文章编号:1001 - 9081(2007)05 - 1038 - 03

一种入侵容忍的广播通讯 KDC 方案

商建伟[1],李 锋[1],张燕燕[2]
(1. 山东大学 网络信息安全研究所,山东 济南 250100; 2. 山东政法学院 司法信息系, 山东 济南 250014)
(shangjw@yahoo.com.cn)

摘 要:在使用密钥管理中心(KDC)进行广播通讯密钥分配的网络安全协议中,保证 KDC 的安全并提供高效率的密钥服务是一个非常重要的课题。区别于目前的域分割和服务器备份方案,使用双变量多项式作为门限构造函数,在多个分布式 KDC 服务器上分发不同的伪随机数产生函数,需要特定数目的授权服务器联合才能计算出最终的对称密钥,保证少于一定数目的 KDC 服务器被攻击后不能对系统产生威胁,从而保证了分布式 KDC 的安全性,并且能够避免广播通讯密钥分配过程中的效率瓶颈和单点失败。

关键词:入侵容忍;密钥管理中心;伪随机数产生函数;对称密钥
中图分类号: TP309 **文献标识码**:A

An intrusion tolerant KDC scheme for multicast communication

SHANG Jian-wei[1], LI Feng[1], ZHANG Yan-yan[2]
(1. *Institute of Network Security, Shandong University, Jinan Shandong* 250100, *China*;
2. *Department of Judicial Information, Shandong College of Political Science and Law, Jinan Shandong* 250014, *China*)

Abstract: Key Distributed Center (KDC) is an important component for generating symmetric key in multicast communication without using public key cryptography. It is important to keep KDC security and provide efficient symmetric key service. Different from the current partition to domain or replication solution, the proposed scheme uses bivariate polynomials to construct threshold distributed pseudo-random function, distribute the bivariate polynomials across the KDC servers, only the united authorized set of servers can compute the pseudo random for key. It ensure certain number of unauthorized server will not threaten the security of the whole network after being attacked. Therefore, enhance the security of distributed KDC servers was enhanced, and bottlenecks or single points of failure can be prevented.

Key words: intrusion tolerant; Key Distributed Center (KDC); pseudo random function; symmetric key

0 引言

从 1978 年 Needham-Schroeder 协议诞生开始,具有可信第三方的对称密钥协议得到了广泛应用,典型的协议包括:NSSK 协议[1]、Otway-Rees 协议[2]、Yahlom 协议[3]、大嘴青蛙协议[3]、Denning-Sacco 协议[4]、Woo-Lam 协议[5]、Kerberos[6]协议。这类协议的共同特点是采用 KDC 产生并分发对称密钥,在实际的应用网络中 KDC 需要和所有的实体共享一个对称密钥,记为 k_u,表示实体 u 与 KDC 之间的预共享对称密钥。当实体 u 和 v 之间需要通讯时,其中一方向 KDC 申请会话密钥,KDC 产生 u、v 之间的会话密钥 $k_{u,v}$,然后用 k_u 和 k_v 加密后发送给密钥申请方,u、v 分别使用 k_u 和 k_v 解密得到会话密钥 $k_{u,v}$。使用 KDC 分配对称密钥有很多优点,比如,新用户加入时无需广播新用户的密钥等。然而在广播通讯的应用场合如视频会议等,其缺点非常明显,主要包括:(1)效率问题:KDC 会造成"单点失败";(2)安全问题:因为 KDC 拥有网络中的所有 k_u,如果 KDC 被攻破,整个网络都会受到安全威胁;(3)可用性差:KDC 是密钥分发的处理瓶颈,并且如果 KDC 不可访问,会造成整个网络系统的瘫痪。

为了解决上述广播通讯的密钥分配问题,通常使用域分割和服务器并行方案,然而这两种方法还不能解决目前的安全性和可用性问题。域分割方案把网络分成子网,并为每个子网分配不同的域,每个域都使用一个 KDC 管理密钥,当某个 KDC 被攻破只能影响一个子网的应用。然而这种方法不能有效地解决安全性和效率问题,因为不同域之间的 KDC 通讯非常复杂,并且 KDC 仍然拥有域上的所有密钥。服务器并行方案采用多个 KDC 服务器并行提供密钥服务,这种方法提高了可用性但是降低了安全性。因为每个并行服务器上都保存所有的 k_u,攻破并行服务器中的任何一个就可以攻破整个网络。这两种方法都无法解决广播通讯的密钥分配情况,因为这些分布式的密钥服务器无法把广播通讯的组名映射成同一个对称密钥。

本文提出的入侵容忍广播通讯 KDC 方案使用(k,n)秘密共享技术能够很好地解决广播通讯中的密钥分配问题,使用多个 KDC 服务器并行提供密钥服务,其中任意 k 个授权的 KDC 服务器组合都能够完成 $k_{u,v}$ 的计算,即使攻破了 $k-1$ 个服务器仍然不能计算出 $k_{u,v}$。采用双变量多项式构造(k,n)门限,能够实现广播组名到会话密钥的映射,并且其密钥具有一致性,即任意 k 个授权的密钥服务器通过拉格朗日插值获得广播会话密钥都是相同的。方案具有高效性、稳定性、健壮

收稿日期:2006 - 11 - 30;**修订日期**:2007 - 02 - 07
基金项目:国家 973 规划资助项目(G1999035802);国家 863 计划资助项目(2001AA141120)
作者简介:商建伟(1977 -),男,山东济宁人,博士研究生,主要研究方向:密码学、网络信息安全; 李锋(1968 -),男,山东济宁人,博士研究生,主要研究方向:密码学、网络信息安全; 张燕燕(1973 -),女,山东济南人,讲师,主要研究方向:密码学、网络信息安全.

性、可扩展性、健忘性、易于密钥更新等特点,可以有效地避免广播通讯时密钥分发的效率瓶颈。最后证明了本文提出的方案是可证安全的,并具有 proactive 安全特性。

1　模型定义

在 Shamir 的秘密共享方案[7,8]中,任意取 k 个部分密钥就能够生成秘密密钥,我们也希望在入侵容忍的 KDC 设计中达到这种效果,但 Shamir 的方案中必须先恢复秘密密钥,并且无法根据不同的广播群生成不同的通讯密钥,这是我们所不希望的,我们希望在任何情况下都不恢复秘密密钥,并能够把不同的广播群名称映射成不同的密钥。采用双变量多项式,固定一个变量 x,用变量 y 作为产生伪随机数的同余多项式,最后利用朗格朗日插值可以得到通讯密钥。为了能够提供高效率的密钥分配服务,使用多台 KDC 服务器并行提供密钥服务是可行的方法。使用 (k,n) 门限的伪随机数产生函数为广播群的实体产生广播通讯会话密钥,可以根据广播群名称等信息在 n 个 KDC 服务器中任选 k 个产生同一个对称密钥。这里首先对方案进行模型定义(见图 1),并介绍其应该满足的基本性质。

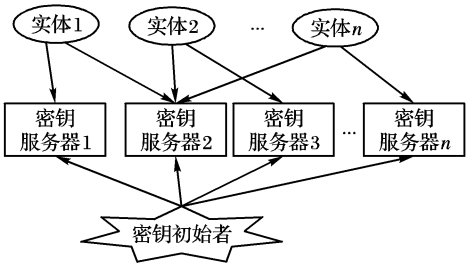

图 1　分布式密钥管理中心模型

初始基础:应用网络环境为 APP,其中包含 n 个 KDC 密钥服务器定义为 $S_1S_2\cdots S_n$,每个实体 u 至少能够和 k 个密钥服务器通过对称加密通道连接。

初始化过程:KDC 初始化时,由密钥初始者 S_D 产生密钥 α,并为每个密钥服务器 S_i($1\leqslant i\leqslant n$)产生一个服务器子密钥 α_i,初始化完成后通过安全途径保存密钥 α。

基本操作:实体 u 计算 $f(x)$,操作如下:

(1) 实体 u 连接任意 k 个授权的密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$,并发送消息 $<u,x>$。

(2) 每个密钥服务器 $S_{i_j}(j=1,2,\cdots,k)$ 验证 u 的权限,如果可以计算 $f(x)$,则计算 $F(\alpha_{i_j},x)$ 并把结果返回给实体 u。

(3) u 计算 $f(x)=C(h,F(\alpha_{i_1},x),\cdots,F(\alpha_{i_k},x))$。

定义 1　(k,n) 门限伪随机数产生函数。

(k,n) 门限的伪随机数产生函数是一个多项式时间可计算的三元组 $<S,F,C>$,其中 S 为密钥共享函数,F 为共享计算函数,C 为组合构建函数。记 $F_m=\{f_\alpha\}$ 是伪随机数产生函数的集合,安全参数为 m,初始密钥为 α。

(k,n) 门限的伪随机数产生函数满足以下条件:

(1) $\forall f_\alpha\in F_m, S(\alpha)=<\alpha_1,\alpha_2,\cdots,\alpha_n>$。

(2) 对于任意的 $1\leqslant i_1<\cdots<i_k\leqslant i_n$,$f_\alpha(x)=C(<i_1,F(\alpha_{i_1},x)>,\cdots<i_k,F(\alpha_{i_k},x)>)$。

(3) 对于任意的 $1\leqslant i_1<\cdots<i_{k-1}\leqslant i_n$,

$C(<i_1,F(\alpha_{i_1},x)>,\cdots,<i_k,F(\alpha_{i_{k-1}},x)>)$ 无法确定的 $f_\alpha(x)$ 的值。

(4) 根据 $\{f_\alpha(x_i)\}_{i=1}^{j}$,$1\leqslant j<m$,无法确定 $f_\alpha(x_{j+1})$,并且也无法得到 $f_\alpha(x)$ 的多项式形式,以及系统的密钥安全参数 m。

2　入侵容忍的广播通讯 KDC 方案

这里基于双变量多项式构造 (k,n) 门限伪随机数产生函数,方案无需密钥服务器间进行任何共享计算,只需要广播通讯密钥的申请实体 u 与任意 k 个授权的密钥服务器进行一次通信。所给的方案分成环境准备、密钥服务器子密钥生成、广播通讯影子密钥生成、广播通讯密钥构造四个阶段,前两个阶段由密钥初始者完成,后两个阶段由实体 u 与构造广播通讯密钥的 k 个授权密钥服务器合作执行。

第 1 阶段:环境准备

密钥初始者 S_D 定义有限域 Z_p,方案中的所有的数学计算都是在 Z_p 上完成。

定义 $F=\{P(x,y)\}$ 为有限域 Z_p 上的双变量多项式集合,F 中元素的表现形式为:

$$\begin{aligned}P(x,y)=M&+a_{11}+a_{12}y^1+\cdots+a_{1m}y^{m-1}+a_{21}x+\\&a_{22}xy^1+\cdots a_{2m}xy^{m-1}+\cdots+a_{k1}x^{k-1}+\\&a_{k2}x^{k-1}y+\cdots+a_{km}x^{k-1}y^{m-1}\end{aligned}$$

其中 x 为 $k-1$ 次,y 为 $m-1$ 次。

密钥初始者 S_D 选取有限域 Z_p 中的 km 个随机数,作为密钥 α 定义多项式 $P(x,y)$ 的系数,密钥 α 定义了 F 中的一个元素 f_α,函数的值域属于有限域 Z_p。

这里假设 KDC 与实体 u 之间的初始密钥分配已经完成,实体 u 在申请广播通讯密钥时至少能够与 k 个密钥服务器进行秘密通讯。

假设已经制定了所有实体 u 到广播组名 h 之间的映射规则 $h=\varphi(u)$,并制定了密钥服务器对实体的认证规则。

第 2 阶段:密钥服务器子密钥生成

密钥初始者 S_D 在第 1 阶段选择了密钥 α,从而确定了 F 中的双变量多项式,密钥初始者 S_D 为应用网络环境中的 n 个 KDC 服务器 $S_1S_2\cdots S_n$ 计算子密钥 $\alpha_i(1\leqslant i\leqslant n, i\in\mathbf{Z})$。

$$\begin{aligned}\alpha_i(y)=P(i,y)&=M+a_{11}+a_{12}y^1+\cdots+a_{1m}y^{m-1}+a_{21}i+\\&a_{22}iy^1+\cdots+a_{2m}iy^{m-1}+\cdots+a_{k1}i^{k-1}+\\&a_{k2}i^{k-1}y+\cdots+a_{km}i^{k-1}y^{m-1}\end{aligned}$$

α_i 为变量 y 的 $m-1$ 次多项式。

密钥初始者 S_D 经过安全可靠信道把子密钥 α_i 送给密钥服务器 S_i。

第 3 阶段:广播通讯影子密钥生成

实体 u 申请广播通讯的会话密钥时,向任意 k 个可以通过安全可靠信道连接的密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$ 发送广播密钥请求,密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$ 收到广播密钥请求后负责为实体 u 生成 k 个影子密钥,首先各密钥服务器验证实体 u 的身份(通过发送长度为 n 的认证信息实现),并把实体 u 的身份信息映射为广播组名信息,$h=\varphi(u)$(第 1 阶段假定已经定义了实体到广播组名的映射规则)。

密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$ 完成影子密钥计算,

$\beta_{i_j,h}=F(\alpha_{i_j},h)=P(i_j,h),1\leqslant j\leqslant k, j\in\mathbf{Z}$

如果实体 u 收到了 $<i_j,\beta_{i_j,h}>$ 表示 u 完成了对密钥服务器 S_{i_j} 的访问。

第 4 阶段:广播通讯密钥构造

实体 u 从 k 个密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$ 接收到 $<i_j,\beta_{i_j,h}>$ $(1\leqslant j\leqslant k)$,$u$ 根据 $\{<i_j,\beta_{i_j,h}>\}_{j=1}^{k}$ 执行拉格朗日插值计算,因为 F 中的双变量多项式 $P(x,y)$ 可以转化为以下形式:

$$P(x,y) = M + q_1(y) + q_2(y)x + q_3(y)x^2 + \cdots + q_k(y)x^{k-1}$$

其中 $q_i(y)$ 为 y 的 $m-1$ 次多项式($1 \leqslant i \leqslant k$)。当 y 固定为 h 时,定义 $f(h) = P(0,h)$,根据拉格朗日插值可以计算得到:

$$\begin{aligned} f(h) &= P(0,h) \\ &= M + q_1(h) \\ &= \sum_{j=1}^{j=k}\left[P(i_j,h)\prod_{r=1}^{r=k,r\neq j}\frac{-i_r}{i_j-i_r}\right] \\ &= \sum_{j=1}^{j=k}\left(\beta_{i_j,h}\prod_{r=1}^{r=k,r\neq j}\frac{-i_r}{i_j-i_r}\right) \end{aligned}$$

定理 1 $f(h)$ 为关于 h 的伪随机数发生函数

证明 $F = \{P(x,y)\}$ 为有限域 Z_p 上的双变量多项式集合,F 中元素的表现形式为:

$$P(x,y) = M + a_{11} + a_{12}y^1 + \cdots + a_{1m}y^{m-1} + a_{21}x + a_{22}xy^1 + \cdots a_{2m}xy^{m-1} + \cdots + a_{k1}x^{k-1} + a_{k2}x^{k-1}y + \cdots + a_{km}x^{k-1}y^{m-1}$$

可以表示成

$$P(x,y) = M + q_1(y) + q_2(y)x + q_3(y)x^2 + \cdots + q_k(y)x^{k-1}$$

$q_i(y)$ 为 y 的 $m-1$ 次多项式($1 \leqslant i \leqslant k$)。

由第 4 阶段的 $f(h)$ 的计算及拉格朗日插值的性质可知,任意的 k 个密钥服务器的插值运算结果必为 $f(h) = P(0,h)$,即 $f(h) = P(0,h) = M + q_1(h)$,因为方案中的所有计算都在有限域 Z_p 上,所以该函数为关于 h 的 $m-1$ 次同余随机数发生器,其函数值在有限域 Z_p 是伪随机分布的。

定理 2 方案是 proactive 安全[9] 的

证明 首先根据拉格朗日插值性质,任意的 $k-1$ 个服务器都无法完成插值运算得到 $f(h) = P(0,h) = M + q_1(h)$,因此攻击者即使掌握了 $k-1$ 个服务器也无法对系统造成攻击。因为对称密钥都在有限域 Z_p 中,因此密钥的值可以非常小(比如 128bit),同时可以获得比较大的密钥空间 m(比如 10^6)。根据同余伪随机函数的性质,其密钥空间内的密钥必将是均匀分布的,因此无法根据已经计算出来的通讯密钥获取新的对称密钥,攻击者根据已经获取的通讯密钥信息,无法完成对函数 $P(0,y)$ 的插值运算,所以在两次密钥更新的时间间隔内无论是对 $k-1$ 个服务器攻击还是对 $m-1$ 个密钥值进行攻击都无法获得 KDC 的安全密钥,因此系统是 proactive 安全的。

根据定义 $f(h) = P(0,h)$,本文所述的方案具有以下特点:

(1) 安全性:使用门限构造函数,攻击 $k-1$ 个服务器并不能威胁 KDC 的安全,也不能得到任何的 k_u 信息,因为 m 为 KDC 的安全参数,攻击者即使得到了 $m-1$ 个 $f_\alpha(x)$,也无法完成拉格朗日插值运算,所以也无法得到 $f_\alpha(x)$ 的多项式形式。

(2) 高效性:该方案在执行过程中,实体 u 与密钥服务器之间只进行一趟通讯,密钥服务器之间没有进行任何共享计算,因此也没有密钥服务器之间协同计算的代价。方案中 n 个服务器可以并行提供密钥服务,和服务器并行方案相比,需要经过 k 次计算才能完成密钥产生,但是方案可以使用 x 的低次多项式降低插值运算的复杂度,综合考虑该方案能够并行提供高效的密钥服务。

(3) 可扩展性:当需要对 KDC 的密钥服务器进行扩充时,只需在第 1 阶段由密钥初始者 S_D 为新增加的密钥服务器 S_r 计算子密钥 α_r,并通过安全可靠的信道把子密钥 α_r 分发给新增加的密钥服务器 S_r,这里:

$$\begin{aligned} \alpha_r &= P(r,y) \\ &= M + a_{11} + a_{12}y^1 + \cdots + a_{1m}y^{m-1} + a_{21}r + a_{22}ry^1 + \cdots + a_{2m}ry^{m-1} + \cdots + a_{k1}r^{k-1} + a_{k2}r^{k-1}y + \cdots + a_{km}r^{k-1}y^{m-1} \end{aligned}$$

(4) 健忘性:在方案的第 3 阶段,实体 u 可以通过安全可靠信道向 KDC 的任意 k 个密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_k}$ 申请广播通讯的影子密钥,访问任何密钥服务器 S_{i_r},($1 \leqslant r \leqslant k$),不依赖于前面访问的密钥服务器 $S_{i_1}S_{i_2}\cdots S_{i_{r-1}}$。

(5) 密钥更新:根据双变量多项式的性质,每个 KDC 服务器密钥 α_i 都是关于 y 的 $m-1$ 次多项式,并且不同的密钥服务器子密钥不同,因此只需要更新安全参数 m 的值就可以完成广播通讯密钥的自动更新。

(6) 健壮性:可以采用最简单的 Reed-Solomon 码[10] 的纠错功能防止密钥服务器的欺骗,这里可以要求实体 u 访问 $k' > k$ 个服务器,具体的实现方法参考文献[10],这里不再赘述。

3 安全性分析

该方案的安全性是可以保证的。

首先是一个密钥服务器的泄露和被敌人掌握只能泄露其掌握的部分秘密。因为 α_i 是关于 y 的 $m-1$ 次多项式,并且 α_i 没有暴露 KDC 密钥 α 的任何信息及 $P(0,y) = M + q_1(y)$ 的信息,$q_1(y)$ 为 y 的 $m-1$ 次多项式。任意一个 α_i 不暴露秘密密钥 α 的任何信息,即条件信息熵 $H(\alpha \mid \alpha_i) = H(\alpha)$。由于 α_i 与 $\alpha_j (i \neq j)$ 时是独立的随机变量,所以有 $H(\alpha \mid \alpha_i) = H(\alpha)$ 即多个随机的 α_i 也不反映 α 的任何信息,理论上说,任意 $k-1$ 个密钥服务器的泄露都不泄露秘密密钥 α。

其次,通过密钥服务器到实体 u 的广播信道也不能掌握密钥 α 的任何信息,通过密钥服务器到实体 u 的广播信道也不能掌握秘密信息 α 及 $P(0,y) = M + q_1(y)$ 的信息,在广播信道上只有各个服务器的 $\beta_{i,h} = F(\alpha_i,h) = P(i,h)$ 信息,攻击者即使能够进行 $f(h) = P(0,h) = M + q_1(h)$ 的插值运算,在密钥空间 m 内,因为 $P(0,y) = M + q_1(y)$ 为 y 的 $m-1$ 次多项式,攻击者也不能得到 $P(0,y) = M + q_1(y)$ 的任何信息也不能得到密钥 α 的任何信息。

最后,因为实体 u 与密钥服务器之间存在通讯密钥 k_u,所以可以实现实体 u 与密钥服务器之间的身份认证,防止密钥服务器欺骗,更安全的身份认证可以使用公钥密码体制进行改进。

防止密钥服务器的欺骗可以采用 Reed-Solomon 码[10] 的纠错功能。

4 结语

由于可以使用低次的 x 多项式减少实体 u 执行拉格朗日的插值运算,而 y 的次数为 m 即 KDC 系统中的密钥空间可以是一个相对比较大的整数,比如 $P(x,y)$ 中 x 的次数为 2,实体 u 只需要进行两次插值运算。方案采用 (k,n) 门限为广播通讯产生会话密钥,n 个密钥服务器可以并行提供密钥服务。n 的大小没有限制,可以根据业务的需要确定密钥服务器的数量,所以方案可以提供安全、可靠、高效的密钥服务,能够有效地避免广播通讯时密钥分发的效率瓶颈问题。最后,方案的安全性是可以保证的,并且具有 proactive 安全性。

(下转第 1053 页)

4）网络响应组件将作出响应,根据攻击 IP 地址列表给 192.168.1.10 发送 RST 包来解除对 192.168.1.10 的 DDoS 攻击,通过通信组件告知 node1 和 node2,还需要禁止更多的 IP 地址列;

5）node1 和 node2 的本地响应组件根据接收到的响应动作指令阻止所有攻击 IP。

在这个例子里,node1 和 node2 均为 manager 的订阅者,传递的信息包括超告警和响应动作。

2.5　其他

由于汇聚点管理多个本地 Agent,为避免单点失效,我们采用通信领域的主从备份机制,一旦关键点失效,立即进行主备倒换,可增强系统的健壮性。该模型事实上不存在物理的中心控制点,仅仅是逻辑上的,而且可以通过动态配置工具改变逻辑上的中心控制点使攻击者难以找到中心控制点的位置,这样可以避免传统分布式系统中央控制点成为攻击瓶颈的缺陷。

响应动作需要通过网络传递,因此需要定义统一的针对不同平台的格式规范,本文并不具体描述该规范,事实上该规范属于关联和汇聚组件的最终输出的一部分,因为关联和汇聚组件最后输出的是攻击者意图以及响应防御动作。

本模型没有涉及通信中的保密机制,通信保密机制已经相对成熟,我们可以基于 IPSEC 协议传递信息,同时使用密钥和数字签名的方式来保证信息收发方的真实性。

3　结语

本文提出一种分布式 IDS 系统模型,基于已有各种集中式 IDS,仅增加后台信息转换组件将告警信息转换为标准的 IDMEF 格式;数据分析单元基于 CRIM 框架,将 IDMEF 信息进行分类、汇聚和关联,关联组件分散在各采集点以及汇聚节点上,有效利用了网络资源;动作响应、格式转换以及分析单元采用自治 Agent 实现,综合了传统集中式 IDS 和 AAFID 框架的优点;节点间信息传递基于订阅模式,结合逻辑树组织结构,使攻击者难以找到中心控制点,避免攻击瓶颈。使用该模型能较为迅速并经济的搭建一个性能良好的分布式 IDS 系统。

今后工作主要包括:1）IDMEF 格式转换组件的开发;2）各关联和汇聚组件的实现,我们拟综合已有算法,通过设计一种攻击场景和攻击过程的因果关联语言并解释相关脚本来实现;3）网络传递协议的设计与实现,规范定义各通信代理之间的信息传递格式;4）实现网络配置工具。

参考文献:

[1] ROESCH M. Snort user manual 2.6.0[EB/OL]. http://www.snort.org/docs/snort_htmanuals/htmanual_261/, 2006-05-23.

[2] PORRAS P. The common intrusion detection framework architecture [EB/OL]. http://gost.isi.edu/cidf/drafts/architecture.txt, 1999-09-10.

[3] DEBAR H. The intrusion detection message exchange format[EB/OL]. http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-16.txt, 2006-03-16.

[4] PORRAS P, NEUMMAN P. EMERALD: event monitoring enabling response to anomalous live disturbances[A]. The 20th National Information System Security Conference[C]. Baltimore, Maryland, USA, 1997.353-363.

[5] SPAFFORD E, ZAMBONI E. Intrusion detection using autonomous agents[J]. Computer Networks, 2000, 34(4): 547-570.

[6] JANAKIRAMAN R, WALDVOGEL M, ZHANG QI. Indra: a peer-to-peer approach to network intrusion detection and prevention[A]. Proceedings of IEEE WETICE 2003[C]. Linz, Austria, 2003.

[7] WHITE G, FISCH E, POOCH U. Cooperating security managers: a peer-based intrusion detection system[J]. IEEE Network, 1996, 10(1): 20-23.

[8] 马恒太,蒋建春,陈伟峰,等. 基于 Agent 的分布式入侵检测系统模型[J]. 软件学报,2000,11(10):1312-1319.

[9] HOCHBERG J, JACKSON K, STALLINGS C. NADIR: an automated system for detecting network intrusion and misuse[J]. Computers and Security, 1993, 12(3):235-248.

[10] CHEN S. GRIDS: a graph based intrusion detection system for large networks[A]. Proceedings of the 19th National Information System Security Conference[C]. 1996.361-370.

[11] 穆成坡,黄厚宽,田盛丰. 入侵检测系统报警信息聚合于关联技术研究综述[J]. 计算机研究与发展,2006,43(1):1-8.

[12] NING P, CUI Y, REEVES D. Analyzing intensive intrusion alerts via correlation[A]. Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID) 2002[C]. Lecture Notes in Computer Science 2516, Berlin, Springer-Verlag, 2001.74-94.

[13] IBM Tivoli staff. Tracking and analyzing intrusion attempts with WebIDS[EB/OL]. http://www.ibm.com/developerworks/tivoli/library/t-webids/, 2003-01-01.

[14] Poppi S. Snort IDMEF plugin[EB/OL]. http://sourceforge.net/projects/snort-idmef/, 2005-11-15.

[15] CUPPENS F. Managing alerts in a multi-intrusion detection environment[A]. Proceedings of 17th Annual Computer Security Applications Conference (ACSAC)[C]. USA, 2001.22-31.

(上接第 1040 页)

参考文献:

[1] NEEDHAM R, SCHROEDER M. Using encryption for authentication in large networks of computers[J]. Communication of the ACM, 1978, 21(12):993-999.

[2] OTWAY D, REES O. Efficient and timely mutual authentication. Operating Systems Review, 1987, 21(1):8-10.

[3] BURROWS M, ABADI M, NEEDHAM R. A logic of authentication [A]. Proceedings of the Royal Society of London A, 1989, 426:233-271.

[4] DENNING D, SACCO G. Timestamps in key distribution protocols [J]. Communications of the ACM, 1981, 24, (8):533-536.

[5] WOO T, LAM S. A lesson on authentication protocol design[J]. Operating systems Review, 1994, 28(3):24-37.

[6] MILLER SP, NEUMAN C, SCHILLER JI, *et al*. Kerberos authentication and authorization system[M]. Project Athena Technical Plan Section E.2.1, MIT, 1987.

[7] SHOUP V. Practical threshold signatures[A]. Proceedings of the Eurocrypt 2000[C]. Bruges (Brugge): Springer-Verlag, 2000. 207-220.

[8] FRANKEL Y, GEMMELL P, MACKENZIE PD, *et al*. Optimal-Resilience proactive public-key cryptosystems[A]. IEEE Symposium on Foundations of Computer Science[C]. 1997. 384-393.

[9] CANETTI R, GENNARO R, HERZBERG D, *et al*. Proactive Security: Long-term protection against break-ins[J]. CryptoBytes, 1997, 3(1).

[10] MCELIECE RJ, SARWATE DV. On sharing secrets and Reed-Solomon Codes[J]. Communications of the ACM, 1981, 24(9):583-584.