L2TPv3 协议安全性研究

赵蕾，马跃
北京邮电大学计算机科学与技术学院，北京 (100876)
E-mail：man998223@gmail.com

摘　要：研究了第二层隧道协议 L2TPv2 的工作原理，讨论了该协议的安全缺陷， 针对 L2TPv2 协议的安全漏洞，进而分析了 L2TPv3 协议的控制消息与数据消息关于安全性的改进，包括不定期认证、数据加密和完整性检查等，并通过试验示范了利用 L2TPv3 建立安全 VPDN 连接的过程。

关键词：隧道；L2TPv2；L2TPv3；安全性
中图分类号：TP393　　**文献标识码：**A

0．引言

随着现今社会经济的发展，各个公司都努力拓展业务，使得业务涉及的范围也越来越大。为了使得分支机构的员工共享公司内部信息，需要使公司网络覆盖到外地甚至国外。解决这些问题的一个办法是公司租用专用线路来通信，这种方式成本太高，并且企业还需购买专门的接入设备进行维护，这也增加了企业的管理负担。

在VPDN[1]的实现中，将使用廉价的Internet网取代专用线路，当外地用户需要访问企业内部资源时，只需要拨号到当地的ISP，然后由ISP使用VPDN设备将用户接入到企业内部网。这不仅为企业节省了费用而且还减轻了企业的管理负担。

VPDN主要使用的是隧道技术，其中，常用的隧道协议是L2TPv2[3]，最新的版本是L2TPv3[4]。

1．L2TPv2协议

1.1 工作原理

二层隧道协议L2TPv2是IETF吸纳了CISCO公司的二层转发协议L2F和Microsoft公司的点对点隧道协议PPTP的优点而制定的一个标准，它吸取了两者的优点[3]，其原理如图1所示。

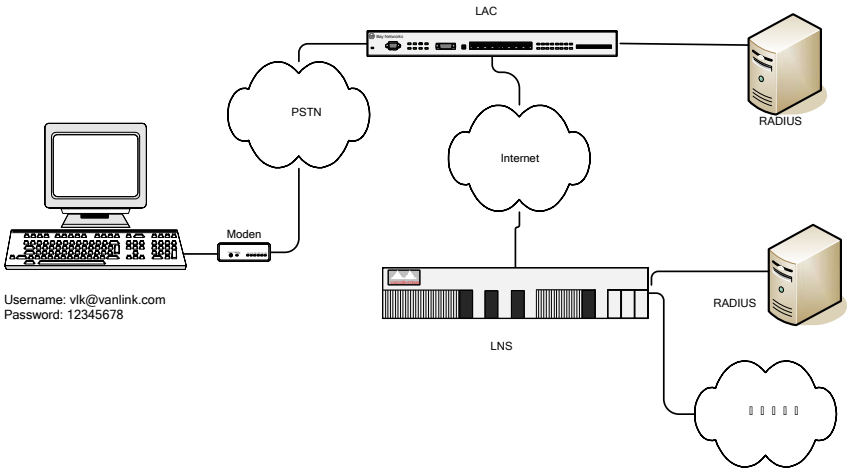

图 1 L2TPv2 原理图

在图1所示的拓扑中，L2TP系统是由L2TP接入集中器（LAC），L2TP网络服务器(LNS)

和远端拨号用户(RH)等三部分组成。其中，LAC一般在ISP端，LNS一般在企业内部网。

通常L2TPv2具有两种隧道类型：强制隧道和自愿隧道。在图1所示的强制隧道中，远端拨号用户通过PSTN连接到LAC，LAC通过拨号用户的电话号码，或者用户名的域名部分，确定要指向的LNS地址，并开始和对端的LNS协商建立隧道和会话。当隧道建立之后，LNS端可以继续和远端用户进行PPP层的协商和身份验证，当然LNS可以通过配置不再次进行验证。而在自愿隧道中，若没有RH，LAC直接通过隧道访问LNS，并通过LNS访问企业内部资源。

在LAC和LNS之间存在两种类型的连接，一种是隧道连接，它定义了一个LAC和LNS对，另一种是会话（session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个PPP会话过程。在一个隧道连接上可以承载多个会话连接，L2TP连接的维护以及PPP数据的传送都是通过L2TP消息的交换来完成的。

而L2TP消息可以分为控制消息和数据消息两种类型，控制消息用于隧道连接和会话连接的建立和维护，数据消息则用来承载用户的PPP会话数据包。控制消息中的参数用AVP属性值对（Attribute Value Pair）来表示，使得协议具有很好的扩展性，在控制消息的传输中还应用了滑动窗口机制，以实现控制消息的重传和拥塞控制。L2TP数据消息的传输不采用重传机制，所以它无法保证传输的可靠性，但这一点可以通过上层协议如TCP等得到保证，数据消息的传输可以根据应用的需要灵活地采用流控或非流控机制，甚至可以在传输过程中动态地使用消息序列号从而动态地激活消息顺序检测和流控功能。在采用流控的过程中，对于失序消息的处理采用了缓存重排序的方法来提高数据传输的有效性。

1.2 安全缺陷

L2TP协议的安全性依赖于：（1）PPP提供的认证，比如CHAP或者PAP认证；（2）L2TPv2本身提供的隧道验证和AVP隐藏。

在使用中，L2TPv2存在很多安全问题[1][2]：（1）隧道验证仅仅定义了对隧道终端实体的身份认证，而不是认证隧道中流过的每个报文，这样的隧道无法抵抗插入攻击和地址欺骗；（2）由于没有针对每个报文进行完整性校验，就有可能进行拒绝服务攻击（DOS），即发送一些假冒的控制信息，导致L2TPv2隧道或者底层PPP连接的关闭。（3）虽然PPP报文的数据可以加密，但PPP协议不支持密钥的自动产生和自动刷新，这样进行监听的攻击者就可能最终攻破密钥，从而得到所传的数据。

为了实现L2TP的安全性，现在多使用L2TPv2+IPSEC解决方案[5]，但是由于IPSEC在穿越NAT时有一定局限性，使得L2TP性能得到减弱。所以L2TP最好能独立于IPSEC，实现隧道的自身保护机制。而L2TPv3在很大程度上可以改进隧道的自身保护机制，提高了安全性。

2．L2TPv3协议的安全性分析

针对L2TPv2安全上的漏洞，IETF进而提出了L2TPv3[4]。L2TPv3和L2TPv2的不同之处主要在以下几点：

(1) 将和 PPP 相关的 AVP、以及包含在 L2TP 数据消息头部中的一些和 PPP 相关的域剥离掉；

(2) 将 Session ID 和 Tunnel ID 从以前的 16bit 变为了 32bit；

(3) 认证整个控制消息，而不是以前的只认证消息的一部分。

此外，L2TPv3可在隧道中转发PPP、HDLC、帧中继和以太网等第二层帧，而L2TPv2

只能通过隧道转发PPP帧。

有两种通过IP网络传输L2TPv3分组的方法：1）L2TPv3 over IP（使用IP协议ID115）；2）L2TPv3 over UDP（使用目标端口1701），L2TPv3 over IP的开销较低，但在L2TP隧道必须穿越网络地址转换（NAT）设备或防火墙的环境中，L2TPv3 over UDP就很有用。下文中，以L2TPv3 over UDP举例。

与L2TPv2中数据消息和控制消息使用相同的头部不同，L2TPv3中，数据消息和控制消息使用不同的头部格式[4]。以下将针对安全性，对这两种消息分别进行分析。

2.1 控制消息

L2TPv3 提供了对所有控制消息的认证和整体性检查。这一机制称为控制消息认证，它包括一种计算 L2TPv3 控制消息头和数据的 Hash 函数，一个预先配置的共享密码（shared_secret），以及一个本地(local_nonce)和远端的随机数(remote_nonce)。Hash 函数算出的结果封装在 Message Digest AVP 中。Message Digest AVP 的格式如图 2 所示：

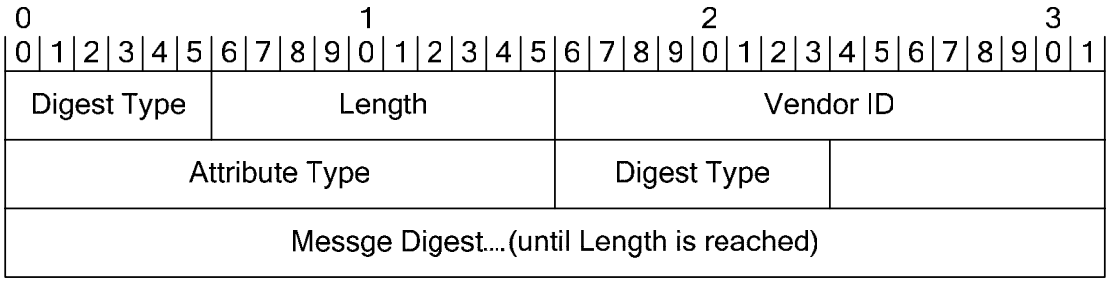

图 2 Message Digest AVP 格式

在 L2TPv3 中，发送方和接收方必须提前协商好用于认证的密码（shared_secret）。除了 SCCRQ 控制消息，其它控制消息的 Message Digest 计算方式为：1）shared_key=HMAC_MD5(shared_secret)；2)Message Digest = HMAC_Hash（shared_key,local_nonce+remote_nonce+control_message），其中，“+”表示串连。

当发送方发送控制消息时，用控制消息头和控制消息中所有的 AVPs，随机数（nonce）以及 shared_key 为输入，运算 hash 函数，产生一个 Message Digest AVP 添加到控制消息尾部。

当接收方收到控制消息后，运用相同的算法产生一个本地期望的摘要（digest），将收到消息的摘要（digest）和本地计算期望的摘要（digest）值相比较，如果不相等，则扔掉该控制消息。

L2TPv3 中的确认消息和 L2TPv2 的确认消息也不一样。L2TPv2 中 ZLB 消息仅仅包含了控制消息头，无法包含 Message Digest AVP 以进行认证。L2TPv3 中使用了带有 Message Digest AVP 的 Explicit-Acknowledgment 消息来取代了 ZLB 消息，换句话说，Explicit-Acknowledgment 是一种带认证的确认消息。

在 L2TPv2 中，如果攻击者（attaker）截获了 L2TPv2 数据包，并且获取了 L2TPv2 头部的一些标识，则攻击者可以伪装成 LAC 或者 LNS 向对端发送一些控制消息，在这里，拿 StopCCN 消息举例。为了发送 StopCCN 伪消息，攻击者必须构造 StopCCN 消息，因此，他需要获得源 IP 地址，猜测包含在 StopCCN 消息中的 Tunnel ID，Assigned ID 和 Ns。其中，Tunnel ID 和 Ns 都是 2 个 8bit 无符号整数。攻击者猜测 Tunnel ID，Assigned ID 和 Ns 组合，

则有 $2^{(16+16+16)}$ ＝281474976710656 种。在 100Mbps 的网络中，假设每个攻击包的大小是 320bits，则攻击者发送所有的组合，得需要 281474976710656*320/100Mbps≈29 年。

而由下图 3 所示的 L2TPv3 控制消息头格式可以看出，Control Connection ID 是 32 位的，Ns 是 16 位的，再加上 Digest 最长为 20 字节，三者的组合有 $2^{(32+16+20*8)}$ ≈4.11376*10^{62} 种，同样地，还是假设每个攻击包大小是 320bits，同时还是在 100Mbps 的网络中，则攻击者发送完所有组合，得需要 4.11376*10^{62} *320/100Mbps≈1.3*10^{57} seconds，约为 4.2*10^{49} 年。 因此我们可以说 L2TPv3 足以抵制破坏控制连接的假 StopCCN 消息。

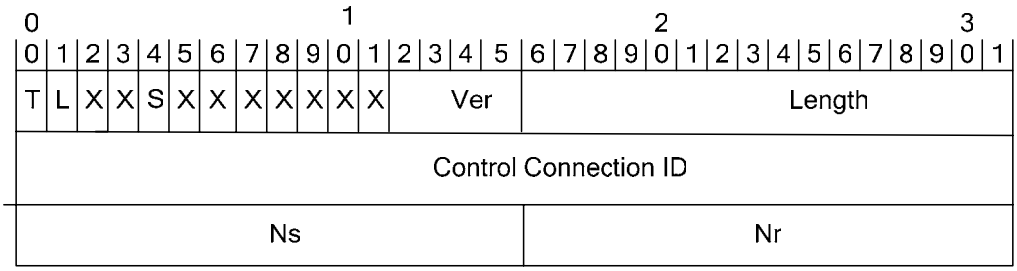

图 3 L2TPv3 控制消息头

2.2 数据消息

L2TPv3 的数据消息头格式如下图所示：

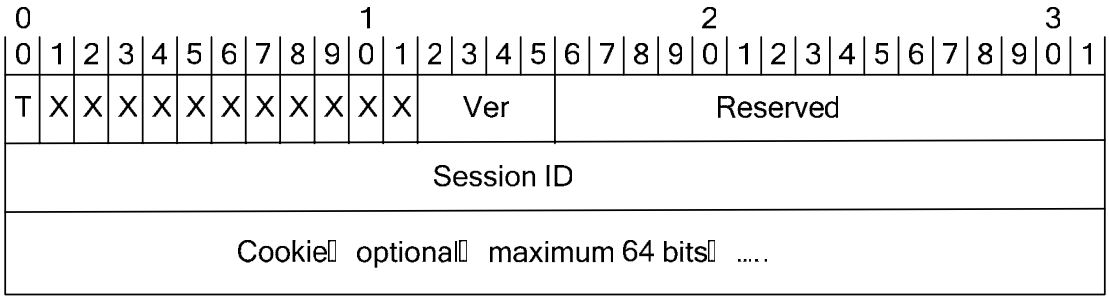

图 4 L2TPv3 数据消息头

其中，Cookie 值是可选的随机 Cookie 值，它是变长的，最长 64 位。该 Cookie 值可防范盲目插入攻击（blind insertion attack）。也就是说，如果攻击者不能窃取网络中传输的分组，将很难把分组插入到数据流中。这是因为很难猜测到正确的 Cookie 值，在最坏的情况下将会有 2^{16} 种不同的取值。

3．利用L2TPv3建立安全性VPDN连接的过程

L2TPv3 隧道模型有三种类型：1）LAC－LNS 隧道模型；2）LNS-LNS 隧道模型；3)LAC-LAC 隧道模型。以下以 LAC-LNS 隧道模型为例说明 L2TPv3 连接建立过程，其中 RADIUS 采用 Linux 下的 GUN RADIUS，L2TPv3 为 vanlink 公司自主研发的路由器，在试验中，启用 L2TPv3 的验证功能，则所有的控制消息都必须包含一个 Message Digest AVP，其连接过程如下：

1) 用户端通过modem向ISP发起呼叫，用户名为vlk@vanlink.com，密码为：jjjddd；

2) 如果ISP的拨号服务器（LAC）支持L2TPv3，并已经打开了VPDN服务，在接收到用户

拨入请求之后，取得用户名等信息；

3) LAC对用户信息进行进行PAP或者CHAP认证；

4) LAC将认证信息（用户名，密码）发送给RADIUS服务器进行认证；

5) RADIUS服务器认证该用户，如果认证通过则返回该用户对应的LNS地址，隧道密码等相关信息，并且LAC发起Tunnel连接请求；

6) LAC向指定LNS发起Tunnel连接请求，即向LNS发送SCCRQ消息，注意，SCCRQ中Message Digest AVP的值计算有所不同，因为此时还没有获得通过SCCRP告知的LNS的nonce；

7) LAC向指定LNS发送带有Control Message Authentication Nonce AVP的SCCRQ消息，LNS必须在回送的SCCRP消息中带有Control Message Authentication Nonce AVP和Message Digest AVP，前者包含了LNS生成的随机数。而Message Digest AVP中包含一个hash值，参考2.1，可知它是由LNS使用下列输入计算得到的：控制消息头和控制消息中所有的AVPs，自己随机数（nonce），对端随机数（nonce）以及shared_key；

8) LAC使用相同的输入执行同样的运算，如果本地计算得到的散列值和Message Digest AVP中的散列值相同，则来自LNS的控制消息得到验证，最后，LAC向LNS发送SCCCN消息，表明隧道建立成功；

9) 隧道建立之后，LAC 和 LNS 协商建立 PPP 会话：LAC 端将 ppp 协商参数传送给 LNS；

10) LNS将接入请求信息发送给RADIUS服务器进行认证；

11) RADIUS服务器认证该请求消息，如果认证通过，则返回响应信息；

12) 会话建立之后，远端用户的 PPP 进程还是通过隧道和隧道上的会话转发与 LNS 上的 PPP 进程通信，进行 PPP 层的链路控制协商，确定远端用户端的 IP 地址等。在 LNS 上可以配置是否再对远端用户进行一轮身份验证；

13) 协商结束，远端用户开始和 LNS 上的 PPP 进程进行透明的数据通信。

图 5 显示了 RADIUS 中用户信息数据库信息，这里 RADIUS 只验证用户名和密码：

```
mysql> select * from passwd;
+-----------------+------------+----------------+--------+
| user_name       | service    | password       | active |
+-----------------+------------+----------------+--------+
| vlk@vanlink.com | Framed-PPP | jjjddd         | Y      |
| test12          | Framed-PPP | 20TzBXsT4NcG.  | Y      |
| test11          | Framed-PPP | 20FrkMKg6YmUQ  | Y      |
| jiangmen1       | Framed-PPP | jiangmen1      | Y      |
| vlk@cisco.com   | Framed-PPP | jjjddd         | Y      |
| vanlink         | Framed-PPP | jjjddd         | Y      |
+-----------------+------------+----------------+--------+
```

图 5 RADIUS 中用户信息数据库

4. 结束语

本文在研究二层隧道协议 L2TPv2 的工作原理基础上，讨论了其安全性漏洞，进而分析了 L2TPv3 协议，相比于 L2TPv2，L2TPv3 不仅局限于承载 PPP 帧，还可承载更多类型的数据包，在安全性上，不仅仅对隧道终端实体进行认证，而且可以对每个数据包进行认证，有效地防止了 DOS 攻击，提高了第二层隧道的安全性和健壮性。

参考文献

[1] 何宝宏，《IP 虚拟专用网技术》 [M]，人民邮电出版社，2002
[2] 龚丽君，张颖江，“增强型第二层隧道协议 eL2TP 的加密机制” [J]，湖北工学院学报，2003，**18** (3)：31～33
[3] IEFT RFC 2661, August 1999, Layer Two Tunneling Protocol "L2TP". [S]
[4] IEFT RFC 3931, March 2005, Layer Two Tunneling Protocol - Version 3 (L2TPv3). [S]
[5] IEFT RFC 3193, November 2001, Securing L2TP using IPsec.[S]

Security research of L2TPv3 protocol

Zhao Lei, Ma Yue
College of Computer Science & Technology, Beijing University of Posts and Telecommunications, Beijing (100876)

Abstract

In this paper the principle of L2TPv2 protocol is introduced, and then its security drawback is discussed. To improve the performance of security, L2TPv3 is brought forward. We analyze the control message and data message of L2TPv3 for security improvement, which includes aperiodic certification, data encryption and integrality examination. Further the procedure of establishing safe VPDN connection using L2TPv3 is set forth.

Keywords：tunnel; L2TPv2; L2TPv3; security