主动网基于交叉证书的多信任域认证模型

蒋业逢[1],黎忠文[1],荣 蓉[2]
(1. 厦门大学 信息科学与技术学院,福建 厦门 361005;
2. 厦门大学 软件学院,福建 厦门 361005)

摘 要:认证是保证主动网安全性的前提和基础,传统的主动网认证采用基于证书的认证方法,由于基于身份的 PKI(ID - PKI)可以避免传统公钥密码体制中使用证书带来的种种弊端,因此越来越倍受关注。多种认证技术的并存是不可避免的事实,如何在不同类型的信任域间实现跨域认证是主动网安全研究的重要问题之一。在探讨 ID - PKI 在主动网上实施问题的基础上,提出了一种基于交叉证书的多信任域认证模型,在不同类型的信任域间提供双向实体认证,能较好地符合主动网认证的实际需要。

关键词:主动网;认证;交叉证书;ID - PKI
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673 - 629X(2007)11 - 0145 - 04

Cross - Certificate Based Authentication Model for Multi - Domain on Active Network

JIANG Ye-feng[1],LI Zhong-wen[1],RONG Rong[2]
(1. School of Info. Sci. & Tech., Xiamen University, Xiamen 361005, China;
2. Software School of Xiamen University, Xiamen 361005, China)

Abstract: Authentication is the premise and foundation of safety on active network. Active networks traditionally carry out authentication with Certificate - PKI; however, it is less efficient than ID - PKI which has been increasingly researched recently. Because of the coexistence of multi - PKI, how to implement authentication for multi - domain would become one of the most important problems on active network security. Analyzes the applications of ID - PKI on active network, and proposes a certificate - based authentication model for multi - domain, which supports cross - domain mutual entity authentication and is very suitable for practice of authentication on active network.

Key words: active network; authentication; cross - certificate; ID - PKI

0 引 言

主动网络是一种新兴的可编程数据交换网络,用户可以直接向网络节点插入定制程序,或者通过在报文分组中包含可执行的程序代码段(这些代码段由网络节点激活执行)来配置或扩展网络功能[1]。由于主动网的授权用户拥有了比传统网络授权用户更多的访问能力,对他们的认证直接关系到主动网的安全。主动网需要从逐跳(hop - by - hop)和端到端(end - to - end)两个方面进行认证服务保证网络的安全[2]。

ID - PKI 以基于身份的公钥密码体制(ID - PKC)为基础,可以从身份信息直接计算出用户的公钥[3]。由于它抛弃了对证书的使用,避免了使用证书带来的种种额外开销,在传统网的安全领域,特别是加密方面得到广泛研究和应用[4]。

然而,到目前为止,将 ID - PKI 应用于主动网的研究却很少。主动网中传输着大量的数据和代码,通信流量比传统网中的大出很多;而且,主动网环境对安全的要求相当严格,所以,ID - PKI 能够适应主动网的特点,必将在主动网中得到充分的应用。鉴于上述情况,文中提出在主动网上利用 ID - PKI 实施认证的思路,并研究如何与传统的基于证书的 PKI(Certificate - PKI)进行跨域认证,提出了一种基于交叉证书的多信任域认证模型[5]。

收稿日期:2007 - 01 - 10
基金项目:福建省 2004 年自然科学基金资助项目(A0410004);厦门大学院士基金资助项目(0630 - E23011);厦门大学新世纪优秀人才支持基金资助项目(0000 - X07116);广东省自然科学基金资助项目(06029667);广东中山市 2006 年科技计划项目
作者简介:蒋业逢(1982 -),男,江苏南通人,硕士研究生,研究领域为网络安全;黎忠文,博士,副教授,CCF 会员,研究领域为实时系统高安全和高可靠技术。

1 ID - PKI 与主动网

1.1 ID - PKI 介绍

ID - PKI 的思想是由 Shamir 在 1984 年首次提出来的[3]。它是一种基于身份的密码体制,用户可以使用任何有意义的字符串作为自己的公钥,如名字、E - mail 地址等,密钥中心 TA(又称为信任中心 Trusted Authority)结合自己的系统参数为用户产生相应的私钥。TA 作为可信第三方,其地位类似于传统 PKI 中的 CA[6]。

ID - PKI 不仅具有一般 PKI 的所有优点,还拥有很多自己的独特之处,它主要有如下优点:

①用户可以根据自己的身份信息计算出自己的公钥,可以在刚加入信任域的时候从 TA 处获得自己的私钥,简化了 PKI 的系统结构和密钥协商机制[7]。

②ID - PKI 不需要在认证的过程中传送证书,节约了带宽。

③用户不需要验证 CA 对证书的签名,节约了自身的计算能力。

④用户不必为每一个通信伙伴存储证书,只需要存储 TA 的系统参数,节约了存储空间。

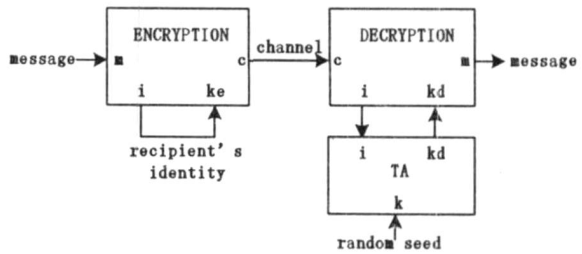
由于 ID - PKI 有众多的优点,非常适合于任务繁杂、通信量很大的主动网环境,必将在主动网中得到充分的应用和发展。

1.2 ID - PKI 在主动网上的应用

主动网由于其环境的特殊性,对分组报文的认证不仅会出现在信源和信宿端,还可能出现在传输路径上的各个主动节点间[2]。在对主动网进行逐跳认证时,对传输的消息用认证密钥和密钥 HASH 算法计算消息的数字摘要,作为主动报文中完整性选项的附件发送给接收者,确保信息在传输时不被破坏、修改和假冒,从而实现对相邻主动节点的完整性保护。

主动网在基于身份的信任域中进行端到端的认证和完整性保护时可以采用数字签名技术。当通信双方处在同一个信任域时,可以类比我们所熟悉的邮件系统:只要知道了对方的邮箱地址,就可以向对方发送邮件,这个邮件只有收件方本人才能阅读;可以从对方的邮箱地址得知邮件的发送方,而且只有发件方本人才能用此邮箱地址发信。利用 ID - PKI 进行加密和签字的过程分别如图 1 中的(a),(b)所示[3]。

当通信双方处在不同的信任域时,需要在不同的信任域间实现跨域认证。不同的 TA 使用一组不同的系统参数,由此计算出来的私钥与公钥的对应关系可能不同,因此,它们的用户在通信时无法理解对方的签密信息,所以它们必须交换各自的参数以满足通信双方的互信要求[8]。在主动网中,通过交叉证书在 TA 之间交换参数是很好的选择。



(a) ID-PKI 加密示意图

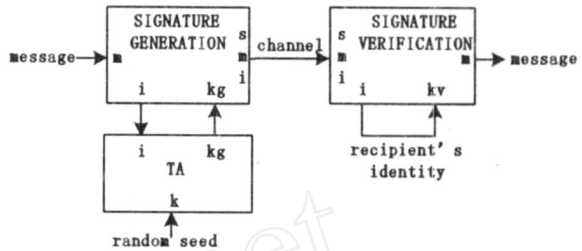


图 1 ID - PKI 签密过程示意图

如图 2 所示,TA1、TA2、TA3 是对等的信任中心,它们通过相互颁发证书来实现用户互信。例如,在图 2 中,U1 和 U2 进行通信之前,TA1 和 TA3 必须交换各自的系统参数。TA1 通过给 TA2 颁发证书 1 把系统参数传给 TA2,TA2 再通过给 TA3 颁发证书 2 把系统参数传给 TA3,这样便建立起一条从 TA1 到 TA3 的证书链,TA3 从证书链中获得 TA1 的参数信息。同样地,TA1 也可以获得 TA3 的参数信息。

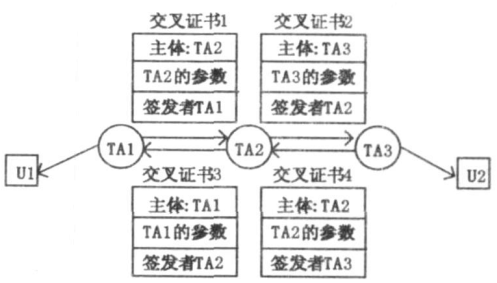


图 2 交叉认证

需要特别注意的是,以这种方式建立的 PKI 系统在信任中心的层面上实行基于证书的认证机制,而在各自的信任域内却仍然实行基于身份的认证机制[5]。

接下来讨论在不同类型的多信任域间主动网如何实现跨域认证。从讨论中可以看到,如果需要认证的两个用户处在不同类型的信任域中,证书路径问题、证书策略问题等将变得非常复杂。

2 多信任域认证的模型

在不同类型的多信任域间实现跨域认证的首要前提,就是处在不同信任域中的认证双方必须能够理解对方所使用的认证机制和加密算法等[5]。在主动网环

境中,可以通过向主动包中插入配置代码并发送到信任域中的每一个主动节点上,以此对主动节点进行预先自动配置来满足实现认证的前提。

为了简化讨论,只分析具有两个信任域的情形,并假定一个是基于证书的信任域 A,另一个是基于身份的信任域 B。

2.1　系统结构

该认证模型的系统结构如图 3 所示。

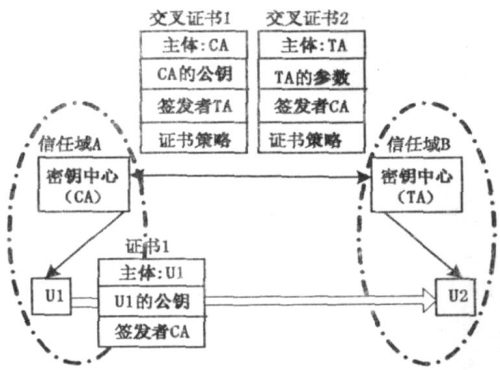


图 3　多信任域认证模型

在此模型中,CA 和 TA 相互颁发证书。CA 为 TA 生成一个交叉证书,其中包含 TA 的公共系统参数和信任域 B 中与信任域 A 中的用户有关的策略信息;类似地,TA 也为 CA 生成一个交叉证书,其中包含 CA 的公钥和信任域 A 中的一些相关的策略信息。

当许多 CA 和 TA 进行互联时,信任的传递会变得很混乱,有时可能会无法寻找信任路径;而且,随着信任路径的增长,信任可能会丢失。另外,即使证书路径的寻找没有问题,对证书策略(CP)和认证业务声明(CPS)的分析也使得确认证书有效性的机制变得困难[5]。

首先解决证书路径问题。证书路径问题是目前急需解决的关键技术之一。目前一般采用目录信息树的思路,参照网络路由算法中的路由表,在各个信任中心建立一个目录服务器。当有证书链经过本地 CA 或 TA 时,通过查找本地的目录服务器找到证书链的下一跳。另外,可以通过信任中心对信任域进行选择,以及对某些路径的屏蔽,可以保证证书路径的完整,以优化证书路径。

再一个就是证书策略问题。证书策略由一组规定组成,用以指明证书用于特定团体或具有相同安全要求的应用类型和范围。当两个实行不同证书策略的信任域互联互通时,需要对两个不同体系的策略建立对应关系。CA 和 TA 中的策略映射功能完成双方策略的正确对应,并通过签发的证书中的策略映射表将这种关系告诉使用者,从而使策略在不同的信任域中互相理解。

经过分析,这两个问题是可以得到解决的,所以,我们设计的模型是有理论基础和实际可行的。下面讨论主动包和证书的设计,然后着重思考模型认证协议的设计。

2.2　主动包和证书的设计

根据主动网的认证特点,设计模型中使用的证书和主动包的格式如下:

首先,分析证书的类型和格式。参照文献[5]对证书的格式和内容进行的分析和比较,我们认为采用 X.509v3 身份证书作为交叉证书比较合适。利用证书的扩展项保存信任域 B 的身份标识、系统参数和策略信息等,这样,A 中的用户就可以根据这些附加信息对交叉证书进行处理。图 4 为我们设计的交叉证书的格式,证书中的扩展项被用来保存信任域 B 的系统参数和策略信息。

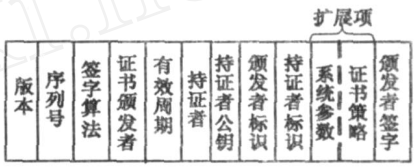


图 4　交叉证书格式

主动包(Capsule)的格式如图 5 所示,其中 ANEP 报头是为了使得 Capsule 的格式遵循主动网络封装协议,便于主动网络之间的互通,它具体包含有标志位、类型标识符、报头长度、报文长度、源地址和目的地址等[9]。完整性选项主要包含密钥标识、序列号和消息摘要三部分,用于保证主动包的逐跳安全。证书用于主动节点(ANN)对主动包进行认证,如果发送方处于信任域 A,发送 Capsule 前必须将自己的证书放入其中相应的位置,否则,证书设为空。数字签名用于对 Capsule 进行完备性检测,防止 Capsule 在传输的过程中被篡改。

ANEP 报头	主动代码指针	数据	控制策略	完整性选项	证书	数字签名

图 5　主动包格式

2.3　认证协议的设计

由于信任域 A 和信任域 B 的不对称性,需要从两个方向分别对认证的协议进行描述。

●首先,讨论从 U2 发送签密消息到 U1 的情形,此时的协议如下所示:

1) U2 获取 U1 的证书,得到 U1 的公钥和系统参数。

2) U2 利用 U1 的认证方式给 U1 发送经过签密的主动包。

3) U1利用自己的私钥解开主动包,并验证主动包的安全性和完整性。

协议执行的详细过程如下:

(1) U2首先查找本地有没有U1的证书,如果有,则检查证书的状态标志验证证书的有效期。如果本地没有U1的证书或者证书已经过期,则构造从TA到U1的证书链TA《CA》CA《U1》(见图3)。该证书链涉及到两个证书,交叉证书1和证书1。U2向TA注册得知TA的公钥,从而从TA《CA》(即交叉证书1)解出CA的公钥,接着利用CA的公钥从CA《U1》(即证书1)解出U1的公钥,并根据证书中的系统参数信息获知U1的认证方式。

(2) U2创建将要发送给U1的主动包,利用HASH函数计算主动包中静态部分的数字摘要,并用自己的私钥对数字摘要进行签名;接着,根据U1采用的认证方式利用U1的公钥对主动包中的可变部分进行加密。然后,将经过签密之后的主动包发送给U1。

(3) U1收到主动包之后,用自己的私钥解开主动包,用U2的公钥解密数字签名从而导出数字摘要,并对主动包中的静态部分作同样HASH计算得到一个新的数字摘要,将两个摘要的哈希值进行结果比较,如相同则签名得到验证,否则无效。

●上述讨论基于B中的用户的角度,下面,从A中的用户的角度来讨论如何从U1发送签密消息到U2。此时的交换协议要比上述协议来得简单,因为U1不需要从U2那里获得公钥,直接用U2的身份标识作为公钥加密主动包。协议主要如下:

1) U1根据U2的认证方式给U2发送经过签密的主动包。

2) U2利用自己的私钥解开主动包,并验证主动包的安全性和完整性。

具体执行过程如下:

(1) U1创建将要发送给U2的主动包,利用HASH函数计算主动包中静态部分的数字摘要,用自己的私钥对数字摘要进行签名,接着根据U2采用的认证方式利用U2的公钥对主动包中的可变部分进行加密。然后,将经过签密之后的主动包和自己的证书一起发送给U2。

(2) U2收到主动包之后,根据交叉证书2中的系统参数从TA计算出自己的私钥,并利用该私钥解开主动包,从U1的证书中得到U1的公钥,用U1的公钥解密数字签名从而导出数字摘要,并对主动包中的静态部分作同样HASH计算得到一个新的数字摘要,将两个摘要的哈希值进行结果比较,如相同则签名得到验证,否则无效。

3 安全性分析

该认证模型的安全性主要基于两点:一是模型所依赖的Certificate-PKI和ID-PKI的安全性;二是文中认证协议的安全性。文中所使用的Certificate-PKI系统的安全性在实际的应用中已得到证明和认可,ID-PKI的安全性决定于底层ID-PKC算法安全和运营安全,这些不在讨论范围内,文中假定其总是安全的。至此,只考虑认证协议的安全性。认证协议的目标是实现双向实体认证和密钥协商。该协议的安全性需要从两方面讨论:一个是逐跳安全;另一个是端到端安全。

首先是逐跳安全。逐跳安全一般通过主动包中的一些字段来保证,在文中是完整性选项字段,其中密钥标识字段防止主动包的伪造或篡改;序列号字段防止消息重发;消息摘要防止主动包信息的丢失或篡改。文中的协议主要用于端到端认证,对逐跳认证的影响不大,因此能够保证逐跳认证的安全。

利用该协议,可以实现端到端的双向认证。首先,发送方可以通过安全的方法(构建证书链、发布有效合理的证书策略等)获取接收方的公钥,并通过主动包将自己的公钥发给接收方,以完成密钥协商。双方进行通信时,发送方用接收方的公钥加密主动包,由于只有接收方才有相应的解密私钥,由此,验证了接收方的身份;发送方用自己的私钥对主动包中的数字摘要进行签名,接收方用发送方的公钥解密数字签名,可以验证发送方的身份。

4 结束语

在已有的Certificate-PKI和ID-PKI的基础上,利用交叉证书设计了一个在不同类型的多信任域间实现跨域认证的模型。该模型能够在不同类型的信任域间提供安全的双向认证,比以往的在单一信任域中和同种类型的多信任域间工作的认证框架更符合主动网的实际应用需要。下一步将开展基于交叉证书的访问控制策略问题的研究。

参考文献:

[1] 高发桂,高 路. 主动网络安全机制的分析与研究[J]. 微机发展,2005,15(11):34-36.

[2] 唐 寅. 基于授权的主动网络安全防护技术研究[D]. 成都:电子科技大学,2003.

[3] Shamir A. Identity-based Cryptosystems and Signature Schemes[C]//Advances in Cryptology-CRYPTO'84,LNCS 196. Berlin:Springer-Verlag,1984:47-53.

(下转第152页)

加密是通过对信息的重新组合,使得自由收发双方才能解码还原信息的传统方法,它是以密钥为基础的。网络信息加密的目的是保护网内的数据、文件、口令和控制信息,保护网上传输的数据.网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全。端点加密的目的是对源端用户到目的端用户的数据提供加密保护;节点加密的目的是对源节点到目的节点之间传输链路提供加密保护。各税务机关可根据各自的网络情况选择上述三种加密方法。

(2) 身份认证的安全检查。

身份认证是用户向系统出示自己证明的过程,以阻止非法用户的不良访问[4]。有多种方法可以鉴别一个用户的合法性,密码是最常用的,但由于有许多用户采用了很容易被猜到的单词或短语作为密码,使得该方法经常失败。还可以采用其他方法进行识别,例如利用人体生理特征(如指纹、眼睛视网膜底纹等)的识别、智能卡等。

(3) 数字签名。

这种技术主要用于防止非法伪造、假冒和篡改信息。接收者能够核实发送者,以防假冒;发信者无法抵赖自己所发的信息;除合法发信者外,其他人无法伪造信息。发生争执可由第三方做出仲裁。数字签名是基于公共密钥的身份验证[5]。

利用数字签名技术,在税务信息系统网上申报纳税的时候,纳税单位可以利用自己的单位证书在申报材料上签名,这样就可以确保材料的不可篡改性和单位的不可抵赖性。同样,数字签名也可以应用于公文流转当中,领导在审批材料当中利用自己的个人数字证书对其进行签名操作,以代替一般的手写签名,使得办公速度提高,而且更为安全、严密。

4 总 结

随着"金税三期"建设的全面进行,国税网络安全问题需要更加重视。最后需要说明的是,只有将防火墙、VPN、IDS、物理隔离系统和防病毒等安全技术相互结合,才能构建出安全强度更高、安全隐患和漏洞更少、安全风险更低的安全网络,才有可能使用户将关键数据业务安全地拓展到不信任网络上,或在互不信任的网络之间安全地行数据交换,使税务网络真正达到建以致用的目的。

参考文献:

[1] 徐伟清. 构建安全网络架构保障网上申报安全[J]. 上海财税,2002(7):39 - 40.

[2] 国家税务总局信息中心. 金税工程三期:将税收信息化进行到底[J]. 中国税务,2002(1):26 - 28

[3] 史文军. 税收信息化的技术准备[J]. 山东税务纵横,2002(5):13 - 16.

[4] 陈彦学. 信息安全理论与事务[M]. 北京:中国铁道出版社,2000.

[5] Adams C, Lloyd S. 公开密钥基础设施 ——概念、标准和设施[M]. 北京:人民邮电出版社,1999.

(上接第 144 页)

的可靠性标准、成本诸因素选择适当的技术,以获得系统最佳的可靠性。

参考文献:

[1] 王东盛. 软硬件可靠性设计结合可提高系统可靠性[J]. 质量与可靠性,1994,28(4):32 - 36.

[2] 祝 福,肖彦直. 计算机控制系统的抗干扰技术[J]. 计算机与数字工程,2005,33(5):66 - 68.

[3] 郦 萌. 软件容错技术[J]. 质量与可靠性,1994,21(2):27 - 30.

[4] 袁由光. 可靠系统的设计理论与实践[M]. 北京:科学出版社,1988.

[5] 温如春,罗小燕,雷小华. 单片机系统 PC 失控的软件措施[J]. 机电一体化,2004,27(5):95 - 96.

(上接第 148 页)

[4] Martin L. Identity - Based Encryption:A Closer Look[J]. The Global Voice of Information Security,2005,12:22 - 24.

[5] Price G, Mitchell C J. Interoperation between a Conventional PKI and an ID - based Infrastructure[C]// Chadwick D W, Zhao G. Public Key Infrastructure, Second European PKI Workshop:Research and Applications, EuroPKI 2005. Canterbury, UK, 2005. Revised Selected Papers, LNCS 3545, Berlin: Springer - Verlag, 2005:73 - 85.

[6] 路晓明,冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报,2006,34(4):577 - 581.

[7] Boneh D. Franklin M. Identity - based Encryption from the Weil Pairing[C]// Advances in Cryptology - CRYPTO 2001, LNCS 2139. Berlin:Springer - Verlag, 2001:213 - 229.

[8] Chen L, Harrison K. Certification of Public Keys within an Identity - based System[C]// Information Security, 5th International Conference, ISC, LNCS 2433. Berlin: Springer - Verlag, 2002:322 - 333.

[9] 王建国,李增智,王 宇,等. 通用的主动网络安全机制[J]. 西安交通大学学报,2002,36(8):818 - 821.