Chapter 1.11
Security Assessment of Networks

Aftab Ahmad
Norfolk State University, USA

ABSTRACT

In this chapter, a novel performance model for assessing security of a layered network has been proposed. The work is motivated by the fact that there is a need for a reference framework to account for all threats to a networked system. There are few such models available, and one of them is recommended by the International Telecommunications Union (ITU). The proposed assessment model is based on the ITU security framework, recommended in the ITU-T Recommendation X.805. We employ this model to quantify network security against five threat categories mentioned in the recommendations. The quantification has been done based on the recommended measures against all threats. A threat vector has been proposed that defines required measures for a particular threat category. Other vectors, such as the security implementation vector define how effectively these measures are implemented in a given device, system, or network. As a simple application of the proposed model, the security provided by the IEEE 802.15.4 standard is analyzed, viewing it as an 'end-to-end' system (e.g., for ad hoc sensor network applications). The proposed security assessment model can be applied to any type of network (wireless, wired, optical, service oriented, transport, etc.). The model can be employed to obtain security assessment in the form of five security metrics, one for each threat category (destruction, corruption, removal, disclosure, and interruption). An expression for the overall security against all threats has also been derived.

DOI: 10.4018/978-1-61350-101-6.ch111

1. INTRODUCTION

Security provisioning has become an essential part of network architecture standardization process. Every new standard in networking, be it an interface standard, link level, routing level or end-to-end level, has some features to secure the exchange of information. This has resulted in a boost of user confidence in using network infrastructure for sensitive data, such as business plans, credit cards and other ecommerce applications. The open competition staged by NIST to decide the Rijndael algorithm for the Advanced Encryption System (AES) is a testimony to the international cooperation for securing information in computers. Standardization of SHA Hash algorithm has strengthened the data integrity solutions. The public key infrastructure (PKI), perhaps not as well-defined as we might like it to be, is gearing towards as secure a communications between a business and its customers as there can be. Third party Digital Certificates (DC) are used quite commonly, making non-repudiation a thing of the present rather than future. There are, in fact, measures for all security threats and usually it is the human error that results in successful attacks rather than a breaking of encryption algorithms. In the midst of all these developments, we have forgotten a fundamental concept of comparing commodities – security being the commodity in this case. The fundamental concept in question is the measurement of security. If we could measure security, we could shop for it and quantify our level of confidence in the security system that we install. While fundamental breakthroughs are needed to define security measurement systems, the next best thing is to have assessment solutions for comparative analysis of security systems in networks. This Chapter addresses the same issue for networked systems. The main goals of this chapter relate to underlining the need for security assessment as well as proposing an assessment model for networkable systems. The proposed system gets as close to measuring the security as current state-of-research allows and provides a direction to designing full-fledged security performance models, as more research becomes available.

We show in this Chapter that the ITU-T Network Security Framework (X.805) can also be employed in deriving a performance model for assessing a security system. The Chapter is organized as follows: in the next section, the problem background is discussed along with current research. Following the background discussion, an account of security components is presented that also includes the basic structure of the ITU-T X.805 recommendation. This is followed by the proposed usage of X.805 in developing a security assessment model. An application of the model is included to assess the security provided by the popular sensor network standard IEEE 802.15.4. Following this example are Future Research Directions, Conclusions and References.

2. BACKGROUND

Information assurance systems have evolved into highly complex systems, based on a large number of sub-systems and components. There are too many factors that influence the performance of a security system. Even a small part of it can be quite complex to analyze. For example, an encryption algorithm has to be complex enough so that it can't be reverse-engineered even if publicized, such as what happened with RC4. There are many ways in which an encryption algorithm can be compromised; it could have weak key generation, distribution or/and regeneration mechanisms, weak random number generation mechanism, or simply could allow one of the several attacks (Heys, 2010). In networked systems, information assurance can be even more challenging as the sources of compromise multiply due to a number of protocol layers and types of activities (user data exchange, signaling information exchange or management data). Consequently, each activ-