Computers and Electrical Engineering 47 (2015) 299–317

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Awareness and reaction strategies for critical infrastructure protection ☆

Lorena Cazorla *, Cristina Alcaraz, Javier Lopez

Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain

ARTICLE INFO

Article history:
Received 29 September 2014
Received in revised form 13 August 2015
Accepted 13 August 2015
Available online 12 September 2015

Keywords:
Critical infrastructure protection
Control systems
Countermeasures
Intrusion detection and response systems

ABSTRACT

Current Critical Infrastructures (CIs) need intelligent automatic active reaction mechanisms to protect their critical processes against cyber attacks or system anomalies, and avoid the disruptive consequences of cascading failures between interdependent and interconnected systems. In this paper we study the Intrusion Detection, Prevention and Response Systems (IDPRS) that can offer this type of protection mechanisms, their constituting elements and their applicability to critical contexts. We design a methodological framework determining the essential elements present in the IDPRS, while evaluating each of their sub-components in terms of adequacy for critical contexts. We review the different types of active and passive countermeasures available, categorizing them and assessing whether or not they are suitable for Critical Infrastructure Protection (CIP). Through our study we look at different reaction systems and learn from them how to better create IDPRS solutions for CIP.

1. Introduction

Critical Infrastructures (CIs) around the globe provide the most necessary services to society, so their continuous correct operation is of paramount importance. Control systems, such as Supervisory Control and Data Acquisition (SCADA), perform the management and the regulation of behavior of the internal devices and systems of these infrastructures. They are considered a fundamental component within CIs, having an impact in the overall performance of other interconnected critical infrastructures. Thus, the protection of CIs and their control infrastructures is currently seen as an essential part of national security in numerous countries around the world.

Recent reports from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) show that security incidents and cyber-attacks against control systems are increasing, and they are getting more aggressive and sophisticated. Known large-scale cyber attacks targeting CIs and Industrial Control Systems (ICSs), such as Stuxnet, the Nitro Attacks and the Maroochy water breach, show that CIs and ICSs are becoming increasingly targeted by different types of malicious attacks [1].

For this reason, and as dictated by governments and institutions around the globe, the integrity and availability of all these critical systems have to be protected against the numerous threats they face every day [2]. Approaches for Critical Infrastructure Protection (CIP) arise from several perspectives: preparedness and prevention, detection and response,

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. J. Garcia-Alfaro.

* Corresponding author.
E-mail addresses: lorena@lcc.uma.es (L. Cazorla), alcaraz@lcc.uma.es (C. Alcaraz), jlm@lcc.uma.es (J. Lopez).

http://dx.doi.org/10.1016/j.compeleceng.2015.08.010
0045-7906/

mitigation and recovery, international cooperation, etc. [2]. As a tool to respond to this need for protection, intrusion detection has been at the center of intense research in the last decade, due to the rapid increase of cyber-attacks on computer systems.

Intrusion detection refers to a variety of techniques for detecting threats in the form of system faults (anomalies) or malicious and unauthorized activities. A technique that focalizes this detection effort is the Intrusion Detection System (IDS) [3]. IDS solutions have been proposed for multiple environments, and they could result in very valuable protection tools for ICS environments. However, their application to the protection of critical systems must comply with the strict constraints and restrictions of ICSs [2].

However, when intrusive behavior is detected by the IDS in a critical scenario such as ICSs, it is desirable to take evasive and/or corrective response actions to prevent these attacks from succeeding, and ensure the safety of the computing environment [2,4]; such countermeasures are referred to as intrusion response. Incidentally, as threats become more abundant and sophisticated, and given the special characteristics of CIs, apart from detection mechanisms, new and more powerful solutions have to be deployed in order to safeguard them and to avoid faults and consequent cascading effects. To fight this domino effect, besides providing efficient detection mechanisms, we need to focus on the response, mitigation and recovery needs of CIs.

Solutions that can provide these functionalities are the Intrusion Prevention Systems (IPSs), also called Intrusion Response Systems (IRSs) [4] and Intrusion Detection, Prevention and Response Systems (IDPRSs) [5]. An IPS/IRS/IDPRS is "*software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents*" [3]. In the remainder of the text, we will refer to these systems as IDPRSs, since we will use the term Response System (RS) to denominate a specific element of the whole system. The IDPRS is often integrated as an extension of the IDS, but it usually receives less attention than the IDS research due to the intrinsic complexity of developing the mechanisms to offer an automated and correct response to certain events.

Traditionally, and particularly in ICSs, the response to a threat was manually triggered by the system's human administrator, and required a high degree of expertise. However, the increasing complexity and speed of the cyber-attacks in recent years, and the intricate possible ramifications of a system's faults show the acute need for complex intelligent dynamic RSs [4]. Therefore it has become necessary to use sophisticated advanced techniques from autonomic computing, machine learning, artificial intelligence and data mining to build intelligent and smart IDPRSs. Together with the deployment of IDS solutions in these contexts, automatic and intelligent response mechanisms have to be put in place to help protect CIs and prevent cascading failures to other interdependent infrastructures [6].

The structure of the paper is as follows. Section 2 presents a taxonomy for IDPRS solutions for CIP, where the different elements existent in these systems are analyzed in terms of applicability to CIs. Section 3 provides a review of the state of the art IDRPS solutions developed in the recent years. Section 4 presents an analysis of the reviewed solutions, studying the main countermeasures available that can be implemented in an IDPRS for CIP, and discusses the main strengths and weaknesses of the solutions. Lastly, in Section 5 the conclusions and future work are outlined.

2. Taxonomy of intrusion prevention and reaction solutions

To understand the IDPRS, it is important to also understand the nature of the event they attempt to detect, the environment where they operate, the different kinds of processes that can be triggered to protect the surveilled system, and the possible types of solutions that can be launched. In order to provide safe IDPRS solutions to protect critical systems, we need to identify those desirable features, and most importantly, the characteristics that constrain the application and deployment of response solutions in critical contexts such as CIs.

Protection mechanisms put into place to safeguard CIs must be tailored to their environment, taking into account its constraints in order to ensure the correct operation of the system as a whole. IDPRS solutions, similarly to IDSs, are designed to monitor and protect hosts (*host-based architecture*), or networks (*network-based architecture*) [3]. A host-based IDPRS must be tailored to the node where the solution is running, it must operate within the constraints imposed by the host, and therefore it should be well integrated with its environment. Network IDPRS solutions monitor the traffic of communication networks, and can be deployed in radically different contexts.

Generally, the internal networks of CIs and their ICSs can be divided into three main types: *corporate networks*, the *SCADA center* and *remote substations*. The first are the business local area networks connected to a SCADA to gain access to critical data streams on SCADA servers (e.g., historical data, alarms, etc.). Corporate networks are general-purpose complex infrastructures where the nodes of the network (e.g., servers, gateways) have moderate to high computational capabilities and the constraints of these networks are minimal. SCADA centers are in charge of constantly monitoring the controlled infrastructures, using their communication networks to reach remote substations.

The nodes connected to SCADA centers are usually powerful, e.g., SCADA servers, gateways and some powerful Remote Terminal Units (RTUs) in the main remote substations. However, the protocols they use are proprietary and restricted, thus the IDPRS solutions deployed in this environment could use powerful computational resources, but they have to be designed for the specific communications protocols. Remote substations constitute those control networks based on field devices (e.g., sensors, actuators) and communication interfaces (e.g., RTUs, gateways, base stations) capable of transmitting commands