文章编号:1001 - 9081(2006)12 - 2935 - 03

可信计算在 VPN 中的应用

刘宏伟,卫国斌
(北京科技大学 信息工程学院,北京 100083)
(iu_81@126.com)

摘 要:对虚拟专用网 VPN 进行了研究。VPN 使用户远程办公成为可能,但是 VPN 不能认证主机的配置,入侵者通过有 VPN 访问权限的主机获得非法的访问权限,使得终端不安全,同时相应的使网络接入也不安全。可以利用可信计算技术解决这些问题,其中可信平台模块通过绑定密钥认证 VPN 完整性,而可信网络连接认证网络连接安全性,以确保终端、网络接入和通信的安全可信。

关键词:虚拟专用网;可信计算;可信平台;可信网络连接
中图分类号: TP393.08 **文献标识码**:A

Application of trusted computing compliance in VPN

LIU Hong-wei, WEI Guo-bin
(*School of Information Engineering, Beijing Science and Technology University, Beijing* 100083, *China*)

Abstract: Virtual Private Network (VPN) was studied. VPN enables telecommunication, but it cannot authenticate the configuration of computers. If a computer used for VPN access was compromised, an attack could exploit it to gain unauthorized access and make endpoint insecure. When being connected to the corporate network, the computer becomes a distributor of the untrustworthy endpoint to other computers on the enterprise network. Trusted computing technology can be used to solve these problems. To guarantee the security and trustworthiness of the endpoints, network connection and communication, Trusted Platform Module (TPM) was used to bind keyed attestation to authenticate the integrity of VPN, and Trusted Network Connect (TNC) was used to authenticate the security of network connections.

Key words: Virtual Private Network (VPN); trusted computing; Trusted Platform Module (TPN); Trusted Network Connect (TNC)

0 引言

虚拟专用网(Virtual Private Network,VPN)利用公用互联网作为信息传输媒介,通过安全隧道,用户认证和访问控制等技术实现信息的安全传输,成本低,但同时其安全问题也更为突出。企业必需确保其 VPN 上传送的数据不被攻击者窥视和篡改,并且要防止非法用户对网络资源或私有信息的访问。但是 VPN 不能认证主机的配置,若主机本身不安全,有不安全的网络连接或被病毒感染,就不能保证终端信息安全。

作为网络终端的主机是发起对网络和网络中各类设备攻击的入口,终端的安全也就成为整个体系最重要的一个环节。而要解决终端安全问题,必须要有相应的硬件支持,可信平台模块可以用来增强主机安全,同时可信网络连接针对网络的安全性和完整性设计,防止不安全设备接入和破坏网络的机制,确保了终端的安全防护。

本文针对当前 VPN 的缺点,运用可信计算技术和相关认证,保证了信息在端点和传输过程中的安全。

1 可信计算关键技术

1.1 可信平台模块(Trusted Platform Module,TPM)

可信计算平台作为实现可信计算技术的核心,已经成为信息系统的基础性和平台性设备,其可信根源来自于可信平台模块 TPM。TPM 是一块嵌入在 PC 主板上的系统级安全芯片,它集成了数字签名、身份认证、信息加密、内部资源的授权访问、信任链的建立和完整性测量、直接匿名访问机制、证书和密钥管理等一系列可信计算所必须的基础模块,为各种安全应用提供了一个功能强大的平台。TPM 的构成如图 1 所示,其主要功能有:

1) 保护功能:用来保护和报告存储在 TPM 的平台配置寄存器 PCR(Platform Configuration Register)中的完整性测量值,提供密钥管理、随机数的生成和系统状态的封装。

背书密钥 EK(Endorsement Key)是 TPM 的可信任性的基础,产生于 TPM 内并存储在它的屏蔽区域,唯一标识一个有效的 TPM。使用 EK 只能通过保护功能,并要验证平台拥有者的授权或声明物理存在。

TPM 与一个可信计算平台通过物理方式绑定在一起,平台的拥有者向 TPM 中植入拥有者的授权数据来取得平台的拥有权。声明物理存在向 TPM 表明:当前拥有者正在本地操作该平台,TPM 对拥有者的后续操作给予足够的信任而不需要验证其他数据。读取 EK 的公钥部分,将拥有者口令的明文经 SHA-1 运算得到共享秘密信息,使用 EK 的公钥部分得到 OWNER 和 SRK 的加密的共享秘密信息,发送给 TPM。TPM 使用 EK 的私钥部分,解密共享秘密信息,将 OWNER 和 SRK 的共享秘密信息存储在屏蔽区域内。

TPM 可以产生多个身份证明密钥 AIK(Attestation Identity Key),用于对其提供的数据信息进行数字签名。在保护功能内,声明平台拥有者的授权数据产生一个 AIK。使用 SRK 对 AIK 的私钥部分及授权数据等敏感信息进行加密,加密后的

收稿日期:2006 - 06 - 20;**修订日期**:2006 - 08 - 25

作者简介:刘宏伟(1968 -),男,河北保定人,副教授,博士,主要研究方向:信息安全、计算机系统结构; 卫国斌(1981 -),男,山西万荣人,硕士研究生,主要研究方向:信息安全.

密钥保存在 TPM 的存储设备上。需要一个公正第三方为每个 AIK 颁发证书以证明 AIK 的可信及与 TPM 的绑定关系。AIK 的证书使用公正第三方的私钥对 AIK 的公钥及相关信息进行签名。公正第三方使用 EK 的公钥部分对 AIK 的证书进行加密,以保证该证书只能被 AIK 所绑定的 TPM 解密并使用。

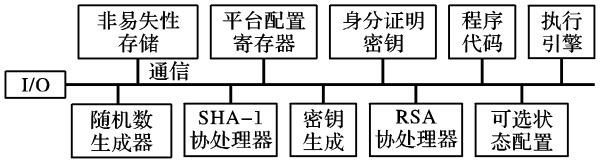

图 1 TPM 的构成

2) 完整性测量和存储:完整性测量是获得影响平台完整性的平台特性度量过程,封装存储则保护敏感数据并把度量存储在日志里,度量的摘要存于 PCR。TPM 有一个平台配置寄存器的集合,每个 PCR 为 20 字节,存放测量值的摘要。至少要有 16 个 PCR,对当前的值与新的测量值进行 SHA-1 操作得到新的 PCR。

3) 完整性报告:指完整性存储内容的证明过程,使用存储在 TPM 的屏蔽区域的私钥来保护。PCR 记录从启动到装载操作系统、装载应用软件的完整性和平台运行状态。平台进行完整性测量和存储,生成完整性报告并通过挑战协议向另一平台提供认证,PCR 的值用 AIK 签名。挑战者通过比较签名与期望值来验证平台的完整性、状态和配置。

4) 证明:验证远程平台是否可信的过程。证明是个协议,使远程 R 能够得到或认证主机 P 的测量日志,远程平台 R 发送给平台 P 一个值(nonce)。P 调用 TPM_Quote,包含 nonce 和当前 TPM 寄存器的值,用 AIK 进行签名。P 发送相应的 AIK 证书、引用值和测量日志给 R。R 用第三方的公钥来认证 AIK 证书,然后用 nonce 和 AIK 的公钥来认证引用值,再使用引用值来认证测量日志。

5) 评估和决定:当平台在通信时评估另一平台的完整性可信,需要评估双方执行同一策略的另一平台,评估结果包含可信级别。

6) 执行和响应:依赖评估平台的详细配置,平台把给定的特定策略集看成是策略执行点,并对评估的平台有相应的响应。

访问请求 AR(Access Requestor)把完整性测量报告给策略决定点 PDP(Policy Decision Point)获得网络的访问,根据访问请求执行评估和决定,把结果发送给策略执行点 PEP(Policy Enforcement Point)执行,TPM 起着很重要的作用。

1.2 可信网络连接技术

可信网络连接技术(Trusted Network Connection,TNC)是基于主机的可信计算技术,通过使用可信主机提供的终端技术,实现网络访问控制的协同工作。由于完整性校验被终端作为安全状态的证明技术,所以用 TNC 的权限控制策略可以估算目标网络的终端适应度。TNC 构架通过提供一个由多种协议规范组成的框架来实现一套多元的网络标准,提供如下功能:

1) 平台认证:用于验证网络访问请求者身份,以及平台的完整性状态。

2) 终端策略授权:为终端的状态建立一个可信级别,使终端被给予一个可以登录网络的权限策略从而获得在一定权限控制下的网络访问权。

3) 访问策略:确认终端机器以及其用户的权限,并在其连接网络以前建立可信级别,平衡已经存在的标准、产品及技术。

4) 评估、隔离及补救:确认不符合可信策略需求的终端机能被隔离在可信网络之外,如果可能执行适合的补救措施。

2 认证技术

2.1 封装认证

操作系统运行时,TPM 参考 VPN 参数进行锁定,若主机配置与以前文件日志存储相同,TPM 提供的数据封装为加密文件系统储存密钥,将测量数据记录在测量存储器内,最后的数据存储在 TPM 内。平台的代理程序收集存储于 TPM 内的最后数据、存储器保存的测量数据记录和 TPM 的确认数据,若平台正常运作,确认数据应与平台的测量数据吻合。在确定平台是否值得信赖之前,TPM 将密钥储存起来确保不会泄漏。也可在远程服务器上存储文件密钥,若主机的 TPM 是服务器可信的,服务器发送密钥给此操作系统和原始应用程序。

2.2 IPSEC 完整性认证

IPSEC 的 IKE 有两个阶段:第一阶段,协商创建一个通信信道(IKE SA),并对该信道进行认证,为双方进一步的 IKE 通信提供机密性、数据完整性以及数据源认证服务;第二阶段,使用已建立的 IKE SA 建立 IPsec SA。IKE SA 是双向的,决定第二阶段用来通信的加密算法和密钥,使用它协商认证包头 AH(Authentication Header)、封装安全负载 ESP(Encapsulating Security Payload)间的安全关联。AH 支持认证包头,ESP 支持认证包头和加密,第二阶段的协商决定了在 AH 和 ESP SA 使用的加密算法和密钥。在 IKE 的两个阶段使用 IKE SA 来执行认证,认证是计算的加强,显示计算机用户希望能够打开选择的部分的配置细节。因为第一阶段认证了两个部分(为密钥交换做认证,通过共享密钥和公钥对通信双方进行认证),使基于策略的控制可用,建立 IKE SA,用来保护认证不被偷听。

使用由认证负载组成的新 IKE 认证交换类型,通过单向或双向认证互相发送,在第一阶段结束时,根据每一部分初始化或接收另一部分的认证交换,定义新的认证功能策略配置。

尽管保护同 IKE SA 认证交换,但人为的攻击仍然可能发生,若不使用认证,即使 IKE SA 和认证终端不一致,攻击者也能用合法的机器获得 VPN 的访问权限。若攻击者希望获得 VPN 的访问权限使用计算机 C1,同时有另一台计算机 C2 来确认 VPN 的安全策略,攻击者可获得来自于 VPN 的从 C1 到 C2 认证请求和从 C2 接收 VPN 的认证回复,用 C1 来确认 VPN 的安全策略。

针对这个缺点,在拥有 TPM 提供功能的主机平台上使用绑定密钥认证 BKA(Bound Keyed Attestation)。认证终端双方知道 BKA 和 IKE SA 的共享信息,如果攻击者不能得到这些,那么攻击不可能发生。VPN 网关选择一个可重用和一个不可重用(nonce)的满足算法要求的随机数,使用 Diffie-Hellman 加密算法计算公钥,并把绑定密钥的认证消息,包含加密算法的参数、计算的公钥和网关选择的不可重用随机数发送给 VPN 客户端。VPN 客户端用可重用的随机数,根据加密算法计算出公钥,计算认证共享信息,应用 TPM 提供的 SHA-1 绑定认证信息。同时用 SHA-1 计算初始化的认证值,从 TPM 获得包含此认证值的引用。最后,VPN 客户端把包含客户端产生的公钥、认证信息、认证值、测量日志和 AIK 认证证书的绑定密钥发送给 VPN 网关。

VPN 网关用相同算法计算认证共享信息,用共享信息计算 VPN 客户端认证信息的期望值,若接收的认证信息与期望值不匹配,发送绑定密钥错误给 VPN 客户端,否则,用相应的

授权的公钥认证 AIK 证书,用此 AIK 证书和 VPN 客户端的认证值认证引用,用此引用认证响应的测量日志,若任一认证失败,或 VPN 网关不认为客户端的测量日志可信,发送绑定密钥错误消息给 VPN 客户端,否则,计算它的绑定值,发送包含这个绑定值的消息给 VPN 客户端,使 IKE 第二阶段可用。

2.3　网络接入安全性认证

当请求连接时,根据 TNC 体系结构接口间消息流动如图 2 所示,进行用户认证、平台认证和完整性检测。

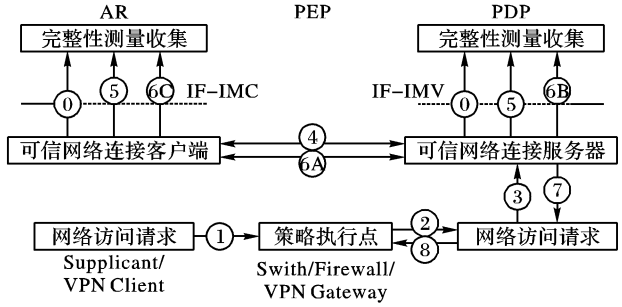

图 2　TNC 体系结构的消息流

流 0:通过使用平台绑定,可信网络连接客户端 TNCC(TNC Client)装载相关的完整性测量收集 IMC(Integrity Measurement Collector),检测 IMC 的完整性,TPM 执行称为 PCREXTEND 的操作,以便将数据散列,并将之储存到 R0 至 R15 的 PCR 寄存器内,作终端平台认证的可信网络连接服务器 TNCS(TNC Server)需要预先制定完整性的要求,并交给完整性测量核验者 IMV(Integrity Measurement Verifier),因此完整性检测完成。初始化 IMC,确保 TNCC 和 IMC 有效连接。同样,TNCS 装载相关的 IMV。

流 1:当网络连接被触发,在 AR 上的网络访问请求 NAR(Network Access Requestor)在网络层初始化连接请求。

流 2:收到网络连接请求,PEP 发送网络访问请求给网络访问授权 NAA(Network Access Authority)。NAA 配置用户认证,平台认证和完整性检测。NAA 和 AR 之间产生用户认证,AR 和 TNCS 之间进行完整性检测和平台认证。任何一环节的认证失败都将导致后面的事件不能进行。

流 3:用户和 NAA 间的用户认证成功,NAA 将会通知 TNCS 的连接请求。

流 4:TNCS 将会执行 TNCC 的平台认证、检验,有效的 AIK 证书被两终端所使用。

流 5:TNCS 和 TNCC 的平台认证成功,TNCS 给 IMV 指出一个新的连接请求发生,执行完整性检测握手。TNCC 和 IMC 执行相同操作,IMC 经过 IF-IMC 把 IMC-IMV 的消息传给 TNCC,IF(InterFace)为接口。

流 6A:完整性检测握手发生,TNCS 和 TNCC 对等连接,把通过 NAR、PEP 和 NAA 的消息进行交换,到 TNCS 满足 AR 的完整性状态。

流 6B:TNCS 通过 IF-IMV 传送 IMC 消息给匹配的 IMV,IMV 分析 IMC 的消息。如果 IMC-IMV 要交换更多的消息,通过 IF-IMV 提供消息给 TNCS。IMV 通过 IF-IMV 把它的决定和评估结果传给 TNCS。

流 6C:同样通过 IF-IMC,TNCC 把来自 TNCS 的消息传给匹配的 IMC。

流 7:当 TNCS 同 TNCC 完成了完整性检测握手,发送 TNCS 的决定给 NAA。

流 8:NAA 发送网络访问决定给 PEP。NAA 把它的最终决定给 TNCS,TNCS 发送给 TNCC。

3　VPN 结合可信计算技术的应用

当一个企业网的一个平台(E1)有权访问另一个网络的一个平台(E2),E1、E2 终端路由和网关之间存在 VPN,并且 E1 上产生的通信量能路由到 E2 及被签名。来自 AR 的信息被路由到 E2 之前,AR 的配置被 PEP 验证,同时 E2 相信 E1-PEP 被校验。

VPN 建立时,根据 TPM 提供的功能,如果不满足平台认证,则建立失败。否则在 E1 和 E2 的平台上,两个网络的管理员决定通用的配置信息,E1 上的 PEP 被看成是一个 VPN 端点,在 AR 上应用 E1-PEP,E1-PEP 和 E2-PEP 建立 VPN 连接,通用的配置信息被分配到在各自网络域上的 PDP。

连接时,AR 在 E2 上发现信息并向 E2 发送消息,选择与 E1-PEP 通信的访问操作并调用。E1-PEP 认证 AR 作为 E1 环境的部分并收集 AR 的完整性值,E1-PDP 根据 E1-E2 通用配置信息同 AR 完整性值比较。当配置信息满足,E1-PEP 允许来自 AR 的包传送到 E2,在 VPN 有效的 E2 使用会话密钥保护来自 E1 的包。

TNC 完整性由预先设定的策略所定义,认证性保证了系统通过认证只能被授权用户所使用。通过将策略植入 TPM 来判断平台的完整性和用户的认证性。在拥有 TPM 的主机上运用数据封装、IPSEC 完整性认证和网络接入安全性认证,确保终端的安全可信,用户的合法性和资源的一致性使用户按照规定的权限和访问控制规则进行操作,各个权限级别的人只能做与其身份规定的访问操作,只要控制规则合理,整个资源访问过程是安全的;将非法访问者隔离,防止意外的非授权用户的访问,从而减轻服务器的压力,以防拒绝服务攻击,防止不安全系统接入网络;VPN 采用 IPSEC 实现网络通信全程安全保密,确保传输连接的真实性和数据的机密性、一致性,防止非法的窃听和侵入。从而保证了平台的可信、网络的安全和传输的安全。

4　结语

当前 VPN 协议如 IPSEC 不能认证用户的计算机的配置,终端的安全不能保证,侵入者非授权访问 VPN 就不能确保信息的安全。VPN 和可信计算技术结合利用相关的认证来保证终端可信、网络接入和网络通信的安全从而构成一个信息安全保障架构,相信随着可信计算的发展和相关技术的完善,安全将会越来越完善。

参考文献:

[1] TRUSTED COMPUTING GROUP . TCG Trusted Network Connect TNC Architecture for Interoperability[EB/OL]. https://www.trustedcomputinggroup.org/downloads/specifications, 2005.

[2] TRUSTED COMPUTING GROUP. TPM Main Part 1 Design Principles [EB/OL]. https://www.trustedcomputinggroup.org/downloads/specifications, 2005.

[3] TRUSTED COMPUTING GROUP. TCG Specification Architecture Overview Revision 1.2 [EB/OL]. https://www.trustedcomputinggroup.org/downloads/specifications, 2004.

[4] XIA HD, KANCHANA J, BRUSTOLONI JC. ENFORCEMENT OF SECURITY POLICY COMPLIANCE IN VIRTUAL PRIVATE NETWORKS[EB/OL]. http://www.cs.pitt.edu, 2005.

[5] 李军. 渐成热门的网络端点安全技术[J]. 计算机安全, 2005, (1).