Chapter 33
Key Management

Chuan-Kun Wu
Chinese Academy of Sciences, China

ABSTRACT

In secure communications, key management is not as simple as metal key management which is supposed to be in a key ring or simply put in a pocket. Suppose Alice wants to transmit some confidential information to Bob over the public networks such as the Internet, Alice could simply encrypt the message using a known cipher such as AES, and then transmit the ciphertext to Bob. However, in order to enable Bob to decrypt the ciphertext to get the original message, in traditional cipher system, Bob needs to have the encryption key. How to let Alice securely and efficiently transmit the encryption key to Bob is a problem of key management. An intuitive approach would be to use a secure channel for the key transmission; this worked in earlier years, but is not a desirable solution in today's electronic world. Since the invention of public key cryptography, the key management problem with respect to secret key transmission has been solved, which can either employ the Diffie-Hellman key agreement scheme or to use a public key cryptographic algorithm to encrypt the encryption key (which is often known as a session key). This approach is secure against passive attacks, but is vulnerable against active attacks (more precisely the man-in-the-middle attacks). So there must be a way to authenticate the identity of the communication entities. This leads to public key management where the public key infrastructure (PKI) is a typical set of practical protocols, and there is also a set of international standards about PKI. With respect to private key management, it is to prevent keys to be lost or stolen. To prevent a key from being lost, one way is to use the secret sharing, and another is to use the key escrow technique. Both aspects have many research outcomes and practical solutions. With respect to keys being stolen, another practical solution is to use a password to encrypt the key. Hence, there are many password-based security protocols in different applications. This chapter presents a comprehensive description about how each aspect of the key management works. Topics on key management covered by this chapter include key agreement, group-based key agreement and key distribution, the PKI mechanisms, secret sharing, key escrow, password associated key management, and key management in PGP and UMTS systems.

DOI: 10.4018/978-1-4666-2919-6.ch033

1. INTRODUCTION

In the world of secure communications, a key is usually something used to encapsulate a message, just like our metal keys which are used to secure locks. An electronic key can also be used for the purpose of authentication, and a metal key sometimes plays the same role. So from the application point of view, an electronic key has much similarity with a metal key. Note that the way to manage metal keys can be quite simple: simply put the metal keys in a pocket, or in a key ring attached in one's belt, or put them in a handbag. This simple way of metal key management has been proved to be fairly secure in most of the cases in our normal life. One may naturally think about the possibility of electronic key management simply by memorizing in human brains. Unfortunately our brains are neither reliable no secure, and our memory has been proved to be a bad way of managing electronic keys.

It is noted that the electronic world is very different from the real one, and the electronic key management is much more complicated than the metal key management. With respect to the electronic key management, there are sophisticated theories and methodologies. This chapter tends to give a comprehensive introduction of the fundamental techniques in key management issues, where without confusion, a key means an electronic key.

To commence the introduction, let's make a scenario. Let Alice be someone in the world who wants to communicate securely with Bob, who is also someone somewhere in the world, on the earth or even in the space yet reachable via electronic signals. In order to provide confidentiality of their communications, Alice uses an encryption algorithm which can be publicly available, e.g. the advanced encryption standard (AES). Alice can do the encryption easily, and send the encrypted message (called ciphertext) to Bob. Now the problem is how does Bob decrypt the ciphertext? Here we do not care about the reliability of the communication, and we assume that Bob does not have problems in correctly receiving the ciphertext. Obviously there should be a way for Alice to send the encryption key to Bob, or equivalently there should be a way for letting Alice and Bob share a common encryption key, so that Alice's encryption can be decrypted by Bob, but not anyone else. In 1976, Diffie and Hellman presented a way for letting secrets to be shared over the public channels, where even if all the communications over the public channels are eavesdropped by an attacker, the attacker is not able to guess/compute the shared key between Alice and Bob (Diffie & Hellman, 1976). This is the well-known Diffie-Hellman key agreement scheme, which is introduced in Section 2.

A natural generalization of the key agreement between two communication parties is the key agreement problem for a group of members, and an alternative key management for a group of members is called key distribution, where a trusted third party playing the role as a key distribution center is needed. This problem is discussed in Section 3. This chapter then further introduces some practical key management solutions for Ad Hoc and sensor networks. This can be found in Section 4.

Now Alice can find a way to agree/share on a common key with Bob whenever they want to establish a secure communication. However, in the commercial world, Alice may not exactly know who Bob is, she knows Bob by some publicly available information such as name, email addresses, or even IP addresses. However all these kinds of information can be faked. How does Alice know that the one at the other end of the communication network is really the Bob that she intends to communicate with? Even with a Diffie-Hellman key agreement protocol, there can be a man-in-the-middle attack. This problem is actually a problem of trust, here by trust we mean that one is convinced that the information being trusted is genuine, and not having been faked. There does not seem to have a solution to