# High-Speed Intrusion Detection in Support of Critical Infrastructure Protection

Salvatore D'Antonio[1], Francesco Oliviero[2], and Roberto Setola[3]

[1] Lab. ITeM - Consorzio Interuniversitario Nazionale per l'Informatica - CINI
[2] Dipartimento di Informatica e Sistemistica - University of Napoli Federico II
[3] Complex Systems & Security Lab - University CAMPUS Bio-Medico of Roma

**Abstract.** Telecommunication network plays a fundamental role in the management of critical infrastructures since it is largely used to transmit control information among the different elements composing the architecture of a critical system. The health of a networked system strictly depends on the security mechanisms that are implemented in order to assure the correct operation of the communication network. For this reason, the adoption of an effective network security strategy is seen as an important and necessary task of a global methodology for critical infrastructure protection. In this paper we present 2 contributions. First, we present a distributed architecture that aims to secure the communication network upon which the critical infrastructure relies. This architecture is composed of an intrusion detection system (IDS) which is built on top of a customizable flow monitor. Second, we propose an innovative method to extrapolate real-time information about user behavior from network traffic. This method consists in monitoring traffic flows at different levels of granularity in order to discover ongoing attacks.

**Keywords:** critical infrastructure protection (CIP), critical information infrastructure protection (CIIP), intrusion detection, flow monitoring, security management, SCADA.

## 1 Introduction

Many daily operations currently rely on services provided through systems generally indicated as critical infrastructures [1] [2] [3], such as electric grid, oil and natural gas production, transportation and distribution, water supply networks. An emerging common feature of these infrastructures is their reliance on the widespread use of distributed information, communication and control systems, both to provide more efficient and innovative services, and to meet novel user requirements and expectations. Indeed, the operation and management of these infrastructures depend more and more on the existence and correctness of the communication network.

In order to manage, control and supervise such complex, highly non-linear infrastructures, targeted control systems, called SCADA (Supervisory Control And Data Acquisition), are currently used. A SCADA system is generally composed of a master station, where system intelligence is concentrated, and a large

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 222–234, 2006.

number of RTUs (Remote Terminal Units), which are geographically distributed. RTUs are equipped with both sensors capable to gather information about the status of the infrastructure and actuators. Data gathered by RTUs are transmitted to the master station, where data analysis and integration are performed both to get a global view of the infrastructure status and to define appropriate commands to be sent to actuators. RTUs communicate with the master station by sending and receiving it short control messages.

Digital information gained more and more importance for infrastructure operation, as a result, what we might call a "cyber component" of each critical infrastructure grew, thus, giving rise to the need to integrate and make interoperable the different elements that compose information systems. These cyber components are connected in complex ways and represent the information infrastructure on which the critical system relies. The increasing success of information and communication technologies, together with the progressive disuse of dedicated communication networks are bringing a new way of controlling and managing critical infrastructures, which are currently organized as strictly connected, albeit different, elements of a single system rather than as autonomous entities to be appropriately integrated.

Control systems for critical infrastructures are rapidly moving from dedicated and proprietary solutions towards IP-based integrated frameworks made of off-the-shelf products. Unfortunately, this trend brings with it security issues since in the new scenario SCADA systems are exposed to cyber-related threats.

While physical security of critical infrastructure components (including the control system) as well as protection from direct cyber attacks (e.g., hacking) have been already investigated [4] [5], little attention has been devoted to analyzing vulnerabilities resulting from the use of commercial communication networks. As stated in [6] terrorists might attack the communication network through physical or cyber actions in order to undermine the capability of controlling the critical system [7]. Therefore, new kinds of events undermine the health of networked critical infrastructures: (i) cyber-attacks, including specific actions aiming to disrupt communication services as well as effects of wide spectrum attacks to the computer equipment devoted to control the lifeline system, and (ii) failures in the information exchange due to problems regarding the communication network which connects the control system to the remote units. Delayed or errored information can bring to situations where incorrect actions are undertaken.

The remainder of the paper is structured as follows. In section 2 we present an integrated framework capable of protecting the network by following an intrusion detection strategy based on traffic flow monitoring. Section 3 illustrates the use of data mining techniques for the definition of classification criteria. In section 4 an innovative approach for real-time traffic analysis is illustrated. It is shown how data coming from a flexible flow monitoring system can be effectively analyzed to identify ongoing attacks. Related work is presented in section 5. Finally, section 6 provides some concluding remarks, together with information concerning our future work in this field.