Intrusion Detection in SCADA Networks

Rafael Ramos Regis Barbosa and Aiko Pras

University of Twente
Design and Analysis of Communication Systems (DACS)
Enschede, The Netherlands
{r.barbosa,a.pras}@utwente.nl

Abstract. Supervisory Control and Data Acquisition (SCADA) systems are a critical part of large industrial facilities, such as water distribution infrastructures. With the goal of reducing costs and increasing efficiency, these systems are becoming increasingly interconnected. However, this has also exposed them to a wide range of network security problems. Our research focus on the development of a novel flow-based intrusion detection system. Based on the assumption that SCADA networks are *well-behaved*, we believe that it is possible to model the *normal* traffic by establishing relations between network flows. To improve accuracy and provide more information on the *anomalous* traffic, we will also research methods to derive a flow-based model for *anomalous* flows.

1 Introduction

Large industrial facilities such as water distribution infrastructures, electricity generation plants and oil refineries need to be continuously monitored and controlled to assure proper functioning. SCADA (Supervisory Control and Data Acquisition) systems are commonly deployed to aid these actions, by automating telemetry and data acquisition. Historically, SCADA systems were believed to be secure because they were isolated networks: an operator station, or human-machine interface (HMI), connected to remote terminal units (RTUs) and programmable logic controlers (PLCs) through a proprietary purpose-specific protocol.

Yielding to market pressure, that demands industries to operate with low costs and high efficiency, these systems are becoming increasingly more interconnected. Many of modern SCADA networks are connected to both the company's corporate network and the Internet[1]. Furthermore, it is common that the HMI is a commodity PC, which is connected to RTUs and PLCs using standard technologies, such as Ethernet and WLAN (see Figure 1). This has exposed these networks to a wide range of security problems. Probably the most well-know attack to a SCADA system happened at Maroochy Water Services in Australia [2]. An attacker was able to successfully interfere with the communications, causing pumps not to work properly and preventing alarms to be sent. Areas were flooded and rivers polluted with sewage. Another example happened in 2003, when the Davis-Besse nuclear power plant in Ohio was infected with

B. Stiller and F. De Turck (Eds.): AIMS 2010, LNCS 6155, pp. 163–166, 2010.

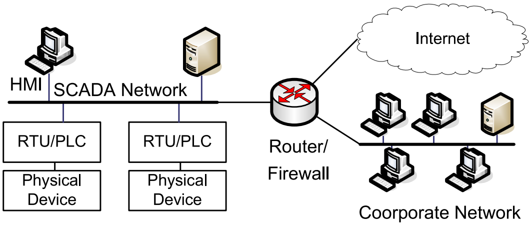

Fig. 1. Typical modern SCADA topology.

the Slammer worm [3]. The attack made the network highly congested, causing safety and plant process systems to fail for several hours.

In the face of these problems, SCADA security has become a main concern of both industry and government, leading to several efforts to increase security in these industrial networks. The American National Institute of Standards and Technology (NIST) published a guideline document that identifies several threats and vulnerabilities of such networks and discusses recommended countermeasures [4]. A report by the Netherlands Organization for Applied Scientific Research (TNO) describes thirty-nine SCADA Security Good Practices for the drinking water sector [5].

This paper describes our research proposal to address the problem of intrusion detection in SCADA networks. Based on the assumption that the traffic in these networks is *well-behaved*, we plan to build models for the network traffic based on relations between network flows, and detect attacks as violations of these models. In addition, we will research methods to create similar models to anomalous traffic, creating attack signatures at flow level.

2 Related work

There is extensive work in the area of intrusion and anomaly detection in computer networks. In this section we focus our literature review on SCADA networks. In [6], an application-specific intrusion detection system (IDS) for embedded systems, such as RTUs and PLCs, is proposed. Security polices are generated by a middleware that constantly monitors an application to define the accepted behaviour. When detecting a policy violation, the middleware can take actions that range from logging events to terminating connections. Valdes et al. [7] proposes protocol-level models for intrusion detection in process control networks. These models describe expected values for packet fields, relations between dependent fields in one or multiple packets.

The challenges involved in securing controls systems are discussed in [8]. The main idea behind their approach for intrusion detection is to understand the interactions between the network and the physical system they control. Packets are considered normal or abnormal based on the effect they have in the control system. Another approach, described in [9], is based on the observation that the contents of random access memory (RAM) of PLCs follow specific flows that persist over time. Packets are classified as normal or abnormal, by considering the effects they have in the contents of a PLC's RAM.

In contrast to the individual packet inspection described in these works, our proposal aims to detect intrusions at the network level, by analysing relation between flows. We argue that the former solutions are not suitable to detect attacks such as Denial of Service (DoS) and port scans.

3 Approach

Our goal is to develop an anomaly-based IDS using flows to model the network traffic. We want to describe the network traffic by finding relations between flows. Consider a typical activity that generates data in SCADA networks, a server polling field devices for data. In consequence of this activity several connections will be generated, one for each field device. As polling is commonly periodic, this would create a clear flow pattern in the network. In the case an engineer manually starts a polling instance, a different set of connections would be observed. For example, a connection to the authentication server might be added. A flow model for this activity would include all possible variations.

We envision a IDS capable of automatically generating flow models and detect anomalies as violation of such models. While it might be too hard to use this approach to describe all traffic in a enterprise IT network, we believe it is possible to use it to model SCADA traffic. Our assumption is that SCADA traffic is *well-behaved*, when compared with traditional IT systems. This is due a number of reasons:

- **Fixed number of network devices.** As a critical infrastructure, availability is a main concern in SCADA. The number of servers and clients rarely change over time. This does not hold for traditional IT networks, where new clients can be easily added and, normally, the consequences of a server being offline for a short period are not so severe.
- **Limited number of protocols.** Traditional IT networks might provide a multitude of services, such as web browsing, email, instant messaging, voice over IP and file sharing. This is not expected in a SCADA network.
- **Regular communication patterns.** Most of the SCADA traffic is generated in a polling fashion. Masters query a number of slaves for data, and only eventually a slave starts the communication to notify a significant event. In contrast, given the large amount of protocols, and the quantity of human-generated connections, the traffic in traditional IT networks is too unpredictable.

As a complement to this approach, we plan to investigate how to create similar models to anomalous traffic. The objective is to increase the accuracy, by creating flow-level signatures of attacks, and also to provide more information about the anomalous traffic. We believe that modelling the anomalous traffic is a more challenging task, as attackers are motivated to conceal their activities.

In summary, the main research question we propose to answer is: *how to build network traffic models based on correlation between flows?* We will evaluate what techniques are best fit to cluster flows to build such network models. We consider techniques such as deterministic finite automata, used in [10] to create flow models that identify application sessions, and Markov models. In addition, to deal with problems like what attacks we should consider and where in the network the IDS should be deployed, we plan to carry out a vulnerability assessment to refine our notion on what are the biggest threats to SCADA networks.

4 Validation

In order to validate our findings we intend to use real-world traffic captured in a Dutch water distribution infrastructure. However, due to the critical nature of the network, we might not be able to perform all the necessary measurements. If necessary, we also consider to study other protocols with similar characteristics to SCADA traffic (i.e., regular communication patterns), such as SNMP, and to make use of simulation models.

References

1. Igure, V., Laughter, S., Williams, R.: Security issues in SCADA networks. Computers & Security 25(7), 498–506 (2006)
2. Slay, J., Miller, M.: Lessons learned from the maroochy water breach. International Federation for Information Processing 253, 73 (2008)
3. Beckner, W.D.: NRC Information Notice 2003-14: Potential Vulnerability of Plant Computer Network to Worm Infection (2003)
4. Luiijf, E.: SCADA Security Good Practices for the Drinking Water Sector. Technical Report - tno.nl (2008)
5. Stouffer, K., Falco, J., Kent, K.: Guide to supervisory control and data acquisition (SCADA) and industrial control systems security (2006)
6. Naess, E., Frincke, D., McKinnon, A., Bakken, D.: Configurable Middleware-Level Intrusion Detection for Embedded Systems. In: 25th IEEE International Conference on Distributed Computing Systems Workshops, pp. 144–151 (2005)
7. Valdes, A., Cheung, S.: Intrusion Monitoring in Process Control Systems. In: Proceedings of the Forty-Second Hawaii International Conference on System Sciences, p. 17 (2009)
8. Cárdenas, A., Amin, S., Sastry, S.: Research challenges for the security of control systems. In: Proceedings of 3rd USENIX workshop on Hot Topics in Security (HotSec), San Jose, CA, USA (2008)
9. Rrushi, J., Kang, K.d.: Detecting Anomalies in Process Control Networks. In: Critical Infrastructure Protection III: Third IFIP WG 11. 10 International Conference, Hanover, New Hampshire, USA, pp. 151–165. Springer, Heidelberg (2009)
10. Kannan, J., Jung, J., Paxson, V., Koksal, C.: Semi-automated discovery of application session structure. In: Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, p. 132. ACM, New York (2006)