

基于自动信任协商的可信网络研究

李熊达¹, 何 利²

(1. 成都信息化技术应用发展中心, 四川 成都 610041;

2. 重庆邮电大学 计算机学院, 重庆 400065)

摘 要:网络安全应该是立体的,可信平台仅仅在一定程度上保证了终端的安全,应用层的安全依靠的是信息交互双方的安全访问控制。自动信任协商是建立可信网络客户端和服务端信任关系的有效办法。文中在可信平台的基础上构建了可信网络结构,根据自动信任协商理论提出了可信网络的信任协商模型,分析了基于自动信任协商的可信网络的访问控制和策略协商问题,在理论上分析了可信网络的框架模型。给出了在 P2P 网络中的典型应用示例,为可信网络的应用建模提供了参考。

关键词:可信网络;自动信任协商;可信计算平台

中图分类号:TP393.02

文献标识码:A

文章编号:1673-629X(2009)09-0150-04

Study of Trusted Network Based on Automated Trust Negotiation

LI Xiong-da¹, HE Li²

(1. Chengdu Information Technique Application Development Center, Chengdu 610041, China;

2. School of Computer Science and Technology, Chongqing University
of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Safe network should be all-directional, trusted platform only sure terminal safety to a certain degree, safety on application layer is based on access control of information interaction both sides. Automated trust negotiation is an effective means to build the relation on client and server. Builds a trusted network structure based on trusted platform, and gives trusted model of trusted network according to automated trust negotiation theory, and analyses the problems of access control and measure negotiation on trusted network based on automated trust negotiation. Also analyses frame model of trusted network in theoretically. Finally, a classic application example on peer-to-peer network is provided, which provides reference to the application modeling of trusted network.

Key words: trusted network; automated trust negotiation; trusted computing platform

0 引 言

随着近几年 IP 网络的急剧增长导致了网络面临新的安全挑战,其中最大的挑战来自于主要终端设备点对点的身份认证和授权,以及网络的访问控制。终端层的平台验证是安全和网络访问要求授权的关键,并且由于网络中针对第二层(数据链路层)和第三层(IP层)的重放攻击、篡改攻击、替换攻击等大量增加和对更高层的网络攻击的增长,需要对网络的访问进行控制^[1-3]。因此要求通信双方即客户端和服务端是值得信任的,这种信任首先要求通信双方各自具有

完整信任关系。

可信计算^[4]技术是一种专门针对保护计算机终端的技术,其规范 TCG(Trusted Computing Group)主要致力于保护终端内部的资源安全、系统可靠性。TCG 的核心内容是为各种计算平台提供全套信任验证的可信平台模块(Trusted Platform Module, TPM)并建立信任及可信性的机制,并且 TPM 还可以提供平台的完整性设置、创建和使用数字签名以及隐私保护的机制,这在一定程度上保证了终端的安全问题,但是由于可信终端组成的网络广泛应用于商务、政务以及科学实验活动,因此如何在分布式计算环境中的通信主体间建立信任关系成为一个重要问题。传统的访问控制技术主要基于请求方的身份进行授权,需要设定统一的安全管理域,然而,在开放的互联网中,即使有可信平台作为访问的基础,但是由于参与主体数量的规模大、运行环境的异构性、活动目标的动态性以及自主性等特

收稿日期:2008-12-18;修回日期:2009-03-06

基金项目:重庆市自然科学基金(CSTS2007BB2445);重庆邮电大学青年自然科学基金(A2008-34)

作者简介:李熊达(1975-),男,浙江杭州人,工程师,硕士,主要研究方向为网络通信协议、可信计算。

点,各资源主体往往隶属于不同的权威管理机构,使得基于身份的访问控制技术在跨多安全域进行授权及访问控制时显得力不从心,暴露出许多弱点,因此,需要寻求一种更为有效的信任关系建立方法,实现从基于身份的访问控制技术到新技术的转化,因此基于可信计算平台的可信网络需要在两个交互用户间建立信任关系。

可信网络要确保各终端是可以相互信任的,由 Winsborough 等人提出的自动信任协商^[5](Automated Trust Negotiation, ATN)概念为可信网络的建立提供了很好的理论基础,它通过信任证、访问控制策略等有效地在交互双方建立了信任关系。

1 自动信任协商理论模型

自动信任协商通过协商者相互提交信任凭证来自动建立信任关系,在 ATN 中,服务提供端要为其提供的服务定义相应的控制策略,实现对客户端的访问控制,ATN 为了提高协商的安全性和对协商者的隐私进行保护,把用户的凭证也视为一种受保护的资源,并通过凭证访问策略对凭证进行保护。

定义 1(ATN 抽象模型)

设客户端信任证集为 AccessRequestorCreds, 服务方信任证集为 ServerCreds, 对于每份信任证 C 的保护, 记作 GovAccessRequestor(c), 协商的信任证披露序列定义为

$$\{C_i\} i \in [0, 2n+1] = C_0, C_1, \dots, C_{2n+1}, \text{其中 } n \in N, C_i \subseteq \text{AccessRequestorCreds}, C_{i+1} \subseteq \text{ServerCreds}.$$

自动信任协商理论^[6]要求敏感凭证在传输过程中得到保护和存储,可信网络的基本要求就是通过可信的凭证递交建立可信平台之间的信任关系,而可信平台通过硬件提供的密钥生成、存储和密码运算功能使协商者相互之间能够自主、高效地完成凭证递交通信,因此笔者以自动信任协商为理论基础,提出了基于自动信任协商的可信网络模型。

2 基于自动信任协商的可信网络模型

可信网络结构必须是通用的,可以包容不同的网

络设备、协议以及网络拓扑结构,因此可以给出可信网络的结构。

该结构主要包含了二个实体:服务请求端和服务提供端。如图 1 所示。

2.1 可信网络结构组成

可信网络结构中的所有的组件和结构都是逻辑的, 可以根据功能需求的一个简单软件、一个硬件设备或者一个冗余设备。其中:

1) 服务请求端指的是某个请求访问被保护网络的模块。可信网络服务请求模块(简称 TNCC)负责建立网络访问的组件,可以由运行在服务请求端上的一个程序执行,在一个服务请求端上可以有几个 NAR 同时连接到不同的网络链路中。同时收集来自于 IMCs 的完整性认证信息并整合本机平台报告和 IMC 的验证结果。

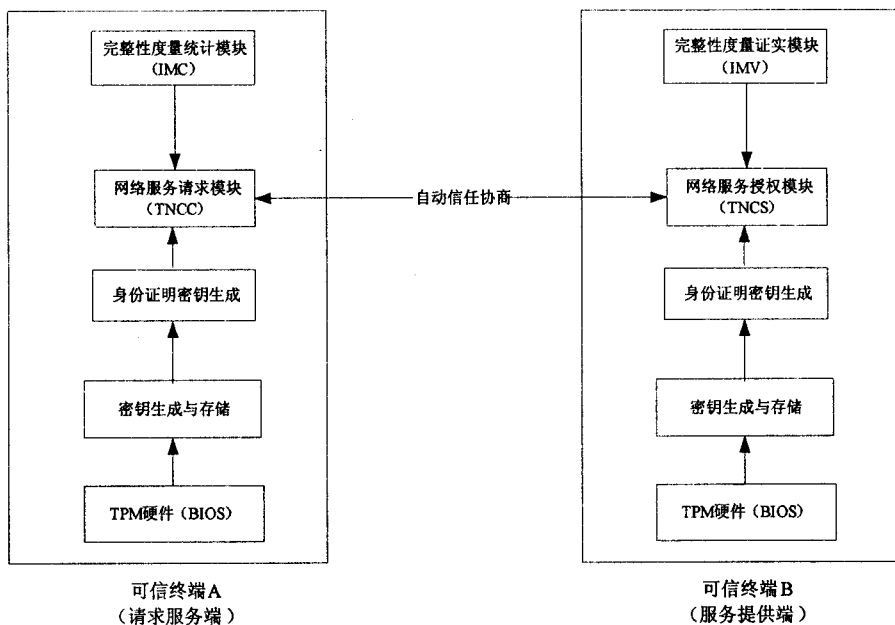


图1 基于自动信任协商的可信网络结构

完整性统计模块^[7](Integrity Measurement Collector, IMC)也是一个运行在服务请求端上的软件组件,报告服务请求端整体的安全情况,包括服务请求端上的反病毒参数设置、个人防火墙状态等,以及服务请求端上的其它安全情况。可信网络的基本思想是一个可信网络的客户端或服务端拥有多个 IMCs 关联,因此允许用户配置包括一定范围安全产品的完整性策略。

2) 服务提供端是指根据服务实施服务请求端请求决策的模块。可信网络服务授权模块(简称 TNCS)决定是否同意客户端访问的一个组件,验证服务请求端的完整性度量是否遵从了策略执行模块的安全策略。同时管理 IMVs 和 IMCs 之间信息流的组件,它收集来

自 IMV 的行为建议,并把这些基于策略的建议整合成完整的 TNCS 建议。

完整性度量模块^[8] (Integrity Measurement Verifier, IMV)则是一个证实服务请求端完整性特殊方面的组件,证实是基于来自于 IMCs 或其它数据信息源的测试。

2.2 可信网络的访问控制策略

访问控制策略是 ATN 的核心内容,规定了访问受保护资源所需提供的信任证集,虽然 Internet 具有多变性,但必须要求策略语言简洁具有可描述性,所以访问控制策略需要合理的约束,才能保证 ATN 的可应用性。可信计算平台的 TPM 正好提供了这种合理的控制策略。在 TPM 中存储着两种密钥:凭证密钥 (Endorsement Key, EK) 和身份认证密钥 (Attestation Identity Key, AIK),凭证密钥 EK 是一个模长 2048 比特的 RSA 公私钥对,在 TPM 内部产生,永远不会暴露在 TPM 外部。EK 的公钥部分包含在 TPM 所存储的凭证证书中,该证书用以提供平台的真实性证明,对一个 TPM 而言,EK 是唯一的。身份认证密钥 AIK 用来提供平台的身份证明,而这些密钥和凭证不仅为网络实体提供了可靠的身份标识,同时它们的硬件存储方式从根本上也防止了敏感信息的泄漏。

2.3 可信网络的协商策略

可信网络的本质是建立实体匿名验证,并在一对终端之间建立一个安全通道。自动协商理论为这种安全通道的建立提供了理论支持,Winsborough 等人^[6]将协商状态抽象为资源请求方和提供方之间信任证披露序列 $Q = \{C_1, C_2, \dots, C_n\}$ 的构造过程,如果协商过程中每份信任证 C_i 都是可公开的,则称 Q 为安全披露序列 (safe disclosure sequence)。在协商双方对隐私信息的自治保护技术控制即可信计算硬件平台控制下,这个协商过程可以描述为类似于 TCP 协议的协商过程,主要是在终端之间建立连接前完成可信信息的相互披露。图 2 是协商策略的实施过程。

这个协商过程可以分为两个部分:可信平台认证和完整性检测握手过程。

●可信平台认证阶段:

服务请求端开始一个网络连接请求和完整性检测握手尝试,TNCC 会发现这些请求并加载每一个相关 IMC 的特殊平台绑定。TNCC 进而对 IMC 进行初始化,主要是初始化定义必要连接的 IDs 和 IMC IDs,确

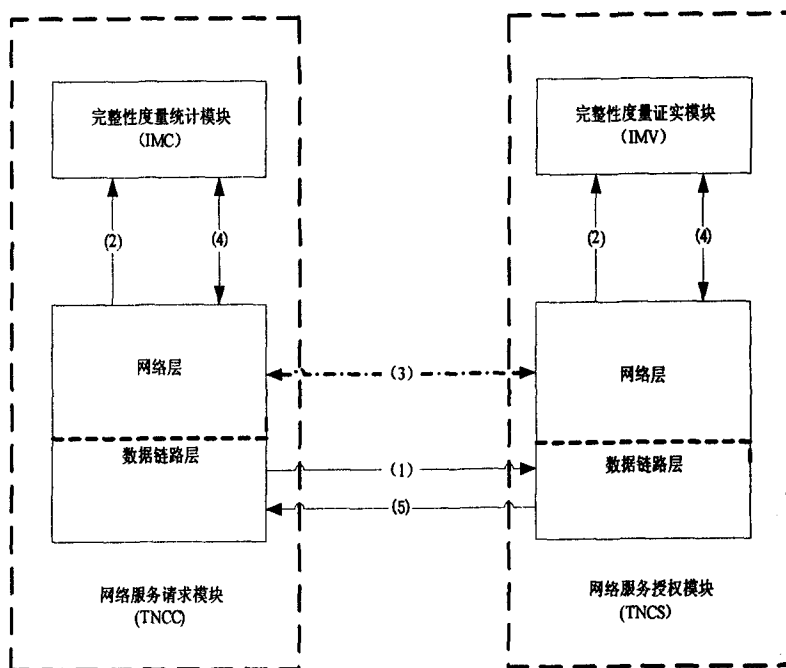


图 2 协商策略实施过程

保 TNCC 有一个和 IMC 合法的连接状态。

在这个初始化过程中,TNCC 可能检测 IMCs 的完整性,这种检测就是对 IMCs 进行 hash(哈希)处理,并且把哈希值添加到 PCR 中,这个添加过程为 $PCR[n]_i \leftarrow SHAI(PCR[n]_{i-1} || measureddata)$,在 TPM 中最少有 16 个 PCR,每个 PCR 是 TPM 内部的一个 20 字节的存储区域,总长度为 160 个比特,保存测量值的累计摘要,由历史数据组成,其中 i 是 PCR 被更新的次数。TNCS 和 IMV 可以在时间顺序发生过程中得到终端平台证明的机会。相似的,TNCS 必须用特殊平台绑定的方法加载每一个和 IMV 相关的信息。当一个网络连接尝试被发起后,无论是自动的还是由用户发起的,在服务请求端的链路层和网络层初始化一个连接请求。

(1) TNCS 在接受到一个来自 TNCC 的网络连接请求后,会认为该请求已经实施了用户证明、平台可信证明和完整性检测握手。用户证明发生在 TNCS 和服务请求端之间,平台可信证明和完整性检测握手也可以发生在服务请求端和 TNCS 之间。由于证明过程已经开始,任何一个验证失败都会导致其他的验证和完整性检测中止。也就是说,假如用户和 TNCS 之间的用户证明失败,那么平台可信证明和完整性检测握手过程就不会继续执行。

如果服务请求端上的用户和 TNCS 之间的用户证明成功,则表示本次连接请求的协商第一步结束。

●完整性检测握手阶段:

TNCS 和 TNCC 协商完成共有的平台可信证明。

比如说:有效的可信 AIK(AIK 是由 TPM 生成的, TPM 只可以有一个 EK,但是可以有多个 AIK,AIK 用来保护 EK 的私密性,TCG 规定 EK 永远不能被泄露)会在所有终端间被使用。

(2)如果 TNCC 和 TNCS 之间的平台可信证明成功,TNCS 会告知 IMVs 一个新的连接请求已经发生,并且完整性检测握手协议需要 TNCS 执行。同样的,TNCC 也会通知 IMCs 一个新的连接请求已经发生并且一次完整性检测握手过程已经被 TNCC 执行。IMCs 会回发一些 IMC-IMV 之间的通信信息给 TNCC。

(3)为了执行完整性检测握手过程,TNCS 和 TNCC 会互通信息完成完整性检测。这些信息会持续到 TNCS 满意 AR 的完整性状态为止。

(4)TNCS 会把每一个 IMC 信息和 IMV 进行匹配。每一 IMV 都会分析 IMC 信息,如果一个 IMV 需要和 IMC 交换更多的信息,它会提供一个信息给 TNCS。如果 IMV 准备决策出一个 IMV 行为建议和 IMV 评估结论,它会把这些向 TNCS 进行汇报。同样的,TNCC 会发送来自 TNCS 的信息和 IMC 进行匹配,并且把来自 IMCs 的信息传送给 TNCS。当 TNCS 完成了它和 TNCC 的完整性检测握手后,它会形成 TNCS 的行为建议。当然,TNCS 也可能因为其他的安全策略请求还没有被 AR 满足而不同意访问请求,即使 AR 已经通过了完整性检测。

(5)TNCS 会发送它的网络访问决定给控制策略执行模块去执行,当然 TNCS 也会把它的最终决定提交给 TNCS,再由 TNCS 提交给 TNCC。

当该协商过程结束后,AR 就可以对被保护网络资源进行访问了。

3 应用示例

下面举例说明基于自动信任协商的可信网络的实现过程。

P2P(Peer to Peer)网络结构^[9,10]区别于 Client/Server 结构或 Browser/Server 结构最显著的特点是整个网络不存在中心节点(或中心服务器),其中的每一个节点(peer)大都同时具有信息消费者、信息提供者和信息通讯等三方面的功能。但是结构化的 P2P 面临的问题之一就是节点之间的相互认证的问题,以及如何防止恶意的节点加入到覆盖网络中。另外结构化的 P2P 系统虽然之间可以采用 hash 表的方式进行查询,消息冗余较小,但是在查询过程中同样存在由于虚假查询引发的拒绝服务问题,只是程度和利用的方式不同。因此采用基于自动信任协商的可信网络的完整性验证和汇报机制可以有效地解决这一问题。现有

的具体应用是:P2P 网络中每个节点平台都支持 TCG 可信平台规范,并具有相应的凭证证书,在 P2P 网络拥有一个唯一的标识。

P2P 网络中节点代号是形式为 $N_p = f^p$ 的字符串,其中 f 是来自网络的名字,利用一个哈希函数进行转换,是 TPM 对节点 P 的代号密值,从而产生匿名代号。通过使用匿名代号机制,某个节点的行为将具有一定的相关性。因为基于自动信任协商的凭证验证并不泄漏平台标识(EK),所以节点的行为和特定的 TPM 无关,因此代号可以有效地保护节点的行为,而且代号只和特定平台的 TPM 相关。一个给定的节点可能需要在不止一个 P2P 网络中活动,通过网络名来确定密钥得到代号,可以保证在不同的网络中,节点的行为依旧保持不相关性,从而有效地保障了 P2P 网络中节点的私密性和安全性。

4 结束语

网络系统的安全性是保证一个应用能够在所有重要领域中使用的基础,而在网络应用日益广泛的今天,要构筑一个可信安全的资源共享环境,需要参与网络的各个终端的安全(可信计算保证)以及通信双方的访问安全,基于自动协商信任的可信网络的提出为构建这种“立体”的网络安全模式提供了理论依据,今后的研究重点是如何保证可信网络中信息流的安全传递,真正做到终端安全、访问控制安全再到信息流传递的“立体”安全网络。

参考文献:

- [1] CG Specification Architecture Overview Specification (Revision 1 - 2) [EB/OL]. 2004. <https://www.trustedcomputinggroup.org/downloads/TCG-1.0-Architecture-Overview.pdf>.
- [2] Trusted Mobile Platform Specification Hardware Architecture Description [EB/OL]. 2004. http://www.trustedmobile.org/TMP_HWAD_rev100.pdf.
- [3] 李 菲,乔佩利.网络深层防御体系模型的研究与实现[J].计算机技术与发展,2008,18(2):87-90.
- [4] Trusted Computing Group(TCG). TCG Specification Version 1.2 Revision 62. TPM Main Part 1: Design Principles[EB/OL]. 2003 - 10. <https://www.trustedcomputinggroup.org/downloads/tpm1p-mainrev-62-Part-1-Design-Principles.pdf>.
- [5] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation[C]//In: DARPA Information Survivability Conf. and Exposition. New York: IEEE Press, 2000: 88 - 102.

应曲线如图 4 所示。

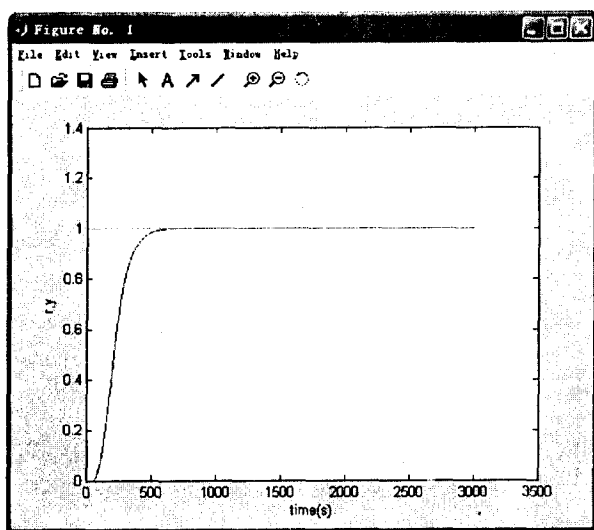


图 3 基于 BP 神经网络的 PID 控制器仿真结果

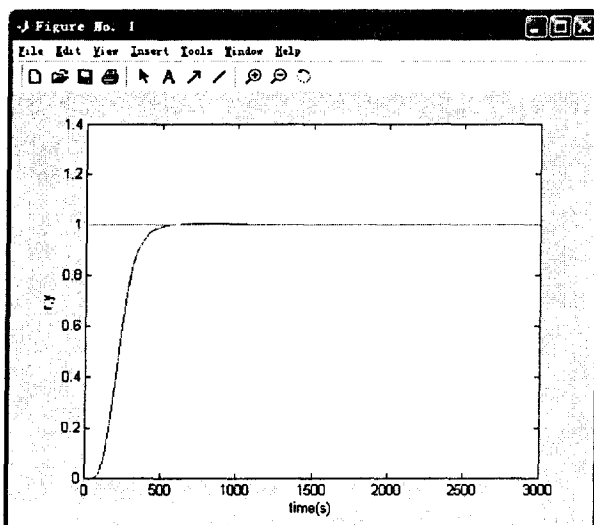


图 4 单神经元自适应 PID 控制器仿真结果

从仿真结果可以看出,基于神经网络的 PID 控制可以取得较好的自适应效果。基于 BP 神经网络的非线性学习能力优于单神经元,然而容易陷入局部极小解。单神经元 PID 结构简单,容易实现,但是神经元比例系数必须离线调整。

5 结束语

传统的 PID 温度控制方法,在实施控制之前必须进行被控对象的参数辨识,在很大程度上影响了控制的效率。神经网络以其强大的非线性学习能力著称,利用误差进行网络权值调整,从而实时校正 PID 控制器的参数,可以达到较好的自适应控制效果,在吹瓶机的温度控制系统中有一定的应用价值。从基于 BP 神经网络和基于单神经元的 PID 控制算法的比较不难看出:BP 神经网络结构较复杂,适合于单片机中使用;而基于单神经元的算法简单易实现,适合于 PLC 中使用。然而,神经网络有其自身难以克服的缺陷,如容易陷入局部极小值、神经网络结构参数设置缺少理论依据等问题,利用神经网络进行的 PID 控制尚有改进的空间。

要实现真正智能的理想控制,还应该寻求同其他优化算法如模糊控制、遗传算法、人工免疫算法等的互补结合。

参考文献:

- [1] 刘 璟,梁昔明.一种结合数值优化的 PID 控制器的设计与仿真[J].计算机技术与发展,2007,17(4):24-26.
- [2] Astrom K J. Toward intelligent control[J]. IEEE Control System Magazine, 1989,47(2):60-64.
- [3] 陶永华.新型 PID 控制及其应用[M].北京:机械工业出版社,2002.
- [4] Anderson J A. Introduction to Neural Networks[M]. Cambridge, MA: MIT Press, 1995.
- [5] Kumar S. Neural Networks(影印版)[M].北京:清华大学出版社,2006:199-201.
- [6] 李祥飞,邹莉华.基于混沌变量优化的神经网络 PID 控制[J].计算技术与自动化,2008(3):35-38.
- [7] 李英春,王孟效.基于 BP 神经网络 PID 的漂白温度控制算法的研究[J].微计算机信息,2006,22(12-1):41-42.
- [8] 孟志达.智能控制在退火炉温度控制中的应用研究[D].天津:天津大学,2006.

(上接第 153 页)

- [6] 赵纪涛,马 莉,王现君,等.一种自适应的模糊关联规则挖掘算法[J].计算机技术与发展,2008,18(5):43-46.
- [7] Trusted Computing Group. TNC IF-IMC Specification v1.2 [EB/OL]. 2007-02. <https://www.trustedcomputinggroup.org/downloads/TCG-3.0 Architecture Overview.pdf>.
- [8] Trusted Computing Group. TNC IF-IMV Specification v1.2 [EB/OL]. 2007-02. <https://www.trustedcomputinggroup.org/downloads/TCG-4.0 Architecture Overview.pdf>.
- [9] Balfe S, Lakhani A D, Paterson K G. Securing peer-to-peer networks using trusted computing[M]. [s. l.]: IEEE Press, 2005:271-298.
- [10] Sailer R, Zhang R. Design and implementation of a TCG-based integrity measurement architecture[C] //Proceedings of the 13th Unix Security Symposium. San Diego: [s. n.], 2004.