A STUDY OF SECURITY APPROACHES FOR THE DEVELOPMENT OF MOBILE GRID SYSTEMS

David G. Rosado, Eduardo Fernández-Medina
University of Castilla-La Mancha, GSyA Research Group-Information Systems and Technologies Institute
Escuela Superior de Informática, Paseo de la Universidad 4, 13071 Ciudad Real, Spain

Javier López
University of Málaga, Computer Science Department, Málaga, Spain

Keywords: Secure Software Development, Security, Mobile Grid Computing, Security Architectures.

Abstract: Mobile Grid systems allow us to build highly complex information systems with various and remarkable features (interoperability between multiple security domains, cross-domain authentication and authorization, dynamic, heterogeneous and limited mobile devices, etc), which demand secure development methodologies to build quality software, offering methods, techniques and tools that facilitate the work of the entire team involved in software development. These methodologies should be supported by Grid security architectures that define the main security aspects to be considered, and by solutions to the problem of how to integrate mobile devices within Grid systems. Some approaches regarding secure development methodologies of Grid security architectures and of the integration of mobile devices in the Grid have been found in literature, and these are analyzed and studied in this paper, offering a comparison framework of all the approaches related to security in Mobile Grid environments.

1 INTRODUCTION

The growing need to construct secure systems, has encouraged the scientific community to demand a clear integration of security into the development processes (Jurjens 2001; Flechais, Sasse et al. 2003; Steel, Nagappan et al. 2005). However, generic software development methodologies are not appropriate for the development of every kind of software system. For instance, generic development processes are sometimes used to develop Grid specific systems (Foster, Kesselman et al. 1998; Welch, Siebenlist et al. 2003) without taking into consideration either the subjacent technological environment or the special features and particularities of these specific systems. In fact, the majority of existing Grid applications have been built without a systematic development process and are based on ad-hoc developments (Dail, Sievert et al. 2004; Kolonay and Sobolewski 2004).

The development of wireless technology and mobile devices currently enables us to access the network service from anywhere at any time (Bruneo, Scarpa et al. 2003). Provided that mobile devices have limited computing capacity, the Grid becomes an important computation service provider that enables mobile users to perform complicated jobs (Trung, Moon et al. 2005). This, however, comes at a price. Mobile computing with networked information systems increases the risks to sensitive information supporting critical functions in the organization which are open to attacks (Talukder and Yavagal 2006; Weippl, Holzinger et al. 2006).

Grid Security is hard to achieve as the resources are dynamic, heterogeneous, geographically located and under the control of multiple administrative domains (Sastry, Krishnan et al. 2007; Bhanwar and Bawa 2008). Furthermore, security in the mobile platform is even more critical owing to the open nature of wireless networks. A Grid infrastructure that supports the participation of mobile nodes will thus play a significant role in the development of Grid computing.

In this paper, we will carry out a systematic review (Kitchenham 2007) of the existing literature about different approaches related to the secure

Rosado D., Fernández-Medina E. and Lopez J. (2010).
A STUDY OF SECURITY APPROACHES FOR THE DEVELOPMENT OF MOBILE GRID SYSTEMS.
In *Proceedings of the 5th International Conference on Software and Data Technologies*, pages 133-138
DOI: 10.5220/0003005201330138

development of Mobile Grid systems, beginning with security approaches for development methodologies in information systems, and by studying whether these methodologies can be used to build mobile Grid systems. We also analyze several Grid security architectures found in literature which take into account specific security aspects for this kind of systems. Finally, we study some approaches related to how to incorporate mobile devices into an existent Grid infrastructure and the difficulties encountered when attempting to do so.

The remainder of the paper is organized as follows: In section 2, we shall analyze the different approaches studied that we believe to be most important for our comparison. In Section 3, we shall present a comparison between all the approaches related to security in the Mobile Grid and, finally, we shall show our conclusions.

2 ANALYZING APPROACHES

In this section we analyze the different approaches related to security in Mobile Grid environments. The set of approaches selected has been divided into three topics: 1) security approaches in development methodologies; 2) Security architecture for Grid environments, and 3) the incorporation of mobile devices into the Grid.

2.1 Secure Development Methodologies

2.1.1 Secure Unified Process

The Secure Unified Process (Steel, Nagappan et al. 2005) is a methodology for the integration of security into software systems, and is based in the Unified Process (Kruchten 2000). For the authors, security is represented as a set of features that fortifies the entire application or service with safeguards and countermeasures for potential risks and vulnerabilities.

2.1.2 Secure Tropos

Tropos (Bresciani, Giorgini et al. 2004) is an agent oriented software engineering methodology. Secure Tropos is a security oriented extension (Giorgini, Mouratidis et al. 2007) which includes security related concepts such as a security constraint which is defined as a restriction related to security issues, such as privacy, integrity and availability, which may influence the analysis and design of the information system under development.

2.1.3 UMLSec

UMLsec (Jurjens 2001) is proposed as an extension of UML for modelling the security properties of computer systems, according to suggestions made in (Devanbu and Stubblebine 2000). UMLsec uses standard extension mechanisms to introduce new semantics into UML models but only addresses a few specific security requirements.

2.1.4 AEGIS

AEGIS (Appropriate and Effective Guidance for Information Security) (Flechais, Sasse et al. 2003), is a secure software engineering method that integrates security requirements elicitation, risk analysis and context of use, bound together through the use of UML.

2.2 Grid Security Architectures

2.2.1 OGSA Security

The *Open Grid Services Architecture* (OGSA) (Open Grid Forum 2006) is a *service-oriented architecture* (SOA) that represents an evolution towards a Grid system architecture based on Web service concepts and technologies, autonomic computing principles, and open standards for integration and interoperability (Foster, Kesselman et al. 2002).

2.2.2 Grid Security Infrastructure - GSI

The Grid security infrastructure (GSI) was implemented as a Globus Toolkit component providing security mechanisms. The GSI has emerged as an essential middleware component that has been integrated into many tools.

2.2.3 EGEE Security

The Enabling Grids for E-sciencE (EGEE) project is funded by the European Commission and aims to build on recent advances in grid technology and develop a service grid infrastructure which is available to scientists 24 hours-a-day. The security architecture inherits many of the thoughts from previous projects and parallel ongoing efforts.

2.2.4 EGA Security

The EGA reference model defines an Enterprise Grid as being a collection of interconnected (networked) grid components under the control of a

grid management entity (Enterprise Grid Alliance Security Working Group 2005). Components have security properties and attributes, and may define specific dependencies that can be used to support the enforcement of security policies and to ensure minimal exposure.

2.2.5 Legion Security

The Legion project, developed at the University of Virginia, is an attempt to provide GRID services that create the illusion of a virtual machine (Foster and Kesselman 2004). The primary goal of the Legion security architecture is to enable participants in a GRID system to expose their resources in a manner compliant with their local policies (Ferrari 1998; Chapin, Wang et al. 1999).

2.2.6 Globe Security

Globe (Global Object Based Environment) is a wide area distributed system which was developed in order to constitute a middleware level between the operating system and the application level (van Steen, Homburg et al. 1999).

2.3 Mobile Devices in the Grid

2.3.1 Leech Approach

The authors of this approach (Phan, Huang et al. 2005) consider grid and cluster computing from a different architectural perspective, namely from the viewpoint of using small-scale, highly heterogeneous devices that can serve as nodes within a distributed grid system.

2.3.2 Mobile-to-Grid Middleware Approach

The authors present an architecture (Sajjad, Jameel et al. 2005) for a middleware enabling heterogeneous mobile devices to access Grid services by providing support to the delegation of jobs to the Grid, secure communication between the client and the Grid, offline processing and adaptation to network connectivity issues.

2.3.3 Mobile OGSI.Net Approach

The authors of this proposal investigate the use of Microsoft .NET Compact Framework and study Mobile OGSI.NET (Chu and Humphrey 2004) which is an implementation of the OGSI.NET implementation for mobile devices. The aim is to bring the benefits of Grid computing to mobile users while addressing resource limitations and intermittent network connectivity.

2.3.4 Grid-m Approach

Grid-M (Platform for Lightweight Grid Computing) (Hans A. Franke, Fernando L. Koch et al. 2007) is a platform for building Grid Computing applications in embedded and mobile computing devices. It provides the Application Programming Interface (API) to connect Java-developed applications in a Grid Computing environment and its runtime profile is small enough to be used in Mobile Computing applications.

3 COMPARISON FRAMEWORK

These approaches concerning Security in the Mobile Grid have been compared by considering a set of criteria related to different aspects of the secure development of mobile Grid systems that we believe must be studied in each approach if we are to analyze them in depth and compare whether they fulfil certain security objectives in mobile Grid environments. Therefore, criteria such as "*grid security requirements"*, "*based on grid computing"* and "*based on mobile devices"*, indicate the incorporation of aspects related to the mobile Grid. Criteria such as "*UML support"*, support tools and practice cases refer to elements which help us to apply and understand the approaches. "*Reusability"* and "*scalability*" are desirable properties in Grid systems. Criteria such as "*grid and mobile security considerations*", and "*support security policies*" are considered because they indicate the security level defined both for the grid and mobile environments of each approach and the security policy management supported. Criteria such as "*grid and mobile technology"* indicate if the current grid and mobile technologies have been used in the implementation of the approaches. Finally, "*intermediates"* and "*standards*" are criteria which indicate types of solutions applied to achieve security in the approaches.

We define these comparison criteria as follows:

- Grid Security Requirements (GSR): this indicates the set of security requirements to take into account in any Grid system such as delegation, trust, access control, global/local policies, authentication, single sign-on, etc.
- Based on Grid computing (BGC): this indicates the adaptation of the specific characteristics of

Grid computing such as anonymity, mobility, offline processing, etc.

- Based on Mobile Devices (BMD): this indicates the adaptation of the specific characteristics and limitations of the mobile devices.
- UML Support (UML): this deals with the utilization of UML models which may help us to define and design many aspects of the approaches.
- Support Tools (ST): this deals with the available tools defined to help us to apply techniques, methods and mechanisms.
- Practice Cases (PC): this indicates examples and study cases of how to apply the solutions proposed to obtain a validation of the approach.
- Reusability (REU): this deals with the reuse property of components which improve the end product and reduce time and effort.
- Intermediate (Proxy/Middleware) (INT): this deals with the availability of intermediates, both hardware and software, which complete and execute part of the work, providing a solution to a particular problem.
- Security Considerations (SC): this indicates that security considerations, specifications and features have been considered and taken into account such as PKI, encryption, flexible credentials format, secure communication, identity/keys management, security protocols and policies, etc.
- Grid and mobile technologies (GMT): this indicates that the current technologies for Grid and mobile computing are taken into account such as WTLS, IPSec, TLS, WEP, AES, RSA, ECC, and so on.
- Use of Standards (UST): this indicates the utilization of standards in the definition and implementation of methods, techniques and mechanisms which offer solutions to security problems.
- Security Policy Support (SPS): this indicates that security policies have been taken into account and are managed, controlled, defined and updated between the different Grid domains.
- Scalability (SCA): this deals with the scalability property of the solutions presented in the case of adding new elements, or the modification of existent ones.

Table 1 summarizes the main features of the proposals discussed in this paper. The values "Y", "N" and "~" indicate respectively that the criteria involved: are taken into account in the approach, are not taken into account in the approach, and are partially taken into account in the approach. "*Partially taken into account*" means that the criteria are not considered as a whole in the approach, and only one part or set is fulfilled.

Secure Unified Process uses UML to describe and specify the result models of each task or activity, and Secure Tropos is a agent oriented methodology in which security aspects are incorporated into the Tropos methodology but these approaches are not related to Grid environments and mobile devices.

UMLsec incorporates security properties into the UML model. This approach was not developed for mobile Grid environments but it is possible to model certain security aspects which are common to many systems, including mobile Grid systems. AEGIS is the only approach found in which the authors attempt to apply the methodology to Grid systems, although they do not explain how to do this, and do not define guides and practices for capturing specific security aspects in Grid systems.

OGSA represents an evolution towards a Grid system architecture based on Web Service concepts and but the lack of support for mobile devices, including security aspects, makes this incomplete for mobile Grid systems. GSI offers solutions for Grid environments in which mobile devices are not considered, and this proposal does not offer solutions for the risk and possible attacks that appear in mobile computing. EGEE Security defines practice cases and tools which help to build the middleware and build applications based on Grid computing, and which use Web service standards. EGA Security defines a grid management entity which manages a set of security functions and policies for Enterprise Grid to establish a secure connection with the grid components that participate in the system. These two approaches do not consider mobile components in the grid and consequently do not consider mobile security aspects. Legion Security defines a set of security mechanisms and policies to enable participants in a Grid system to expose their resources in a manner which is compliant with their local policies. This approach does not consider the security of mobile participants with mobile devices and a wireless network. The security considerations for Grid systems presented in Globe Security approach coincide with the security considerations for distributed systems, but are not exclusive to Grid environments. Mobile computing aspects are not taken into account.

Leech takes into account security aspects for wireless network and mobile devices through the proxy which must additionally be protected to safeguard Grid systems with mobile devices.

Table 1: Comparison framework of the analyzed approaches.

Approaches/Criteria	GSR	BGC	BMD	UML	ST	PC	REU	INT	SC	GMT	UST	SPS	SCA
SUP	N	N	N	Y	N	N	Y	N	N	N	Y	N	Y
Secure Tropos	N	N	N	N	Y	Y	N	N	N	N	N	N	N
UMLSec	N	N	N	Y	Y	Y	N	N	~	N	Y	N	Y
AEGIS	N	Y	N	Y	Y	Y	Y	N	~	N	Y	N	N
OGSA	Y	Y	N	N	Y	Y	Y	~	Y	N	Y	Y	Y
GSI	~	Y	N	N	Y	Y	Y	~	Y	Y	Y	Y	N
EGEE Security	Y	Y	N	N	Y	Y	N	N	Y	~	Y	Y	Y
EGA Security	N	Y	N	N	Y	N	N	N	Y	~	Y	Y	N
Legion Security	~	Y	N	N	N	Y	N	~	N	~	Y	Y	Y
Globe Security	N	~	N	N	Y	Y	N	N	~	Y	N	N	Y
Leech	N	Y	Y	N	Y	N	N	Y	Y	Y	Y	N	Y
Mobile-To-Grid	N	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y
Mobile OGSI.net	N	Y	Y	N	Y	N	Y	Y	N	Y	Y	N	Y
Grid-M	N	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N	Y

Mobile-To-Grid contains security services, based on GSI, that permit the secure communication between the mobile user, the middleware and the Grid. This approach treats mobile devices like external elements and the security must be implemented outside the Grid environment. Mobile OGSI.net extends an implementation of grid computing, OGSI.NET, to mobile devices. This approach does not specify security aspects for these environments, and only defines connection modules between Grid services and mobile services. Grid-M defines new functionalities of security for mobile devices and uses an API to connect applications in Grid environments and mobile devices; however, the security of this API is not within the Grid security environment and may cause risks and vulnerabilities in the system.

4 CONCLUSIONS

With regard to the proposals discussed in this paper, we can conclude that no proposal covers all the security criteria for building mobile Grid Systems. As regards the various security methodologies proposed, we can see that none of them, with the exception of the AEGIS approach, is designed to build Mobile Grid Systems.

Many proposals for Grid system security architectures and scalable approaches which use standards for their implementation also exist, but these offer no solutions to the incorporation of mobile devices or consider the security aspects that are so important in mobile computing. Finally, various proposals concerning the incorporation of mobile devices into Grid systems exist, but this incorporation takes place outside the Grid through intermediaries. These approaches do not regard mobile devices as being part of the Grid's own resources.

We can therefore conclude that there is a need for an integration element in which a systematic development process is defined that is capable of analyzing the security requirements and necessities for Grid systems with mobile devices from the first stages of development. It is necessary to design a reference security architecture for the Mobile Grid which is reusable and scalable and can be incorporated into any development, offering guidelines, methods and mechanisms to protect this type of systems, and in which the mobile devices are treated as resources of the Grid environment itself, and not as external elements incorporated by intermediaries.

ACKNOWLEDGEMENTS

This research is part of the following projects: QUASIMODO (PAC08-0157-0668), SISTEMAS (PII2I09-0150-3135) and SEGMENT (HITO-09-138) financed by the "Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha" (Spain) and FEDER, and MEDUSAS (IDI-20090557) and BUSINESS (PET2008-0136) financed by the "Ministerio de Ciencia e Innovación (CDTI)" (Spain).

REFERENCES

Bhanwar, S. and S. Bawa (2008). Securing a Grid. World Academy of Science, Engineering and Technology.

Bresciani, P., P. Giorgini, et al. (2004). "TROPOS: An agent-oriented software development methodology." *Journal of Autonomous Agents and Multi-Agent Systems 8*(3): 203-236.

Bruneo, D., M. Scarpa, et al. (2003). Communication paradigms for mobile grid users. *3rd IEEE/ACM International Symposium on Cluster Computing and the Grid* (CCGRID'03).

Chapin, S., C. Wang, et al. (1999). "A New Model of Security for Metasystems." *Future Generation Computer Systems* 15(5-6): 713-722.

Chu, D. and M. Humphrey (2004). Mobile OGSI.NET: Grid computing on mobile devices. *5th IEEE/ACM International Workshop on Grid Computing - Grid2004 (at Supercomputing 2004).*

Dail, H., O. Sievert, et al. (2004). Scheduling In The Grid Application Development Software Project. *Grid resource management:* state of the art and future trends: 73-98.

Devanbu, P. T. and S. G. Stubblebine (2000). Software engineering for security. *22th International Conference on Software Engineering,* ACM Press.

Enterprise Grid Alliance Security Working Group. (2005, 8 July 2005). "Enterprise Grid Security Requirements Version 1.0."

Ferrari, A., Knabe, F., Humphrey, M., Chapin, S., Grimshaw, A. (1998). A Flexible Security System for Metacomputing Environments. T. R. CS-98-36, Department of Computer Science. Univ. of Virginia.

Flechais, I., M. A. Sasse, et al. (2003). Bringing Security Home: A process for developing secure and usable systems. *New Security Paradigms Workshop (NSPW'03),* Ascona, Switzerland.

Foster, I. and C. Kesselman (2004). The Grid2: Blueprint for a Future Computing Infrastructure. San Francisco, CA, *Morgan Kaufmann Publishers; 2 edition.*

Foster, I., C. Kesselman, et al. (2002). The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. *Open Grid Service Infrastructure WG*, Global Grid Forum.

Foster, I., C. Kesselman, et al. (1998). A Security Architecture for Computational Grids. *5th Conference on Computer and Communications Security*, San Francisco, USA, ACM Press.

Giorgini, P., H. Mouratidis, et al. (2007). Modelling Security and Trust with Secure Tropos. Integrating Security and Software Engineering: Advances and Future Visions. H. M. a. P. Giorgini, Idea Group Publishing: 160-189.

Hans A. Franke, Fernando L. Koch, et al. (2007). Grid-M: Middleware to Integrate Mobile Devices, Sensors and Grid Computing. T*hird International Conference on Wireless and Mobile Communications (ICWMC'07)* Guadeloupe, French Caribbean.

Jurjens, J. (2001). Towards Development of Secure Systems Using UMLsec. *Fundamental Approaches to Software Engineering* (FASE/ETAPS).

Kitchenham, B. (2007). Guideline for performing Systematic Literature Reviews in Software Engineering. Version 2.3, University of Keele (Software Engineering Group, School of Computer Science and Mathematics) and Durham (Department of Conputer Science).

Kolonay, R. and M. Sobolewski (2004). Grid Interactive Service-oriented Programming Environment. Concurrent Engineering: The Worldwide Engineering Grid, Tsinghua, China, *Press and Springer Verlag.*

Kruchten, P. (2000). The Rational Unified Process: An Introduction, Addison-Wesley.

Open Grid Forum (2006). The Open Grid Services Architecture, Version 1.5.

Phan, T., L. Huang, et al. (2005). Chapter 5: Integrating Mobile Wireless Devices Into the Computational Grid. Mobile Computing Handbook. M. Ilyas and I. Mahgoub, Auerbach Publications.

Sajjad, A., H. Jameel, et al. (2005). AutoMAGI - an Autonomic middleware for enabling Mobile Access to Grid Infrastructure. *Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services.*

Sastry, M., R. Krishnan, et al. (2007). A New Modeling Paradigm for Dynamic Authorization in Multi-Domain Systems. *Fourth International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Saint Petersburg, Russia.

Steel, C., R. Nagappan, et al. (2005). Chapter 8. The Alchemy of Security Design Methodology, Patterns, and Reality Checks. Core Security Patterns:Best Practices and Strategies for J2EE, Web Services, and Identity Management, Prentice Hall: 1088.

Talukder, A. and R. Yavagal (2006). Chapter 18: Security issues in mobile computing. *Mobile Computing, McGraw-Hill Professional.*

Trung, T. M., Y.-H. Moon, et al. (2005). A Gateway Replication Scheme for Improving the Reliability of Mobile-to-Grid Services. *IEEE International Conference on e-Business Engineering (ICEBE'05).*

van Steen, M., P. Homburg, et al. (1999). "Globe: A Wide-Area Distributed System." IEEE Concurrency: 70-78.

Weippl, E., A. Holzinger, et al. (2006). "Security aspects of ubiquitous computing in health care." *Elektrotechnik und Informationstechnik* 123(4):156-161.

Welch, V., F. Siebenlist, et al. (2003). Security for Grid services. 1*2th IEEE International Symposium on High Performance Distributed Computing* (HPDC-12 '03), IEEE Computer Society.