嵌入式防火墙系统的实现

刘玉莎 张晔 张志浩 (同济大学计算中心 200092)

摘要:针对目前日益突出的网络安全问题,尤其是内部网安全问题,本文对现有安全技术所普遍存在的若干隐患与不足进行了深入地探讨,并提出了一种崭新的安全体系结构——嵌入式防火墙系统(EFS),该模型以基于 Kerberos 协议的认证模块为核心,并集授权、安全数据传输和审计等机制于一体。

关键词:网络安全 防火墙 认证 密钥

1. 前言

目前保护网络安全最主要手段之一就是构筑防火墙,它是一道界于开放式、不安全的公共网与信息资源汇集的内部网之间的屏障。以前人们更为关心的可能是如何保护内部网络中的资源及信息不受外部攻击者肆意破坏或盗窃。然而,随着网络技术的迅猛发展及用户应用水平的不断提高,资深 IT 人员已越来越多地意识到内部网络用户(以前通常被认为是可信任的企业雇员)对网络已造成了前所未有的威胁。据各种统计资料表明,70% 的攻击实际上来自于所谓的"安全网",即内部网。

传统防火墙结构是无法满足当今的安全需求的。这个结论可以从以下的分析中得出。

(注:以下所有的讨论都将针对包过滤防火墙技术以及电路层网关技术。虽然,应用网关也是目前一种十分流行且被普遍认为安全性较高的技术方案,但在本文中将不加以探讨。这是由于该技术不能透明地支持各种应用,换言之,必须为每种应用分别编写各自的代理程序,才能获得防火墙的支持;此外,该技术还将导致较低的性能。因而一般无法适应内部网中应用程序灵活多样、网络传输速率较高的特点。)

(1)高成本。内部网中需要保护的主机或资源越多,需要设置的安全检查点就越多,这意味着更高的设备成本及系统维护开销。简言之,成本增加了。

(2)高管理负担。对于 IT 管理人员来说,他们将面临极大的挑战来管理、维护如此多的防火墙设备。

(3)低性能。由于有大量的安全检查点被安置于企业内部的各种路由设备上,内部网中所有的通信,无论是否需要进行安全检查,都将不可避免地经过若干个安全检查点,以至于造成相应的传输延迟,降低了网络性能。

(4)站点到站点的 VPN(Virtual Private Network:虚拟专用网)。虽然目前有越来越多的防火墙产品集成了对 VPN 的支持,但是一般来说,这些 VPN 只是在介于两个网关之间的公共网络上建立了一条加密的数据通道,然而在通信进入该隧道以前,或是越过目标站点网关以后,它将完全以明文的形式暴露于内部网络之中。可想而知,安全隐患就出现了。

(5)复杂的状态同步机制。为了实现高可用性,两个或更多个路由设备将被对等地放置于网络入口处。为了实现安全,防火墙被分别安装在这些路由设备上,同时,每个防火墙的状态必须始终保持完全一致,这是由于原本属于同一会话连接的 IP 包完全可能通过不同的传输路径。因此,一个复杂的状态同步机制必须引入安全系统。

由此可见,无论是基于包过滤的防火墙技术还是基于应用网关的防火墙技术,都不能很好的解决内部网络的安全问题。针对此种现状,本文提出了一种崭新的防火墙结构——嵌入式防火墙系统(EFS),以有效地解决日益突出的内部网安全问题。

2. 总体介绍

总体而言,EFS 不仅仅是一种单纯的提供访问控制手段的防火墙设备,它还集成了一整套解决网络安全问题的各种应用,为大量的网络用户及需保护的网络资源提供了一个可管理的、分布式的、安全的计算环境。它使用了一种简化的、基于公钥的 Kerberos 协议以实现透明的认证,并综合了其他一些网络安全技术,包括授权、安全数据传输、审计等,并提供了一种集中式的管理机制。

3. 系统结构

EFD 核心系统一般可以分为四个主要部件:客户认证代理、嵌入式防火墙代理、票据授予服务器(TGS)和认证服务器(AS)。

客户认证代理运行于用户所使用的客户端主机。它的主要功能是在申请各种服务前向 AS 和 TGS 请求相应的票据,并在申请服务时发出相应的票据。在必要的场合,它还将负责反向验证服务器票据的合法性,实现双向认证。该部件处于网络层,接受用户登录,并透明的实现 Kerberos 票据的申请及转发,构成了 Kerberos 实体。

嵌入式防火墙代理运行于受该系统保护的服务器主机。它主要用于验证客户所发送的票据，以决定是否将 TCP 连接请求或 UDP 包送往更高层进行处理。该部件同样处于网络层，构成了 Kerberos 的应用服务器实体。

TGS 与 AS 的功能与 Kerberos 协议中的定义基本一致，只是在 TGS 上增加了授权管理的机制，详细资料请查阅参考文献[1]，这里将不再赘述。

4. 简化的实现机制

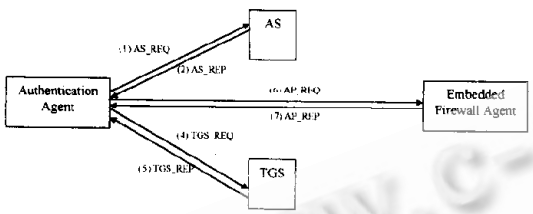

图 1　系统实现机制原理图

AS：Authentication Server，认证服务器

TGS：Ticket Granting Server，票据授予服务器

AP：Application Server，应用服务器

在开始陈述实现机制前，先作一些说明。为了实现严格的认证，同时又保证较高的效率，EFS 中使用了简化的 Kerberos 协议。此外，公钥算法的采用也极大地提高了 Kerberos 原有的性能。有关实现机制的进一步信息和使用改进后 Kerberos 协议所带来的益处，本文将不再进行赘述。详细内容可通过 Email 方式（liuyusha@rocket-mail.com，zhangye2000@hotmail.com）与作者进行联系。

(1)客户登录 EFS 系统时，客户认证代理将提示并获取相应的用户名和口令。为获取访问权限，客户必须提供所获悉的内容，如口令或 PIN（Personal Identification Number：个人身份标识码），并出示所具有的设备，如 Token。这就是两重因子认证机制。然后客户认证代理再将该口令作用于相应的用户数字证书（一般以文件的形式存放于磁盘上，或是其他安全设备，如智能卡），以产生用户的私有密钥。此外，需注意的是，明文口令的处理时间应尽可能短。使用后应立即予以销毁。因而，仅当客户同时具有正确的口令和含有私有密钥的设备，客户的代理才能够进行身份验证。在用户登录完成后，客户代理将自动向 AS 发送请求 AS_REQ，以申请 TGT。

(2)认证服务器 AS 收到客户的 AS_REQ 后，发回应答消息 AS_REP，其中包括一个提交给 TGS 的票据，称为 TGT。TGT 首先用 AS 的私有密钥 $PrvK_{as}$ 签名，然后用 TGS 的公开密钥 $PubK_{tgs}$ 加密，使得只有 TGS 能正确解读 TGT。

(3)客户认证代理得到 AS 发回的 AS_REP 后，用 $K_{c,as}$ 解密，获取并保存与 TGS 通信的会话密钥 $K_{c,tgs}$ 及 TGT，供申请服务时使用。

(4)当客户需要使用某一服务时，客户认证代理将首先截获请求 TCP 连接的 IP 包，并根据 Socket 匹配以判断是否已具有获取该服务的票据。如有，则直接将此票据附加于该 IP 包，形成 AP_REQ，发往服务器（执行步骤 7）；否则，客户认证代理必须首先向 TGS 申请相应的应用票据，这一阶段包括如下过程：首先向 TGS 发送请求 TGS_REQ，其中包括了由步骤 1 所获取的 TGT，同时还包括了被申请应用服务器的信息（包括应用服务器名、服务名、应用服务器票据的有效使用期限等）。此外，TGS_REQ 中还包含随机生成的 nonce，以及一个用该客户与 TGS 的会话密钥 $K_{c,tgs}$ 加密的认证算子。

(5)TGS 在收到客户认证代理发来的 TGS_REQ 后，用 $PrvK_{tgs}$ 将 TGT 解密，以获取客户与其的会话密钥 $K_{c,tgs}$，随后用得到的 $K_{c,tgs}$ 将认证算子解密，将算得的检验与自己生成的 HASH 函数结果相比较，以检查客户身份的合法性和消息的完整性。若两者匹配，且被申请的服务已在 EFS 注册，并需要认证时，TGS 将搜索用户权限表，以检验客户是否具有指定服务的使用权限。在授权通过后，TGS 生成 TGS_REP，并发回客户。

(6)客户认证代理得到 TGS 发回的 TGS_REP 后，首先确定所申请的服务是否需要认证。若无需认证，客户代理将恢复先前的连接请求；否则，则从 TGS_REP 中获取服务的票据和与应用服务器之间的会话密钥 $K_{c,ap}$，并将它们放入原来的连接请求包中，形成 AP_REQ，发往应用服务器。

(7)驻留于应用服务器上的嵌入式防火墙代理收到 AP_REQ 后，用 $PrvP_{ap}$ 解开票据，获取会话密钥 $K_{c,ap}$，以验证用户身份。如果合法，则将该 IP 包递交上层处理，否则予以丢弃。嵌入式防火墙代理在验证完用户身份后，若发现票据中还包括双向认证要求，则将发回用会话密钥加密的 nonce 值等信息，以证明其身份。

（注：有关 UDP 的处理方式与 TCP 基本相同，但是，客户认证代理将截获每一个 UDP 包，并附加相应的票据。如果需实现双向认证或扩展的安全服务（如数据机密性），则须使用动态过滤或状态评估等技术，维护 UDP 的“连接”。）

5. 系统总体特色

(1)防止来自于内、外部网络的攻击。这是本系统的一个主要特色。由于本系统的嵌入式防火墙代理部件将被直接安装在所有需要安全保护的应用服务器上，因此

传统防火墙介于内、外网之间的检查点被转移到了有保护需求的服务器自身，对于装载嵌入式防火墙代理的机器而言，来自于其自身以外任何机器的通信，无论其所处位置，都需经过嵌入式防火墙代理的检查及过滤。

(2)透明认证

①用户级透明。目前一些先进的防火墙产品提供了一类称之为客户认证的技术。尽管该机制同样支持所有的 IP 应用，但在用户获取网络资源的访问权限前，必须经由 Web 或 Telne 访问某一防火墙以实现认证，这显然对用户不具有透明性。

然而就 EFS 来说，用户无须亲自与防火墙连接以获取认证，而是由驻留在客户机上的认证代理自动与 AS、TGS 等连接，交换相应的票据，实现整个认证过程。简言之，EFS 是完全透明于用户的。

②程序员级透明。在 Unix、Linux 系统中，提供了另一种认证机制，该机制是由称之为 PAM(Pluggable Authentication Modules)的模块所实现的。该模块在一定程度上实现了认证和应用的分离，对程序员而言，具有相当的透明性。然而，为了实现认证，程序员仍然需要在源程序中加入对特定 PAM 库的调用代码，这样，一旦认证策略或认证算法有所改变时，只需系统管理员改变相应的配置文件即可，而无需重新编译该应用程序。由此可见该机制只是在一定程度上实现了透明性。

然而在 EFS 中，即使应用程序本身从未考虑过实现任何认证机制，EFS 仍可使其支持严格的身份认证过程，从而实现了认证与应用的完全独立。因此，EFS 具备了程序员级的透明性。

(3)安全会话。由于 Kerberos 协议为每个会话均提供了一个随机的会话密钥，从而实现了安全的会话传输。此外，通过与公共密钥技术的结合，EFS 提供了四种数据传输的安全级别(平文，保密性，完整性，和不可否认性)，从而在两台通信主机之间形成了一条私有通道。

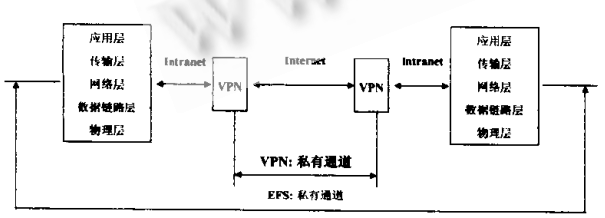

图 2 端对端 VPN 与 EFS

而传统的 VPN，仅是对在公共网部分传输的数据进行加密，而一旦通信抵达了目的网关之后的内部网时，就仅以明文的形式存在了。此种做法的前提是内部网是可信任的网络，然而，事实恰恰证明事与愿违。因此，传统的端对端、用户对端的 VPN 应当扩展为点对点的加密通道，以支持真正的安全通信。EFS 提供了支持安全会话的有效解决方案。

(4)过滤条件丰富多样。由于本系统使用了基于 Kerberos 的认证协议，因此它主要的过滤条件是“用户身份”，这也是其区别于传统防火墙的特点之一。与此同时，由于在 Kerberos 协议中，票据包含了机器地址域，这就保证了基于 IP 或 NIC 地址过滤方式的实现。此外，系统同样可以进行各种条件的组合过滤。

(5)一次签放。由于运用了 Kerberos 票据的概念，一次签放的机制得以实现。每张票据中都含有一个可事先定制的过期时限，也就是票据的有效期；同时，在有效期过期之前，客户认证代理将自动申请票据的续用，从而在保证安全的有限时间内，实现一次签放的机制。这将极大地方便用户及管理人员。

对于用户来说，他们只需在登录系统时进行一次认证，便可以使用所有的安全服务。

对于管理员而言，他们将无须再为每一种应用程序或服务，建立、维护一张独立的用户帐号表，而仅需维护一套 EFS 帐号，并精确定义用户访问各种服务的权限即可，这也有助于管理员将各个服务的安全性作为一个整体集中起来综合考虑，极大地增加了系统的安全系数。

(6)集成的安全解决方案。显然，认证是整个网络安全的基础和前提，然而它仅仅是通往信息安全的第一步。除此之外，安全数据传输及完善的审计工具也是必须的。因此，EFS 涵盖了网络安全的各个方面，力图提供一套完整、全面的安全解决方案。

(7)统筹规划，集中管理。将内部网中所有的防火墙或检查点集中在一个集成的控制台上统一管理是企业安全策略得以正确实施的关键，因为这将有助于对整个网络定义一套统一的、一致的、企业级的安全策略。

由于 EFS 将在每台需保护的主机上安装嵌入式防火墙代理，而该代理的主要工作是验证 Kerberos 票据，因而无须在本地存放过滤规则表。所有的安全策略将被统一保存在 TGS 上，无须分发到各个检查点。因此，一个负责整个企业访问控制及授权的集中式控制台自然而然地形成了。

当然，在某些情况下，在部门中实施恰当的自治式管理策略还是必须的。此时，多 TGS 模型将能很好的适应

这种需求(请参见下一节)。可见,EFS 是集中式管理和自治式管理的完美结合。

(8)分布式。由于 EFS 继承了 Kerberos 协议的分布式特点,因此,EFS 中的每个 AS 都将建立并维护自己的域(Realm)。此外,通过确立跨域(Inter－Realm)密钥,在本域(Local Realm:LR)中被认证的客户可以直接使用另一个与本域建立了信任关系的域中的服务,从而实现了分布式认证。具体过程如下所述:

①首先,另一域中的某个 TGS(RTGS:Remote TGS)将自己以 Principal 的身份注册到本域中;

②要使用他域服务的客户在为本域的 TGS 认证后,获得一张发往 RTGS 的票据;

③当 RTGS 收到后,则使用 Inter－Realm Key 解密,以确认票据的真实性;然后,RTGS 发出最终客户所请求服务的票据给相应的服务器,同时告之此客户是为另一域所认证的。

事实上,Kerberos 协议除了可实现直接的信任关系外,还可建立等级式的域组织方式,而这对于多个具有松耦合合作关系的企业而言,大有裨益。

6.系统模型

系统具有极强的适应性,在不同的应用环境中,一般可根据不同的企业规模和管理模式将系统划分为四种典型系统模型。

(1)单 AS 单 TGS 模型(SASTM)。该模型一般适用于小型企业。由于企业规模有限,系统用户及需安全防护的服务较少,因此适合于集中式管理,所以在系统中,仅需配置一台 AS 及 TGS 即可。

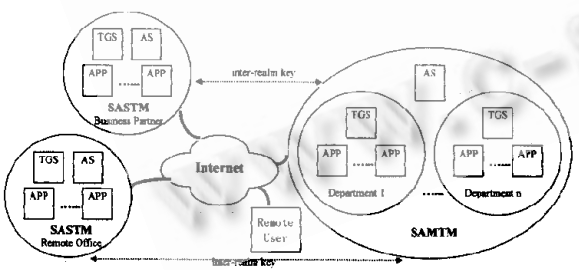

图 3 多 AS 模型

(2)单 AS 多 TGS 模型(SAMTM)。适用这种模型的企业一般具有一定规模。由于各个部门规模较大,独立的、分布式的管理各个部门的安全策略显得更为有效、可行。因此,在这种环境中,可为每个部门配置各自的 TGS,并由各部门自行制定相应的安全策略。

(3)多 AS 模型(MAM)

该模型通常用于跨地域的单位或具有密切合作关系的企业环境中。在这种情况下,一般而言,各个域之间需进行既相互独立、又相互信任的分布式管理。因此,可以在每个域中放置一台独立的 AS,负责本域的认证,而各个 AS 之间再通过"信任链"的机制以实现分布式的认证。当然,在各个域中可以按照具体的情况以确定到底是使用单 AS 单 TGS 模型还是单 AS 多 TGS 模型。

(4)等级型 AS 模型(HAM)。在多个具有松耦合合作关系的企业环境中,就必须使用等级型 AS 模型。首先必须明确的是,是一个企业所使用的模型必然是以上介绍的三种基本模型之一。为了实现不同企业之间的信任关系,则必须增加更高一级的 AS,以协调认证多个原本互不信任的域。

7.结束语

目前,整个系统模型已在 Linux 操作系统上得以实现。在不久的将来,系统还将实现运行于 Windows 系统平台上的客户认证代理及运行于 NT 和 Unix 上的嵌入式防火墙代理。届时,一个完整的、跨平台的安全解决方案将会形成。

值得一提的是,尽管 EFS 能很好地解决内部网和外部网的安全问题,然而,与传统防火墙技术及虚拟专用网技术结合使用仍然是有相当必要的。毕竟在安全问题上,"多多益善"。

参考文献

[1] Kohl J, Neuman C. (1993－09) RFC 1510: The Kerberos Authentication Service (V5).

[2] Atkinson R. (1995－08) RFC 1826: IP Authentication header.

[3] Atkinson R. (1995－08) RFC 1827: IP Encapsulating Security Payload (ESP).

[4] Cheswick, W. R. & Bellovin, S. R. (1994) Firewalls and Internet Security, Repelling the Wily Hacker, Addison－Wesley, Reading, MA.

(来稿时间:1999 年 3 月)