Red Team Planning/Methodology

Bruno Leao, Tobias Ahlgrim, Siddharth Bhela, Daniel Grinkevich, Sindhu Suresh

Supervisory Parameter Adjustment for Distribution Energy Storage (SPADES) Workshop

Introduction

Red Team **goal**: design and implement attacks to adequately test developed cyber defense functionality

Comprehensive list of cyberattacks for power distribution grid → very large range of possibilities

Assumptions and requirements defined and discussed with the project team → **limit scope** focusing on what is relevant

Methodology for proper definition of attacks

At this point, Red Team information is shared with the whole team

Assumptions

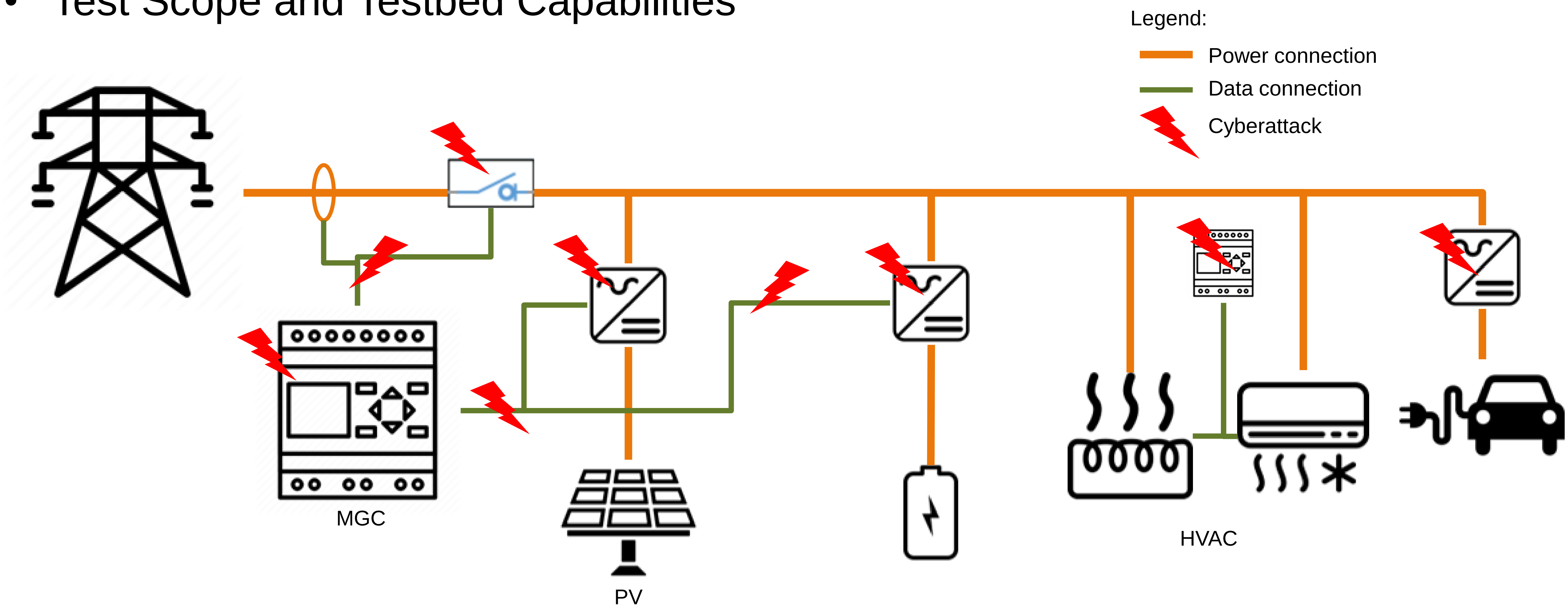
- Test Scope and Testbed Capabilities
- Power Grid Architecture
- Key Performance Indicators
- Attack Definition

Assumptions

- Test Scope and Testbed Capabilities
  - All tests are based on capabilities of PyCIGAR tool
  - Functional simulation (doesn’t include computational systems and network communication)
  - Attacks
    - Changes in functional behavior
    - Manipulations of data exchange
  - Time resolution: 1s (quasi-steady state simulation)

Assumptions

- Test Scope and Testbed Capabilities



Assumptions

- Power Grid Architecture
  - Initially using standard models
    - IEEE-37
    - IEEE-240 (IOWA-240)
  - NRECA models based on coop utilities
  - Only devices which can be used in quasi-steady state simulation

Assumptions

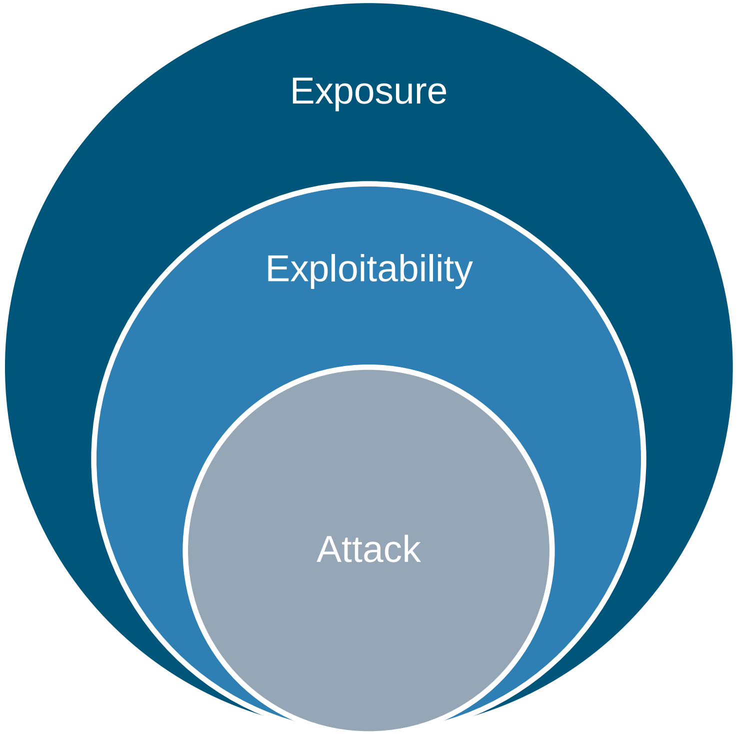
- Key Performance Indicators
  - What should a successful attack achieve?
    - Tier 1
      - Power delivery disruption
      - Instability (oscillation)
      - Imbalance
    - Tier 2
      - Equipment useful life degradation
      - Power quality degradation
    - Pending means for assessment/quantification

Assumptions

- Attack Definition
  - Pre-defined parameter set
  - Immediate impact in the system
    - Even for equipment useful life
  - Some attacks are out of scope
    - Switching off circuit
    - Adversarial machine learning (training)

Attack Budget

- Quantification of the effort or resources needed or available to execute an attack on a specific system, device, or component
- **Attack cost** has three layers
  - Exposure[1] (low, medium, high)
  - Exploitability[1] (low, medium, high)
  - The Attack (effort or skills needed for success)
- Type of attacker defines **attack budget and applicable layers**
  - Unskilled hacker or "script kiddie"
  - Skilled hacker
  - Security researcher / penetration tester
  - Malicious user (normal and privileged)
  - Nation state or malicious corporation sponsored attack



Pending means for assessment/quantification

1. Adapted from The Common Vulnerability Scoring System (CVSS) - Access Vector and Access Complexity

Attack Categories

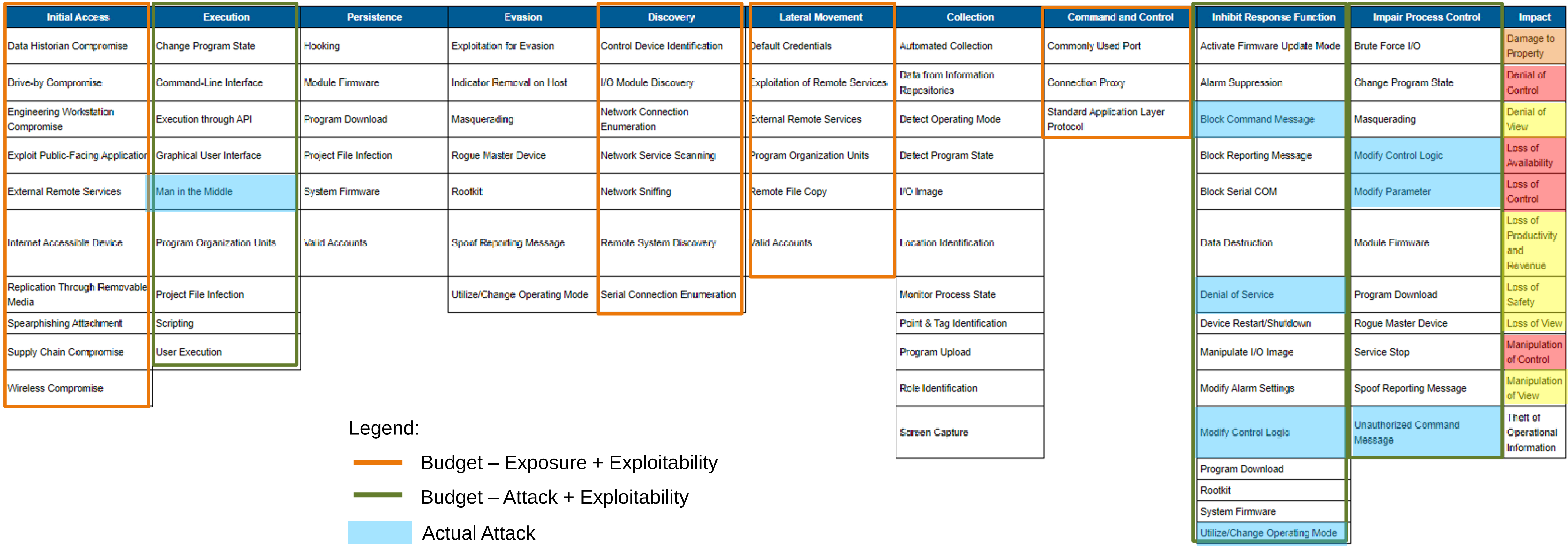
- Component Level
  - Attacks aiming at device functionality
  - Inverter, controller, breaker, protection devices, loads
- System Level
  - Attacks aiming at system level behavior
- Communication
  - Attacks at data exchange
- ML Controller (double-check with Dan)
  - Attacks specifically focused on the ML controller

Extended from: D. Wei et al. “Protecting Smart Grid Automation Systems Against Cyberattacks”, IEEE Transactions on Smart Grid, 2011.

Attack Categories

SIEMENS
Ingenuity for life

MITRE, ATT&CK for Industrial Control Systems



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Legend:

━ Budget – Exposure + Exploitability

━ Budget – Attack + Exploitability

🟦 Actual Attack

🟥 Tier 1 Impact

🟧 Tier 2 Impact

🟨 Achievable with additional info/assumptions

Other Aspects of Attack Definition

Attack Vector Implementation

- Manual Analysis
- RL-based automation/optimization (based on PyCIGAR)

Listing of envisioned attack vectors

Take into consideration specific battery operation use cases from utilities

- T&D Deferral
- Peak Shaving
- Backup Power / Grid Expansion

Conclusion and Future Work

- Assumptions and methodology for definition of attacks are almost done
  - Pending aspects will be discussed/defined right after workshop
- Preparation of report detailing Red Team approach (deliverable 12/31/2020)
- After report, start work towards:
  - Analysis of actual systems (pending definition)
  - Implementation of attacks (familiarize with PyCIGAR, analyze models when available and implement attacks)

SIEMENS
Ingenuity for life

Contact page

Bruno Leao

Siemens Technology

755 College Road East
Princeton, NJ 08540

USA

E-mail: bruno.leao@siemens.com

siemens.com