IPSec协议的远程证明扩展

王 剑[1,2] 汪海航[1] 杨 健[1,3]
(同济大学电子与信息工程学院 上海 201804)[1] (河南科技大学电子与信息工程学院 洛阳 471003)[2]
(大理学院数学与计算机学院 大理 671003)[3]

摘 要 传统IPSec协议在建立安全通信连接时,没有考虑终端自身安全问题,而可信计算的远程证明机制就是为被接入方提供接入方的自身安全证明,将其引入IPSec协议可以弥补建立IPSec连接时的终端安全漏洞。首先分析了IPSec协议的IKE协商过程和可信计算技术的远程证明机制,然后以基于数字签名的IKE主模式流程为例,提出在IKE协商阶段引入远程证明机制的IPSec远程证明扩展协议流程及安全分析。该协议引入带有SKAE扩展项的身份证书,实现对终端身份和系统完整性的双重认证,确保端到端的安全连接。协议在保证通信信息的机密性、完整性、新鲜性之外,也充分保护终端平台隐私性。

关键词 IPSec,IKE协商,远程证明,可信计算,完整性度量
中图法分类号 TP309 **文献标识码** A

Remote Attestation Extension for IPSec

WANG Jian[1,2] WANG Hai-hang[1] YANG Jian[1,3]
(School of Electronics and Information, Tongji University, Shanghai 201804, China)[1]
(School of Electronics and Information Engineering, Henan University of Science and Technology, Luoyang 471003, China)[2]
(School of Mathematics and Computer Sscience, Dali University, Dali 671003, China)[3]

Abstract Standard IPSec doesn't provide any guarantees about the integrity of the endpoints when an IPSec linkage is established. And the remote attestation in trusted computing is to provide security evidence of the user for the accessed server. So it can avoid terminal security vulnerability in IPSec to introduce the remote attestation into IPSec. IKE negotiation of IPSec and remote attestation mechanism were analyzed firstly. Then taking IKE main mode based on figure signature for example, an extended IPSec protocol based on remote attestation and its security analysis were presented. In the extended IPSec protocol, remote attestation mechanism was introduced into IKE negotiation. This protocol can complete double authentications including identity and system integrity by using a certificate with a SKAE extension to ensure an end-to-end secure linkage. Besides, the protocol can guarantee not only information's confidentiality, integrity and freshness, but also endpoints' privacy.

Keywords IPSec, IKE negotiation, Remote attestation, Trusted computing, Integrity measurement

1 引言

传统通信安全协议的认证方法中,网络认证设备都只以待接入设备是否掌握认证协议需要的口令或密钥来判断待接入设备是否可以接入受保护的网络,而不关心待接入设备本身是否是安全可信的,没有真正建立从端到端的安全连接。TCG(Trusted Computing Group,可信计算组)在文献[1]中提出了在建立可信网络连接时进行远程证明的思想,从终端入手解决安全问题,为端到端的安全连接提出了很好的解决思路和弥补办法。那么如何将可信计算的远程证明思想和传统网络安全接入技术结合在一起,真正实现从接入源头开始的安全保障非常值得深入研究,也已经引起许多研究者的关注和探讨。如文献[2-5]等都分别介绍了在TLS协议中融合远程证明的不同方法。文献[6,7]都认为以上方法均有不足,其中文献[6]提出了基于口令认证和TPM证明的可信通道的建立方法,文献[7]提出了基于OpenSSL的可信通道的实现方法。这些文献都以TLS/SSL协议为例讨论传统协议和可信技术的融合,而本文以另一个常用的传统安全协议IPSec为例对此问题进行研究,将其与TCG组织提出的可信计算的远程证明机制相结合,通过对IPSec协议的远程证明扩展,在建立IPSec连接时,不仅完成终端身份认证,而且进行终端平台完整性认证,在终端和服务器之间建立一条远程端对端的可信通道。

2 可信计算远程证明机制

"可信计算"技术的核心是被称为"可信平台模块"(TPM)

到稿日期:2010-07-21 返修日期:2010-11-12 本文受国家863计划项目(2006AA01Z438)资助。
王 剑(1978—),女,博士生,讲师,主要研究方向为信息安全,E-mail:wangjian_migi@sina.com;汪海航(1965—),男,博士,教授,主要研究方向为信息安全、智能信息系统、电子商务;杨 健(1976—),男,博士生,讲师,主要研究方向为智能信息系统。

的安全芯片，完成可信度量的存储、可信度量的报告、密钥产生、加密与签名，以及数据安全存储等功能。通过在计算机系统中嵌入一个可抵制篡改的独立计算引擎，使非法用户无法对其内部数据进行更改，从而确保了身份认证和数据加密的安全性，通过这一系列安全特性来提高终端系统的安全性。

2.1 远程证明思想

远程证明是为了确保加载在远程主机的可执行映像和应用程序执行环境的安全而产生的，特别是确保安全边界外的计算设备可信性。远程证明过程中，待证明系统为了证明的需要，将系统所有模块信息和相关配置发送给质询方，向质询方提供其平台上自引导开始之后运行过的所有组件信息——包括名字、版本，质询方获得了待证明系统的相关信息后便可推断出系统的当前状态以及预测其后续行为。服务器利用远程证明机制限制客户应用，通过针对性地选择远程的应用程序，可防止恶意程序或者可能被利用的有缺陷应用对服务的滥用，防止误用木马程序、避免与恶意的终端连接[8]。通过这些限制，达到增强终端可信性，加强系统安全的目的。

2.2 远程证明系统结构

远程证明要求被验证的计算设备发送某些数据结构到质询方，用于证明其身份和状态。这种数据结构就是证明向量，是本地主机当前状态的声明，能够使质询方远程验证计算机设备当前的运行环境状态。质询方通过远程证明机制，可以得到被验证的计算设备的可信度量报告，依据此来推断出被验证的计算设备的安全状态，评估当前平台的可信度，从而可以根据该平台的可信级别来实施他们认为能够在该级别下实施的操作。

远程证明系统结构主要由三部分组成：完整性度量机制、证明机制以及验证机制。TPM 的完整性度量机制定义了度量的内容，并保证证明向量是由本地主机产生的，能正确反映本地主机当前安全状态，且能够抵抗来自本地主机的恶意用户的攻击；证明方通过证明机制用 TPM 的 PCR（平台配置寄存器）保存在可信链建立过程中生成的度量值，并用 AIK（身份证言密钥）私钥签名，阻止恶意主机伪造证明向量；质询方则通过验证机制验证可信报告中的完整性度量信息，对证明方的可信性进行评估。证明向量通过网络传送到远程主机时，必须保证其在传输过程中的机密性和完整性。

2.3 远程证明过程

在 TCG 规范中[9]描述了远程证明过程，如图 1 所示，远程证明包含以下几步：

1. 质询方请求获取被验证平台的相关信息；

2. 驻留在被验证平台的代理收集 TPM，SML（存储度量日志）等相关实体信息；

3. 驻留在被验证平台的代理从 TPM 得到当前 PCR 值；

4. TPM 用 AIK 密钥对 PCR 值签名；

5. 代理收集 TPM 身份证书、被签名的 PCR 值和 SML 等信息，发送给质询者；

6. 质询者验证应答，验证签名和证书，检查 SML。

远程证明机制的实施是与具体的下层传输协议无关的，其中 PCR 为 TPM 专门提供的受保护区域、外部程序只能通过专用的接口访问，用于保存在可信链建立过程中生成的度量值。SML 中包含按可信度量顺序保存的相关度量事件日志。

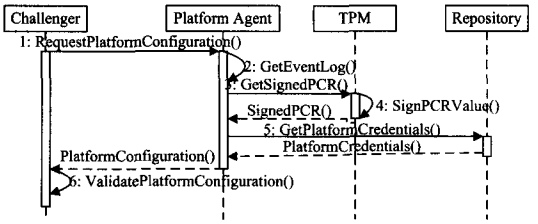

图 1 TCG 远程证明过程

3 IPSec 协议

IPSec 是一种在 IP 环境下支配安全管理的标准技术，由 Internet 工程任务组（IETF）开发。IPSec 能够减少利用 IP 欺骗进行 Internet 攻击的威胁，可以大大促进对安全要求严格的应用，如电子商务、虚拟专用网（VPN）、Extranet 等应用的发展。IPSec 可以有效保护 IP 数据报的安全，所采用的具体保护形式包括数据源验证、无连接数据的完整性验证、数据内容的机密性保护、抗重播保护等。IPSec 通过使用 AH（认证头）、ESP（封装安全载荷），以及 IKE（因特网密钥交换）协议来达到这些安全目标。

AH 为 IP 数据包提供无连接数据完整性和数据源身份认证，同时具有防重放攻击的能力。ESP 为 IP 数据包提供数据的保密性（加密）、无连接的数据完整性、数据源身份认证以及抗重放攻击保护。而 IKE 协议用于协商 AH 和 ESP 协议所使用的密码算法，并将算法所需的必备密钥放在合适的位置。因此，建立远程可信 IPSec 连接是通过基于 IKE 协议的协商来提供相互身份认证和信息加密密钥的。也就是说，讨论 IPSec 协议的远程证明扩展其实就是对 IKE 协议的远程证明扩展。

3.1 IKE 协议

IKE 协议是一个以受保护的方式为 SA（安全关联）协商并提供经认证的密钥信息的协议。IKE 协议是 IETF 定义的一种混合型协议，使用了 3 个不同协议的相关部分：ISAKMP（Internet 安全关联和密钥交换协议）[MSST98]、Oakley 密钥确定协议[Orm98]和 SKEME[Kra96][10]。

IKE 由两个阶段组成：第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步的 IKE 通信提供机密性、消息完整性以及消息源验证服务；第二阶段，使用已建立的 IKE SA 建立 IPSec SA。IPSec 的目标是相互认证和保护 IP 包，而相互认证事实上已经在 IKE 第一阶段完成，因此对 IKE 协议的远程证明扩展就是对 IKE 协议的第一阶段协商的远程证明扩展，也就是在此阶段的协商中除了身份的认证外，扩展可信度的证明和验证，如果证明方的可信度量结果不能符合质询方的要求，则协商失败，不必再进行第二阶段的 IPSec SA 的建立。

3.2 IKE Phase 1

IKE 阶段 1 有两种模式的交换：对身份进行保护的“主模式”交换以及根据基本 ISAKMP 文档制定的“野蛮模式”交换。主模式交换将密钥交换信息与身份、认证信息分离，从而保护了身份信息，身份信息受到了前面生成的 Diffie-Hellman 共享密钥的保护，共需要 6 条消息。野蛮模式允许同时传送与 SA、密钥交换和认证相关的载荷，减少了消息的往返次数，但无法提供身份保护功能。本文以主模式为例说明 IKE 的远程证明扩展，主模式有 4 种不同的身份验证方法：预共享密

钥(PSKEY)、数字签名、标准公钥加密和修订公钥加密。不同的验证算法提供的安全强度不同,使得交换消息的内容也各不相同,但达到的目的是完全一致的,最终都是生成安全通道 SA。不管对于哪一种验证方式,双方都要分别计算 SKEYID 值,它是所有会话密钥生成的基础,为衍生下一级双方共享的密钥材料做准备。总的来说,其分为基于数字证书和预共享密钥两种方式。基于预共享密钥身份验证的方式,相对来说是一种比较弱的身份验证方法而且在远程访问应用中具有明显局限性[11]。本文以基于数字证书认证方式中的数字签名主模式流程为例说明 IKE 协商的远程证明扩展。基于数字签名的主模式消息流程如图 2 所示[10]。

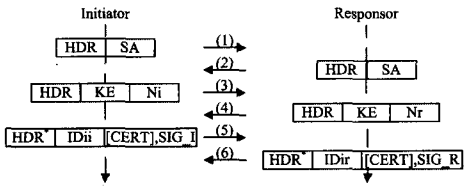

图 2 基于数字签名的主模式消息流程

SIG_I 和 SIG_R 是散列的签名。这里的 5,6 消息中增加了可选的载荷,可进行证书的交换,验证的是散列的签名而不仅仅是散列。

4 在 IKE 协商阶段中引入远程证明的 IPSec 扩展协议

4.1 可信连接建立涉及的密钥及证书

证言身份密钥(AIK):对应一组公私密钥对,专门对来源于 TPM 的数据进行签名,实现对运行环境测量信息进行签名从而提供计算平台环境的证言。凡是经过 AIK 签名的实体,都表明已经经过 TPM 的处理。AIK 只用于签名 TPM 内部产生的数据,对于上层数据的签名必须使用其它签名密钥进行。特别地,AIK 只对不可迁移密钥进行证明。

AIK 证书($Cert_{AIK}$):AIK 证书是在终端用户向私有 CA(Privacy CA)提交申请之后由私有 CA 产生[12],用来证明 AIK 的合法性。申请 AIK 证书时需要向私有 CA 提交 EK 证书、平台证书和一致性证书。AIK 证书不能取代一般的公钥证书作为验证上层应用数据签名的公钥分发证明。

证明加密密钥(K_{enc}):非对称密钥对 K_{enc} 是一对不可迁移密钥,可以调用 TPM_CreateWrapKey()函数,在需要建立安全连接之前创建,并由 AIK 对其进行证明。AIK 的私钥由于只能用于签名 TPM 内部产生的数据,因此不能对由 TPM 外部实体产生的数据进行处理,而在认证会话中 TPM 外部数据进行加密或签名是难以避免的,因此引入 K_{enc} 作为会话建立时需要的密钥。

K_{enc} 证书($Cert_{enc}$):K_{enc} 证书是带有 SKAE(主题密钥证言证据)扩展项[13]的 X.509 v3 证书,用来替代 IKE phase1 协商中的证书证明终端身份。SKAE 证书扩展项中有一个结构 TPMCertifyInfo,该结构实际是由 TPM_CERTIFY_INFO 结构与该结构的签名组成。TPM_CERTIFY_INFO 结构中包括 PCR 值以及证书中主题公钥的摘要值 pubkeyDigest。TPM_CERTIFY_INFO 的签名是由 AIK 的私钥完成,因此在验证 TPMCertifyInfo 时,应使用 AIK 的公钥。通过验证 SKAE 扩展项中的 AIK 签名以及主题公钥 PK_{enc} 的摘要可以使验证方相信 K_{enc} 受到 TPM 保护并且密钥操作都在 TPM 内部完成。带有 SKAE 扩展项的 $Cert_{enc}$ 证书如下所示:

$Cert_{enc}$:={serial_no, issuer, subject, PK_{enc}, TPM_CERTIFY_INFO, sign{TPM_CERTIFY_INFO} SK_{AIK}, sign{$Cert_{enc}$} SK_{CA}}

4.2 远程证明扩展的 IKE 交互流程

4.2.1 相关标识与算法公式

HDR:ISAKMP 头,其交换类型就是交换的模式。加 * 号表明 ISAKMP 头后面的载荷是加密的;

CK-I:ISAKMP 头中的发起者 cookie;

CK-R:ISAKMP 头中的响应者 cookie;

SA:带有一个或多个建议载荷的安全关联载荷;

DH-X=g^x mod p:发起者的 Diffie-Hellman 公开值;

DH-Y=g^y mod p:响应者的 Diffie-Hellman 公开值;

Ni/Nr:20(或者 16)字节随机数;

IDx:表示载荷,x 是 ii 或 ir,ii 表示 ISAKMP 发起者,ir 表示 ISAKMP 响应者;

〈P〉_b:载荷〈P〉的主体,即没有 ISAKMP 头的载荷;

SKEYID=PRF (Ni_b | Nr_b, g^{xy});

SKEYID_d=PRF (SKEYID, g^{xy} | CKY-I | CKY-R | 0),用于产生 IPsec SA 的密钥;

SKEYID_a=PRF (SKEYID, SKEYID_d | g^{xy} | CKY-I | CKY-R | 1),用于认证后继的 ISAKMP 消息的密钥;

SKEYID_e=PRF (SKEYID, SKEYID_a | g^{xy} | CKY-I | CKY-R | 2),用于加密 ISAKMP 交换的密钥;

HASH_I=PRF (SKEYID, DH-X | DH-Y | CKY-I | CKY-R | SAi_b | IDii_b);

HASH_R=PRF (SKEYID, DH-Y | DH-X | CKY-R | CKY-I | SAi_b | IDir_b);

SIG_I:被签名的 HASH_I 载荷;

SIG_R:被签名的 HASH_R 载荷。

4.2.2 交互信息流程

经过远程证明扩展的基于数字签名的 IKE 第一阶段交互流程如图 3 所示。这里只描述了 IPSec 用户终端向服务器端进行单方面完整性证明的过程,也可进行双向完整性证明,服务器端向终端进行完整性证明过程同理。交互流程基于 TCG 规范中的远程证明架构及证明过程,整个设计的原则是除可信计算基(TPM 芯片)之外的任何实体都不可以直接接触身份、密钥和证书等隐私信息。因此,远程证明代理只作为 IKE 协商过程的门户,整个过程又分为以下 3 个阶段。

协商安全参数:IPSec 终端平台的远程证明代理作为连接的发起者 Initiator 向 TPM 发出建立 IKE 连接请求,TPM 收到请求生成 cookie(CK-I)并返回。远程证明代理向响应者 Responsor 即 IPSec 服务器发送封装有建议载荷的 SA 载荷,就 4 个强制性参数值进行协商:(1)加密算法:选择 DES,AES 或 3DES 等;(2)hash 算法:选择 MD5 或 SHA;(3)认证方法:选择证书认证、预置共享密钥认证或 Kerberos v5 认证;(4)Diffie-Hellman 组的选择。响应者生成自己的 cookie(CK-R),并发送 SA 载荷,表明它所接受的正在协商的 SA 建议。每个 SA 的 cookie 是独一无二的,一个可能生成 cookie 的方法是采用 MD5、SHA-1 或其他支持的杂凑函数对通信方源地址、目的地址,UDP 源端口、目的端口,本地生成的保密随机

数和当前的日期、时间的连接进行杂凑运算。

交换 DH 公开值：远程证明代理向 TPM 发出 DH 交换请求，由 TPM 计算 DH 公开值，并生成 nonce，nonce 是计算共享密钥所必需的。双方进行 DH 值交换，即可各自生成完全一样的共享主密钥，保护紧接其后的认证过程。

身份及完整性验证：远程证明代理向 TPM 发出认证请求后进入 IKE 协商的第三阶段。TPM 接到请求，生成认证载荷，并对响应方需要验证的所有 ISAKMP 载荷用 SKEYID_e 加密。加密后的 ISAKMP 包由远程证明代理发送给响应方。响应方用 SKEYID_e 对 ISAKMP 包解密后，依次进行以下验证：

(1)解析身份载荷，并用来验证签名载荷；

(2)验证 AIK 证书的有效性及合法性，这可以通过 SKAE 扩展项中的 TpmIdentityCredentialAccessInfo 索引到 AIK 证书，在验证 AIK 证书的有效性后获得 AIK 公钥；

(3)验证 Certenc 证书中 SKAE 扩展项的签名字段，即验证 TPM_Certify_Info 的 AIK 签名；

(4)验证主题公钥的完整性，即计算 Certenc 证书中的 PKenc 摘要，与 TPM_Certify_Info 结构中的公钥摘要值域 pubkeyDigest 进行比对，如果一致，则说明密钥的完整性得到了保证；

(5)验证 TPM_Certify_Info 结构中的 PCR 值，确认对方平台的完整性。以上 5 次验证中任何一次失败，即 IKE 协商失败。

3 个阶段若顺利完成，则 IKE Phase1 协商成功，双方获得共享密钥：SKEYID_d，SKEYID_a，SKEYID_e，所有密钥保存在 TPM 中，远程证明代理仅获得密钥句柄。

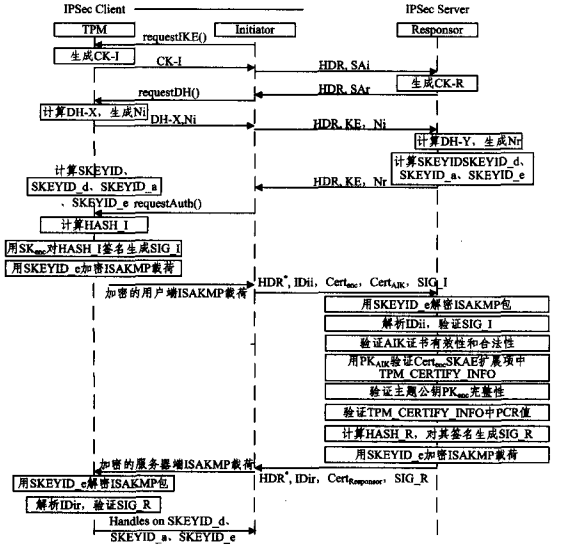

图 3　远程证明扩展的 IKE 交互流程

5　安全分析

将可信技术与传统安全协议相结合建立远程可信通信通道，应可以达到以下安全目标：(1)既具备传统远程安全通信通道的安全属性，即在双方得到认证的前提下保证通信数据的完整性、机密性、新鲜性等特点，又兼顾终端安全状态；(2)通信双方连接建立前除身份认证之外，还应进行平台自身完整性的认证；(3)在认证和交互过程中，应确保通信双方的平台配置、证书、密钥等隐私信息不泄漏给任何第三方或尽量减少不必要的隐私暴露[5]。可信计算技术和 IPSec 协议都具备各自的安全性能，我们提出的将可信计算与 IPSec 技术结合来建立的远程安全通信连接可以满足以上安全需求。

端到端的安全：IPSec 可以有效保护 IP 数据报的安全，在不安全的网络环境中为通信双方提供安全通道，提供数据源验证、无连接数据的完整性验证、数据内容的机密性保护、抗重播保护等安全性能，解决了信息的安全远程传输问题；而可信计算机制通过可信度量、可信存储、强隔离等措施保护和监控本地平台完整性，使终端平台的安全可见并可控。根据远程证明机制，通信双方相互提交和验证完整性报告，并在确认对方完整性符合本地安全需求后建立连接，使得终端安全被纳入通信安全保障边界，保证了端到端的安全。

完整的认证链：本文方案中使用带有 SKAE 扩展项的身份证书 Certenc 来替代原 IKE 协商过程中使用的普通证书，终端的身份及完整性认证通过 $Cert_{enc}$ 和 $Cert_{AIK}$ 组成的证书链来保证。$Cert_{enc}$ 由一个 CA 签名，并用其公钥验证有效性。$Cert_{enc}$ 扩展项中的 TPM_CERTIFY_INFO 结构由 AIK 私钥签名，并由 AIK 的公钥进行验证，其完整性和有效性保证了 PCR 值的可信。而同时，该结构中的公钥摘要值域 pubkeyDigest 的验证又保证了主题公钥 PK_{enc} 的完整性。通过这些签名和认证，可以向对方保证平台的完整性值及用于协商的密钥都是被密封和保护在同一个 TPM 内的，是可以被信任的。在验证过程中，如图 3 所示，验证方首先进行普通的身份认证，再进行证书链的合法性认证，最后进行完整性值的认证，确保了一条完整的认证链。

隐私的机密性：整个系统中，只有 TPM 被认为是可信的，本着这个原则，所有进行签名、加密的密钥和生成密钥的材料以及 PCR 值都被封存在 TPM 中，平台中的任何其他实体或者通信双方之外的任何第三者都不能获取或访问。而且所有的密钥操作和运算都在 TPM 内部完成，即使远程证明代理也只作为建立连接的门户，不参与任何明文的存取和计算，也只能获得最终共享密钥的句柄。另一方面，由于方案中加入了平台配置及完整性的验证，使得通信双方可以在验证对方符合自己的安全策略之后再建立连接，这在一定程度上避免了自己的隐私数据被恶意终端骗取和泄露。

结束语　传统的安全协议通过身份认证、加密传输等方式为信息的远程传输建立安全通道，然而这些协议都没有考虑终端安全问题，没有实现真正的端到端的安全。可信计算技术正是针对终端安全提供解决方案，通过远程证明机制向对方提供终端安全性证明。本文将可信计算技术与传统的常用安全协议 IPSec 相结合，提出 IPSec 的远程证明扩展协议，利用带有 SAKE 扩展项的身份证书替代普通的 IKE 协商证书，在建立连接之前，对终端不仅进行身份认证，而且进行完整性的评估和验证，为弥补传统安全协议缺失终端安全考虑的漏洞给出了解决思路，并在最后给出了协议的安全性分析。在今后的工作中，会更多考虑协议的性能改善，以适应越来越广泛的无线应用中移动终端的接入安全问题。

参 考 文 献

[1] Trusted Network Connect Work Group. TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.2 Revision 4[S]. 2007

[2] Jiang S, Smith S, Minami K. Securing Web servers against insider attack[C]// Proceedings of 17th Annual Computer Security Applications Conference. IEEE Press, 2001: 265-276

[3] Sadeghi A R, Stüble C, Wolf M, et al. Enabling fairer digital rights management with trusted computing[C]// Proceedings of ISC'07. LNCS 4779. Springer, 2007: 53-70

[4] Stumpf F, Tafreschi O, Röder P, et al. A robust integrity reporting protocol for remote attestation[C]// 2nd Workshop on Advances in Trusted Computing, WATC'06. 2006: 1-12

[5] Gasmi Y, Ahmad-Reza S, Patrick S, et al. Beyond Secure Channels[C]// Proceedings of the 2nd ACM Workshop on Scalable Trusted Computing, STC 2007. Alexandria, VA, USA, November 2007: 30-40

[6] Zhou Lingli, Zhang Zhenfeng. Trusted Channels with Password-based Authentication and TPM-based Attestation [C]// Proceedings of International Conference on Communication and Mobile Computing. 2010: 223-227

[7] Armknecht F, Gasmi Y, Sadeghi A-R, et al. An Efficient Implementation of Trusted Channels based on OpenSSL[C]// Proceedings of STC'08. Fairfax, Virginia, USA, October 2008: 41-50

[8] 林宏刚. 可信网络连接若干关键技术的研究[D]. 成都: 四川大学, 2006

[9] Trusted Computing Group. TCG Specifi_ cation Architecture Overview Specification's Revision1. 2[S]. https: // www. trustedcomputinggroup. org. Apr. 2004

[10] Davis C R. IPSec: VPN 的安全实施[M]. 北京: 清华大学出版社, 2002

[11] 范红. 互联网密钥交换协议及其安全性分析[J]. 软件学报, 2003, 14(3): 600-605

[12] Trusted Computing Group. TCPA Main Specification V1. 1b [S]. http: // www. trustedcomputinggroup. org/specs/TPM/TCPA_Main_TCG_Architecture_v1_1b. pdf, Sep. 2003

[13] 徐锐, 王震宇, 康新振. 可信计算环境证书机制中 SKAE 扩展项的分析[J]. 信息工程大学学报, 2008, 3(9): 90-93

(上接第 13 页)

[58] Sekar R, Bendre M, et al. A Fast Automaton-Based Method for Detecting Anomalous Program Behaviors[C]// Proceedings of the 2001 IEEE Sympo- sium on Security and Privacy. May 2001: 144

[59] Henry H F, Kolesnikov O M, et al. Anomaly Detection Using Call Stack Information[C]// Proceedings of the 2003 IEEE Symposium on Security and Privacy. 2003: 62-68

[60] Sekeh M A, Maarof M A. Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls[C]// Information Assurance and Security, 2009, IAS. 2009: 154-157

[61] Zhen L, Bridges S M, Vaughn R B. Combining static analysis and dynamic learning to build accurate intrusion detection models [C]// Proceedings of the 3rd IEEE International Workshop on Information Assurance. March 2005

[62] 李闻, 戴英侠, 连一峰, 等. 基于混杂模型的上下文相关主机入侵检测系统[J]. 软件学报, 2009, 20(1): 138-151

[63] Parampalli C, Sekar R, Johnson R. A practical mimicry attack against powerful system-call monitors[C]// Proceedings of the 2008 ACM symposium on Information, computer and communications security. Tokyo, Japan, March 2008

[64] Wagner D. Mimicry attacks on host-based intrusion detection systems[C]// Proceedings of the 9th ACM conference on computer and communications security. Washington, DC, USA, 2002

[65] Kruegel C, et al. Automating mimicry attacks using static binary analysis[C]// Proceedings of the 14th Conference on USENIX Security Symposium. Baltimore, MD, 2005: 11-11

[66] Chen Shuo, et al. Non-control-data attacks are realistic threats [C]// Proceedings of the 14th Conference on USENIX Security Symposium. Baltimore, MD, 2005: 12

[67] Sufatrio, Yap R. Improving host-based ids with argument abstration to prevent mimicry attacks[C]// Proceedings of the International Sypmosium on Recent Advances in Intrusion Detectino(RAID). 2006: 146-164

[68] Tandon G, Chan P. Learning useful system call attributes for anomaly detection[C]// Proceedings of the 18th International FLAIRS Conference. 2005

[69] Li Peng, et al. Bridging the Gap between Data-flow and Control-Flow Analysis for Anomaly Detection[C]// Computer Security Applications Conference, 2008. ACSAC 2008. Annual, 2008: 392-401

[70] Pang Jian-jing, Peng Xin-guang. Detection of Programs Behaviors on Context Dependency[C]// Networks Security, Wireless Communications and Trusted Computing. 2009: 382-385

[71] Giffin J T, Dagon D, et al. Environment-sensitive intrusion detection[C]// Recent Advances in Intrusion Detection(RAID). September 2005

[72] Kruegel C, Mutz D, Valeur F, et al. On the detection of anomalous system call arguments[C]// Proceeding of ESORICS 2003. Berlin, Heidelberg: Springer-Verlag, 2003: 326-343

[73] Tandon G, Chan P. Learning rules from system call arguments and sequences for anomaly detection[C]// ICDM Workshop on Data Mining for Computer Security(DMSEC). 2003: 20-29

[74] Maggi F, Matteucci M, Zanero S. Detecting Intrusions through System Call Sequence and Argument Analysis[J]. Dependable and Secure Computing, 2010, 7(4): 381-395

[75] Mutz D, Robertson W. Exploiting Execution Context for the Detection of Anomalous System Calls[C]// Proceedings of the International Symposium on Recent Advances in Intrusion Detection(RAID). Gold Coast, Australia, 2007: 1-20

[76] Mutz D, Valeur F, Vigna G, et al. Anomalous system call detection[J]. ACM Trans, Inf. Syst. Secur., 2006, 9(1): 61-93

[77] Tandon G, Chan P. On the learning of system call attributes for host-based anomaly detection[J]. International Journal on Artificial Intelligence Tools, 2006, 15(6): 875-892

[78] 李红娇, 李建华. 基于程序行为异常检测的数据流属性分析[J]. 上海交通大学学报, 2007, 41(11): 1778-1782

[79] 黄金钟, 朱淼良, 郭晔. 基于文法的异常检测[J]. 浙江大学学报: 工学版, 2006, 40(2): 243-248

[80] 罗隽, 丁力, 潘志松, 等. 异常检测中频率敏感的单分类算法研究[J]. 计算机研究与发展, 2007, 44(Suppl.): 235-239

[81] 伏晓, 谢立. 安全报警关联技术研究[J]. 计算机科学, 2010, 37(5): 9-14