Policy Based and Trust Management for Critical Infrastructure Protection

Filipe Caldeira*†, Edmundo Monteiro*, Paulo Simões†
*CISUC - DEI, University of Coimbra, Coimbra, 3030-290, Portugal
{fmanuel, psimoes, edmundo}@dei.uc.pt
†Polytechnic Institute of Viseu, Viseu, 3504-510, Portugal

***Abstract*—Critical infrastructure (CI) services are consumed by the society constantly and we expect them to be available 24 hours a day. A common definition is that CIs are so vital to our society that a disruption or destruction would have a severe impact on the social well-being and the economy on a national and an international level. CIs can be mutually dependent on each other and a failure in one infrastructure can cascade to another interdependent infrastructure to cause service disruptions. Methods to better assess and monitor CIs and their interdependencies in order to predict possible risks have to be developed.**

This work addresses the problem of the quality of information exchanged among interconnected CI, the quality of the relationship in terms of trust and security and the use of Trust and Reputation management along with the Policy Based Management paradigm is the proposed solution to be applied at the CI interconnection points for information exchange.

***Keywords*-Critical Infrastructures, ICT security, Trust and Reputation Management**

I. Introduction

Although large efforts have been made in modelling CI risks, the information gathered from those models is still kept inside each CI and is not shared among interdependent CI.

The introduction of mechanisms for sharing risk information can, along with more resilient CI, increase the security level of multiple interdependent CI. To achieve these service levels, a robust, resilient and inter-dependencies-aware alerting system need to be implemented. This is the main goal of MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures) FP7-ICT project, aiming the design and implementation of a real-time risk level dissemination and alerting system [1]. MICIE overall architecture is presented in Figure 1.

In this work we briefly present the MICIE Alerting System and describe the mechanisms for information exchange among CI, namely, the Secure Mediation Gateway (SMGW), the trust and reputation mechanisms and the use of the Policy Based Management paradigm.

II. Policy Based Management

The SMGW Manager handles issues regarding authorization, authentication and accounting controlling both interaction with peer SMGWs and all the internal operation of the SMGW, including also testing, alarming, management of intrusion prevention and detection functions and the management of the Reputation Service[3] .

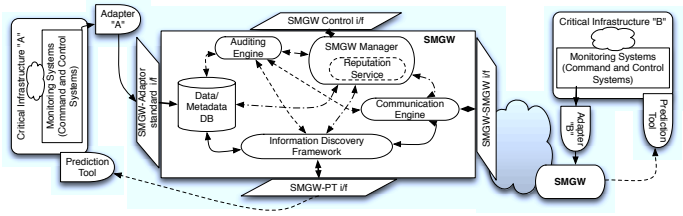

Figure 1. MICIE overall system and SMGW architecture [2]

The proposed approach provides the CI operator with a tool where he can define, in a high level manner, the behaviour he pretends for the system. Traditional approaches are mainly oriented to the management of individual components, not considering the system structure as a whole.

The CI operator can define policies that will address the relations between local SMGW and foreign SMGWs, including defining how each particular CI can connect and data access policies. The SMGW manager GUI will allow browse existent information and define actions that remote SMGWs can perform (e.g. write and/or read risk information). All data access controls are implemented with a high level of granularity thus maintaining simplicity [4].

III. Trust Model

Although a communication system for information exchange among CIs can be seen as a closed system where it is supposed that partners trust each other, it's possible for a partner CI to provide inaccurate information, either maliciously or due to faulty components in its monitoring framework.

In this context the need of a Trust and Reputation Service on each CI was identified, able to maintain real time trust information about peering CIs and interdependent services. This service will monitor information exchanged between peers and also the partner behaviour in terms of ICT security in order to manage reputation and to infer a trust level for each one.

The interactions between peers are monitored to gather intelligence about the partnership. Thus if one partner CI behaves incorrectly according to defined policies, for example by repeating the tentative of retrieve private information, this can be seen as an ICT incident and evaluate a trust indicator based on this type of information.

The Trust and Reputation Service (TRS) evaluates information exchanged between CIs in order to infer a trust level for each transaction. This service incorporates a level of trust on the data received from each partner, allowing that trust levels are incorporated in risk assessments as a mean to improve its accuracy and its resilience to inconsistent information. It will be possible, for instance, to give more weight to highly trusted data or to ignore data provided by low-trust partners [2].

IV. Conclusion

This work reports some research achievements in MICIE project, namely the development of a Policy based Management tool for the SMGW and the incorporation of the concept of Trust and Reputation in the SMGW.

Trust indicators and the use of policies can enhance risk indicators accuracy, help incorporating trust in system management and also help CI operator to evaluate the relation between his CI and their peers.

Results from the validation process are promising, demonstrating the ability to improve CI interoperation security.

Prototypes for the presented solutions are already developed and the Authors expect to evaluate this proposal within the MICIE project starting with a simple reference scenario that encompasses a small portion of an electricity distribution network and an interdependent telecommunications network [5]. Planned validation work for the MICIE project will also include more complex scenarios, provided by the Israel Electric Corporation.

References

[1] Micie, "Micie - tool for systemic risk analysis and secure mediation of data ex-changed across linked ci information infrastructures," *FP7-ICT-SEC-2007.1.7 – 225353 – Annex I – "Description of Work"*, 2008.

[2] F. Caldeira, E. Monteiro, and P. Simões, "Trust and reputation for information exchange in critical infrastructures," *5th Int. Conf. on Critical Infrastructures Information Security (CRITIS 2010), Athens, Greece, 23-24 September*, 2010.

[3] F. Caldeira *et al.*, "Secure mediation gateway architecture enabling the communication among critical infrastructures," in *Future Network and MobileSummit 2010 Conference*, 2010.

[4] F. Caldeira, E. Monteiro, and P. Simoes, "Trust and reputation management for critical infrastructure protection," *Proc. of the 6th Int. Conf. on Global Security, Safety & Sustainability (ICGS3'10), Braga, Portugal, 1-3 September*, 2010.

[5] P. Capodieci *et al.*, "Improving resilience of interdependent critical infrastructures via an on-line alerting system," *Complexity in Engineering, 2010. (COMPENG '10)*, 2010.