

网络传输层安全协议 SSL 的安全性研究

吴凯 陈晓苏 肖道举

(华中科技大学计算机科学与技术学院)

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

1 引言

最近十几年来, 计算机网络, 特别是 Internet 的飞速发展在诸多方面不同程度地改变了人们工作和生活方式。信息时代的政治、经济、文化、个人生活对 Internet 的依赖与日俱增。Internet 这一开放的环境在带给人们极大便利的同时, 也使人们面临着各种安全威胁。特别是由于我国计算机研发能力还比较弱, 大多数网络设备依赖于进口, 很难从网络设备自身控制其安全性; 另一方面, 在网络建设、运行和使用过程中, 一般考虑最多的是效率、共享和开放, 而对安全、保密、抗攻击及可控制性等考虑甚少, 这样就给网络信息的安全留下了隐患, 目前互联网和内部的企业网上存在很多的安全漏洞, 而这些安全漏洞已被或将要被一些高科技犯罪分子所利用, 从而可能对社会经济和国家利益造成巨大的损失。

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。

2 SSL 协议

2.1 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, 位于可靠的传输层协议之上(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。

2.2 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。

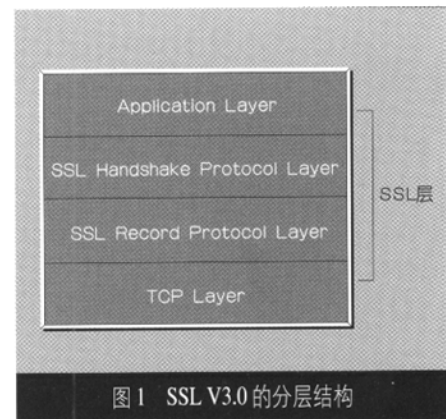


图 1 SSL V3.0 的分层结构

The Security Research of the Network Transport Layer Security Protocol SSL

2.3 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。

3 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。假设攻击者能够在通信通道上实施被动窃听和修改、删除、重放和其他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。

3.1 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。

3.1.1 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:

$$\text{server-write-key} = \text{MD5}[\text{master-key}, "0", \text{challenge}, \text{connection-id}]$$

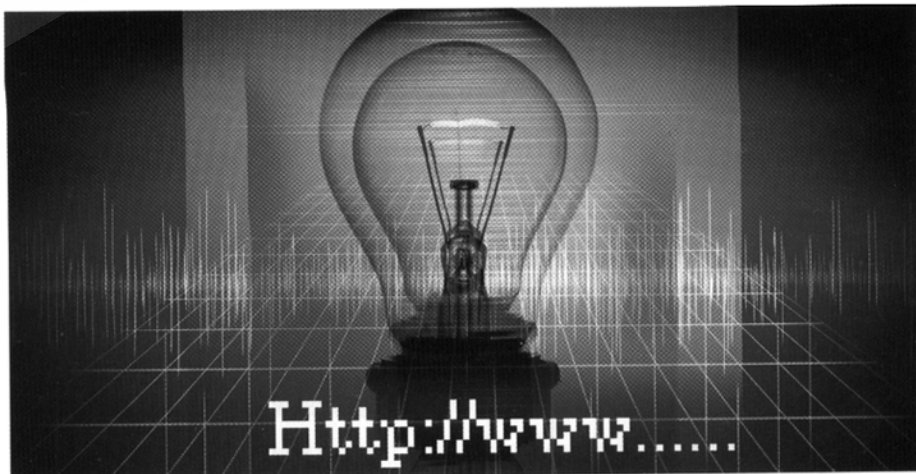
$$\text{client-write-key} = \text{MD5}[\text{master-key}, "1",$$

$$\text{challenge}, \text{connection-id}]$$

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。



The Security Research of the Network Transport Layer Security Protocol SSL

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知识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。

3.2 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。

3.2.1 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。

3.2.2 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。

3.2.3 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。

3.2.4 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。

3.2.5 结论

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。

3.3 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。

3.3.1 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。

3.3.2 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。

4 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 Authority, 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。 ■

- 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, Licentiate's Thesis, Helsinki University of Technology, December 1997.