KEY MANAGEMENT

SFWR ENG 4C03 - Computer Networks & Computer Security

Researcher: Jayesh Patel
Student No. 9909040

Revised: April 4, 2005

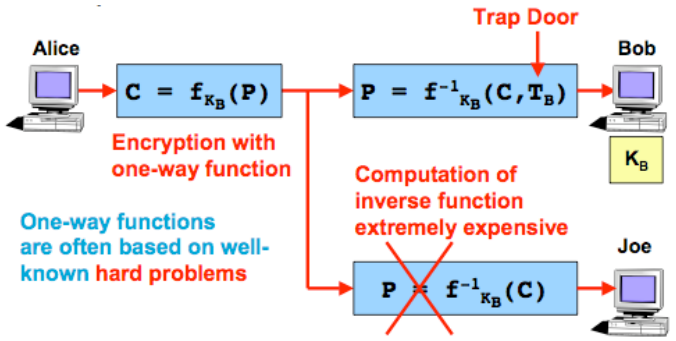
Introduction

Key management deals with the secure generation, distribution, and storage of keys. It plays a vital role in computer security today as practical attacks on public-key systems are typically aimed at key management as opposed to the cryptographic algorithms themselves. This report will investigate the techniques used in the distribution of secret keys used to decrypt and encrypt messages with particular focus on the Diffie-Hellman distribution scheme.

Essential Principles of Public-key Cryptography

Public key cryptographic systems are based on one-way functions which convert plain text into ciphertext using a small amount of computing power, but whose inverse function is extremely expensive to compute. Thus, it is not feasible for someone to decipher the plain text from the ciphertext in a reasonable amount of time.[4]

The term "trap door" is used to describe the fact that the intended user of the ciphertext is able to decipher the ciphertext easily since he/she holds the private key. Finally, public key cryptosystems are usually based on known hard problems such as taking the discrete logarithms over a finite field (as in the case of the Diffie-Hellman key exchange). See Figure 1 for an outline of public key cryptosystems.[4]



Source: "Secure Network Communications." Strong Internet Security. http://www.strongsec.com/tutorials/security.htm

Figure 1. The Notion of Public Key Cryptosystems

The Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a pubic-key cryptographic system whose sole purpose is for distributing keys. Diffie-Hellman is an example of a

public-key distribution scheme (PKDS) whereby it is used to exchange a single piece of information, and where the value obtained is normally used as a session key for a private-key scheme.[2]

How Diffie-Hellman Works

The Diffie-Hellman distribution scheme works as follows assuming two people, named Alice and Bob respectively, wish to exchange a key over an insecure communication channel:

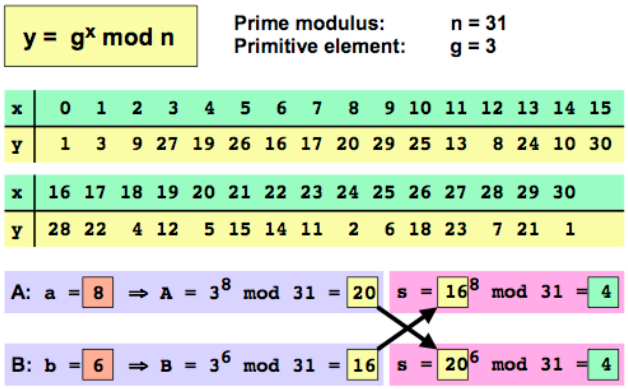
1. Both Alice and Bob agree on the selection of a large prime number n, a primitive element g, and the one-way function $f(x) = g^x \bmod n$ (Note: both n and g are made public).

2. Alice selects a large random integer a and sends Bob the value $A = g^a \bmod n$. Bob selects a large random integer b and sends Alice the value $B = g^b \bmod n$.

3. Alice computes $s = B^a \bmod n$ (= g^{ba} mod n).
Similarly, Bob computes $s = A^b \bmod n$ (= g^{ab} mod n).

4. Alice and Bob now both share the same secret key s. The computation of $x = f^{-1}(y)$ is extremely hard; therefore, someone attempting to listen to the key-exchange cannot determine s even by knowing the values of A, B, n, and g.

Figure 2 illustrates a trivial example of the procedure described above for clarification purposes of the technique.



Source: "Secure Network Communications." Strong Internet Security. http://www.strongsec.com/tutorials/security.htm

Figure 2. Diffie-Hellman Algorithm Example

Authentication

The Diffie-Hellman key exchange is vulnerable to attacks whereby an intruder intercepts messages between the sender and receiver, and assumes the identity of the other party (often known as the *man in the middle attack*). Consequently, the Diffie-Hellman algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are established between legitimate parties.[4]

Advantages and Disadvantages

This leads to a summary of the advantages and disadvantages of the Diffie-Hellman scheme. Its advantages are the security factors with respect to the fact that solving the discrete logarithm is very challenging, and that the shared key (i.e. the secret) is never itself transmitted over the channel.[2]

Nonetheless, the algorithm has its share of drawbacks including the fact that there are expensive exponential operations involved, and the algorithm cannot be used to encrypt messages - it can be used for establishing a secret key only. There is also a lack of authentication.[2]

Alternatives

It is appropriate at this time to consider some of the alternatives to the Diffie-Hellman key exchange. The first option is the manual exchange of the key through a non-electronic medium. However, for obvious reasons, this method is very slow and inefficient. A second approach is to use a key distribution center (KDC) which selects a key and physically delivers it to both parties. Although this method requires secure links to the KDC or the use of another key to distribute the new key (i.e. increased cost), it is still very flexible and efficient.[3]

Conclusion

The Diffie-Hellman key exchange algorithm has proven to be one of the most interesting key distribution schemes in use today. However, one must be aware of the fact that although the algorithm is safe against passive eavesdropping, it is not necessarily protected from active attacks (whereby an intruder impersonates one of the parties involved in the exchange). For this

reason, the Diffie-Hellman algorithm should be complemented with an authentication mechanism. This approach for key distribution appears to be one of the preferred methods used in practice today.

References

1. Charlie Kaufman, Radia Perlman, and Mike Speciner. Network Security: PRIVATE Communication in a PUBLIC World, 2nd edition. Prentice Hall, 2002.

2. "Key Generation and Distribution." CSE 7349: Network Security Systems, Spring 2005. Simon Fraser University. Retrieved 25 March 2005 from the World Wide Web: http://engr.smu.edu/-nair/courses/7349/key_distribution.ppt

3. "Secret Key Distribution." National Institute of Standards and Technology, Computer Security Division. Gaithersburg, MD. Retrieved 25 March 2005 from the World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-7/node209.html

4. "Secure Network Communications." Strong Internet Security. Retrieved 26 March 2005 from the World Wide Web: http://www.strongsec.com/tutorials/security.htm

5. Stallings, William. "Introduction to Number Theory." Web Site for the Books of William Stallings. Retrieved 26, March 2005 from the World Wide Web: http://williamstallings.com/Extras/Security-Notes/lectures/publickey.html