SSL 协议安全缺陷分析

The Analysis of Security Vulnerabilities of SSL Protocol

胡国华 袁树杰 (安徽理工大学安全技术与工程教研室 安徽 淮南 232001)

摘要:本文介绍了 SSL 协议的工作原理,对 SSL 协议存在的几个安全缺陷和攻击方法进行了分析,并提出了可行的解决策略。

关键词:SSL 协议 安全缺陷 解决策略

1 引言

随着计算机网络技术的飞速发展,信息时代的人们对 Internet 的依赖性越来越大。当今时代,电子商务和电子政务的应用越来越广泛,然而网络安全问题严重束缚了计算机网络的进一步应用。

安全套接层 SSL(Secure Sockets Layer)协议是由 Netscape 公司设计开发的安全协议,主要用于加强应用程序之间的数据的安全性。SSL 协议是基于 Web 应用的安全协议,它采用了 RSA 算法、RC4 – 128、RC – 128、三重 DES 算法和 MD5 等加密技术实现两个应用层之间的机密性、可靠性和数据完整性,并采用 X.509 数字证书实现鉴别,其加密的目的是建立一个安全的通讯通道,而且该通道可在服务器和客户机两端同时实现支持。本文章主要讨论 SSL 协议的工作原理及其存在的安全漏洞和实际解决方案。

2 SSL 基本工作原理

SSL 协议用来建立一个在客户和服务器之间安全的 TCP 连接,尤其可被用来认证服务器,可选地认证客户,执行密钥交换,提供消息认证,而且还可以完成在 TCP 协议之上的任意应用协议数据的完整性和隐蔽性服务。SSL 为在 Internet 上安全地传送数据提供了一个加密通道,建立一个安全连接,主要实现以下工作:加密网络上客户端和服务器相互发送的信息;验证信息在传送过程是否安全完整;运用非对称密钥算法验证服务器;验证客户身份;交换应用层数据。

3 SSL 协议安全漏洞

SSL 协议在服务器与客户之间建立了一条安全通道,保证了在互联网上通信的保密性,但它也不是绝对安全的,SSL 协议存在一定的缺陷和漏洞。

3.1 通信业务流攻击

3.1.1 攻击原理

通信业务流攻击试图通过检查未保护的包的某些域或会话属性,发现有价值的信息。例如,通过检查没有经过加密的 IP 包的源地址、目标地址、TCP 端口等内容,能够获得有关通信双方的 IP 地址、正在使用的网络服务等信息,在某些特定情况下,甚至可以获得有关商业或个人关系方面的信息,当然这些信息是有价值的。而在 SSL 协议中记录头中如记录长度等信息没有被保护,这是潜在的隐患。攻击者通过检查通信业务流中密文信息的长度,有可能发现 Web 通信中 URL 请求的相关信息,当浏览器连接到 Web 服务器时,浏览器发送的包含 URL 的 GET 请求数据包是加密的,Web 服务器返回的 Web 页也是加密的,但是通信业务流攻击,攻击者可以得到 Web 服务器的 IP 地址、URL 请求的长度和返回的 Web 页面长度等信息,这些信息足以使攻击者发现用户访问的是什么 Web 页面。因为,目前高级的 Web 搜索引擎技术能够在可以公开访问的 Web 服务器上,搜索到给定 URL 长度和 Web 页面长度的页面。这种攻击能够成立的原因是密文长度揭露了明文信息的长度。由于 SSL 协议只对分组密码算法有填充机制,而对于流密码算法该协议是不支持的,所以这种潜在的可能性攻击还需要引起我们的重视。

3.1.2 解决策略

该攻击仅仅是描述了一种潜在的可能性，能够攻击成功还需要许多前提条件。但是，这种潜在的可能性应当引起注意，在具体应用过程中尽量避免。SSL 协议无法抵抗通信业务流攻击，而且以 SSL 协议为基础的传输层安全协议 TL S 协议仍然不能抵抗这种攻击，这是由于协议的设计目标和其所处的网络层次结构决定的。在 TL S 协议中也没有作出改进，只是在文档中强调了协议的设计目标和这种攻击的危险性，告诫协议的应用者不能在未保护的通信业务流中暴露机密信息。对于通信业务流攻击，只能通过应用者的谨慎，尽量避免泄漏有关重要信息。

3.2 密钥交换算法欺骗

3.2.1 攻击原理

在有些情况下，服务器用 Server Key exchange 消息来交换密钥，并用自己的长期有效的证书为临时的公开参数签名，同时发给客户，客户使用这些公开参数和服务器交换密钥，获得共享的主密钥。SSL 协议规定可以使用 RSA 算法和 Diffie – Hellman 等多种密钥交换算法，但 KeyExchange Algorithm 这个域并不包含在服务器对公开参数的签名内容中，这样攻击者可以滥用服务器对 DH 参数的签名来欺骗客户，使之认为服务器发送了对 RSA 参数的签名，攻击者使用 Cipher Suite 回转攻击（在交换 finished 消息之前攻击者就能够通过后继的攻击获得所有秘密，所以能够伪造 finished 消息，则该攻击是能够获得成功的），使服务器使用临时的 DH 密钥交换，而客户使用临时的 RSA 密钥交换，这样，DH 的素数模 p（dh – p）和生成因子 g（dh – g）将被客户理解为 RSA 的模 p（rsa – modulus）和指数 g（rsa – exponent）。那么，客户将使用假的 RSA 参数加密主密钥发送给服务器。攻击者截获 RSA 加密的值 gkmod p，因为 p 是素数，所以可以容易地求出其第 g 个根，从而恢复出主密钥的 PKCS 编码 k。在消息交换的最后，客户的主密钥值为 k，服务器的值为 gxy mod p，这里的 x 是攻击者任意选择的。这样，主密钥就被泄露给攻击者了，则以后的所有消息交换过程都可以被攻击者伪造，协议不再有任何安全性可言。

3.2.2 解决策略

这种安全缺陷也可以通过协议实现者的特殊处理加以避免，协议应用者需要在接收到 key exchange 消息时仔细检查公开参数域的长度，就能够区分所使用的密钥交换算法，如 DES 算法密钥长度为 40bit，从而避免这种攻击。

3.3 Change Cipher Spec 消息丢弃

3.3.1 攻击原理

SSL 握手协议中有一个小的漏洞，那就是在 finished 消息中没有对 change cipher spec 消息的认证保护。从而存在一种潜在的攻击方法——丢弃 change cipher spec 消息。在正常的通信情况下，双方的通信流程如下：

(1) C →S：[change cipher spec]
(2) C →S：[finished]{a}k
(3) S →C：[change cipher spec]
(4) S →C：[finished]{a}k
(5) C →S：{m}k

但存在一种特殊的情况，在这种情况下，中间人 M（man – in – the – middle – attack）采取 Change Cipher Spec 消息丢失攻击，这种攻击的前提是当前的 CipherSuite 不作 MAC 保护；未决的 CipherSuite 不作加密，作 MAC 保护，那么攻击的消息流如下：

(1) C→M：[Change Cipher Spec]
(2) C→M：[finished]{a}k
(3) M→S：[finished]a
(4) S→M：[change cipher spec]
(5) S→M：[finished]a
(6) M→C：[finished]a
(7) C→M：{m}k
(8) M→S：m

其中{*}k 表示记录层协议对数据进行加密保护；m 表示明文的应用数据；n 表示 finished 消息中的认证码，是对所有握手消息进行 MAC 计算结果（但不包括 Change Cipher Spec 消息的认证）。

从以上过程可以看出，在接收到 Change Cipher Spec 消息之前，当前的 CipherSuite 不加密，不作 MAC 保护，直到收到 Change Cipher Spec 消息之后，记录层才开始对通信数据进行加密和完整性保护。假如只对密码族进行认证而从不加密，这样中间人攻击者将窃取并删除 Change Cipher Spec 消息，致使通信双方将不再更新当前的密码族（Cipher Suite），即不再对传递的数据作 MAC 认证和加密。由于商定的密码族不起作用，这样协议失去了对数据的认证能力，从而中间人攻击者在通信双方不知道的情况下，可以任意修改会话数据。

3.3.2 解决策略

将 Change Cipher Spec 加入到 Finished 消息的消息认证计算中，这样才符合认证协议的上下文原则。当然，也可以不修改协议的基本框架，在发送 Finished 消息之前要求收到 Chang Cipher Spec 的消息，否则引起协议的致命错误并会中断连接，这实际上是协议实现者对 SSL 协议缺陷的弥补工作。

3.4 证书攻击和窃取

3.4.1 攻击原理

公共 CA 机构并不总是很可靠的，因为对于用户的证书，公共 CA 机构可能不像对网站数字证书那样重视和关心其准确性。由于微软公司的 IIS 服务器提供了“客户端证书映像”功能，用于将客户端提交证书的名字映射到 NT 系统的用户帐号，在这种情况下，攻击者就有可能获得该主机的系统管理员的权限；当然，如果攻击者不能利用上面的非法的证书突破服务器的话，他们还可以尝试运用暴力攻击获取访问的权限，运用暴力攻击客户端认证的方法是：攻击者编辑一个可能的用户名字列表，然后为每一个名字向 CA 机构申请证书。每一个证书都用于尝试获取访问权限。用户名的选择越好，其中一个证书被认可的可能性就越高。暴力攻击证书的方便之处在于它仅需要猜测一个有效的用户名，而不是猜测用户名和口令。

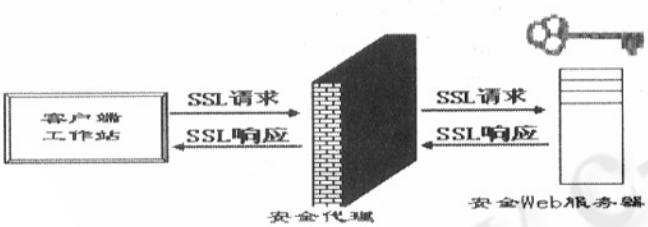

图 1 客户端 SSL 通信安全代理工作原理示意图

攻击者还可能窃取有效的证书及相应的私有密钥，其最简单的方法是特洛依木马病毒，这种攻击几乎可使客户端证书形同虚设，它攻击的是证书的一个根本性弱点：私有密钥——整个安全系统的核心——经常保存在不安全的地方，对付这种攻击的唯一有效方法是将证书保存到智能卡或令牌之类的设备中。

3.4.2 解决策略

证书的安全可以采用 IDS（Intrusion Detection System），它是一种用于监测攻击服务器企图的技术和方法。典型的 IDS 监视到网络信息与保存在数据库中的已知攻击“特征”或方法进行比较，如果发现攻击，IDS 可以提醒系统管理员切断连接或甚至实施反攻击等。但是，如果网络通信是加密的，IDS 将无法监视攻击者，而且反而可能会使攻击者更为轻松的实施攻击。解决的方法是通过 Proxy 代理服务器的 SSL，可以在一个 SSLproxy 代理服务器程序上使用这项资料审查技术。SSL proxy 是一个连接在 80 端口上接受纯文字的 HTTP 通信请求的软件，它会将这些请求通过经由 SSL 加密过的连接，转寄到目标网站。在连接端口 80 开一个听取 Socket（侦听），通过 open SSL0.9.6 指令，将所有进入这个 Proxy 的数据传送出去。通过这个 SSL Proxy 机制，只要将安全扫描软件指向 Proxy 的 IP 地址，就可以用来审查 SSL 服务器，从而满足信息传输安全的需求，其使用 proxy 代理服务器的工作原理如图 1。

4 结束语

本文主要讨论了 SSL 协议的体系结构及特点，重点分析了 SSL 协议的安全性中存在的一些常见漏洞，但这些问题均可以通过一定的方法得以弥补和解决。作为一个复杂的安全协议，SSL 的安全机制是比较完善的，一般情况下能够抵抗窃听、篡改、会话劫持及中间人攻击等多种手段。SSL 协议的设计与高层应用和底层网络协议无关，可以方便的集成到多种网络中去，可根据不同的安全需求，选择协议提供的多种密码算法和密钥交换协议，目前已广泛地应用在浏览器与 WEB 服务器之间的安全通信中。然而，SSL 协议仅仅是网络安全工具的一种，必须紧密结合其它网络安全工具，才能构造出全面、完善、安全可靠的网络。

参考文献

1 Frier P Karlton ,P Kocher. The SSL3. 0 Protocol ,Netscape Communications Corp ,1996 ,18.
2 Davis Wagner ,Bruce Schneier. Analysis of the SSl 3. 0 Protocol [M] . 1996.
3 Tim Dierks ,Christopher Allen. The TLS Protocol Version 1. 0 , IETF RFC2246 ,January ,1999.
4 戴英侠、左英男、许剑卓，SSL 协议的安全缺陷与改进[J]，中国科学院研究生院学报，2000，17(1)：86－92。
5 任静、李涛，客户端 SSL 安全代理的设计与实现[J]，四川大学学报，2002，(2)：17－18。