The Center for Cyber Defenders

Expanding Computer Security Knowledge

DHS Critical Spares

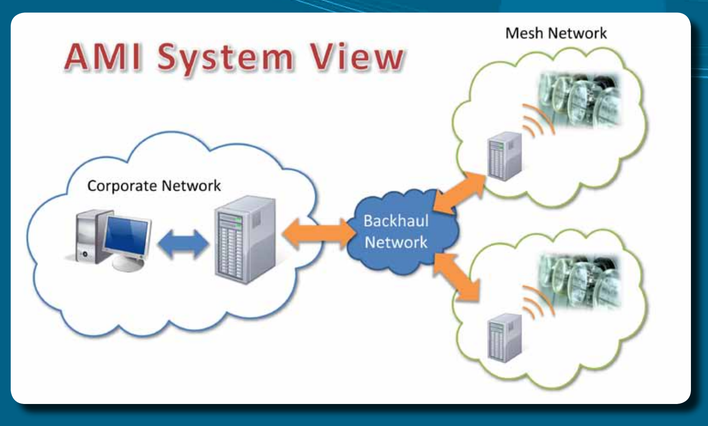
Brian Pendleton, Brigham Young University; Elizabeth Walkup, University of Tulsa;
Ryan Birmingham, Missouri University of Science and Technology

SAND2011-4967P

Project Mentors: Abe Clements, 5621; Bryan Richardson, 5628

Problem Statement:

- **Project Overview — AMI Assessment**
  - The goal of the DHS Critical Spares project is to ensure that critical infrastructure is adequately secured against failure and attack. Our portion of the project is to evaluate the security of a commercial Automated Metering Infrastructure (AMI) "smart meter" system. It is being deployed in the field using an adversary-based methodology known as **Red Teaming**. This project will help to ensure that our national infrastructure remains secure.
- **Technical Challenges**
  - Quickly characterize a complex system with many components
  - Identify potential targets and attacks against them
  - Model adversary capabilities
  - Identify attack mitigations

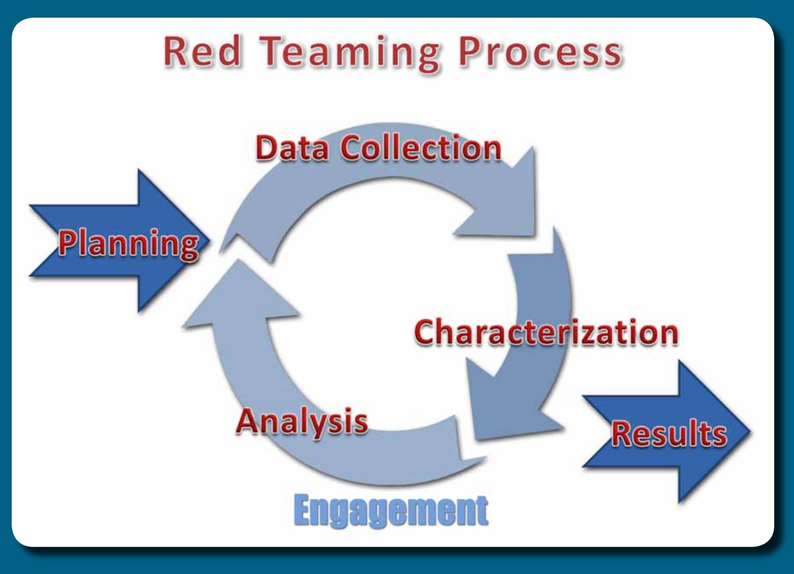


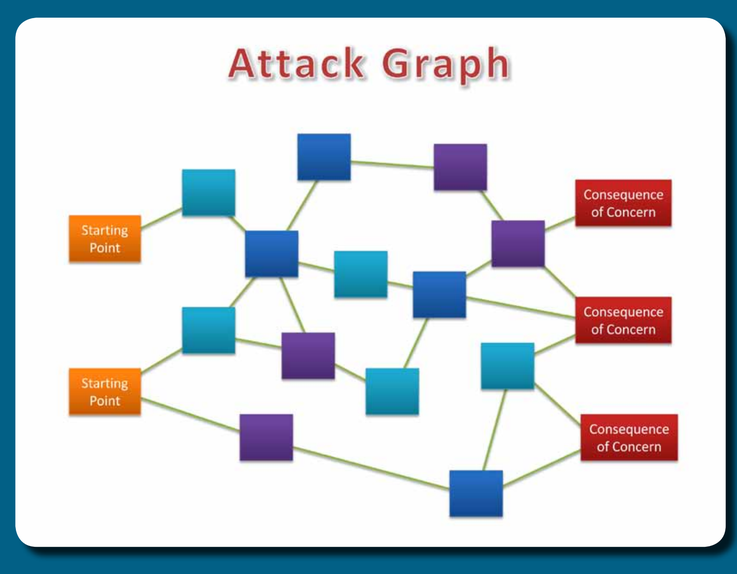
Red Teaming Overview:

- **Red Teaming** consists of authorized, adversary-based assessment of a system for defensive purposes
- **Planning**
  - Understand the customer's goals for the assessment
  - Determine what resources will be needed to conduct the assessment
- **Data Collection**
  - Validate the information about the system provided by the customer
  - Gather additional information about how the system works
- **Characterization**
  - Develop views of the system: Physical, Spatial, Logical, Temporal, Functional, Data Flow, and Consequence
  - Look for risks in the system both before and after attack mitigations are applied
- **Analysis**
  - Build an attack plan that exploits weaknesses in critical parts of the system
  - Test and record how the system responds to the attack
- **Reporting**
  - Keep detailed records of everything that is done during the assessment, informing the customer of: methodology, adversary model, understanding of the system, and the conclusion or mitigation strategies and any other relevant data

Benefits and Goals of the Assessment:

- **Vendor Benefits**
  - Gain a better understanding of their system and how it could be used or misused by an attacker
  - Determine which of their defenses and practices are effective and which are not
  - Learn how they could make the "smart meter" system more secure in the future by finding vulnerabilities and recommending mitigations
  - Determine critical system assets and how they can be kept online in a crisis
- **Utility Benefits**
  - Learn how they should configure the system when they are installing it
  - Determine what defenses they need to provide in their networks
  - Determine where defensive efforts and spares/backups should be focused
- **Red Team Benefits**
  - Gain experience
  - Learn new skills
  - Establish a baseline for evaluating the DHS Critical Spares methodology
- **National Benefits**
  - Ensure that the country's critical infrastructure is secure





Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-4967P.