IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. II (Mar – Apr. 2015), PP 37-42
www.iosrjournals.org

Privacy Protection in Distributed Industrial System

[1] P.Sheela Rani, [2] B.Malavika, [3] D.Menaka
1.Assistant Professor, Dept of I.T, Panimalar Institute of Technology,Anna University , Chennai,India.
2.IIIrd Year .Student, Dept of I.T, Panimalar Institute of Technology,Anna University , Chennai,India.
3.IIIrd Year .Student, Dept of I.T, Panimalar Institute of Technology,Anna University ,Chennai,India.

Abstract: *Although awareness is constantly rising, that industrial computer networks (in a very broad sense) can be exposed to serious cyber threats, many people still think that the same countermeasures, developed to protect general-purpose computer networks, can be effectively adopted also in those situations where a physical system is managed/controlled through some distributed Information and Communication Technology (ICT) infrastructure. Unfortunately, this is not the case, as several examples of successful attacks carried out in the last decade, and more frequently in the very recent past, have dramatically shown. Experts in this area know very well that often the peculiarities of industrial networks prevent the adoption of classical approaches to their security and, in particular, of those popular solutions that are mainly based on a detect and patch philosophy. This paper is a contribution, from the security point of view, to the assessment of the current situation of a wide class of industrial distributed computing systems. In particular, the analysis presented in this paper takes into account the process of ensuring a satisfactory degree of security for a distributed industrial system, with respect to some key elements such as the system characteristics, the current state of the art of standardization and the adoption of suitable controls (countermeasures) that can help in lowering the security risks below a predefined, acceptable threshold.*

Keywords: *Industrial networks, information security, network security, risk assessment, security analysis and monitoring, security countermeasures.*

I. Introduction

Interconnection through digital communication networks is of primary importance, today, in many distributed heterogeneous environments where people and things, besides services and data, have to be protected against injuries and damages. This is the case, for instance, of critical infra-structures designed for energy, gas, and water distribution, transportation systems, and air traffic control, but, even with different characteristics, the same is also true for other application domains, such as Industrial Process Measurement and Control (IPCM), Supervision, Control and Data Acquisition (SCADA), Distributed Control (DC), Metering, Monitoring and Diagnostic (MMD), Networked Electronic Control and Sensing (NECS), and Distributed Automation (DA) systems. Although peculiarities can be identified for each scenario , a set of common security characteristics exists, which allows us to consider these systems as belonging to a single broad class. With a slight abuse of terminology, we will call this class either Privacy of Networks or Industrial Automation Control Systems (IACSs) in the following, provided that no ambiguity could arise.

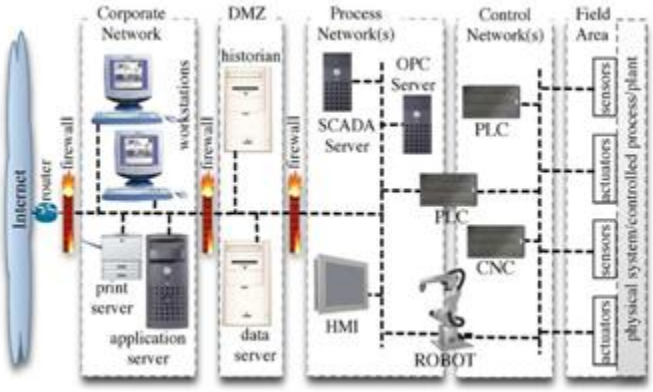

Fig. 1. Typical connections of IACS to corporate networks and the internet.

In the case of the picture, the IACS communication infra-structure (the three rightmost blocks) can access the Internet through a DBCS network: dashed lines inside each block may represent different kinds of media (i.e., Ethernet cables, phone lines, fiber optics, radio and WiFi links) and proper equipment (routers, gateways, modems, access points and so on). The key point, however, is that the IACS infrastructure is directly

interfaced to a physical system , through its sensors and actuators, while this does not occur in the case of DBCS. Fig. 1 also shows that two main different kinds of (sub)networks can be found in typical IACS, that is, control networks responsible, for instance, for enabling the correct and effective behavior of regulation loops according to the system (even hard) real-time requirements, and process networks designed to support supervisory and management functions through SCADAs and other specialized software modules. It is worth remembering that, although process net-works are less concerned with real time than their control counterparts , nevertheless they often have to grant satisfactory performance in term of the maximum acceptable response time.

The main goal of this paper is to make an overall assessment of the current situation most industrial distributed computing systems are experiencing, with respect to security. To this purpose, we consider the typical steps that have to be followed to ensure a satisfactory security level for IACS and discuss the main elements involved in this process, such as the system characteristics, the current state of the art of standardization and the adoption of suitable controls (countermeasures) that can be employed to lower the security risks below a predefined, acceptable threshold.

Roughly speaking, current researches dealing explicitly with the security of IACS can be classified in two main categories. The first one takes into account the system as a whole, and deals with its characteristics from a global point of view. These studies include, for instance, some innovative approaches to the design and development of a secure system, the design of security analysis techniques and tools and the assessment, evaluation and management of risks at the system level. The second broad category includes those scientific activities carried out to tackle specific security problems at the component level. For our purposes, the term component refers to any (collection of) h/w and/or s/w mechanism(s) that can be used to improve the security of (a part of) the system. Typical examples of components are security protocols, authentication schemes and algorithms, firewalls, intrusion detection systems and so on. Obviously, system-level strategies often rely on or make use of mechanisms and solutions designed and implemented at the component level.

Table II: Security Requirements In Iacs And Dbcs

	IACS	DBCS
increasing priority ⇑	availability	confidentiality
	integrity	integrity
	confidentiality	availability

Table III: Different Criticalities Between Iacs And Dbcs

	IACS	DBCS
h/w & s/w patching & upgrading	critical	not critical
real-time constraints	critical	not critical
consequences of failures	critical	not critical
performance & power	critical	not critical

II. Related Work

From a historical perspective, security requirements of IACS were traditionally specified by organizations that were active in a number of critical infrastructure domains including, for ex-ample:

- water and gas distribution;
- electricity transmission and distribution ;
- gas and oil production ;
- food production and distribution;
- transportation systems.

In all of these areas, the importance of security has always been recognized as progressively increasing since ever. The hetero-geneity in standardization approaches, however, enabled the de-velopment of a number of ad hoc security guidelines and recom-mendations, tailored to the specific needs of the application contexts which they were conceived for however, is that ISM concerns the whole organization of a com-pany including, with the following examples given here :

- training and commitment of employees and managers;
- relationships with partners, suppliers and customers;
- business continuity;
- legal and contractual requirements;
- compliance with security policies and standards;
- technical compliance;
- asset management;

- access control;
- communications and operations management;
- physical and environmental security.

Note that all aspects listed above are strictly related: for in-stance, the commitment of management ensures necessary re-sources and investments (training, equipment, and audits), while the training of employees enables the understanding of security mechanisms and techniques, as long as the correct implementa-tion of policies and procedures

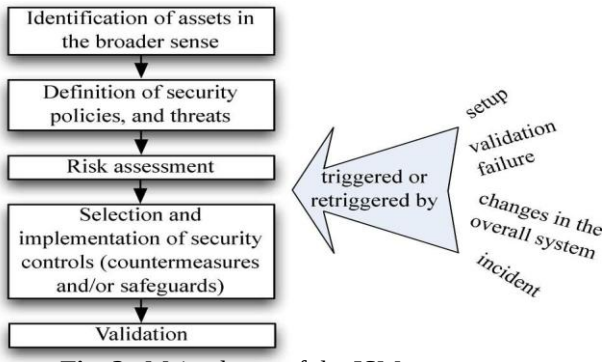

Fig. 2. Main phases of the ISM process.

Validation is aimed at proving that the overall risk has been lowered below an acceptable threshold and usually involves both offline (i.e., new risk assessment sessions) and run-time (i.e., monitoring and measurements) activities. The whole sequence of steps is then repeated whenever: 1) the results checked in the validation phase do not match expec-tations (inadequate risk reduction); 2) changes are introduced in any part/component of the overall system, including equip-ment, policies, risk levels, business, regulatory or legal requirements, newly discovered threats or vulnerabilities and so on; or 3) the run-time monitoring activities detect a security incident with consequences exceeding the acceptable severity threshold (estimated consequences are part of the results produced during the risk assessment)

III. Proposed system

IACS Risk Assessment

Risk consequences are often measured in terms of monetary losses, since this metric is widely understood and popular at the management level, although it could appear somewhat improper when referred to injuries or environmental damages. Risk assessment techniques, which have been explicitly developed for IACS so far, can be classified in three main categories , depending on the way the model of the system is developed.

A. Hierarchical Holographic Models

HHM is a methodology conceived to decompose a com-plex system with inter-dependencies into several independent views (subsystems), each one focusing on different aspects and needs (e.g., the description of the short/long term behavior of the system with not commensurable time scale, its represen-tation with diverse levels of abstraction that are useful to different people such as technicians and managers, and so on). After views have been specified, HHM allows to combine all "specific" models in a coherent way and to capture all possible sources of risk.

In order to rank, filter and manage the identified risks, en-hanced the work in by introducing a Risk Filtering, Ranking and Management (RFRM) technique, that is mainly intended to both re fine/prioritize the most meaningful risks, and prune those which can be considered as negligible, through a step-based approach.

B. Inoperability Input–Output Models

IMM overcomes some limitations of the HHM approach for systems with complex inter- dependencies among their com-ponents. In IMM, the system is hierarchically decomposed into a number of subsystems which interact exchanging resources. The input of the risk analyzer is the initial perturbation triggered by an attack, while produced results are the possible cascading inoperabilitie and economic losses.

The analysis of simple costs is a general limit of most techniques available today. Some studies have started to circumvent this problem with the introduction of operational data to estimate the consequences of inoperability in highly interdependent infrastructures. As estimations are unavoidably provided by sector - specific experts, a methodology has also been pro-posed in , which is based on fuzzy numbers, to deal with the problem of subjectivity.

C. Probabilistic Risk Assessment

The broad notion of PRA includes a number of methodologies and tools based on a shared characterization of the concept of risk, that is, the severity (magnitude) of the consequences of an event and the likelihood that the event itself can occur . Usually, the underlying models of the system be-long to the wide category of graphs (sometimes reduced to trees when dealing with simpler systems and/or inter-dependencies or when a coarser grained analysis can be considered satisfac-tory). In most cases, graph vertices represent the system components while edges describe dependencies. On the other hand, the ways graphs are analyzed fall in two subcategories of PRA, that is either deductive (backward) or inductive (forward) analysis techniques.

1) Deductive Analysis: Deductive analyzers define a so-called top event representing the unwanted consequences of attacks or failures. Starting from the affected system compo-nents, the model is then explored until the origins of the attack or failure are found. Typical examples of deductive analysis are the fault tree analysis (FTA) , dealing with faults, and the attack tree analysis , where the top event is the attacker goal rather than a fault.

2) Inductive Analysis: Inductive analyzers start from a triggering event and compute all its possible consequences. The work presented in is a case of inductive analysis where binary decision diagrams (BDDs) are adopted to improve the performance of the analysis.

IV. IACS System-Level Security

From a systemic point of view, a very big challenge, de-manding for deep technical innovations, is the development of a new kind of IACS which are security-aware. Until recently, in fact, security issues have not been considered too seriously in the early planning phases of a new system. The main reason is that security is often perceived as a sort of (even important) add-on, that may be included in the system at a later time or, howsoever, whenever it is needed . This way of thinking has influenced the research community for quite a long time, and is still affecting many scientific and technical works also today. Most papers appeared in the literature, indeed, present techniques and solutions to either introduce/improve security mechanisms in some existing system or superimpose security after a system has been conceived and developed to satisfy its functional, application and performance requirements. From a certain point of view, this approach might also be considered reasonable, at least up to a point, due to the following reasons:

- Redesigning (parts of) existing IACS is simply unfeasible or exaggeratedly expensive in most case.

A second big challenge where a radical change of direction is needed is in how IACS security problems are tackled and solved today. In fact, most techniques and solutions developed so far have been based on a "static" view of security, but systems, components, threats, and attacks change continuously and new challenges have always to be faced . This demands new methodologies and information security support to evaluate and assess the security level of IACS, to check their vulnerability to new and different types of attacks, and to suggest the adoption of suitable countermeasures, which can be developed only after a significant turn of mentality in the approach.

Fortunately enough, although IACS can be very complex sys-tems, they usually have a reduced network dynamics when com-pared with DBCS, since the set of users and protocols involved is smaller and almost fixed, while system topologies are simpler . In perspective, this factor can be leveraged to simplify the development of models and analysis techniques and the intro-duction of countermeasures.

V. IACS Security Controls

While security strategies and policies are mainly dealt with at the system level, mechanisms to enforce and support them are usually of interest of the component level. As already men-tioned before, in this paper we use the term component with a meaning broad enough to include a number of security-related controls and techniques such as, for instance, cryptography and cryptographic protocols, which are adopted for ensuring privacy and authentication in the communication. This section, in particular, focuses on those controls concerning (intrusion) prevention, detection, and reaction to security attacks. Although these three aspects are conceptually distinct, they are rarely considered separately, as in many practical situations countermeasures are conceived to tackle two of them (typically detection and re-action) or even all of them at the same time

A. Prevention Controls

In principle, contributions to IACS intrusion prevention should follow a well-established sequence of four steps, given here.

1) Definition of the security goals (i.e., explicit security policies or requirements).
2) Implicit/explicit development of one or more models of the attacker/threat that could violate the above policies.
3) Some kind of security analysis and/or validation to prove that the proposed security controls are able to satisfy the requirements, even against the modeled attacker/threat.

Some performance evaluation to check that the proposed controls do not affect the system behavior negatively (e.g., with respect to the real-time and/or power constraints .

The security requirements in the highly demanded collabo-rative control of distributed device networks under open and dynamic environments were addressed in , by inserting a Security Agent (SA) layer between each entity and the inse-cure network environment. Through a PKI, SA should be able to guarantee all of the desired security properties, though no formal proof is provided that performance and functional requirements are really satisfied.

B. Detection Controls

Preventing any threat to assets is clearly not possible and this is true, in particular, for IACS, where the dynamics of changes in h/w and s/w during the system lifetime is by far slower than the evolution of attack methods and technologies (see Table I). Keeping the system under continuous monitoring is then essential, both to rapidly notify the people in charge when dangerous situations occur, and to trigger (automatic) reactions for fault mitigation and healing. In fact, this is the primary goal of intrusion detection controls.

Intrusion detection in computer networks is a well-known and established issue, which dates back to the eighties at least. Intrusion Detection Systems are designed to quickly discover the presence of attacks in progress or the occurrence of failures, by means of some evidence gathered from the live system, while it is performing its operations. Not only ideal IDSs should avoid that some attacks go undetected (false negatives), but they are also requested not to cause false positives, that is, alarms raised when no attack is in progress. In the following, we will call ac-curacy, this characteristic which is one of the main areas where continuous research and development are needed.

Table VII: Main Methodologies For Detection

	network-based	
signature-based	[91]	
anomaly detection-based	stateless	stateful
	[93]–[96] [98]–[102]	[92], [97] [103]–[105]

Signature- based techniques require the explicit definition of "signatures" of known attacks in terms of characteristic mes-sage patterns. Unfortunately, two main drawbacks have to be carefully considered in this case: first the exact characterization of attacks is a difficult task which can signi ficantly affect the effectiveness of detection. This means that the derivation of suitable signatures , has to start almost from scratch.

1.Stateless IDSs: DoS attacks to a generic control system (sampling rate equal to 0.02 s, controller and plant intercon-nected through the Internet) were simulated in . In particular, the characterization in terms of packet delays, jitters, and losses and their correlation to the rise and settling times of the controlled system were used to measure how much the system performance could be affected by DoS. Authors then proposed to deploy IDSs on the network routers, and showed how the rise and settling times of the controlled system improved under the same attacks.

2) Stateful IDSs: When information concerning the whole system is exploited, both attacks and faults can be detected and even predicted. This also enables IDSs to reason about the attacker's goals instead of the attack mechanisms, a characteristic which can be particularly useful when dealing with threats conceived to slowly shift the system behavior to an unsafe state.

Finally, a rough estimation of main IDS issues covered in re-search papers could be derived in a way similar to the discussion already carried out in the prevention subsection. In the case of IDSs, however, accuracy and performance impact are the two topics of utmost importance.

From this point of view less than 67% of the punlished papers has dealt with accuracy, whereas performance has been explicitly tackled and discussed only by 27% of them. These two indicators are sufficiently low to conclude that much more effort and future studies are strongly needed in this area.

VI. Conclusion

This paper has dealt with the current situation of security in IACS. We have shown that, nowadays, security in IACS as a never-ending cyclical process that moves through a well-defined set of main phases, . Each phase has then been addressed in this paper, with respect to the current state of the art, to give an idea of the problems and scientific/technical challenges that have to be tackled in order to reduce the security risks under a predefined, acceptable threshold.

In this framework, the study and development of automatic/ semiautomatic analysis IT techniques and tools that are able to deal with security at a global (system) level, can be of significant help in making each phase of the management process easier and more efficient. Indeed, we think that, because of the complexity and size of many IACS, quick and effective security management decisions and (re)actions will become harder to take in the near future, so that the scientific community is expected to propose and develop new advanced techniques to support IACS security experts and managers in carrying out their tasks.

References

[1]. Security for Industrial Automation and Control Systems Part 1: Termi-nology, Concepts, Models, ANSI/ISA Std. 99.00.01-2007.
[2]. K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST SP 800-82, 2008.
[3]. D. Dzung, M. Naedele, T. P. von Hoff, and M. Crevatin, "Security for industrial control systems," Proc. IEEE, vol. 93, no. 6, pp. 1152–1177, Jun. 2005.
[4]. G. N. Ericsson, "Cyber security and power system communica-tion—Essential parts of a smart grid infrastructure," IEEE Trans. Power Del., vol. 25, no. 3, pp. 1501–1507, Aug. 2011.
[5]. Security for Industrial Automation and Control Systems Part 1: Termi-nology, Concepts, Models, ANSI/ISA Std. 99.00.01-2007.
[6]. K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST SP 800-82, 2008.
[7]. D. Dzung, M. Naedele, T. P. von Hoff, and M. Crevatin, "Security for industrial control systems," Proc. IEEE, vol. 93, no. 6, pp. 1152–1177, Jun. 2005.
[8]. G. N. Ericsson, "Cyber security and power system communica-tion—Essential parts of a smart grid infrastructure," IEEE Trans. Power Del., vol. 25, no. 3, pp. 1501–1507, Aug. 2010.

Author's Biography

P.Sheela Rani, is an Assistant Professor, in Department of Information Technology at Panimalar Institute of Technology , Chennai, India . She received M.E degree in Computer Science & Engineering dept in 2011 at Anna University, Trichy, India. She has 8 years experience in Teaching.. She is the Life member of ISTE. Area of Interest are Network Security, Computer Networks, Cryptography & Security. [rpsheelarani2014@gmail.com].

Malavika is a third year student in the Department of Information Technology at Panimalar Institute of Technology , Chennai, India. Area of Interest is Computer Networks. (malavika.guru@gmail.com).

D.Menaka is a third year student in the Department of Information Technology at Panimalar Institute of Technology , Chennai, India. Area of Interest are Computer Networks and Network Security. (menu.rosh95@gmail.com*)*