Chapter 1
Network Security

Ramakrishna Thurimella
University of Denver, USA

Leemon C. Baird III
United States Air Force Academy, USA

ABSTRACT

Three pillars of security—confidentiality, integrity, and availability—are examined in the context of networks. Each is explained with known practical attacks and possible defenses against them, demonstrating that strong mathematical techniques are necessary but not sufficient to build practical systems that are secure. We illustrate how adversaries commonly side-step cryptographic protections. In addition, we contend that effective key management techniques, along with privacy concerns must be taken into account during the design of any secure online system. We conclude with a discussion of open problems for which fundamentally new methods are needed.

INTRODUCTION

Confidentiality, integrity and availability, often abbreviated CIA, are key security requirements in any risk analysis. In short, confidentiality is the privacy of an object, integrity is the trustworthiness and dependability (accuracy and consistency of information), and availability refers to the fact that a resource can reliably be used when desired. Stamp (2006) contains more detailed definitions of these concepts.

DOI: 10.4018/978-1-61520-783-1.ch001

The most common use of cryptography online is to provide confidential and authenticated communication between two parties, either in the context of web transactions or for remote access. In order to accomplish this, one needs an effective key management scheme. As a way of demonstrating that many security concepts are intertwined, we present keyless jam resistance, a method that can broadcast messages using radio frequency communication without any prior secret shared between the sender and receiver.

Possibly the most difficult to achieve form of confidentiality is privacy of the identity of an individual performing some action, more com-

monly referred to as anonymity. While a common security goal is non-repudiation—the assurance that an individual can not retract his responsibility for an action—it's dual, the ability to disclaim responsibility for an action can be equally desirable. Modern mechanisms for generating anonymity combine the use of large groups of operators with a public-key infrastructure and data encryption to decouple an individual's action from their identity.

The remainder of this chapter is organized as follows. The following section presents the necessary background material for this chapter. Next we discuss confidentiality and integrity. After that, a key aspect of privacy, online anonymity, is discussed. Availability is described throughout the chapter and discussed briefly in a separate section. Key Management section presents a comprehensive list of methods to distribute secret keys. Wireless Availability section shows how to eliminate the need for keys by presenting a novel algorithm to do jam resistance communication. We conclude with a discussion of open problems in the last section.

BACKGROUND

In this section, we begin with the basics of cryptography, pointing out the difference between symmetric and asymmetric encryption, followed by a description of the Diffie-Hellman key exchange protocol. Next, we present an abstract description of the man-in-the-middle attack. After that, we give some networking details that are necessary to understand a concrete man-in-the-middle attack on modern local-area networks.

Cryptography

We first begin with a general discussion on cryptography. Figure 1 shows the process of encryption followed by a description. First, the plaintext is transformed into cipher text by applying a key K_e. Applying another key K_d, possibly different from K_e, retrieves the original.

In symbols, this process is shown as $P = D(K_d,E(K_e,P))$.

The encryption and decryption methods, when combined, are known as a *cipher*. When the decryption key is the same as the encryption key, or efficiently derivable from it, the process is known as *symmetric* encryption; otherwise, it is called *asymmetric* encryption. Two popular symmetric encryption methods are Advanced Encryption Standard (AES) (Daemen & Rijmen, 2002) and Triple Data Encryption Standard (3DES) ("Data Encryption Standard," (2009)). The main difficulty with symmetric encryption is *key distribution*—getting the communicating parties to agree upon a common key. This problem is discussed at length later in the Chapter.

In public key cryptography, each communicating entity maintains one private key and one public key, K_{priv} and K_{pub} respectively. Extending the previous notation, asymmetric encryption can be shown as $P = D(K_{priv},E(K_{pub},P))$.

As the names imply, the public key is made available freely to anyone who wishes to use it, but the private key is kept secret. So, if Alice wishes to communicate with Bob, she encrypts the message with Bob's public key (which is openly available) and sends the encrypted message to Bob. Anyone eavesdropping on this communication cannot de-

Figure 1. Process of encryption and decryption