Internet Key Exchange

Philip Gomolisky

2015-11-15

Contents

1 Abstract

The subject of cryptography is exchanging secrets between two strangers who have nothing in common but need to talk over a secure network. Using a key to exchange information that needs to be secret between two destinations or more is important. So the Internet Engineering Task Force was created to establish the first regulations on Internet Key Exchanges.

2 Introduction

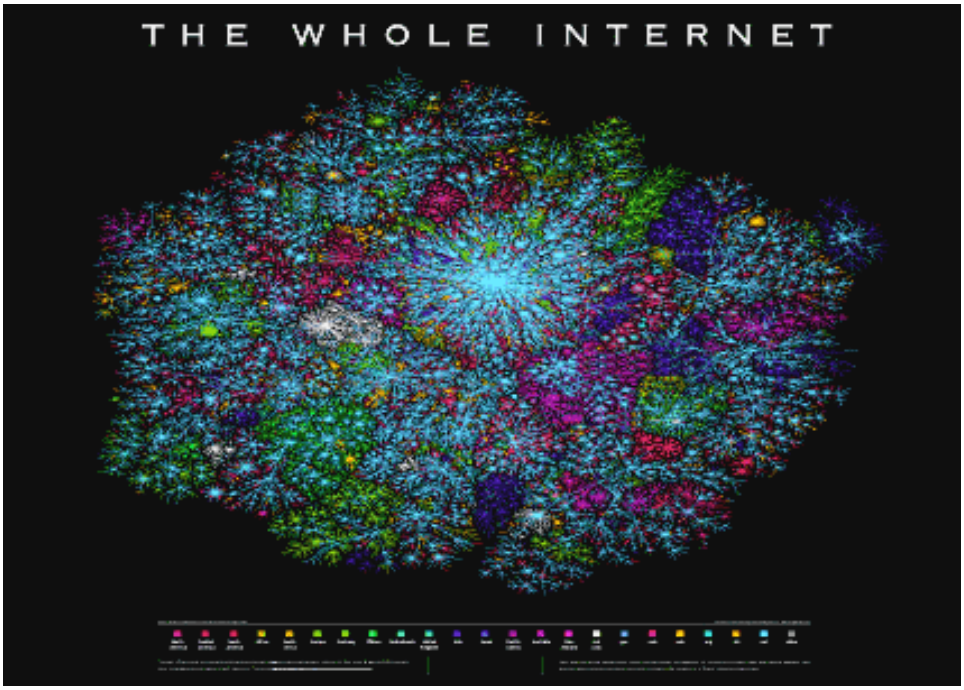

Figure 1: This is the internet

With the formation of the internet we see information everywhere. In order to have some type of rules and regulations an organization was started to help with the unrest of the internet. This organization is called the Internet Engineering Task Force or IETF. This organization helps secure the internet by using well established algorithms and other types of code generating patterns. Algorithms are used for securing messages of unsecure networks for public and private use. Cryptography is an ever expanding field of scientific study. It encampasses many broad topics like security exchange and Internet encryption algorithms. The IETF established Internet Key Exchanges or IKE to help generate algorithms for secure message transactions. Two of the moat popular key exchange algorithms are Diffie-Hellman and

RSA. Diffie-Hellman is popular as a secure network encryption algorithm using modular arithmetic and secret keys that each person uses to secure their message. Both the sender and recipient have key pairs. Key pairs are essentially public keys. Using the public keys and both parties private keys they can compute the same shared number. RSA is similar in security to Diffie-Hellman. It requires a public key and a private key. Together forming a key pair.

2.1 Acronyms

IKE can be used to configure any of these algorithms for secure transactions. STS is a protocol that is used in public key cryptography. Station-to-Station is based off of Diffie-Hellman. It provides mutual key and entity authentication. STS also gives perfect forward secracy which is if one message is not secret then not all messages there after are as secret. Forward Secracy helps in this process since it does not use the same algorithmic pattern for every message sent so if one message is broken into then not all messages would be decrypted.

Internet Security Association and Key Management or ISAKMP is a framework for authentication and key exchange which it is also independent of any one particular key exchange. A Security Association is a protocol that helps protect the security of the communication transmissions throughout the internet. Using hash functions to look up the exact data and mapping it to an exact path creats a identification for the user. Security for the internet protocol or IPsec is a layer of security to help establish and provide security for internet traffic. This protocol is only a small part of internet security. SKEME was a presentation at the IEEE sympodium in 1996 which outlines the destribution of a key exchange technique with anonymity, repudiability, and key refreshment. With these acronyms we are introduced to IKE and the destribution of these terms and techniques are listed in the IETF RFC's. With mathematical equations and algorithms it is likely that someone or something would devise ways of making them breakable or easier to decipher.

3 History

Cryptography has been around since the early Egyptians 4000 years ago[1]. The Egyptians used a substitution cipher, which is using one symbol or character to replace the original. Cryptography was brought into the 20th century with the fighting in World War I and World War II. Throughout the war cipher texts were created to protect secrets and strategies during these conflicts. The Zimmerman Telegram was an encrypted message that described Germany's intentions to help Mexico reclaim territory in New Mexico, Texas, and Arizona that belonged to the United States[1].

This revelation changed the course of history in World War I by bringing the United States to declare war on Germany and there allies. The United States at that time joining the war, it was essential to encrypt their messages since they were getting deciphered by the Germans. So the U.S. Army devised a cipher using a Native American language, Choctaw. This language would be proven harder to decipher since it was not commonly spoken. This cipher helped turn the tide around in favor of the United States and into the history books.Introduced in WWI a machine that encrypted messages was invented by Arthur Sherbus. Since the war ended it was too late to help the Germans and Arthur would have to wait another 20 years or so to finally see his invention in action. Beginning in the 1930's a financial collapse of the trading market in the United States of America effected everybody in America, Europe and around the world. Germany was greatly effected and looked anywhere to find relief. Running in the newly created Nationalist Party Adolf Hitler began his presidential candidacy in 1932 then succeeded as fuhrer in 1934 with the death of then President Paul von Hidenburg. A war would follow in 1939 and would encampus the whole world. When WWII has started secrecy was needed more than ever, to ensure secure messages the Germans used a device that was invented during WWI. The Enigma machine was first of its kind using gears and rotors to send encrypted messages. This machine could encrypt messages that was computationally hard as $10^{1}14$ possible configurations.[1] So brute force would not work to decipher these codes. Flaws to the design was its downfall. A similar machine was built in Japan during this time. Modern Cryptography techniques use secrete keys to encrypt and decrypt messages. These techniques can be relativley hard to break.

3.1 Modern Cryptography

A "One-time Pad" for example has been proven unbreakable.[1] Algorithms were used in conjunction with public and private keys to form key exchanges that would help encrypt then decrypt texts written with them. Diffie-Hellman key exchange was introduced in 1976.[2] Through the efforts of Whitfield Diffie, Martin Hellman and Ralph Merkle the solution of how to secure information from an insecure source was realized. RSA is an algorithm that Ron Rivest, Adi Shamir and Leonard Adleman went public with in 1978. James Ellis during World War II was the creator of these first ideas that revolutionized cryptoggraphy. Ellis described a system where the user takes a public key and sends it to a friend the friend locks the message he wants to send and mails it back to the user who unlocks it with a secret key. This was the start for both Diffie-Hellman and RSA. With these algorithms being used for message sending and the internet becoming more popular in the late 1990s there needed to be some kind of governing body to regulate these types of message sending algorithms. In 1998 to be percise the IETF

Figure 2: World War II Flag Raising

was assigned to regulate these types of information transactions. So in that same year to help secure message traffic the IETF created the IKE or internet key exchange. The Oakley protocol describes in detail the specification of how to set up a secure key exchange. This protocol uses any algorithm a user wants. If a user wants Diffie-Hellman, RSA. Diffie-Hellman was Oakleys go to algorithm. He uses it to create D-H groups which are related to the exchange key algorithm that helps determine message security. With the Oakley protocol we see the emergence of the IKE.

4 IKE; How it works

The Internet Key Exchange that the IETF created used specifications from the Oakley protocol, ISAKMP and SKEME. The Oakley protocol calls for using "modes"[3] or "a series of key exchanges."[3] The services that were provided by each "mode"[3] are, "(e.g. perfect forward secracy for keys, identity protection, and authentication)."[5] Using Diffie-Hellman as a, "secure key distribution mechanism"[5] to relay messages. This algorithm is simple to use and did not require to much computational time. That is with little time needed to share a common public key it is very effecient plus

establishing that key is fast. Since this key protocol is generic it needs to be secure for long periods of time, for many years. STS protocol is a part of the security of the Oakley protocol with Perfect Forward Secrecy or PFS to ensure future encrypted messages not be decrypted. Identity protection was another "mode" that the oakley protocol established.

Authentication is used as part of the identity protection and since the oakley protocol uses the users public key we see a hash function used to retain the certification of these keys.[3] This is just saying that in order for the public key to work the protocol uses a function that identifies the user and uses the right public key to encrypt or decrypt a message. The Oakley protocol is one of the steps needed to create a working IKE. Another part of a IKE creation is the Internet Security Association and Key Management Protocol. In the ISAKMP document provided by the IETF, we see that the management system is a fundamental part of the IKE because it helps establish the Security Associations. ISAKMP is a protocol that "establishes, modifies, deletes Security Associations."[4] In order for these keys to be secure and stay secure a management system needs to be uniquely qualified so that it can handle single and multiple threats. With the interest in threats and unprotocted transmissions, SKEME was a presentation that outlined the specifics of "a versitile key exchange technique which provides anonymity, repudiability, and quick key refreshment."[5] SKEME was created to help the growing internet community with newer more innovative techniques to secure fast key refreshment. The IKE is looking for an exchange of many keys and many users with encryption and decryption, with time rates not increasing and security still strong. The IKE uses these three protocols to establish a building block for a protocol that generates, "security associations, virtual private networks, and identity protection,"[5] in a very flexible confiuration that can use a number of different algorithm schemes to give a layer of protection. The first part of the IKE is the consideration of an Attribute Class. IKE uses an Attribute Class implementation which uses encryption based off of DES, MD5 and SHA, a pre-shared key and MODP.[5]

4.1 Oakley, ISAKMP, SKEME

The second part of IKE is the Encryption Algorithm Class. This class identifies Diffie-Hellman as a good algorithm to use in order for secure communications. This is the equation using a public key encryption which is used in phase 1.The user's key is $(g^a modp, g, p)$.[2] The recievers random key is, $g^b modp$ with this public key being sent to the reciever then back with the random key the user uses, $(g^a)^b modp$ as the private key[2]. The notation is easy to follow and fast to implement. This creates a SA which can be either generated in main mode to protect the identity of users or in aggressive mode which does not. Exchanges also consist of different authen-

tication with signatures and different key exchanges like RSA. This is part 1 of the 2 phases that are defined by the ISAKMP. IKE also uses this phase as an initiation phase. The second phase uses IPsec and SA's to negotiate the key material which is called "Quick Mode" for IKE[5].

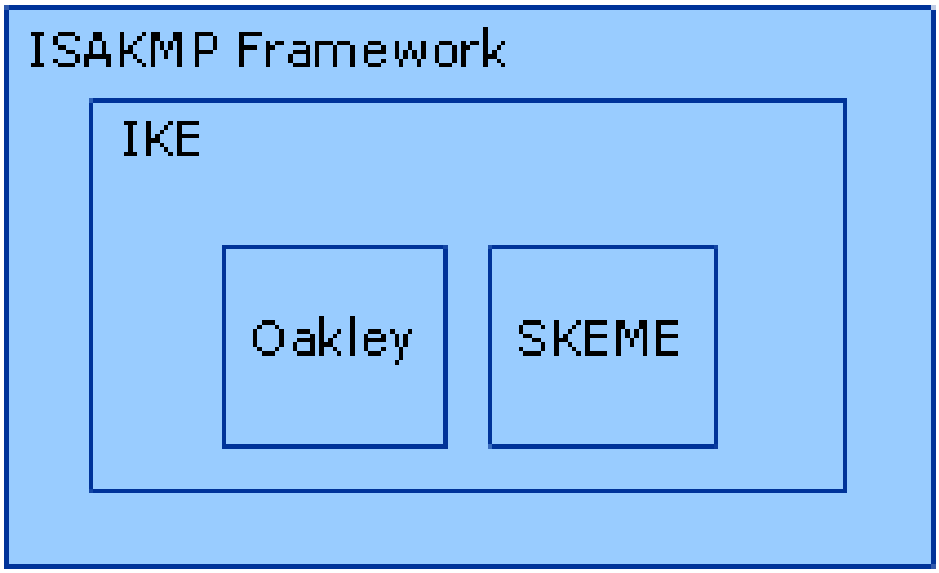

Figure 3: IKE

The last mode is "New Group Mode," which is used to help phase 1 and is in phase 2[5]. So this protocol starts with a Security Association using an, "encryption algorithm, hash algorithm, authentication method, and information about a goup in order to do Diffie-Hellman."[5] ISAKMP along with IKE use these attributes in order to create Security Associations and not to be used by any other services that are in a negotiation with IKE. What could be negotiated would be "prf" or a pseudo-random function.[5] A pseudo-random function works with only one input in a range. Running this multiple times should produce the same output. Prf's are part of the hash algorithm of the attribute list. A HMAC or hash-message authentication code would be used if the parties would not consent to the prf.[6] These Hash Algorithms would use MD5, SHA, and Tiger.[6] Diffie-Hellman would be a group that is defined as, "the group in which to do the Diffie-Hellman exchange is negotiated,"[5] and these groups are typically known as "Oakley Groups."[5]

These Groups are, "specified using a defined group description."[5] These groups consist of an attribute class, with, "values 2^15 and higher are used for private group identifiers." [5]

A Group Type is a set of four values that supports two MODP groups, and two EC2N groups. A MODP group or Modular Exponential is a group

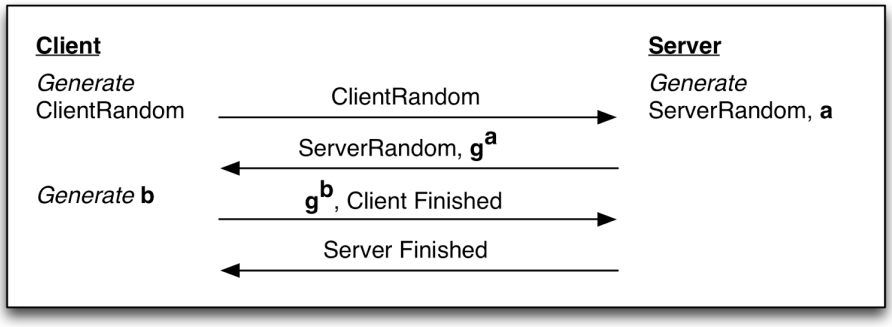

Figure 4: A picture of Diffie-Hellman Key Exchange.

implemented by Oakley and IKE as id 1 and id 2. These two groups use a prime to do there encrypting.[5] The id 1 prime is:

$$2^768 - 2^704 - 1 + 2^64 * [2^638pi] + 149686$$

id 2 prime is:

$$2^1024 - 2^960 - 1 + 2^64 * [2^894pi] + 129093$$

The EC2N or Elliptic Curve Group Over $GF(2^N)$ is the other two groups that IKE originally focused on. "The curve is based on the Galois Fields $GF[2^155]$"[5] for id 3 and "Galois Field $GF[2^185]$,"[5] for id 4. Which just means its a Galois Field with a size where 2 as a prime and 155 or 185 is a positive integer or p^k. The two inputs for the EC2N are a irreducible polynomial and the equation for the elliptic curve. The irreducible polynomial is:

$$u^155 + u^62 + 1$$

for id 3 and:

$$u^185 + u^69 + 1$$

for id 4. The elliptic curve equation is:

$$y^2 + xy = x^3 + ax^2 + b$$

for both id's.

"The data in the exchange payload is x from (x, y), a point on the elliptic curve when taking a random secrete Ka and calculating $Ka * P$, $*$ is the repitition of the group addition and double operations, P is the curve point with x coordinate equal to generator 1 and the y coordinate determined from the defining equation."[5] Also, "The equation of curve is implicitly known by the Group Type and the A and B coefficients. There are two

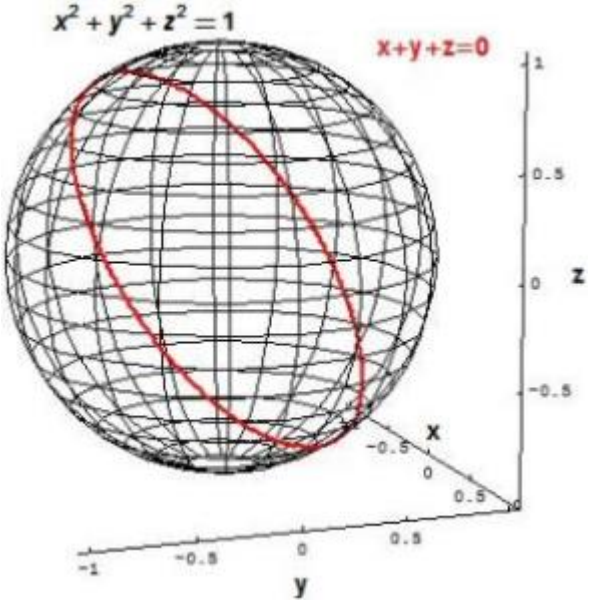

Figure 5: This is a Galois Field

possible values for the y coordinate: either one can be used successfully."[5] A "Life Type" is the last area to be described in IKE. It is a security notification on how to deal with SA's that are generated by the ISAKMP.[5] In essence this protocol can establish PFS or Perfect Forward Secracy. Three descriptions on how this can be established is; Main Maode exchange to protect identities which establish a SA, Quick Mode exchange negotiates security protection, and Deletion which provides removal of the SA and associate state. These Life Types are represented in seconds and kilobytes. This protocol is to ensure the security of VPN's and IPsec's.

5 Applications

IKE's used to ensure the security of different protocols. The most used of these are IPsec or Internet Protocol Security and VPN's or Virtual Private Networks. IPSec's are communication operations that function to manage system SA's with security protocols like AH and ESP.[7] An AH or Authentication Header which, "provide for connectionless integrity and data origin authentication for IP datagrams and provides protection against replay attacks," [7] is part of the security of the IPSec. ESP is a part of the same security architecture. Encapsulating Security Payloads or ESP helps provide for confidentiality, authentication, integrity, anti-replay service, and traffic-flow confidentiality.[7] SA's are used by IPsec with ISAKMP to provide framework authentication and key exchange. Authenticated keying is

provided by either, "manual configurations with pre-shared keys, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), or IPSECKEY DNS records."[7] VPN's are privet networks extended over public networks which could be the internet.[8] This is saying that these networks are public but sending information over a VPN makes the information secure. These VPN's are established to help share a point-to-point connection which use connections, virtual tunneling protocols, or traffic encryption.[8]

6 Evolution and Vulnerability

In 2005 the IETF issued a new version of the IKE which was based off of a combination of different documents that helped support the performance of mutual authentication and SA's. The second version defines many different documents which are, "Internet Security Association and Key Management Protocol (ISAKMP, REF 2408), IKE (REF 2409), the Internet Domain of Interpretation (DOI, RFC 2407), Network Translation (NAT) Traversal, Legacy authentication, and remote address acquisition."[9] These documents are put into effect with this new version of IKE. There are twelve goals to this revised version of IKE:

1. Defining IKE in a single document and incorporate NAT Traversal, Extensible Authentication, and Remote Address acquisition;

2. Simplifying IKE by replacing the eight intitial exchanges with a single four message exchange and also authentication methods for the AUTH payload would be change to use more effeciently;

3. Removing Domain of Interpretation (DOI), Situation, and Labled Domain Identifier fields, with the Commit Bit and Authentication only;

4. Decreasing latency in some cases by having 4 messages and setting up a CHILD SA;

5. Replacing syntax for protecting IKE messages with ESP to simplify analysis of security and implementation;

6. Reducing the number of CREATE CHILD SA exchanges from 3 to 2 with acknowledging all messages even errors;

7. Increasing robustness for message handling with exchanges being held off until the message is recieved;

8. Fixed weaknesses of symmetries in hashes;

9. Specified traffic selectors to not overload ID payloads;

10. Specified error messages to make clear what went wrong;

11. Simplified clarification of network failures and Denial of Service attacks;

12. Maintaining IKEv1 syntax and magic numbers to port over to IKEv2;

These goals where an improvement on the specifications of IKEv1. This help IKE improve by using many new techniques that where created for an existing system in IKEv1 and help establish a growing interst on improving old ideas and making them function to the fullest with IKEv2. These twelve improved goals can give hints at such things as vulnerabilities of IKE.

7 Conclusion

Internet Key Exchange has been around since the proposal for a such a thing in 1998. With cryptology dating back to Egyption times its a relatively new concept suing algorithms to encrypt and decrypt messages. In order to create an attack free message these algorithms would need to be extremely hard to break. Thats when we are introduced to the Diffie-Hellman algorithm and RSA. With the introduction of the internet these algorithms grew to popularity. With the internet a new threat appeared, which is message sending. In order to send a private message we need to have different protocols to ensure that the message stayed safe. So the Internet Society which is known as the IETF was born to regulate such concerns and to properly handle situations that can be considered threats to the publics activity on the internet. With the IETF involved Internet security became a reality for the users of this system. But threats of all kinds lingure and not all transactions are safe so new regulations and versions of proposed protocols have to be realized. There are vulnerabilities to any system so in order to comprehend such things the system needs to be broke down and put back together so if somerhing does to wrong repairs and upgrades can be made.

References

[1] Nicholas G. McDonald, "Past, Present, and Future Methods of Cryptography and Data Encryption", University of Utah, (2009)

[2] "Diffie-Hellman Key Agreement Method","RTFM Inc.","The Internet Society"

[3] "The Oakley Key Determination Protocol","University of Arizona","The Internet Society"

[4] "Internet Security Association and Key Managemnet Protocol", "National Security Agency", "The Internet Society"

[5] "The Interbet Key Exchange", "Cisco Systems" "The Internet Society"

[6] H. Krawczyk M. Bellare R. Canetti,"HMAC: Keyed-Hashing for Message Authentication", "IBM", 1997

[7] "Wikipedia", "IPsec", "en.wikipedia.org/wiki/IPsec"

[8] "Wikipedia", "VPN", "en.wikipedia.org/wiki/Virtual Private Network"

[9] "Internet Key Exchange (IKEv2) Protocol", "Microsoft", "The Internet Society"

Figure 1 shows the internet.

Figure 2 shows war.

Figure 3 shows IKE.

Figure 4 shows Diffie-Hellman.

Figure 5 shows a Galois Field.