A Model-based Approach to Self-Protection in SCADA Systems

Sherif Abdelwahed, Qian Chen
Electrical and Computer Engineering
Mississippi State University

9th International Workshop on Feedback Computing
JUNE 17, 2014 • PHILADELPHIA, PA
usenix

MISSISSIPPI STATE UNIVERSITY

Outline

- Introduction and Related Works
- Self-protecting SCADA Systems
- Case Study of the Water Storage Tank
- Conclusion and Future Work

Introduction

SCADA System

- Supervisory Control and Data Acquisition (SCADA) systems are a type of industrial control system (ICS) that adopts many aspects of Information and Communications Technology (ICT/IT) to monitor and control physical (cyber-physical) processes.
  - A SCADA system includes: sensors, actuators, programmable logic controllers (PLCs), remote terminal units (RTUs), human machine interfaces (HMIs), and master terminal units (MTUs).
  - Field devices such as PLCs and RTUs collect and convert sensor sourced analog measurements to digital data. The digital data are then sent back to MTUs via communication links (e.g., Internet, radio, microwave, and satellite).
  - In near real-time this data is processed by MTUs and displayed on HMIs to enable operators to make intervening control decisions.

Cyber Security Concerns of SCADA Systems

- Stuxnet Worm (2010): A root kit compromised PLCs to subvert the enrichment facilities ICS to temporally derail Iran's nuclear program by destroying roughly 1000 centrifuges.
  - Social engineering was used to carry a flash drive infected by the worm into the secure facilities.
  - Using stolen legitimate digital certificates from reputable companies, the worm implanted itself into the victims computing environment.
  - Using four different zero-day vulnerabilities to distribute and exploit Windows based computers.
  - Once detecting an installed HMI (e.g., Siemens SIMATIC PCS 7, WinCC, and STEP 7), carrying out a man-in-the-middle attack for sending fake commands to increase the operating speed of the Iranian IR-1 centrifuge from 1,064 hertz to 1,410 hertz for 15 minutes before returning to its normal running frequency.

Cyber Threats Facing SCADA Systems

- Vulnerabilities residing in:
  - Open and standardized protocols (e.g., Modbus, ICCP, and DNP)
  - Internet-based cyber communications.
- Security issues inherited from ICT/IT systems:
  - Operating System
  - Commercial-off-the-shelf applications

Related Works

- Intrusion detection systems (IDSs): detect and classify SCADA-specific attacks
  - ***Anomaly detection:*** comparing real-time system performance with the normal system model to detect known and zero-day attacks.
    - Mahalanobis distance
    - Neural networks
  - ***Signature detection:*** matching observations to misuse patterns of SCADA system behavior. This approach solely identifies and classifies known attacks.
    - Snort
- Most IDSs respond to attacks passively and suffer from the problem of high false alarm rates, which lead to improper responses and high performance overheads.

Contributions

- Designing a self-protecting SCADA system
  - Using the model-based approach to develop process control system model
  - Switching between fully-autonomous and semi-autonomous modes
  - Simple to configure and deploy
  - Supporting reliable, sustainable, and resilient self-protection performance
- Using a case study to validate the self-protection property
  - System Model
  - Intrusion Estimation
  - Intrusion Detection
  - Live Forensics Analysis
  - Intrusion Response

Contributions (Cont'd)

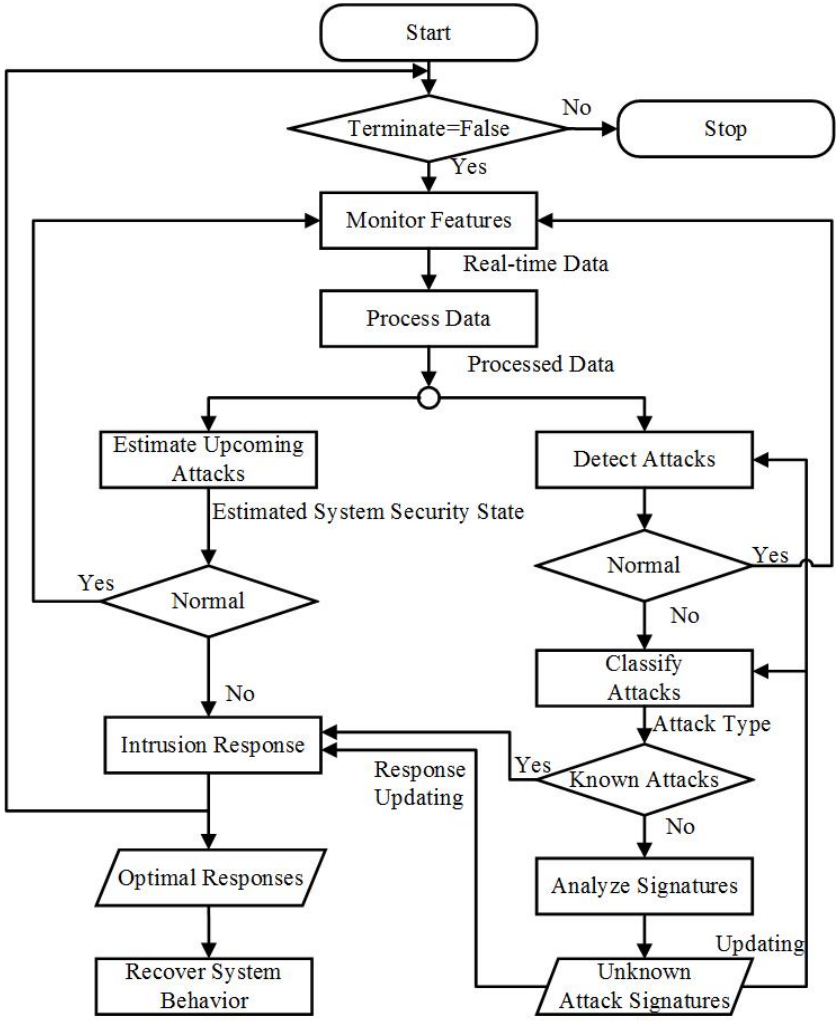
- Generic approach
  - Extending to protect various domain with few modifications
  - Without rebuilding the system or network architecture

Self-protecting SCADA Systems

9th International Workshop on Feedback Computing
JUNE 17, 2014 • PHILADELPHIA, PA
usenix

MISSISSIPPI STATE UNIVERSITY

The Outline of Self-Protecting SCADA System

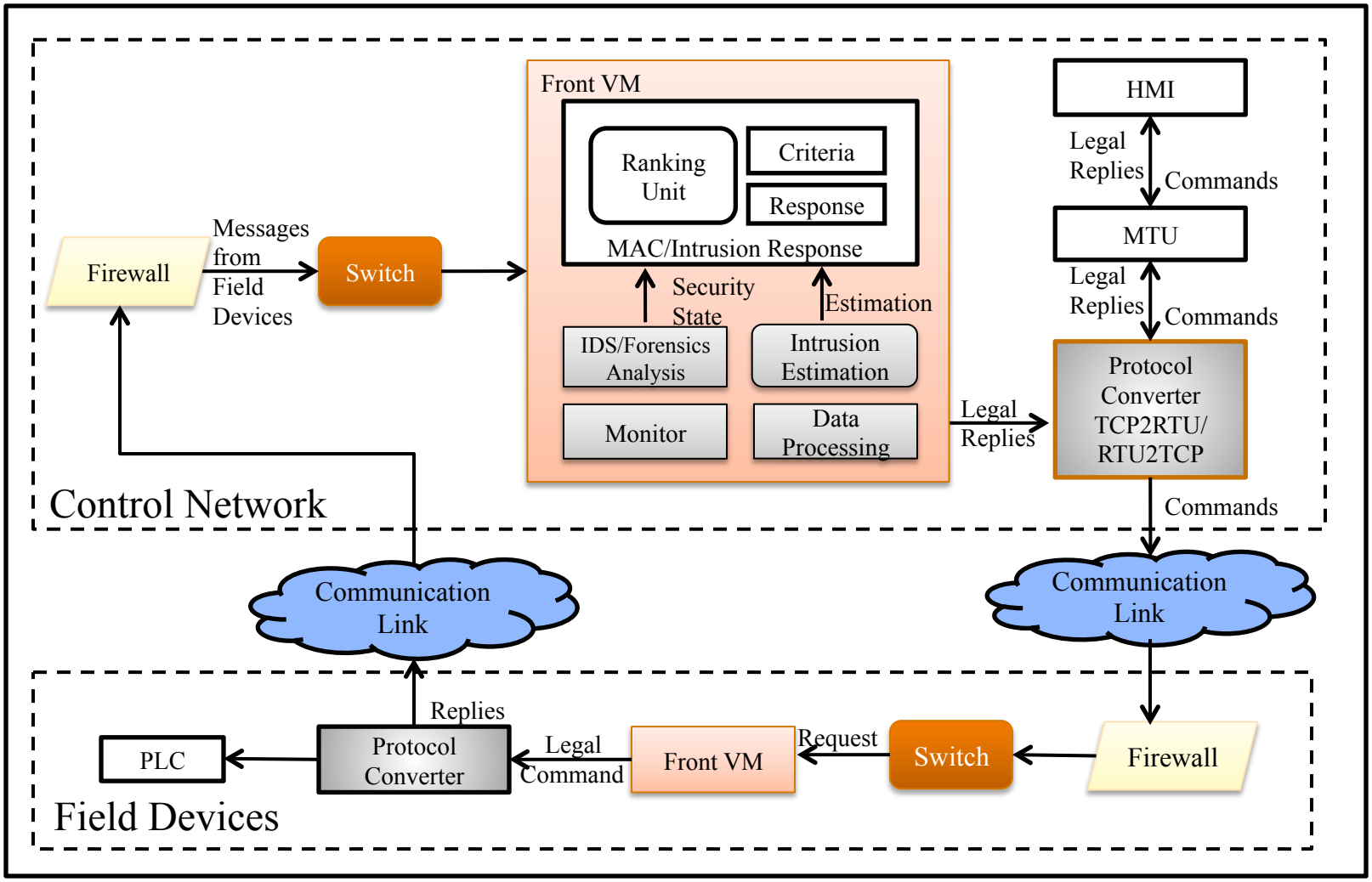


- Autonomic computing aims at self-protecting SCADA systems from cyber attacks with minimal human intervention.
  - estimating upcoming attacks and sending early warnings
  - detecting and classifying attacks
  - Investigating causes and impacts of zero-day attacks
  - autonomously or semi-autonomously implementing responses to eliminate cyber attacks.

9th International Workshop on Feedback Computing
JUNE 17, 2014 • PHILADELPHIA, PA
usenix

MISSISSIPPI STATE UNIVERSITY

The Self-Protecting SCADA System Architecture



Monitor and Data Processing

- The monitor module collects real-time data of the physical system performance and SCADA system security performance.
  - For a water storage tank, the selected feature includes:
    - water levels
  - For the security of SCADA systems, selected features include:
    - Modbus TCP/IP packet header
    - Protocol data units
    - TCP connection rates
- The data processing module processes measurements collected by the monitor module. The formatted and pre-processed datasets are then forwarded to the intrusion estimation and intrusion detection modules.

Intrusion Estimation

- The estimation module uses the historical observations of controlled variables of a physical model $\underline{\omega}(k-1,r)$ and selected security features of the SCADA system $\underline{\lambda}(k-1,r)$ to determine future performance of the physical system.

Predicted Value of Control Variable (e.g. Water Level), and Security Features (e.g. TCP TCP/IP packet rates and TCP connection rates)

$$\hat{\omega}(k) = \phi_k(\underline{\omega}(k-1,r))$$

$$\hat{\lambda}(k) = \phi_k(\underline{\lambda}(k-1,r))$$

Historical Datasets

Predicted Security State of the SCADA System

$$\hat{x}(k) = f(x(k), \hat{\omega}(k), \hat{\lambda}(k))$$

Intrusion Detection and Live Forensics Analysis

- Intrusion detection is the second line of defense
- The intrusion detection system adopting anomaly and signature detection techniques can detect known and unknown attacks in real time
- Live forensics analysis learning unknown attack patterns without disrupting system operations is added to protect against zero-day and evolving attacks
  - Monitoring and analyzing network traffic, front VM system performance, and auditing files using forensics tools (e.g., Wireshark) and statistical theories (e.g., Naive Bayesian Network)
  - Updating detection algorithms of the IDS and active response library so that the zero-day attacks can be prevented in the future

Intrusion Response

- The intrusion response system selects a proper response to recover the physical system behavior back to normal.
- The multi-criteria analysis controller (MAC) implements the evaluation of recommended responses. The assessment of each response must take into account four criteria, and they are:
  - Criterion 1: Enhancement of Security
  - Criterion 2: Operational Costs
  - Criterion 3: Maintenance of Normal Operations
  - Criterion 4: Impacts on Properties, Finance, and Human Safety

Fuzzy-logic Decision Making Method

The total Score for a recommended R_i Response

$$S_i = \sum_{j=1}^{3} W_{i,j} * C_{i,j}$$

Weight of Criterion j for Response i

Value of Criterion j for Response i

Criterion $j \in \{1,2,3\}$

e.g. **Response**: Replacement of Compromised Devices.
Weight values for each criterion are the same: 1/3

Criterion One	Criterion Two	Criterion Three	Criterion Four	Total Score
0	0.5	0	0.5	1/3*0+1/3*0.5+1/3+0=0.17 (Auto or Semi-Auto) (Criterion four > 0.5 "Semi-Auto"; < 0.5 "Auto")

A Case Study of the Water Storage Tank

Virtual Testbed

- The water storage tank is modeled by a laboratory-scale control system in Mississippi State University SCADA Security Laboratory.
- The MTU is connected to a Human-Machine-Interface (HMI) server via a RS-232 serial port
- The MTU connects to the RTU wirelessly

SCADA System Exploits

- We injected a malicious command that modified the register values of the water storage tank alarm condition when the water storage tank was set to the "Auto" control mode
- Auto control mode:
  - The pump was turned on when the water level reached the low alarm condition (represented by L); when the water level increased to the high alarm condition (denoted by H), the pump was turned off automatically
  - The attack first evaded the authentication process
  - Then sent an illicit command to change L setpoint from 50.00% to 40.00% ; altered H setpoint from 60.00% to 70.00%.
  - HH (the high high alarm) setpoint was modified to 80. 00% from 70:00%; LL (the low low alarm) was changed to 10.00% from 20.00%.

Physical Model of the Water Storage Tank

- A linear physical system of the water storage tank was modeled relying on the observations of the physical system when it was automatically controlled

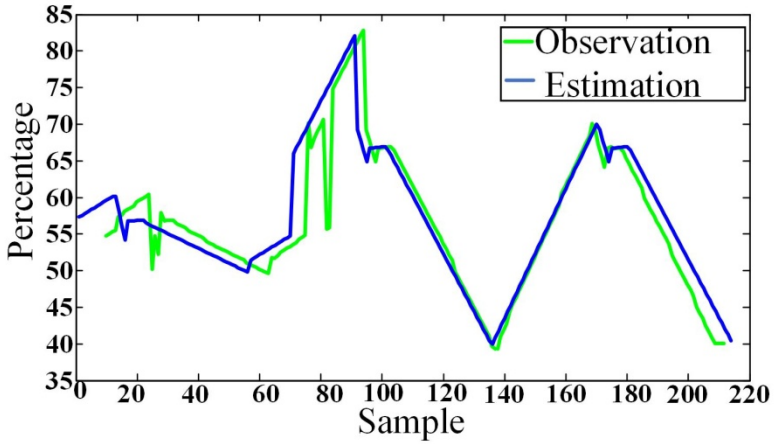
Water Level

Samples

$$\omega(k) = A * k + B$$

$$\hat{x}(k) = f(x(k), (\hat{A} * k + B), \hat{\lambda}(k))$$

Coefficients
when $1 \le t \le 35$: A = 0.256 and B = 51.181
when $36 \le t \le 39$: A = -1.976 and B = 62.090
When $40 \le t \le 45$: A = 0.032 and B = 56.718
When $46 \le t \le 80$: A = -0.202 and B = 56.686



Observations and Estimations of the Water Level Without Self-Protection

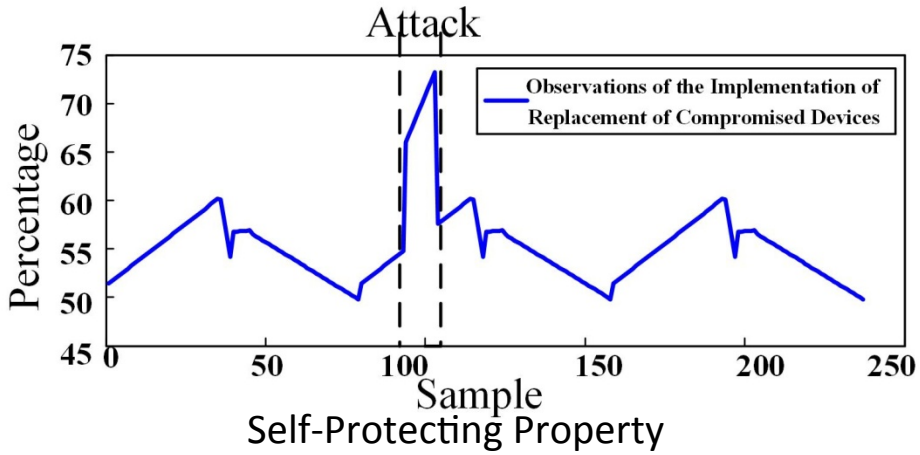
Evaluation of Recommended Responses

Ranking	Response	C1	C2	C 3	C 4	Total Value (Auto or Semi-Auto)
2	Dropping Malicious Commands	0.5	0.3	0.1	0.2	0.3 (Auto)
4	Termination of Physical Processes	0	0.8	1	1	0.6 (Semi-Auto)
1	Replacement of Compromised Devices	0	0.5	0	0.5	0.17 (Auto or Semi-Auto)
3	One time authentication	0.8	0.3	0.2	0.2	0.43 (Auto)
5	Isolation of Compromised Devices	0.5	0.8	0.8	0.6	0.7 (Semi-Auto)

The optimal response evaluated by the MAC to defend against malicious command injection attack is ”Replacement of Compromised Devices.”

Experimental Results

- It shows that at sample 94, the malicious command injection attack modified alarm conditions
- The water level was abnormally increased to 65.99%.
- At sample 104 when “Replacement of Compromised Devices” was implemented, a replica PLC containing original ladder-logic programs replied to the MTU and sent commands to control water level of the water storage tank.
- The water level was returned back to normal rapidly and efficiently with the application of autonomic computing technology



Self-Protecting Property

Conclusion

- This research applied autonomic computing technology to protect the SCADA system from cyber attacks.
- This new technology integrates current security solutions so that the system can proactively monitor, estimate, detect, and react to known and unknown attacks with little or no human intervention.
- It also ensures the SCADA system is accessible 24/7.
- The self-protection property has been validated through an experiment of protecting a water storage tank from malicious command injection attack
  - The self-protecting SCADA system maintained normal infrastructure operations and regulated the water level back to the normal operation region when alarm conditions were changed by attackers.
  - The overhead time for identifying and protecting the SCADA system was short.

9th International Workshop on Feedback Computing
JUNE 17, 2014 • PHILADELPHIA, PA
usenix

MISSISSIPPI STATE UNIVERSITY

Future Work

- In the future, we will simulate more sophisticated cyber attacks to validate the efficiency of the approach.
- We will also employ autonomic computing technology to self-protect the next generation SCADA systems from cyber assaults.

Thank You

MISSISSIPPI STATE
UNIVERSITY