Lecture 10: Key Distribution for Symmetric Key Cryptography and Generating Random Numbers

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

February 10, 2017
9:33am

©2017 Avinash Kak, Purdue University

Goals:

- Why might we need **key distribution centers**?
- **Master key** vs. **Session key**
- The **Needham-Schroeder** and **Kerberos** Protocols
- Generating **pseudorandom** numbers
- Generating **cryptograhically secure pseudorandom** numbers
- Hardware and software entropy sources for **truly random** numbers
- **A word of caution regarding software entropy sources**

CONTENTS

10.1: THE NEED FOR KEY DISTRIBUTION CENTERS

- Let's say we have a large number of people, processes, or systems that want to communicate with one another in a secure fashion. Let's further add that this group of people/processes/systems is not static, meaning that the individual entities may join or leave the group at any time.

- A simple-minded solution to this problem would consist of each party physically exchanging an encryption key with every one of the other parties. Subsequently, any two parties would be able to establish a secure communication link using the encryption key they possess for each other. **This approach is obviously not feasible for large groups of people/processes/systems, especially when group membership is ever changing.**

- A more efficient alternative consists of providing every group member with a single key for securely communicate with a **key distribution center** (KDC). This key would be called a **master key**. When A wants to establish a secure communication link with B, A requests a **session key** from KDC for communicating with B.

- In implementation, this approach must address the following issues:
  - Assuming that A is the initiator of a session-key request to KDC, when A receives a response from KDC, how can A be sure that the sending party for the response is indeed the KDC?
  - Assuming that A is the initiator of a communication link with B, how does B know that some other party is not masquerading as A?
  - How does A know that the response received from B is indeed from B and not from someone else masquerading as B?
  - What should be the lifetime of the session key acquired by A for communicating with B?

- The next section presents how the Needham-Schroeder protocol addresses the issues listed above. A more elaborate version of this protocol, known as the Kerberos protocol, will be presented in Section 10.3.

10.2: THE NEEDHAM-SCHROEDER KEY DISTRIBUTION PROTOCOL

A party named A wants to establish a secure communication link with another party B. Both the parties A and B possess **master keys** K_A and K_B, respectively, for communicating privately with a **key distribution center** (KDC). [In a university setting, there is almost never a need for user-to-user secure communication links. So for folks like us in a university, all we need is a password to log into the computers. However, consider an organization like the U. S. State Department where people working in different U.S. embassies abroad may have a need for user-to-user secure communication links. Now, in addition to the master key, a user named A may request a session key for establishing a direct communication link with another user named B. This session key, specific to one particular communication link, would be valid only for a limited time duration. This is where Needham-Schroeder protocol can be useful.] Now A engages in the following protocol (Figure 1):

- Using the key K_A for encryption, user A sends a request to KDC for a **session key** intended specifically for communicating with user B.

- The message sent by A to KDC includes A's network address (ID_A), B's network address (ID_B), and **a unique session identifier**. The session identifier is a **nonce** — short for a "number used once" — and we will denoted it N_1. The primary requirement on a nonce — a random number — is that it be unique to each request sent by A to KDC. The message sent by A to KDC can be expressed in shorthand by

Click here to download full PDF material