MEDUSA

Mining Events to Detect Undesirable uSer Actions in SCADA

Dina Hadžiosmanović, Damiano Bolzoni , Pieter Hartel
(DIES, University of Twente, The Netherlands)

WHAT

SCADA systems are computer systems used for monitoring equipment and controlling industrial processes
(e.g. power plants, water treatment facility, gas distribution network).

Today's SCADA systems:

- use legacy technologies;
- use proprietary protocols;
- used to be isolated - nowadays may be (indirectly) connected to the Internet.

THREATS

SYSTEM-RELATED THREATS - an attacker hits computers, networks, sensors, programmable logic controllers (PLCs) or radio signals to cause failures in SCADA systems.

✓ **MEASURES TAKEN:** NIDS monitoring network traffic [2], checking protocol specifications [1], etc.

PROCESS-RELATED THREATS - an attacker gains user access rights and performs legitimate SCADA commands to cause a failure or misconfiguration in the industrial process.

✗ **MEASURES TAKEN:** None.



OUR GOAL

DETECT

- **UNAUTHORISED USERS**
- **OPERATIONAL MISTAKES**
- **HARMFUL CONFIGURATIONS**

WHAT IF

- an attacker changes device parameters (e.g., tank capacity),
- an attacker changes the range of allowed actions for a specific device (e.g., one cannot stop a pump),
- an attacker changes topology (e.g., makes a device invisible).
- an attacker produces a harmful operational sequence:

GOOD intentions	BAD intentions
How to change a water source for one neighborhood?	**How to overflow a tank and cause a disaster?**
• Switch to manual mode;	• Switch to manual mode;
• Check status in tank A;	• ~~Check status in tank A;~~
• Check status in tank B;	• ~~Check status in tank B;~~
• Stop pumping from tank A;	• **Stop pumping from tank A;**
• Start pumping from tank B;	• **Start pumping from tank B;**
• Check status in the flow;	• ~~Check status in the flow;~~
• Resize bandwidth to fit capacity;	• ~~Resize bandwidth to fit capacity;~~

APPROACH

DATA MINING

SCADA Logs

BECAUSE:

- SCADA logs are quantity and quality rich,
- SCADA behaviour is regular and predictable,
- System users lack time and skills to analyse logs manually.

PLAN

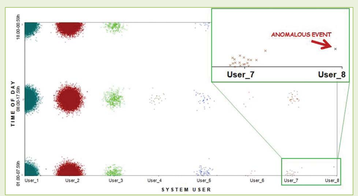
BUILD DETECTION MODEL ON SCADA LOGS

1. Learn patterns of normal behavior from SCADA logs
2. Detect outliers using data mining algorithms
3. Inspect sequences of events
4. Offline to real-time analysis

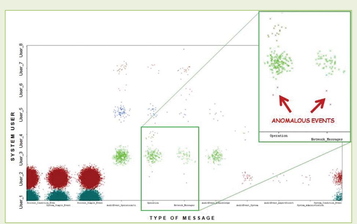
PRELIMINARY RESULTS


SCADA log


MEDUSA



An anomalous user activity in late night hours



Unexpected error messages on system users

UNIVERSITY OF TWENTE.

References:
[1]C. Bellettini and J. L. Rrushi, "*Vulnerability analysis of SCADA protocol binaries through detection of memory access taintedness*," in Proc. 8th IEEE SMC Information Assurance Workshop (L. J. Hill, ed.), pp. 341– 348, 2007.
[2]O. Linda, T. Vollmer, and M. Manic, "Neural network based intrusion detection system for critical infrastructures," in IJCNN'09: Proc. International Joint Conference on Neural Networks, pp. 102–109, IEEE Press, 2009.