文章编号:1001 - 9081(2006)05 - 1081 - 03

基于用户可信度的误用入侵检测系统的研究

郭庆北[1,2],张华忠[1],丁秀明[3]
(1. 山东大学 计算机科学与技术学院,山东 济南 250100;
2. 济南大学 信息科学与工程学院,山东 济南 250022; 3. 江南大学 信息工程学院, 江苏 无锡 214036)
(guoqb@126.com)

摘 要:提出了基于用户可信度的误用 IDS 模型,该模型对 IDS 框架结构、签名匹配策略及协同机制都进行了改进。鉴于通用入侵检测框架 CIDF(Common Intrusion Detection Framework)结构中缺少对入侵等级划分的机制,提出了基于用户可信度量化的等级划分方法,提高了系统的合理性。定义了误用 IDS 安全级别,通过预警原理实现低安全级别 IDS 对未知入侵的预防作用。另外,在用户可信度 IDS 中使用了局部性原理,进而改善了签名匹配策略并提高了签名的匹配效率和准确率。

关键词:用户可信度; 局部性原理; 预警; 自动响应
中图分类号: TP393.8 **文献标识码**:A

Misuse intrusion detection system based on user trust degree

GUO Qing-bei[1,2], ZHANG Hua-zhong[1], DING Xiu-ming[3]
(1. *School of Computer Science and Technology, Shandong University, Jinan Shandong* 250100, *China;*
2. *School of Information Science and Engineering, Jinan University, Jinan Shandong* 250022, *China;*
3. *College of Information Engineering, Southern Yangtze University, Wuxi Jiangsu* 214036, *China*)

Abstract: In this paper, a misuse detection model for IDS based on user trust degree (UTD) was firstly presented. This model improves the architecture of IDS, the strategy of signature matching, and the cooperation mechanism. UTD-IDS presents a means of graded partition that based on UTD whereas there is a lack of graded partition in the architecture of CIDF, so it improves the rationality of the system. The safety level of misuse IDS was defined and the IDS of lower safety level may prevent unknown intrusion from damage by the early-alert principle. In addition, was reformed full advantage of local principle were taken in UTD-IDS, then the strategy of signature matching, so it improves the efficiency and accuracy of signature matching.

Key words: user trust degree; local principle; early-alert; automation response

目前大多数 IDS 都采用 CIDF 或者类似于 CIDF 的框架结构,CIDF 几近成为 IDS 的事实标准,但是 CIDF 这一框架结构缺少对入侵等级的描述,也就不可能根据入侵等级进行响应,使得系统缺少公平性及合理性,要改变这种状况就必须改善 CIDF 框架结构中存在的不足之处,就需要在 CIDF 框架结构基础上构建等级划分模型,而要构建这样的模型是非常困难和关键的。还有目前不同的 IDS 特征库安装与升级不一致造成 IDS 安全级别的不同,如何使得低安全级别的 IDS 对未知入侵进行预警就需要设计相应 IDS 预警原理来实现。

本文将介绍一种基于用户可信度的误用 IDS 方案,该方案通过构建基于用户可信度 IDS 模型,实现了基于用户可信度的等级划分,通过预警原理实现低安全级别 IDS 对未知入侵的预防作用。另外,模型利用局部性原理引入了用户可信度表管理,提高签名的匹配效率与准确率,使得该模型非常适合当前高速网络的发展。

1 用户可信度的基本概念

1.1 用户可信度的定义

当任意用户访问目标系统(目标主机或者目标网络)时,此次访问可能是合法的访问,也可能是入侵行为。如果访问用户一直进行合法的访问,则目标系统对用户具有较高的信任度,相反,目标系统对用户信任度较低。这种目标系统对访问用户根据当前访问状态以及此前访问记录而产生的信任程度,称之为用户可信度。影响用户可信度的因素主要是以下两个方面:

(1) 入侵强度(intrusion intensity)。入侵强度是指网络入侵对目标系统的危害程度,入侵强度越大,危害程度则越大。入侵强度的不同,目标系统对用户的信任程度也就不同。入侵方式是决定这种危害程度的主要因素,入侵方式不同,入侵强度也不同。根据研究发现,网络入侵方式正在不断的升级,对目标系统的危害越来越大。

(2) 入侵频率(intrusion frequency)。入侵频率是指单位时间内网络入侵行为发生的次数。入侵频率越大,用户可信度越小,反之越大。用户可信度是动态变化的,它会随着用户访问行为的变化而变化,而入侵频率充分体现了用户行为的变化。

1.2 用户可信度模型

用户可信度模型是根据影响用户可信度的两个参数建立的,而且模型充分体现了用户可信度的所有特征。任何一种入侵方式对目标系统的影响可以分为三个阶段:在入侵方式产生初期由于对入侵方式的未知因此对目标系统的入侵强度很大;随着相应签名的建立及各目标系统签名的安装或升级,该种入侵方式的入侵强度随着时间的推移逐渐降低;一段时间之后入侵强度逐渐趋近于零。根据入侵强度变化规律构建

收稿日期:2005 - 11 - 21;**修订日期**:2006 - 03 - 01

作者简介:郭庆北(1976 -),男,江苏沛县人,硕士研究生,主要研究方向:网络安全、入侵检测; 张华忠(1963 -),男,山东济南人,教授,主要研究方向:网络安全、网络与分布式系统、传感器网络; 丁秀明(1978 -),女,山东潍坊人,硕士研究生,主要研究方向:Web Services 技术、网格计算.

入侵强度数学模型：

设入侵方式集合 $I=\{I_0,I_1,\cdots,I_n\}$，其中下标 i 代表入侵方式产生的次序，集合 I 对应的签名集合 $D=\{D_0,D_1,\cdots,D_n\}$，其中签名元素 D_i 对应入侵元素 I_i，函数 $t(I)$ 表示入侵方式 I 产生的时间。

$$I(I_m,t)=e^{-\lambda(t-t(I_m))} \tag{1}$$

其中，$I(I_m,t)$ 表示在 t 时刻入侵方式 I_m 所产生的入侵强度，λ 为调节系数并且 $\lambda>0$。

用户可信度主要由入侵强度及入侵频率两个因素决定，并且入侵强度的不同及入侵频率的变化都将对用户可信度造成不同的影响。用户可信度变化特征描述如下：

(1) 用户可信度的变化范围是[0,1]，用户可信度为 0 表示用户是完全不可信的，而用户可信度为 1 表示用户是完全可信的。

(2) 用户可信度主要由入侵强度及入侵频率两个因素决定。用户可信度与入侵强度和入侵频率均成反比，并且若一段时间内用户无入侵访问目标系统则用户可信度将增大，并且该状态持续时间越长用户可信度增大的也就越大。

(3) 用户可信度的上升幅度小于下降幅度。在单位时间内入侵发生与入侵没有发生等概率情况下，用户可信度上升幅度小于下降幅度，这是为了更好的安全考虑的。

根据用户可信度的变化特征构建用户可信度模型：将 $[0..t]$ 时间划分若干单位时间 $[t_0,t_1]$、$[t_1,t_2]\cdots[t_{m-1},t_m]$，$n_i$ 表示单位时间 $[t_{i-1},t_i]$ 内发生的入侵次数，函数：

$$f(n)=\begin{cases}0, & n=0\\ -1, & n>0\end{cases}$$

及

$$g(n)=\begin{cases}1, & n=0\\ 0, & n>0\end{cases}$$

为控制函数，主要是控制用户可信度值的变化。常量矩阵 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 及 $(\lambda_1,\lambda_2,\cdots,\lambda_n)$ 均为调节系数矩阵，主要是调节入侵访问用户可信度值的减小幅度，其中 $1>\sigma>0$、$\lambda>0$，并且入侵方式 I_i 对应 (σ_i,λ_i)，可由系统进行定义，μ 及 η 也为调节系数，主要是调节无入侵访问用户可信度值的增大幅度，其中 $\mu>0$、$\eta>0$，也由系统进行定义。

$$UTD(t_m)=\begin{cases}1, & UTD\geq 1\\ 0, & UTD\leq 0\\ 1+\sum_{i=1}^{m}\left[f(n_i)\cdot\sum_{j=1}^{n_i}\sigma_{ij}\cdot I^{ij}\cdot e^{\lambda_{ij}\cdot F(t_i)}\right. & \\ \quad\left.+g(n_i)\cdot\frac{\mu}{\overline{I^{ij}}}\cdot e^{-\eta\cdot F(t_i)}\right], & \\ 0<UTD<1\end{cases} \tag{2}$$

其中：$UTD(t_m)$ 表示 t_m 时刻的用户可信度，I^{ij} 表示在单位时间 $[T_{i-1},T_i]$ 内第 j 次入侵访问的入侵强度，$\overline{I^{ij}}=\sum_{j=1}^{i}\sum_{k=1}^{n_j}I^{jk}/\sum_{j=1}^{i}n_j$ 表示平均入侵强度，$F(t_i)=\sum_{k=1}^{i-1}n_k/i$ 表示入侵频率。

该模型主要优点如下：

(1) 模型根据入侵方式以及入侵频率的不同，给出用户可信度量化的等级划分，使得 $0\leq UTD\leq 1$。而 CIDF 框架模型缺少对信任的等级划分，从用户可信度理论来分析 CIDF，其用户可信度等于 0 或者 1，用户可信度模型体现了系统的公平合理性。

(2) 用户可信度的动态性，用户可信度随着用户访问状态的变化而改变。随着用户访问状态的变化，入侵方式及入侵频率不断变化，由此而计算出的用户可信度也在不断变化。

(3) 模型支持多种入侵方式并存的入侵情况。模型中入侵强度的描述不限于一种入侵方式，即使多种入侵方式同时入侵，模型也是可以表示出来，这使得模型有更好的实用价值，适合当前实际的网络入侵检测。

(4) 模型既适合主机 IDS，又适合网络 IDS。该模型是一个通用的 IDS 模型，并不局限于特定类型的 IDS，既可用于主机 IDS 又可用于网络 IDS。

2 UTD-IDS 框架结构及工作原理

UTD-IDS 框架结构包含数据采集器、用户可信度表管理器、事件分析器、UTD 生成器以及入侵响应单元等。数据采集器负责从高速网络上采集数据并承担简单数据包过滤，然后将数据传递给 UTD 表管理器；UTD 表记录当前一段时间内入侵用户的基本信息，UTD 表管理器将采集的数据包源 IP 地址与 UTD 表中的记录进行匹配，如果匹配不成功，则将数据传递给事件分析器，如果匹配成功，则将数据以及 UTD 表中记录的入侵方式传递给事件分析器；事件分析器是 IDS 的核心部件，如果已知 UTD 表中的入侵方式，则先根据已知的入侵签名进行匹配，否则根据事件数据库中记录的特征集来匹配数据包，如果匹配不成功，则认为是正常访问，如果匹配成功，则说明是某种入侵访问，将相关信息传递给 UTD 生成器；UTD 生成器根据获得的相关信息生成用户可信度并更新 UTD 表，然后将相应的用户可信度及相关信息传递给响应单元；响应单元负责分析接收的信息并决定对入侵事件进行响应或者响应撤销。UTD-IDS 框架结构如图 1 所示。

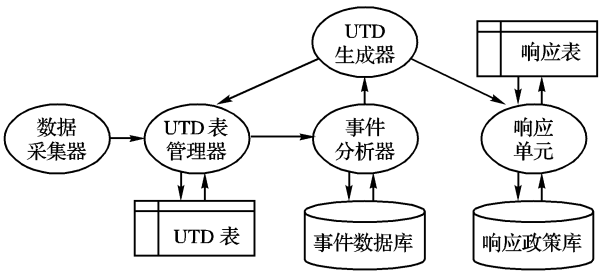

图 1 UTD-IDS 框架结构

根据 UTD-IDS 各部件功能及工作过程，给出相应的状态转换图，如图 2 所示。

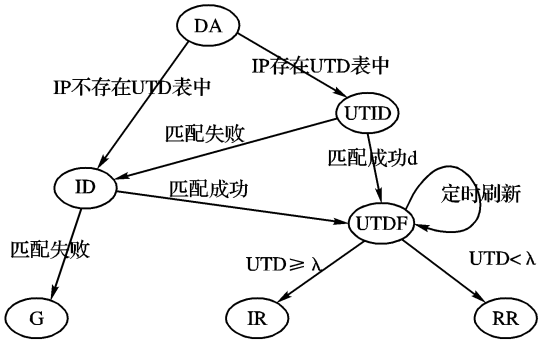

图 2 状态转换

当访问数据到达目标系统时，UTD-IDS 首先检查访问用户是否存在 UTD 表中，若存在则进行用户可信度入侵检测，若不存在则进行传统入侵检测，即根据与特征库中的签名匹

配结果来确定访问是否是入侵。用户可信度入侵检测首先根据 UTD 表中对应的入侵方式进行入侵检测,若签名匹配成功,则更新用户可信度,并且根据用户可信度值进行相应等级的入侵响应,而若签名匹配不成功,则进行传统入侵检测。若检测为另一种入侵方式,同样更新用户可信度,并且根据用户可信度值进行相应等级的入侵响应。

2.1　UTD 表工作原理

在 UTD-IDS 中 UTD 表的主要功能是记录当前的一段时间内访问用户的 UTD 及访问状态信息等,使得系统的管理更加方便。UTD 表的结构如表 1。

表 1　UTD 表结构

Source IP Address	Intrusion mode	UTD	TTL	Fla

其中,Source IP Address 字段表示访问用户的 IP 地址;Intrusion mode 字段表示入侵方式;UTD 字段表示用户可信度;TTL 字段表示当前记录的生命期;Flag 字段为标志字段,表示 UTD 是否本地计算生成,若 Flag = 0 表示 UTD 来源于相邻 IDS,若 Flag = 1 表示 UTD 为本地计算生成,该字段主要用于 IDS 协同预警功能

按照局部性原理,任意用户在时间和空间上再次访问同一目标系统的概率是相当高的。根据网络入侵的特点及 2004 年网络安全状况调查技术分析报告(2004 年,公安部公共信息网络安全监察局与中国计算机学会计算机安全专业委员会共同举办了全国首次信息网络安全状况调查活动),局部性原理同样适用于各种网络入侵攻击目标系统的行为。因此如果 IDS 能够有效的记录检测的结果并加以利用,按照局部性原理将能较好地提高 IDS 签名匹配的效率和准确率,UTD 表就是基于这种思想而建立的。就个别访问而言,系统增加了 UTD 表的检索时间,但就整体而言,系统节省了大量的签名匹配时间,并且签名匹配的准确率也有很大提高,大大提高了 IDS 运行效率,而且这使得 UTD-IDS 非常适用于当前高速的网络。

UTD 表的管理与维护:

(1) UTD 表的初始化:UTD 表在建立时为空表,不在 UTD 表中的任一访问用户都被默认为完全不可信的,就需要按照入侵检测签名匹配过程进行签名匹配,如果签名匹配成功,将按照公式(2)计算出 UTD,并将相关信息记录至 UTD 表,而如果签名匹配不成功,则认为用户是完全可信的,不记录至 UTD 表。

(2) UTD 表的更新:UTD 表的更新主要是两个方面的原因,一方面是新用户的入侵访问,另一方面是 UTD 表中已存在记录的变化。对于新用户的访问,当 UTD 表未满时新用户的入侵访问将在 UTD 表中增加新的记录,而当 UTD 表满时将替换 UTD 表中最旧的记录。而对于已存在用户的访问,从公式(2)可以看出,随着时间的推移无论 UTD 表中的用户是否继续入侵,UTD 值都将更新,具体的更新可由式(2)推导。

2.2　UTD-IDS 协同预警原理

对于误用检测 IDS 而言,IDS 的安全级别除了与所使用的检测技术、操作系统以及数据包捕获技术等有关外,更重要的是特征库是否进行及时的更新,及时更新的特征库将能检测更多的入侵方式,安全级别也就越高。基于这种特征构建用户可信度 IDS 安全级别模型。

设 IDS 的签名集合为 $D = \{D_0, D_1, \cdots, D_n\}$,其中特征元素 D_i 对应着入侵元素 I_i,$t(D)$ 表示签名 D 产生的时间,ρ 表示单位时间内平均产生的签名个数。θ_1 表示 IDS 的可能漏警率,θ_2 表示 IDS 的必然漏警率。

$$L(t,\theta_1,\theta_2) = \frac{|D|}{|D| + (t - t(D_n))\rho}(1 - \theta_1 - \theta_2) \quad (3)$$

其中,$L(t,\theta_1,\theta_2)$ 表示在 t 时刻 IDS 所具有的安全级别。可能漏警率 θ_1 是指由于 IDS 设计的缺陷、IDS 部署的问题以及数据包捕获技术等而造成的漏警率,它可以通过技术的改进而避免。必然漏警率 θ_2 是指由于 IDS 检测技术的不完善而造成的漏警率,它是不可避免的。漏警率 $\theta = \theta_1 + \theta_2$。

根据网络访问的局部性原理,当一个 IDS 检测到某攻击源入侵时,在一段时间内其相邻 IDS 所属系统很可能受到该攻击源的相同入侵。另外,由于各 IDS 特征库安装或升级不一致,因此各 IDS 的安全级别可能不同。这也就是说,对于某些攻击高安全级别的 IDS 可以检测出来,而低安全级别的 IDS 可能产生漏警。但是,通过 UTD-IDS 协同预警功能可以使低安全级别的 IDS 可以对其未知入侵进行预警。

下面给出 UTD-IDS 协同预警原理,如图 3 所示,其中,$I(User)$ 表示用户 $User$ 的某种入侵,IDS_0 与 $IDS_1 \sim IDS_n$ 相邻,IDS_i 的安全级别为 L^i,签名集合为 D^i。

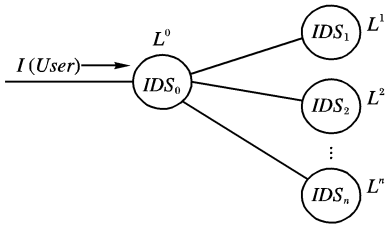

图 3　IDS 协同预警拓扑图

(1) 在特征集发生变化时向相邻的 *IDS* 发送特征集更新信息,使得各 *IDS* 知道其相邻 *IDS* 的安全级别;

(2) 当 IDS_0 受到入侵 I_m 的攻击时,如果 IDS_0 能够监测到入侵 I_m,则 IDS_0 向其相邻安全级别低于 IDS_0 并无法检测到入侵 I_m 即满足下述条件的 IDS_i 发送预警信息;

$$\frac{|D^i|}{(1 - \theta_1^i - \theta_1^i)\cdot\max(|D^0|,|D^i|)} < \frac{|\{I_0,I_1,\cdots,I_m\}|}{\max(|D^0|,|D^i|)} < \frac{|D^0|}{(1 - \theta_1^0 - \theta_1^0)\cdot\max(|D^0|,|D^i|)}$$

(3) IDS_i 将收到预警信息写入用户可信度表,并置 *User* 的 *UTD* 等于 0;

(4) 当 IDS_i 收到 *User* 访问时,拒绝其访问,当 *IDS* 特征集升级后方可允许 *User* 访问。

通过这种方法可以在一定程度上防止 *IDS* 对未知入侵对目标系统的攻击损害,达到预警作用。

3　传统 IDS 与 UTD-IDS 比较

UTD-IDS 在传统 IDS 基础上引入了用户可信度概念,给出了用户可信度的等级划分方法,对 IDS 框架结构、签名匹配策略及协同机制都进行了改进。下面给出传统 IDS 与 UTD-IDS 的比较结果:

(1) UTD-IDS 通过用户可信度实现入侵量化的等级划分,而传统 IDS 不对入侵进行严格的等级划分,这很难体现系统的公平合理性。

(2) UTD-IDS 利用局部性原理实现高效的签名匹配,提高签名匹配效率与准确率。而传统 IDS 主要是通过全局签名匹配来检测是否存在入侵,这将很难用于大规模的入侵检测系统。

(下转第 1095 页)

勾结的分享者是腐败的或不诚实的。攻击者可以得到腐败的分享者所拥有的任何秘密信息。

(2) 安全性

命题 1　对任何两个最小合格子集 $A_i = \{H_{i1}, H_{i2}, \cdots, H_{ik}\}$ 和 $A_j = \{H_{j1}, H_{j2}, \cdots, H_{jm}\}$,如果 A_i 和 A_j 中的成员都收到有效的份额,并且 $F_i(\alpha)$ 和 $F_j(\alpha)$ 也有效,那么由 A_i 中成员的份额所恢复出的秘密与由 A_j 中成员的份额所恢复出的秘密必定相同。

证明　由份额的分配算法及秘密的恢复算法可知,如果最小合格子集 A_i 和 A_j 中的成员的份额及公开信息 $F_i(\alpha)$ 和 $F_j(\alpha)$ 都有效,那么 $(I_{i1}, F(I_{i1}))$, $(I_{i2}, F(I_{i2}))$, $\cdots$, $(I_{ik}, F(I_{ik}))$ 及 $(\alpha, F_i(\alpha))$ 是 k 次多项式 $F_i(x)$ 上的 $k+1$ 个点,$(J_{i1}, F(J_{i1}))$, $(J_{i2}, F(J_{i2}))$, $\cdots$, $(J_{im}, F(J_{im}))$ 及 $(\alpha, F_j(\alpha))$ 是 m 次多项式 $F_j(x)$ 上的 $m+1$ 个点,因而它们各自唯一地确定出 $F_i(x)$ 和 $F_j(x)$。于是它们各自恢复出秘密 $F_i(0)$ 和 $F_j(0)$,由分配算法可知 $F_i(0) = F_j(0) = s$。证毕

命题 2　攻击者无法恢复秘密而且不能阻止由诚实的分享者构成的合格子集正确地恢复秘密。

证明　设 $A_i = \{H_{i1}, H_{i2}, \cdots, H_{ik}\}$ 是任一合格子集,由于攻击者无法得到 A_i 的全体成员的所有份额,他最多只能知道与 A_i 相应的 k 次多项式 $F_i(x)$ 上的 k 个点(其中包含了一个公开点 $(\alpha, F_i(\alpha))$),由这些点无法确定出 $F_i(x)$,也无法确定出 $F_i(x)$ 上的其他任何一个点。因此,攻击者无法恢复出秘密。另外,由于至少存在一个合格子集,其中的所有分享者都是诚实的,攻击者无法阻止这样的合格子集正确地恢复秘密。证毕

命题 3　攻击者所获得的信息是独立于被分享的秘密 s 的。即我们设计的密钥托管协议是安全的。

证明　首先,从分发者分发秘密份额所使用的多项式 $F(x)$ 来说,由于 $F(x)$ 的次数为 $n-1$,而攻击者所能知道的 $F(x)$ 上的点的个数不超过 $n-1$,因此,攻击者不能获得关于秘密 s 的任何信息;其次,从对应于每一最小合格子集 $A_i = \{H_{i1}, H_{i2}, \cdots, H_{ik}\}$ 的多项式 $F_i(x)$ 来说,$F_i(x)$ 的次数为 k,而攻击者最多只能知道 $F_i(x)$ 上的 k 个点,因此,他不能得到关于 $F_i(x)$ 的常数项 s 的任何信息。

综上可知,攻击者所获得的信息是独立于被分享的秘密 s 的。即设计的基于单向函数的密钥托管协议是安全的。证毕

由于在恢复密钥时,每个托管代理提交的是其屏蔽子密钥,$x_i = h(\alpha + s_i) \pmod p$。根据单向函数不可求逆的特性,其他人无法通过 x_i 求出 H_i 的子密钥 s_i,即每个托管代理的子密钥并没有因为通信密钥的恢复而被公开,从而可以继续使用。

同样,任何人也无法通过公开信息 α 及有序数组 $(y_1, y_2, \cdots, y_n)$ 与 $(d_1, d_2, \cdots, d_n)$ 来获取托管代理的屏蔽子密钥及秘密子密钥。

另外,当某个成员提供他的屏蔽子密钥后,可以通过验证等式 $y_i = h(x_i) \pmod p$ 是否成立,来判断该成员提供的份额是否有效,从而可以检验恶意参与者。

(3) 动态性分析

如果用户 A 要更换密钥,用户 A 只需和密钥管理中心重新协商密钥 s',用户再重新选择一个 $\alpha'(\alpha' \neq \alpha)$ 及一个新的 $n-1$ 次多项式 $F'(x)$, $F'(x) \neq F(x)$,满足 $F'(0) = s'$ 为新密钥,然后利用新的 α' 及 $F'(x)$ 更新公开的 α 与 $F_i(\alpha)$ 及有序数组 $(y_1, y_2, \cdots, y_n)$ 与 $(d_1, d_2, \cdots, d_n)$,而不必更换托管代理的子密钥;当有新成员 H_{n+1} 加入时,用户 A 只需随机生成一个 s_{n+1} 作为 H_{n+1} 的秘密子密钥。分配密钥时,完全可以按照文中的方案进行,而无须更改其他成员的子密钥;当删除某个成员时,用户 A 只需在其余 $n-1$ 个成员中分配密钥即可,也无须更改其他成员的子密钥。

7　结语

本文的动态密钥托管方案采用 ElGamal 公钥体制设计,由用户和密钥管理中心共同参与来产生用户的密钥,解决了文献[3]中的方案存在的问题;在进行密钥分配时,由用户、密钥管理中心和托管代理共同参与,既能保证托管内容的有效性、安全性,又能避免来自托管者的欺骗,确保了合法监听活动的有效实施;本方案应用可验证的动态密钥分拆体制,不但减少了各个托管代理者的地位、所拥有的权利及可靠性的差别,使得各托管代理在协议中所起的作用完全对等,能应用于更一般的接入结构;用户间通信时,可以动态选择会话密钥和恢复该密钥所用的多项式;方案恢复会话密钥时,可以对任意指定的托管方成员增加、减少、更换,而不必更改托管的密钥碎片,减少了通信量,提高了效率。

参考文献:

[1] DENNING DE. SMID M. Key escrowing today[J]. IEEE Communication Magazine, 1994, 32(9): 55-68.

[2] 宋荣功,詹榜华,胡正名. 基于多层次可验证共享协议的密钥托管方案[J]. 电子学报,1999,27(6):136-137.

[3] 蒋绍权,张玉峰. 部分密钥托管的监听体制[J]. 软件学报,2000,11(8): 1133-1137.

[4] GENNARO R. Theory and practice of verifiable secret sharing[D]. Massachusetts Institute of Technology (MIT); Cambridge, 1996.

[5] 张福泰,王育民. 无条件安全的广义可验证秘密分享协议[J]. 计算机研究与发展,2002,39(10):1199-1024.

[6] 何业峰,张建中. 基于单向函数的广义动态秘密分享方案[J]. 贵州大学学报(自然科学版),2003,20(4):358-360.

(上接第 1083 页)

(3) UTD-IDS 通过协同预警原理可以使低安全级别的 IDS 可以对其未知入侵进行预警,防止入侵对目标系统的进一步的攻击损害。而传统 IDS 的预警功能实现主要是分析入侵,并根据入侵的特点来检测将要到来的入侵。

参考文献:

[1] ZHANG J, DING Y, GONG J. Intrusion detection system based on fuzzy default logic[A]. FUZZ-IEE 2003[C]. St. Louis Missouri USA, 2003, 2(12243):1350-1356.

[2] HUANG MY, WICKS TM. A large scale distributed intrusion detection framework based on attack strategy analysis[J]. Computer Networks, 1999, 31(23-24). 2465-2475.

[3] YANG W, FANG BX, LIU B, *et al.* Intrusion detection system for high-speed network[J]. Computer Communications, 2004, 27(13): 1288-1294.

[4] DASARATHY BV. Intrusion detection[J]. Information Fusion, 2003, 4(4):243-245.

[5] ULVILA JW, GAFFNEY J, JOHN E. Evaluation of intrusion detection systems[J]. Journal of Research of the National Institute of Standards and Technology, 2003, 108(6):453-473.

[6] SIN LN, LEE MC. Intrusion detection system models[A]. Proceedings of the International Conference on Security and Management[C]. v 1, Proceedings of the International Conference on Security and Management, SAM 2003, 2003. 359-364.

[7] JIANG WB, SONG H, DAI YQ. Real-time intrusion detection for high-speed networks[J]. Computers & Security, 2005, 24(4):287-294.