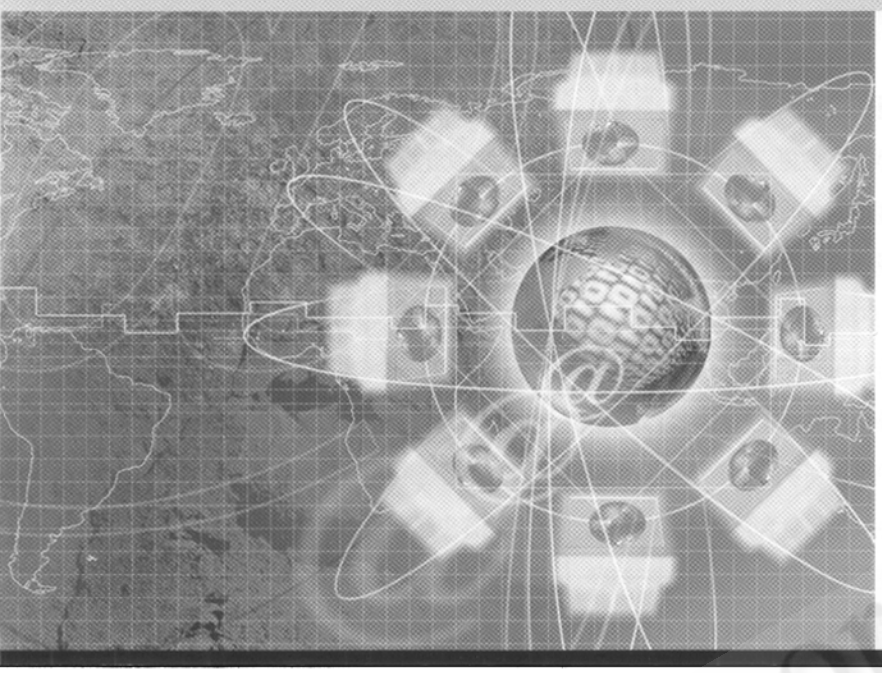

网络传输层安全协议SSL的安全性研究

The Security Research of the Network Transport Layer Security Protocol SSL

吴凯　陈晓苏　肖道举

(华中科技大学计算机科学与技术学院　430000)

摘要：文章简述了SSL V3.0的分层结构、加密属性,并从握手协议层和记录协议层出发对其安全性做出分析。

关键词：SSL协议　握手协议　记录　安全性

考虑一个网络系统的安全性应该从网络信息系统的各个层面来研究,可从信息安全体系的五层结构出发把安全问题划分为数据的安全性、应用层的安全性、网络层的安全性、用户账号的安全性和系统层的安全性,本文立足于研究网络应用层下面传输层的安全协议,如安全套接层SSL(Secure Sockets Layer)。

SSL安全协议最初由Netscape Communication Corporation开发。该公司于1994年11月推出SSL V2.0 Internet-Draft,随后一年多的时间里历经5次修改。SSL V3.0 Internet-Draft于1996年3月推出,它不仅解决了SSL V2.0存在的问题,并且支持更多的加密算法。

1 SSL协议

1.1 SSL V3.0的结构

SSL V3.0由两层组成,低层是SSL记录协议层(the SSL Record Protocol Layer),简称记录层,位于可靠的运输层协议之上(如:TCP),由它对各种更高层协议进行封装;高层是SSL握手协议层(the SSL Handshake Protocol Layer),简称握手层。见图1。握手层允许通信双方在应用协议传送数据之前相互验证、协商加密算法、生成密钥等。记录层封装各种高层协议,具体实施压缩/解压缩、加/解密、计算/验证MAC等与安全有关的操作。

1.2 SSL V3.0的加密属性(cryptographic attributes)

SSL V3.0中对称加密用于加密应用数据,非对称加密用于验证实体和交换密钥,非对称加密算法按用途分为密钥交换算法和数字签名算法。

SSL V3.0给出的序列加密算法有RC4(40位和128位密钥)。给出的分组加密算法有40位密钥的RC2 [RC2 98]、40和56位密钥的DES [DES 83]、3DES [3DES 79]、IDEA [IDEA 92]和Fortezza;另外SSL V3.0指定专为出口使用的40位的DES,命名为DES40。

目前SSL V3.0给出的密钥交换算法有RSA [RSA 78]、Diffie-Hellman [DH 77]和Fortezza_dms [FOR 95];数字签名算法有RSA和DSA。数字签名时,单向hash函数(one-way hash function)做为签名算法的输入。RSA签名中,一个36字节的两个hash函数(一个是SHA hash,一个是MD5 hash)的连结被签名。DSS签名[DSS 94]中,一个20字节的SHA hash被签名。

另外,SSL V3.0指定的hash算法有128位密钥的MD5和160位密钥的SHA。

1.3 SSL V3.0的通信主体

SSL V3.0中定义了两个通信主体:客户(client)和服务器(server)。客户是协议的发起者。虽然SSL V3.0中的通信主体也被称为客户和服务器,但它们的含义与我们通常讲的应用层的客户/服务器结构中的客户和服务器的含义不同。应用层从请求服务和提供服务的角度定义客户和服务器,而SSL V3.0则从在建立加密参数的过程中扮演的角色来定义客户和服务器。当SSL V3.0与应用层协议结合使用时,应用层的客户应用下方的SSL V3.0以SSL客户的身份运行,应用层的服务器应用下方的SSL V3.0以SSL服务器的身份运行。

2 SSL 3.0安全性分析

SSL协议是为客户应用和服务器应用在不安全的通道上建立安全的连接而设计的。因而,我们需要考虑各种可能的安全威胁。我们假设攻击者具有相当的计算资源且不可能从协议之外的任何地方获得保密信息;假设攻击者

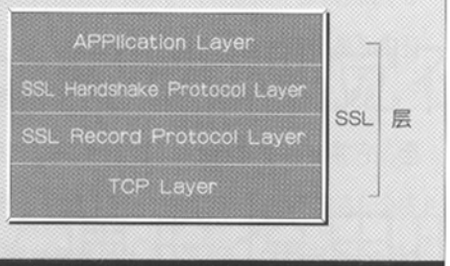

图1 SSL V3.0的分层结构

能够在通信通道上实施被动窃听和修改、删除、重放和其它操纵消息的主动攻击。定义入侵者不击破密码体制而在协议允许的操作范围内获得明文的协议是不安全的协议。对于一个安全协议，需要从多方面对其安全性质进行验证。验证的手段有多种，比如：直观的分析、实际攻击手段的测试，还有形式化的逻辑推理。下面首先给出一种对SSL协议的攻击，然后分别分析SSL V3.0的握手层和记录层是如何设计来抵抗各种安全威胁的，并且给出SSL V3.0存在的某些不足。

2.1 穷尽40位RC4密钥的攻击

这种攻击利用了美国对出口密码产品限制这一事实，美国限制出口的密码产品中对称加密算法的密钥长度为40位（当前已放宽到64位[BXA00]）的；公钥加密算法的密钥长度为512位（当前已放宽到1024位[BXA00]）。这就导致出口的SSL产品的加密强度大大减弱。

对于SSL V2.0 [SSL2 95]和SSL V3.0，穷尽40位RC4密钥攻击的原理基本相同。出口的SSL使用的40位RC4，并不代表做为RC4的输入的密钥确实就是40位，实际上是128位，但只有40位的强度。

对SSL V2.0的攻击。1995年7月14日[Fin1]和8月19日[Fin2] Hal Finney在Internet上先后给出了对Netscape Web server上的SSL V2.0的两个challenge。第一个challenge于同年8月15日被Adam Back、Eric Young和David Byers合作攻破，当天的两个小时后Damien Doligez [Dol 95]也攻破之，Adam Back和Piete Brooks组织了对第二个challenge的攻击[Bro 95]，Damien Doligez也加入其中，攻击从8月24日18:00 (GMT)开始，仅用31.2小时就攻破了第二个challenge。

SSL V2.0中，client和server每次通信时都生成一对会话密钥：server-write-key和client-write-key，分别用于两个方向的加/解密。Hal Finney给出的challenge的cipher选择是RC4_128_EXPORT40_WITH_MD5，这种cipher的会话密钥的生成方法如下：

server-write-key = MD5 [master-key, "0", challenge, connection-id]

client-write-key = MD5 [master-key, "1", challenge, connection-id]

client-read-key与server-write-key相同；server-read-key与client-write-key相同。Challenge和connection-id可分别从明文发送的消息CLIENT-HELLO和SERVER-HELLO中得到。Master-key由两部分构成：clear-key和secret-key。Clear-key为88位，可从消息CLIENT-MASTER-KEY的明文部分得到；secret-key为40位，加密后做为消息CLIENT-MASTER-KEY的密文部分。我们要穷尽攻击的就是secret-key。

假设我们首先寻找正确的server-write-key。对于一个被假设的40位的secret-key，与clear-key一起构成一个master-key；随后用MD5对master-key、challenge、connection-id等做hash；用此hash值做为密钥解密消息SERVER-VERIFY中的密文部分，若得到正确的明文（明文是{0x03, connection-id}），就可断定此hash值就是正确的server-write-key；否则继续检查下一个假设的secret-key，直到找到正确的secret-key为止。得到正确的server-write-key后，用相应的master-key生成client-write-key；随后可用client-write-key解密用其加密的消息。

对于SSL V2.0，这种攻击的危害性很大，因为攻击者得到的是一个会话的master-key，这就意味着使用这个会话进行的所有的加密通信的信息都会被攻击者得到。

穷尽40位RC4密钥的攻击是由于美国对出口密码产品的限制导致的不安全，不是SSL协议自身的安全缺陷，无法从技术上解决。对国内来讲，可以考虑用我国自主产权的加密算法替换外来的SSL实现中的弱强度的加密算法。

2.2 握手协议层的安全性

SSL握手协议本质上是一个密码算法和密钥交换协议。握手过程中，client和server协商各种算法，双方有选择地验证对方，以及生成会话密钥等。握手层重视的是完整性。

2.2.1 验证主体的有效性

SSL V3.0中，通过检查主体的证书实现对主体的验证。验证方得到被验证方的证书后，对证书进行各种检查。CA和证书的理论基础保证了通过证书的方式验证主体的有效性。

2.2.2 Hash算法的使用

SSL V3.0对hash算法使用得很谨慎。在可能的情况下，MD5和SHA一前一后地使用（二者或独立地、一前一后地使用，或嵌套使用），这就保证了一个hash算法被攻破时不至于导致整个协议被攻破。

2.2.3 握手消息中的MAC

SSL V3.0握手协议中有几处使用MAC结构做消息完整性检查。Server Key Exchange消息的Signature结构中的md5_hash和sha_hash使用的是MAC；Client Certificate Verify消息的Signature结构中的md5_hash和sha_hash使用的是HMAC；Finished消息的md5_hash和sha_hash使用的是HMAC。HMAC (Keyed-Hashing for Message Authentication) 是带密钥的hash [HMAC 97]，其安全性比普通的MAC要高得多。Client Certificate Verify消息和Finished消息用到的HMAC的密钥是master secret。HMAC的使用很好地保护了几个SSL V3.0握手消息的完整性。

2.2.4 签名的安全性

Server的公钥或者在server的证书中给出，

或者是Server Key Exchange消息给出的临时公钥。临时公钥被server的签名证书（RSA证书或DSS证书）签名，server对其临时公钥的签名使用了ClientHello.random，所以过去的签名和临时RSA公钥不会被重放，也即Server Key Exchange消息不会被重放。

当client的证书是签名证书时，client发Certificate Verify消息。在该消息中，client对master secret和在该消息之前已发送的所有的握手消息handshake_messages签名，由于handshake_messages包含了ServerHello.random，所以Client Certificate Verify消息不会被重放。

就以上分析来看，握手层提供了较好的安全性，只是有个别域未受完整性保护或检查。当攻击者发起主动攻击时，这些完整性方面的不完善则突出出来。另外，拒绝服务攻击和完全匿名模式下的man-in-the-middle攻击是无法避免的。

2.3 记录协议层的安全性

假设握手协议已安全建立会话状态、选择好加密参数，并生成密钥等。我们从保密性和完整性两方面分析SSL V3.0记录层的安全性。

2.3.1 保密性

SSL V3.0通过各种对称加密算法，例如，RC4、RC2、DES、3DES、Fortezza，来保证数据的保密性。

2.3.2 完整性

SSL V3.0使用加密的MAC保证数据的完整性。

总地看来，SSL V3.0记录层对应用数据保护得很好，未防止流量分析和未保护个别域的完整性，相对来讲威胁较小。

3 结论

通过对SSL V3.0的描述和分析，我们认为SSL3.0采用了数据通信加密、身份验证等安全技术，它在不同层次连接和不同传送方向上都使用了不同的密钥，客户和服务器之间采用了数字签名和认证，结合HASH算法，较好地保证了数据在传送过程中的保密性、可靠性和完整性，防止了欺骗、修改等多种攻击。

总体上该安全协议是可靠的，但也有值得探讨和改进的地方。　对于接近于具体实现的协议，其安全性受实现的影响的程度不可低估。

在国内，对SSL的讨论理论文章比较多，具体实现技术的介绍比较少见，其主要原因在于商业的认证中心（Certificate Authorityh，又称CA中心）在国内还不太成熟，所以建立我们自己的认证中心是SSL大规模应用的基础。

SSL 3.0解决的是点到点之间的信息传输安全，它并没有解决internet上Web站点自身的安全。在实际应用中，网络的安全要综合考虑，对站点进行防护，保证站点上的关键数据：如SSL协议加密和签名时所用到的私钥数据不被泄露，才能保证SSL协议实施的可靠性。因此，结合具体网络的实际情况，利用SSL协议和CA认证技术，并辅以其他的安全技术共同解决安全传输问题。

参考文献

1 Rolf Oppliger著，杨义先，冯运波，立忠献译《WWW安全技术》，人民邮电出版社。

2 W.Diffie，M.E Hellman. NEW Directions in Cryptography. IEEE Transactions on Information Theory, IT -22(6), 1976, pp.644-654。

3 Pekka Nikander, Modelling of Cryptographic Protocols, Licenciate's Thesis, Helsinki University of Technology, December 1997。