Identifying SCADA Devices and their Vulnerabilities on the IoT

SBE TTP: Medium: Securing Cyber Space: Understanding the Cyber Attackers and Attacks via Social Media Analytics

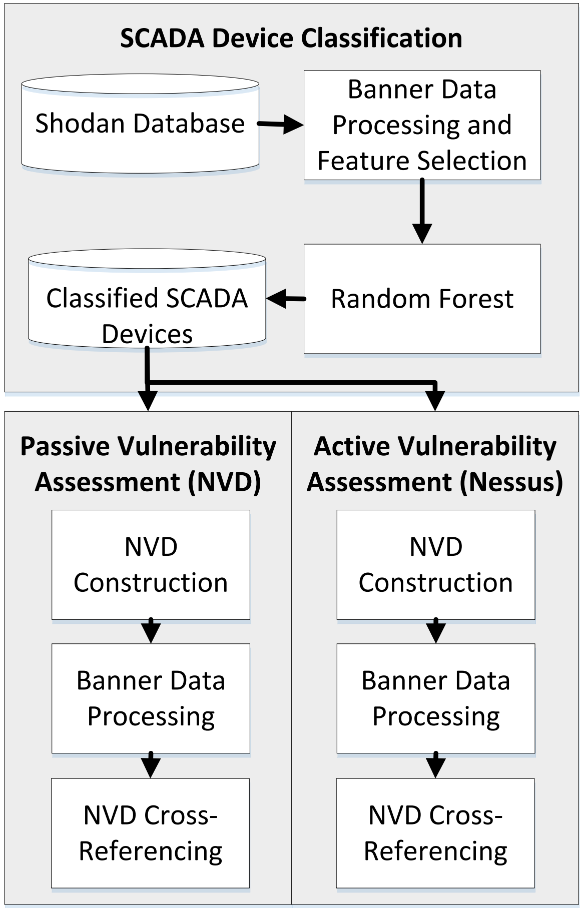
Challenge:

- SCADA systems supervise, maintain and control critical infrastructure (e.g., power plants).
- Little work has attempted to find SCADA devices and their vulnerabilities on the Internet of things (IoT).

Solution:

- Utilize a novel set of features from SCADA device data to train a classifier to identify SCADA devices.
- Leverage Nessus in a distributed framework to automatically identify vulnerabilities of the identified SCADA devices.

Project Number – NSF SES-1314631
Principal Investigators:
-Dr. Hsinchun Chen, University of Arizona
-Dr. Salim Hariri, University of Arizona
-Dr. Ron Breiger, University of Arizona
-Dr. Tom Holt, Michigan State University



SCADA Device Classification

Shodan Database → Banner Data Processing and Feature Selection → Random Forest → Classified SCADA Devices

Passive Vulnerability Assessment (NVD)

NVD Construction → Banner Data Processing → NVD Cross-Referencing

Active Vulnerability Assessment (Nessus)

NVD Construction → Banner Data Processing → NVD Cross-Referencing

Artificial Intelligence Lab
Management Information Systems

Scientific Impact:

- This project contributes to the cybersecurity landscape by identifying potentially devastating vulnerabilities of SCADA systems on the IoT.
- Researchers will have better knowledge on techniques, and tools to automatically identify and assess SCADA vulnerabilities.

Broader Impact:

- Preliminary results show that 4,009/20,461 (19.59%) of devices are susceptible to vulnerabilities such as default credentials, script execution, and Modbus coil access.
- Attacking these devices may have devastating consequences on the infrastructure, and in turn, society.
- Identifying and mitigating these vulnerabilities will ensure a safer cyber space and society.