ELEC-C7420 - Basic principles in networking

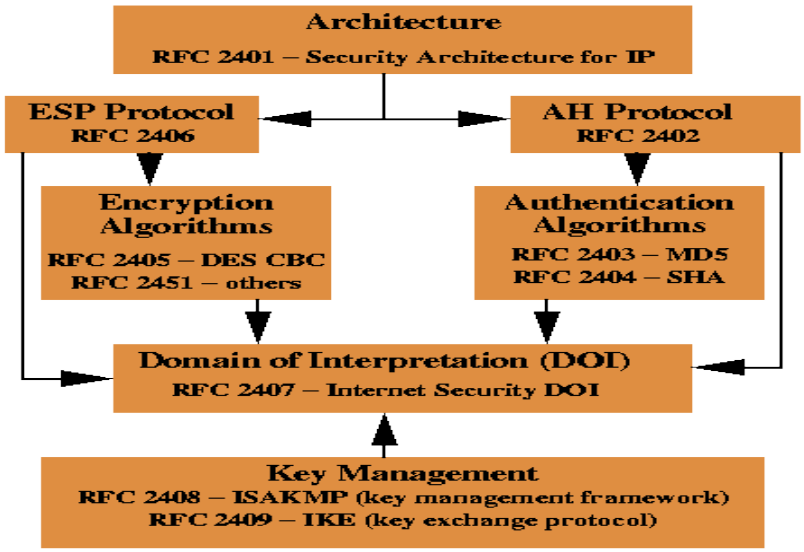
Assignment V – Ipsec & VPN

1 Definition of IPsec

IPsec (abbreviation for IP security) are protocols defined by IETF (Internet Engineering Task Force) for transferring data securely over unprotected networks like the Internet. IPsec acts at the network layer, protecting data by encrypting and authenticating IP packets. IPsec is an obligatory part of IPv6 and optional for IPv4. IPsec protocols incorporate the following features:

1. Encrypt packets before sending them on the unprotected network.
2. IPsec receiver authenticates packets from the sender to ensure the integrity of the data received.
3. Anti replay checks for, and rejects, duplicate packets to prevent DOS attacks.
4. A Key exchange mechanism called IKE is used to securely exchange keys.

2 IPsec Architecture



Source: IPSec Architecture Overview

2.1 Encapsulating Security Payload and Authentication Header

One of IPSec's main goals is the protection of IP datagram's, which is achieved using the Encapsulation Security Payload (ESP) and Authentication Header (AH) protocols. The ESP protocol was designed to provide both authentication and integrity. Due to the mutable nature of certain parts of the IP header, it is impossible for ESP or AH to provide complete confidentiality or integrity protection to the IP header. In ESP everything after the IP header is encrypted and a new ESP header is inserted after the IP header, so it provides no protection to the header. The AH protocol is designed to provide integrity only, so the immutable fields of the IP header and everything after the IP header is integrity protected. Some feel (Microsoft) that AH is somewhat redundant due to the existence of the NULL encryption algorithm,

which, when used with ESP, essentially achieves the same integrity protection as AH; however, AH does provide some integrity protection to the IP header that ESP does not.

2.1.1 Modes of AH and ESP operation

There are two modes of IPsec operation for Authentication Header and Encapsulating Header Payload:

In the **Transport Mode** only the payload of the message is encrypted.
In the **Tunnel Mode** the payload, header and routing information are encrypted. This provides end to end security of data.

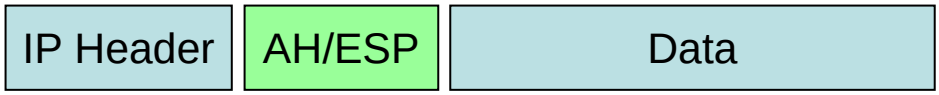


Fig 1. Transport Mode IPsec packet

Tunnel mode works by encrypting the original packet and placing it in the payload of a newly created IPsec packet. An IPsec packet is an IP packet with an AH or ESP header separating the IP header and payload segments. Tunnel mode hides all information of the original packet, however adds an extra layer of processing due to the additional IP header.

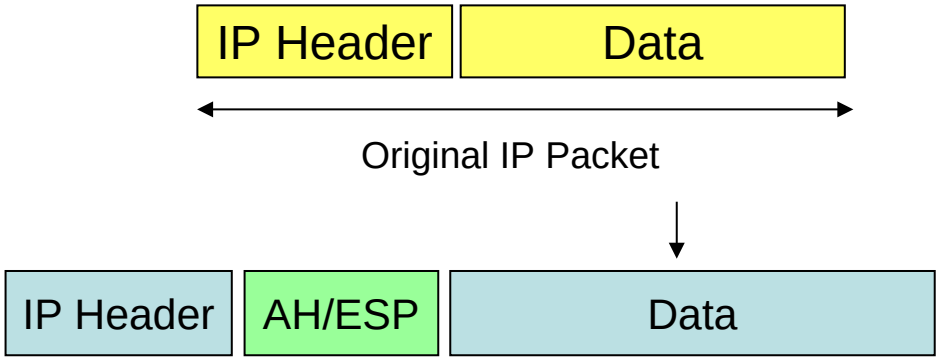


Fig 2. Tunnel Mode IPsec packet

2.2 Encryption Algorithms

IPSec uses a combination of two encryption algorithms; the first algorithm is used to provide confidentiality by encrypting the data, whereas the second is used to insure the data's integrity. IPSec supports a number of different encryption algorithms, including:

- DES, which was developed by IBM in 1974 and was embraced as a national standard in 1977.
- Triple DES is a variation of the original DES; it consists of some minor modifications to the original DES
- AES is the Advanced Encryption Standard and is the official name of the Rjindael algorithm.
- NULL encryption algorithm that does not actually perform any encryption.

2.3 Authentication Algorithms

Authentication in IPSec is used as a means to insure the integrity of the data by hashing everything after the IP header and attaching it to the packet as an integrity checksum value. When the packet reaches the destination host, the same hash is again calculated and the generated value compared to the integrity

checksum value, if they match the data in the packet has not been tampered with. Some of the standard authentication algorithms included in IPSec are:

- HMAC, which is an authentication algorithm for keys that is used in conjunction with an underlying iterative hash function such as MD5 or SHA-1.
- MD5, developed by Ronald Rivest of MIT, takes a message of arbitrary length and generates a unique 128-bit "fingerprint" of the message.
- SHA-1 was a joint project involving the NIST and the NSA. Similar to MD5, SHA-1 takes a message up to 2^{64} bits long and generates a 160 bit fingerprint of the message.

2.4 Internet Key Exchange (IKE RFC – 2409)

Another goal of the IPSec protocol is mutual authentication. This is achieved using the Internet Key Exchange (IKE) protocol, which also provides symmetric key exchange functionality, in addition to mutual authentication. IKE consists of two phases. The first phase involves the establishment of an IKE Security Association (SA), and in the second phase an AH/ESP SA is created. The first phase is further broken down into three key options (each having two modes that can be implemented, a main mode and an aggressive mode). The three key options of IKE Phase 1 are:

2.4.1 Public Key Encryption

- In Main mode this key option involves a six message protocol that results in the creation and exchange of a session key using each party's public/private key pair;
- Aggressive mode achieves the same result as main mode, but using half the number of messages

2.4.2 Public Key Signature

- The Main mode of this key option, also a six message protocol, establishes a shared symmetric key between the two parties by means of public signatures. The last two message exchanged in the protocol are digitally signed by the source party, thereby guaranteeing their authenticity.
- Aggressive mode, again, achieves the same results as the Main mode, but using fewer messages. Aggressive mode achieves fewer messages by removing the messages that allow the parties to mutually agree on which cryptographic algorithm to use, instead the entity initiating the connection, essentially, dictates the crypto to be used.

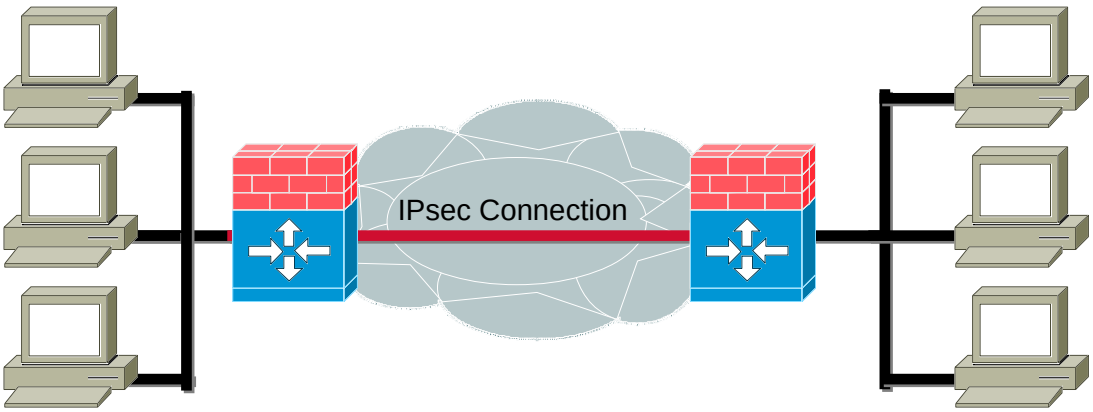
2.4.3 Symmetric Key

- In Symmetric Key Main mode (which is, again, a six message protocol) the session key is established using an existing shared symmetric key. The entity initiating the connection identifies itself to the target entity using its IP address. Once the target entity has identified the initiating entity, it knows which shared symmetric key to use to decrypt subsequent messages.
- The Aggressive mode of this key option uses half as many messages because it does not attempt to hide the identities of the parties that are trying to connect to each other.

3 Scenarios for deployment

The various scenarios for deployment are Host-to-Host, Host-to-Gateway and Gateway-to- Gateway. Below is a diagram showing a Gateway-to-Gateway connection.

Gateway-to-gateway



4 Implementation examples

There are two common approaches for implementing IPsec in the real world. The **bump-in-stack approach** consists of updating the OS network stack with a driver that handles the IPsec protocol. The newly added driver sniffs packets on the stack and applies the necessary IPsec processing appropriately. For example, IPsec client software may be installed and configured on a host to perform IPsec encapsulation on all packets destined for 216.101.194.10 (an IPsec gateway or host). The IPsec software binds to the network stack and sniffs all packets, upon seeing a packet with the remote gateway's IP address, performs the necessary IPsec processing and continues sending it down the stack. This approach works well for remote communication of individual hosts, for example sales employees who want to connect securely from remote locations. The downside of this approach is adding software that binds to the network stack can cause software conflicts with other network applications installed on the host (i.e. Personal firewalls).

The **bump-in-wire approach** consists of adding a network device positioned in front of a host or network that performs the IPsec processing as packets pass through. This approach is the most preferred method because of it single point of configuration and transparency to hosts.

5 Benefits of IPsec

The major benefit of using IPsec is that it operates at the network layer and therefore is application agnostic. No changes are needed to existing applications in order to establish secure communications. Another benefit is that IPsec is a standard, so in theory products from different manufacturers should be interoperable.

6 Limitations of IPsec

Complexity: IPsec is a complicated protocol that is specified over six RFCs. complexity of the standard makes implementation difficult and sometimes incorrect.
Configuration: Another drawback of IPsec is its configuration. IPsec involves the configuration of lengthy key pairs for the client and server.
Performance: IPsec involves a lot of extra processing for encryption and encapsulation/decapsulation of additional IP headers. This extra processing requirement limits the speeds at which IPsec networks can operate.

7 Current areas of research and enhancement for robust data transmission

IPV6 – IPsec is included in the IPV6 standard. A header field in IPV6 corresponds to IPSec AH/ESP header

8 References

- IP Encapsulating Security Payload, http://www.ietf.org/rfc/rfc2406.txt
- IPSec, **http://www.mywiseowl.com/articles/IPsec**
- IP Security (RFC – 2411)**, http://rfc.net/rfc2411.html**
- IPSec Product Overview, **http://66.102.7.104/search?q=cache:S-usqPxYnIJ:www.freesoft.org/CIE/Topics/141.htm+Ipsec&hl=en&start=33**
- IPsec (IP Security Protocol), **http://www.nwfusion.com/details/720.html**
- Understanding IPsec, **http://www.intranetjournal.com/articles/200206/se_06_13_02c.html**
- **Information Security, Principles and Practice,** *Mark Stamp*
- www.solaris.com

Assignment

Create a simple server and client socket and secure the data exchange using VPN. You can use any programming language (Python preferred) and any VPN tunneling application and capture the VPN traffic using Wireshark.

Assessment points are segmented like below.

Total 9 points.

- Successful implementation of server and client (3 Points)
- Successful communication between server and client using VPN (3 points)
- VPN traffic capture using Wireshark (3 Points)

Please share detailed report for the whole process. Report format should-

- Include all the scripts in the annex section.
- include enough snapshots to motivate the assessment and have step by step detailed explanation of the whole procedure.
- Please, note that, the report has to be easy to understand and sequential.

Deadline: 10th April, 2019