INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
© VISHWASHANTI MULTIPURPOSE SOCIETY (Global Peace Multipurpose Society) R. No. MH-659/13(N)
www.vmsindia.org

ISSUES IN KEY EXCHANGE PROTOCOL

Rahul Suryawanshi[1], L. G. Malik[2] and M. V Sarode[3]
[1]Department Of CSE GHRIETW, Nagpur, India
[2]Department Of CSE GHRCE, Nagpur, India
[3]Department Of CSE JCET, Yavatmal, INDIA
rahul.suryawanshi@raisoni.net

Abstract

The main aim of key exchange protocol is to securely exchange the key between source & destination. For security of data, Key can be exchanged by using Asymmetric or Symmetric cryptography. Even though cryptographic algorithms are computationally infeasible to break, the whole system depends on how key securely exchange for avoiding all manner of attacks. In principle, the only remaining problem was that a key actually belonged to its supposed owner. This paper mainly focuses on issues in secure key exchange protocol. Also provides comparative study on key distribution algorithm.

Keywords: Key exchange protocol, Asymmetric key exchanged protocol, Symmetric key exchanged protocol

Introduction

Cryptography is an area of communication which developed for providing security to the senders and receivers for transmitting and receiving confidential data through an insecure channel [4]. The primary goal of cryptography is to provide a means for communicating confidentially and with integrity over a public channel. Confidentiality means that the data transferred is not disclosed to unauthorized parties and Integrity means that the transferred data cannot be modified by an unauthorized person without being detected [14]. It's well accepted that the most effective way to achieve the goal of security is by establishing a common agreed secret key and then by using this key with standard cryptographic algorithms together can use for message encryption and decryption. Thus, the problem of establishing confidential and integrity-preserving communication is commonly reduced to the problem of designing a key exchange protocol that allows the parties communicating over a public network.

The first priority in designing a key exchange protocol is ensuring the security of keys before sharing in sender & receiver. Computationally it is infeasible to break the cryptographic algorithm, but the whole system becomes vulnerable in all manner of attacks if the keys are not securely established [6]. Considering these problem, there are mainly three key-exchanged protocols are proposed. There are mainly three key-exchange protocols are proposed. Two protocols for Asymmetric encryption algorithms where pair of key required. One kept confidential said as Private or secret key and other is publicly known. Using this public key, private key is derived. And one key exchange protocol has been proposed for Symmetric encryption protocol where using single key known as secret or private key data is encrypted and decrypted. These key exchanged protocols are:

1) Diffie–Hellman key exchange
2) Elliptic curve cryptography
3) Quantum Key Distribution

Diffie–Hellman key exchange and Elliptic curve cryptography are well suited for Asymmetric Encryption, but not for symmetric Encryption in which using single privet key we encrypt and decrypt the text. As compared to Asymmetric Encryption, Symmetric key algorithms are computationally much faster as the encryption process is less complicated [5]. Also the memory requirement of Symmetric algorithm is lesser [4]. There are inherent challenges with symmetric key encryption in that the key must somehow be managed. Distributing a shared key is a major security risk.

Quantum Key Distribution is traditional key exchange protocol used for the symmetric encryption. By using the concept of quantum physic, it converts the binary key into photon and send towards the destination. After transmitting key in the network, if any intruder tries to look or hack the encryption key, photon get polarized and detect the attack [14]. But, it also has some limitations. It takes Quantum comparison circuit and complicated mathematical equations to detect the attacks. In Comparison circuit, as photons are compared with received sequence, again some photons get polarized which increase the error rate. Thus for Symmetric encryption technique required some secure key exchanged techniques while using symmetric encryption techniques which can securely exchange the key and detect the networking attacks.

Issues in Key exchange protocol

In key exchange protocol, there are mainly five issues i.e. integrity, security, Key Size for Security, computational overhead & at last Efficiency of protocol [3].

1) Integrity

Integrity means data should reach at destination in the manner it send from source node. Data should not be changed due to networking attacks. These attacks can be done in many ways. Some of those are:-

– Denial of service Attacks: Here, the attacker tries to stop Source node and destination node from successfully carrying out the protocol [1][2]. The intruder can apply this attack in many ways, for example by deleting or modifying the messages that source node wants to share with destination node, or by over-heading the parties with unnecessary computation or communication [3].

– Outsider Attacks: The intruder tries to disrupt the protocol by removing, replaying messages for getting some interesting knowledge i.e. information which is not getting by just looking at the public values [3].

– Insider Attacks: It is possible that one of the participants in key exchange protocol creates some protocol which runs for gaining the knowledge about the secret key of his peer. It's an important attack if one of the participants holds a static secret key which is used for running many key agreement protocols. Here, malicious software is very successful for mounting such kind of attack [3].

The plausibility of these attacks depends on what kind assumptions made about the adversary. For example, if the adversaries replaces or remove any message from the public communication channel, the denial of service attack is impossible to prevent.

2) Security

It is one of the important issue in key exchange protocol. Security means data should not be viewed by any intruder. For this purpose, Asymmetric Key exchanged protocol or Symmetric key exchanged protocol used. In Asymmetric Key exchanged protocol, two keys required. One is public key which is publicly known in network & other is private key of each node. By using public key of destination node & private key of source node, secret key formed. This secret key is used for data encryption & decryption. In Symmetric key exchanged protocol, there is only on secret key shared by source & destination node.

There are two Asymmetric Key exchange protocol hab been proposed Diffie-Hellman Key & Elliptic curve cryptography. By using concept of prime number, Diffie-Hellman protocol exchanges the key between sourec & destination [7]. Figure 1 [9] shows how Diffie-Hellman Key exchange protocol works. Elliptic curve cryptography uses the concept of Discrete Logarithm. Elliptic curve calculations are usually defined over finite field. Fig 2 Shows how ECC work.

Here, Destination node chooses the curve E and pint P on the curve & integer d and calculates Q=d×P and makes it public. Conside *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k. Two cipher texts will be generated let it be **C1** and **C2**.

C1 = k*P
C2 = M + k*Q

M = C2 – d * C1
'M' can be represented as 'C2 – d * C1'
C2 – d * C1 = (M + k * Q) – d * (k * P)
= M + k * d * P – d * k *P (Canceling out k * d * P)
= M (Original Message)

There is only one Symmetric key cryptography has been proposed i.e. Quantum Key distribution. It uses the concept of Quantum Physic. Here first number is polarized using quantum circuit & then send. By the principal of Quantum theory, if external force applied then the polarity of photon get changed. And actual key gets changed. Figure 3 shows [7] the working of Quantum Key Distribution.

3) Key Size

Key size is depends on how key computed. The key must, be long enough so that an attacker cannot try all possible combinations. The keys used in Asymmetric key cryptography have some mathematical structure, thus required higher size of key. Whereas Symmetric key cryptography uses some mechanism like Quantum theory, which required half key size for giving same security as compared to the Asymmetric protocol.

4) Computational Overhead

Computational overhead should be minimum while communicating. If computational overhead increase then data required more time for delivering at destination node. These gives more time to intruder. It's depends on the key size and the mechanism used for the exchanging.

5) Efficiency

Efficiency of key exchange protocol is measure on above three issues & time required for exchanging. For Asymmetric key exchange protocol required more time as it takes two keys for encryption & decryption while Symmetric key exchange protocol take less time. Time required for exchange is also depends on the size of key.

Table 1 shows the comparison of basic three key exchange protocols.

Table 1: Comparison of key exchange protocols.

	Diffie-Hellman Key	ECC	QKD
Integrity	Integrity maintain by Diffie Hellman Key exchange protocol	Integrity maintain by ECC	Some data get changed due to intruder, we have to consider only Unchanged Data
Efficiency	For Encryption & decryption It uses two interdependent keys, thus required more time	For Encryption & decryption It uses two interdependent keys, thus required more time	It uses only one keys, thus required less time while communication
Security	By using concept of Prime number achieve Security.	By using concept of Discrete Logarithm Key is securely exchange..	By using Concept of Quantum Theory, data exchange. Thus Intruder get a Fake key.
Key Size for security	Minimum 1024 bits	Minimum 1024 bits	Minimum 160 bits
Computational Overhead	As Key size increased, Computational Overhead increase	As Key size increased, Computational Overhead increase	As Key size increased, Computational Overhead increase
Cost efficient	Software Based, So no Hardware Required	For ECC using Prime number, it's Software but using Binary Number required Hardware	For applying polarity required Polarization Circuit which is expensive.

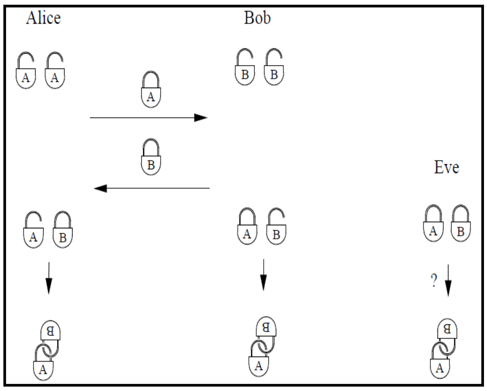


Figure 1: Diffie-Hellman Key Exchange Protocol

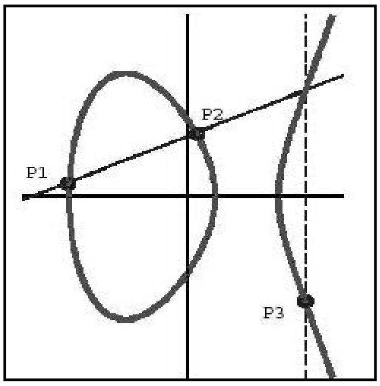
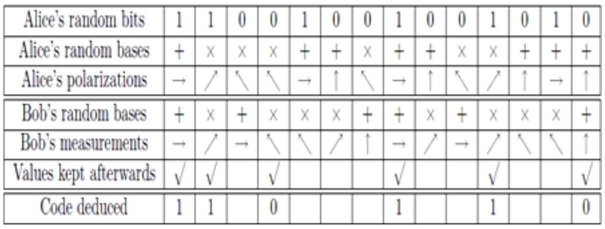


Figure 2: Elliptic curve cryptography



Alice's random bits	1	1	0	0	1	0	0	1	0	0	1	0	1	0
Alice's random bases	+	×	×	×	+	+	×	+	+	×	×	+	+	+
Alice's polarizations	→	↗	↖	↖	→	↑	↖	→	↑	↖	↗	↑	→	↑
Bob's random bases	+	×	+	×	×	×	+	+	×	+	×	×	×	+
Bob's measurements	→	↗	→	↖	↖	↗	↑	→	↗	→	↗	↖	↖	↑
Values kept afterwards	√	√		√				√			√			√
Code deduced	1	1		0				1			1			0

Figure 3: Quantum Key Distribution.

Conclusion

In cryptography, a key is a small piece of information on which the functional output of a cryptographic algorithm depends. This paper addressed issues related to key distribution protocol and outlined the solutions adopted for resolving those issues.It is hoped that it will helpful for improving key exchange protocols on group distribution. This would be a step towards assuring security in cryptographic protocol for real-time applications.

Reference

[1] Markku Antikainen, Tuomas Aura, and Mikko Särelä "Denial-of-Service Attacks in Bloom-Filter-Based Forwarding", Ieee/Acm Transactions On Networking, Vol. 22, No. 5, Pp. 1463 - 1476 October 2014.

[2] Ashish Patil,Rahul Gaikwad "Comparative analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network" International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014) Procedia

Computer Science, Vol 48, pp. 387 – 393,2015

[3] Chandra, S, Paira, S. ; Alam, S.S. ; Sanyal, G. “A comparative survey of Symmetric and Asymmetric Key Cryptography” International Conference on Electronics, Communication and Computational Engineering (ICECCE), 2014, pp- 83 – 93, 17-18 Nov. 2014.

[4] Mohammed Abdulridhu Hussain and Zaid Ameen Abduljabbar “A Logarithm Encryption (EA-LOG) Of Symmetric Cryptography”, IJAET, 2013.

[5] Guang-He Zhang, Carmen C. Y. Poon, Member and Yuan-Ting Zhang “Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks”, IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 1, January 2012.

[6] Junghyun Nam and Dongho Won “Group Key Exchange over Combined Wired and Wireless Networks”, IEEE Journal Of Communications And Networks, Vol. 8, No. 4, December 2006.

[7] Scholz, Matthias. "Quantum Key Distribution via BB84 An Advanced Lab Experiment." University of California, p8, 2007.

[8] Canetti, Ran, and Hugo Krawczyk. "Analysis of key-exchange protocols and their use for building secure channels." Advances in Cryptology—EUROCRYPT 2001. Springer Berlin Heidelberg, pp 453-474, 2001.

[9] Vasco, Maria Isabel González, and Igor E. Shparlinski. "On the security of Diffie-Hellman bits." Cryptography and computational number theory, pp 257-268., 2001

[10] Jean-Francois Raymond and Anton Stiglic “Security Issues in the Diffie-Hellman Key Agreement Protocol”, IEEE Transactions on Information Theory, Vol 22, pp 1–17, 2000.

[11] Yokoyama, VNaoya Torii VKazuhiro. "Elliptic curve cryptosystem." Fujitsu Sci. Tech. J 36. No.2, pp 140-146, 2000.

[12] Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. “Experimental quantum cryptography” Advances in Cryptology—EUROCRYPT’90 (pp. 253-265), January 1991.

[13] Miller, V., “Use of elliptic curves in cryptography”, CRYPTO 85, 1985.

[14] C. H. Bennett and G. Brassard “ Quantum Cryptography :Public Key distribution & coin tossing”, Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India,pp- 175-179, 1984 .

[15] W. Diffie and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 1976.