EVs @ Scale

U.S. Department of Energy

CyberPUNC (Cybersecurity Pillar for Unified National Lab Collaboration)

Deep-Dive Discussion:

Presenter: Barney Carlson

September 20-21, 2022

"CyberPUNC" Overview

- **Objective:**
  - Contribute to the continuously evolving cyber-physical security methods and solutions needed to ensure EV charging infrastructure safety, reliability, & resiliency.
- **Six National Labs:**

- **Four main project areas that focus upon challenges and barriers:**
  1. Implementation and utilization of the latest security methods
  2. Identify vulnerabilities in new technology features and standards
  3. Methods to identify, protect, detect, respond, and recover from cyber-physical security events impacting EV charging infrastructure
  4. Training for the EV charging infrastructure cybersecurity workforce

"CyberPUNC" Relevance

- **Relevance:**
  - Identify: Numerous assessment tasks focused on identification of vulnerabilities and impact severity
  - Protect: Security architectures, tool sets, and training of cybersecurity staff
  - Detect, Respond, & Recover: DOE funded VGI projects focused on mitigation solutions and strategies for EV charging safety, security, and resiliency

courtesy: NIST

"CyberPUNC" Deep-Dive Discussion Agenda

- **Session #1 – Sept. 20:**
  - INL - Overview of EVs@SCALE Cybersecurity Pillar
  - NREL - PKI vulnerability assessment
  - SNL - PKI assessment w/ Emulytics
  - PNNL - Quantum Computing encryption
  - PNNL - Zero Trust architecture
  - ANL - EVSE Cyber Security at Scale: A Look at Large-Scale Cyber Risks
  - Open discussion and collection of feedback
- **Session #2 – Sept. 21:**
  - ANL - Codes & Standards discussion
  - ORNL - Hardware-in-the-loop (HIL) cyber-physical security assessments and evaluation for high-power EV charging stations
  - NREL - EVSE Network Operators Risk Management Framework Tool
  - SNL - *CyberStrike* Training
  - INL - *CyberAuto Challenge*
  - INL - Cross-collaboration with other VGI projects
  - Open discussion and collection of feedback

"CyberPUNC" Industry Engagement

- **We're looking for technical feedback TODAY & TOMORROW**
  - Feedback on current tasks
  - Any missing tasks / proposed areas of focus?
  - Suggestions of prioritization?

- **Industry and Nat. Lab Collaboration is Highly Engaged**
  - Cybersecurity guidance and tools
  - Assessments to identify vulnerabilities
  - Pre-competitive research & development of mitigation solution
  - Training of the cybersecurity work force