Smart Network Access Control for Smart SCADA

Dina Hadžiosmanović, Damiano Bolzoni, Pieter Hartel

Distributed and Embedded Security, University of Twente,
P.P. Box 217, 7500 AE Enschede, The Netherlands
{dina.hadziosmanovic,damiano.bolzoni,pieter.hartel} @utwente.nl

Keywords: SCADA, network access control, behaviour profiling

Abstract

We propose a new approach for regulating and detecting malicious behaviour of network devices in SCADA systems. SCADA (Supervisory Control and Data Acquisition) systems are computer systems used for monitoring and controlling industrial processes. Installations of such systems can be found in power plants and power grid systems, water, gas and oil distribution systems, building monitoring (such as airports, railway stations), production systems for food, cars, ships and other products. Network access control mechanisms regulate access of devices to network resources. Misuses of network devices can impact network and system performances. In the SCADA context, misuses can produce serious damages to industry facilities, cause financial loss and endanger people safety [2, 5]. There are two main types of threats: (1) an unauthorised device connects and starts operating (2) an authorised device starts misbehaving (due to intruder activity or virus infection [2]).

Problem 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). This kind of control can only address the first type of threats. To address the problem of detecting misbehaviour of authorised devices (the second type of threats), we have to classify network traffic and understand which applications/protocols are running on it.

Related work Martinez et al. [3] propose the first behaviour-based network access control mechanism. Authors use network flow statistics to profile behaviour of device in mobile ad hoc networks. Although it is not using rule-based control, this approach still heavily relies on the usage of port numbers (which may be pseudorandom as in the case of SCADA proprietary protocols). To show the feasibility of classifying unknown network traffic without using port numbers, several authors use different approaches on small controlled environments [1, 4].

Our work To address both types of threats, we propose an advanced profiling approach which is port-independent and does not use protocol specifications. Although SCADA systems are complex, we argue that, compared to regular networks, SCADA systems have less dynamic character (e.g., systems are half or

fully automated, IP addressing is static) and thus provide better chances for capturing relevant patterns of communication. Our approach consists of a layered communication behaviour characterization. We profile behaviour of SCADA network devices using four levels of characterization: (1) device fingerprint, (2) connectivity pattern, (3) pseudo-protocol pattern, (4) packet content statistics. The generated profiles represent usual behaviour and are then used to detect anomalous communication patterns.

Contribution The main contributions of our work are:

- we have proposed a new approach to profile behaviour of devices using a combination of four different aspects of communication,
- we have proposed the first behaviour-based network access control mechanism for SCADA,
- we have performed 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. Ramona R. Rantala. Cybercrime against businesses. Technical report, U.S. Dept. of Justice, Office of Justice Programs, Bureau of Justice Statistics, Washington, D.C., 2004.