Defending a SCADA System with the Snort IDS

Michael Kouremetis
Advisor Dr. Remzi Seker
ECSSE Department
Contents

- SCADA Systems
  - Components
- Threats to SCADA Systems
- Design
  - Remote Terminal Unit- Arduino Uno
  - Command Server
- Intrusion Detection Systems
- Snort
- Attack Methods
- Snort Measures
SCADA System

- Supervisory Control and Data Acquisition System
- Industrial Control System
  - Infrastructure
  - Utilities
  - Factories/Facilities
  - Transportation
SCADA - Components

- Supervisory System - receive data and issuing commands
- Remote Terminal/Telemetry Units (RTU) - acquire sensor data and send (digital) data to Supervisory System
- Programmable Logic Controllers (PLC)
- Communication Infrastructure
- Human Interface/Terminal
RTU/PLC- Arduino Uno

- Simple Microcontroller- C Programming Language
- Ethernet Shield-for Ethernet(TCP) connectivity
- LEDS-represent system process
- Motion Sensor- data input
RTU/PLC- Arduino

LED’S

Motion Sensor

Arduino Uno
Supervisory System - Control Server

- Ubuntu 8.04 (Hardy Heron)
- Java SE 6 - Server Application
SCADA Network Design

Control Server

Router

Internet

<- Sense Motion, Request operation

Send command to be implemented->

SCADA-Arduino
Attack Methods

- Denial of Service/Distributed Denial of Service
  - Slow down RTU’s
  - Delay command signals

- Man-in-the-Middle (MITM) Attack
  - Un-encrypted traffic (not uncommon in real applications)

- Obtain Root Control on Command Server
  - PLC’s are by design re-programmable

- Insider Attacks

- Many SCADA systems have components with open internet privileges, no security (forgotten systems)
IDS- Intrusion Detection Systems

- Monitors network or system for malicious behavior in effort to detect intruders
  - Addressing
  - Data Content
  - Traffic Levels
  - Internet/Network Protocols

- Types
  - Passive/Reactive
  - Signature/ Anomaly /Hybrid
  - Hosts/Network
Snort

- Network IDS
- Signature Based
- Traffic Analysis and Real-Time logging
- Primary strategy is rules
Snort - Rules

alert tcp any any -> any 80 (msg:"Web Traffic"; content:"GET";)

Diagram Source: The Security Analysts, secanalyst.org
Network Design 1 w/ Snort

Diagram showing:
- Internet
- Router 1
- IDS
- Server
- SCADA-Arduino
- Attacker

The diagram illustrates a network design with Snort installed on the IDS system, connected to Router 1, which in turn connects to the Internet and other network components.
Network Design 2 w/ Snort

Diagram:
- Internet
- Router 1
- IDS
- Attacker
- SCADA-Arduino
Snort Solution

- **Rule Sets**
  - Current/Updated – large support community
  - Specifically mapped to attack signatures

- **Low Costs**
  - Free Software
  - Windows/Linux Machines (older)
  - Avoid purchasing firewall software/hardware, VPN security
Questions?