CRITICAL UTILITY INFRASTRUCTURAL RESILIENCE

G. Dondossola, G. Deconinck, F. Di Giandomenico, S. Donatelli, M. Kaâniche, P. Verissimo

CESI RICERCA (Italy), KUL (Belgium), CNR-ISTI (Italy), CNIT (Italy), LAAS-CNRS (France), FCUL (Portugal)

Extended Abstract

Introduction

The problem of security and dependability, or generically speaking, *resilience* [1] of Internet-oriented infrastructure systems, such as web server compounds, is reasonably well understood. Although it is not completely mastered (for example, denial of service is still a research subject), it is receiving adequate attention. However, such is not the case with the problem of resilience of *critical utility infrastructures.* This problem is not completely understood, mainly due to the hybrid composition of these infrastructures.

The process control of utility infrastructures is based on the SCADA (Supervisory Control and Data Acquisition) systems which yield the operational ability to acquire data, supervise and control whatever is the business in question (electricity, water, gas, telecomm). However, they also have interconnections to the standard corporate intranets, and hence indirectly to the Internet (e.g., remote access via dedicated or public networks). The aforementioned SCADA systems were classically not designed to be widely distributed and remotely accessed, let alone be open. They grew-up standalone, closed, not having security in mind.

Widely distributed monitoring, protection and control systems, implementing special protection scheme over the power transmission network, are emerging whose architecture is based on open communication infrastructures.

This opening that we observe nowadays is an afterthought in the line of the generic trend of any informatics system. Whilst it seems non-controversial that such a status quo brings a certain level of threat, namely but not only through interference, we know of no work that has tried to equate the problem by defining a model of "modern utilities distributed systems architecture". We believe that evaluation work on such a model will let us learn about activity patterns of interdependencies that will reveal the potential for far more damaging fault/failure scenarios than those that have been anticipated up to now. Moreover, such a model will be highly constructive as well, for it will form a structured framework for: conceiving the right balance between prevention and removal of vulnerabilities and attacks, and tolerance of remaining potential intrusions and designed-in faults.

In fact, this hap hazardous evolution led to the inevitable: access to operational networks such as remote SCADA maneuvering, ended up entangled with access to corporate intranets and public Internet, without there being computational and resilience models that understand (*represent*) this situation and deal with the resulting interference. In consequence, unlike what exists in simpler, more homogeneous settings, e.g. classical web-based server infrastructures on Internet, it is in most circumstances not possible to devise a dependability and security case for these interconnected critical utility infrastructures.

The damage perspectives that may result from this exposure are overwhelming. They range from wrong maneuvering, to malicious actions coming from terminals located outside, somewhere in the Internet. The targets of these actions are computer control units, embedded components and systems, that is, devices connected to operational hardware (e.g., water pumps and filters, electrical power generators and power protections, dam gates, etc.). In the electrical power provision these situations have already been experimented by citizens in various part of the world. As a single example, among blackouts that occurred in the summer of 2003 in several countries, we can remember the North American one, which is very relevant to explain the motivations of this project: as highlighted in the analysis report [2], it was the failure of various information systems that thwarted the utility workers' ability to contain the blackout before it cascaded out of control, leading to an escalating failure, characteristic of interdependent critical infrastructures. This type of failure will be addressed in the project.

Background and Research Challenges

The main challenge for the European CRUTIAL project is to make power control resilient in spite of threats to their information and communication infrastructures. Considering the crucial role of control systems in governing the quality and the stability of the electric power service, it is considered of great importance for the utilities operating the infrastructures to dispose of tools for analyzing threat impacts and of technologies for avoiding, or limiting, most serious consequences. In what follows, we present a brief overview of the state of the art on the major topics involved, and the basic research challenges that the CRUTIAL consortium has identified.

Countries and industrial associations have been attentive to the problem, having produced analyses, studies and recommendations, such as interdependency analyses and models [3,4], assessment of cyber risk to power control systems [10], studies of electronic security in manufacturing and control systems environments, or establishment of process control security requirements [5,7,8,9]. Research initiatives and activities related to the protection of critical infrastructures and security of information and SCADA in electric power systems were launched in the USA and Europe [6]. On the practical side, real test beds for the simulation of attack scenarios to power control and management systems have been built [11].

A large body of research exists on the dependability analysis and evaluation of computer based infrastructures, in particular with respect to *accidental threats*, while the evaluation of security has been mainly based on qualitative evaluation criteria [27]. As regards *malicious threats*, new approaches have been proposed recently for the quantitative evaluation of security based on probabilistic modelling [12,13], and to the study of interdependencies and their impact on critical outages [14,15,16,17].

Some pioneering work addressing this problem [13] must now be complemented by the definition of a comprehensive framework for the modeling and evaluation of resilience taking into account malicious faults as well as accidental faults. An additional relevant issue is the problem of modeling interdependencies in a context characterized by *different operation phases and regimes*, which can be handled by stochastic models for multi-phased systems [26].

Regarding resilient distributed real-time architectures, there is a reasonable body of research, both in the fields of fault tolerance, and of security. Whilst they have taken separate paths until recently, the problems to be solved are of similar nature: keeping systems working correctly, despite the occurrence of mishaps, which we could commonly call faults (accidental or malicious); ensure that, when systems do fail (again, on account of accidental or malicious faults), they do so in a non harmful/catastrophic way. A unifying approach has slowly emerged during the past decade, and gained impressive momentum recently: intrusion tolerance. In short, instead of trying to prevent every single intrusion or fault, these are allowed, but tolerated: the system has the means to trigger mechanisms that prevent the intrusion from generating a system failure.

A number of isolated works, mainly on protocols, took place that can be put under the IT umbrella [18,19,20,21] , but only recently did the area develop significantly, with two main projects OASIS and MAFTIA [22], respectively in the US and the EU, doing structured work on concepts, mechanisms and architectures. Some recent results on protocols resilient to malicious faults [23] and on architecting and programming with trusted components [24] open interesting prospects on how to simultaneously tolerate faults and intrusions on critical utility infrastructures.

Research Agenda

The project focuses on the electrical power infrastructure and the information infrastructures, by considering different topology realms and different kinds of risks:

- distinguishing the backbone from the specific information networks and from the infrastructures dedicated to the control and monitoring of the electric power infrastructure, as they usually have different levels of protection;
- distinguishing faults of different kinds and severities, such as electric power outages and cyber attacks;
- handling all faults (accidental and intentional malicious) under common approaches and mechanisms.

In order to master the complex mechanisms of global failures particular focus should be put on the study and modeling of the *types of failures* that are characteristic of interdependent critical infrastructures. Although the modeling of such failures has received increasing interest in the last years [25] after the large blackouts of electric power transmission systems in 1996 and 2003, this problem is still open and further developments are needed:

- Cascading failures that occur when a disruption in one infrastructure causes the failure of a component in a second infrastructure,
- Escalating failures that occur when an existing failure in one infrastructure exacerbates an independent disruption in another infrastructure, increasing its severity or the time for recovery and restoration from this failure
- Common cause failures that occur when two or more infrastructures are affected simultaneously because of some common cause.

In order to withstand effectively the above-mentioned combinations of faults and intrusions, and handle them in an automated way, the study of resilient architectures devoted to the critical utilities infrastructure problems are included in our research agenda:

- architectural configurations that induce prevention of the more severe interaction faults, and attack and vulnerability combinations;
- middleware devices that achieve tolerance of the remaining faults/intrusions (architectural blocks, protocols);
- sophisticated system monitoring mechanisms.

References

[1] "R&D challenges for Resilience in Ambient Intelligence (RAmI)", Report of the workshop held in Brussels, 19th March 2004, http://rami.jrc.it.

[2] US-Canada Power System Outage Task Force, *Interim Report: Causes of the August 14th Blackout in the United States and Canada*, November 2003, 134 p.

[3] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, understanding, and analysing critical infrastructures interdependencies", *IEEE Control Systems Magazine*, Dec. 2001, pp. 11-25.

[4] A. Wenger, J. Metzger, M. Dunn, I. Wigert, "Critical Information Infrastructure Protection", *International CIIP Handbook 2004*, ETH the Swiss Federal Institute of Technology Zurich, 2004.

[5] G. Ericsson, "Managing Information Security in an Electric Utility", *Electra Magazine - Cigré*, n. 216, October 2004.

[6] *Sandia SCADA Program High-Security*, Report SAND2002-0729, April 2002.

[7] Falco & oth. "IT Security for Industrial Control Systems".

[8] Recommendations 800-30 2002, by Stoneburner *et al.* "Risk Management Guide for Information Technology Systems".

[9] Report: April 2004 "System Protection Profile - Industrial Control Systems".

[10] G. Dondossola, O. Lamquet, "Cyber Risk Assessment in the Electric Power Industry", Cigrè Electra Magazine n. 224, February 2006.

[11] G. Dondossola, J. Szanto, M. Masera, I. Nai Fovino, "Evaluation of the effects of intentional threats to Power Substation Control Systems", International Workshop on Complex Network and Infrastructure Protection (CNIP06), Rome 28-29 March, 2006.

[12] D. M. Nicol, W. Sanders, K. Trivedi, "Model-based Evaluation: From Dependability to Security", IEEE Transactions on Dependable and Secure Computing, 1 (1), pp.48-65, 2004.

[13] R. Ortalo, Y. Deswarte, M. Kaâniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security", IEEE Transactions on Software Engineering, Vol. 25, N°5, pp.633-650, September-October 1999.

[14] M. Masera, "An approach to the Understanding of Interdependencies", *Proc. Power Systems and Communications Infrastructures for the Future*, Beijing, Sep. 2002.

[15] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructures interdependencies", *IEEE Control Systems Magazine*, Dec. 2001, pp. 11-25.

[16] E.E. Lee, J. E. Mitchell, W.A.. Wallace, "Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems", *Proc. 37th Annual Hawaii International Conference on Systems Sciences*, Jan. 2004.

[17] K. Schneider, C.-C. Liu, "A proposed method of partially-decentralised power system protection" *International Conference on Securing Critical Infrastructures, CRIS 2004*, Grenoble, France, October 25-27, 2004.

[18] Y. Deswarte, L. Blain, J.C. Fabre, Intrusion tolerance in distributed computing systems, Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy. pp. 110-121, 1991.

[19] L. Alvisi, D. Malkhi, E. Pierce, M. Reiter, R. Wright, Dynamic Byzantine quorum systems. Proceedings of the IEEE International Conference on Dependable Systems and Networks, pp. 283-292, 2000.

[20] G. Ateniese, M. Steiner, G. Tsudik, New multi-party authentication services and key agreement protocols. IEEE J. of Selected Areas on Communications, vol. 18, 2000.

[21] M. Hiltunen, R. Schlichting, C. Ugarte, Enhancing survivability of security services using redundancy, Proceedings of the IEEE International Conference on Dependable Systems and Networks, pp. 173-182, 2001.

[22] A. Adelsbach, D. Alessandri, C. Cachin, S. Creese, Y. Deswarte, K. Kursawe, J. C. Laprie, D. Powell, B. Randell, J. Riordan, P. Ryan, W. Simmonds, R. Stroud, P. Veríssimo, M. Waidner, A. Wespi. Conceptual Model and Architecture of MAFTIA. Project MAFTIA deliverable D21. January 2002. http://www.research.ec.org/maftia/deliverables/D21.pdf.

[23] Miguel Correia, Nuno Ferreira Neves, Paulo Veríssimo, Lau Cheuk Lung, Low Complexity Byzantine-Resilient Consensus, Distributed Computing, vol. 17, n. 3, pp. 237--249, March 2005.

[24] Miguel Correia, Paulo Veríssimo, Nuno Ferreira Neves, The Design of a COTS Real-Time Distributed Security Kernel, Fourth European Dependable Computing Conference, Toulouse, France, October 2002 © Springer-Verlag.

[25] I. Dobson, B.A. Carreras, V. Lynch, D.E. Newman, "Complex Systems analysis of series of blackouts: cascading failure, criticality, and self-organization", Bulk Power System and Control, Aug. 2004, Cortina d'Ampezzo, Italy.

[26] A. Bondavalli et al., "Dependability Modelling and Evaluation of Multiple Phased Systems using DEEM". IEEE Transactions on Reliability, 53(4): p. 509-522, 2004.

[27] G. Dondossola, M. Masera, O. Lamquet, Emerging standards and methodological issues for the security analysis of the Power System information infrastructures, 2004 Conference: Securing critical infrastructures, Grenoble 25-27 October 2004.