Methods for Dependability and Security Analysis of Large Networks

Ioannis Chochliouros
OTE S.A., General Directorate for Technology, Greece

Anastasia S. Spiliopoulou
OTE S.A., General Directorate for Regulatory Affairs, Greece

Stergios P. Chochliouros
Independent Consultant, Greece

INTRODUCTION

Dependability and security are rigorously related concepts that, *however*, differ for the specific proprieties they mainly concentrate on. In particular, in most commonly applied cases found in practical design techniques (Piedad & Hawkins, 2000), the dependability concept usually includes the security one, being a superset of it. In typical cases, security mainly comprises the following fundamental characteristics: confidentiality, integrity, and availability. Indeed, dependability mainly encompasses the following attributes (Avizienis, Laprie, Randell, & Landwehr, 2004): (1) availability: readiness for correct service; (2) reliability: continuity of correct service; (3) safety: absence of catastrophic consequences on the user(s) and the environment; (4) confidentiality: absence of unauthorized disclosure of information; (5) integrity: absence of improper system alterations; and (6) maintainability: ability to undergo modifications and repairs. The present work primarily intends to deal with formal methods, appropriate to perform both security and dependability analysis in modern networks.

In general, security analysis of great networks takes the form of determining the exploitable vulnerabilities of a network, and intends to provide results or appropriate informative (or occasionally experimental) data about which network nodes can be compromised by exploiting chains of vulnerabilities, as well as specifying which fundamental security properties are altered (e.g., Confidentiality, Integrity, Availability). Therefore, such type of analysis is also referred as "network vulnerability analysis." On the other hand, dependability analysis of networks typically intends to determine specific dependencies within the nodes (or the services offered) of the (appropriate) underlying network, so as to provide results about the consequences of (potential) faults (on services or hosts) and to find out which among these faults are able to cause unacceptable consequences, in terms of the basic dependability attributes. At this specific evaluation, it should be noted that it is possible to consider attacks (as well as attack consequences) as faults.

A great variety of formal modeling and analysis techniques for dependability evaluation can be applied in the security domain (and vice-versa) (Nicol, Sanders, & Trivedi, 2004). Nevertheless, there is an important difference between the accidental (or unintentional) nature of faults (which are commonly considered in dependability assessment) and the intentional, human nature of cyber attacks. In fact, faults can only be realistically modeled by taking into account their probabilistic occurrences, while attacks due to the intentionality nature of a (potential) intruder, are more likely to be simply considered as "possible" or "impossible," although it can even be of extreme interest to consider their probabilities of success in order to determine the likelihood of attack paths. However, in a more general approach, dependability evaluation implicates the performance of a more sophisticated analysis (usually stochastic) because it likes to consider the probability of faults and the acceptability of faults' consequences. Anyway, it should be mentioned that when there is no particular interest in providing a quantitative evaluation of dependability, then it results that there is no practical need to model the likelihood

of faults. Therefore, the same techniques used to perform classical security analysis can be used to perform dependability analysis, with satisfactory results.

It is quite remarkable to point out the fact that the two separate suggested methods of analysis have many common features. Among other aspects they share the following options:

- They require the retrieval of many informative data from the selected nodes of the underlying network, in order to build the necessary models, for further assessment.
- They both work on dependency models. Vulnerability analysis can be performed on dependency model of vulnerabilities, while dependability analysis uses models that represent more general dependencies.
- They need to know the requirements for each specific (dependability or security) attribute. This is usually done in terms of the severity of failure of systems and services (e.g., in terms of costs) or in terms of its acceptability, that can be either expressed in absolute terms (typically for security) or in terms of an acceptable probability or frequency (usually for dependability).
- They need to perform a scalable analysis in order to be able to handle real networks.

In the following parts of the present work we examine the state-of-the-art of modern dependability analysis in parallel with current issues affecting further development. In addition, we examine and evaluate the basic context for performing security analysis. Both attempts have been performed in the scope of large networks.

BACKGROUND: CURRENT ISSUES OF MODERN DEPENDABILITY ANALYSIS

The International Federation for Information Processing Working Group 10.4 (www.dependability.org) defines dependability as the "trustworthiness of a computing system which allows reliance to be justifiably placed on the services it delivers." It should be noted that the concept of "Reliance" is contextually subjective, because it depends on the particular needs of an organization. In fact, different organizations like to focus on different systems attributes, such as availability, performance, resilience to failures, and ability to not be subject to catastrophic failures, as well as different levels of adherence to such attributes. Additionally, an attribute can have different meanings, depending on the specific contexts the definition applies.

In modern applications, it is quite interesting to examine services offered by the existing infrastructures or networks, and more specifically dependability analysis of Web services and of network survivability (Shoniregun, Chochliouros, Laperche, Logvynovski, & Spiliopoulou-Chochliourou, 2004). Thus, a service can be considered as "dependable" if it is trustworthy. For this reason, next to the security aspects, in this case dependability also implicates reliability, availability, and safety. The consequences on such properties are widely influenced by faults that, in turn, cause errors in the actual state of the relevant service offered. Errors (as well as attack consequences) are perceived by the users of a service as failures, that is, deviations of the delivered service from its standard specification, intended for commercial (or any other) use and deployment. For some of the dependability attributes (specifically for reliability, availability, and safety) there exist several probability-based theoretic foundations enabling the dependability analysis. In practice, the aim of a formal analysis (or applied method) is to estimate and predict the values of these dependability attributes, based on some property values (e.g., failure rate, redundancy, etc.) that characterize the basic components of the system. (For example, the goal of reliability analysis is to determine the probability that the system continues to provide services for a particular time period, such as a predetermined mission time).

A typical dependability analysis process mainly requires to: (1) determine possible dependencies among components, systems (e.g., hosts), or services; (2) establish the probabilities of faults for each component, system, or service; (3) decide the acceptability of faults, in term of consequences to dependability attributes; (4) build a model that efficiently represents dependencies; and (5) analyze further the constructed model to provide measurement of fault consequences in terms of dependability attributes, and detailed results about which components of the system do not adhere to a specified acceptability of a (well defined and appropriately examined) fault consequence.

It is possible to make a distinction between two types of formal analysis: qualitative and quantitative. The aim of the former is to determine what the components (or services) are that are deteriorated (or blocked) by faults