·应用技术研究 ·

基于 CAMP信号通路模式的代理服务安全性研究

陈 军[1,2],别立洁[2]

(1. 华中科技大学,湖北 武汉 430074; 2. 信阳职业技术学院,河南 信阳 464000)

摘 要:在分析 CAMP信号通路模式及其数学模型的基础上,对代理服务技术的密码学实现进行了数学理论的分析和应用,依据网络数据传输的参数指标对代理服务的可靠性和安全性进行实施性比较,从一个比较理论化角度进行代理服务安全性研究.

关键词:代理服务;信号通路;密码学

中图分类号: TP309. 06 **文献标识码**: A **文章编号**: 1003-0972(2006)04-0449-03

在网络远程教学分布式系统的应用中,通常要采用客户 —代理服务模型,在这种模型中,运行于客户机和代理服务器上进程间的通信基本上要依赖于远程过程调用(RPC).这样的通信模型一般是同步的,也就是说,客户机在向代理服务方发出请求后就挂起本地进程而等待调用后的结果,代理服务器上的调用进程按要求执行完所要求的数据处理后返回结果,一旦本地进程得到结果后就恢复运行.与远程过程调用相对应的方法称作为远程赋值(REV).网络远程教学的代理服务正是 RPC及 REV等概念的延伸,它是一个由客户端向代理服务器发送的包括代码、数据和执行逻辑的程序,这种代理服务不必马上把结果返回到客户机,可以通过其他服务方进行数据分解,再适当转换把信息传回给客户机,与简单的远程过程调用相比更具自治性[1].这种过程也很好地运用了 CAMP信号通路传导的模式方法.

代理服务技术具有很多优越性:比如,减少远程网络的调用、增加客户机与远程服务器间的异步性、动态更新代理服务接口、引入了并发状态等等.这些特点决定了代理服务技术有着多种应用,例如:在网络分布式传输过程中,代理服务器传送一个请求给远程服务端,使之在代理服务器上执行,一旦连接再次建立后就能把结果带回,达到了信息采集的非交互性.代理服务技术还可用自治方式配置新的信息和软件,从而抵抗部分网络的被动恶意破坏和损坏.代理服务器发送的代码包不仅包括数据,还携带有程序指令,让被动传送的数据更具有某些主动性,使得信息服务方式变得更具多样化.

1 代理服务安全性研究的必要性

1.1 代理服务的安全性

代理服务技术在网络上的引入产生了一些安全问题,在一个开放的网络中,代理服务与远程调用安全属于不同的管理区域,它们的相互可信任度很低,因此有可能产生许多不安全因素.

①代理服务会遭受恶意访问穿透的危险而泄露敏感信息;

②被用户使用的代理所包含的敏感数据可能由于网络的不安全性,或代理服务的恶意访问而泄露;

③代理服务传送的代码、控制流程和结果可能为了罪恶的目的而被服务器更改;

④代理服务器如设置了"否认服务"的攻击,它们占据服务器的资源而阻止代理过程[2].

这些安全包括了代理服务器本身的安全,其中最主要的是保护代理服务免受恶意主机窜扰,也就是说:能否保证代码和执行的完整性、能否远程调用信息而不泄露用户的私钥、能否密封代码的隐私性.

1.2 代理服务安全性研究的依据

在一个封闭的网络中,代理服务不可能发挥其潜能,但要在开放的网络环境中安全运行,就必须解决代理服务的保护问题,其中一种方法可以通过建立限制性的代码传送环境,在代理服务和其安全"接口"之间配置密码安全协议[3],让代理服务不被窜扰而挫败潜在的对手.研究的思路就本文而言准备从以下几方面入手:

①代理服务应尽可能不要求与其附属设备执行交互协议;

②代理服务应被允许在不可信的主机上运行,并且保证其正确运行;

③对代理服务的保护机制是可以证明的.

按照这些要求所采用的保护代理服务的方法,可以去掉代理是明文的代码和数据的假设,不存在固有的原因要求程序必须用明文的方式运行,对信息进行加密后不用深究直接传送.

收稿日期: 2006-03-18

作者简介:陈 军(1972-),男,河南商城人,计算机应用硕士,计算机工程师,主要研究方向:局域网安全性能维护等.

2 基于 CAMP信号通路模式的密码学实现方法

执行密码协议要求其关键字始终处于保护状态并在一个安全执行环境下被处理,让认证生成的密钥保持秘密成为重中之重 . 安全执行环境通常包括提供物理存储和执行支持的信息库 . 在并行计算的环境中,所有的交互操作和原先在内部安全环境中的计算都要放在不安全的空间内执行 . 可见,代理服务的密码实现是基于在一个网络中可执行代码信息安全方面技术的研究,CAMP信号通路模式能很好地解决其执行过程 .

尽管一个实际的认证程序能被保持秘密,然而代理服务的整个程序仍可被滥用来任意验证,这使得该过程没有价值 . 为避免于此,尽管不能在可信环境中运行,用户还应该能确定所通过的认证用的是哪个密钥,哪种加密函数和哪种验证代码,并把它们连接到一起 . 因而本文所要解决的问题是,不但代理服务的构件模块是处于公开的,而且其交互的方法也是暴露的,因此,只单独保证这些项目的安全性是不够的,还要从全局考虑保证其交互过程的安全 .

2.1 防恶意攻击的非交互式赋值函数及实现方案

在可执行程序中隐藏一个函数 f的能力对于代理服务的保护是极其重要的,因为所获代码隐私性直接得到代码的完整性 . 为此,必须加密一个函数使得加密形式保持是可执行的 .

假设源主机 A具有一个计算函数 f的算法,远程主机 B有一个输入 x并且愿意为源主机计算 $f(x)$. 但是源主机不想让远程主机知道 f的实质内容,也就是说在函数加密过程中 A与 B不需要相互交互 . 非交互式赋值函数的协议执行过程如图 1($E(x)$、$P(x)$为生成转换程序) .

对于这样的的执行过程中的非交互式赋值加密用同态函数进行构造[4].

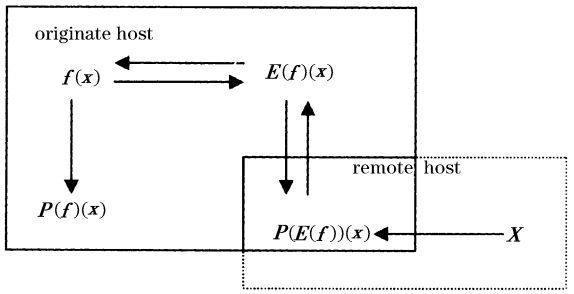

图 1 非交互式赋值协议执行过程

Fig 1 Hand over not with each other type value the agreement carries out the process

假设 R和 S为环,则加密函数为 $E: R \to S$(如果存在一个加法运算使得可以从 $E(x)$和 $E(y)$计算出 $E(x+y)$而不公开 x和 y称作加法同态;同理存在一个混合乘法运算使得可以从 $E(x)$和 $E(y)$ 计算出 $E(xy)$而不公开 x和 y称作混合乘法同态),那么可用 E实现多项式 $U \in R[x_1, x_2, \cdots, x_s]$的非交互式赋值加密函数 .

证明 假设 U为多项式 $\sum_{a_{i1}\cdots i_s} x_1^{i1}\cdots x_s^{is}$

源主机 A生成一个程序 $P(x)$,该程序用下列步骤实现 U:

U每个系数 $a_{i_1\cdots i_s}$用 $E(a_{i_1\cdots i_s})$代替,

当输入 $x_1, x_2, \cdots, x_s$多项式 U就被赋值并存进临时列表 $L: [\cdots, (x_1^{i1}\cdots x_s^{is}), \cdots]$

而列表 $M: [\cdots, E(a_{i_1\cdots i_s}, x_1^{i1}\cdots x_s^{is}), \cdots]$则通过调用混合乘法运算程序对 L的元素及系数 $E(a_{i_1\cdots i_s})$处理而生成的,再通过调用加法运算程序对 M的元素相加[5]. 以下则是 A与 B的程序调用:

A把程序 P送给 B;

B用自己的方式输入 $x_1, x_2, \cdots, x_s$运行 P并获得 $U(x_1, x_2, \cdots, x_s)$;

B把结果 $U(x_1, x_2, \cdots, x_s) = E(P(x))$返回给 A;

A能应用 E^{-1}解密并得到 $P(x)$.

可见,利用同态函数的连续性可将非交互式赋值不间断加密,使得代理服务在应用过程中实现交互过程公开化下数据代码的可靠传送,由于认证程序和密钥都是加密方式给出,减少了代理服务的信息交互操作,从而防止了外来恶意攻击和破坏,整个代理服务系统的安全性就能得到提高 . 论文就该方法的实现通过三步进行验证 .

公钥:源主机 A的验证公钥由函数 $P(E(f))(x)$给出;

程序构造:A选择一个随机有理函数 $r: R^1 \to R$,并构造映射函数 $f_k: R^1 \to R^k$(k为任意自然数),f_k的成分为 $s_i(r, f_1, \cdots, f_k)$, $1 \le i \le k$,然后把函数组 (f, f_k) 送给 B.

程序执行:B计算 $u = f(x)$和 $v = f_k(x)$,那么 (u, v)就是程序的答案输出 .

验证过程:计算 $P_i((E_i)(u))$, $P_i((E_i)(v))$, $1 \le i \le k$, v是 u的验证当且仅当上述结果相等时 .

2.2 建立 CAMP信号通路模式代理服务安全的数学模型

2.2.1 变量设置

代理服务操作在没有病毒、黑客等外来因素干扰下,数据及代码传送应处于稳定状态,假如网络数据传输过程中性能参数指标主要有吞吐量、介质利用率、延迟时间、最大并发连接数、系统恢复力、日志等,每项指标参数变量分别设为 (x_i, y_i), 数据传送持续时间设为 t,在时间间隔为 Δt时,我们假设这些指标参数处于初始水平,即 $(x_1, x_2, \cdots, x_6, y_1, y_2, \cdots, y_6) = (x_1(0), x_2(0), \cdots, x_6(0), 0, 0, \cdots, 0)$,研究各项指标取值变化量[6].

2.2.2 传导通路模式数学求值模型

利用有界函数取值逼近方法求值,引进参数值变量 $H(t)$,由于 $y_i(t)$ 有界,故有 $\lim_{t\to\infty}\frac{y_i(t) - y_i(0)}{t} = 0$,且当 $\lim_{t\to\infty}H(t) = 0$时,存在矩阵 A,使得 $\lim_{t\to\infty}AY = A\lim_{t\to\infty}Y = 0$,其中:

$$A=\begin{pmatrix} a_{11} & 0 & 0 & 0 & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 & 0 \\ 0 & 0 & 0 & a_{44} & a_{45} & a_{46} \\ 0 & 0 & 0 & 0 & a_{55} & a_{56} \\ 0 & 0 & 0 & 0 & 0 & a_{66} \end{pmatrix}.$$

设各变量系数分别为 $l_1, l_2, \cdots, l_6$

$$a_{11} = l_1 H(t) + x_1(0),$$
$$a_{21} = l_1 H(t) + l_2 H(t) + x_2(0),$$
$$a_{22} = l_2 H(t) + x_1(0) + x_2(0),$$
$$a_{31} = l_1 H(t) + l_2 H(t) + l_3 H(t) + x_3(0),$$
$$\cdots$$

$Y = (\frac{1}{t}\int_0^t y(\tau)\,d\tau, \cdots, \frac{1}{t}\int_0^t y(\tau)\,d\tau)^T$,时间间隔 $[0, t]$ 可以看作是持续的,短暂的,所以 $\det(A) = a_{11}a_{22}a_{33}a_{44}a_{55}a_{66}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}\begin{vmatrix} a_{45} & a_{46} \\ a_{55} & a_{56} \end{vmatrix} \neq 0$,从而 $\lim_{t\to\infty} Y = 0$,即 $\forall i, \lim_{t\to\infty}\frac{1}{t}\int_0^t y(\tau)\,d\tau = 0$,故 $\lim_{t\to\infty} y_i(t) = 0 (\forall i)$.

由此,我们可以得到以下结果:

$$\lim_{t\to\infty} x_1(t) = x_1(0) = \frac{1}{t}\int_0^t y(\tau)\,d\tau,$$

$$\lim_{t\to\infty} x_2(t) = x_2(0) = \frac{1}{t}\int_0^t y(\tau)\,d\tau + \frac{1}{t}\int_0^t y(\tau)\,d\tau,$$

$$\lim_{t\to\infty} x_3(t) = x_3(0) = \frac{1}{t}\int_0^t y(\tau)\,d\tau + \frac{1}{t}\int_0^t y(\tau)\,d\tau + \frac{1}{t}\int_0^t y(\tau)\,d\tau$$

$$\cdots$$

2.2.3　代理服务安全性分析

通过 CAMP传导通路模式对其数学模型的分析,我们发现网络数据经过代理服务传输的结构化层次,可以验证数据的加密程度,对数据包通路进行程序验证得到可靠性参数,从而保障客户—代理服务间数据的稳定性、一致性.

引入 Internet中的代理服务技术,由中间件层次提供身份认证、加密信道、访问控制、侵入检测等安全服务.该代理服务系统对用户方浏览器软件和服务器方 Web服务器均不需要作任何改动,只在用户方增加若干个 Client-Proxy,服务器方再加一个安全代理服务器 Server-Proxy即可,就可实现互联远程系统的认证和信息加密,进一步加强了远程教学数据传输的安全性和稳定性.

参考文献:

[1] 谢希仁. 计算机网络 [M]. 大连:大连理工大学出版社, 2000.
[2] 刘清玉. 计算机网络规划设计及实施方案 [J]. 计算机与通信, 1998(3): 48-50.
[3] 戴有炜. NT Server 4.0专业指南 [M]. 北京:清华大学出版社, 1998.
[4] 钟小平. 网络服务器配置与应用 [M]. 北京:人民邮电出版社, 2004.
[5] 曾　明. 代理服务器安装配置与应用 [M]. 北京:人民邮电出版社, 2003.
[6] 蒋　丽、葛明云. 局域网与企业网的实现 [M]. 北京:电子工业出版社, 2003.
[7] 陈　军,柳国杰. 构建防火墙的性能评价模型 [J]. 信阳师范学院学报(自然科学版), 2005, 18(4): 482-485.

Security Research of Surrogate Service based on CAMP Signal Access Mode

CHEN Jun[1,2], BIE Li-jie[2]

(1. Huazhong University of Science and Technology, Wuhan 430074, China;
2. Xinyang Vocational and Technique College, Xinyang 464000, China)

Abstract: Analysis and application of mathematical theory about cryptology of technology of surrogate service are studied based on analysis of CAMP signal access mode and its mathematical model. The reliability and security of surrogate service are compared according to parameter index of network date transfer, security research of surrogate service is carried out from theoritical point

Key words: surrogate service; signal access; cryptology

责任编校:郭红建