Chapter 4

Secure Group Key Agreement Protocols

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

Mala K.
Mepco Schlenk Engineering College, India

ABSTRACT

This chapter focusses on Secure Key Exchange protocols executed among a group of parties, called group key exchange (GKE) protocols. Authentication and Key Establishment are very important in any secure communication. Authentication is generally based on long-term keys which can be associated with identities. To associate identities with long-term keys, we can assume the existence of a public-key infrastructure (PKI) which provides parties with some mechanisms for secure key registration and secure access to long-term keys of prospective peers. In most cases, there is also a need for some temporary keys. The Group Key Exchange protocols can be classified as Centralized, Distributed or Contributory. A few toolkits such as Spread and Cliques for the implementation of Group Key Exchange Protocols are also discussed.

INTRODUCTION

Key exchange is an important problem in cryptographic protocols since algorithms that use symmetric keys need the keys to be distributed to the sending and receiving parties in a secure fashion. Two party key exchange algorithms like the Diffie-Hellman key exchange protocol provide a method of establishing the key between two parties in a secure way. The Group key exchange protocols generalize this key exchange mechanism to a group of more than two parties. This chapter focuses on key exchange protocols executed among a group of parties, called group key exchange (GKE) protocols. GKE protocols will have applications such as satellite TV, Internet video broadcasting, collaborative systems and video/audio conferencing.
KEY AGREEMENT IN SECURE COMMUNICATION

Authentication and Key Establishment are very important in any secure communication. Authentication is generally based on long-term keys which can be associated with identities. The term “long-term key” is usually very broad and covers all forms of information which can be linked to identities. For example, it not only includes cryptographic keys such as DES or RSA keys but also encompasses passwords and biometric information. However, passwords and biometric information rarely used in Group Key establishment since passwords exhibit low entropy and the biometric information cannot be easily used for remote authentication.

To associate identities with long-term keys, we can assume the existence of a public-key infrastructure (PKI) which provides parties with some mechanisms for secure key registration and secure access to long-term keys of prospective peers. We can assume that the PKI, or, more precisely, the involved registration and certification authorities, is unconditionally trusted to securely and reliably associate the correct identities and keys of entities. We can assume that the PKI, or, more precisely, the involved registration and certification authorities, is unconditionally trusted to securely and reliably associate the correct identities and keys of entities. It is not required that the certification authorities verify on registration to ensure a public key pair is unique nor is it required that the party registering a public key also knows the corresponding secret key. For example, an adversary will be able to register a public key of some-body else under his name.

Security properties — such as authenticity, integrity and confidentiality — are normally only meaningful when guaranteed during a complete session of closely related interactions over a communication channel whether it is a single transfer of e-mail between two parties or a long-standing connection between two servers. In most of these cases, there is a need for some temporary keys, e.g., an encryption key for a shared-key encryption scheme in the e-mail scenario or a key for a message authentication code in the second example. The goal of using temporary keys instead of using the long-term keys directly is three-fold: (1) to limit the amount of cryptographic material available to cryptanalytic attacks; (2) to limit the exposure when keys are lost; and (3) to create independence between different and unrelated sessions.

Furthermore, if our long-term keys are based on asymmetric cryptography, using session keys based on (faster) symmetric cryptography can bring a considerable gain in efficiency. The establishment of such temporary keys, usually called session keys, often involves interactive cryptographic protocols. These protocols should ensure that all the required security properties, such as the authenticity and freshness of the resulting session key, are guaranteed. Such protocols are called key establishment protocols.

Authentication is central to security. However, the term is very broad and can mean anything from access control, authentication of entities, data origin or keys to non-repudiation. A protocol providing entity authentication (often also referred to as identification) informally means that a party successfully engaging another party in such a protocol can be assured of the other party’s identity and its active presence during the protocol.

KEY AGREEMENT APPROACHES

Several group key management approaches have been proposed in the last decade. These approaches fall into three categories: 1) Centralized, 2) Distributed and 3) Contributory. Centralized group key management is conceptually simple as it involves a single entity (or a small set of entities) that generates and