IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 13, Issue 4 Ver. II (Jul. – Aug. 2017), PP 16-18
www.iosrjournals.org

An Overview of Key Exchange Protocols

Chuck Easttom[1]
[1]*(Collin College Professional Development Department USA*
Corresponding Author: Chuck Easttom

Abstract: *Key exchange protocols are a fundamental aspect of information security. A clear understanding of these protocols is required for security practitioners who wish to apply such protocols in SSH, TLS, or similar secure communications protocols. This paper provides a generalized overview of the most widely used key exchange protocols as well as an analysis of any weaknesses in such protocols.*

Keywords: *Diffie-Hellman, MQV, Key exchange, ElGamal*

Date of Submission: 03-07-2017 Date of acceptance: 03-05-2017

I. Introduction

Key exchange protocols are used in all secure communications. Virtual Private Networks, encrypted web traffic, SSH, all depend upon first exchanging a symmetric key. Despite this pivotal role in secure communications, many network security practitioners do not have a clear understanding of these protocols. The purpose of this paper is to provide a clear overview of each of the major key exchange protocols as well as any issues with those protocols.

II. Diffie-Hellman

Diffie Hellman, was the first publicly described asymmetric algorithm. This is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel. In other words, Diffie-Hellman is often used to allow parties to exchange a symmetric key through some unsecure medium, such as the internet. It was developed by Whitfield Diffie and Martin Hellman in 1976.

The Diffie-Hellman has two parameters called p and g. Parameter p is a prime number and parameter g (usually called a generator) is an integer less than p, with the following property: for every number n between 1 and p-1 inclusive, there is a power k of g such that n = g^k mod p [1]. Literally, g is able to generate all n's in the set of p to p-1 by raising g to some power k, mod p.To illustrate this concept, I will use the ubiquitous Alice and Bob examples. Alice and Bob to illustrate this

Alice generates a random private value a and Bob generates a random private value b. Both a and b are drawn from the set of integers

They derive their public values using parameters p and g and their private values. Alice's public value is ga mod p and Bob's public value is gb mod p.

They exchange their public values.

Alice computes gab = (gb)a mod p, and Bob computes gba = (ga)b mod p.

Since gab = gba = k, Alice and Bob now have a shared secret key k [2].

This framework for establishing a shared key over an insecure medium is based on fundamental mathematics that makes it suitable for constructing efficient cryptographic systems with strong security properties [3].

This is shown in figure 1

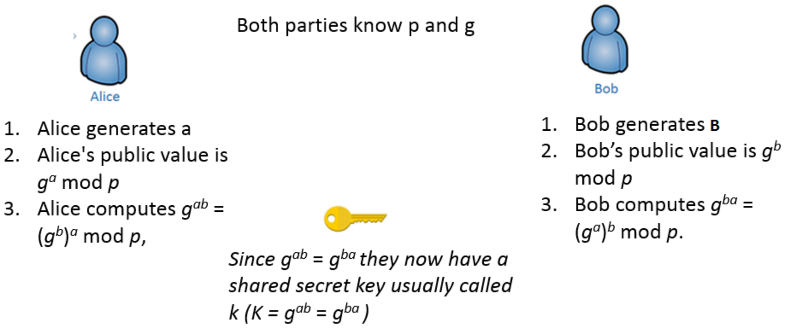

Both parties know p and g
Alice
Bob
1. Alice generates a
2. Alice's public value is g^a mod p
3. Alice computes g^{ab} = $(g^b)^a$ mod p,
1. Bob generates B
2. Bob's public value is g^b mod p
3. Bob computes g^{ba} = $(g^a)^b$ mod p.
Since g^{ab} = g^{ba} they now have a shared secret key usually called k ($K = g^{ab} = g^{ba}$)

Figure 1 *– Diffie-Hellman*

Diffie Hellman was the first published asymmetric cipher and is widely used for key exchange. It is used in protocols such as IPSec and SSH to generate a shared key.

There have been various improvement sin Diffie Hellman. Some, such as those discussed later in this paper, are significant departures from Diffie Hellman, such as are described subsequently in this paper, to minor modifications. Among the modifications to Diffie Hellman are the addition of authentication [4][5].

III. Elgamal

It is based on the Diffie–Hellman key exchange. It was first described by Taher Elgamal in 1984. ElGamal is based on the Diffie Hellman key exchange algorithm described earlier in this chapter. It is used in some versions of PGP.

The ElGamal algorithm has three components: the key generator, the encryption algorithm, and the decryption algorithm[6]. We will keep with the format we have used so far, that of using Alice and Bob.

Alice generates an efficient description of a multiplicative cyclic group G of order q with generator g.

Note: You should remember groups from chapter 5. A cyclic group is a group that is generated by a single element, in this case that is the generator g. With a multiplicative cyclic group, each element can be written as some power of g.

Next Alice chooses a random from x from a set of numbers {0,…,q-1)

Then Alice computes h = gx Remember g is the generator for the group and x is a random number from within the group.

h, G,q, and g are the public key, x is the private key.

If Bob wants encrypt a message m with the public key Alice generated, the following process is done:

Bob generates a random number y is chosen from {0,..,q-1}. Y is often called an 'ephemeral key'

Next Bob will calculate c1. That calculation is simple: $c1 = g^y$

next a shared secret $s = h^y$ is computed.

the message m is converted to m' of G

Next Bob must calculate c2. That calculation is relatively easy: c2 = m' * s

Bob can now send c1 and c2 = as the encrypted text

To decrypt a message m with the public key the first person generated, the following process is done:

The recipient calculates $s = c1^x$

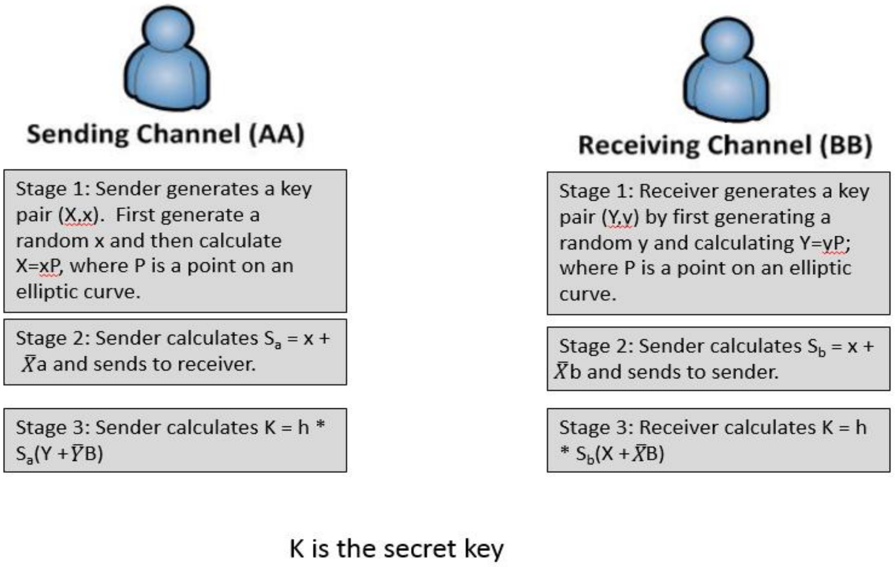
The then the recipient calcualtes $m' = c2 * s^{-1}$

Finally, m' is converted back to the plain text m

The structure should look somewhat similar to Diffie Hellman. The algorithm has a similar basic structure. ElGamal is based on the difficulty of solving the discrete logarithm problem within a cyclic group[7][8].

IV. MQV

Like ElGamal, MQV (Menezes–Qu–Vanstone) is a protocol for key agreement that is based on Diffie–Hellman. It was first proposed by Menezes, Qu and Vanstone in 1995 [9] then modified in 1998. MQV is incorporated in the public-key standard IEEE P1363 [10]. You can see the MQV process in figure 2.



Stage 1: Sender generates a key pair (X,x). First generate a random x and then calculate X=xP, where P is a point on an elliptic curve.

Stage 2: Sender calculates $S_a = x + \bar{X}a$ and sends to receiver.

Stage 3: Sender calculates $K = h * S_a(Y + \bar{Y}B)$

Stage 1: Receiver generates a key pair (Y,y) by first generating a random y and calculating Y=yP; where P is a point on an elliptic curve.

Stage 2: Sender calculates $S_b = x + \bar{X}b$ and sends to sender.

Stage 3: Receiver calculates $K = h * S_b(X + \bar{X}B)$

K is the secret key

Figure 2 MQV

The primary advantage MQV has over Diffie-Hellman is that MQV is authenticated [11]. Though there now exist variations of Diffie-Hellman that are authenticated, the original protocol was not. There are also variation of MQV that are based on an elliptic curve and are thus called Elliptic Curve MQV (ECMQV)[12].

V. Conclusion

The three key exchange protocols discussed in this paper are the most widely used, and most thoroughly studied key exchange protocols. These protocols are central to a wide range of security technology. A thorough understanding of the details of each; Diffie-Hellman, MQV, and Elgamal, is critical to understanding the exchange of symmetric keys.

References

[1] Diffie, W.; Hellman, M. "New directions in cryptography", IEEE Transactions on Information Theory. 22 (6): 644–654, November 1976. doi:10.1109/TIT.1976.1055638.

[2] Steiner, Michael, Gene Tsudik, and Michael Waidner. "Diffie-Hellman key distribution extended to group communication." Proceedings of the 3rd ACM conference on Computer and communications security. ACM, 1996.

[3] Boneh, Dan. "The decision diffie-hellman problem." Algorithmic number theory (1998): 48-63.

[4] Bresson, Emmanuel, et al. "Provably authenticated group Diffie-Hellman key exchange." Proceedings of the 8th ACM conference on Computer and Communications Security. ACM, 2001.

[5] Boyko, V., MacKenzie, P., & Patel, S. (2000). Provably secure password-authenticated key exchange using Diffie-Hellman. In Advances in Cryptology—Eurocrypt 2000 (pp. 156-171). Springer Berlin/Heidelberg.

[6] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." IEEE transactions on information theory 31.4 (1985): 469-472.

[7] Easttom, C. (2014). Modern Cryptography: Applied Mathematics for Encryption and Information Security. New York City, NY: McGraw Hill.

[8] Law, L., Menezes, A., Qu, M., Solinas, J., & Vanstone, S. (2003). An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, 28(2), 119-134.

[9] Vanstone, S. A., Menezes, A. J., & Qu, M. (1999). U.S. Patent No. 5,933,504. Washington, DC: U.S. Patent and Trademark Office.

[10] Menezes, A., Menezes, F. A., Qu, M., Vanstone, S., & Sutherland, K. J. (1995). Elliptic curve systems. In IEEE P1363, Part 4: Elliptic Curve Systems.

[11] D.S. Chan, *Theory and implementation of multidimensional discrete systems for signal processing*, doctoral diss., Massachusetts Institute of Technology, Cambridge, MA, 1978.

[12] Blake-Wilson, S., D. Brown, and P. Lambert. Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS). No. RFC 3278. 2002.

An Overview of Key Exchange Protocols