Smart Device Profiling for Smart SCADA

Dina Hadžiosmanović, Damiano Bolzoni, Pieter Hartel

University of Twente, The Netherlands

Abstract. SCADA (Supervisory Control and Data Acquisition) systems are computer systems used for monitoring and controlling industrial processes such as power plants and power grid systems, water, gas and oil distribution systems, production systems for food, cars and other products.
We propose a new approach for regulating and detecting malicious behaviour of network devices in SCADA systems. Our approach consists of building profiles that describe normal communication between pairs of devices in the network. Each profile describes four aspects of network communication: device fingerprint, connectivity pattern, pseudo-protocol pattern and packet content.
We validate our approach using network traffic from two real-life SCADA installations.

Problem

In this paper we address two types of threats against SCADA environments: (1) an unauthorised device connects and start operating (2) an authorised device starts misbehaving (due to intruder activity or virus infection [2]).

Traditional countermeasures typically address these threats using network access control mechanisms and intrusion detection systems. We argue that applying current countermeasures in SCADA environments has limitations due to the specific character of SCADA networks.

Network access control mechanisms regulate access to network resources and thus typically address the first type of threats. In practice, network access control is implemented through a rule-based configuration on network devices to define legitimate network traffic (based on IP/MAC addresses and port numbers). Martinez et al. [3] propose the first behaviour-based network access control mechanism. The authors use network flow statistics to profile behaviour of device a in mobile ad hoc network. This approach fails in cases when port number is (pseudo) random (which is often the case with proprietary protocols both in and out of the SCADA context). Several authors propose approaches for traffic classification that do not use port numbers [1, 4].

To address the problem of detecting misbehaviour of authorised devices (the second type of threats), various intrusion detection systems can be applied. The most reliable approach for understanding the higher level protocol behaviour is by using protocol specifications, such as in Bro [5]. However, at the moment of writing, there are no SCADA protocol parsers publicly available.

Solution

To address both types of threats, we propose an advanced profiling approach which is port-independent. Although SCADA systems are complex, we argue that, compared to "regular" networks, these systems have a less dynamic character (e.g., systems are half or fully automated, IP addressing is static). Also, SCADA infrastructures often have several groups of redundant or similar devices within one installation. These devices operate in a similar way and use the same network protocols (e.g., a plant typically has several PLCs that use the same protocol and communicate with the same server). Because of this, we believe that SCADA environments provide good chances for capturing relevant patterns of communication and characterizing various types of devices and their behaviours.

Our approach consists of a layered communication behaviour characterization. We use network traces from the plant installation to build a graph of directed communication patterns. For every directed link in the graph, we build a profile of usual communication. To build the link profile, we use four levels of characterization: (1) device fingerprint, (2) connectivity pattern, (3) pseudo-protocol pattern, (4) packet content statistics.

During testing, we compare the current graph profile and the normal profile to detect anomalous communication of an individual device or between a group of devices.

Contribution The main contributions of our work are:

- we propose a new approach to profile behaviour of devices using a combination of four different aspects of communication,
- we propose the first behaviour-based network access control mechanism for SCADA,
- we perform preliminary experiments with positive results on two real-life SCADA installations.

References

1. Laurent Bernaille, Renata Teixeira, Ismael Akodkenou, Augustin Soule, and Kave Salamatian. Traffic classification on the fly. *SIGCOMM Comput. Commun. Rev.*, 36:23–26, April 2006.
2. Nicholas Falliere, Liam O Murchu, and Eric Chien. Symantec security response: W32.stuxnet Dossier. Technical report, 2011.
3. Vanessa Frias-Martinez, Joseph Sherrick, Salvatore J. Stolfo, and Angelos D. Keromytis. A network access control mechanism based on behavior profiles. In *Proceedings of the 2009 Annual Computer Security Applications Conference*, ACSAC '09, pages 3–12, Washington, DC, USA, 2009. IEEE Computer Society.
4. Patrick Haffner, Subhabrata Sen, Oliver Spatscheck, and Dongmei Wang. ACAS: Automated construction of application signatures. In *Proceedings of the 2005 ACM SIGCOMM Workshop on mining network data*, MineNet '05, pages 197–202, New York, NY, USA, 2005. ACM.
5. Vern Paxson. Bro: A system for detecting network intruders in real-time. *Comput. Netw.*, 31:2435–2463, December 1999.