

IP Network Security: IPsec (Internet Protocol Security)

Hyung-Joon Kim

Dept. of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, New Jersey

Abstract

With the historical breakthrough in the Internet, Internet Protocol (IP) has been the most dominant technology used for internetworking today. These days, most organizations and individuals heavily rely on the Internet to do everyday business. Since an enormous number of networking applications and services were developed and served by virtue of the Internet protocol suite, security concerns have been also reflected on the development of security protocols, which mostly operate on the top of the IP network layer; for instance, SSL/TLS, SSH, SFTP, S/MIME, and so forth. However, all these protocols are served on the application layer while the lower, IP network layer, still had fundamental vulnerability, which has allowed adversaries to make a new type of security attacks such as DoS (Denial of Service) and DDoS (Distributed Denial of Service). After all, with the high demand for secure IP layer, the invention of IPsec (IP security) kicked off and it has evolved through a series of versions; now, IPsec is adopted as a mandatory for IPv6. This paper is a report on the story of IP network and related security issues, and the overviews of IPsec.

1. Introduction

Without doubts, the Internet is one of the most, if not the most, brilliant inventions in the 20th century. Oddly enough, the history of the Internet dates back to the 1950s, the beginning of the Cold War era. Since the nuclear arms race between the Soviet Union and the U.S. had begun, the U.S. Department of Defense started considering better command-and-control network that could survive a nuclear bomb. After a long history of the U.S. government's efforts to create an innovative network, Advanced Research Projects Agency Network (ARPANET), the origin of the Internet, was developed by ARPA, a defense research organization under the U.S. Department of Defense, and launched its very first service with only four nodes: UCLA, UCSB, Stanford Research Institute, and University of Utah. It was in December 1969 that the world's first packet-switching network was born. After the ARPANET rapidly grew in the first few years, the gigantic potential of the ARPANET turned out to be apparent enough to make many other countries and research institutes rush to build ARPANET-like networks. After TCP/IP standards were released in 1983, National Science Foundation Network (NSFNET), a backbone to which regional academic institutes and research labs were connected, was interconnected to the ARPANET. Before long, the sub-networks connected to the ARPANET exponentially grew worldwide. The universe of such interconnected networks was later called the Internet. In addition, a network specifically using Internet Protocol (IP) – as a part of TCP/IP protocol suite – to communicate with others is called an IP network.

In the historical evolution of the Internet, Internet Protocol (IP) has been the most dominant technology used for internetworking today. Needless to say, these days IP network is deployed all over the places in the world: governmental agencies, academic communities,

entrepreneurial companies, small businesses, and individual households. By the superb interconnectivity of IP network, data transmission has never been easier and cheaper than ever. In compliance with the worldwide demand for internetworking, IP network has been rapidly expanding itself. In addition, as the world encounters a ubiquitous networking era, IP network is expected to grow even larger by accommodating not only data transmission of conventional computer networks but also that of telecommunications and broadcasting networks, home appliances, and many other future participants.

Since an enormous number of networking applications and services were developed and served by virtue of the internet protocol suite, security concerns have been also reflected on the development of security protocols, which mostly operate on the top of the IP network layer; for instance, SSL/TLS, SSH, SFTP, S/MIME, and so forth. Despite the existence of security protocols at the application layer, however, there have been fundamental vulnerabilities in the IP network layer that have allowed adversaries to make a new kind of security attacks such as DoS (Denial of Service) and DDoS (Distributed Denial of Service). Until then, security doesn't take account of "availability" – when service is requested. Indeed, today's high dependency on the Internet has gradually elevated the importance of "availability" as a major security issue; accordingly, renovation movements to add security to Internet Protocol have been initiated. After all, with the high demand for secure IP layer, the invention of IPsec (IP security) kicked off and it has evolved through a series of versions; now, IPsec is adopted as a mandatory for IPv6.

Yet, IPsec along with IPv6 has not been deployed much in practice; in fact, IPsec is only limitedly, but appreciatingly, used to establish a virtual private network (VPN). However, it is undeniable that IPsec is equipped with great security features that the IP network layer lacks, and worthy taking a look at IPsec since it's a mandatory for the next-generation IPv6. This paper is a report on the story of IP network from security point of view, and the basics of IPsec as well as its related issues.

2. IP Network Overview

The Internet consists of many subsets of interconnected networks; that is, the Internet is a network of networks. While the Internet is somewhat abstractly in the highest level of hierarchical network structures, a sub-network specifically using Internet Protocol for communication is called an IP network. Since Internet Protocol (IP), as a part of TCP/IP protocol suite, is most widely used today for interconnection in the Internet, the terms, the Internet and IP network, are often used together. In this paper, though, IP network is strictly referred to a network specifically using Internet Protocol – as a part of TCP/IP protocol suite – (hereinafter IP for short) as the name suggests.

The reason that IP stands out as the most dominant technology is that it provides a very efficient way of internetworking to achieve universal service across heterogeneous networks. Recall the history of the world's first packet-switching network, ARPANET, later became the Internet. From the very outset, it was designed for networking systems to interconnect to others in such a way that it ensures a high order of "survivability" as a whole. Thus, even if one or more sub-networks get disconnected, the whole network remains fully connected. To put it in another way, if a packet departs from a system interconnected to the network, the packet somehow finds a route to the intended destination system in spite of failures in the intermediate paths between the sender and the destination. Like this, IP was designed from the

beginning with the idea of internetworking in mind. Its primary goal is to provide an efficient way to transport packets from source to destination regardless of whether they are on the same network or whether there are disconnected routes or different networks in between them. This is why IP is considered as the most ideal protocol, at least so far, to achieve universal service across heterogeneous networks. For this reason, moving to 3G and beyond[†], recently there have been vigorous efforts to converge telecommunication and broadcasting networks to IP network. Not surprisingly, in the near future, home appliances and many other participants will transmit data to some extent over IP network.

To transport packets from source to destination, IP has a relatively simple structure – it minimally contains what it's supposed to contain. Actual complex routing mechanisms underlie the IP network layer. The details of the IPv4 header will not be presented in the paper, but the important note is that there are no security features at all to protect the source and destination addresses or contents in IP datagrams. Although, in theory, the security option in the option fields can be used for a military router to detour secret information without passing through enemy countries [1:436], there are neither authentication nor encryption. This has been recognized as a major security hole in IP since IP network had undergone various security attacks. The followings are highlighted among those attacks related to the weakness of IP:

- ***IP spoofing*** – It's an illegitimate creation of a fake packet with a forged source IP address so that it can deceive the destination system about the sender. IP spoofing is not an attack itself, but it is widely used for notorious attacks to conceal the identity of a sender, masquerade as another system, or simply confuse the destination system about where to reply.
- ***Session hijacking*** – It's an exploitation of a valid communication session between two parties. Using a packet sniffer program, an eavesdropper can hijack valid session information, and then misuse it for various malicious purposes. And also, in early careless implementations of TCP/IP, session hijacking can be done by simply predicting the sequence number of an IP packet.
- ***Man-in-the-middle attack*** – It's a malicious attack in between two lawful parties as the name says. In a man-in-the-middle attack, an attacker intercepts a message in the middle of the communication between two victims, and then performs various follow-up attacks such as stealing, modifying, and at worst destructing valuable information intended to send to a legitimate receiver, phishing, DoS, and so forth.
- ***DoS (Denial of Services) attack*** – It's a new type of security attack in which an attacker make a victim consume computing resources to respond to the attacker's "false" requests. Thus, a DoS attack simply try to exhaust a system's resources to make them unavailable to intended services rather than trying to access valuable information in which traditional attacks may be interested. As modern industries

[†] 3G and beyond refers to future mobile technology including 3G (the 3rd generation) such as W-CDMA, 1xEV-DO, HSPA, and 4G (the 4th generation) such as WiMax. Its service provides the ability to transfer both voice and data simultaneously with high bandwidths. Therefore, by 3G and beyond technology, mobile phone can be used to not only make telephone calls but also exchange graphical messages, download music and video contents, watch TV provided by DMB (Digital Multimedia Broadcasting) service, or make video calls.

heavily rely on the services over the network, the security concern about DoS has been raised more and more.

- ***DDoS (Distributed Denial of Services) attack*** – It's a successor to a classic DoS. In a DDoS attack, multiple compromised systems, often called “zombies”, cooperates in a distributed manner to attack a victim. For this, malware are used to carry DDoS attack mechanisms. As malware pull the trigger at a doomsday, infected systems inject massive traffic to the target victim. DDoS attack is a serious security threat these days because its magnitude is much greater than a classic DoS's, and it's much harder to defend and identify attackers. Besides, most of the time, the compromised systems are unaware of being infected with malware.

To strengthen the weak security of IP, most of the efforts have been put on the upper application layer, according to the need of each application. For instances, SSL/TLS was invented to provide secure data communications over the Internet; it's designed to support various protocols but best known as secure web protocols for web browsing, email, instant messaging, and other web transactions. SSH (Secure Shell) and SFTP (Secure File Transfer Protocol) replaced very aged Telnet and FTP, respectively. S/MIME (Secure Multipurpose Internet Mail Extension) was invented to provide a secure email mechanism using public key cryptography and digital signature. All these protocols provide authentication and confidentiality at the application ends. None of them, however, can be a direct solution to the vulnerability of the IP network layer that has allowed the above-mentioned attacks.

3. Internet Protocol Security (IPsec)

To add security to a weak creation, the first thing security people would think of is to employ their best friend – cryptography. The same game is very much here for IP. IPsec uses cryptographic techniques to validate the sender and recipient and encrypt the contents in IP datagrams; thus, authentication, confidentiality, and integrity are all added. A key design note of IPsec is to provide such security at the IP network layer of the TCP/IP protocol stack rather than the application layer; that is, IP datagram defends by itself. To implement IPsec without alteration of the existing TCP/IP protocol suite and upper layer protocols, IPsec simply wraps the existing IP (both IPv4 and IPv6) datagram with another datagram that can be protected by authentication, encryption, and integrity check. This means that “all IP packets can be protected, irrespective of the upper layer protocol being carried in the packet payloads, and that no re-engineering of applications is required in order to take advantage of the security provided by IPsec [2:72].” Interestingly, the idea might sound odd – encapsulating an IP packet within a new IP packet. More importantly, according to [3:36],

One of the critical problems in designing cryptography below the application layer in network design is that its requirements do not always parallel standard cryptographic protocols. For instance, many cryptographic protocols base themselves on a client/server model. At the IP layer, this concept does not truly exist. All IP endpoints on a network are peers, and the imposition of client and server roles is imposed by superior protocols.

In fact, this problem may affect the design of IPsec as well. To achieve security protection in the IP network layer, IPsec introduces many of complex, abstract, lengthy, and debatable components in the architecture. This paper can't and won't cover all the important concepts, terminologies, and mechanisms used in IPsec, but will briefly taste the nature of IPsec.

Security Association (SA) defined in [5] is a simplex “connection” that defines mutually agreeable security services, mechanisms, and keys used to protect communication between IPsec peers. In other words, SA specifies the way how the traffic carried by it should be handled at end points of IPsec-enabled systems for secure communication. Since a SA is a one-way connection, a pair of two SAs, one in each direction, is required for bi-directional communication between peers, and the SAs should be stored at each end point of IPsec-enabled systems.

SA carries out the security services by the use of IPsec's two protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). Authentication Header (AH) defined in [6] is primarily to provide authentication and integrity check – not encryption. AH guarantees data origin authentication of IP datagrams and provides optional integrity protection against replaying attacks. The other protocol, Encapsulating Security Payload (ESP) defined in [7], provides the same set of security services as AH – plus confidentiality. Yet, this is not just *another* feature. Because two protocols are overlapped except the encryption functionality, Niels Ferguson and Bruce Schneier suggested that AH be eliminated [4:7]. In fact, according to [5:8], since ESP is equipped with full functionality, AH is expected to play a diminishing role and therefore it has been no longer a mandatory for IPsec implementations.

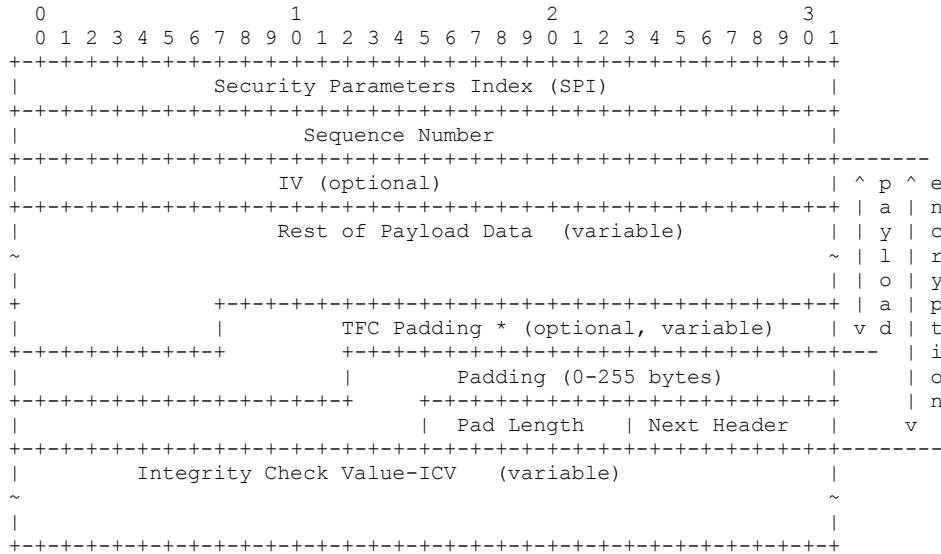


Figure 1. Encapsulating Security Payload Format

Having all said that, both AH and ESP have some common important fields: Next Header, Security Parameters Index (SPI), Sequence Number Field, and Integrity Check Value (ICV). Although the fields reside on the different places in each header format of AH and ESP, they works at the same way. Next Header indicates the type of the following payload, which is an original IP packet being encapsulated with a new IP packet. For example, a value of 4

indicates IPv4, a value of 41 indicates IPv6, and a value of 6 indicates TCP. This is how IPsec datagrams are linked together with respect to the original IP datagrams encapsulated in IPsec. Security Parameters Index (SPI) is used by a recipient to identify the Security Association (SA) to which incoming packet is bound. That is, SPI helps the recipient quickly associate the security (cryptographic) parameters needed to perform inbound processing. Sequence Number Field contains a monotonically increasing counter value for each packet sent. Similar to that of TCP, this field is used for anti-replay protection that IP didn't have before. Finally, Integrity Check Value (ICV) is a vital field used to deliver data origin authentication by checking the integrity of a message. ICV is computed by Message Authentication Code (MAC) algorithms based on symmetric cryptography (e.g. AES) or one-way hash functions (e.g. MD5, SHA-1, SHA-256, etc). In addition to those common fields in both AH and ESP, ESP has more fields for encryption capability as shown in Figure 1 [2:76]. Payload and variable length padding of packets are inserted in the additional fields, and then they are encrypted by symmetric cryptography altogether with Next Header. The details of cryptographic algorithm requirements for AH and ESP are defined in [8].

The IPsec protocols can be deployed on two operation modes: transport mode and tunnel mode. Two modes are defined in [5], and the insertion of AH and ESP in each mode are explained in their respective standards [6], [7]. In transport mode, the header of an original packet is preserved and either AH or ESP is inserted after the original IP header and before a next layer protocol (e.g. TCP, UDP, etc). In transport mode, only the payload and some header fields undergo cryptography processing of IPsec. Transport mode is primarily intended to protect the next layer protocols and used for a host-to-host IPsec environment. On the contrary, in tunnel mode, a new IP header followed by either AH or ESP is inserted before an original IP packet. That is, the original packet, called an inner IP packet, is entirely encapsulated within a new IP packet, called an outer IP packet. In tunnel mode, the original packet plus some header fields are treated as the new payload of the outer packet. Thus, the entire packets are protected by cryptography processing of IPsec. Tunnel mode is typically used at a security gateway. The reason is that an IPsec packet wrapped with a standard IP header can be appropriately forwarded into an IPsec-unaware destination by a security gateway. In this manner, the hosts need not be IPsec-aware and the security is guaranteed in gateway-to-gateway fashion. Thus, tunnel mode can be used for network-to-network, network-to-host, or host-to-host IPsec environment, depending on whether or not peers are IPsec-aware.

While all these fundamental protocols and operation modes define specific formats and mechanisms, there is another key element in IPsec. That is Security Policy Database (SPD) defined in [5]. SPD can be thought of as a set of processing rules that define what traffic is to be processed by IPsec in what fashion. In some sense, it's similar to the rules for conventional packet filtering mechanisms. Depending on the rules set up in SPD, a packet may be simply discarded, a packet may be bypassed encryption processing, if not necessary, but required for integrity check, or a packet may be undergone a complete IPsec processing. The rules in SPD are manually configured by a security administrator, by hand, as they are done in other traditional rule-based management system. Thus, that might be a tedious and error-prone task as the complexity of policy for a network grows. Nevertheless, it's a necessary part of IPsec because all packets are not likely to afford the overhead of IPsec processing in one fixed fashion when the network undergoes heavy traffic. If bottlenecks occur in IPsec, that might be

another vulnerability that allows attackers to target DoS/DDoS on IPsec itself. The related concerns are introduced in the next section.

There are two other key components in IPsec: Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE). Two components of IPsec were originally defined in separate documents, but the latest versions were combined to IKEv2 in [9]. It defines the overall structure of protocols used to establish SAs that include shared secret information and a set of cryptographic algorithms used for secure communication. Thus, IKE actually performs mutual authentication and establish and maintain SAs. The cryptographic algorithms required for key exchange are defined in [10].

4. Related Issues and Works

IPsec employs cryptography for authentication, confidentiality, and integrity. However, those security features were not originally provided all-in-one. As mentioned earlier in this paper, IPsec has evolved through a series of versions and the specifications were defined a number of documents. The initiative step of the development of IPsec was innovative. Nevertheless, the early version of IPsec was so abstract and complex and didn't offer a clear guideline for implementations. In fact, a whole bunch of criticisms and concerns about IPsec can be found in almost every earlier report. Among them, the complexity of IPsec is one of the most perceptible issues discussed in [2], [3], [4]. Niels Ferguson and Bruce Schneier said, "IPsec is too complex to be secure. The design obviously tries to support many different situations with different options [4:4]." The complexity of possible combination of methods and protocol options for IPsec can lead erroneous configurations and implementations, and therefore the chances to create another security weakness are likely to rapidly grow when they are used incorrectly [4:4]. The complexity problem is not only resulted from IPsec itself but from the transition from IPv4 to IPv6. The good thing for IP network security is IPv6, the next-generation IP, adopts IPsec as a mandatory. However, unsmooth transition from IPv4 to IPv6, which is highly likely to happen in the next few years, will increase the complexity of security systems and therefore may cause possible incompatibility and vulnerabilities [11].

Another concern results from the use of cryptographic algorithms that IPsec primarily benefits from. The use of encryption and authentication has well-known side effects, which bring about heavy computations that consume considerable amount of time and resources. As a result, the computational burden in using IPsec can "paradoxically" lead DoS/DDoS attacks that intentionally target on IPsec itself [12:6]. Sending heavy traffic or false packets that stimulate IPsec's processing can successfully exhaust the resources of IPsec-enabled systems at will. To mitigate such mutant DoS attacks, "hierarchical" (or layered) defense approaches can be significantly effective on filtering out some hostile traffic [12], [13]. According to [12], trivial nonce-based validation before IPsec's processing can efficiently reduce some attack traffic to avoid turning IPsec from a protection to an opportunity for attack. Another approach using lightweight authentication random bit string, called "classifier", provides the same effect of hierarchical defense [13].

5. Conclusion

With the power of TCP/IP protocol suite, IP network has been incredibly successful since the need for internetworking was emphasized, and even more it sees huge potential in

upcoming ubiquitous networking era. Meanwhile, IP network has also suffered from many attacks that utilize the vulnerabilities of IP protocol. As a consequence, IPsec was invented to resolve the fundamental weakness of IP by putting security services in the IP network. The security services include data origin authentication, confidentiality and connectionless integrity check of contents in IP datagrams, anti-replay attack option, and access control and filtering by security policy. Despite early unsatisfactory outputs, IPsec has improved from the first generation one by one. Finally, IPsec is adopted by IPv6 as a mandatory and many modern operating systems now have IPsec capability. However, the evolution of IPsec needs to continue in order to simplify its complex architecture and implementations. More importantly, reducing the computational overhead of IPsec and employing helper systems are critical to avoid turning itself from a protection to a target for “smarter” attackers.

References

- [1] Andrew S. Tanenbaum, *Computer Networks*, Fourth Edition, Prentice Hall PTR, New Jersey, 2002.
- [2] Kenneth G. Paterson, "A Cryptographic Tour of the IPsec Standards," *Information Security Technical Report*, Vol. 11, No. 2, Elsevier Ltd., 2006, pp. 72-81.
- [3] Neil Dunbar, "IPsec Networking Standards – An Overview," *Information Security Technical Report*, Vol. 6, No. 1, Elsevier Ltd., 2001, pp. 35-48.
- [4] Niels Ferguson and Bruce Schneier, "A Cryptographic Evaluation of IPsec," Unpublished manuscript, Feb. 1999. [Online]. Available: <http://www.schneier.com/paper-ipsec.html>. [Accessed: Mar. 24, 2007].
- [5] S. Kent and K. Seo, Security Architecture for the Internet Protocol, IETF RFC 4301, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4301.txt>.
- [6] S. Kent, IP Authentication Header, IETF RFC 4302, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4302.txt>.
- [7] S. Kent, IP Encapsulating Security Payload, IETF RFC 4303, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4303.txt>.
- [8] D. Eastlake 3rd, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), IETF RFC 4305, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4305.txt>.
- [9] C. Kaufman, Ed., Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4306.txt>.
- [10] J. Schiller, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), IETF RFC 4307, Dec. 2005, <http://www.rfc-editor.org/rfc/rfc4307.txt>.
- [11] Philip Hunter, "IPv6: Security Issues," *Network Security*, Vol. 2004, Issue 1, Elsevier Ltd., Jan. 2004, pp. 17-19.
- [12] Joseph D. Touch and Yi-Hua Edward Yang, "Reducing the Impact of DoS Attacks on Endpoint IP Security," *Proceedings of the 2nd IEEE Workshop on Secure Network Protocols*, Nov. 2006, pp. 6-11.
- [13] H. Johnson, B. Qaisrani, M. Fiedler, A. Nilsson, and S. F. Wu, "Hierarchical Defense Structure for Mitigating DoS Attacks," *Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies ICNICONSMCL '06*, IEEE Computer Society Press, Apr. 2006.