Chapter 6
Security of Dependable Systems

Naveed Ahmed
Technical University of Denmark, Denmark

Christian Damsgaard Jensen
Technical University of Denmark, Denmark

ABSTRACT

Security and dependability are crucial for designing trustworthy systems. The approach "security as an add-on" is not satisfactory, yet the integration of security in the development process is still an open problem. Especially, a common framework for specifying dependability and security is very much needed. There are many pressing challenges however; here, we address some of them. Firstly, security for dependable systems is a broad concept and traditional view of security, e.g., in terms of confidentiality, integrity and availability, does not suffice. Secondly, a clear definition of security in the dependability context is not agreed upon. Thirdly, security attacks cannot be modeled as a stochastic process, because the adversary's strategy is often carefully planned. In this chapter, we explore these challenges and provide some directions toward their solutions.

INTRODUCTION

We are increasingly dependent on complex and advanced technology systems. Usually we realize this dependence only when such a system fails. For example, the cloud of ashes, resulting from a volcanic eruption on Iceland (Shukman, 2010), grounded most of the aircrafts in Europe and made millions of travelers realize how much their lives depend upon the correct operation of air traffic.

We often decide to take the risk of being dependent on certain systems. From a rational point of view, the property that allows trusting such systems is called dependability. When implementing dependability measures, it is important to determine the economic value of a system; if a system is not constrained by the cost then its dependability is the decisive metric to judge the feasibility of producing the system. Let us consider a few applications, in which the dependability is vital for their practical use. The readers should

DOI: 10.4018/978-1-4666-4707-7.ch006

note that different applications have potentially different dependability requirements.

The Air Traffic Control (ATC) makes the day-to-day operations possible for the commercial aviation. ATC is a worldwide system that manages the air-traffic, prevents mid-air collisions and guides pilots to safely reach their destinations. Therefore, a safe and 24-hours available ATC system is necessary. For the ATM terminals of banks, availability and security are important, in order to prevent any malicious or accidental loss of money while also delivering the expected level of service to the customers. In an automobile, the reliable operations of the steering wheel and the braking system are the matter of life or death for the driver. In the healthcare sector, X-ray machines are widely used but their safety against the accidental leakage of radiation is vital for the health of operators and patients.

Although the precise definition of dependability is a subject of discussion, many people consider dependability as the ability to deliver a service that can be trusted (Avizienis, Laprie, Randell and Landwehr, 2004). The requirements of service define the intended behavior of a system, e.g., data storage, stock management, social networking and air travelling. The societal value of a system is only due to the usefulness and the demand of its service.

The prefix "critical" in a system name is often used to emphasize that the failure to deliver the service might have serious consequences, e.g., on the human's health or on the environment. These systems are further classified under the names of safety-critical, mission-critical and security-critical systems. A critical system requires an accurate assessment of its dependability so that the relevant service can be guaranteed[1]. In a different context, the same prefix critical is used with the name of an individual component of a system to indicate that the correct operation of the component is necessary for the correct operation of the system.

Dependability requirements are not merely associated with complex or critical systems. In fact, every man-made system (no matter how big or small it is) needs to be dependable, although the actual requirement of dependability may differ. For instance, consider a chair, which is not a mission-critical system. Still, a certain level of dependability is required to make it useful; for example, the chair should be reliable enough to be usable by a person weighing up to 120 kg, and its service (sitting function) should have a certain level usability in terms of comfort. Such non-critical systems, however, are not very interesting for an advanced dependability analysis.

For many simple systems, dependability is trivial to achieve; for instance, a program that calculates the factorial of a number is easy to write so that it behaves safely, i.e., it may suffice to check the input to ensure that it is not too large or negative, which could cause the program to loop forever. On the other hand, writing a control application for an autonomous medical robot (e.g., a robot surgeon) is a pretty daunting task, which may require the use of formal methods to guarantee safe operation. More advanced techniques for dependability analysis, such as continuous-time Markov chains (Nicol, Sanders and Trivedi, 2004), are often used to evaluate complex and critical systems.

The description in this chapter, however, is independent of the problem of designing a dependable system; rather we focus on how to define and specify the security aspect of the system. We employ the following notations in this chapter: We use an *italic* font for a term when its precise use is required in that context; we use the term *classic dependability* to refer to the dependability that does not include any security requirement; we use the terms *attacker* and *adversary* interchangeably. We use the term *non-security* for a property that is not a security property. We use the term *insecurity* if an expected security property is absent.