Network Working Group   Baiju Patel
INTERNET-DRAFT   Intel
Category: Standards Track   Bernard Aboba
<draft-ietf-pppext-l2tp-security-05.txt>   William Dixon
October 1999   Glen Zorn
                                                          Microsoft

Securing L2TP using IPSEC

Status of this Memo

Copyright Notice

Abstract

This document discusses how L2TP may utilize IPSEC to provide for tunnel
authentication, privacy, and integrity and replay protection. Both the
voluntary and compulsory tunneling cases are discussed.

Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional",
"recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as
described in [2].

Terminology

Voluntary Tunneling
          In voluntary tunneling, a tunnel is created by the user,
          typically via use of a tunneling client. As a result, the
          client will send L2TP packets to the NAS which will forward
          them on to the LNS. In voluntary tunneling, the NAS does not
          need to support L2TP, and the LAC resides on the same machine
          as the remote PPP peer.

Compulsory Tunneling
          In compulsory tunneling, a tunnel is created without any
          action from the user and without allowing the user any choice.
          As a result, the user will send PPP packets to the NAS/LAC,
          which will encapsulate them in L2TP and tunnel them to the
          LNS. In the compulsory tunneling case, the NAS/LAC must be
          L2TP capable.

[1]. Introduction

L2TP, described in [1], is a protocol that tunnels PPP traffic over
variety of networks (e.g., IP, SONET, ATM). Since the protocol
encapsulates PPP, L2TP inherits PPP authentication, as well as the PPP
Encryption Control Protocol (ECP) [10], and the Compression Control
Protocol (CCP) [9]. L2TP also includes support for tunnel
authentication, which can be used to mutually authenticate the tunnel
endpoints. However, L2TP does not define tunnel protection mechanisms.

IPSEC is a protocol suite defined by IETF working group on IP security
to secure communication at the network layer between communicating
peers. This protocol is comprised of IP Security Architecture document
[6], the Internet key exchange (IKE) [7], the IP authentication header
(AH) [3] and the IP encapulating security payload (ESP) [4]. IKE is the
key management protocol while AH and ESP are used to protect IP traffic.

This draft proposes use of the IPSEC protocol suite for protecting L2TP
traffic over IP and on-IP networks, and discusses how IPSEC and L2TP
should be used together. This document does not attempt to standardize
end-to-end security. When end-to-end security is required, it is
recommended that additional security mechanisms (such as IPSEC or TLS)
be used inside the tunnel, in addition to L2TP tunnel security.

[2]. L2TP security requirements

L2TP tunnels PPP traffic over both IP and non-IP public networks.
Therefore, both the control and data packets of L2TP protocol are
vulnerable to attack. Examples of attacks include:

[1]. **The adversary may try to discover user identities by snooping data** packets.

[2]. **The adversary may try to modify packets (both control and data).**

[3]. **The adversary may try to hijack the L2TP tunnel or the PPP connection** inside the tunnel.

[4]. **An adversary can launch denial of service attacks by terminating PPP** connections, or L2TP tunnels.

[5]. **An adversary may attempt to disrupt the PPP ECP negotiation in order** to weaken or remove confidentiality protection. Alternatively, an adversary may wish to disrupt the PPP LCP authentication negotiation so as to weaken the PPP authentication process or gain access to user passwords.

To address these threats, the L2TP security protocol MUST be able to provide authentication, integrity and replay protection for control packets. In addition, it SHOULD be able to protect confidentiality of control packets. It MUST be able to provide integrity and replay protection of data packets, and MAY be able to protect confidentiality of data packets. An L2TP security protocol MUST also provide a scalable approach to key management.

The L2TP protocol, and PPP authentication and encryption do not meet the security requirements for L2TP. L2TP authentication typically mutually authenticates LAC to LNS at tunnel origination and may periodically re-authenticate. Therefore, it does not protect control and data traffic on a per packet basis. Thus, L2TP tunnel authentication leaves the L2TP tunnel vulnerable to attack. PPP authenticates the client to the LNS, but also does not provide per-packet authentication, integrity, or replay protection. PPP encryption meets confidentiality requirements for PPP traffic but does not address the authentication, integrity and key management requirements. In addition, PPP ECP negotiation, outlined in [10] does not provide for a protected ciphersuite negotiation. Therefore, PPP encryption provides a weak security solution, and in addition does not assist in securing L2TP control channel.

Key management facilities are not provided by the L2TP protocol. However, where L2TP tunnel authentication is desired, it is necessary to distribute tunnel passwords.

Note that several of the attacks outlined above can be carried out on PPP packets sent over the link between the remote PPP peer and the NAS/LAC, prior to encapsulation of the packets within an L2TP tunnel. While strictly speaking these attacks are outside the scope of L2TP security, in order to protect against them, the PPP peer SHOULD provide

for confidentiality, authentication and integrity protection for PPP
packets sent over the dial-up link. Authentication and integrity
protection are not currently supported by PPP encryption methods,
described in [11]-[13].

2.1. L2TP Security Protocol

The L2TP security protocol MUST provide authentication, integrity and
replay protection for control packets. In addition, it SHOULD protect
confidentiality of control packets. It MUST provide integrity and
replay protection of data packets, and MAY protect confidentiality of
data packets. An L2TP security protocol MUST also provide a scalable
approach to key management.

To meet the above requirements, all L2TP security compliant
implementations MUST implement IPSEC ESP for securing L2TP control
packets and SHOULD implement IPSEC ESP for protection of L2TP data
packets. All mandated cipher suites, including NULL encryption, of
IPSEC ESP MUST be supported. Note that if confidentiality is not
required (e.g., L2TP data traffic), ESP with NULL encryption may be
used. The implementations MUST implement replay protection mechanisms
of IPSEC.

L2TP security MUST meet the key management requirements of the IPSEC
protocol suite. IKE SHOULD be supported for authentication, security
association negotiation, and key management using the IPSEC DOI [5].

2.2. Stateless compression and encryption

Stateless encryption and/or compression is highly desirable when L2TP is
run over IP. Since L2TP is a connection-oriented protocol, use of
stateful compression/encryption is feasible, but when run over IP, this
is not desirable. While providing better compression, and somewhat more
secure encryption, when used without an underlying reliable delivery
mechanism stateful methods magnify packet losses, and thus are
problematic when used over the Internet where packet loss can be
significant. In addition, although L2TP is connection oriented, the
L2TP specification [1] does not mandate packet ordering, which can
create difficulties in implementation of stateful compression/encryption
schemes. However, these considerations are not as important when L2TP
is run over non-IP media such as ATM, X.25, or Frame Relay, since these
media guarantee ordering, and packet losses are typically low.

2.3. Implementation considerations for L2TP over Non-IP networks

L2TP requires that a non-IP network supports packet transport, so that
the non-IP network should be able to carry L2TP control and data
packets.

Since ESP functions are defined on the IP payload (excluding the IP
header), the presence of an IP header is not a requirement for use of
ESP. Therefore, L2TP implemented on non-IP networks MUST be able to
transport IPSEC ESP packets. The "next payload" field of the ESP header
MUST be set to the L2TP protocol number. IANA has assigned 115 as the
protocol number for L2TP.

IKE messages use UDP transport. Therefore, in order to be compliant
with the IKE protocol on non-IP media, the non-IP media (which is
capable of transporting packets) MUST support transport of UDP
datagrams. Since the IP header is not present in the UDP datagram over
non-IP media, the UDP checksum MUST be set to zero by the source and
ignored by the destination.

The exact mechanisms for enabling transport of ESP and UDP packets over
non-IP media MUST be addressed in appropriate standards for L2TP over
specific non-IP networks.

3. L2TP/IPSEC interoperability guidelines

The following guidelines are established to meet L2TP security
requirements using IPSEC in practical situations. Note that this section
is not a requirement for an implementation to be L2TP security
compliant. Its purpose to make the implementors aware of certain
efficiency and security considerations.

In the scenarios that follow, it is assumed that both L2TP clients and
servers are able to set and get the properties of IPSEC security
associations, as well as to influence the IPSEC security services
negotiated. Furthermore, it is assumed that L2TP clients and servers
are able to influence the negotiation process for PPP encryption and
compression.

3.1. Compulsory tunnel

In the case of a compulsory tunnel, the dial-in host will be sending PPP
packets to the LAC, and will typically not be aware that its packets are
being tunneled, nor that any security services are in place between the
LAC and LNS. From the point of view of the LNS, it will note arrival of
a PPP data packet encapsulated in L2TP, which is itself encapsulated in
an IP packet. Assuming that the LNS is able to retrieve the properties
of the Security Association set up between itself and the LAC, it will
have knowledge of the security services in place between the LAC and
itself. Thus in the compulsory tunneling case, the dial-in host and the
LNS have unequal knowledge of the security services in place between
them.

Since the LNS is capable of knowing whether confidentiality,
authentication, integrity and replay protection are in place between the
LAC and itself, it can use this knowledge in order to modify its
behavior during PPP ECP and CCP negotiation. For example, let us assume
that LNS confidentiality policy can be described by one of the following
terms: "Require Encryption," "Allow Encryption" or "Prohibit
Encryption". If IPSEC confidentiality services are in place, then an
LNS implementing a "Prohibit Encryption" policy will act as though the
policy had been violated. Similarly, an LNS implementing a "Require
Encryption" or "Allow Encryption" policy will act as though these
policies were satisfied, and would not mandate use of PPP encryption or
compression. Note however, that this is not the same as insisting that
PPP encryption and compression be turned off, since this decision will
depend on the policy of the dial-in host.

Since the dial-in host has no knowledge of the security services in
place between the LAC and the LNS, and since it may not trust the LAC or
the wire between itself and the LAC, the dial-in host might want to
ensure sufficient security through use of end-to-end IPSEC or PPP
encryption/compression between itself and the LNS.

A dial-in host wishing to ensure security services over the entire
travel path would not modify this behavior even if it had knowledge of
the security services in place between the LAC and the LNS. This is
because the dial-in host needs to negotiate confidentiality services
between itself and the LNS in order to provide privacy on the wire
between itself and the LAC. Similarly, the dial-in host needs to
negotiate end-to-end security between itself and the endstation in order
to ensure confidentiality on the portion of the path between the LNS and
the endstation.

Given that the dial-in host will typically not trust the LAC and will
negotiate confidentiality and compression services on its own, the LAC
may only wish to negotiate IPSEC ESP with null encryption (described in
[14]) with the LNS, and the LNS will request replay protection. This
will ensure that confidentiality and compression services will not be
duplicated over the path between the LAC and the LNS. This will
typically result in better scalability for the LAC, since encryption
will be handled by the dial-in host and the LNS.

The dial-in host can satisfy the need for confidentiality services in
one of two ways. If it knows that all endstations that it will
communicate with are IPSEC-capable (or if it refuses to talk to non-
IPSEC capable endstations), then it can refuse to negotiate PPP
encryption/compression and negotiate IPSEC ESP with the endstations
instead. If the host does not know that all endstations it will contact
are IPSEC-capable (the most likely case), then it will negotiate PPP
encryption/compression. This may result in duplicate

compression/encryption which can only be eliminated if PPP
compression/encryption can be turned off on a per-packet basis. Note
that since the LNS knows that the dial-in host's packets are being
tunneled but the dial-in host does not, the LNS can ensure that
stateless compression/encryption is used by offering stateless
compression/encryption methods if available in the ECP and CCP
negotiations.

3.2. Voluntary tunnel

In the case of a voluntary tunnel, the dial-in host will be sending L2TP
packets to the NAS, which will route them to the LNS. Over a dial-up
link, these L2TP packets will be encapsulated in IP and PPP. Assuming
that it is possible for the dial-in host to retrieve the properties of
the Security Association between itself and the LNS, the dial-in host
will have knowledge of any security services negotiated between itself
and the LNS. It will also have knowledge of PPP encryption/compression
services negotiated between itself and the NAS.

>From the LNS's point of view, it will note a PPP packet encapsulated in
L2TP, which is itself encapsulated in an IP frame. This situation is
identical to the compulsory tunneling case. Assuming that the LNS is
able to retrieve the properties of the Security Association set up
between itself and the dial-in host, it will have knowledge of the
security services in place between the dial-in user and itself. Thus in
the voluntary tunneling case, the dial-in host and the LNS have
symmetric knowledge of the security services in place between them.

Since the LNS is capable of knowing whether confidentiality,
authentication, integrity check and replay protection is in place
between the dial-in host and itself, it is able to use this knowledge to
modify its PPP ECP and CCP negotiation stance. If IPSEC confidentiality
is in place, the LNS can behave as though a "Require Encryption"
directive had been fulfilled, not mandating use of PPP encryption or
compression. Typically the LNS will not insist that PPP
encryption/compression be turned off, instead leaving this decision to
the dial-in host.

Since the dial-in host has knowledge of the security services in place
between itself and the LNS, it can act as though a "Require Encryption"
directive had been fulfilled if IPSEC ESP was already in place between
itself and the LNS. Thus, it can request that PPP encryption and
compression not be negotiated. Note that if IP compression services
cannot be negotiated, it will typically be desirable to turn off PPP
compression if no stateless method is available, due to the undesirable
effects of stateful PPP compression.

Thus in the voluntary tunneling case the dial-in host and LNS will
typically be able to avoid use of PPP encryption and compression,
negotiating IPSEC confidentiality, authentication, and integrity
protection services instead, as well as IP compression (if available).

This may result in duplicate encryption if the dial-in host is
communicating with an IPSEC-capable endstation. In order to avoid
duplicate encryption/compression, the dial-in host may open two tunnels
with the LNS, each using a seperate security association. One SA would
use ESP with null encryption or AH, while the other would negotiate
confidentiality/compression. Packets going to an IPSEC-capable
endstation would run over the ESP with null encryption security
association (and associated L2TP tunnel), and packets to a non-IPSEC
capable endstation would run over the other tunnel/SA. This
configuration would probably require host routes i (either dynamic or
static) to be installed on the dial-in host.

Also note that the dial-in host may wish to put confidentiality services
in place for non-tunneled packets travelling between itself and the NAS.
This will protect the dial-in user against eavesdropping on the wire
between itself and the NAS. As a result, it may wish to negotiate PPP
encryption and compression with the NAS. As in compulsory tunneling,
this will result in duplicate encryption and possibly compression unless
PPP compression/encryption can be turned off on a per-packet basis.

4. IKE negotiation of L2TP filters

When using IKE Identity Protect Mode (Main Mode then Quick Mode
exchanges), the IKE quick mode is used to negotiate an IPSEC security
association for the protocol and port combination about to be used by
L2TP. The 5-tuple filter specification is passed by the initiator
during either Quick Mode ID Payload.

L2TP implementations MAY use a dynamically assigned UDP source port, but
SHOULD use an initial destination port of 1701. L2TP implementations
MAY use UDP port 1701 as both source and destination port number.

When using pre-shared key authentication, a specific filter for each LAC
IP must be present for the LNS to accept incoming IKE L2TP SA requests.
Filter matching is most specific for the 5-tuple. When using
certificate authentication, an LNS can be configured to access
negotiations from any LAC. The LAC would request certificate
authentication in the first main mode packet. The LAC and LNS MAY use
IKE certificate request payloads (CRP) to agree on a certificate
credential to use.

Similarly, when certificate authentication is used an L2TP LAC doing
compulsory tunneling can be configured to initiate an IKE L2TP SA

request to any LNS. However when using pre-shared key authentication, a
specific filter for each destination IP must be present to initiate
outgoing IKE L2TP SA requests.

L2TP LACs SHOULD negotiate the IPSEC security association before sending
the first L2TP UDP packet in order to avoid a race condition between the
time that the LAC is capable of sending secured packets using the new
IPSEC SA, and the time that the LNS would receive the secured packet.
If the LNS is very busy, it may take some time before it can install the
new IPSEC security association into its inbound IPSEC packet processor.
Also, L2TP round trip tunnel negotiation time will be adversely affected
if this time also includes the IPSEC IKE negotiation time.

4.1. Voluntary Tunnels

LNS Filters (certificate authentication):

>From <LNS IP> to <Any IP>, protocol UDP, source port 1701, dest port Any
>From <Any IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701

LNS Filters (pre-shared key authentication):

>From <LNS IP> to <LAC IP>, protocol UDP, source port 1701, dest port Any
>From <LAC IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701

LAC Filters (any method):

>From <LAC IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701
>From <LNS IP> to <LAC IP>, protocol UDP, source port 1701, dest port Any

The LAC filter From <LNS IP> to <LAC IP> is needed to ensure that if the
LNS were to initiate rekey of quick mode first, thus proposing this
filter in the quick mode ID payload to the client, that the client would
accept it.

4.2. Compulsory Tunnels

LNS Filters (certificate authentication):

>From <LNS IP> to <Any IP>, protocol UDP, source port 1701, dest port Any
>From <Any IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701

LNS Filters (pre-shared key authentication):

>From <LNS IP> to <LAC IP>, protocol UDP, source port 1701, dest port Any
>From <LAC IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701

LAC Filters (certificate authentication):

>From <LAC IP> to <Any IP>, protocol UDP, source port Any, dest port 1701
>From <Any IP> to <LAC IP>, protocol UDP, source port 1701, dest port Any

LAC Filters (pre-shared key authentication):

>From <LAC IP> to <LNS IP>, protocol UDP, source port Any, dest port 1701
>From <LNS IP> to <LAC IP>, protocol UDP, source port 1701, dest port Any

4.3. Gateway-gateway filters

In the gateway-gateway case either side may initiate the tunnel so that
the filters are symmetric. Since in this case the tunnel endpoints are
typically known to each other beforehand, specific filters are used for
the endpoints, and so that they can be used with either pre-shared key
or certificate authentication.

Gateway Filters (any method):

1. From <GW1> IP to <GW2 IP>, protocol UDP, source port Any, dest port 1701
2. From <GW2> IP to <GW1 IP>, protocol UDP, source port Any, dest port 1701
3. From <GW1> IP to <GW2 IP>, protocol UDP, source port 1701, dest port Any
4. From <GW2> IP to <GW1 IP>, protocol UDP, source port 1701, dest port Any

Filters 1 and 2 handle outbound L2TP tunnel initiation traffic when the
source port is dynamically mapped and cause the destination to agree to
terminate an L2TP tunnel when the source initiates, so as to filter L2TP
clear text inbound. Filter 3 and 4 secure the outbound traffic from the
destination to the source when the source initiates with dynamically
assigned source port.

Note: An LNS which is terminating both voluntary tunnels (from Any
Source IP address) and gateway-gateway L2TP SA requests MAY use the same
filter to accept both voluntary client and gateway L2TP SA requests when
using certificate authentication and CRPs to negotiate specific
certificate credentials.

5. Security considerations

IPSEC IKE negotiation MUST negotiate an authentication method specified
in the IKE RFC 2409 [7].

When X.509 certificate authentication is chosen, the LNS is expected to
use an IKE Certificate Request Payload (CRP) to request from the client
a certificate issued by a particular certificate authority or may use
several CRPs if several certificate authorities are trusted and
configured in its IPSEC IKE authentication policy. The certificate
credentials provided by the L2TP client during the IKE negotiation MAY
be those of the machine or of the L2TP user. When the L2TP user

certificate is used, the client MUST ensure that only traffic from that
particular user is sent down the L2TP tunnel.

The LNS SHOULD be able to trust several certificate authorities in order
to allow tunnel client end-points to connect to it using their own
certificate credential from their chosen PKI. Client and server side
certificate revocation list checking MAY be enabled on a per-CA basis,
since differences in revocation list checking exist between different
PKI providers.

L2TP implementations MAY use dynamically assigned ports for both source
and destination ports only if security for each source and destination
port combinations can be successfully negotiated by IKE.

A single preshared key for all IKE authentication to an LNS SHOULD NOT
be used. IKE pre-shared authentication key values SHOULD be protected
in a manner similar to the password used by L2TP for tunnel
authentication.

6. Acknowledgements

Thanks to Gurdeep Singh Pall, David Eitelbach, Peter Ford, and Sanjay
Anand of Microsoft, John Richardson of Intel and Rob Adams of Cisco for
many useful discussions of this problem space.

7. References

[1] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G., and
     Palter, B., "Layer Two Tunneling Protocol L2TP", RFC 2661, August
     1999.

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

[3] Kent,S., Atkinson, R., "IP Authentication Header", RFC 2402,
     November 1998.

[4] Kent,S., Atkinson, R., "IP Encapsulating Security Payload (ESP)",
     RFC 2406, November 1998.

[5] Piper, D., "The Internet IP Security Domain of Interpretation of
     ISAKMP", RFC 2407, November 1998.

[6] Atkinson, R., Kent, S., "Security Architecture for the Internet
     Protocol", RFC 2401, November 1998.

[7] Harkins, D., Carrel, D., "The Internet Key Exchange (IKE)", RFC
     2409, November 1998.

[8] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)", STD 51,
     RFC 1661, July 1994.

[9] Rand, D., "The PPP Compression Control Protocol (CCP)", RFC 1962,
     June 1996.

[10] Meyer, G., "The PPP Encryption Control Protocol (ECP)", RFC 1968,
     June 1996.

[11] Sklower, K., Meyer, G., "The PPP DES Encryption Protocol (DESE)",
     RFC 1969, June 1996.

[12] Sklower, K., Meyer, G., "The PPP DES Encryption Protocol, Version 2
     (DESE-bis)", RFC 2419, September 1998.

[13] Hummert, K., "The PPP Triple-DES Encryption Protocol (3DESE)", RFC
     2420, September 1998.

[14] Glenn, R., Kent, S., "The NULL Encryption Algorithm and Its Use
     With IPsec", RFC 2410, November 1998

8. Authors' Addresses

Baiju V. Patel
Intel Corp
2511 NE 25th Ave
Hillsboro, OR 97124

Phone: 503-264-2422
Email: baiju.v.patel@intel.com

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-936-6605
EMail: bernarda@microsoft.com

William Dixon
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-703-8729
EMail: wdixon@microsoft.com

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-703-1559
EMail: gwz@acm.org

9. Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any
intellectual property or other rights that might be claimed to pertain
to the implementation or use of the technology described in this
document or the extent to which any license under such rights might or
might not be available; neither does it represent that it has made any
effort to identify any such rights. Information on the IETF's
procedures with respect to rights in standards-track and standards-
related documentation can be found in BCP-11. Copies of claims of
rights made available for publication and any assurances of licenses to
be made available, or the result of an attempt made to obtain a general
license or permission for the use of such proprietary rights by
implementors or users of this specification can be obtained from the
IETF Secretariat.

The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary rights
which may cover technology that may be required to practice this
standard. Please address the information to the IETF Executive
Director.

10. Full Copyright Statement

11. Expiration Date

This memo is filed as <draft-ietf-pppext-l2tp-security-05.txt>, and
expires April 25, 2000.