New Research Dimensions for the Formal Analysis of Critical Information Infrastructures Security Requirements *

Abstract:

Global connectivity of computing and storage resources opens up the possibility of sabotaging and misusing information to a degree never seen before. The exponential growth in the scale of distributed data management systems and corresponding increase in the amount of data being handled by these systems require efficient management by maintaining consistency, ensuring security, fault tolerance and good performance in terms of availability and security.
Achieving high confidence in security design requires the use of adequate modelling techniques. Goal-oriented requirements engineering methods such as KAOS support this by allowing the security analyst to capture of goals (in particular security properties), to model assets, to discover threats (or security anti-goals) and address them by operational security requirements enforced by responsible components. This analysis can be refined down to a formal level, supported by model-checking tools.
However, a comprehensive analysis of security requirements of critical information infrastructures (CII) requires additional parameters such as risk analysis, analysis of data isolation techniques, forensics, etc.
In this paper, we present our approach to integrate those new dimensions in KAOS for the formal analysis of security requirements. A Grid-based Data Management System (GDMS) is used as a case study in this work. Holistic view of the requirements model is presented to highlight the role of each new dimension in the comprehensive security requirements analysis of GDMS.

Formal Analysis of Security Requirements:

Formal analysis is based on the mathematical techniques for the specification, development, and verification of a system under consideration. This analysis though inflicts higher design costs yet it is desirable to enhance the reliability and robustness of any design in general and of high-integrity systems in particular. Security requirements are widely used in the modern system designs where resources are generally placed beyond the administrative control of the majority of the

* This research work is supported by the European Network of Excellence CoreGRID (project reference number 004265). The network aims at strengthening and advancing scientific and technological excellence in the area of Grid and Peer-to-Peer technologies. The CoreGRID webpage is located at www.coregrid.net

stakeholders. Moreover, the complexity of such highly scalable architectures makes it impossible to evaluate its security requirements by *simple examination*. This situation leads the security designers to opt for the formal techniques for the analysis of the security requirements of their designs.
Formal techniques widely used for security requirements analysis include KAOS [1], I-STAR [2], and TROPOS [3]. We have chosen KAOS for this work as it is comparatively more adaptive for the new dimensions without loosing its core methodology. We have employed Grid Data Management Systems (GDMS) as a case study to show the advantages of adding new dimensions in the existing ones.

KAOS:

KAOS treats requirements as a federation of four models namely goal model, responsibility model, operations model, and responsibility model. They collectively form a requirements model of the system under investigation. The desired system property (security in our case) is treated as *goal* in KAOS. Goals are structured into directed acyclic graphs, which ensure that analysts justify more strategic, high-level goals with at least one other goal that explains why the high-level goals are in the model. Goals can be refined as a collection of sub-goals that describe how to reach the refined goal. Verification, validation and conflicts resolution techniques for the goals have also been developed. The goal model also allows the analyst to capture and structure anti-goals which are the dual of goals, wished by malicious agent working against the achievement of system goals. The security related anti-goals are called threats. KAOS has been applied successfully to specify the goals and requirements in over 30 industrial projects in domains ranging from aerospace to publishing.

Grid Data Management System (GDMS):

Grid data management systems offer a common view of storage resources distributed over several administrative domains. The storage resources may be not only disks, but also higher-level abstractions such as files, or even file systems or databases. In this paper, we extend our previous work on modelling of security requirements of grid data management systems [4] where we addressed issues related to storage management policies by modelling security requirements at the application level, and the requirements on mechanisms for using storage semantic web services. In this paper, we extrapolate the existing dimensions [5] to effectively address the security requirements of critical information infrastructures.

New Research Dimensions:

This section elaborates the set of three new dimensions that we have identified and worked on their applicability in the formal security requirements analysis of critical information infrastructures.

Risk Assessment

We define risk assessment as a mandatory step for adequately addressing the threats within the critical information infrastructure [6]. Risk assessment includes the analysis of consequences and probability of occurrence. The former can be estimated using a priori knowledge about the presence of a vulnerability, the ease to exploit it and attack figures from honeypots. The later is related to the strategic importance of the broken goal. In the goal oriented approach, those figures can decorate the security requirements leaves and can be propagated up to more strategic goals for taking security design decisions among possible alternative (and the related costs) to address them. This second step involves considering a number of risk mitigation actions which in proper combination will reduce the risk to an acceptable level given possible drawbacks in terms of performance, usability and costs. Among other models, Defect Detection and Prevention (DDP) [7] developed by NASA can also be employed for risk analysis.

Data Isolation

Data confidentiality is an indispensable requirement of commercial organisations. However business also requires sharing data. Controlling the balance between those is critical and requires appropriate model depending on the context. The proven role-based access control can reach its limits in context where the conflict of interests plays significant role in the overall organisational datasets security strategy. Sound security assurances are sought by these organisations before even thinking of the *externalisation* of resources. Alternative models such as the Chinese wall [8] can help here to formalise dynamic data isolation as a security requirement of critical information infrastructure.

Forensics

We need to include this dimension to handle the post-attack scenarios. Forensics techniques should be powerful enough to trace the point(s) where security breach took place. We treat a security breach as a failure of dealing with the security requirements e.g. lack of envisioning a comprehensive set of security requirements; failure to properly address the envisaged security requirements, etc. We propose the use of events

monitoring and distributed honeypot [9] to obtain information about the malicious entities.

Conclusions

This work presents our idea of extending the existing range of security requirements parameters to effectively address the security requirements of critical information infrastructures (CII). Due to its inherent large scale, dynamic and complex nature; CII security requirements analysis requires enrichment of the conventional set of security requirements parameters. In order to make CII dependable systems, we need to include reliability indicators to mitigate the risks. Likewise, we need to endow with confidentiality assurances by providing data isolation. Finally, security requirements model of CII should also encompass the post-attack scenario by providing the traces of events that lead to the accident.
This work is still in progress and a number of other issues for future research remain open.

References

1. Dardenne A., Lamsweerde A. and Fickas S., *Goal-Directed Requirements Acquisition*, Science of Computer Programming Vol. 20, North Holland, 1993, pp. 3-50
2. Yu E., 'Towards Modelling and Reasoning Support for Early-Phase Requirements Engineering', Proceedings of the 3rd IEEE Int. Symp. on Requirements Engineering (RE'97) Jan. 6-8, 1997, Washington D.C., USA. pp. 226-235.
3. Bresciani P., Giorgini P., Giunchiglia F., Mylopoulos J., Perini A., 'Modeling early requirements in Tropos: a transformation based approach', Second International Workshop on Agent-Oriented Software Engineering (AOSE-2001). Montreal, Canada, May 29th 2001.
4. Naqvi S., Massonet P., Arenas A., 'Security Requirements Model for Grid Data Management Systems', Lecture Notes in Computer Science (LNCS 4347), pp 30-41, ISBN 9783540690832, 2006
5. van Lamsweerde A., *Elaborating Security Requirements by Construction of Intentional Anti-Models*, Proceedings of ICSE'04, 26th International Conference on Software Engineering, Edinburgh, May. 2004, ACM-IEEE, pp 148-157.
6. The European Project ASSESSGRID – www.assessgrid.eu
7. Feather M., Cornford S., Dunphy J., and Hicks K., 'A Quantitative Risk Model for Early Lifecycle Decision Making', *Proceedings of the Conference on Integrated Design and Process Technology*, Pasadena, California, June 2002.
8. Brewer D., Nash M., 'The Chinese Wall security policy', Proceedings of the IEEE Symposium on Security and Privacy 1989, 1-3 May 1989 pp 206 - 214
9. Yang G., Rong C., Dai Y., *A Distributed Honeypot System for Grid Security*, Proceeding of the Grid and Cooperative Computing 2003 (GCC2003), Shanghai, China, 2003, pp 1083-1086