Abstract

L2TP/IPsec is a secure VPN which tunnels Layer 2 packets. This protocol has been discussed and a solution has been proposed to create an L2TP/IPsec tunnel under FreeBSD. This research paper discusses how mobility support is added to the L2TP/IPsec tunnel. The new solution tunnels Layer 2 packets without incurring tunnel-re-establishment at handoff, without losing packets during handoff, achieves better security than current mobility solutions for VPN, and supports fast handoff in IPv4 networks. First, a general framework of the mobility solution is introduced, followed by details of the eight modifications required to achieve a fully working system. Finally, the analysis and discussion on the security and the performance of the new solution are provided.

Keywords: Authentication Header,ESP,IPSec,VPN, etc…

1. INTRODUCTION

The VPN protocols examined do not have a native ability to cope with mobile clients. Adding mobility support to existing VPN protocols is one way to solve the problem. A VPN that transfers Layer 2 packets will be chosen as it has a better range of applications and can transfer almost all kinds of Internet packets: IP packets, non-IP packets (such as IPX packets) and Layer 2 packets (such as PPP packets [11]). A brief comparison among different Layer 2 VPN is shown below.

- Layer 2 MPLS VPN has big security issues. It assumes that ISP network can be trusted and all the packets within ISP network are not encrypted
- OpenVPN is not widely used and is relatively weak in security.
- PPTP is weak in security and is patent encumbered. It is difficult to modify PPTP.
- L2TP provides Layer 2 tunneling functions and together with IPsec provides good security. Although L2TP/IPsec tunnels do not support NAT, IPv6 (next generation network) has an almost infinite number of addresses that makes NAT unnecessary.

The L2TP/IPsec tunnel has been chosen to add mobility support because it has a good range of applications (transferring Layer 2 packets) and is strong in security (using IPsec).

Layer 2 Tunneling Protocol (L2TP) is one of VPN protocols. It receives packets on the OSI Layer 2 (Data Link Layer) and secures the packets inside the OSI Layer 5 (Session Layer). It does not provide strong authentication method by itself and often the L2TP packets are sent inside IPsec for a better security. Compared with current VPN technologies, a VPN that transfers Layer 2 packets has a better range of applications as it can transfer almost all kinds of Internet packets: IP packets, non-IP packets (such as IPX packets) and Layer 2 packets (such as PPP packets).

Internet Protocol Security (IPsec) is one of the VPN technologies and is a suite of protocols. It receives packets on the OSI Layer 3 (IP Layer) and secures the packets inside the IP layer. IPsec uses Internet Key Exchange (IKE) protocol to generate security keys and to handle security key exchange between the VPN server and the VPN concentrator, and uses Authentication Header (AH) or Encapsulating Security Payload (ESP) to encrypt and to protect IP packets. IPsec has strong security and it has already been integrated into the next generation network (IPv6).

2. SOLUTION OVERVIEW

First, the real world problem will be analyzed with the topology as shown in Figure1. Consider several persons work together using a PPP network inside a moving vehicle, a L2TP/IPsec concentrator is used to encapsulate PPP packets and to tunnel to the remote server. When the vehicle moves, the public IP address of the L2TP/IPsec concentrator (Point D in Figure1) is changed. Point C is a loopback interface, and its IP address does not change. Other IP addresses inside the vehicle (Point A and B) are private IP addresses, which do not change even if persons move inside the vehicle.
vehicle. The IP addresses outside the vehicle (Point E, F, G and H) do not change, as they are fixed IP addresses. In summary, only the IP address of Point D is changed when the vehicle moves.

Figure 1: Loopback interface solution for IPSEC/L2TP Tunnel

The goal of this research paper is to add mobility support to existing L2TP/IPsec tunnel so that the tunnel can keep sending packets with low delay, without the cost of re-establishing the tunnel and without losing packets. The proposed solution is to let the tunnel concentrator communicate with tunnel server directly, without any home agent or foreign agent (like Mobile IP), without involving new headers. ESP is used to protect L2TP packets and to update IPsec information and the reasons will be explained in updating ip change information in ipsec. In order to increase the performance, the new solution only modifies the kernel part of IPsec because all the IPsec information for L2TP/IPsec mobility support (ESP, SPD and SADB) is inside the IPsec kernel. In order to reduce the communication between kernel and user space, and make debugging easier, most of the modifications are made to user space code of L2TP. This is because most L2TP tunnel information is saved under user space. The detailed procedure is described below.

1. The tunnel concentrator updates IPsec tunnel information and tells the tunnel server directly that its IP address is changed in IPsec from the old IP address to the new IP address.
2. The tunnel server confirms the IP change, updates IPsec tunnel information and sends back a confirming message.
3. The tunnel concentrator tells the tunnel server directly, with encryption, that the sequence number of the last data message received. In the ULP solution (see Section 6.4 for details), the IP change information under L2TP should also be sent in that message.
4. The tunnel server decrypts and verifies the packet. If the packet verification is successful, the tunnel server updates the tunnel information in L2TP, and sends a reply message indicating whether tunnel server has buffered enough packets and the sequence number of the last data message received.
5. The tunnel concentrator decrypts and verifies the reply packet. If either tunnel server or tunnel concentrator buffers not enough packets, the tunnel concentrator cuts off the user connection. If buffered enough packets, the tunnel concentrator updates the tunnel information in L2TP, sends the missing packets which do not reach tunnel server and asks the tunnel server to send the missing packets which do not reach tunnel concentrator.
6. The tunnel server sends the missing packets. Finally the VPN can resume operation with new data packets.

There are eight modifications to implement the mobility support.

2.1 Updating IP Change Information in IPSEC

For security reasons, IP change information must be encrypted and transferred to the other peer. It is best to add the information to ESP payload, not ISAKMP (Internet Security Association and Key Management Protocol) [9] or IKE (Internet Key Exchange). The reasons are as follows:

1. Avoid SA reestablishment. SA modification within ISAKMP is accomplished by creating a new SA deleting the old SA at any time after the new SA is established [9]. Sending information within the ESP payload can modify existing SAs instead of creating new ones.
2. Reduce the communication between kernel and user space under UNIX. ISAKMP and IKE messages are handled in user space while ESP and SA database are under UNIX kernel. Sending information within ISAKMP and updating SA database (SA database must be changed when handling IP change) needs communication between UNIX kernel and user space. Sending information within ESP and modifying SA database can eliminate the communication between kernel and user space.
3. ISAKMP is already obsolete in IKEv2. ESP packets are used to transfer IPsec address change information and two private NOTIFY message types (250 and 251) are written into the Next Header field in the ESP header to signal this activity. Other information, such as SPI, in the ESP header is the same as normal ESP headers in the old IPsec tunnel. In the IPSEC-ADDRESS-UPDATE...
(message type 250) packet, the ESP payload contains the IP addresses of the end points of the IPsec tunnel when setting up the tunnel and the current addresses. In the IPSEC-ADDRESS-REPLY (message type 251) packet, the ESP payload contains the same information as in the IPSEC-ADDRESS-UPDATE message and the action taken at VPN gateway, i.e. ADDRESS-UPDATE-SUCCEEDED. The encryption method has not changed in these ESP packets.

2.2 Updating IP change and data sequence number information in L2TP

Different L2TP information should be exchanged in different L2TP/IPsec tunnel implementations. In the loopback interface solution, the IP addresses of the L2TP tunnel (Point B, C, F and G in Figure 1) are not changed. Therefore, only the sequence number of the last data message received should be exchanged for re-transmitting lost packets. In the ULP solution, the external IP address of the L2TP tunnel concentrator (Point C in Figure 2) is changed. Therefore, both IP change information and the sequence number of the last data message received should be exchanged. The port number of L2TP tunnel is not changed in our situation. If the port number is changed then L2TP tunnel should be re-established.

![Figure 2: Figure 7-2 IPsec/L2TP Tunnel Topology in ULP solution](image)

The L2TP packet is situated inside the IPsec packet. IP change information is updated in IPsec first and then in L2TP. L2TP is responsible for flow control of the VPN tunnel. In the ULP(Upper and Lower Protocol) solution, an L2TP control packet with four AVPs (Attribute-Value Pair) is used for the notification message: L2TP-ADDRESS-UPDATE (Message Type 40), OLD-ENDPOINT-ADDRESS (Attribute Type 42), NEW-ENDPOINT-ADDRESS (Attribute Type 43), and LAST-DATA-NUMBER (Attribute Type 44). In the loopback interface solution, an L2TP control packet with two AVPs is used for the notification message: L2TP-SEQUENCE-UPDATE (Message Type 45) and LAST-DATA-NUMBER (Attribute Type 44).

In the ULP solution, an L2TP control packet is used with five AVPs (Attribute-Value Pair) for the reply message: L2TP-ADDRESS-UPDATE-REPLY (Message Type 46), OLD-ENDPOINT-ADDRESS (Attribute Type 42), NEW-ENDPOINT-ADDRESS (Attribute Type 43), ENOUGH-DATA-BUFFERED (Attribute Type 47) and LAST-DATA-NUMBER (Attribute Type 44). In the loopback interface solution, an L2TP control packet with three AVPs is used for the notification message: L2TP-SEQUENCE-REPLY (Message Type 48), ENOUGH-DATA-BUFFERED (Attribute Type 47) and LAST-DATA-NUMBER (Attribute Type 44).

2.3 Saving ip change information in L2TP and IPSEC

Both L2TP and IPsec information are saved in a list inside the memory (not a separate database). L2TP information is saved under user space while IPsec information is saved in the FreeBSD kernel. The IP addresses of the end points of IPsec tunnel when setting up the tunnel and the current addresses (mobile address) are saved in SA database in the IPsec kernel. Similar addresses are saved in the L2TP authentication database in the ULP solution. No modification is needed in the L2TP authentication database in the loopback interface solution. All the packets will be sent according to the new IP addresses. The old IP addresses are only used to identify the original connection.

2.4 Buffering lost packets

In the L2TP/IPsec tunnel, L2TP is responsible for tunnel and flow control, while IPsec is responsible for security only. The proposed solution requires a buffer function to be added to L2TP. Transmission Control Protocol (TCP) [7] is a good example for buffering and flow control and it is used as a reference for buffering packets in L2TP. The proposed solution has added a fixed size circular buffer to the L2TP tunnel. TCP requires the receiver to respond with an acknowledgment message as it receives the data. However, packet acknowledgment is not used in an L2TP tunnel because wireless network resources are very limited and packet acknowledgment requires too much network traffic (a response message has to be sent for every data message received) [7]. The size of the circular buffer must be negotiated...
in the setup phase of the L2TP tunnel. The size has been placed in the "Framing Capabilities" AVP in SCCR (Start-Control-Connection-Reply) and SCCRQ (Start-Control-Connection-Request) messages. The "Framing Capabilities" AVP is reserved for future use in L2TP specification [8].

A sequence number must be added to the L2TP data message to support lost packet transfer (retransfer packets that could not reach the old IP address). Sequence numbers are only optional in L2TP data message as described in L2TP specification [8]. Both the tunnel server and the tunnel concentrator buffer packets they sent, and save the sequence number of the last message they received. Therefore, decision of whether buffered enough packets can be made according to the following formula:

The sent buffer contains the packet with the sequence number: (the sequence number of the last message they received of the peer+1). If the sequence number of the last message they received of the peer equals to max sequence number size, the sent buffer should contains the packet with the sequence number 0.

2.5 Solving authentication problems

The proposed solution could not pass the old authentication of the L2TP/IPsec tunnel. The challenge here is to devise a new security system without adding new security vulnerabilities. There are two databases for security information in IPsec: SPD (security policy database) and SADB (security association database). SPD contains user information, such as the IP address of end users (addresses of Point A and F in Figure2, or addresses of Point A and H in Figure1). SADB contains connection and encryption information, such as the end points of IPsec tunnel (addresses of Point C and D in Figure2, or addresses of Point D and E in Figure1). The proposed solution only modifies the SA information (the IP address of Point C in Figure 2, or the IP address of Point D in Figure1). The following modifications have been made to IPsec authentication:

(1) When creating an SA (security association) in SADB, save the tunnel end point addresses as initial tunnel end point addresses and also as current addresses (mobile addresses).

(2) When an IPsec server or concentrator sends IPsec packets, the packets are sent to the mobile addresses of the tunnel. Initial tunnel end point addresses are only checked in IPsec update messages.

(3) When an IPsec server or concentrator receives IPsec packets, the packets are checked according to the mobile addresses of the tunnel.

(4) Before an IPsec server or concentrator sends the IPSEC-ADDRESS-UPDATE packets, the mobile addresses of the SA in SADB are updated. Otherwise, the IPSEC-ADDRESS-UPDATE packets may be sent from old tunnel end point addresses.

(5) When an IPsec server or concentrator receives an IPSEC-ADDRESS-UPDATE packet, the packet is decrypted according to SPI (normal IPsec packets are also decrypted according to SPI (Security Parameter Index)) and then is checked according to the content of the packet. If the packet is an IPSEC-ADDRESS-UPDATE packet and SA can be found according to initial tunnel end point addresses, update mobile addresses of the SA in SADB.

(6) SPD check does not change because the addresses in SPD are the addresses of end users (Point A and Point F in Figure 7-2, or Point A and Point H in Figure 7-1) and these addresses do not change in our solution.

No modification of L2TP authentication is needed in the loopback interface solution. The following modifications were made to L2TP authentication in the ULP solution:

(1) When creating an L2TP tunnel, save the tunnel end point addresses as initial tunnel end point addresses and also as current addresses (mobile addresses) in the L2TP connection list.

(2) For normal L2TP packets, verify that the IP addresses and port values in the L2TP packet match the saved mobile node addresses and port numbers.

(3) For L2TP address update messages, check the initial tunnel end points addresses and update mobile addresses in the L2TP connection list.

2.6 Updating Route Information

The routing table of the tunnel concentrator should be updated before the IPsec update message is sent. The routing table of the tunnel server should be updated after receiving the IPsec update message. If a network interface changes its IP address, all routes related to that interface will automatically be deleted under FreeBSD. A related route has to be added when an IP address is changed.

However, updating route information may not be necessary in an L2TP/IPsec mobility solution. It depends on how the tunnel concentrator gets a new IP address. The new IP address is got by using the "ifconfig" command. In this situation, all routes related to the IPsec external interface (Point D in Figure1) will be deleted and a new route to the tunnel concentrator has to be added by the L2TP/IPsec mobility solution. In experimentation on real devices, the new IP
address is got from a DHCP server [13]. DHCP servers usually assign an IP address and a default route to DHCP client. The default route will route all packets from DHCP client (the tunnel concentrator in the solution) to DHCP server when no other route exists for a given IP packet's destination address. In this case, tunnel packets will be routed to DHCP server and then to the tunnel server. Then, no route information needs to be updated in the experiment on real devices.

2.7 Detecting IP Change
Detecting IP change is a necessary part of any mobility support. This change can be detected by scanning the interface address periodically or by a system event which shows a possible IP change on the interface. FreeBSD will delete related routes when an interface changes its IP address. This event triggers the new system to detect the IP change and then to update the L2TP/IPsec tunnel. Another important note is that the new IP address must be a valid IP address. Otherwise, the L2TP/IPsec tunnel will become invalid on real network devices. Getting new IP addresses is not a part of this solution, but it is a necessary part of VPN handoff. Other software or systems should be used to get a new IP address when current Internet connection is lost. During handoff, tunnel packets will keep sending without reaching their destination. These packets will be buffered in L2TP side. When a new IP address is available, the novel solution will detect the IP change and handle the handoff.

2.8 Solving Synchronization problems
ESP and SADB are two entities which work together under the FreeBSD kernel. SA information in SADB should not change when handling ESP packets. When the tunnel concentrator changes its IP address and also updates SA information, it is possible to build an ESP packet with its old IP address in the ipsec4_precess_packet() function and send the packet to its new IP address in the ip_output() function. This synchronization problem occurs when the mobile node changes networks and if not properly handled may cause problems with IPsec or may cause an Intrusion Detection System to suspect that hacking is happening. A flag is added to the FreeBSD kernel to solve this problem. When the tunnel concentrator wants to update the SA information, it enables the flag so that all the tunnel traffic, except the update message itself, will be dropped in the ipsec4_preccess_packet() function. Lost packets are already buffered in L2TP. The tunnel concentrator then updates the SA information and sends the IPsec tunnel update message. After the tunnel concentrator receives the confirmation packet, the flag is disabled so that tunnel traffic will be encrypted and passed on.

3. SECURITY CONSIDERATIONS
On consideration, it appears that the new solution does not introduce any new security issues to the L2TP/IPsec tunnel as every packet is protected by IPsec during handoff. The solution adds IP change information to the ESP payload which is encrypted and could not be seen by other online users. These packets may be captured by someone to attempt a replay attack, however the sequence number defined in the ESP header will cause any replay to be ignored. The L2TP update messages are also protected by ESP and again sequence number checks on ESP packets stop any replay attack from being successful. The vulnerability of the solution to other attacks, such as Denial-of-Service (DoS) attacks, should be the same as the vulnerability in regular IPsec operations.

4. PERFORMANCE IMPLICATIONS
Here, the performance of the new approach is compared with that of "IPsec over Mobile IP" [5] first, then "mobility support for IPsec" [4], and then "IKEv2 Mobility and Multihoming Protocol" [12]. A detailed analysis will be shown in Section 8.4. L2TP is used to encapsulate Layer 2 packets and to provide Layer 2 tunneling functions [1,8]. L2TP traffic will not take into account in this comparison as other solutions do not provide Layer 2 tunneling function.

In the new solution, the traffic involved in the initial tunnel setup process is identical to the traffic of standard L2TP/IPsec tunnel. It is assumed that the mobile node does not handoff in the setup phase, a relatively uncommon occurrence. IPsec over Mobile IP solution is also able to handle the handoff but it needs to perform Mobile IP registration with UDP packets (at least 48 bytes) and typically adds one additional roundtrip for Mobile IP registration in setup. In IPv4, the negotiation between Home Agent and Foreign Agent is also needed.

In the process of transferring data, IPsec over Mobile IP solution has one more Mobile IP header (at least 26 bytes in IPv4 [10] and 6 bytes in IPv6 [3]) compared to the new approach. This traffic overhead is large especially when sending small packets. Also, the agent discovery packets in Mobile IP should be sent at least once a second [6]. This adds up to the traffic overhead particularly in a wireless system. In the process of handoff, IPsec over Mobile IP has to
use one roundtrip for Mobile IP update and six roundtrips for IPsec update [2]. However, the new solution uses only 1 round trip for IPsec information update.

In summary, the new solution has a smaller overhead and faster handoff than IPsec over Mobile IP by avoiding double tunneling and connection reestablishment. The above advantage will greatly increase the efficiency and performance especially in resource-constrained wireless networks where mobile nodes move frequently between networks. Compared with "mobility support for IPsec" [4] and "IKEv2 Mobility and Multihoming Protocol" [12], the new method has better performance. ESP packets are used to update IPsec information instead of ISAKMP or IKE packets. The new method avoids SA reestablishment and reduces the communication between kernel and user space.

5. CONCLUSION

A new and novel mobility support for the L2TP/IPsec tunnel has been proposed. The new solution tunnels Layer 2 packets without incurring tunnel-re-establishment at handoff, without losing packets during handoff, achieves better security than current mobility solutions for VPN, and supports fast handoff in IPv4 networks. The new solution is to let the tunnel concentrator communicate with the tunnel server directly, without any home agent or foreign agent, without involving new headers. The communication is protected by ESP which is strong in security. The implementation of this solution will have better performance. It only modifies the kernel part of IPsec, and most of the modifications under L2TP are made to user space code. Compared to other IPsec mobility solutions, the new solution has better performance and can tunnel Layer 2 packets while other solutions cannot. No packet loss on network transfer is another advantage that other solutions do not have.

References


AUTHOR

Sridevi, at present working at karnatak University, Dharwad,Karnataka state. And persuing part time Ph.D at Mangalore University, under the guidance of Dr.Manjaih.D.H. Her research areas are Computer Networks and Mobile Communication systems.