

PKI 在虚拟专用网络中的应用

张小波, 程良伦

(广东工业大学自动化学院, 广州 510006)

摘要: 虚拟专用网络(VPN)中的 IPSec 协议不能解决通信各方的身份认证问题。为此, 在 VPN 中引入 PKI 认证技术, 描述 PKI 在 VPN 中的应用, 包括身份认证、密钥管理和访问控制 3 个方面, 给出 PKI 在 VPN 中的配置模型与功能模型, 并对 VPN 用户数字签名的实现过程进行分析。

关键词: 虚拟专用网络; 公开密钥基础设施; IPSec 协议; 数字签名

Application of PKI in Virtual Private Network

ZHANG Xiao-bo, CHENG Liang-lun

(Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China)

【Abstract】 IPSec protocol in Virtual Private Network(VPN) can't validate the user's identification by its weak identity authentication. This paper introduces the Public Key Infrastructure(PKI) technology into VPN, describes the application of PKI in VPN, including identity authentication, key management, access control. It gives the configuration model and function model of PKI, and analyzes the implementation of VPN user's digital signature.

【Key words】 Virtual Private Network(VPN); Public Key Infrastructure(PKI); IPSec protocol; digital signature

DOI: 10.3969/j.issn.1000-3428.2011.15.035

1 概述

目前, Internet 已经成为各企业普遍使用的一个信息工具, 使得异地中的各企业可以方便地相互通信。作为一个公众信息网, Internet 提供各用户自由的接入, 并实现相互之间的信息交换。建立在 Internet 公共信道基础上的虚拟专用网络(Virtual Private Network, VPN)则要实现私有通信, 需要 Internet 满足私有通信所需的各种安全要求。因此, 安全问题也就成为 Internet 通信的关键, 必须采用相应的安全协议或机制来解决当前 Internet 网络通信存在的各种安全缺陷: (1)网络上一台主机伪装成另外一台主机与其他主机通信。(2)网络上一台主机监视其他主机间的通信。(3)黑客监视并截取一个通信会话, 从而伪装成通信的一方参与通信。

安全 VPN 采用专门的协议 IPSec 和标准的加密算法来建立并维持一个通信连接, 能够防止通信被监视或中断。但其还存在很难验证通信各方标识的缺陷, 尤其是当接入 VPN 的用户数量不断膨胀的情况下这种缺陷更加明显。

公开密钥基础设施(Public Key Infrastructure, PKI)可以提供一个认证标准来验证用户或系统的标识, 从而解决 VPN 中 IPSec 存在的安全缺陷。同时, PKI 还提供通信的数据进行加密传输和对应的密钥证书管理体系, 这正是 IPSec 所缺乏的。因此, 本文对 PKI 在虚拟专用网络中的应用进行了研究。

2 PKI 技术简介

2.1 加密算法

PKI 是用来实现基于公钥密码体制的证书产生、管理存储、发行和撤消等功能的安全平台, 它使用户可以在多种应用环境下方便的使用加密和数字等签名技术, 从而保证网上数据的机密性、完整性、不可抵赖性^[1]。

PKI 使用一个加密密钥和一个解密密钥。通信双方无需事先交换密钥就可以进行通信, 其中加密密钥不同于解密密

钥, 加密密钥公之于众。RSA 非对称公钥密码算法是目前网络上进行保密通信和数字签名的最有效的安全算法, 也是 PKI 用得比较多的一种加密算法; 除了 RSA 算法外, DSA 算法也是 PKI 用的较多的一种数字签名算法; 目前还提出了一种新的安全系数较高的椭圆曲线数字签名算法。

2.2 认证机制

PKI 通过认证中心(CA)、注册中心(RA)和目录服务器等来实现认证机制。认证中心作为权威的、可信赖和公正的第三方机构, 它主要负责产生、分配并管理所有参与网上通信的实体所需的身份数字证书。

注册中心是数字证书注册审批机构, 是认证中心的证书发放与管理的延伸。它负责证书申请者的信息录入, 审核以及证书发放等工作; 同时, 对发放的证书完成相应的管理功能, 这部分功能根据需要也可以集成在认证中心中。

目录服务器是采用 LDAP 协议建立的存放证书及相关信息的目录系统, 存放的证书包括用户的数字证书和属性证书等。用户或相关的应用通过 LDAP 来访问证书库获取相应的证书和证书失效列表。

3 VPN 策略

VPN 策略是 PKI 的一个扩展。策略在属性证书中定义, 用来指明某个用户或设备的附加信息, 例如允许某 2 个用户

基金项目: 国家自然科学基金资助项目(60673132); 国家自然科学基金广东省联合基金资助重点项目(U0935002); 广东省自然科学基金资助项目(8351009001000002, 07117421); 广东省重大科技专项基金资助项目(2009A080207008); 广东工业大学青年基金资助项目(405095245)

作者简介: 张小波(1977—), 男, 讲师、博士研究生, 主研方向: 传感器网络, 嵌入式系统, 智能控制; 程良伦, 教授、博士生导师

收稿日期: 2011-02-01 **E-mail:** zxb_leng@163.com

则使用 SA 中指定的加密算法, 将数据包在 ESP(Encapsulating Security Payload)中加密, 并产生相应的 AH(Authentication Header)。加密后的数据包就由建立的 VPN 安全通道传送给接收方。

5.3 VPN 用户数字签名的实现

若用户 A 想与用户 B 进行私有通信, 需要传送消息 m 则在双方的身份验证完后将消息 m 进行签名。A 利用其私有密钥 d 对 m 加以签名得签名文 $S: D(m)=S=M^d \pmod{N}$ 并将 m 与签名文 S 送给 B。B 收到 m 与 S 后, 利用 A 的公开密钥 (e, A) 进行验证: $E(S)=S^e=m' \pmod{N}$ 。若 $m'=m$ 则验证正确, 否则验证失败。由于任何人都可利用 A 的公开密钥进行验证, 且只有 A 知道 d 来产生 S 。因此, 当 A 与 B 发生矛盾时, 由第三者可以做出公正的判断。

若将公开密钥密码系统与数字签名系统相结合, 则可同时达到秘密通信和数字签名的目的。设在网络中使用用户 A 与 B 分别依密钥产生方法, 产生其各自的公开密钥 (e_A, N_A) 及 (e_B, N_B) , 并分别有各自的私人密钥 d_A 与 d_B 。若用户 A 要加密传送明文 m 和签名文 S 给 B, 则 A 首先对 m 以 d_A 签名, 得签名文 S 。并用 B 的公开密钥对 S 加密, 得密文 C 。即:

$$\text{签名文: } S=D_A(m)=m_A^d \pmod{N_A}$$

$$\text{加密文: } C=E_B(S)=S_B^e \pmod{N_B}$$

用户 B 收到密文 C 后, 先以其密钥 d_B 对 C 解密得 S 。接着, 再利用 A 的公开密钥, 进行验证。即:

$$\text{解密文: } D_B(C)=C=S' \pmod{N_B}$$

$$\text{验证: } E_A(S')=(S')_A^e \pmod{N_A}=m' \pmod{N_A}$$

当一个用户接入 VPN 时, 接入用户(发送方)可以指定接收方, 发出的消息只能被指定的接收方阅读。令发送方为 A 接收方为 B, PKA 和 SKA 分别为 A 的公开密钥和私人密钥, PKB 和 SKB 分别为 B 的公开密钥和私人密钥, A 发送的消息为 M 。数字签名的实现过程^[5]如图 3 所示。

具体步骤如下:

- (1) A 用 DSA 算法和 SKA 对 M 进行计算, 产生数字签名 X ;
- (2) A 用 B 的公开密钥 PKB 对 $(M+X)$ 进行加密, 产生 $E_{pkb}(M+X)$, 发送到 B;
- (3) B 收到后, 用他的私人密钥 SKB 对消息解密, 产生 $D_{skb}(E_{pkb}(M+X))=M'+X$;
- (4) B 用 DSA 算法和 A 的公开密钥 PKA 对 M 进行计算,

可以算出一个数字签名 X' 。

(5) B 验证数字签名 X' 与 X 是否相等, 如果相等则该次传输过程合法, 否则为不合法。

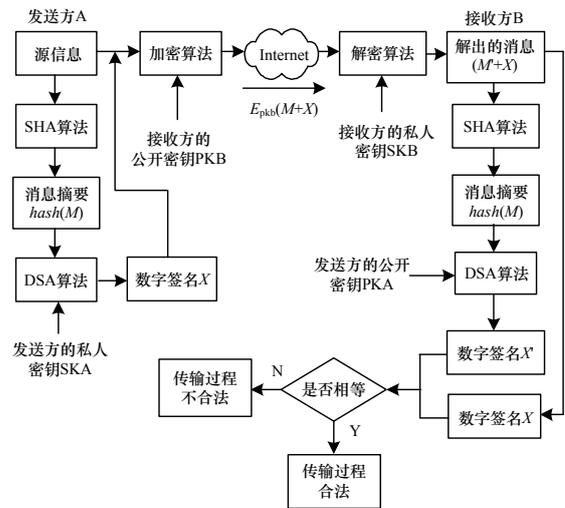


图 3 VPN 用户数字签名过程

6 结束语

本文对 PKI 在 VPN 中的应用进行了研究。PKI 将加密密钥和数字证书进行集中管理, 加强了 VPN 解决方案的相互协作性。采用带 PKI 的 VPN 解决方案, 各企业可以在较高的安全保障情况下充分利用 Internet 来满足企业内部的需求, 并与其他商业伙伴建立 B2B 的商务连接与通信, 因此, 该方案具有较高的实际应用价值。

参考文献

- [1] 邹翔, 刘浩, 王福. 基于 PKI 的网络边界安全监控方法[J]. 计算机工程, 2010, 36(1): 140-142.
- [2] 邢协永. PKI 及其在 VPN 解决方案中的整和应用[J]. 湖南经济管理干部学院学报, 2004, 15(1): 110-111.
- [3] 陆敏锋, 平玲娣, 李卓. 基于 IPSec 网络协议的 VPN 测试系统[J]. 计算机工程, 2010, 36(3): 156-158.
- [4] 余胜生, 周敬利, 陈向荣. IPSec-VPN 中应用 PKI 的研究与实现方案[J]. 计算机仿真, 2003, 20(3): 44-48.
- [5] 徐建兵, 曲俊华. 公开密钥加密体系和数字签名技术的研究[J]. 现代电力, 2004, 21(1): 80-85.

编辑 顾姣健

(上接第 99 页)

数的方法。实验结果表明, 该方法可以获得良好的融合效果, 具有一定应用价值。然而, 在文中放缩的程度还有较大的提升空间, 这也是今后值得研究的一个方面。

参考文献

- [1] Langelaar G C, Setyawan I, Legendijk R L. Watermarking Digital Image and Video Data[J]. IEEE Signal Processing Magazine, 2000, 17(5): 20-46.
- [2] Lin Wei-Hung. An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization[J].

IEEE Transactions on Multimedia, 2008, 10(5): 746-757.

- [3] 高智慧, 肖俊, 王颖, 等. 一种含边信息的小波域视频水印算法[J]. 计算机工程, 2009, 35(21): 123-124.
- [4] 何传江, 李建国, 苗婷. 结合分形编码的小波域水印方法[J]. 中国图象图形学报, 2009, 14(5): 871-876.
- [5] 李建国, 陶小鱼, 苗婷, 等. 基于能量估计的灰度水印系统分析[J]. 计算机工程, 2009, 35(14): 154-157.

编辑 陈文