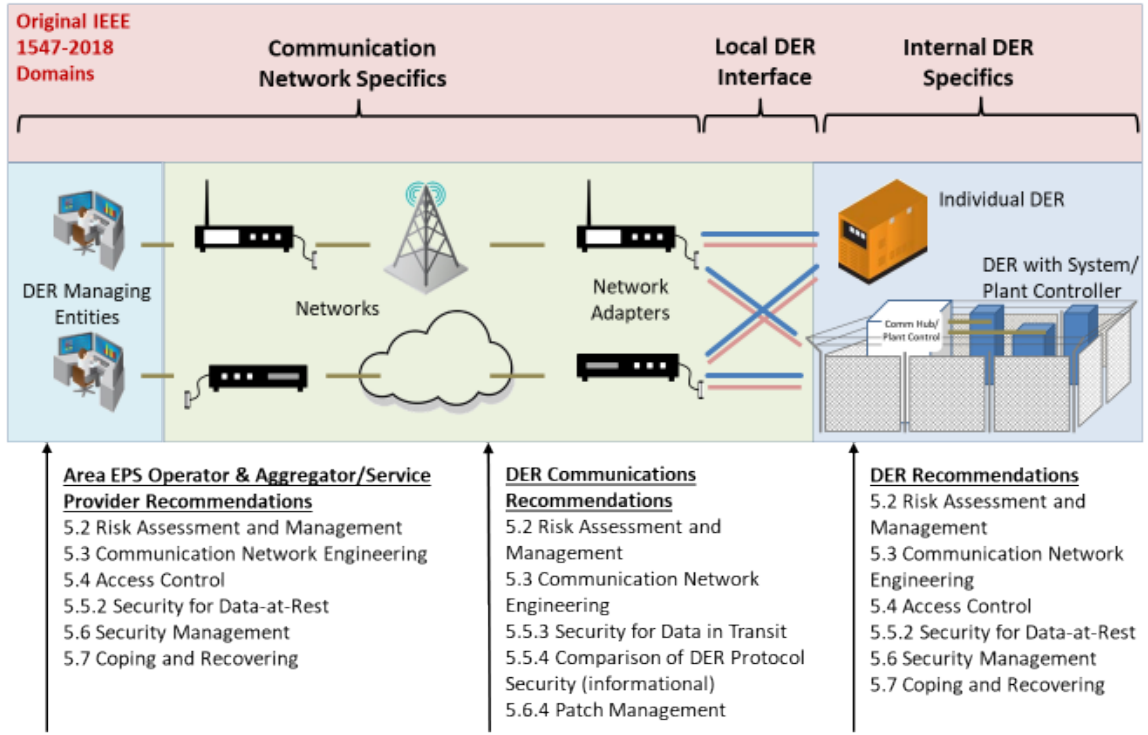
- **Defined requirements and specifications for using blockchain to ensure the security of private keys in DER manufacturing environments.**
- Leads: Jörg Brakensiek (Wivity) and Alfred Tom (Wivity)

Workgroup information: https://sunspec.org/cybersecurity-work-group/
Email: support@sunspec.org to participate!

DER Cybersecurity Standardization

IEEE 1547.3: Guide for Cybersecurity of DER Interconnected with Electric Power Systems

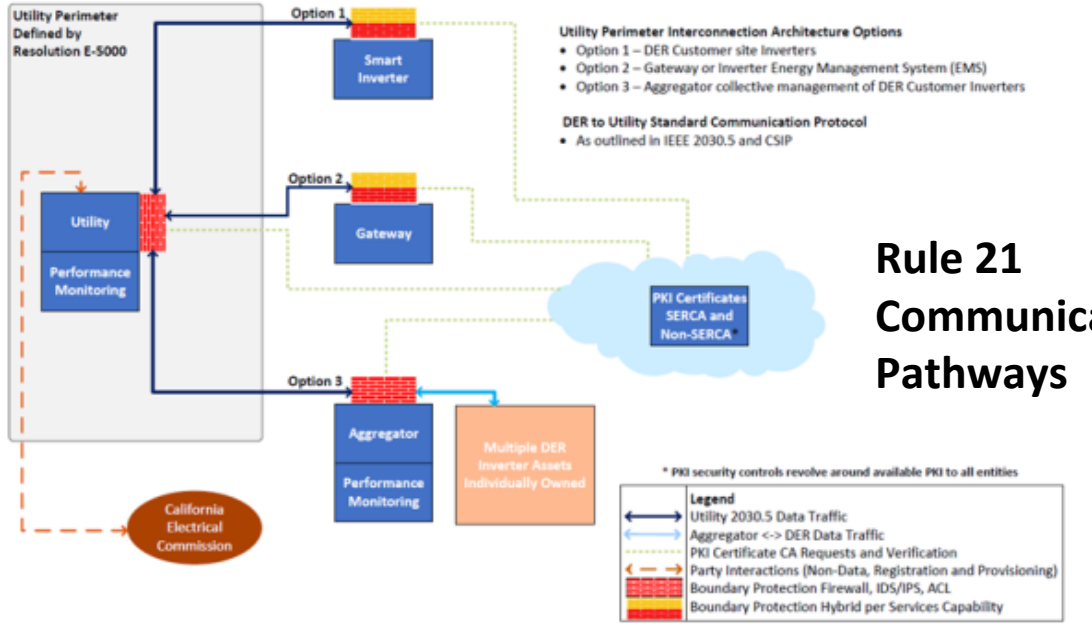
- **Recommendations for utilities, vendors, and aggregators for securing DER systems**
- **Balloting planned for late 2021**



IEEE 1547.3 Scope with Clause 5 Recommendations

California Electric Rule 21

- **CPUC Resolution E-5000 required Utilities (SCE, PG&E, SDG&E) to meet with stakeholders to address cybersecurity concerns.**
- **IOU goal: Create a *Utility Cybersecurity Requirements Guide for Communication to DER Facilities*. Current topics being debated within workgroup:**
  - **Boundary Protection**
  - **Communication Protocols**
  - **Cipher Suites**
  - **Certificates**
  - **Authentication, Authorization and Access Control**
  - **Registration and Provisioning**
  - **System Logs and Reporting Mechanisms**
  - **Malicious Code Protection**
  - **Zero-trust models**



Rule 21 Communication Pathways

Electric Vehicle Red Team Assessments

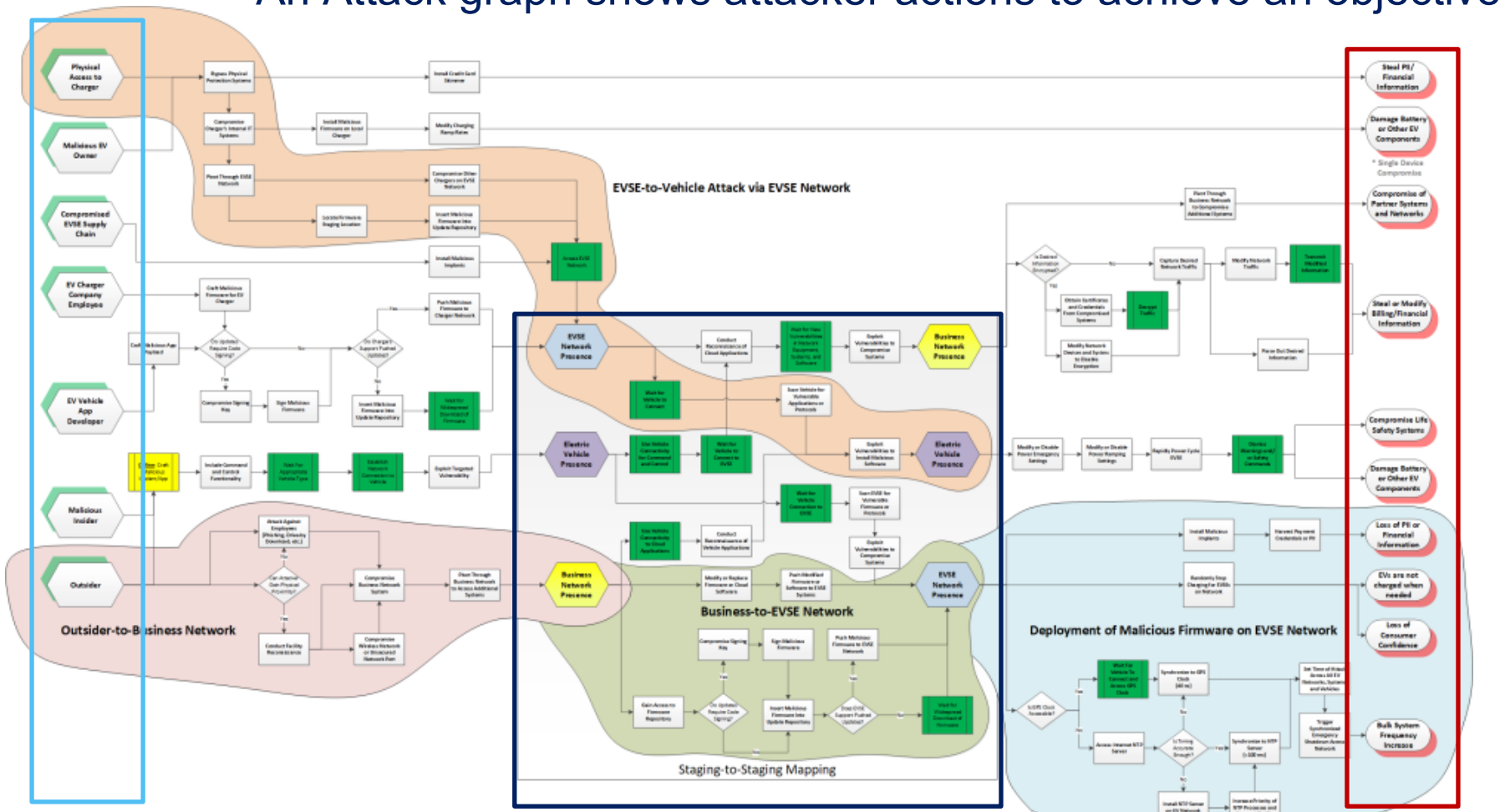
Sandia, PNNL, and ANL have a DOE Vehicle Technologies Office-funded project to secure EV chargers

- Working with EV charger vendors to understand vulnerability/risk landscape
- To date, the red team has investigated:
  - 8 DCFCs and 4 Level 2 chargers (from 10 companies)
  - 2 backend networks
  - OCPP 1.6 and ISO 15118-2 PKI requirements
- Findings have been incorporated into best practices
  - Specific vulnerability information has been provided to industry partners
  - Partners have already addressed many of the findings, or incorporated changes/mitigations into product roadmaps
  - Specific details have been abstracted out of public recommendations

EV Supply Equipment (EVSE) Attack Graphs

- EV Charger Attack Graph
  - 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

An Attack graph shows attacker actions to achieve an objective



Access Points:
attacker starting locations

Staging Points:
network presence/pivoting

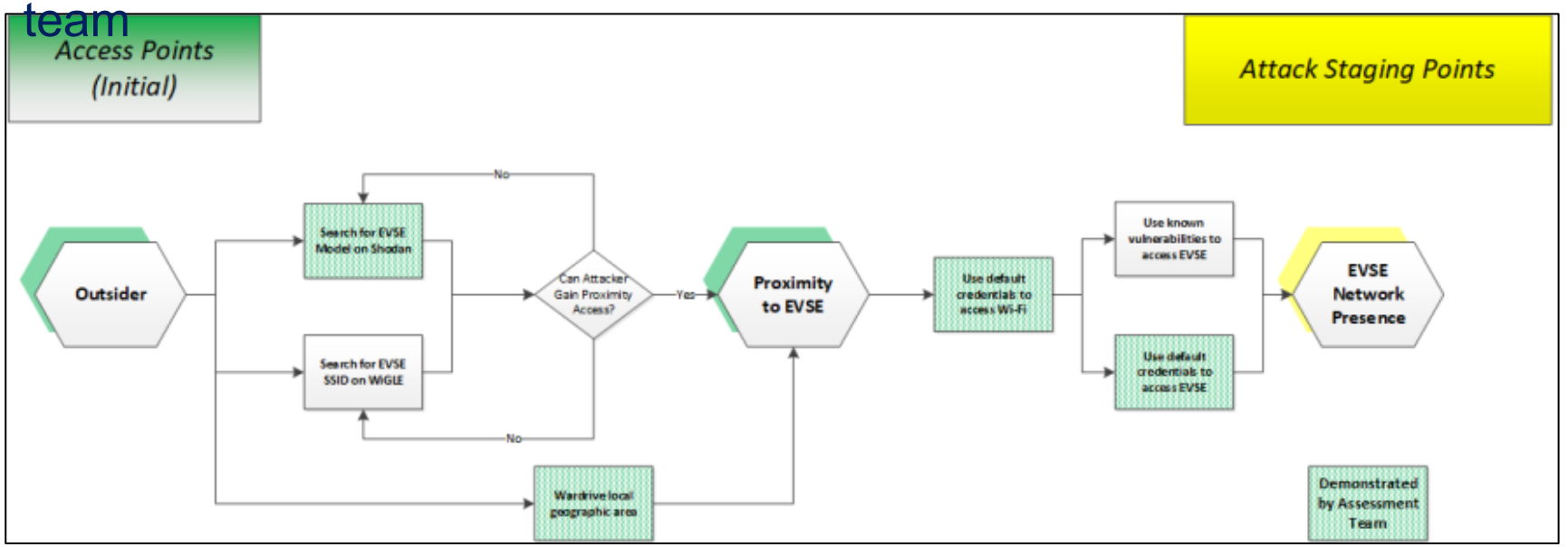
Consequences of Concern:
impacts

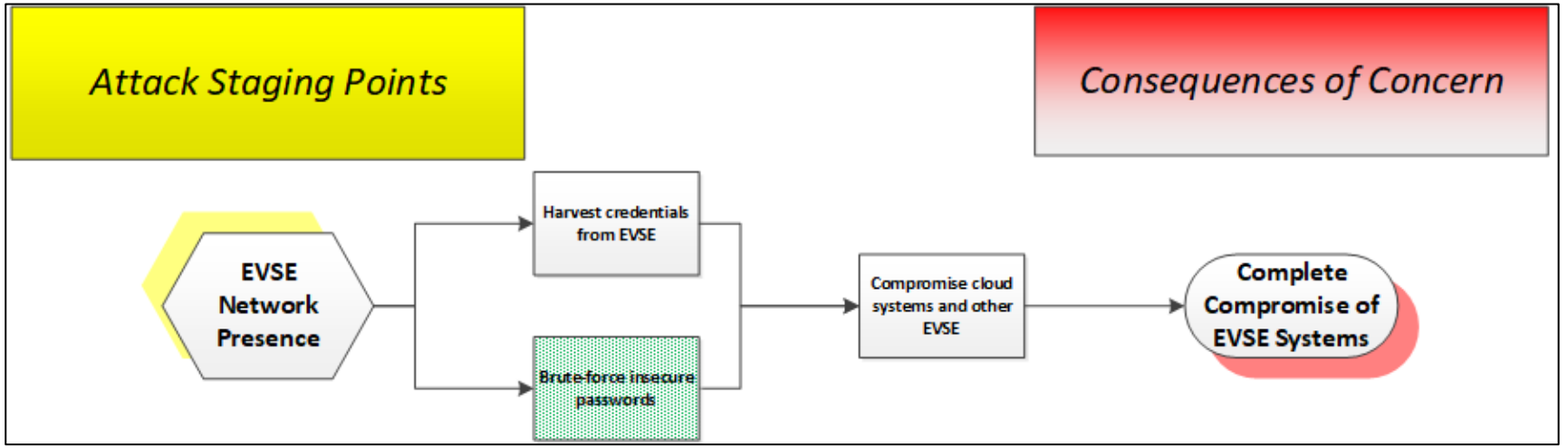
Details in B. Anderson, "Securing Vehicle Charging Infrastructure Against Cybersecurity Threats," 2020 SAE Hybrid and Electric Vehicle Symposium, Pasadena, CA, 28-30 Jan 2020. https://www.researchgate.net/publication/339053631_Securing_Vehicle_Charging_Infrastructure_Against_Cybersecurity_Threats

EV Charging Attack Graphs

- The green nodes have been successfully demonstrated on various EVSE models.
- Current testing is being done in partnership with an EVSE vendor.
- EVSE vendor is providing a replica of their cloud infrastructure for the assessment efforts.
- **Major Risk:** One EVSE owner was ***not aware*** of the Wi-Fi Access Point installed in the equipment.

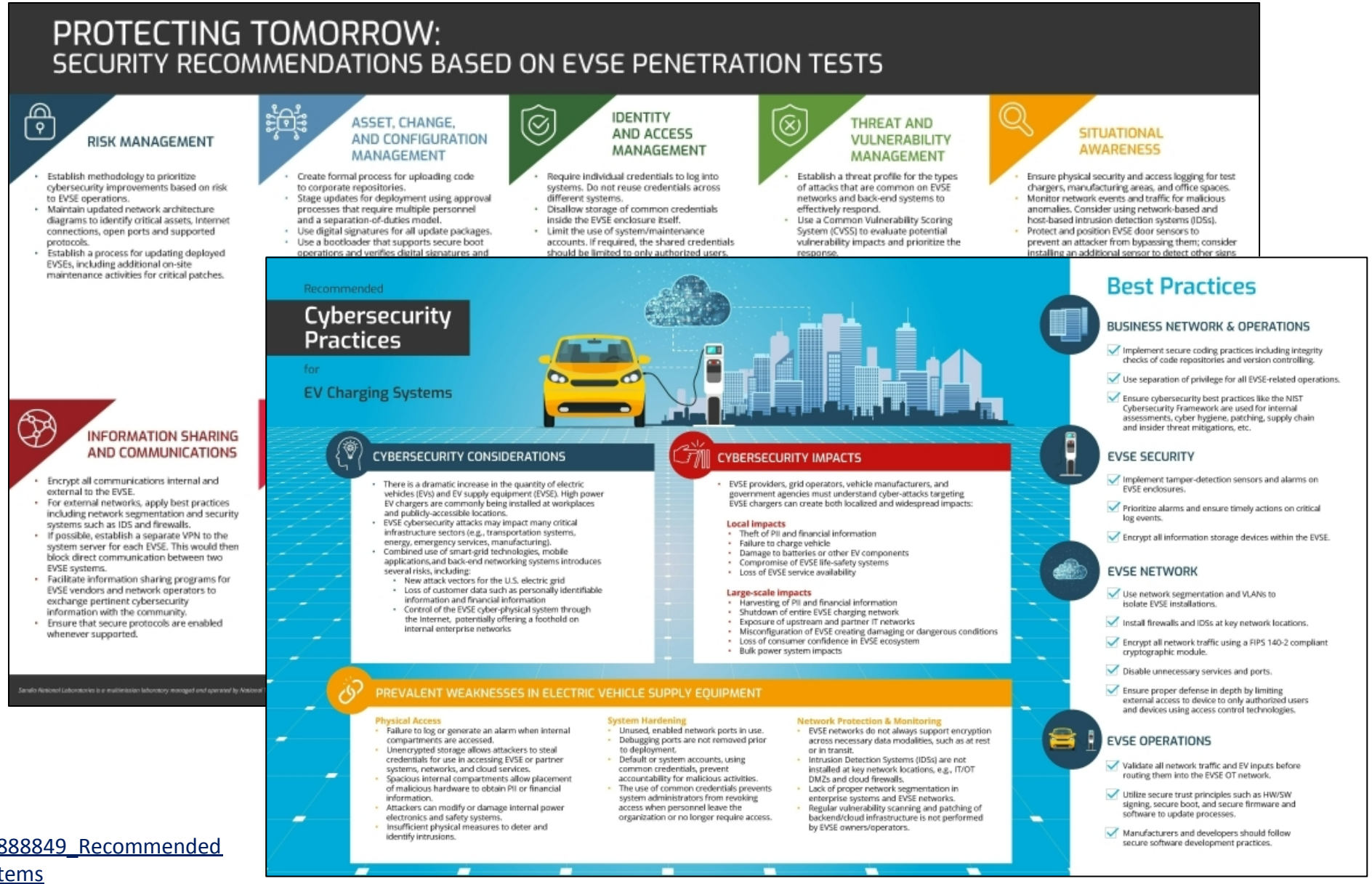
Specific graphs show the current attack path being investigated by the red team





Best Practices Infographic for Industry

- Guide is based on findings from hands-on assessments of systems
  - EVSE
  - Cloud systems
  - EVSE vendor and provider:
    - Business networks
    - Processes and procedures
    - Supply chain
- Covers all critical areas of the EVSE ecosystem in a single, concise document
- Provides the high-level view of the entire ecosystem ensuring critical security aspects are not overlooked
- There have been many recent public EVSE vulnerability disclosures.



https://www.researchgate.net/publication/344888849_Recommended_Cybersecurity_Practices_for_EV_Charging_Systems

Thank you!

Jay Johnson
Renewable and Distributed Systems Integration
Sandia National Laboratories
P.O. Box 5800 MS1033
Albuquerque, NM 87185-1033
Phone: 505-284-9586
jjohns2@sandia.gov