Security Measurement Model for Large Scale Dynamic Systems *

Syed Naqvi, Michel Riguidel

Computer Science and Networks Department
École Nationale Supérieure des Télécommunications
46 Rue Barrault, 75013 Paris, France
{naqvi, riguide}@enst.fr

Abstract

This article presents an overview of our proposed Security Management Model (SMM) for large scale dynamic systems. The goal of the SMM is to offer a simplified view of the overall system by taking into consideration the relevant data for the evaluation of the security assurance. A new thin infrastructure composed of the data/information relevant to the security evaluation of the system and services is proposed in SMM.

1. Introduction

Traditionally, network administrators handle privileges, exceptions, policies and other security settings; however, today's exponential growth of the mobile networks and their dynamic interconnections have made it impossible for the network administrators to manually handle all the security functions. Moreover, the increasing complexity of these heterogeneous networks has lead to a number of security flaws. Any change or adjustment in a highly dynamic context is prone to inconsistencies that result in the serious security vulnerabilities. Hence it is desirable to develop security assurance infrastructure that can monitor and manage the overall state of security at any instant of time. This security assurance infrastructure requires interaction with the core security infrastructure, so that the authorizations, exceptions, and security management as a whole, can be achieved. The provision of such security assurances is the prime objective of the BUGYO Project [1].

The rest of the paper is organized as: A brief description of the project BUGYO is given in section 2. The Security Management Model (SMM) is presented in section 3. Some conclusions are drawn in section 4 with a note of our future directions.

* *This research is supported by the European Eureka-Celtic Project BUGYO (Building Security Assurance in Open Infrastructures) under reference number CP02-002*

2. The BUGYO Project

The BUGYO project aims to define a security framework to measure, document and maintain the security assurance level of services based on telecommunications system. The project intends to fill the current gap of a general way to measure the confidence that operators and end customers can have in the security of the infrastructure, in end-to-end security services and in the security of end-to-end services above those architectures.

The main focus of the BUGYO project is to build a framework providing integrated means to measure the security assurances of a telecommunications infrastructure and the overlay services in open infrastructures. The project addresses security as a full system approach, and the major expected result is a system security assurance framework including methodologies, control metrics and measures, best practices, tools and a certification cockpit. The *security cockpit* represents the interface for the operator or the service provider to perform necessary operations in order to obtain and maintain a security assurance level for a specified service.

3. The Security Measurement Model (SMM)

3.1. Overview

The main idea behind the proposed modeling follows the originally proposed Web model [2] for document interlinking. If a subject s is a logical entity related to an object of evaluation. s obtains a well-formatted document d_s that is established on demand by an appropriate agent b_s. These agents are designed to be able to gather security assurance related information about s. The document d_s is specific to the particular requirements on s. In other words, the different entities are not the same and possess different document formats and agents. The security cockpit can be used at any time to connect to one of the deployed b_s to visualize the network map and the deployment of the updated implementation of any b_i. Metaphorically, s can be considered as a web-server serving a specific dynamically generated webpage d_s and is dynamically established by b_s.

In this metaphor, the security cockpit appears as a web-browser and as an independent web-crawler.

3.2. Proposed Model

Our proposed model is a directed graph of security assurance related documents starting with the object of evaluation (typically a service) at the root. According to this model, every logical, service-related entity s is represented by its security assurance related document d_s. The edges of this graph are security evaluation related dependencies, represented by arrows. The applied semantics of an arrow leading from a document d_A to a document d_B is "d_A's security assurance depends on d_B's security assurance". In other words, to evaluate the security assurance of the entity A, one needs to consider the security evaluation of an entity B.

In a dynamic view, we need to represent data flows. That is why every instantiation of the presented model is required to provide a special format for data flows (i.e. sessions, flows, exchanges, etc.) A data flow has a source and a destination. It typically traverses various entities. Thus, its security assurance evaluation typically depends on several entities.

The BUGYO project has considerable performance constraints and, hence, it requires efficient mechanisms. These constraints give birth to the idea of defining a new infrastructure composed of the data/information relevant to the security evaluation of the system and services. The resulting simplified database will form a Security Assurance Information Base (SAIB). A SAIB is a collection of information that can be managed by the cockpit and is relative to a subject or an object of the system. The SAIB allow the cockpit to evaluate the security assurance of this subject or object.

A topological graph allows the cockpit to join the different SAIB and to collect the information relative to the security assurance of all the subjects and the objects. In order to evaluate the overall security assurance of the infrastructure the cockpit has to know the dependencies between these subjects and objects. The cockpit evaluates the overall security assurance of the system and the management team is informed of the current assurance level.

3.3. Open Issues

This work is still in progress and hence there are some open issues that require further research considerations. A list of some of these open and working issues is provided in this section:

Identification of the entities to be measured: Security assurance *metrics* are fundamental for the identification of the entities to be measured or a set of measurable, direct and indirect, security relevant and security enforcing entities that can be mapped to specified security assurance metrics.

Determination of the granularity of the various entities: The sets of entities and relations constitute the system model. They are the basis for the system security assurance measurement. In some cases, the entities of a system are complex themselves and, possibly, referred to as subsystems, which in turn are divided into entities.

Quantification of the security assurance with two proposed graphs: Methods aggregating the results for individual system entities, possibly including other factors, to system-wide security assurance values are needed.

Semantically expressed assurance: Some mechanisms are needed to express semantically the assurances. It may lead to the evolution of a Security Assurance Language. Questions are: does SMM need a *new* language? Does SMM require a *descriptive* or an *executable* language?

How to guarantee the security of the cockpit: What about the Security Management Model if the cockpit itself is attacked?

Evaluation of the usability of the proposed model: This is one of the core issues of the project: how to use the SMM to proceed to security assurance evaluation? Which set of security related characteristics and entities have to be considered? Which classification of basic model entities has to be made? Which metrics will be used? Which dependency and topological graph should be used?

4. Conclusions and Future Directions

Complexity of large scale dynamic systems is a major obstacle to measure the security assurance. These systems have to be modeled in such a way that security relevant and security enforcing entities to be measured are captured. The Security Management Model (SMM), briefed in this paper, is an effort towards the adequate representation of security assurance mechanism of such systems.

This work is still in its nascent state with a number of open issues. We foresee that in the coming months, a refined SMM will be emerged with comprehensive analytical validations. This stage will be followed by the implementation of the model on a real test-bed.

5. References

1. The Eureka-Celtic Project BUGYO – http://projects.celtic-initiative.org/bugyo
2. The Web Model– http://www.w3.org/DesignIssues/Model.html