Chapter 10
Using Indicators to Monitor Security Risk in Systems of Systems:
How to Capture and Measure the Impact of Service Dependencies on the Security of Provided Services

Olav Skjelkvåle Ligaarden
SINTEF ICT & University of Oslo, Norway

Atle Refsdal
SINTEF ICT, Norway

Ketil Stølen
SINTEF ICT & University of Oslo, Norway

ABSTRACT

Systems of systems are collections of systems interconnected through the exchange of services. Their often complex service dependencies and very dynamic nature make them hard to analyze and predict with respect to quality in general, and security in particular. In this chapter, the authors put forward a method for the capture and monitoring of impact of service dependencies on the security of provided services. The method is divided into four main steps focusing on documenting the system of systems and IT service dependencies, establishing the impact of service dependencies on risk to security of provided services, identifying measureable indicators for dynamic monitoring, and specifying their design and deployment, respectively. The authors illustrate the method in an example-driven fashion based on a case within power supply.

DOI: 10.4018/978-1-4666-2083-4.ch010

INTRODUCTION

In today's business environment, companies (businesses, enterprises, organizations) co-operate with other parties by providing and/or requiring information and communication technology (ICT) supported services. The ICT-systems facilitating such co-operation are often so-called system of systems (SoS). An SoS may be thought of as a kind of "super system" comprising a set of inter-connected systems that work together towards some common goal.

(Allen, 2005) defines governance as "*setting clear expectations for the conduct (behaviors and actions) of the entity being governed, and directing, controlling, and strongly influencing the entity to achieve these expectations.*" In an SoS setting, a company is often expected to provide services fulfilling requirements to security. If the services are not provided according to their security requirements, then it may have severe consequences for the company providing them. Thus, the company needs to govern the security of the provided services. Risk assessment is a necessity for ensuring that risks to security of provided services are at an acceptable level. However, it is not straight-forward to assess risk to security of provided services in an SoS. Firstly, the exchanged services may require other services in order to function. Such requirements result in so-called service dependencies. Change in the security attributes of one service may easily cause the security attributes of its dependent services to change as well. Secondly, the different systems may be under different managerial control and within different jurisdictions. For the systems that are outside our control, we have limited knowledge of their security risks, structure, and behavior. Thirdly, such a large number of systems, controlled and operated by different parties, evolve rapidly in a manner that may be difficult to predict.

To cope with this situation we propose the use of detailed dependency models to capture the impact of services dependencies, trust relations as a basis for analysis in the case of insufficient documentation, and monitoring to cope with evolution. Our main result is a method facilitating the set-up of such monitoring. This method can be used in security governance for the purpose of assessing to what extent the security expectations to the provided services are achieved.

The method is divided into four steps. Service dependencies and trust relations are identified and documented in the first step. In the second step we conduct a security risk analysis to capture the impact of service dependencies on risk to security of provided services. The identified trust relations are used when analyzing service dependencies involving systems of which we have insufficient documentation. In the third step we identify the security risks to be monitored, as well as measureable indicators for monitoring their risk values. In the fourth and final step we specify how these indicators should be designed, i.e., how they should be calculated, and deployed in the SoS, i.e., how data needed in the calculations should be extracted and transmitted within the SoS in question. The result of applying the method is a security risk picture parameterized by indicators, each defined by design and deployment specifications.

The rest of the chapter is organized as follows: in the next section (Section 2) we introduce basic terminology and definitions. Section 3 presents the methodological approach, while the four steps of the approach are demonstrated on an example case within power supply in Sections 4 – 7. In Section 8 we present related work, while we conclude and indicate further research in Section 9.

BASIC TERMINOLOGY AND DEFINITIONS

In this section we provide basic terminology, definitions, and conceptual models for system of systems, risk, and related concepts.