Security Aspects of SCADA and Corporate Network Interconnection: An Overview

Paulo S. Motta Pires
Luiz Affonso H.G. Oliveira
Departamento de Engenharia de Computação e Automação
Universidade Federal do Rio Grande do Norte
Natal, 59.078-970, RN, BRAZIL
(pmotta, affonso)@dca.ufrn.br

Abstract

SCADA (Supervisory Control and Data Acquisition) systems play an important role in industrial process. In the past, these used to be stand-alone models, with closed architecture, proprietary protocols and no external connectivity. Nowadays, SCADA rely on wide connectivity and open systems and are connected to corporate intranets and to the Internet for improve efficiency and productivity. SCADA networks connected to corporate networks brought some new seecurity related challenges. This paper presents an overview of the security aspects of this interconnection.

1: Introduction

SCADA (Supervisory Control and Data Acquisition) systems accomplish functions that include supervision and real-time control of local or remote processes. These systems are composed of computers, software and devices used for data acquisition and digital input/output in order to perform process interaction.

SCADA systems have a strategic importance since they are adopted by the industries of a country's infrastructure. The applications of SCADA technology reach virtually the entire spectrum of the productive sector. Just to name a few, we can find these systems being used on chemical, petrochemical and electric power production and distribution; water distribution; oil and gas pipelines, nuclear plants, intelligent buildings and vehicle traffic control.

From monolithic systems, based on mainframes with closed architectures, vendor-dependent and with limited connectivity, SCADA systems have evolved to open systems with an architecture strongly based on connectivity. It is frequent, in this new model, the interconnection of SCADA networks with corporate networks, and with the Internet. This interconnection of networks with distinct characteristics and purposes is done aiming the increase of corporate efficiency, competitiveness and productivity.

It is very important to point out that the interconnection of SCADA networks, which are essentially directed to supervision and process control, and the corporate networks, directed to processing, storage and retrieval of information, incorporates some security problems which can compromise or interrupt the operation of critical processes. Eventual security problems, that were restricted to each one of the network environments, are now shared. The compromising of one of the networks can have catastrophic consequences.

In this paper we present an overview of security aspects that can result from the interconnection of a SCADA network and a corporate network. The paper is organized in four sections. In Section 2, we present an overview of SCADA systems. In this section, security problems that can be found in SCADA systems are emphasized, considering they are isolated from other networks. In Section 3, we present the aspects that must be considered regarding the security of corporate networks. The comprehension of the security problems of each one of the networks isolated can make it possible to foresee the security procedures that must be considered seeking the protection of the interconnection. In Section 4, we present an architecture that is commonly used to integrate both networks, and also analyze some security aspects that is consequence of the integration of these systems. In Section 5, we make considerations, present the conclusions and ideas aiming futures works.

2: SCADA Systems

SCADA systems are composed of a central processing unit, called Central Station or MTU (Master Terminal Unit), and some Remote Stations, called RTU (Remote Terminal Unit). These components exchange data through a communication media.

The operator interacts with the system through a graphics visualization unit available in the Central Station. This interface, known as the HMI (Human-Machine Interface), is updated in real-time with the data collected from the industrial plants by the RTUs.

By using the Central Station, the operator has access to a graphic representation of the processes that are being supervised or controlled, as well as the graphic representation of variables that are being monitored. The operator also has access to other functionalities, such as report generation and command operations over the plant devices, for example.

The Remote Stations are composed of sensors for data acquisition, of a component that carries out the communication between the Remote Station and the Central Station, and of a component responsible for executing instructions coming from the Central Station. Usually, SCADA systems have a software, which runs on one or more workstations, and is responsible for coordinating the functions of acquisition and real-time data storage of the several remote devices. Data stored on workstation are processed and presented to the operators through that graphic interface previously mentioned. Figure 1 shows the simplified architecture of a SCADA system.

Once they are physically and logically independent of other corporate systems, SCADA systems were traditionally implemented to be strictly operational, therefore concerns about security were not part of projects. This statement was proven when procedures that have potential security problems were analyzed and considered safe thanks to the

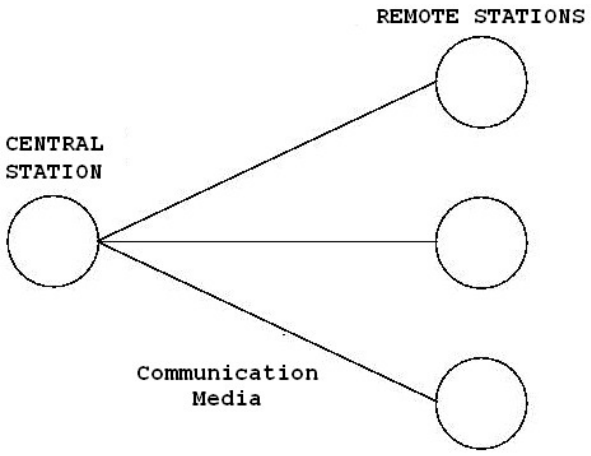

Figure 1. Simplified Architecture of a SCADA system. The system is composed of a Central Station and some Remote Stations, connected through of communication media.

isolation of initial SCADA systems. Some of these procedures, presented in [1], are:

- User authentication based only on a common password;
- Data transferred in plain text;
- Use of protocols considered *a priori* safe due to the fact they are proprietary;
- Used protocols do not implement any kind of authentication;
- Communication and control channels (dedicated lines, dial-up lines or communication channels through radio or satellite) are property of third-parties, and
- Software that is part of a SCADA system are implemented in operational systems considered unsafe.

Problems related to security became still more important considering the evolution that is occurring on SCADA systems. SCADA is becoming less logically isolated and evolving to open architectures strongly centered on connectivity. With the goal of increasing the efficiency, competitiveness and productivity on corporations, SCADA networks are being connected to corporate networks and, consequently, to the Internet itself.

In next section, we present a brief description of the most common security problems inherent to corporate networks.

3: Corporate Networks Security

SCADA networks, as seen on previous paragraphs, with aim towards process control and management. This way, security measures should guarantee that a security failure does not result in disastrous consequences and also guarantee that the system is reliable

and controllable [2]. Reliability is the guarantee that the system and its components will perform its duties under certain conditions for all the time these conditions remains; controllability is the guarantee that the system, if well-fed by its actuators, will perform the functions that it was developed to do.

Corporate networks, though, is supposed to perform the processing, storage and retrieval of corporate data. These networks have characteristics and purposes that are different from those of SCADA networks. Security procedures on corporate networks are implemented with the goal of guaranteeing confidentiality, integrity and availability of the data [3]. Confidentiality is the guarantee that the information will only be shared among authorized personnel. Confidentiality presupposes the previous classification of users and of the information to be protected, and also requires adoption of reliable tools for identifying and authenticating users. Integrity is the guarantee that the information is authentic and complete. The available information can not suffer any kind of modification, accidental or malicious. This context includes the guarantee that the information was generated by a trustworthy source. The third factor, availability, is the guarantee that the information is accessible whenever it is necessary. A security failure in corporate network is a breach of at least one of these guarantees.

Security breaches may allow a user privileged access to data it is not supposed to be authorized to access. It can also allow that a malicious user degrade network services or interfere in some dangerous way on the operation of these systems. There are several ways to exploit security breaches or degrade network services. The following ones stand out:

- Propagation of malicious code;
- Denial of services;
- Vulnerability exploitation of the operational system or applications, and
- Bad configuration of services.

Among malicious codes, we can stand out the viruses, the worms and the Trojan horses. Viruses need a host application to be effective. They are activated only when the host application is activated. Potentially more dangerous, worms are independent, autonomous software and can be spread by themselves or using other ways of transportation, such as attachments on electronic messages/mail [4]. Trojan horses are software that disguises itself as useful software. Like the viruses, they are only activated after user interaction. Most of them install backdoors that allows access for the malicious user to the target machine.

Several arrangements can be made in order to avoid or minimize the effects of security vulnerabilities exploitations for the corporate network. Among them, we can mention:

- Development and implementation of a security policy;
- Installation, in strategic places in the network, of mechanisms against malicious codes;
- Allowance to remote access only with encrypted sessions;
- Use of cryptography to protect sensitive files;

- Systematic installation of operational systems' and applications software' updates, and
- Investments in training the personnel.

To increase even more the protection level of the systems, some procedures must also be motivated:

- Maintenance of time sync among all network equipment;
- Establishment of consistent backup policies;
- Physical and logical segmentation of the network;
- Storage and analysis of logs;
- Enabling of only strictly necessary services;
- Use of firewalls;
- Use of intrusion detection systems, and
- Creation of a team of analysis and response to security incidents.

More information can be found on [5, 6, 7].

In next section, we will discuss the security problems that can arise from the interconnection of the SCADA network with the corporate network.

4: The Interconnection of Networks

Frequently, SCADA networks and corporate intranets are connected. This integration of networks with distinct characteristics and purposes happens with the goal of increasing the corporate efficiency, competitiveness and productivity.

One of the used architectures to accomplish the integration of the SCADA network with the corporate intranet is shown on Figure 2. In this Figure, the Internet connection, usually made through the corporate network, is not represented.

In this architecture, the interconnection of the SCADA network with the corporate intranet is accomplished through the use of a Gateway, an equipment that has at least two network interfaces.

Some variations of this architecture are based on functions that the Gateway performs. For example, to make it possible for the data generated from the SCADA network to be accessed by corporate users, the Gateway should store some data available on the SCADA server. This data can be collected by a script that accesses a standard service on SCADA server (such as FTP, for example), or accesses a service on SCADA server that was specifically developed to retrieve the necessary data. The presentation of SCADA data to corporate users is usually made through the use of the HTTP (Hypertext Transport Protocol) client-server technology. On the Gateway, automatic operations are performed in order to process the acquired data and, after some necessary transformations, these are presented to the user in form of pages coded in a script language (HTML, PHP, ASP, JavaScript). The user accesses the information by using

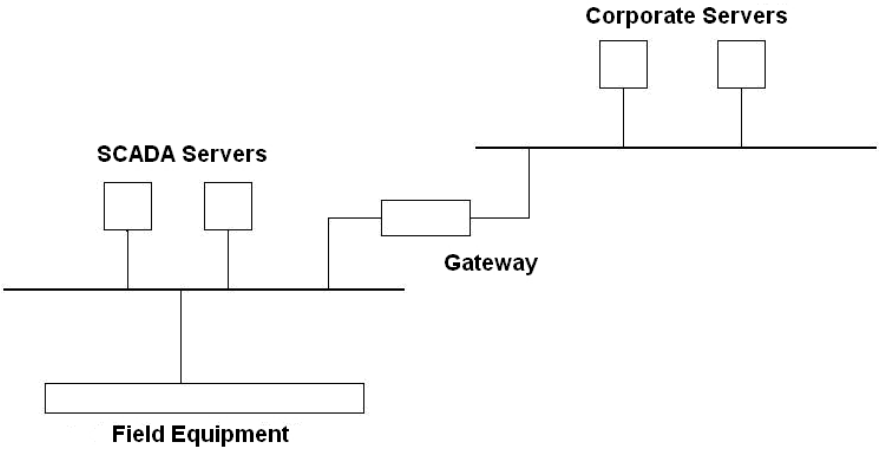

Figure 2. Interconnection of SCADA and corporate network. The networks are connected through a Gateway.

a regular browser, which is a HTTP client software. In this particular kind of solution, it is not allowed to the corporate user any kind of mismanagement over the processes that are being supervisioned or monitored [8]. Information can be accessed at any time and from any corporate network equipment. Therefore, the results of multiple control centers can be accessed and visualized in a monitor of a common corporate workstation. This solution does not depends on operational systems and can be implemented once the hardware and software on corporate network support a browser, and once a HTTP server can be installed on the Gateway. Another possibility is to enhance the Gateway with a convenient middleware in order to make it possible for the corporate user also to interact directly with the processes that are being supervisioned or controlled [9].

The interconnection of SCADA and corporate networks brought to the former some situations that was before restrict to the corporate environment, or, as seen on section 2, was not considered problematic on the operation of isolated SCADA networks. Aspects such as the access permission to corporate users, the possibility of executing remote commands, the use of unsafe communication protocols, bad configuration of equipments, the use of public networks to transmit sensitive data, transmission of plain text data, malicious code spreading and the possibility of exploiting programming bugs became part of the universe of a system that was not affected before because it was isolated. Now, with its interconnection, the possibility of occurring a security incident greatly increases. Besides, it should be taken into consideration the impact that the monitor processes may suffer in case of exploitation of a security breach in any one of the two involved environments. As usually SCADA networks are responsible for supervising and monitoring critical processes, a slight security problem can have more serious consequences.

Once there is a compromising of a system placed on the corporate network or on the SCADA network, any device or equipment that is accessible from those may also be compromised. Considering the SCADA network as the target, the main risks are [10]:

- Use a denial of service attack in order to compromise the SCADA server service or the network in which the server is on;
- Compromise the SCADA server itself. This will allow that any command that is available to the operator be also available to the attacker, and that the data can be deleted, altered or corrupted, or still that sniffers, key-loggers, or rootkits be installed, and
- The use of the SCADA server itself to perform attacks against some third party.

It is important to mention the fact that in SCADA networks it is common to see the coexistence of new systems with old ones, many of them with known vulnerabilities. This facilitates the intrusion and is consequence of the fact that performing updates usually implicates in stopping processes, or is dependent of an authorization from the manufacturer or the vendor.

We have shown that the interconnection between the SCADA network and the corporate network implicates in some new technical challenges. They should now implement mechanisms and defense rules and should perform operations that were restrict to IT personnel. It also brings to IT professionals the responsibility of acting on a network with distinct characteristics from those they are used to deal with.

5: Conclusions

In this work we presented an overview of the security aspects that must be taken into consideration in the interconnection of SCADA networks to corporate networks. It is important to stand out that this is an irreversible tendency. However, as we showed, this convergence of technologies may also bring complications, mostly in the security subject. The consequences of security vulnerability exploitation can be catastrophic because SCADA networks are usually responsible for supervising and controlling processes, and those are fundamental to the productive infrastructure.

This work reinforces that we are dealing with the integration of two networks with completely distinct characteristics and goals and that they are, today, operated and managed by professional with different visions and qualification. Therefore, to the industrial network professional it should be given the opportunity of being trained in security technologies that are today adopted on corporate networks, and also, to the IT professional, it should be given training in industrial network technologies in order to perform its duties understanding this special environment needs. Adequate, continuous training can be extended to the whole corporation in order to decrease the possibility of occurring security breaches. Another verification is that the corporate' security policy also must now includes SCADA networks, respecting its distinct characteristics and the specific training of its operators. An adequate policy will allow, for example, that a security update to be performed in corporate network also be performed on SCADA network.

It is important to point out that any preventive mechanism that happens to be installed must take into consideration the processing characteristics performed on SCADA networks. The implementation of security mechanisms may decrease the system perfor-

mance, making the adoption unfeasible. Penetration tests and scanners should be used very carefully in a SCADA network in order to maintain the operational integrity of the system.

We also verified the importance of investments aiming the establishment of standards and procedures to be adopted when performing the evaluations components and systems present in the interconnected network. There are already some initiatives aiming the building of national laboratories acting in identifying vulnerabilities, developing methodologies and proposing actions aiming the increase on SCADA systems security and its integration with other systems. The reader is refered to [11] to find detailed security considerations for industrial protocols and some case studies.

On Department of Computer Engineering and Automation of Federal University of Rio Grande do Norte, there are works being developed in tools for risk evaluation of integrated systems (SCADA and the corporate network), use open source software to integrate SCADA and corporate systems, and analysis of security measures in use of convergent industrial and corporate networks.

ACKNOWLEDGMENTS Authors would like to express their gratitude to the Department of Computer Engineering and Automation (DCA) of Federal University of Rio Grande do Norte (UFRN) and to the REDIC (Instrumentation and Control Research Network) for the support received along the development of this work. The authors would like to thank the reviews for their comments, which greatly improved the quality of this paper.

References

[1] W.F. Rush, J.A. Kinast, How to protect SCADA Systems from Cyber-Attacks: Recognizing Risks is the First Step in Protecting SCADA Systems, available on `http://www.gasindustries.com/articles/july03b.htm`, in October, 2005.

[2] A. Tilch, M. Ames, SCADA Security - Why the IT Security Approach Fails, AusCERT Conference 2004, May 2004.

[3] M. Bishop, Computer Security: Art and Science, Addison-Wesley-Longman, June 2004.

[4] N. Weaver, W. Paxson, S. Staniford, R. Cunnigham, A Taxonomy of Computer Worms, available on `http://www.cs.berkeley.edu/~nweaver/papers/taxonomy.pdf`, in October, 2005.

[5] C. Kaufman, R. Perlman, M. Speciner, Network Security: Private Communication in a Public World, Prentice Hall, 2nd. Edition, 2002

[6] S. Northcutt, J. Novak, Network Intrusion Detection, New Riders Publishing, 3rd. Edition, 2003.

[7] E.E. Schultz, R. Shumway, Incident Response: A Security Guide to Handling Systems and Network Security Breaches, New Riders Publishing, 2002.

[8] M. Wollschlaeger, Intranet-Based Management Framework for Industrial Communication Systems, 7th. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 2, pp. 823-830, October, 1999.

[9] W. Kastner, C. Csebits, M. Mayer, Linux in Factory Automation? Internet Controlling of Fieldbus Systems!, 7th. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 1, pp. 27-31, October, 1999.

[10] J. Pollet, Safety Considerations for SCADA/DCS Cyber Attacks, available on `http://www.isa.org/InTechTemplate.cfm?Section=Departments4&template=/ContentManagement/ContentDisplay.cfm&ContentID=31538`, in October, 2005.

[11] D. Dzung, M. Naedele, T.P. Von Hoff, M. Crevatin, Security for Industrial Communication Systems, Proc. IEEE, Vol. 93, No. 6, pp. 1152-1177, June, 2005.