OAK RIDGE National Laboratory

Tools, Techniques, and Methodologies: A Survey of Digital Forensics for SCADA Systems

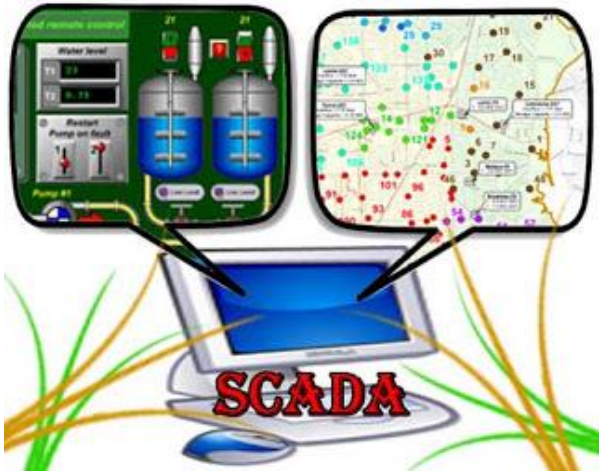
Presenters: Rima Asmar Awad, Saeed Beztchi
Co-Authors: Jared M. Smith, Stacy Prowell, Bryan Lyles

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

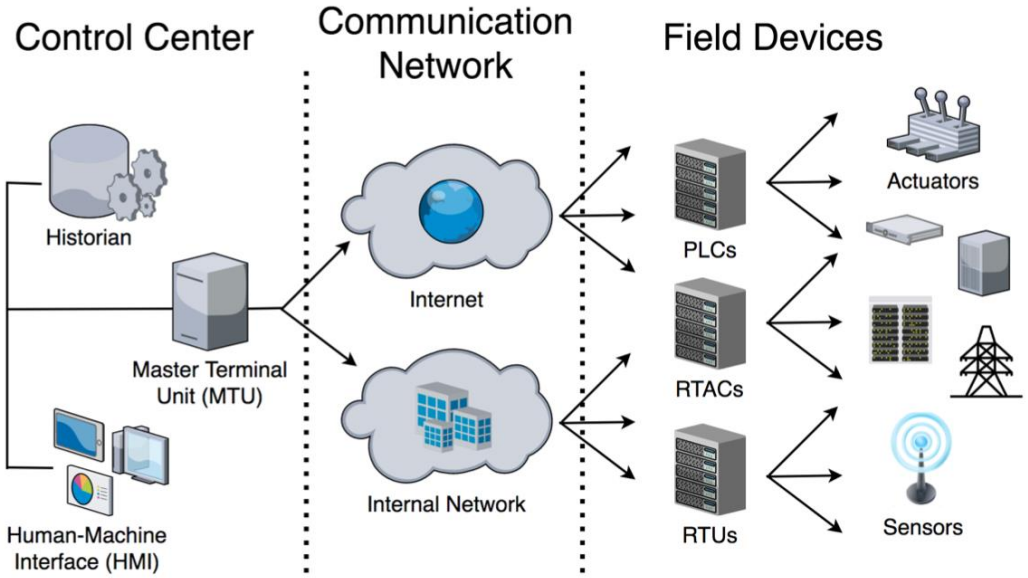
U.S. DEPARTMENT OF ENERGY

Overview

- Supervisory control and data acquisition (SCADA) system
  - Type of control system that is spread over a wide area and can supervise individual components
- Early SCADA systems were intended to run as isolated networks
  - Simple I/O devices to transmit signals between master and remote devices



SCADA Architecture



The Problem …

- Today's SCADA system evolved to communicate over public IP networks, or directly to the internet in some cases
- Sabotaging /compromising SCADA systems requires security analysts to get to the root cause of the attack as quickly as possible

The Problem …

- Most data collection and forensic analysis systems focus on the traditional IT infrastructure and the communication networks
- Very little forensic works focus on SCADA devices
- No known methodology to safely acquire live data on SCADA system without interrupting the service

SCADA Cyber attacks

- Stuxnet, discovered in 2010 and infected 50,000 to 100,000 computers around the world
- BlackEnergy appeared first in 2007 with DOS functionality
- Crash Override, known in 2016 as the first malware designed to attack electric grid system

Challenges - Technical

- Deterministic network traffic
- Customized operating system kernels
- Resources constrained devices
- Inadequate logging
- Extensive lower data

Challenges - Research

- Using simulation
- Building small-scale SCADA systems
- Industry collaboration

Survey List

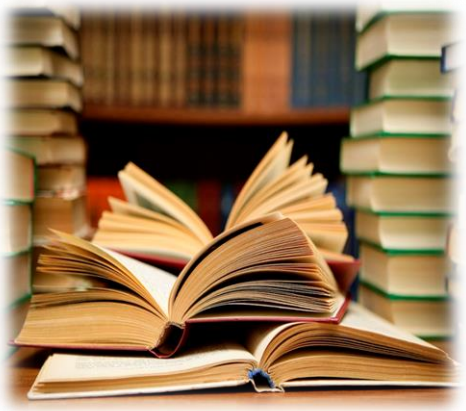


Figure 1: Overview of the Architecture of a Typical SCADA Environment

Category	Specific Domain, Device, or Protocol	Reference
Technical Challenges		van der Knijff [42], Stüttgen *et al.* [37], Iqbal *et al.* [21], Kilpatrick *et al.* [24]
Research Challenges		van der Knijff [42], Ahmed *et al.* [2], Slay *et al.* [33], Vaughn *et al.* [44]
Frameworks/Methodologies	Sensor Networks	Cardenas *et al.* [6]
	Events and Logging	Taveras *et al.* [38]
	Siemens S7 PLC	Yau *et al.* [47]
	Attacks against PLCs	Chan *et al.* [7]
	Incident Response	Eden *et al.* [15]
	Data Retrieval and Incident Response	Eden *et al.* [13]
	Applying Existing IT Tools to SCADA, Case Study on USB-based Attacks	Betts *et al.* [4]
	Data Retrieval	Stirland *et al.* [36]
	Live Data Acquisition	Ahmed *et al.* [3]
	Integrating with Legacy Systems, Network Protocol Analysis	Chandia *et al.* [9]
	Network Data and Device Memory Acquisition/Data Retrieval	Van Vliet *et al.* [43]
	Large-Scale Multi-Protocol and Device Testbed	Adhikari *et al.* [1]
Network Forensics	Fuzzing DNP3 and Modbus	Devarajan *et al.* [12]
	Siemens S7 PLCs	Kleinmann *et al.* [25]
	Wireless Sensor Networks, Multi-Agent Systems	Elhoseny *et al.* [16]
	DNP3, Modbus, Snort IDS	Valli *et al.* [41]
	Firewalls and Network Segmentation	Mittal *et al.* [29]
	GE-SRTP Protocol, GE Fanuc Series 90-30	Denton *et al.* [11]
Device Forensics	Data Retrieval, Differential Analysis	Gougeon*et al.* [20]
	Water Treatment Testbeds, Sensor State	Junejo *et al.* [22]
	PLCs, Memory Analysis (addresses)	Yau *et al.* [48]
	Siemens TIA Portal, Logging and Event Collection	Chan *et al.* [8]
	Siemens S7-1200 PLC, Ladder Logic, Data Retrieval	Yau *et al.* [46]
	File Analysis, Package and Dependency Analysis	Schlegel *et al.* [31]
	Siemens S7 PLC, Memory Analysis (addresses)	Wu *et al.* [45]
	PLC Firmware Analysis, Baseline Creation	McMinn *et al.* [28]
	Programmable Controller Communication Commands (PCCC), File Analysis	Senthivel *et al.* [32]
	JTAG data capture, Memory Analysis (raw dumps), Offline Analysis	Breeuwsma *et al.* [5]

Table 1: Summary of Reviewed Literature

State of the Art

- SCADA forensics can be done on different levels of the system:
  - Control Center
  - Communication Network
  - SCADA Device

Control center Forensics

- Control centers are often composed of traditional IT-based OS's, such as Windows or Linux
- Retrieving data in a live manner has been well-addressed by many existing forensics tools
    - Volatility
    - Rekall
    - EndCase
    - Redline

SCADA Frameworks/Methodologies

SCADA Live Forensics: Real Time Data Acquisition Process to Detect, Prevent or Evaluate Critical Situations (Taveras et al.)

- Proposes model with a finite state automaton as an agent to monitor SCADA events in real-time
  - Events compared against set of rules to determine changes
  - Agent can switch to forensic mode to log the information for use in a forensic investigation

SCADA Frameworks/Methodologies

A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure (Eden et al.)

- Presents overview of SCADA forensics process
    - Proposes model for SCADA incident response and improvements

Forensic Readiness for SCADA/ICS Incident Response (Eden et al.)

- Identifies assets of system and provides tools for data retrieval
    - Discusses stages during an incident response process and order in which volatile data needs to be acquired to maintain data integrity and prevent losing useful data

SCADA Network Forensics

Unraveling SCADA Protocols: Using Sulley Fuzzer (Devarajan et al.)

- Present the Sulley fuzzer for SCADA systems
  - Detects protocol anomalies, unauthorized communication, and DDOS
  - Various components including agents to monitor SCADA network communication and logging PCAP files

Accurate Modeling of The Siemens S7 SCADA Protocol For Intrusion Detection And Digital Forensic (Kleinmann et al.)

- Describe the packet parsing and protocol models needed to build an IDS for networks with Siemens S7 PLCs
  - Describes packet formats
  - Proposes a DFA model for interpreting traffic
  - Evaluation is mildly positive, though had one percent false positive rate

SCADA Network Forensics

Secure Automated Forensic Investigation for Sustainable Critical Infrastructures Compliant with Green Computing Requirements (Elhoseny et al.)

- Addresses challenging nature of SCADA systems and the need for SCADA forensics automation
  - Propose a framework for an automated forensic framework for SCADA networks
    - Takes live data acquisition into consideration
    - Based on emerging technologies (MAS, WSN)
    - Two phases: Phase one preserves live data, phase two launches offline agents

SCADA Network Forensics

Snort IDS for SCADA Networks (Valli et al.)

- Used open-source tools to provide network analysis for SCADA systems
  - DNP3 and MODBUS
    - Main protocols examined
  - Involves methodology for SCADA systems to be provided with robust IDS system
    - Testing for vulnerabilities
  - Determined mitigation can be employed if an attack is later recognized

SCADA Network Forensics

Leveraging the SRTP protocol for over-the-network memory acquisition of a GE Fanuc Series 90-30 (Denton et al.)

- Examine GE-SRTP protocol, used by General Electric
  - Reverse-engineered and analyzed, can change logic of program
  - Tool for PLC to read memory and access to memory registers

SCADA End-point Device Forensics

Forensic of Embedded Systems using JTAG (Breeuwsma et al.)

- Extract raw memory dumps of end-point device using JTAG port
  - Memory dump can be analyzed offline

Towards a SCADA Forensics Architecture (Wu et al.)

- Forensics model for SCADA systems to gather and analyze data from hardware
  - Process consists of preserving and documenting the digital evidence
  - Siemens S7 PLC used to show changes in certain memory addresses over time

SCADA End-point Device Forensics

Detecting anomalous behavior of PLC using semi-supervised machine learning (Yau et al.)

- Tackle challenge of different PLC architectures with OCSVM and semi-supervised machine learning algorithm in model
  - Accurately determine abnormal behavior
  - OCSVM classifies anomalous behavior from trained model of normal operations
  - Architecture understanding is solved by obtaining certain memory addresses
  - Values used to train model to target events

SCADA End-point Device Forensics

A Firmware Verification Tool for Programmable Logic Controllers (McMinn et al.)

- Developed tool that captures serial data during firmware upload and compares with benign baseline version
  - Does not require any modification to SCADA system
  - Capable of creating a protocol profile to emulate future communication without the presence of a PLC

SCADA End-point Device Forensics

Memory Carving in Embedded Devices: Separate the Wheat from the Chaff (Gougeon et al.)

- Discusses how data stored on embedded devices can be useful for forensic investigations
  - Can be obtained with no authentication using API
  - Raw data not simple to interpret
- Automatic recognition technique
  - Performs differential analysis
  - Dumps of devices using same application, “boosting”
  - Claim 99.8% recognition of meaningful data

SCADA End-point Device Forensics

Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning (Junejo et al.)

- Incorporate Secure Water Treament (SWaT) testbed to find PLC vulnerabilities
  - ML based intrusion detection application
  - Sensor and actuation states saved into historian
  - Dataset divided into training and testing with ten unique attacks on each
  - Possible zero-day attacks

Discussion

- Much work has been done to illustrate the challenges of effective forensics in a SCADA environment
    - The community needs to push towards developing more practical, experimentally tested, and generally applicable tools and techniques
- The majority of the proposed frameworks suffer from being too high-level or lack practical evaluation
    - For the frameworks with case studies or experimental methodologies, there are often not immediate paths forward for building generally useful tools to accomplish the goals claimed by implementing the proposed framework

Recommended Future Work

- Future work should continue to push forward methods to analyze specific device state
  - Memory, firmware, packages, and other forensic data,
  - Not only targeting the network communications.
- A goal should be to construct security primitives, forensic tooling, and methodologies that apply to many devices and protocols
  - Researchers should strive to find unifying principles and methods to build tools that function for multiple devices and communication protocols

Conclusion

- With the rise of attacks against critical infrastructure and Industrial control systems, security practitioners must leverage digital forensics in increasingly complex ways
- Collecting, aggregating, and analyzing forensics data, breaches and attacks are able to be discovered and remediated
- There exists a significant gap in the complexity, generality, and versatility of forensics tools, techniques, and methodologies for SCADA environments
- Researchers need to continue focusing on building general tooling for SCADA forensics, extend their work beyond high-level, architectural frameworks, and focus on enabling forensics for SCADA field devices beyond the network communications alone

Thanks!

Rima Asmar Awad - awadrl@ornl.gov
Saeed Beztchi - beztchisa@ornl.gov
Jared M. Smith - smithjm@ornl.gov
Bryan Lyles - lylesjb@ornl.gov
Stacy Prowell - prowellsj@ornl.gov