Encapsulating Security Payload:

Strengths and Weaknesses

Shawn W. Toderick

DTEC 6823

East Carolina University

July 23, 2004

INTRODUCTION

IP Security is a large and complicated specification that has many options and is very flexible. The Encapsulating Security Payload protocol can handle all of the services IPsec requires. This paper will attempt to discuss the Encapsulating Security Payload (ESP) protocol – a comparison with Authentication Header, and ESP weaknesses and strengths.

OVERVIEW OF IPSEC

In November 1998, the RFCs for IP Security (IPsec) were released – RFC 2401 through RFC 2411. As specified in RFC 2401 [1], IPsec provides security services at the IP layer by enabling a system to select required parameters, such as security protocols, security algorithms for the services, and any cryptographic keys the service requires.

IP-level security services cover authentication, confidentiality, and key management. Authentication verifies the sender and that the packet has not been altered, confidentiality provides encryption, and key management addresses the secure exchange of keys.

IPsec call for two security protocols – Authentication Header (AH) which provides authentication, and Encapsulating Security Payload (ESP) which provides authentication, encryption, or both. IPsec also has two modes of operation: transport mode and tunnel mode.

Ferguson and Schneier [2] address the complexity that the combination of the two protocols and two modes create. Ferguson and Schneier discuss the

complexity of IPsec and its components, which is outside the scope of this paper. It should be noted though, that they recommend the elimination of transport mode (which they believe to be a subset of tunnel mode) and AH (due to the elimination of transport mode) without the loss of any functionality.

AH AND ESP COMPARISON

This comparison between the AH protocol and the ESP protocol encompasses IPv4 implementations only.

AH, defined in RFC 2402 [3] provides support for data integrity and authentication of IP packets. AH provides authentication of the payload and the packet header and protects against replays with the use of sequence numbers, but does not provide confidentiality (encryption).

ESP, defined in RFC 2406 [4], provides confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. ESP authentication is provided by the combination of the data origin authentication and connectionless integrity services, which are optional. Anti-replay, also optional, may only be used if data origin authentication is employed.

The main difference between AH and ESP is the extent of the coverage of authentication services. ESP only protects those IP header fields it encapsulates, while AH protects as much of the IP header as possible as well as upper-level protocol data. [5] This may cause problems since some header fields change while in transit. To avoid these problems, AH needs be aware of all data

formats used at these upper levels. [2] This problem can be avoided by using ESP in tunnel mode.

AH requires less overhead than ESP since it only inserts an header into the IP packet (ESP requires the use of a header and trailer.) AH relies on the use of ESP or another mechanism to provide confidentiality. If confidentiality is required, this will cause additional overhead with using AH, especially if using ESP. If confidentiality is provided by ESP, then ESP should also provide authentication. This reduces the use of a packet running two security protocols.

AH provides a stronger authentication than ESP in transport mode, but in tunnel mode both protocols are equal in authentication strength. Without the use of transport mode the use of AH provides no benefits over ESP.

ESP WEAKNESSES

ESP's overhead weakness (compared to AH) has been addressed above. AH also has the following advantages over ESP:

- AH is never export restricted
- AH is mandatory for IPv6 compliance

Since ESP can use encryption, the particular type of encryption is restricted by export laws. Global implementations of ESP will need to use weaker encryption schemes. AH has no export restrictions, and therefore the strongest authentication required can be implemented in any situation. AH and ESP both have IPv4 and IPv6 specifications, but the use of ESP with IPv6 is

optional. If a particular implementation of IPsec uses only ESP for IPv4, any migration to IPv6 will require the incorporation of AH.

ESP also has weaknesses within itself, not just when compared to AH. RFC 2406 requires the use of Initialization Vectors in certain situations: if the algorithm used to encrypt the payload requires cryptographic synchronization data, e.g., an Initialization Vector (IV) . . . MUST indicate the length, any structure for such data, and the location of the data as part of an RFC specifying how the algorithm is used with ESP. [4, pg 5] This means that the IV is included in the ciphertext of every packet to allow the receiver to decrypt individual packets regardless of packet loss or reordering of packets.

Nuopponen and Vaarala [6] show that if "initialization vectors are chosen in a predictable manner in ESP, an adaptive chosen plaintext vulnerability opens up." An attacker can break low entropy plaintext blocks using brute force [6], as well as verifying strongly suspected plaintext [7]. While these attacks are difficult, they are possible in restricted situations.

There also exists a conflict between ESP and TCP performance enhancement proxy (PEP) deployed in IP wireless networks. "It is impossible for an intermediate gateway outside sender or receiver's security enclaves to analyze an IPsec header to extract TCP flow identification and sequence number . . . the PEP agent cannot obtain the information needed to generate acknowledgments or retransmit data segments." [8] Zhang argues that IPsec's tunnel mode and layering principles are unsuitable for new networking services and applications such as:

- Traffic Engineering
- Traffic Analysis
- Application –Layer Proxies/Agents
- Active Networks

In situations such as this, secure socket layer (SSL) or transport layer security (TLS) can provide the necessary data security. SSL/TLS operate at the Transport layer of the OSI model, and only encrypt the TCP data not the TCP header. This allows intermediate devices to view and use the TCP state information. In this aspect, SSL/TLS are a rival for IPsec, but only where TCP is concerned. SSL/TLS does not work on UDP, ICMP or other Transport layer IP protocols.

ESP STRENGTHS

As stated earlier, ESP provides the authentication function of AH as well as confidentiality making AH virtually unnecessary in an IPv4 environment.

In some instance of virtual private network (VPN) implementation, emphasis is placed on the *virtual* aspect. Strayer [9] argues that MPLS-based VPNs, using traffic engineering and resource management (QoS), provides a dedicated *private network*. This *private network* is only illusionary because MPLS does not take into account confidentiality, which ESP provides for IPsec-based VPNs. Without the use of encryption, attackers can sniff a network and obtain potentially damaging information. Also, MPLS does not work well outside of an Autonomous Systems (AS), as Strayer points out. This makes MPLS

practically useless between partner corporations – where IPsec, with tunnel mode, can provide the required security.

Most of ESP's strengths against other secure data transit technologies lie within IPsec's strength as a superior method to provide secure data transfer over unsecured networks.

SUMMARY

While different technologies exist that provide security for IP data in transit, such as SSL/TLS, IPsec provides the greatest overall IP coverage. Within the various options of IPsec to implement the three areas of IP level security – authentication, confidentiality, and key management – Encapsulating Security Payload provides the best solutions for authentication and confidentiality over Authentication Header (which provides no confidentiality by itself.) Even with these advantages of IPsec using ESP, there is a lot of room for improvement to make ESP a better security protocol.

REFERENCES

[1] Kent, Stephen, and Atkinson, Randal, “Security Architecture for the Internet Protocol,” RFC 2401, Nov 1998. Available from http://www.faqs.org/rfcs/rfc2401.html

[2] Ferguson, Niels, and Bruce Schneier, “A Cryptographic Evaluation of IPsec,” Feb 1999 Available from http://www.macfergus.com/pub/IPsec.html.

[3] Kent, Stephen, and Atkinson, Randal, “IP Authentication Header,” RFC 2402, Nov 1998. Available from http://www.faqs.org/rfcs/rfc2402.html

[4] Kent, Stephen, and Atkinson, Randal, “IP Encapsulating Security Payload (ESP),” RFC 2406, Nov 1998. Available from http://www.faqs.org/rfcs/rfc2406.html

[5] “Cisco Networking Academy Program Fundamentals of Network Security Companion Guide,” Cisco Press, 2004.

[6] Nuopponen, Antti and Vaarala, Sami, "Attacking Predictable IPsec ESP Initialization Vectors,” Helsinki Univeristy of Technology. 2002 Available from http://www.hut.fi/~svaarala/espiv.pdf

[7] Nuopponen, Antti and Vaarala, Sami, "An Attack against IPsec Transport Mode HTTP Access." Helsinki Univeristy of Technology. 2002. Available from http://www.hut.fi/~svaarala/publications/espiv/webaccess.html

[8] Zhang, Yongguang. "A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks." IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS Volume 22, Number 4 (2004). Available from http://ieeexplore.ieee.org/xpl/abs_free.jsp?arNumber=1295063

[9] Strayer, W. Timothy, “Privacy Issues in Virtual Private Networks,” Computer Communications, Volume 27, Issue 6, April 2004, Pages 517-521. Available from http://www.ir.bbn.com/documents/articles/vpn04.pdf