Advanced Metering Infrastructure Attack Methodology Document

Matthew Carpenter
ASAP Red Team Lead
matt@inguardians.com

Introduction to Attack Methodology

- Guide for consistent testing

- Authors:
  - Matthew Carpenter
  - Travis Goodspeed
  - Joshua Wright
- Editing and Technical Review:
  - Bradley Singletary
  - Ed Skoudis

Target Audience

- Utilities and Vendors
  - Security Teams
  - Internal Attack Teams
  - Management
- Third-Party Analysis Teams

Purpose and Scope

- Purpose:
  - – Consistent Testing Between Different Architectures
  - – Assist Utilities in Testing Their Own Systems
  - – Help Vendors Prepare
- Scope: Attacking Embedded Equipment
  - – Meters and Support Architecture
    - Not on the Utility Premise
  - – **Not** in scope: Utility Premise Systems
      - – ERP
      - – MDUS
      - – SCADA
      - – Head-Ends

Document Overview

- Principles of AMI Vulnerability Assessments
  - Instructing Testing Team
  - Quality Assessment Principles
- Lab Construction
  - Key equipment we will use to test
- Vulnerability Types
  - Specific vulnerabilities we will be looking for
    - Actual vulnerabilities found may not be in this list
- Attack Methodology

Attack Methodology

- Reconnaissance
  - Information Gathering
    - Identifying system components (mcus, eeproms, etc…)
    - Researching network infrastructure
- Initial Analysis
  - Shallow analysis of target device(s)
    - Fully assess key areas of interest
- Deep Analysis
  - Areas of interest as identified during Initial Analysis
- Exploitation
  - Combining “Possibilities” together to form Attacks

Got Vulns?

- Testing begins very soon...
  - Coming to a lab near you!

Questions?

Discussion?

matt@inguardians.com

AMI-SEC Collaboration Site

http://osgug.ucaiug.org/utilisec/amisec