CRITICAL INFORMATION INFRASTRUCTURE SECURITY – NETWORK INTRUSION DETECTION SYSTEMS

Lieutenant General Professor Cristea DUMITRU, PhD*

Critical Information Infrastructure security will always be difficult to ensure, just because of the features that make it irreplaceable for other critical infrastructures normal operation. It is decentralized, interconnected, interdependent, controlled by multiple actors (mainly private) and incorporating diverse types of technologies. It is almost axiomatic that the disruption of the Critical Information Infrastructure affects systems located much farther away, and the cyber problems have direct consequences on the real world. Indeed, the Internet can be used as a multiplier in order to amplify the effects of an attack on some critical infrastructures. Security challenges increase with the technological progress. One of the last lines of defense which comes to complete the overall security scheme of the Critical Information Infrastructure is represented by the Network Intrusion Detection Systems.

Keywords: *Critical Information Infrastructure Security; Intrusion Detection Systems; SCADA; NIDS.*

Introduction

The modern society has become increasingly dependent on the availability, reliability, safety and security of many technological infrastructures. Information systems are a necessity for humanity because of the important social and economic benefits offered, and the serious consequences arising from their failure. Critical infrastructures consist of those physical and information technologies, networks, services and supplies which, if damaged or destroyed, could have a serious impact on the health, safety and security or economic well-being of citizens or the effective functioning of governments. [1] In our opinion, for society to survive, the following critical infrastructures must operate, at least to a minimum: water, electricity and fuel supply; transport and communication system; food supply and waste management; financial and insurance

* Professor, PhD, „Carol I“ National Defence University, Bucharest, Romania, corresponding member of the Academy of Romanian Scientists, Military Sciences Section, AFCEA (Armed Forces Communications and Electronics Association) member, Lieutenant General (ret.), former Chief of Romanian J6 (Directorate of IT&C in General Staff) - (e-mail: cristea.dumitru@clicknet.ro).

system; information and telecommunication networks; military defense systems; emergency, health and rescue services; Legal system, public agencies and public administration etc.

Electricity supply and information and telecommunication networks can be considered of crucial importance, since all other critical infrastructures owe them their proper functioning. We consider that in recent decades critical infrastructures have become dependent on information and communication technology, such as fixed and mobile telephony, Internet or ground and satellite networks for information management, communications and control functions. The Critical Information Infrastructure controls the management of the power plants, dams, national energy system, air traffic control systems, utility distribution systems, financial system, to name only some of the constituent elements of critical infrastructures. Because all these sensitive physical installations rely on the Critical Information Infrastructure, the latter's security is of national interest.

The security assessment of the Critical Information Infrastructure and a series of tests and reports made by stakeholders in both the public and private sector emphasize the social, political and economic dependence of the contemporary society on the information and communication technology and the constantly increasing number, scale, sophistication and impact of natural or human-caused threats. We are currently witnessing a trend towards the use of information and communication technology in order to obtain political, economic and military supremacy, including by using offensive capabilities.

Governments and all providers of vital services do not make security and resilience weaknesses publicly known unless required to do so. Even under these conditions, we know many examples of threats to critical infrastructures caused by security and resilience deficiencies of critical information infrastructures: in 2007 and 2008, there were large-scale cyber attacks in Estonia, Lithuania and Georgia; in 2008, the intercontinental submarine cables disruption in the Mediterranean Sea and the Persian Gulf affected Internet traffic in many countries; in April 2009, U.S. federal security officials warned on the U.S. electrical grid penetration of "cyber spies", after which some software that could be used to disrupt the system remained in the network; in July 2009, U.S. and South Korea were forced to cope with intentional interruptions of service (involving taking control of 100,000-200,000 computers, that became "zombies"), which affected the functioning of numerous government sites. Moreover, as shown by the recent events in the Southern Mediterranean, some regimes are prepared and able to prohibit or undermine, for political purposes, the access of their own citizens to information means of communication, especially Internet and mobile communications. Such unilateral domestic interventions can have serious consequences on other parts of the world. [2] For a better understanding of these different threats, we can divide them into the following categories: For operation, such as advanced persistent threats or continuous and coordinated attacks against government agencies, for economic and political espionage (e.g. Net Ghost [3]), identity

theft, recent attacks against the trading system of CO_2 reduction certificates or against government information systems; For sabotage, such as DDoS attacks (Distributed Denial of Service) or spam generated by botnets (e.g. Conficker network made of 7 million computers and Mariposa network in Spain with 12.7 million computers), Stuxnet and disruption of means of communication; For destruction. This is a scenario which has not materialized yet, but given the increasing use of information and communication technology in the critical infrastructures (e.g., smart grids and water distribution networks) it is not excluded for the years to come.[4]

As mentioned above, the Critical Information Infrastructure plays a fundamental role in the management of critical infrastructures such as the electricity grid, oil and gas production, water supply networks, etc. A common feature of these critical infrastructures is the widespread use of distributed information and command and control systems, both to provide more efficient services and to meet consumer needs. To manage, control and supervise the operation of such complex infrastructures, SCADA (Supervisory, Control and Data Acquisition) control systems are currently used. SCADA are modern systems, designed for the tracking and operational management of industrial processes based on online data acquisition from a huge number of units equipped with sensors able to collect information about the state of the infrastructure and centralized actuators. But SCADA-based systems are not secure, as long as the systems and networks are using commercial products, the network equipments are IP-based, and the interconnection requires Internet service, which ultimately opens the door to potential aggressors.

Technical measures meant to ensure the Critical Information Infrastructure security

After analyzing several reports on cyberspace security and lessons learned resulted from cyber attacks, we consider of utmost importance that the following technical measures be adopted to ensure the Critical Information Infrastructure security:

- **Authentication technologies** – authentication schemes for network components such as hardware, software applications, data and users are required for a wide variety of purposes, including identification, authentication and verification of data integrity. These schemes should prove their safety, be easy to verify, be used for a variety of components and be executed quickly. Traditional cryptographic methods have focused on security, but they cannot be sufficiently effective for extended use in environments where, for example, a single network router has to authenticate millions of data packets per second. Better results were obtained with cryptographic protocols.

- **Securing basic protocols** – only a few of the protocols governing the Internet operation have an appropriate security level. For example, to divert data traffic on an alternative site, an attacker can easily fool protocols such as Border Gateway Protocol (BGP) (which controls the routes followed by data packets in their movements on the Internet) or services such as Domain Name System (DNS) (which controls the data packet destination). Such attackers can intercept, monitor, alter or manipulate Internet traffic, often without being detected. For the

Internet to become a reliable medium of communication, secure versions of basic protocols must be developed to counter threats such as the denial of services, data alteration and deceiving. Besides, we consider that basic protocols should be secured against the disabling attacks which take advantage of the protocols' weaknesses.

- **Securing software engineering and software assurance** – commercial software applications engineering suffers from a lack of rigorous scientific controls necessary to produce quality applications, secured at an acceptable cost. Common software engineering practices permit dangerous errors occurrence, allowing many attack programs to compromise every year the normal operation of millions of computers.

- **Holistic security of the system** – effective security in a global infrastructure, layered and complex as the Internet and its nodes, requires more than securing its components. Making clear authentication methods, security protocols for basic Web operations and improving the software engineering are part of the equation that must tackle the Internet security issue. However, the most important issue that researchers need to consider is the end-to-end architectural approach of the security of the whole, which transcends the security for each element. Fundamental research must develop entirely new holistic security architectures, including hardware equipments, operating systems, networks and software applications.

- **Monitoring and detection** – regardless of the progress in research, unanticipated events may still occur. When this happens, you need tools to monitor and understand the event and the adoption of appropriate defensive measures. The ability of the current instruments to monitor abnormal network activities and to quickly identify the causes is insufficient evolved. The advantage the attackers have now will increase as they are improving, and the Internet becomes more vast and complex.

- **Mitigation and recovery methodologies after attacks** – secured systems must be designed to respond quickly to attacks and unexpected events and be able to recover any resulting damage, a more challenging task in the case of the scale and complexity of the Internet and its nodes. This issue has been addressed in systems of extraordinary complexity, such as the space shuttles, through substantial investment in order to obtain maximum reliability and redundancy. Not a single comparable effort has been invested so far in developing reliability methods for the Internet and computer systems against the attacks.

- **Catching attackers and deterring illegal computer activities** – arresting and conviction of the attackers are the main target of law enforcement and equally serves as a deterrent to illegal computer activities. Current capabilities to investigate cyber crime, identify perpetrators, gathering and presentation of evidence and sentencing attackers are only satisfactory.

- **Modeling and test bench for new technologies** – one of the barriers to rapid development of new cyber security products is the lack of realistic models and test benches for testing the cutting-edge technology in an environment similar to the reality. So far there has been

some research to shape the Internet, but this was somewhat simplistic and with little impact in practice. The issue is very difficult because of the complexity and size of the Internet.

- **Non-technological problems that can compromise cyber security** – a large number of non-technological factors, i.e., psychological, societal, institutional, legal and economic, can compromise cyber security in a way that cannot be solved only by network or software engineering. Installing technologies that do not take into account these factors may aggravate the problems intended to be solved. Research on human and organizational aspects of Critical Information Infrastructure can explore solutions that also aim at the human behavior.

Intrusion Detection Systems – concepts

Traditional prevention techniques such as user authentication, data encryption, avoiding programming errors and firewalls are the first line of defense for network security. Since all these methods have weaknesses that can affect the overall security of a network, we intend to approach and develop in this article the particular aspects of the Intrusion Detection Systems in computer networks.

Intrusion detection is the process of monitoring the events occurring at the level of a computer system or network and analyzing them to look for signs of intrusion. Intrusions are attempts to achieve unauthorized actions of penetration by bypassing the security mechanisms of a computer system and / or networks. They are caused by attackers accessing the system from the Internet, authorized users of the system trying to obtain additional privileges without permission or authorized users using unduly privileges assigned to them. [5]

An Intrusion Detection System (IDS) is a software / hardware system responsible for detecting suspicious data whose presence in the network may be considered unauthorized. The IDS inspects all network activity and identifies suspicious data structures that may indicate an attack from someone attempting to connect or to compromise a system. Unlike a firewall that limits network access to prevent intrusions but does not warn of an attack or unauthorized connections within the network, IDS evaluates suspected intrusion activities and signals them. The IDS captures and inspects all traffic, whether it is allowed or not, and, based on the content of the transmitted packets in the network at IP or application level, triggers an alarm when a suspect event occurs. Developing these processes, IDS analyzes the data source, and, after preprocessing the inputs, allows a detection engine to decide, based on a set of classification criteria, whether the data are normal or not, according to a behavioral model. This process is obviously more complicated in the situation of ensuring security in real time, as user behavior analysis should be done as quickly as possible in order to reduce data packet loss. Once the user's behavior was determined, it is used to define a set of classification criteria necessary to the detection engine for identifying abnormal activities. [6]

IDS systems are usually of three types: independent hardware systems that monitor traffic, software application for a dedicated server or a hardware module type "add-in" to

existing firewall. The IDS can analyze traffic data and control a wide range of types of attacks, including DoS (Denial of Service) or DDoS (Distributed Denial of Service), which usually tend to block networking or user access to resources.

Today there are IDS systems dedicated to monitoring and protecting both the network level and locally, at server and even desktop level. Solutions aimed at protecting the network level are divided into two categories:

- Online IDS - systems that analyze the traffic in a network node, in hidden mode, remotely, without actually passing traffic through the point where they are installed. Online IDS can monitor all traffic on a network, both external and internal, being connected to the monitoring port of the respective switch, at which point all traffic can be collected. This type of IDS succeeds to fully analyze traffic and alert on the activities inconsistent with the security policy established at the network and may even take steps to block these connections or sessions, or to manage and modify firewall policies.

- Inline IDS - systems that monitor a specific connection and analyze the traffic directly, representing a filter installed behind a firewall and in front of the network servers and critical systems. Inline IDS monitor only the traffic from the point of connection, the traffic passing through it; its role is to recognize attacks and the actions which are not conform to the required policies and to filter any unauthorized traffic in that point.

Intrusion detection systems for servers (HIDS - Host-based Intrusion Detection Systems) monitor applications and specific files, including registry settings and alert if unauthorized access, modification, deletion, or copying data residing on the monitored system. Their role is to maintain policies (sets of rules) imposed on that server and to report any unauthorized access attempts; it can even replace the damaged files automatically to ensure data integrity. An alternative to HIDS are the centralized systems of network intrusion detection (CHIDS - Centralized Host-based Intrusion Detection Systems) serving the same purpose, but additionally they perform a pooled analysis done by sending all data to a central node analysis.

The ability to alert only if real attacks and really dangerous for that computer network occur makes the difference between a good IDS system and the rest. Therefore, to obtain a competitive solution, a good IDS should be backed by specialized configuration, maintenance and adjustment performed by professionals.

Many IDS systems developed so far to respond to cyber attacks directed at networks have problems processing real-time traffic volume, which increases continuously. Consequently, it is necessary to adapt security analysis techniques for processing a high volume of traffic in high speed networks like Gigabit Ethernet networks.

Intrusion Detection Systems in high-speed networks

Network Intrusion Detection Systems (NIDS) are an important and practical tool for the network security. They perform security analysis of data packets by monitoring network. The constant increase in network speed and data traffic volume imposed new challenges on

these systems. In our opinion, in order to ensure an accurate detection of intrusions, NIDS must detect data packets at the speed of data transfer in network. To maintain performance and efficiency of IDS and given the trend towards the proliferation of high-speed networks, studies have shown that IDS with distributed architecture should be chosen. [7] In such a configuration, network traffic is taken by a multitude of sensors that process, each, only a fraction of traffic, reducing the possibility of data packets loss due to overload. Each sensor reads the data packets then compares their contents with the database of attack signatures and sends alarms to the management unit when an attack or a behavior contrary to security policies are detected. The NIDS management unit receives alerts or suspicious packets, stores them in a file and launches the appropriate actions. The responses of the NIDS management unit include: notification of the network administrator, automatic re-configuration of the intrusion-blocking system or implementation of mechanisms to provide support for manual intervention on the system. [8]

Such a NIDS has, in our opinion, the following features: Uses common servers, without special hardware requirements; Operates stably on high-speed networks and provides a low rate of data packets loss; Assigns traffic to nodes as evenly as possible and adapts to the network traffic variety; Achieves an appropriate balance between the rate of data packets loss and the complexity of the working algorithm; Integrates the alert messages issued at node to detect the multi-object attacks targeting the entire network; Provides simultaneously the high level ratio between the analysis objective of the macroscopic trend of the network security, and feedback and reaction response.

With the ability to process and analyze in real time the network security for high-speed networks, the distributed NIDS architecture allows for scalability and greater flexibility of the hierarchical structure. [9] Based on this architecture, NIDS effectively monitors the security of Critical Infrastructure Information networks, providing a better assessment and prediction of threats and cyber attacks.

Conclusions

Control systems of the critical infrastructures are increasingly under the threat of cyber attacks, due to the use of computer networks and IP-based communications. Moreover, we consider that digital information is more important for the operation of critical infrastructures, and, as a result, what we call Critical Infrastructure Information conditions the integration and interoperation of the elements that make up each critical infrastructure.

The approach of our study was aimed at highlighting new ways of control and management of the Critical Information Infrastructure security using intrusion detection systems in computer networks.

NOTES

[1] Cf. Commission of the European Communities, *Critical Infrastructure Protection in the Fight against Terrorism*, COM (2004) 702 final, Brussels, 20.10.2004, p.3.
[2] Joint Communication – A Partnership for Democracy and Shared Prosperity with the Southern Mediterranean, COM (2011) 200, 08.03.2011.
[3] Reports on the project *Information Warfare Monitor*: "*Tracking Ghost Net: investigating a Cyber Espionage Network*" (2009) and "*Shadows in the Cloud: Investigating Cyber Espionage 2.0*" (2010).
[4] World Economic Forum*, Global Risks 2011*.
[5], [8] Sorin SOVIANY, Sorin PUŞCOCI, Gheorghiță PESCARU, Radu DRAGOMIR, *Sisteme de detecție a intruziunilor*, Telecomunicații, Anul LI, Romania, no.2/2008, p.45.
[6] Salvatore D'ANTONIO, Francesco OLIVIERO, Roberto SETOLA, *High-Speed Intrusion Detection in Support of Critical Infrastructure Protection*, Lecture Notes in Computer Science, Volume 4347/2006, p.224.
[7] Cristopher KRUEGEL, Fredrik VALEUR, Giovanni VIGNA, Richard KEMMERER, *Stateful Intrusion Detection for High-speed Networks*, Proceedings of IEEE Symposium on Security and Privacy, 2002.
[9] Zhi-Jun LU, Jing ZHENG, Hao HUANG, *A Distributed Real-Time Intrusion Detection System for High-Speed Network*, Journal of Computer Research and Development, 2004.

A B B R E V I A T I O N S

BGPBorder Gateway Protocol
CHIDSCentralized Host-based Intrusion Detection System
DDoSDistributed Denial of Service
DNSDomain Name System
DoSDenial of Service
HIDSHost-based Intrusion Detection System
IDSIntrusion Detection System
IPInternet Protocol
NIDSNetwork Intrusion Detection System
SCADA Supervisory, Control, and Data Acquisition