IMPLEMENTATION OF IPSEC PROTOCOL

Mr. Hitesh dhall[1]
Asstt. Prof. , MCA
Deptt.
SPGOI
Rohtak, India
e-mail:
Hitesh_dhall001@yahoo.co.in

Ms. Dolly Dhall[2]
Asstt. Prof. , MCA
Deptt.
SPGOI
Rohtak, India
e-mail:
dollychugh2001@yahoo.co.in

Ms. Sonia Batra[3]
Asstt. Prof. , MCA
Deptt.
SPGOI
Rohtak, India
e-mail:
batra2302sonia@gmail.com

Ms. Pooja Rani[4]
Computer Teacher.
Holy Family School
Gohana, India
e-mail:
batra2302sonia@gmail.com

Abstract

The aim of this paper is to present the implementation of IPSec Protocol. IPSec protocol provides an end user to end user traffic with ensuring authenticity and confidentiality of data packet. IP sec is a successor of the ISO standard Network Layer Security Protocol (NLSP). NLSP was based on the SP3 protocol that was published by NIST, but designed by the Secure Data Network System project of the National Security Administration (NSA).
IPSec is officially specified by the Internet Engineering Task Force (IETF) in a series of Request for Comments addressing various components and extensions, including the official capitalization style of the term.IPSec defines encryption, authentication and key management routines for ensuring the privacy, integrity and authenticity of data in a VPN as the information traverses public IP networks. Because IPSec requires each end of the tunnel to have a unique address, special care must be taken when implementing IPSec VPNs in environments using private IP addressing based on network address translation. Fortunately, several vendors offer solutions to this problem. However, they add more management complexity.

Key words: IPSec, ISO, Network Layer Security Protocol (NLSP), Internet Engineering Task Force (IETF), National Security Administration (NSA), Internet Engineering Task Force (IETF), VPN

I. INTRODUCTION

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session[7]. IPSec can be used to protect data flows between a pair of hosts, between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. IPSec is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3. Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of these models. Hence, IPSec can be used for protecting any application traffic across the Internet. Applications need not be specifically designed to use IPSec. The use of TLS/SSL, on the other hand, must typically be incorporated into the design of applications.

The basic services that IPSec provides are:-

1. Access Control How should the load on the visited Web sites be minimized?
2. Connectionless integrity
3. Origin authentication
4. Replay protection
5. Rejection of replayed packet

All these services provide greater security to the data communication in any network, that's why the research proposed for secure data communication in ad-hoc network by IPSec protocol.

II. IPSEC ARCHITECTURE

This includes various components of IPSec, how they interact with each other, the protocols in the IPSec family, and the modes in which they operate. The IP Sec working group at the IETF has defined 12 RFCs (Request for Comments). The RFCs define various aspects of IPSec - architecture, key management, base protocols, and the mandatory transforms to implement for the base protocols.

THE IPSec ROADMAP

The IPSec protocols include - AH, ESP, IKE, ISAKMP/Oakley, and transforms. In order to understand, implement, and use IPSec, it is necessary to understand the relationship among these components. The IPSec roadmap defines how various components of IPSec interact with each other. This is shown in Figure 1.

IP Sec is a suite of protocols and it is important to understand how these protocols interact with each other and how these protocols are tied together to implement the capabilities described by the IPSec architecture.

978-0-7695-4640-7/12 $26.00 © 2012 IEEE
DOI 10.1109/ACCT.2012.64

The IPSec architecture defines the capabilities the hosts and gateways should provide. For example, IPSec architecture requires the host to provide confidentiality using ESP, and data integrity using either AH or ESP and entirely protection. However, the architecture document does not specify the header formats for these protocols. The architecture discusses the semantics of the IPSec protocols and the issues involved in the interaction among the IPSec protocols and the rest of the TCP/IP protocol suite[4]. The ESP and the AH documents define the protocol, the payload header format, and the services they provide. In addition these documents define the packet processing rules. However, they do not specify the transforms that are used to provide these capabilities. This is because the new transforms can be defined when the algorithms used by the older transforms are proved to be cryptographically insecure. However, this does not mandate any change to the base protocols. The transforms define the transformation applied to the data to secure it. This includes the algorithm, the key sizes and how they are derived, the transformation process, and any algorithmic-specific information. It is important to be specific about the necessary information so that different implementations can interoperate. Let us consider the DES-DBC transform that is defined for ESP. If we do not specify how the Initialization Vector is derived, the two implementations end up deriving the Initialization Vector in different ways, and they will never be able to interoperate.

IKE generates keys for the IPSec protocols[6]. IKE is also used to negotiate keys for other protocols that need keys. There are other protocols in the Internet that require security services such as data integrity to protect their data. One such example is OSPF (Open Shortest Path First) routing protocol. The payload format of IKE is very generic. It can be used to negotiate keys for any protocol and not necessarily limit itself for IPSec key negotiation. This segregation is achieved by separating the parameters IKE negotiates from the protocol itself. The parameters that are negotiated are documented in a separate document called the IPSec Domain of Interpretation. An important component that is not yet a standard is "policy." Policy is a very important issue because it determines if two entities will be able to communicate with each other and, if so, what transforms to use. It is possible, with improperly defined policies, for two sides to be unable to communicate with each other.

III. IPSec IMPLEMENTATION

IPSec can be implemented and deployed in the end hosts or in the gateways/routers or in both. Where in the network IPSec is deployed depends on the security requirements of the users. This section discusses the capabilities and implications of implementing IPSec in various network devices (hosts and routers).

HOST IMPLEMENTATION

The proper definition of a host in this context is the device where the packet is originating. The host implementation has the following advantages:

- Provides security end to end
- Ability to implement all modes of IPSec Security
- Provides security on a per flow basis
- Ability to maintain user context for Authentication in establishing IPSec Connections

Host implementations can be classified into:

a) Implementation integrated with the operating system (OS). We call it host implementation (for lack of a better term!).
b) Implementation that is a shim between the network and the data link layer of the protocol stack. This is called the "Bump in the Stack" implementation.

a) OS Integrated

In the host implementation, IPSec may be integrated with the OS. As IPSec is a network layer protocol, it may be implemented as part of the network layer as shown in Figure 2. IPSec layer needs the services of the IP layer to construct the IP header. This model is identical to the implementation of other network layer protocols such as ICMP.

There are numerous advantages of integrating the IPSec with the OS. A few key advantages are listed below.

- As IPSec is tightly integrated into the network layer, it can avail the network services such as fragmentation, PMTU, and user context (sockets). This enables the implementation to be very efficient.
- It is easier to provide security services per flow (such as a Web transaction) as the key management, the base IPSec protocols, and the network layer can be integrated seamlessly.
- All IPSec modes are supported.

b) Bump in the Stack

For companies providing solutions for VPNs and intranets, OS integrated solution has one serious drawback. On the end hosts, they have to work with the features provided by the OS vendors. This may limit their capabilities to provide advanced solutions. To overcome this limitation, IPSec is implemented as a shim, and inserted between the network and the data link layer as shown in figure 3. This is commonly referred to as Bump in the Stack (BITS) implementation.

As you may notice, the major issue in this implementation is duplication of effort. It requires implementing most of the features of the network layer, such as fragmentation and route tables[5]. Duplicating functionality leads to undesired complications. It becomes more difficult to handle issues such as fragmentation, PMTU, and routing. An advantage of BITS implementation is the capability of an implementation to provide a complete solution. Vendors providing integrated solutions such as firewalls prefer to have their own client as the OS vendor and may not have all the features required providing a complete solution.

ROUTER IMPLEMENTATION

The router implementation provides the ability to secure a packet over a part of a network. For example, an organization may be paranoid about the Internet and not its own private network. In this case, it may want to secure only those packets destined to the geographically distributed branch as these packets traverse the Internet to build its VPN or intranet. The IPSec implementation provides security by tunneling the packets[2].

The router implementation has the following advantages:

- Ability to secure packets flowing between two networks over a public network such as the Internet.
- Ability to authenticate and authorize users entering the private network. This is the capability that many organizations use to allow their employees to telecommute over the Internet to build its VPN or intranet. Previously, this was possible only over dial-ups (dialing through modem directly into the organization).

There are two types of router implementation:

a) **Native implementation:** This is analogous to the OS integrated implementation on the hosts. In this case, IPSec is integrated with the router software.

b) **Bump in the Wire (BITW):** This is analogous to BITS implementation. In this case, IPSec is implemented in a device that is attached to the physical interface of the router. This device normally does not run any routing algorithm but is used only to secure packets. BITW is not a long-term solution as it is not viable to have a device attached to every interface of the router.

The network architectures for these implementations are shown in figure 4.1 and figure 4.2.

The IPSec implementation on routers has many implications on the packet-forwarding capabilities of the router. The routers are expected to forward packets as fast as possible. In fact, we are already seeing core routers that can forward up to 30 million packets per second! Although IPSec may not be used in the core of the Internet, the implementations should still be concerned about efficiency. The packets that do not require security should not be affected because of IPSec. They should still be forwarded at normal rates. Many implementations make use of some hardware assists to perform public key operations, random number generation, encryption/decryption, and calculating hashes. There are specialized chipsets that assist the basic router hardware with security operations.

Another issue with router implementation is IPSec contexts. Memory on the routers is still a scarce commodity, although this is changing fast with memory prices falling rapidly. As the router has to store huge routing tables and normally does not have huge disks for virtual memory support, maintaining too many IPSec contexts is an issue.

IV. WORKING PRINCIPLE OF IPSEC IMPLEMENTATION

A working principal has been also proposed by this research for implementing the parameters proposed in the above section for both AH and ESP of IPSec implementation[7].

WORKING PRINCIPLE OF AH

After sending data packet with AH header, data packet will be processed only by the destination node. Intermediate nodes will not authenticate the data because security association is established host to host basis from source to destination. If any intermediate malicious node changes the data packet then the authentication data will certainly change. But the node will not be able to generate the same Message Authentication Code or MAC because it doesn't have the shared secret key of source and destination[1]. Upon receiving the data packet destination node will regenerate the MAC and will compare it with the MAC supplied with the Authentication data of AH header and if it matches then the destination will send an ACK packet to acknowledge that authentication and integrity of data has not been violated. Otherwise it drops the packet and does not send the ACK packet. Without receiving the ACK source will re transmit data again.

WORKING PRINCIPLE OF ESP

ESP header will also be processed in the destination node similar to AH header. Intermediate nodes will not be able to see the encapsulated data packet as it is encrypted with the shared key between source and destination and SA is established host to host basis from source to destination. If any intermediate malicious node wishes to change the data packet then it will not be able to do because new IP header, which is outside the encapsulated packet, is only visible to the malicious node. Both the original IP header and data packet is encapsulated using the shared key between source and destination. Upon receiving the packet the destination node will de-encapsulate using the shared key. After successfully decrypting the packet destination will send an ACK packet to acknowledge that the confidentiality, integrity and authenticity has not been broken. On the contrary if source do not receive any ACK from destination then it will retransmit the packet again.

V. ALGORITHM OF THE PROPOSED IPSEC IMPLEMENTATION

After details working principles for implementing both AH and ESP, the research is now proposed an algorithm for secure data communication in ad-hoc network with combining both AH and ESP.

1. Route Discovery by SAODV[3]

SAODV route Discovery: Source→ Destination
[Shared key of both source and destination will be exchanged during this phase]

2. Establishment of SA

Data_Message= ((Sequence Number Counter +AH Information/ESP
Information) EKS-priv) EKD-pub: Source → Destination (With First UDP Packet)
[AH information: authentication algorithm, shared secret key, key lifetime]
[ESP information: encryption algorithm, shared secret key, key lifetime]

3. Data Transmission

IF (AH implemented packet)
Packet with AH header: Source → Destination and Destination → Source
ELSE IF (ESP implemented packet)
Packet with AH header: Source →Destination and Destination → Source

4. ACK_PKT

IF (Check (Authentication) = = true))
Send ACK_PKT
ELSE IF ((De encapsulate (Packet) & & check (Authentication)) = = true)
Send ACK_PKT
ELSE
Drop PKT

5. Receive ACK_PKT

If sender Receive (ACK_PCK) = = true)
Send next packet
Else
Retransmit same data packet

6. ***End***

VI. COMPARISON OF AH AND ESP IMPLEMENTED PROTOCOLS

Table 1 shows, time difference with AH implemented and without AH implemented data packet for variable no of nodes. It shows when number of nodes increases then the time difference also increases. For total number of nodes between 3 to 11 the time difference range is less than 0.5 but when total number of nodes increased from 11 to 15 then time difference rate increase at a rate more than double compares to total no of node in range 3 to 11. Again total no of node above 15 time differences rate of increase is negligible. Figure 5 shows the time difference rate increase dramatically from 11 nodes to 15 nodes then again increases at a steady rate. So AH implemented data packet in ad-hoc networks consume more time to transmit data from source to destination compare to without AH implemented data packet.

Time difference found by this research is from 0.39 ms to maximum 2.1 ms. but for this extra time, all users in the network can get authentication service for all data packet in ad-hoc networks.
On the contrary, the research plots the table 2 for the time difference between ESP implemented packet and without ESP implemented packet. The data shows variation of time difference among difference number of nodes. From total no of nodes 7 to 9 the difference is 0.6 ms then the time difference is decrease from total no of nodes 9 to 11 nodes by 0.1 ms. From total no of nodes 13 to 15, the time difference is maximum 2.4 ms. Again it increase slightly from total number of node more than 15. Figure 6 shows the graph with time difference between ESP implemented packet and with out ESP implemented packet. Here time difference start from 0.5 ms to maximum 2.4 ms.

The research adds 20 bytes for including different SA parameters for implementing AH in existence data packet of ad-hoc networks. Time overhead increase maximum 2.12 ms for total 21 nodes. The extra time is expected theoretically by this research, which matches with the simulation result. This extra time can incur for providing authentication service for data packet in ad-hoc networks. The research also adds 13 bytes for including difference SA parameters for implementing ESP in data packet. Here another 9.89 ms added for considering encryption and decryption time with ESP implemented packet. So, total overhead added by this research for ESP implementation in data packet is 13 bytes time and 9.89 ms for handling encryption and decryption of data packet.

Compare to AH, timing overhead is more in ESP implemented packet. Time difference between ESP implemented packet and with out ESP implemented packet is always more than 9.89 ms except total number of node 13. Time difference between ESP implemented data packet is higher than AH implemented, which the research except theoretically. The nature of time difference with change of variable no of node is almost similarly for both AH implemented packet and ESP implemented packet. But the service provided with ESP implemented packet is more than AH implemented packet.

CONCLUSION

The proposed IPSec implementation attempts to ensure data communication security. Sending and receiving data packets with IPSec needs more time as compared to sending data packets without IPSec. Between AH implemented and ESP implemented data packets, ESP implemented data packets consume more time due to handling encryption. The simulation result of this research also shows the similar result that the research expects theoretically. If an application needs only authentication, then this research proposes to use only AH-implemented data packets with minimum time overhead. The research encourages implementing IPSec with ESP for all security services with moderate time overhead.

REFERENCES

[1] Charles P. fleeger, Shari Lawerence Pfleeger (2003), Security in Computing, Pearson Education, Singapore.

[2] Crawley, E., Nair, R. Rajagopalan, B., and Sandick, H. (Aug. 1998), A Framework for QoS-Based Routing in the Internet, Internet IETF RFC2386.

[3] Manel Guerrero Zapata (2001), Secure Ad hoc On-demand Distance Vector (SAODV) Routing draft-guerrero-manet-saodv, Nokia research center, Internet Draft.

[4] A. Tanenbaum, Computer Networks (2003), (4th ed.), New Jersey, Prentice Hall PTR.

[5] William stalling, Network Security Essentials, Application and standard.

[6] William stalling, Cryptography & Network security, Principles & practice, (3 rd ed.).

.

[7] Bhajandeep Singh, Future of Internet Security –IPSec, http://www.securitydocs.com/library/2926

FIGURES AND TABLES

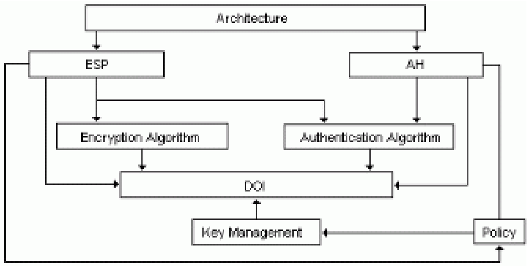
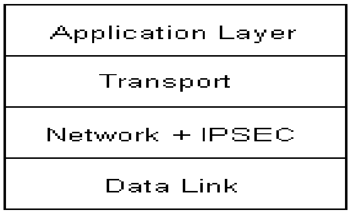
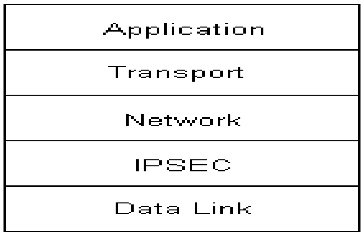


Figure 1: IPSec Roadmap



Application Layer
Transport
Network + IPSEC
Data Link

Figure 2: IPSec stack layering



Application
Transport
Network
IPSEC
Data Link

Figure 3: BITS IPSec stack layering

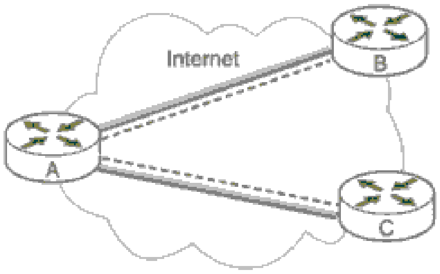


Figure 4.1: Native Implementation deployment architecture

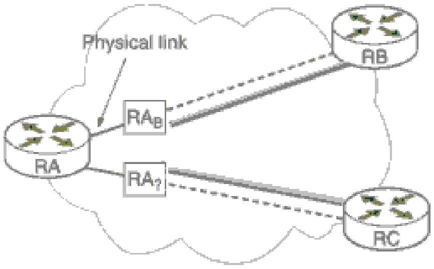


Figure 4.2: BITW deployment architecture

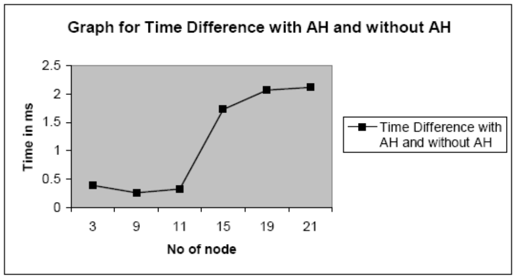


Figure 5: Time difference Graph with AH and Without AH

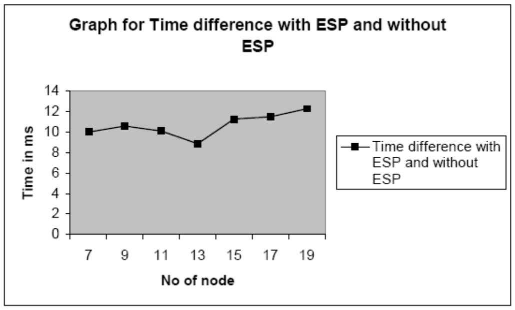
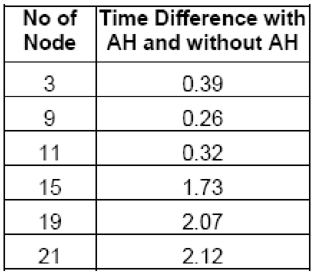
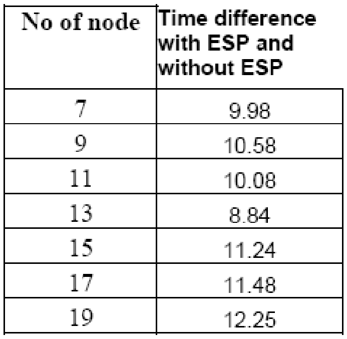


Figure 6: Time difference Graph with ESP and Without ESP



No of Node	Time Difference with AH and without AH
3	0.39
9	0.26
11	0.32
15	1.73
19	2.07
21	2.12

Table 1: Time_difference with AH and Without AH



No of node	Time difference with ESP and without ESP
7	9.98
9	10.58
11	10.08
13	8.84
15	11.24
17	11.48
19	12.25

Table 2: Time difference with ESP and Without ESP