第33卷 第12期 计 算 机 工 程 2007年6月
Vol.33 No.12 Computer Engineering June 2007
·安全技术· 文章编号：1000—3428(2007)12—0142—02 文献标识码：A 中图分类号：TP393.08

一种基于代理的增强浏览器安全性方案

严 佩，苏锐丹
(西安电子科技大学多媒体研究所，西安 710071)

摘 要：介绍了一种基于代理的增强浏览器安全性方案，不仅提高了客户端浏览器和整个安全连接的安全性，还增加了客户端对多用户的支持。讨论了该方案的整体框架，给出了通信模块、证书管理模块和密码服务模块等的功能描述及设计与实现过程中的注意事项。并对该方案的扩展与改进作了说明。

关键词：代理；浏览器；安全性

Proxy-based Scheme to Enhance Browsers Security

YAN Pei, SU Ruidan
(Multimedia Technology Institute, Xidian University, Xi'an 710071)

【Abstract】 This paper presents a proxy-based scheme to enhance the security of browsers and the whole security connection, which also supports multi-user. It describes the overall architecture of the scheme with emphases on discussion of communication module, certificate management module and cryptographic service module and some issues about their design and implementation. It also gives the extension and improvements of the scheme.

【Key words】 Proxy; Browser; Security

1 概述

SSL/TLS(secure socket layer/transport layer security)协议主要用于为 Web 服务器和客户端(Brower)提供基于证书的加密和认证服务，保证通信数据的安全性和完整性。但当前普遍使用的 Web 客户端由于种种原因，其安全性往往不能满足某些特定应用的需求。

以 Microsoft 的 IE 为例，浏览器中普遍存在的缺陷有：(1)所支持的密码算法强度或密钥的长度不能满足要求；(2)所支持的安全通信协议不能满足应用的需要；(3)证书存储机制薄弱，容易受到恶意篡改，如 IE 中的证书存放在操作系统的注册表中，可以通过一段恶意代码向 IE 中插入一个假的证书颁发机构的证书；(4)用户使用 IE 等访问 HTTP 站点时，由于某种原因，安全连接没有成功建立，用户得不到任何的错误提示以及修复建议。这些都极大地削弱了基于 Web 的安全通信的可靠性及可用性，所以有必要对其进行研究和改进。目前对客户端安全性的改进研究主要集中在修改源代码或利用系统的某些密码接口 API 扩充强密码算法和/或安全通信协议，如对于 IE，可以使用 CSP(cryptography service provider)和 SSPI(security support provider interface)进行扩充。

本文主要描述了一种基于代理的方法解决上述问题，系统结构如图 1 所示。

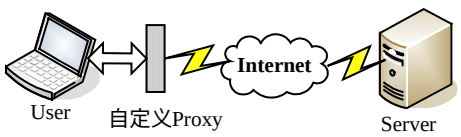

图 1 系统结构

2 SSL/TLS 简介

SSL/TLS 是目前被广泛使用的 2 个基于证书的安全通信协议，主要为 2 个通信实体之间提供数据的保密性和完整性。

假设用户 A 通过 Internet 使用 SSL/TLS 访问一台支持 SSL/TLS 的远程 Web 服务器 S。通常情况下，HTTP 协议数据传输开始前，通信双方就本次通信中将要采用的安全协议版本和密码算法组合进行协商。具体的通信中将采用双方都支持的安全性最高的协议和算法组合进行密钥交换和加密通信等。通信完成后，双方中止连接。

由此得出，双方通信的安全性很大程度上取决于通信双方在通信开始阶段所协商的通信协议和密码算法组合。

出现以下情况时，双方必须采用弱强度密码算法和安全通信协议进行通信，通信的安全性必将大为削弱：

(1)S 采用强度很高的密码算法而 A 的浏览器(IE 等)支持的算法强度比较弱；

(2)S 支持浏览器不支持的某些高强度算法；

(3)S 支持强度很高的安全通信协议而 A 的浏览器(IE 等)支持的通信协议的安全性比较差；

(4)S 支持浏览器不支持的安全通信协议。

虽然可以通过修改现有浏览器的源代码或通过其他方式(如对于 IE，可以使用 CSP 和 SSPI 实现)使之支持强算法和新协议，但这些方式工作量大，且难以测试。

3 基于代理的解决方案

本方案通过在客户端和 Internet 的接口处加入本文的自定义代理(图 1)，用强密码算法和/或自定义安全通信协议替换原用户和服务器连接中采用的弱密码算法和/或安全通信协议及服务器端(如果采用自定义协议，须服务器支持)进行通信。

客户端自定义代理由 3 个模块构成：通信模块，证书管

作者简介：严 佩(1982－)，男，硕士生，主研方向：网络信息安全；苏锐丹，博士生

收稿日期：2006-07-07 **E-mail：**yanpei@huaantech.com.cn

理模块和密码服务模块，具体如图 2 所示。

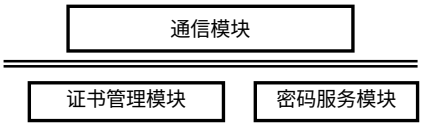

图 2 自定义代理内部结构

(1)通信模块。系统中的核心模块，通常和客户端浏览器处于同一台主机上，负责对浏览器和服务器之间数据流的解密和二次再加密(使用强密码算法)，以及安全协议的转换(将安全性差的安全协议替换为安全性高的或自定义的安全通信协议)。

(2)证书管理模块。管理系统中用到的证书，通常需要和 PKI(public key infrastructure)相结合。

(3)密码服务模块。提供系统所需的密码算法的实现，如 DES、SHA1 等。

(4)其他模块(图中未注明)。如日志管理等，方便系统的管理。

4 通信模块

作为本方案中的核心模块——通信模块，主要负责提高连接的安全性。它可以：

(1)替换浏览器在通信过程中采用的弱密码算法(如可以替换为国密办的国密算法等强可靠性算法)，实现与支持此强密码算法的服务器进行更为安全的标准的 SSL/TLS 通信；

(2)替换通信中采用的安全协议(如 SSL/TLS 等)，采用自定义的符合特定要求的安全通信协议(如支持我国电子商务数字证书认证系统采用的双证书认证的安全协议)与定制的服务器进行安全通信；

(3)在通信模块和服务器之间的安全信道建立失败时，通知客户端错误的原因以及若干修正建议，增强客户端浏览器对用户的友好程度。

假设此时用户 A 使用基于证书的安全通信协议(如 SSL/TLS)通过自定义代理 P 访问服务器 S。为描述方便，引入符号：

Y<<A>>：由 Y 签发的用户 A 的证书，没有必要指明颁发者时可省略 Y；

Private(C)：对应证书 C 的私钥；

CP：代理中内置的证书颁发者；

P：自定义代理。

代理初始化时，代理中有一自签证书 CP<<CP>>以及相对应的私钥。同时，A 必须信任由 CP 签发的任何证书，即将 CP<<CP>>导入自己浏览器的可信任证书颁发机构列表中。如果代理和服务器之间采用基于证书的安全通信协议，则 A 还须将自己的证书导入代理 P，并指明自己私钥的存放位置(可以是本地磁盘或 EKey 等密码设备)作为 P 连接 S 时 P 出示的证书<<P>>和使用的私钥 Private(<<P>>)。

当 A 通过 P 连接站点 S 时，通信过程描述如下：

(1)A 发送连接请求命令(如 CONNECT S)到 P，表示希望 P 为自己建立一条到 S 的安全连接；

(2)P 采用高强度算法与/或自定义的安全协议与 S 建立安全连接(如果采用自定义协议，S 也必须支持此协议)；在基于证书认证的情况下，此过程中 S 使用证书<<S>>；如果 S 要求认证客户端，P 须出示自己的证书<<P>>。如果出于某种原因，连接建立失败，P 将通知客户端错误的原因以及若干修正建议；

(3)P 返回 CONNECTION ESTABLISHED 通知 A 连接建立成功；

(4)P 为 S 产生一公私钥对，并用自签证书 CP<<CP>>对应的私钥为其签发新证书 CP<<S>>；

(5)A 开始发起到 P 的 SSL/TLS 连接。此过程中 P 使用 CP<<S>>，并且 P 不要求客户端认证，即无须 A 出示自己的证书；

(6)连接建立成功后，A 开始发送加密的应用数据。由于 P 拥有 Private(CP<<S>>)，因此 P 可以解密这些数据；

(7)P 使用强密码算法与/或自定义安全协议和 S 通信，并将从 S 获取的应用数据解密后用 P 和 A 在 SSL/TLS 握手时协商的会话密钥加密后发给 A；

(8)通信完成，分别拆除 A 到 P 和 P 到 S 的安全连接。

这样便实现了客户端和自定义代理之间的弱 SSL/TLS 连接和代理和服务器之间的采用强密码算法和/或自定义安全通信协议的强连接。

说明：

(1)通信过程中，第(4)步是必需的。只有这样，P 才可以得到它和 A 之间通信数据的明文，才可能实现密码算法和安全通信协议的替换。

(2)A 必须信任由 CP 签发的任何证书，这样在 A 和 P 建立安全连接时验证 P 出示的证书 CP<<S>>时才可以通过。

(3)由于 A 和 P 处于同一台主机或内部网中，因此 A 和 P 之间的弱安全性连接可以认为是安全的。而 P 和 S 的连接采用了高强度密码算法和/或自定义的安全通信协议，安全性同样也可以保证。

5 证书管理模块

证书管理模块负责存储和管理系统中涉及的证书和私钥。证书的类型不同，代理采用的存储方法也不一样，具体如下：

(1)用户信任的证书颁发机构和服务器的证书

此类证书一般存储在客户端的本地磁盘中，也可以存放在用户的可移动存储器中。为了保证此类证书的存储安全，不会被恶意修改(如非法插入新证书或删除存在的合法的证书)，存放此类证书的证书库须经过用户的签名。用户启用代理时，此类证书在通过用户签名验证后导入到代理中；在当前用户注销时，如果此证书库已被当前用户改动，则询问用户是否要保存这些更改，如果是，提示用户使用自己的私钥对变动后的证书库签名，然后保存。最后，代理销毁刚导入的证书库。

(2)用户自己的证书和私钥

此类证书和私钥除了可以存储在客户端本地磁盘和可移动存储器中，还可以保存在一些密码设备(如 EKey)中，以获取更高的安全性。用户自己的证书和私钥须在用户启动代理时指定。如有需要，用户在导入自己的私钥时需要输入私钥的访问密码。

(3)代理临时生成的证书和私钥

此类证书和密钥由于都是临时生成的，并且都是用来和处于同一主机上或内部局域网的客户端浏览器进行通信，因此不需要特殊的保护。但因为每次通信都要涉及公私钥对的生成，算法开销太大，所以可以采用固定的公私钥对提高系统的效率。

(下转第 147 页)