InSAW-Industrial Security Assessment Workbench

Igor Nai Fovino and Marcelo Masera

***Abstract*— Industry, in parallel with a pervasive use of information and communication technologies, has begun in the last years to take into consideration the use of public information infrastructures (including the Internet) for remotely monitoring, managing and maintaining their technical systems. Concurrently, private and public networks are used for interconnecting technical and business information systems. As a result, industry is increasingly exposed to internal and external cyber-threats, and the security of the ICT infrastructures assumes a predominant relevance. A security assessment methodology, tailored for ICT industrial systems, has been recently developed in order to address such problem. In this paper we present InSAW, a software tool we have developed to implement such methodology in order to help the analysts in modeling and analyze under a security perspective, complex critical systems.**

Index Terms— services, critical infrastructure, security assessment.

I. Introduction

Security threats are one of the main problems of this computer-based era. All systems making use of information and communication technologies (ICT) are prone to failures and vulnerabilities that can be exploited by malicious software and agents. Industrial critical installations present particular features that differentiate them from more conventional ICT systems. Industrial systems combine typical information system (e.g. data bases), with real-time elements implementing the control functions. In the latest years, these hybrid infrastructures started to be connected to internal and external communication networks, creating in this way distributed macro-systems, and ICT security has become a subject of primary concern, especially relevant to the complex field of Critical Infrastructure Protection.

Security risk assessment and management of critical industrial IT infrastructures is a relatively new discipline. Most efforts are concentrated on typical corporate information systems. Industrial systems present some specific features: the co–existence of heterogeneous environments (e.g. real–time and desktop applications), and the constraints deriving from physical phenomena (e.g. power stability) and business objectives (e.g. productivity and performance). These factors determine how IT systems can be handled: for instance, it is not always possible to stop industrial system for installing security patches.

The assessment and management of security issues deal with a varied set of information: some referring to the system characteristics (e.g. identification of vulnerabilities and assets, security policies), other to threats (their intentions, resources, capabilities), and other to the potential attack mechanisms and the relative countermeasures that could be applied in order to avoid or mitigate the effects of negative incidents. In addition one has to consider the interactions of malicious acts with accidental failures and human errors.

The interlinking of information and communication systems into systems-of-systems adds a further level of complexity: while design, configuration, deployment operations and security policies are local, the overall functioning brings about unexpected emergent behaviors and is characterized by interdependencies that can give place to system–wide propagation of negative effects.

Some approaches have been proposed to the analysis of systems-of-systems and infrastructural systems (see next section). They generally aim at linking structural and functional descriptions to security goals, and at associating vulnerabilities to known attacks. On the other hand, Masera and Nai [18, 13, 17], developed in the latest years a comprehensive service oriented theoretical methodology allowing, starting from the description of a system in term of components, services, relationships and data-flows, to identify all the possible dependencies, the cascading effects of low level vulnerabilities, the threats and the exploitable attacks. Such a methodology has been successfully tested on the field for the security assessment of complex system as, for example, Power Plants. [19]. The potentiality of such methodology, are, in our opinion, extremely promising, especially in the analysis of the inter-infrastructures interconnections and dependencies. As every security assessment framework, the one presented by Masera and Nai, in order to be proficient and effective, needs to be supported by proper tools and analysis instruments.

In this paper, after a brief recall of the present state of the art in the ICT security assessment field, and after an overview of such Service Oriented methodology, we present in detail an Industrial Security Assessment Workbench (InSAW), which fully implements and extends such security assessment methodology.

Manuscript received March 13, 2008.

Igor Nai Fovino is with the Joint Research Centre, Institute for the Protection and the Security of the Citizen. (phone: +39 0332786541; fax: +39 0332789576; e-mail: igor.nai@jrc.it, scni.jrc.it).

Marcelo Masera is with the Joint Research Centre, Institute for the Protection and the Security of the Citizen. (phone: +39 0332789238; fax: +39 0332789576; e-mail: marcelo.masera@jrc.it, scni.jrc.it).

II. State of the Art

In the scientific literature, to our knowledge, there is only a work fully tailored for industrial ICT security assessment [18] however there is relevant work in the generic field of ICT security, system modeling and system safety. The assessment of industrial systems is traditionally the field of classical safety risk studies. Only recently security issues have started to be considered of primary relevance. Keeney et al. [1] presented a study on computer system sabotage of critical infrastructures. Stoneburner, Goguen and Feringa [2] in their study on Risk Management for Information Technology Systems described a nine-step procedure for the risk assessment of information systems. Moreover Swiderski and Snyder [3] introduced the concept of threat modeling, and a structured approach for identifying, evaluating, and mitigating risks to system security.

A study of such approach on a Web Application environment is showed in [4]. In addition, there are some tools developed for general purpose like "Microsoft Security Assessment Tool" [7], and "Citicus" [8]. The first one is a traditional "check list" assessment process; in other words, the whole assessment process goes through a series of "question-answer" sessions, guiding the analysis through an iterative process, and producing as output a set of recommendations and best practices. It is quick and easy method, that can only provide rough results far from precise and exhaustive. The second tool, Citicus, is based on the concept of perceived information risks, categorizing them according to some customized criteria.

The OCTAVE approach [5], introduced by the Software Engineering Institute in the late 90s, currently represents the most complete and exhaustive methodology for information systems, but it hasn't been used and conceived for industrial applications. The more relevant tool was developed by the project CORAS (2001-2003) [6], supporting a methodology for model-based risk analysis of security-critical systems – but this methodology has been applied to e-government and e-commerce, not to industrial control systems or, in general to heterogeneous complex systems.

From these methods we can derive some useful remarks. The assessment of security requires the proper description of the system at issue, from all relevant perspectives: policies and operations, structure and function, physical links and information flows, etc.

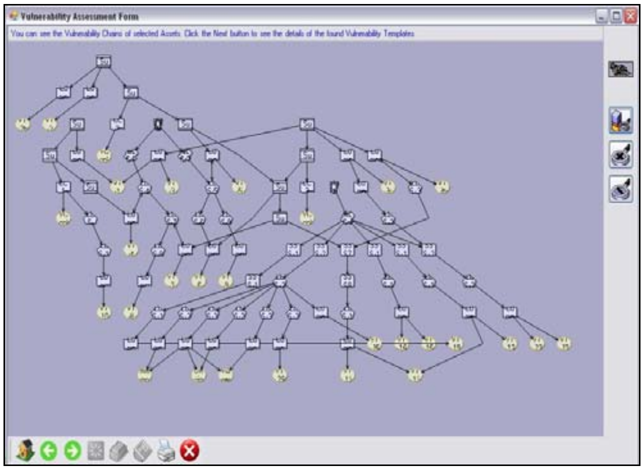
The problem of "Infrastructure Modeling" has been treated mainly for design and operational purposes, but the analysis of security requires further considerations Different approaches have been suggested in order to model systems in light of security. The work presented in [5] by Alberts & Dorofee is a good example of a risk assessment methodology based on a system description. However such a description lacks mainly in two points: it is not formal and, more relevant, it cannot deal with complex System-of-Systems. Folker den Braber et al. present in [6] another risk assessment approach partially based on a system description. It tries to partially capture the concept of adverse environment by introducing (using UML) the concept of "Threat Scenario". This, of course, is an advance in the representation of systems that could be adapted for the description of several interacting systems. Nevertheless, this was not the intention of the authors and represents only a possible adaptation of the methodology. Masera and Nai Fovino in three correlated works [9, 10, 11], present an approach based on the concept of system–of–systems, that preserves the operational and managerial independence of the components while capturing at the same time the concept of relationship among components, services and subsystems. In the present work we adopt as starting point such approach (summarized in a deeper detail in the following section).

Finally, security assessment needs to consider attack scenarios. There exist several methods used to describe security information related to malicious acts. Historically the first approach in that sense was related to the creation of vulnerability databases (of which Bugtraq [12] is an example). However, they are basically focused on the description of vulnerabilities, lacking completely (but that isn't their goal) the description of the means and ways by which they can be exploited by attacks. The most promising approach capturing the latter characteristic is the Graph Based Attack Models [13]. In this category two can be considered the main modeling approaches: Petri Net based Models and Attack Trees models. A good example of the first category is the Attack Net Model introduced by McDermott [14] in which the places of a Petri Net represent the steps of an attack and the transitions are used to capture precise actions performed by the attackers.

The second approach (attack trees), proposed originally by Bruce Schneier [15] is based on the use of expansion trees to show the different attack lines that could affect a system describing their steps and their interrelationships. Such an approach has been extended by Masera and Nai [16] by introducing the concept of Attack Projection.

III. The Service Oriented Security Assessment Methodology, an Overview

As claimed in the introduction, our objective is to provide a tool helping to analyze the critical infrastructures and their interconnections in order to identify implicit dependencies, to detect potential cascading effects, and finally to identify vulnerabilities, threats and attacks which could cause major damages. We have chosen to adopt as reference the work of Masera & Nai [18]. The methodology proposed by Masera & Nai foresees that in order to assess the security of a system, it is necessary to provide a description of the system itself, of its components, of its assets, of the interaction and the relationships among the components, the assets and the external world. Such a description (expressed analytically by tables) could be used to identify in a systematic way the



Vulnerability Assessment Form

You can see the Vulnerability Chains of selected Assets. Click the Next button to see the details of the found Vulnerability Templates

Fig. 1. Disservice Graph

vulnerabilities affecting the whole system. Moreover, as shown in Figure 1, by analyzing the vulnerabilities affecting the different components-subsystems-services of the target system, while at the same time inspecting the different relationships-dependencies-data flows linking together all the actors of the system, it is possible to build a graph of disservice chains, i.e. a graph which systematically illustrates all the possible explicit and implicit cascading effects which can be caused by a low level component affected by a vulnerability.

These vulnerabilities are then described by some significant parameters (e.g. severity, plausibility, resource costs etc.) and used to identify the threats that can be associated to the relevant services provided by the system. Such information is then used to identify and validate candidate attacks which can be exploited against the system. This evaluation gives as feed-back a set of "feasible attacks" with associated indexes which show off the level of exposure of the system. All these operations are quantified by some risk related indexes that are then employed to perform the evaluation of the security failure risk and the countermeasures.

IV. INSAW HIGH LEVEL DESCRIPTION

The Service Oriented Analysis methodology presented by Nai and Masera, is clearly based on the concept of *Knowledge*. In other words, in order to analyze a system, it is needed to possess both detailed knowledge about the elements composing the system itself, and detailed knowledge about vulnerabilities, threats and attacks. The lack of such information compromises obviously any kind of security assessment analysis. On the light of these considerations, a tool which aims at helping the analysts in the evaluation of the security of infrastructures which are usually extremely complex, should provide not only the analysis engines allowing to identify the vulnerabilities, the dependencies etc, but should also act as knowledge repository.

Figure 2 presents a high level description of the software architecture of InSAW. The core of the whole tool is a relational DBMS managing a set of different libraries:

- *Component libraries*: such set of libraries contains a wide range of information (e.g. brand, features, low level services provided, associated vulnerabilities etc.) related to different kind of components. We can store here for example libraries of network components, libraries of electric components, valves etc.
- *Vulnerability libraries*: such libraries contain information about known vulnerabilities, like their severity, their plausibility, the components affected by them etc.
- *Threat libraries*: libraries describing known threats (including potential agents, resources and means needed for implementing attacks).
- *Attack libraries*: such libraries contain the description of attacks according to the well known attack tree paradigm [15].
- *Countermeasure libraries*: they contain the description of the possible countermeasures associated to the known vulnerabilities and attacks.

All these libraries are, in the reality represented by relational DBs managed by the central DBMS.

Finally the "system library" contains the instantiation of all the system analyzed.

On top of the DBMS there is an *Object Translation Layer*. Such an intermediate layer allows adopting an object-oriented approach over a relational database. Following this approach, for describing a system with all its relationships, flows, services etc. the user will have to search the desired components in the libraries, and select and instantiate them into the DB related to the system under analysis. The components instantiated automatically will carry with them all the information related to their vulnerabilities, the low level services provided etc. The user will have only then to design, with the help of visual tools, the remaining elements of the system description, e.g. the data flows, the subsystem interfaces and services etc. All these elements will be then stored in the system DB.

On top of the Object Oriented layer have been developed seven modular units:

- *Library management unit*: It allows managing the different libraries, for exporting and importing them into XML format. The possibility to exchange libraries is a not negligible feature of this framework, in fact in this way, it is possible to use knowledge accumulated by other experts in order to perform a target local analysis.
- *System Description Unit*: it supports the visual description of the system under analysis.

- *Vulnerability Analysis Unit*: such unit supports the vulnerability analysis of the target system. Basically it implements all the algorithms of graph analysis, cycle resolution, pruning and propagation presented in [18], which allows to:
    - Identify the vulnerabilities.
    - Examplify all the implicit relationships, covert channels and cascading effects.
    - Identify the disservice graph.
    - Calculate the associated vulnerability indexes.
- *Threat Analysis Unit*: it implements the threat analysis according to the service oriented methodology. Roughly speaking it allows to link the high level services (i.e. the services provided by the system to the external world) with a set of threats. This facilitates the identification of the services-subsystems-components that could be involved in the carrying out of threats.
- *Attack Analysis Unit*: This unit allows associating a set of attacks (taken from the attack libraries) to services and subsystems. The algorithms in this module associate the abstract attack descriptions with the model of the system under evaluation, exhaustively trying, by inspecting all the possible relationships, dependencies and data flows, to discover which attack pattern could potentially be implemented. During the attack analysis, not only an attack validation is performed. In fact, InSAW also explores the combination between different attacks (macro attacks) and the combination between attacks and failure events (as every component has associated a failure rate).
- *Countermeasure Unit*: on the basis of the results of the previous analysis engines, such module provides a set of suitable countermeasures which can in different measure mitigate the effects of the discovered security holes.
- *Presentation Unit*: such units provides the following features:
    - Query: it allows the user to formulate queries related to different aspects of the information stored into the databases.
    - Report: it allows to generate a wide set of different reports about the analysis performed.

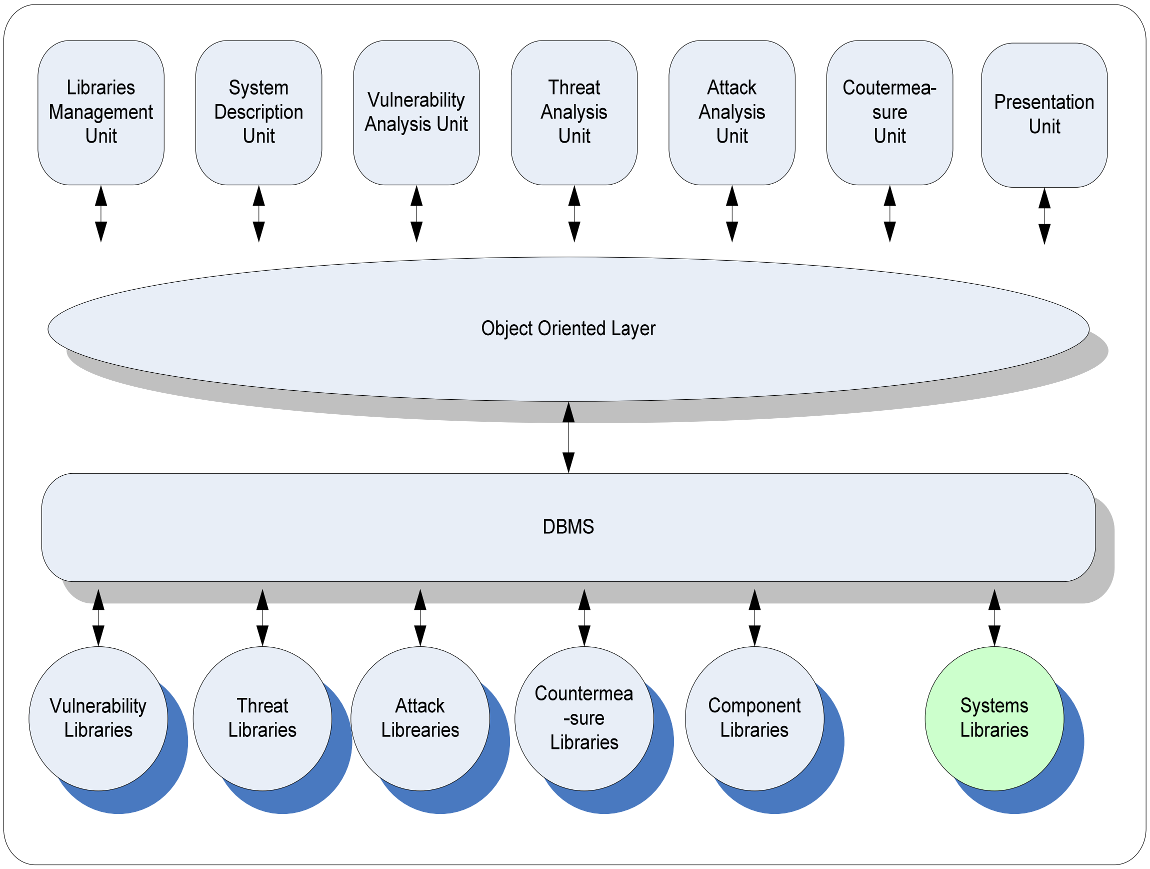


Fig. 2. InSAW High Level Architecture

From a technical point of view, InSAW has been developed in C# over a MSSQL DBMS. The intermediate O.O. layer has been realized by using the “Hibernate” libraries [20] Figures 3 and 4 show some InSAW screenshots

V. Experimental Results

The Service Oriented security assessment methodology and InSAW have been extensively tested during these last two years, mainly using systems taken from the electric power sector. We approached the test phase in a rigorous and systematic manner, starting from smaller systems (e.g. IT systems in substations), passing then to the analysis of medium level industrial control systems [17], and arriving finally to the analysis of complex systems such as power plants [19].

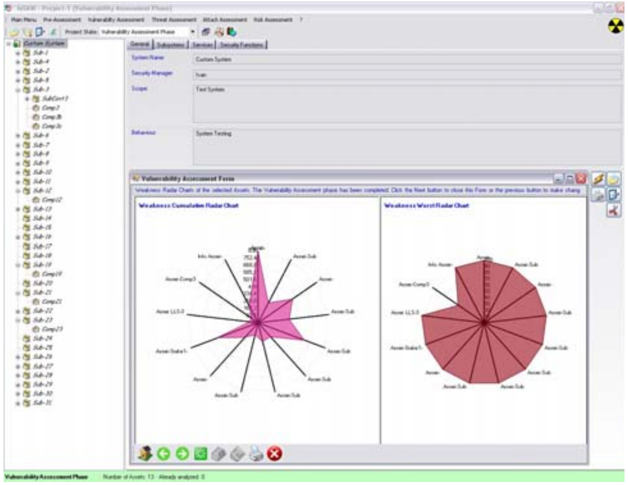

Vulnerability Assessment Form
Weakness Cumulative Radar Chart
Weakness Worst Radar Chart

Fig. 3. InSAW exposure indexes screenshot

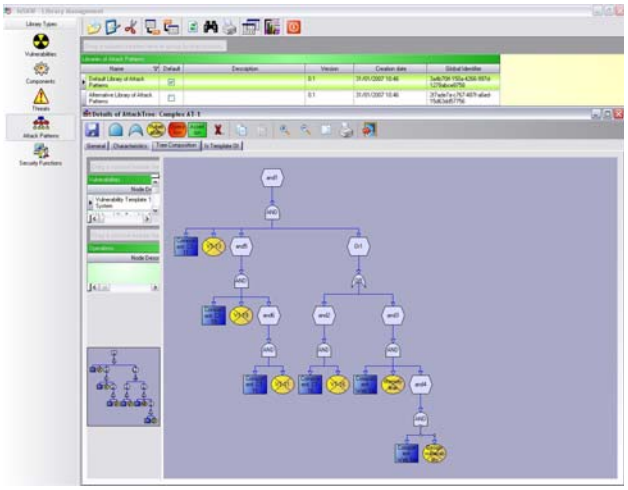


Fig. 4. InSAW Attack Tree Design

Step by step we refined the algorithms and in the meantime we increased the content of our libraries. Referring to the ICT security assessment of a power plant, by using InSAW and its knowledge database, we were able to automatically identify 254 major low level vulnerabilities and 13 successfully exploitable complex attack scenarios which, if realized could have extremely dangerous effects [19].

VI. Conclusions

There is the need, nowadays, of methodologies and tools for assessing the security and the safety of the modern industrial and critical infrastructures. In this paper we presented a comprehensive tool conceived for this purpose. The on-field tests of such tool, which implements a formal service oriented security assessment methodology, has showed promising results in helping to keep safe and secure complex critical infrastructures. Moreover, being based on a system of system modeling approach (each sub-system can be seen as a component which inherits the services and the vulnerabilities of the “composing lower level components”) it appears at the moment extremely appealing for the analysis of the security of interconnected systems (e.g. continental power grids). For the future we plan to explore in depth this research direction. Finally, we plan to integrate the InSAW tool (and the methodology which it implements), with the Trust Cases paradigm [ref.] for structuring the evidence about security into a complete argumentation arrangement.

References

[1] M. Keeney, E. Kowalski, D. Cappelli, A. Moore, T. Shimeall, S. Rogers, “Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors”. CMU, May 2005.

[2] G. Stoneburner, A. Goguen, A. Feringa. “Risk Management Guide for Information Technology Systems”. Special publication 800-3, National institute of Standards and Technology.

[3] F. Swiderski and W. Snyder. “Threat Modeling”, Microsoft Press 2004.

[4] E. Bertino, D. Bruschi, S. Franzoni, I. Nai-Fovino, and S. Valtolina. “Threat modelling for SQL Servers”. Eighth IFIP TC-6 TC-11 Conference on Communications and Multimedia Security (CMS 2004), September 2004, UK, pp189-201.

[5] C. Alberts A. Dorofee “Managing Information Security Risks: The OCTAVE (SM) Approach”, July 2002, Addison Wesley Professional

[6] F. Braber, T. Dimitrakos, B. A. Gran, K. Stølen, J. Ø. Aagedal, “The CORAS methodology: Model-based risk management using UML and UP”, in UML and the Unified Process. IRM Press, 2003.

[7] “Microsoft Security Assessment Tool” https://www.securityguidance.com/

[8] “Citicus ONE”. http://www.citicus.com

[9] M. Masera, I. Nai Fovino, “Models for security assessment and management”. In proceeding of the International Workshop on Complex Network and Infrastructure Protection, 2006.

[10] M. Masera, I. Nai Fovino, “Modelling Information Assets for Security Risk Assessment in Industrial settings”. 15th EICAR Annual Conference, 2006.

[11] I. Nai Fovino, M. Masera, “Emergent Disservices in Interdependent Systems and System-of-Systems”. In proceeding of the IEEE Conference on Systems, Man and Cybernetics, October 8-11 2006, Taipei.

[12] Bugtraq vulnerability database. http://securityfocus.com

[13] J.Steffan, M.Schumacher, “Collaborative attack modeling”. In proceeding of the Symposium on Applied Computing, Madrid, Spain (2002) pp. 253 – 259

[14] J. McDermott, “Attack Net Penetration Testing”. In The 2000 New Security Paradigms Workshop (Ballycotton, County Cork, Ireland, Sept. 2000), ACM SIGSAC, ACM Press, pp. 15-22.

[15] B. Schneier, “Modeling Security Threats”, Dr. Dobb's Journal. https://www.schneier.com/paper-attacktrees-ddj-ft.html (2001).

[16] I. Nai Fovino, M. Masera, “Through the Description of Attacks: a multidimensional View”. In proceeding of the 25th International Conference on Computer Safety, Reliability and Security 26-29 September 2006 Gdansk, Poland, 2006

[17] G. Dondossola, J. Szanto, M. Masera, I. Nai Fovino, “Evaluation of the effects of intentional threats to power substation control systems”. In proceeding of the International Workshop on Complex Network and Infrastructure Protection, Rome, 2006.

[18] I. Nai Fovino, M. Masera. “A service oriented approach to the assessment of Infrastructure Security”. In Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, March 19 - 21, 2007.

[19] I. Nai Fovino, M. Masera, “Power Plant ICT security assessment-A study case”. In Proceeding of the Second Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, George Manson University, Washington, USA, March 19 - 21, 2008.

[20] Hibernate object/relational libraries http://www.hibernate.org /

[21] M. Zagorski and J. Gorski.“ An Approach for Evaluating Trust in IT Infrastructure”. In proceedings of the International Conference on Dependability of Computer Systems (DepCoS-RELCOMEX 2006), 24-28 May 2006, Szklarska Poreba, Poland.