SECURITY FOR CRITICAL INFRASTRUCTURE SCADA SYSTEMS

Miguel AREIAS
EDP Distribuição (EDP Group), Portugal
miguel.areias@edp.pt

Bruno GARRANCHO
CGI, Portugal
bruno.garrancho@cgi.com

Jesus PRIETO
HP,
Espanha
jesus.prieto@hp.com

Carlos Mota PINTO
EDP Distribuição (EDP Group), Portugal
carlos.motapinto@edp.pt

ABSTRACT

In the past decades command and control systems including Supervisory Control and Data Acquisition (SCADA) systems have undergone a major paradigm shift. In SCADA networks the emergence of commercial off-the-shelf (COTS) hardware and software to perform command and control functions, together with the adoption of open standards to enhance interoperability, exposed critical utility IT infrastructures to the security vulnerabilities and threat scenarios common to corporate networks. New threat scenarios exposed by high profile cyber-attacks, e.g.. Stuxnet, have also raised visibility and concern regarding cyber-defence capabilities against advanced persistent threats. A significant challenge for SCADA operations teams is related to the management of the security landscape in critical utility infrastructures, even upon adopting IT security best practices that help management, operations and configuration of the systems and network components that comprise those infrastructures. This paper describes how the strategic guidance decisions impacted cyber-security tactical operations of a SCADA environment, presenting an innovative architecture that is supported by security platforms tailored to the challenging scenario described above, taking into account future evolution scenarios.

INTRODUCTION

This new security architecture is the result of a thorough study of various aspects, both in terms of confidentiality, integrity and availability of all functionalities of SCADA system components and their dependencies. The basic functions continuously collect data from the SCADA infrastructure: analysing deviations from the normal activity by identifying vulnerabilities, correlating security events and generating alerts for immediate, manual or automated action, in the eventual identification of an attack. The goal of this architecture is to reduce the risk of a vulnerability being successfully exploited, by performing: real-time analysis of operational events generated throughout the infra-structures; historical and forensic analysis of cyber-security incidents; statistical analysis for the detection of deviations on behavioural patterns in the infrastructure; and end-to-end cyber-security incident management.

BEYOND PERIMETER DEFENCE

One easy parallel to trace while addressing Cyber-Security for critical utility IT infrastructures is that of securing information in support of military operations. Military strategists long ago abandoned the perimeter defence frame, promoting a Defence in Depth approach. The reasoning is simple, to delay the advance of an attacking force by maintaining multiple, layered lines of defence rather than one strong defensive line: perimeter defence.

Commonly, control systems run on segmented networks that are not in any way connected to the Internet, leading to the perception of an impenetrable perimeter. The Stuxnet incident did publicly expose the feasibility of overcoming this perceived air-gap[1].
In terms of critical infrastructure security, defence in depth is a security strategy wherein defences are overlapped so that a breach in one layer only leads the opponent to the next layer of defences. Layering defences helps to prevent direct attacks against critical systems and data, increases the probability of an eventual attack being detected, and provides the defender with more time to reconfigure defences to manage an eventual attack.

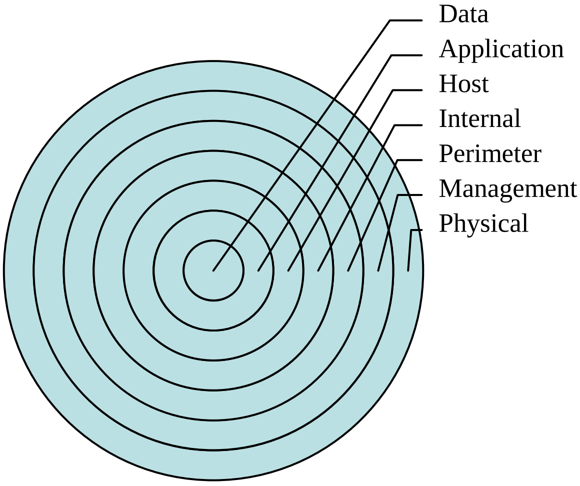

Figure 1 - Illustration of Defence in Depth

Figure 1 illustrates the layers of defensive mechanisms in SCADA infra-structures. These can be described as follows:

- Data. An attacker’s first choice target. Databases, service information and documents contain detailed knowledge on the operational scenario and tend to be trampolines to even more elaborate attacks;
- Application. The piece of software that manipulates the

data;
• Host. The systems that are running applications supporting critical functions;
• Internal Network. The network infrastructure, both active and passive components;
• Perimeter. The network that connects the IT infrastructure to other networks, such as to external users or application support;
• Physical. The tangible aspects in computing. Computers, network devices or facilities;
• Security Management Process. The overall governing principles of the security strategy.

An important principle that guides defence in depth is achieving adequate coverage: an holistic principle, which relates achieving protection from eventual attacks, by deploying security mechanisms, to assure, where fundamental, confidentiality, availability, integrity, authentication and non-repudiation. It is legitimate to say that achieving holistic coverage requires an organic relationship between three key elements: people, technology and operations.

People

Senior level management commitment, based on a clear understanding of the perceived threats, is a key point in the whole strategy of defence in depth.

This orientation must be supported by effective policies and procedures, unambiguous definition and assignment of roles, training of users and system operators, and infrastructure wide personal accountability and auditability.

On another level, but still regarding personnel, it is important to establish physical security and personnel security mechanisms. The goal is to control and monitor access to facilities and elements of the IT infrastructure environment.

Technology

Currently, a wide variety of technologies are available in support of such a holistic view. To assure that the right technologies are procured and deployed, any organization should establish a strict policy for technology acquisition. Where and how to deploy these technologies should be defined along the lines of the Defence in Depth strategy.

From our research and experience, the focus should be on the following general areas:

Networks - An organization needs to deploy security mechanisms at multiple locations to handle several classes of attacks. Adversaries can attack a target from multiple points using either insiders or outsiders. These defensive standpoints should include monitoring the networks and communications infrastructure. The protection mechanisms should include providing confidentiality and integrity for data transmitted over these networks, sensing for Distributed Denial of Service attacks should also be included in both the local and wide area communications networks.

Layering - Even the most capable commercial products have inherent weaknesses. Finding an exploitable vulnerability in a system is just a matter of time and effort. Develop a plan to identify and manage public domain vulnerabilities in our infra-structure.

Robustness - It is necessary to specify the security investment of protection mechanisms as a function of the value of what it is protecting. Additionally choosing where to deploy stronger mechanisms is also of significant importance to the overall strategy.

Detection & Reaction - Mechanisms should be in place in the infrastructure to detect intrusion attempts, analyse and correlate the results and provide information to react accordingly. The goal is to turn infrastructural information into an enabler of the Operations staff functions. These mechanisms should allow Operations staff to clearly identify if the infrastructure is being attacked, as well as what are the sources and targets of the attack.
To address these areas, organizations must deploy multiple mechanisms between the attacker's point of view and his target. Each of these mechanisms must present unique obstacles to the adversary and optimally should include both prevention and detection capabilities. Deploying these measures will help increase the probability of detecting an attacker while reducing his chances of success or making successful penetrations unaffordable.

Operations

Operations focuses on all the activities required to maintain an organization's security posture on a day to day basis. These activities include:

- Managing the security evolution of the deployed technology (e.g. installing patches, managing access control lists);
- Providing secure key management services;
- Performing system security assessments to assess the readiness status of the infrastructure;
- Monitoring and reacting to current threats;
- Attack sensing, warning, and response;
- Recovery and reconstitution;

Operational functions are of utmost importance regarding an organization security posture.

Understanding that cyber-security has become an emergent concern for our societies, specially due to several problems experimented in recent events where some services have been disrupted due to successful cyber-attacks or misuse of information systems [2], EDP Distribuição has decided to perform a cyber-security assessment of its critical infrastructure. The main idea was to challenge the implemented security architectural paradigms, based in a perimeter defence strategy, and find vulnerabilities that could expose its systems and jeopardize the service being provided.

DEALING WITH THE CHALLENGES OF DEFENCE IN DEPTH

As a result of the assessment, EDP Distribuição has decided to promote a Cyber-security Program whose main objective was to shift its own cyber defence paradigm to defence in depth, that way being prepared for near future changes to SCADA brought by Smart Grid initiatives. [3,4,5]
The Program objectives follow the three cornerstone principles described in the previous section: People; Technology; and Operations. All these have undergone a substantial shift in strategy motivated by the recommendations of the cyber security assessment.
The program is divided into several projects, of those we have chosen to give visibility to the following major projects: security policies definition; security awareness and security operations centre capabilities.

The first project, related with Security Policies, was the starting point of the new security strategy for EDP Distribuição. The goal of this project was to define security policies, metrics and requirements, which are the base for future architectural evolutions, always keeping in mind that the main objective is to evolve from a perimeter defence to a defence in depth strategy. Other aspects like network access policies and security architecture references were also included in the deliverables of the project, which will serve as the first step in the evolution of Smart Grid initiatives.

Another project addresses security awareness in the organization. Since security cannot be dissociated from cultural behaviour, it is crucial to create and promote a security culture, from the application end-users to system administrators, through top management and procurement people. Information security should be regarded across all the organization and different roles should have different concerns regarding security. Therefore, it is important to build specific awareness actions to different audiences in order to promote a security culture through the organization.

The most impacting project, that dramatically changed the way security is observed by the organization, is the Security Operation Centre (SOC) implementation. The SOC concept combines all three principles - people, technology and operations - in order to provide a global SCADA IT infrastructure inventory and surveillance, correlating security events, centralizing the security monitoring, analysis and response. Adopting a SOC immensely improves the organization's ability to rapidly recognize and respond to information security events. It also enables EDP Distribuição to provide regulatory compliance evidence in the case, of a NERC-CIP or ISO 27000 based standards audit.

SECURITY OPERATIONS CENTRE FOR SCADA

Core functions of the Security Operations Centre are performed by the Security Information and Event Management (SIEM) platform. A SIEM platform collects data from infra-structure devices allowing for deep correlation, reporting and alerting capabilities.

Guiding the platform development and configuration are inputs from infra-structure management teams, SCADA-specific security policies and an asset classification in regards to business impact.On the other hand, scalability considerations were always present. These considerations derive from the near future massive introduction of new equipment, mostly as a result of the evolution of a traditional SCADA into a Smart Grid.

SCADA Specific Context

There are key differences between traditional IT and critical utility IT architectures that impact the way to deploy an efficient SOC. From a mitigation viewpoint, deploying common IT security technologies into a critical utility IT infrastructure may not be a viable solution. Even if a critical utility IT infrastructure uses the same protocols that are used in corporate networks, the very nature of control system functionality may turn otherwise appropriate security technologies inappropriate. These systems have usually high time sensitive requirements, so latency and throughput brought by security mechanisms may introduce unmanageable delays and have a high impact on the overall SCADA performance.
When supervising such an infra-structure, the SOC entity will have to take into consideration that in SCADA infra-structure:

- Anti-malware technology is very uncommon;
- Technology lifetime is usually over 10 years;
- Change management processes are very complex;
- Patch management processes are rarely supported by, and synchronized with, SCADA software vendors;
- Availability constraints are usually very strict.

Operational Benefits

Building a SOC involves detailing Incident Handling and Risk management processes, which allow for a benefit centric approach to the SOC responsibilities, i.e. SOC is

responsible for operational efficiency.
A SOC formally concentrates tasks and processes that were usually informally executed by several teams in the organization. We have selected the following processes:

- Incident handling is responsibility of the SOC. I.e., the initial incident response, behavioural analysis and incident reporting;
- Risk management is responsibility of the SOC. I.e., SOC is responsible for all risk related actions;
- Vulnerability management and remedial action assignment are responsibilities of the SOC;
- Alerting and reporting processes, which provide compliance and audit capabilities, are also responsibilities of SOC.

The SOC has several tools to perform its functions. Nevertheless, as already stated, one function stands out, the SIEM. The SIEM platform provides the SOC with the proactive monitoring, alerting, notification and event correlation capabilities. In more generic terms, SIEM provides more than a centralized Risk and Threat management solution, it is the cornerstone of the establishment of a holistic security approach for the SCADA infrastructure.

Solution Overview

The chosen solution is built on a multi-tier architecture consisting of information gathering agents and central points of information processing. These can be arranged in a distributed architecture, to support scalability, performance, and flexible deployment requirements.

The solution follows a simple deployment process.

1. Every Security event source is identified and characterized according to its importance in the SCADA infra-structure;
2. Every security event, from every information asset, is sent to a central location;
3. This central location is comprised of two primary functions:
   a. Short term processing and analysis;
   b. Long term storage.
4. Short term processing and analysis support advanced reporting, alerting, correlation and monitoring of security functions across the whole infra-structure;
5. Long term storage provides a repository for all the relevant security information on the environment, for forensic purposes.

The process above is simplified and serves to elucidate some of the functions supported by the SIEM solution, and how do it fits in the SCADA infra-structure. As previously stated, the SIEM is a tool to support SOC processes providing centralized administration, notification, reporting, a Knowledge Base and case management workflow.

FUTURE CHALLENGES

Future Smart Grid initiatives will transform the way electrical power is distributed and used, adding intelligence through the grid to dramatically reduce outages and faults, handle current and future demand and increase efficiency. The security architecture developed by EDP Distribuição was built with the necessary structure to handle a future scaling to Smart Grid scenarios. Supported on architectural principles of Big Data and Real-time Data Analytics, the baseline security concepts will remain to be observed, reported and acted upon. The SOC processes, people and tools will be in constant evolution following a stepwise approach to provide adequate security coverage to the evolving SCADA infra-structure.

Commonly, in an organization, IT Service Management follows the ”functional silos” concept, i.e. aggregation of IT services with end-to-end definitions for availability and performance, that concept loosely relates to the Defence-in-Depth strategy for achieving dependable Critical Utility IT infrastructures. We defend that increasing efficiency requirements dictate that we evaluate the definitions looking for overlap and consolidation. A current trend relates to the consolidation of Network Operations Centres - NOCs and Security Operations Centres – SOCs, the hybrid concept where the anticipated benefits are clear. These, beside technical merits, represent the optimization of resources, alignment of service management teams for operational leverage and a potential increase in responsiveness to business requirements.

REFERENCES

[1] Langner, R, 2011, “Stuxnet: Dissecting a Cyberwarfare Weapon”, Security & Privacy, IEEE Vol. 9, 49-51.

[2] Tsang,R, 2001, “Cyberthreats,Vulnerabilities and Attacls on SCADA Networks”,IEEE Control System Magazine.

[3] Khurana,H, 2011, “Moving beyond defence-in-depth to strategic resilience for critical control systems”,Power and Energy Society General Meeting, IEEE,1-3.

[4] Paulo Moniz, Miguel Areias, Alysson Bessani, 2011, “A Security Architecture for a Smart Grid implementation”, INForum’11.

[5] P. Veríssimo, N. Ferreira Neves, and M. Correia. The CRUTIAL reference critical information infrastructure architecture: a blueprint. International Journal of System of Systems Engineering, 1(1):78–95, 2008. 2.6.