Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 17, 2014

S. Hong
Hughes Network Systems
H. Schulzrinne
Columbia U.

October 14, 2013

PBS NSLP: Network Traffic Authorization
draft-hong-nsis-pbs-nslp-04.txt

Abstract

This document describes the NSIS Signaling Layer protocol (NSLP) for network traffic authorization on the Internet, the Permission-Based Sending (PBS) NSLP. This NSLP aims to prevent Denial-of-Service (DoS) attacks and other forms of unauthorized traffic. PBS NSLP is based on a hybrid approach: a proactive approach of explicitly granting permissions and a reactive approach of monitoring and countering attacks. Signaling installs and maintains the permission state of routers for a data flow. A monitoring mechanism provides a second line of defense against attacks. PBS NSLP uses two security mechanisms: message security for protecting the integrity of the message on end-to-end traffic and channel security for protecting the integrity and confidentiality between adjacent nodes. To authenticate data packets, the PBS NSLP requests a sender to use an existing security protocol, the IPsec Authentication Header (AH).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 17, 2014.

Table of Contents

1. Introduction

This document defines an NSIS Signaling Layer Protocol (NSLP) for network traffic authorization to prevent Denial-of-Service (DoS) attacks and other forms of unauthorized traffic, the Permission Based Sending (PBS) NSLP. PBS NSLP is within the signaling application layer of the NSIS protocol suit which is described in [RFC4080].

In the PBS NSLP, a sender of IP data packets first has to receive permission from the intended receiver before it injects any packets into the network. The term "permission" represents the authority to send data. Therefore, unauthorized packets without permission and attack packets that exceed the permission given to the flow are dropped at the first router that is aware of the PBS NSLP. By default, routers only forward packets that are covered by a permission or may be rate-limited to a very small volume for high-assurance networks. The PBS NSLP has a network traffic monitoring mechanism, the PBS Detection Algorithm (PDA). In PDA, the periodic signaling messages are used to detect the attack flows. PDA provides the second line of defense against malicious traffic, which may have circumvented the permission-based mechanism. If it detects attacks, the signaling message triggers a reaction against the detected attack.

The PBS NSLP exploits the General Internet Signaling Transport (GIST) [RFC5971] that delivers the signaling messages along the data path to configure permission state of routers for a data flow. The message security (public key cryptography) is used to protect messages from being modified by attackers. The channel security (TLS and DTLS) is used to distribute a shared key for IPsec of data packets to the routers along the data path. The IPsec Authentication Header (AH) is used for authentication of the data packets.

Below, Section 4 gives an overview of the design. The PBS NSLP architecture is presented in Section 5. Section 6 describes the PBS NSLP operation. Section 7 presents the security of the message. The PBS detection algorithm is described in Section 8. Section 9 describes PBS NSLP message and object formats. Section 10 describes security considerations.

2. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

The terminology defined by GIST [RFC5971] are used in this document.

In addition, the following terms are used:

Attack: Denial-of-Service (DoS) attack.

Permission: The authority to send data. It is granted by a intended receiver who receives a request from a sender.

Trustworthy network: Routers are trusted and are not compromised. In this, DoS attacks from end users are not considered.

Byzantine network: Neither the sender nor the routers are trusted.

On-path: The data flow path.

On-path attacker: An attacker on on-path, such as a compromised router.

Off-path attacker: An attacker who inserts packets into the data path, but is not located on the data path himself.

Packet drop attack: An on-path attacker that drops legitimate packets.

PBS NE: NSIS Entity (NE) that supports the functions of PBS NSLP.

Flow identifier: A descriptor of data flow. The information in the flow identification are source IP address, destination IP address, protocol identifier, and source and destination port numbers.

4. Design Overview

There are four design requirements: robust, secure, scalable, and able to deflect DoS attacks.

4.1. Robust system

The PBS NSLP should be robust for changes of state. Soft-state supports the robustness of the system. Thus, the permission state is periodically refreshed by signaling messages. At the absence of the state refresh, the permission state is eliminated. The periodic refreshing of the state guarantees the awareness of changes of the permission state and data path.

4.2. Secure system

The permission state setup and management should be secure. The signaling messages that install and modify the permission state and distribute cryptography keys should not be forgeable. PBS NSLP uses message and channel security to protect authentication and integrity of messages. The authentication and integrity of the data messages should be guaranteed. PBS NSLP requests to use IPsec to protect the authentication and integrity of data message.

4.3. Scalable system

PBS NSLP should be scalable to be applicable in high-speed and large scale networks. PBS NSLP functionality does not need to be implemented in all routers. Thus, some of the routers that have PBS NSLP functionality should properly handle the authorization of data flows. In addition, the computational and signaling overhead should be small for scalability.

4.4. Defense against DoS attacks

The PBS NSLP should properly prevent DoS attacks in various network environments. The PBS NSLP uses the hybrid approach of proactive and reactive approaches. This hybrid approach can compensate the disadvantages of both approaches and accelerate the advantages of both approaches.

4.4.1. Proactive Approach

A receiver grants a sender a permission that represents an authority to send data. Therefore, data packets are categorized into two types; authorized packets and unauthorized packets. In the closed network in which all end users have a PBS NSLP functionality, the unauthorized packets without permission are dropped at the first

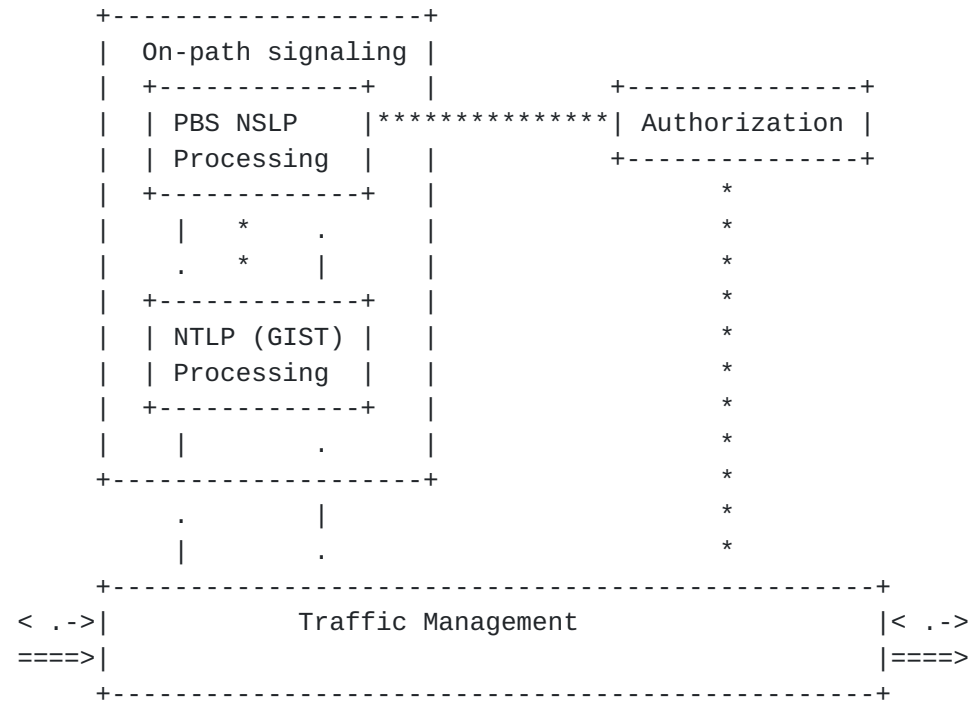
router by default. In the open Internet in which some end users do not have a PBS NSLP functionality, the flows from the end users who do not have a PBS NSLP functionality are rate-limited by default. This explicit permission can control resources on the path from a sender to a receiver. This permission for each flow mitigates the attacks since the attacker cannot exceed the spoofed permission.

4.4.2. Reactive Approach

Even though the attack flow does not have permission, the attack flow might spoof the permission. Therefore, we need to monitor the traffic flow and react against the detected attack. The PBS NSLP has a detection algorithm called PBS Detection Algorithm (PDA). Based on the detection, the PBS NSLP triggers the reaction against the attacks. The details of the PDA are described in Section 8.

5. PBS NSLP Architecture

The PBS NSLP architecture has three components: on-path (path-coupled) signaling, authorization, and traffic management. Figure 1 shows the PBS NSLP architecture.



< -.- > = signaling flow
======> = data flow
******* = configuration

Figure 1: PBS NSLP architecture

5.1. On-path Signaling

On-path signaling installs and maintains permission state, monitors attacks, and triggers the authentication mechanism. The NTLP (GIST) [RFC5971] handles all incoming signaling messages and it passes the signaling messages related to the PBS NSLP. The delivery of signaling messages is handled using a peer-to-peer approach. Thus, each PBS NE forwards the signaling message to the next PBS NE when it receives the PBS NSLP message.

5.2. Authorization

The authorization component decides the granting of permission (amount of volume) for a flow. One of main objectives of this component is to detect and identify the attack. The authorization

component also decides the solution against an attack. There are three solutions: IPsec AH using symmetric cryptography algorithm, IPsec AH using public key cryptography algorithm, and changing the flow path. The details of the detection of and solution against the attack are described in Section 8.

5.3. Traffic Management

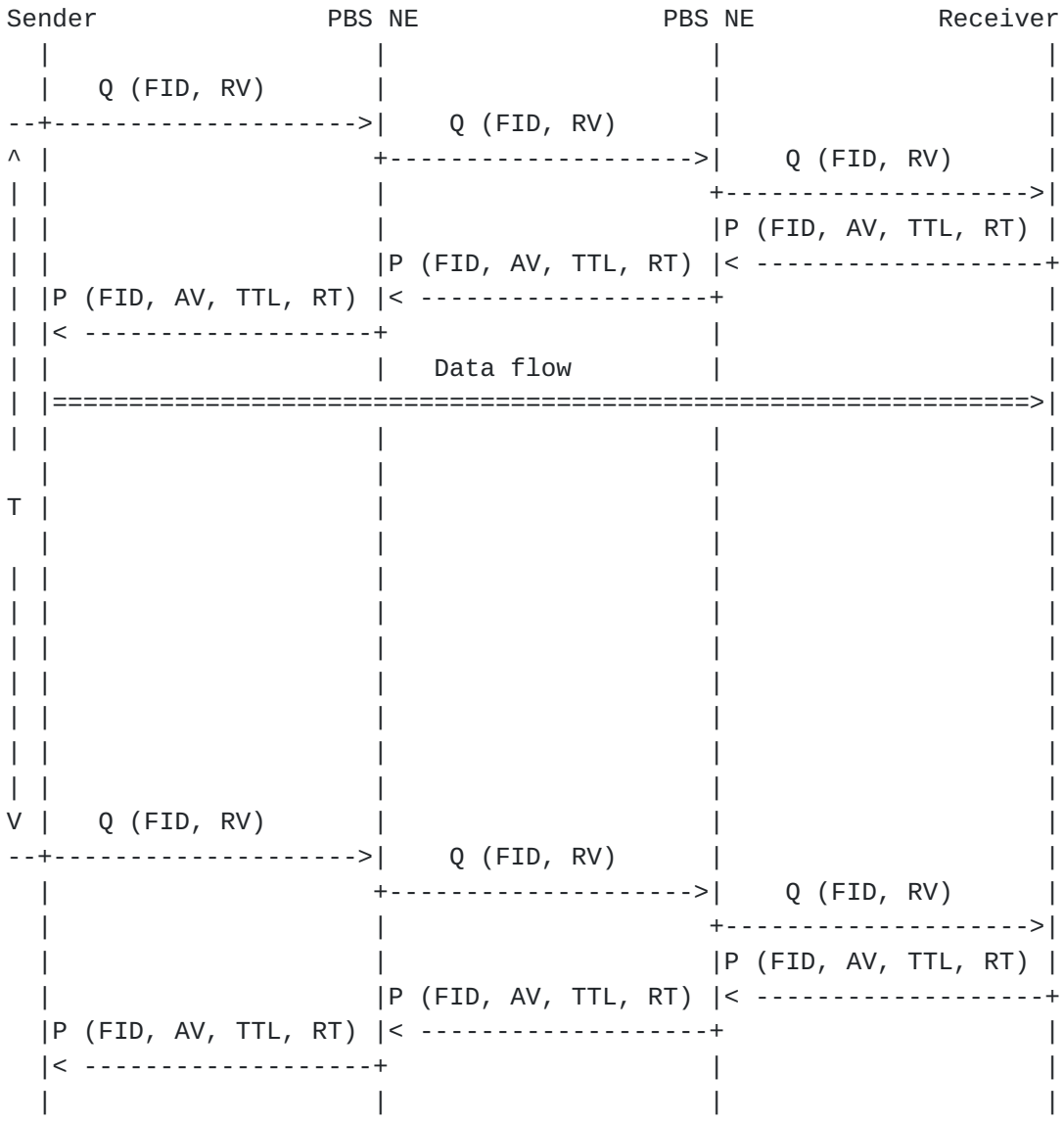
The traffic management component handles all incoming packets, including signaling messages and data packets. It passes signaling messages up to NTLP (GIST). Based on the permission state of flows, the traffic manager screens the data packets to see whether the data packets are authorized. An IP packet filter is used to filter the unauthorized packets. To see whether the flow exceeds the given permission, this component monitors the volume of the data flow that it has received since the permission state was set up. The authentication of packets is verified by this component.

6. PBS NSLP Operation

6.1. Basic Operation

PBS NSLP follows NSIS framework [RFC4080]. Thus, it works on top of the GIST (the implementation of the NTLP). There are two message types in the PBS NSLP, namely Query (Q) and Permission (P) messages. The Query message is sent by a sender to request permission to send data, specifying the volume of data. It contains the flow identification object, 5-tuple (source IP address, destination IP address, source port, destination port, and protocol identifier), describing a data flow. The Permission message is sent by the receiver who grants the permission to the sender along the reverse path of the Query message. The reverse path is set up by the GIST reverse routing state. The Permission message is used to set up (grant), remove (revoke) and modify permission state for a flow. The Permission message contains the flow identification, the allowed volume in bytes, the time limit for the permission, and the refresh time for soft-state. PBS NE stores this information to keep track of permission states. The delivery of signaling messages is performed hop-by-hop between the adjacent PBS NEs. The Query and Permission messages are periodically transmitted to establish soft-state that enables the detection of permission state and security algorithm changes.

Figure 2 shows how permissions are set up between a sender and a receiver. A sender sends a receiver a Query message to request a permission. The receiver returns a Permission messages to allow incoming data packets. After the permission state is set up between the sender and the receiver, the sender can send the allowed volume of data to the receiver during the time interval specified. The sender and receiver periodically sends Query and Permission messages after each soft-state period T.



FID : Flow identification
RV : The volume of data that the sender requests
AV : The volume of data that the receiver grants
TTL : Time limit for the permission
RT : Refresh time for soft-state

Figure 2: Basic operation of PBS NSLP

6.2. Asymmetric Operation

The PBS NSLP supports the asymmetric transmission of Query/Permission messages. After the permission state is set up, if the receiver wants to change the permission state or security algorithm, it sends the Permission message without receiving the Query message.

7. Security of Messages

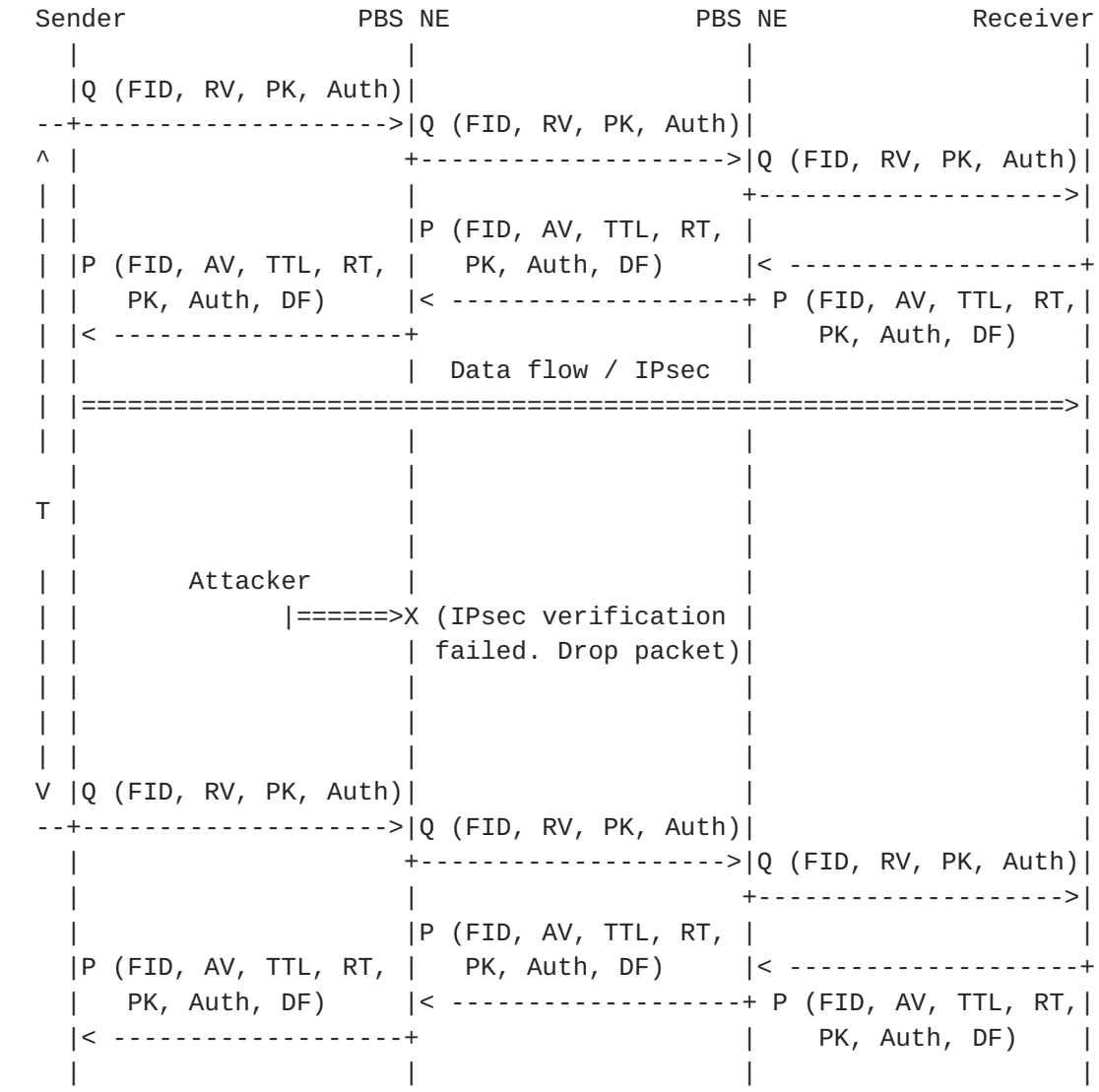
For secure permission state setup and management, PBS NSLP uses a public key cryptography mechanism for the authentication and integrity of signaling messages. Each sender and receiver generates a public/private key pair, and generates a digital signature by encrypting the objects of signaling messages using its own private key (i.e., the sender encrypts the objects of the Query message and the receiver encrypts the objects of the Permission message). Each public key in the form of the X.509 certificate [RFC5280], which is certified by a certificate authority, is distributed by a signaling message to the PBS NEs. The certificate is used to bind a public key and a user name (which includes the common name, an email address and an IP address). The Query message carries the sender's public key and the Permission message carries the receiver's public key. To validate the authentication and integrity of the signaling messages, each PBS NE decrypts the digital signature using the distributed public key. The sequence number of the PBS NSLP message is used to prevent replay attacks.

For the authentication and integrity of data packets, the IPsec Authentication Header (AH) is used. The Permission message carries the shared key and security parameter index (SPI), which are generated by the receiver and will be used for IPsec. When each PBS NE receives the Permission message, it stores the shared key and installs the security association (SA). For each flow, the SA has field values for destination IP address, IPsec protocol (AH or ESP) and SPI. To securely deliver the key and SPI value, channel security (TLS or DTLS) is used between adjacent PBS NEs. PBS NSLP functionality allows PBS NEs to validate the IPsec header that uses transport mode between the two end hosts (sender and receiver) using the shared key.

For the authentication data field in IPsec AH, the sender uses symmetric key cryptography or public key cryptography. In symmetric key cryptography, the shared symmetric key that is delivered in the Permission message is used for the encryption. The public key cryptography method entails using the sender's private key for encryption. The receiver has the right to choose a cryptography algorithm for IPsec based on the policy, network and applications, and this notification is carried in the Permission message.

Figure 3 shows the secure two-way handshakes for permission state setup and how PBS NSLP can prevent attack flows. The authentication field is encrypted by one's private key. The defense object (DF) has the indicated solution against the attack, the cryptographic algorithm for the IPsec authentication field, a shared key, and SPI value. Since the attacker does not have the shared key, the attack

flow failed during IPsec verification.



FID : Flow identification
RV : The volume of data that the sender requests
AV : The volume of data that the receiver grants
TTL : Time limit for the permission
RT : Refresh time for soft-state
PK : The certificate of a public key
Auth : The authentication field
DF : Defense object

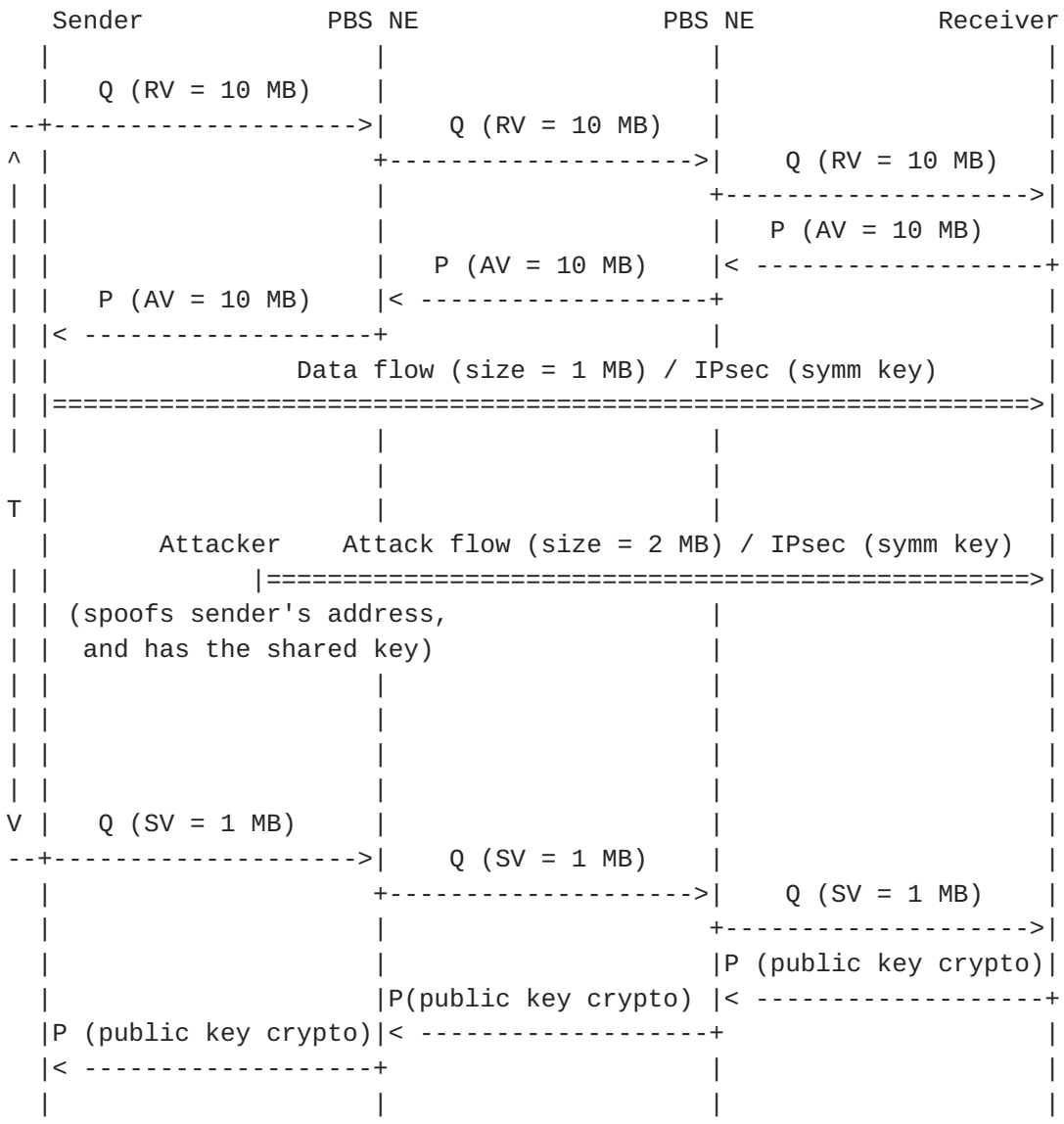
Figure 3: Basic operation of prevention

8. PBS Detection Algorithm (PDA)

Routers that do not have PBS functionality cannot generate bogus data packets because they do not have the shared key. A compromised PBS NE that knows the shared key, however, can generate and insert attack packets when symmetric key cryptography is used in IPsec AH. Furthermore, an off-path attacker (i.e., external attacker) might obtain the shared key by controlling compromised PBS NEs. In addition, compromised routers, which may or may not be PBS NEs, can drop legitimate packets. To prevent these attacks in this Byzantine network, PBS NSLP requires monitoring of network traffic and detecting attacks. The detection algorithm is called the PBS Detection Algorithm (PDA). PDA uses a soft-state mechanism of PBS NSLP, where a sender periodically sends the Query message that contains the volume of data it has sent after permission was granted. The receiver compares the volume of data in the signaling message with the volume of data that has been received. If they differ, the receiver suspects that there is an attack. Based on the detection, a receiver requests the senders to respond to the attack (using methods like changing the encryption algorithm or changing the path) using the indication in the Permission message.

8.1. Basic Operation of PDA

Figure 4 shows the example of the PDA basic operation. The first two signaling messages (Query and Permission messages) are used to set up the permission state for a flow between the sender and the receiver. We assume that the receiver grants permission to the sender to send a flow of size 10 MB. After setting up the permission state, the sender sends data packets whose total volume is 1 MB. There is an attacker A who spoofs the sender's address and has the shared key, and it sends additional attack packets whose total volume is 2 MB with the correct IPsec header. After the soft-state period T, the sender sends a Query message indicating that it has sent 1 MB of data. The receiver can detect the attack by comparing the volume (1 MB) in the Query message and total volume of data (3 MB) that it has received. After the receiver detects the attack, it sends the Permission messages with an indication to use public key cryptography to generate the authentication field of IPsec header. After that, the attack packets are dropped at a PBS NE because of the IPsec verification failure.



RV : The volume of data that the sender requests
AV : The volume of data that the receiver grants
SV : The volume of data that the sender has sent

Figure 4: Basic operation of PBS detection algorithm (PDA)

8.2. Example of Detecting a Packet Drop Attack (Black Hole Attack)

Drop attack is one of the on-path attacks. It is also known as the black hole attack. A compromised router drops all packets (including signaling messages) or selected packets (e.g., every n packets). PDA can detect the packet dropping attacks by a compromised router.

8.2.1. Drop All Packets

As shown in Figure 5, when a compromised router drops all packets, since the sender does not receive a Permission message after two tries, the sender suspects that the packets have been dropped. Therefore, the sender changes the path. To change the path, the sender can use a relay node used for tunneling or path diversity by multihoming.

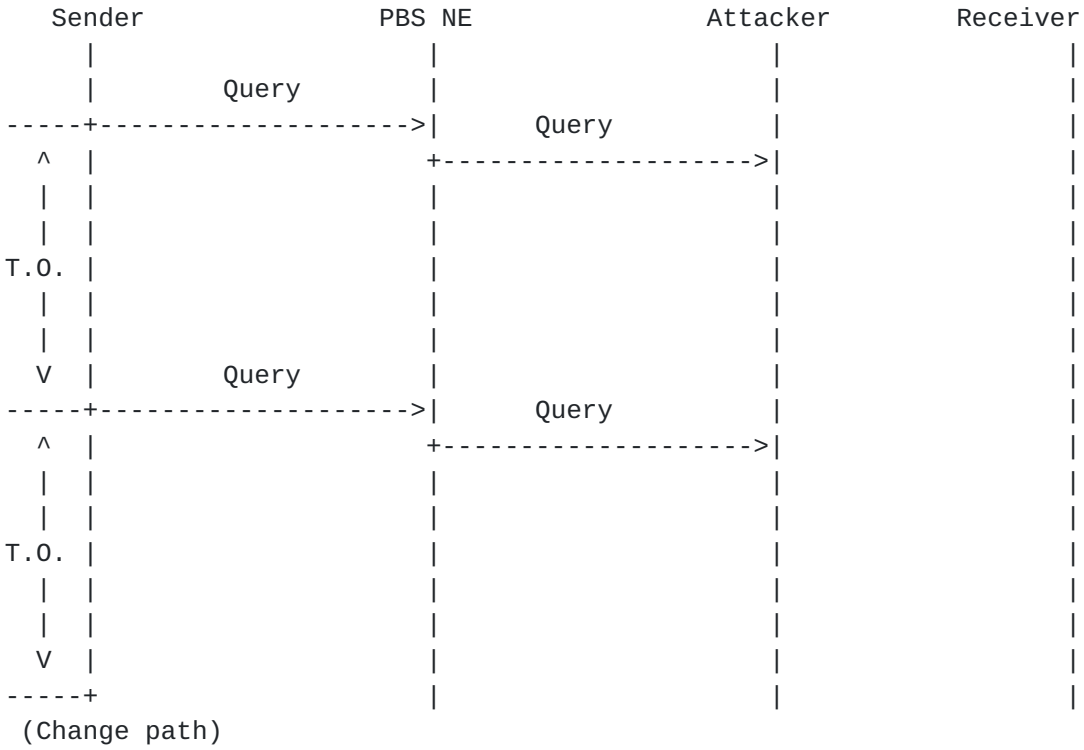


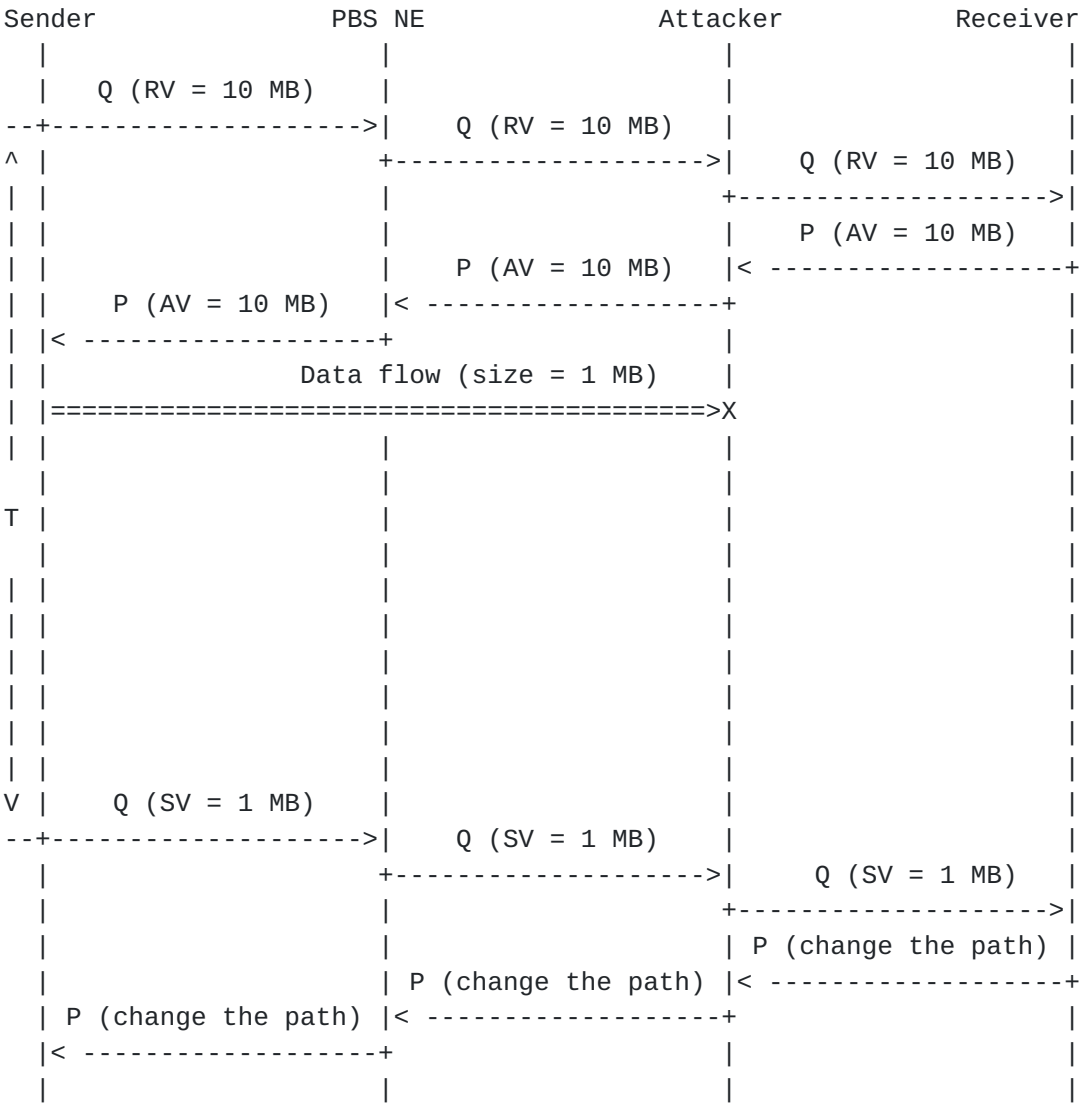
Figure 5: Drop all packets (signal and data packets)

8.2.2. Drop Selected Packets (Drop Only Data Packets)

As shown in Figure 6, when a compromised router drops some data packets, the amount of volume (0 byte in the figure) that the receiver has received and the volume information (1 MB) in the Query message differ, so the receiver suspects that packets have been dropped and sends a Permission message indicating a request to change path.

Data packet loss due to natural causes is also possible, and this is not an attack. Because of PDA, the natural packet loss might be regarded as a dropping attack. To avoid this, we apply a threshold-based decision scheme. If the difference between the amount of delivered packets and the volume information in the Query message is within a defined threshold, this is not regarded as a dropping

attack. The threshold value can be defined by the receiver based on the network environment. PDA can also detect the heavy congestion link where there is significant packet loss.



RV : The volume of data that the sender requests
AV : The volume of data that the receiver grants
SV : The volume of data that the sender has sent

Figure 6: Drop only data packets

9. PBS NSLP Messages Format

A PBS NSLP message consists of a common header and type-length-value (TLV) objects.

9.1. Common Header

All PBS NSLP messages carry a common header. The Figure 7 shows the common header format.

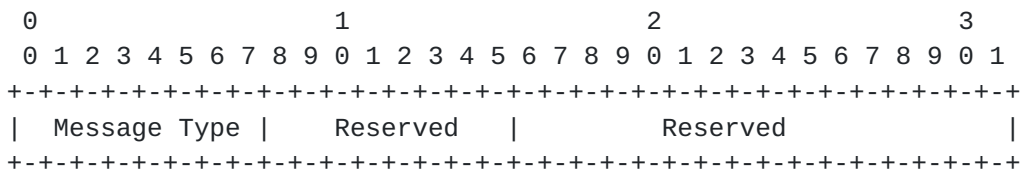


Figure 7: Common PBS NSLP Header

The fields in the common header are the following.

Message type (8 bits):

- 1=Query
- 2=Permission

9.2. Message Formats

9.2.1. Query

Query message is used to request permission and monitor traffic flow.

Query = Common Header / Flow Identification / Message Sequence Number / Requested Volume / Sent Volume / Public Key Certificate / Authentication Data

9.2.2. Permission

Permission message is used to set up, remove, and modify permission state for a flow.

Permission = Common Header / Flow Identification / Message Sequence Number / Allowed Volume / TTL / Refresh Time / Public Key Certificate / Defense / Authentication Data

9.3. Object Format

PBS NSLP objects begin with the common object header. The Figure 8 shows the common object header format.

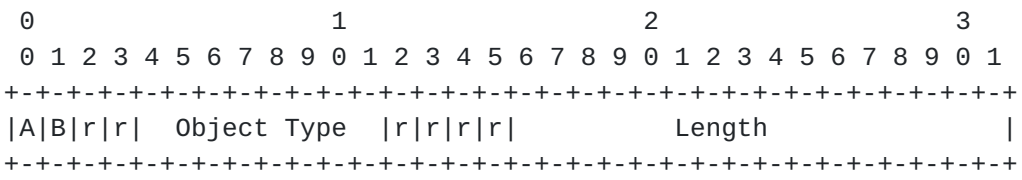


Figure 8: Common Object Header

Object Type (8 bits): The type of the object.

AB=00 ("Mandatory"): If the object is not understood, the entire message containing it MUST be rejected, and an error message sent back.

AB=01 ("Ignore"): If the object is not understood, it MUST be deleted and the rest of the message processed as usual.

AB=10 ("Forward"): If the object is not understood, it MUST be retained unchanged in any message forwarded as a result of message processing, but not stored locally.

Length (16 bits): The byte length of the object.

9.4. PBS NSLP Objects

9.4.1. Flow Identification (FID)

Type: FID

Length: Variable

Version (4 bits): IP address version (version 4 or 6).

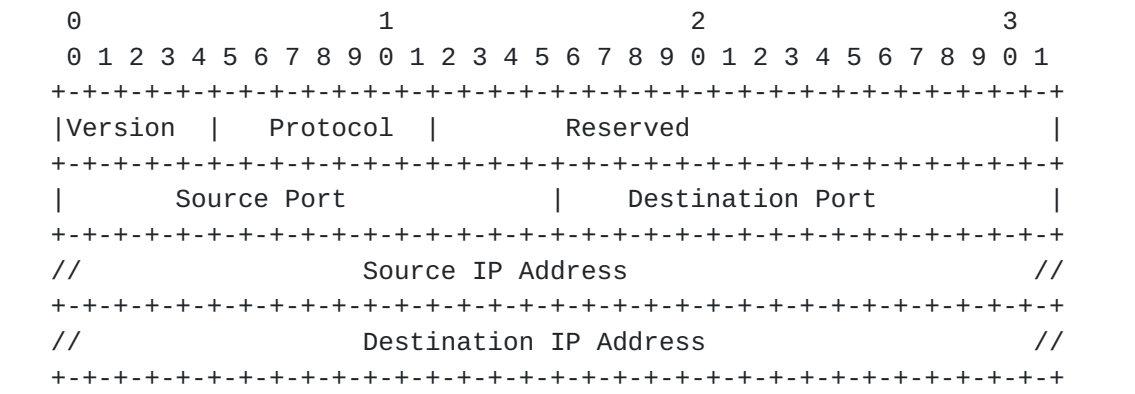
Protocol (8 bits): Protocol identifier.

Source Port (16 bits): The port number of the sender.

Destination Port (16 bits): The port number of the intended receiver.

Source IP Address (variable): IP address of the sender.

Destination IP Address (variable): IP address of the intended receiver.

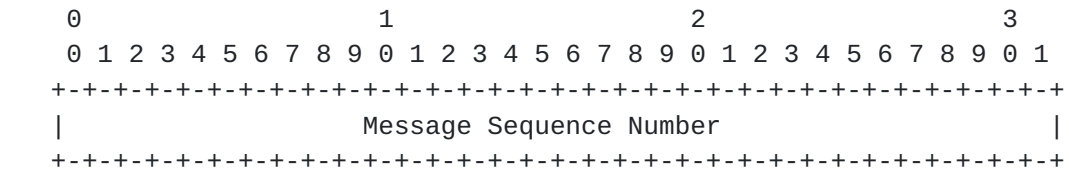


9.4.2. Message Sequence Number

Type: Message-Seq

Length: 32 bits

Value: An incrementing sequence number. Used to prevent a replay attack.

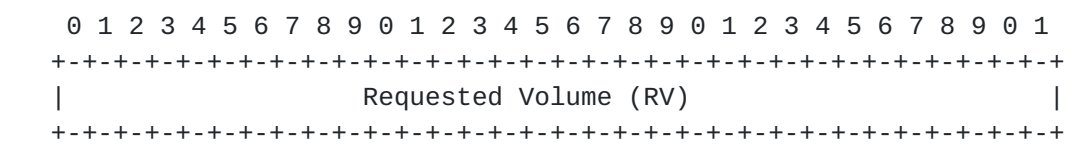


9.4.3. Requested Volume (RV)

Type: Req-vol

Length: 32 bits

Value: The number of bytes that a sender requests for a flow.



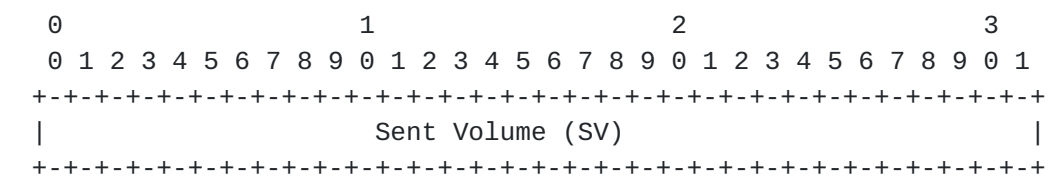
9.4.4. Sent Volume (SV)

Type: Send-vol

Length: 32 bits

Value: The number of bytes that a sender has sent since the sender

received the permission.

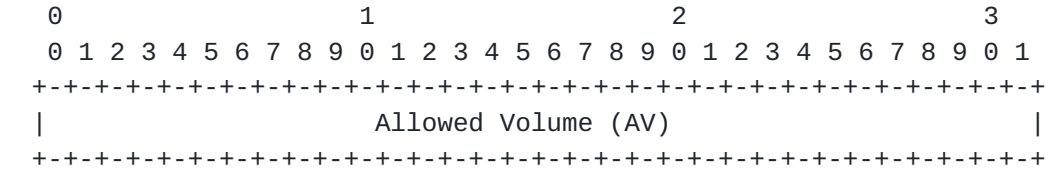


9.4.5. Allowed Volume (AV)

Type: Allow-vol

Length: 32 bits

Value: The number of bytes that a receiver allows for a flow.

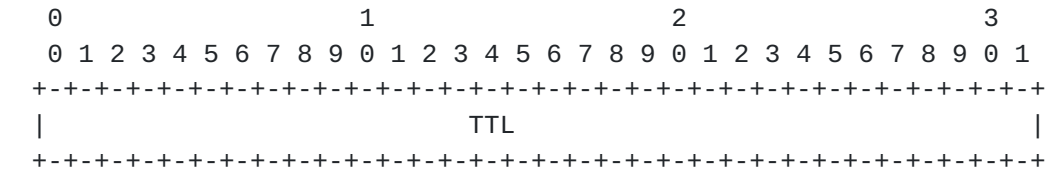


9.4.6. TTL

Type: TTL

Length: 32 bits

Value: The time limit for the permission state of a flow.

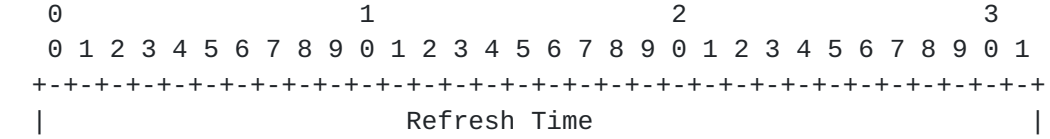


9.4.7. Refresh Time

Type: Refresh

Length: 32 bits

Value: The period for the soft-state.

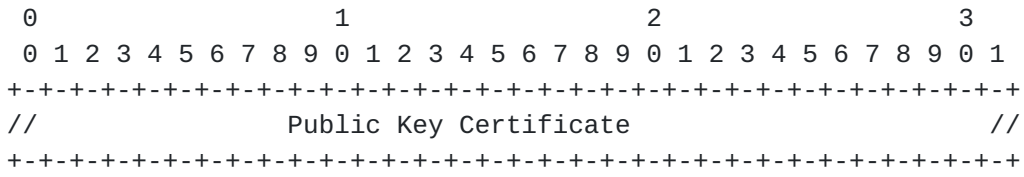


9.4.8. Public Key Certificate

Type: PK-cert

Length: Variable

Value: The X.509 certificate of a node's public key.



9.4.9. Defense

Type: Defense

Length: Variable

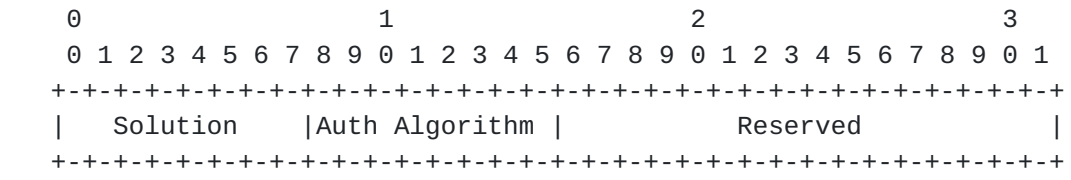
Solution (8 bits): The indicated solution against an attack.

- 1=No action
- 2=IPsec with symmetric key cryptography for a flow
- 3=IPsec with public key cryptography for a flow
- 4=Change the path to avoid the compromised router

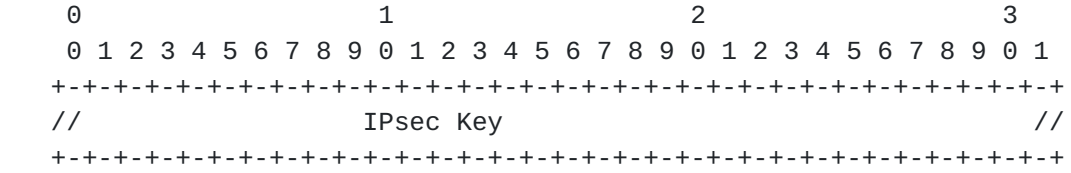
IPsec authentication algorithm (8 bits): The cryptography algorithm for the IPsec authentication field.

- 1=HMAC-SHA1
- 2=HMAC-SHA-256
- 3=HMAC-MD5
- 4=RSA-1024
- 5=RSA-2048
- 6=ECC-160

- 7=ECC-224
- 8=DSA-1024
- 9=DSA-2048
- 10=Algorithm from X.509 certificate



IPsec key (variable): The key for the IPsec authentication field.

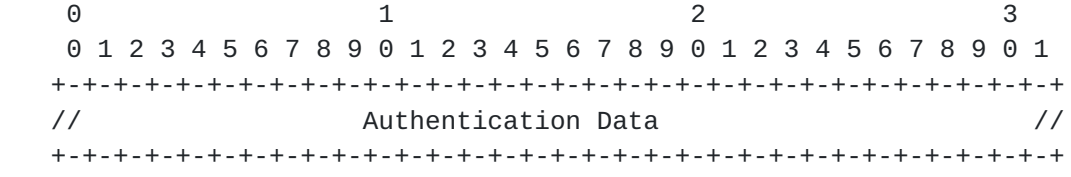


9.4.10. Authentication Data

Type: Auth-data

Length: Variable

Value: The encrypted data of message fields for authentication and integrity. Public key is used for the encryption.



10. Security Considerations

This document describes how to authorize the network traffic between a sender and a receiver along the data path. The authorization is controlled by a receiver by granting the permission to a sender. To prevent spoofing of the legitimate sender's address, IPsec AH is used for data packets.

There are two IPsec headers; the Authentication Header (AH) and Encapsulating Security Payload (ESP). IPsec ESP [RFC4303] can also be used for authentication. However, IPsec AH [RFC4302] suffices the authentication of packets.

The Cryptographically Generated Addresses (CGA) [RFC3972] can work with IPv6 to bind an IPv6 address and a public key, instead of a public key certificate, but cannot work with IPv4.

An attacker can send a lot of signaling messages to make the PBS NE incur computational overhead to validate them. To resolve this problem, PBS NSLP can use a puzzle-based mechanism for per-computation fairness. Since a sender has to spend its CPU time to solve a puzzle before requesting permission, it can provide fairness.

11. Acknowledgements

This work was supported by InterDigital Communications, LLC. The authors would like to thank Swen Weiland for his help in implementing the PBS NSLP.

12. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4080] Hancock, R., Karagiannis, G., Loughney, J., and S. Van den Bosch, "Next Steps in Signaling (NSIS): Framework", RFC 4080, June 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5971] Schulzrinne, H. and R. Hancock, "GIST: General Internet Signalling Transport", RFC 5971, October 2010.

Authors' Addresses

Se Gi Hong
Hughes Network Systems
11717 Exploration Lane
Germantown, MD 20876
US

Email: segi.hong@hughes.com

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Email: hgs@cs.columbia.edu