动态自适应安全的(k, n)先应秘密共享系统设计*)

史庭俊[1,2] 马建峰[1]

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]

(扬州大学计算机科学与技术系 扬州 225009)[2]

摘 要 针对目前先应秘密共享系统基于经验方法的安全参数设置问题,本文将安全检测技术与先应秘密共享方案相结合,提出了动态自适应安全的先应秘密共享系统结构和响应方法。利用系统的安全审计日志,在评估移动攻击安全风险的基础上,分析了系统的共享服务器组由起始安全向入侵转移的渐进过程,建立了系统的状态转移模型,给出了系统的安全性定量分析和评估方法。并且,通过比较不同的门限配置、入侵率和安全阈值等参数情况,说明了维持先应秘密共享系统安全性的一般步骤,通过动态调整运行配置,实现系统安全的自适应控制和管理。给出了该方法应用的具体步骤,并验证了其有效性。

关键词 先应秘密共享,自适应安全,网络安全,移动攻击,马尔可夫链

Adaptive Security for (k, n) Proactive Secret Sharing Schemes

SHI Ting-Jun[1,2] MA Jian-Feng[1]

(The Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071)[1]

(Department of Computer Science and Technology, Yangzhou Univ., Yangzhou 225009)[2]

Abstract The proactive secret sharing (PSS) scheme divides the lifetime of a service into a series of interval, where the shares are periodically refreshed. This paper proposes a quantitative approach to evaluate the security of the proactive secret sharing system against the mobile attacks. Due to the difficulty in estimating quantitatively the attack ability, there have been few efforts to analyze the system security. Using the stochastic modeling techniques, we describe the relationship between the attacker behaviors and the security attributes of system. By probabilistic analysis, we estimate the availability of the proactive secret sharing system. As a result, it shows that the availability is significant dependent on the intrusion rate, the threshold and the time period. According to these results, we can maintain the availability by setting theoretically both threshold and time period based on quantitative approach rather than on the empirical knowledge.

Keywords Proactive secret sharing, Adaptive security, Network security, Mobile attack, Markov chain

1 引言

按攻击行为的特点分类,网络攻击可分为两种类型[1]:静态攻击(static attack)和移动攻击(mobile attack)。由于移动攻击成功入侵并控制一个服务器后,能将攻击目标转移到系统的另一个服务器上,因此,它对于长期连续运行系统(如PKI、CA、KDC等)所带来的安全威胁更加严重。为此,文[1~3]在(k, n)门限秘密共享方案中采用了主动安全机制,即先应秘密共享(proactive secret sharing, PSS)方案。该方案将服务系统的生存期划分为若干定长的连续时间片,其中,每个时间片由份额更新和服务响应两个阶段构成,在保证秘密信息不变的前提下,在份额更新阶段,系统的每个共享服务器无条件执行份额更新协议,更新内容包括秘密份额及内存数据等信息,同时将过期的秘密份额销毁。由于新旧份额信息之间相互无关,因此,移动攻击者通过入侵在前期获得的份额将变得毫无用处。这样,攻击者欲获得完整的秘密信息,则必须在一个时间片内入侵不少于门限值数量的服务器。与传统秘密共享方案[4]相比,PSS方案具有更强的安全性,其安全强度不仅与系统所采用的密码协议相关,而且还与门限值、更新周期等配置参数及攻击者的入侵能力密切相关。假设密码协议是安全的,那么,增大门限值或减小更新周期有利于提高系统的安全性,但是,这会造成系统的计算及通讯代价增加,同时亦会带来系统协议设计及分析困难等问题。特别是,在份额更新阶段,系统将暂停用户服务,因此,如果系统过于频繁地暂停服务,用户将是无法忍受的[5]。解决此问题的有效方法是在系统中引入自适应安全(adaptive security)机制[6]。所谓自适应安全是指系统采用非固定的安全工作模式,为获得最佳服务性能,能够根据其状态或环境的变化动态调整运行行为和安全规则。这里的变化是指系统部件故障、运行模式调整、用户需求改变或入侵风险波动等。1998年,Rabin[7]首先将自适应安全的思想用于RSA门限方案,其后,针对不同的应用背景,多种具有抗自适应攻击(adaptive attack)的门

*)基金项目:国家自然科学基金重大计划(90204012)、"863"高技术研究发展计划(2002AA143021)、教育部优秀青年教师资助计划、教育部科学技术重点研究项目、总装备部武器装备基金项目。史庭俊 博士研究生,主要研究方向为信息安全;马建峰 教授,博士生导师,主要研究方向为信息安全、密码学、编码学。

限密码方案[8~10]被相继提出。然而,这些工作的重点仅局限于自适应安全协议设计及其安全性分析等方面,对于自适应安全系统的结构和响应方法没有涉及。网络系统作为一个整体,如果仅从这两个方面研究其安全性问题显然是不全面的。

基于门限密码方案,本文提出了自适应安全的先应(k, n)秘密共享(Adaptively-Secure Proactive Secret Sharing, ASPSS)系统的结构和响应步骤,通过分析秘密共享系统由安全态向入侵态转移的过程,建立了系统安全性与系统状态和环境变化的定量关系,通过动态调整体统的运行配置参数:更新周期和系统门限,实现系统安全的自适应控制和管理。

2 ASPSS 系统模型

ASPSS 系统主要由共享服务器组和自适应控制器组成。共享服务器组 $S=\{S_1, S_2, \cdots, S_n\}$,其中每个服务器 S_i($1\leqslant i\leqslant n$)通过完全的点到点通信信道互连起来,它们共享一个秘密信息 X,S_i 与自适应控制器互连并共享一个会话密钥 K_i。S_i 分别秘密持有 X 的一个秘密份额 x_i,S 中任意数目不少于 k 的服务器集合能够重构出信息 X。系统全局时钟能以可变时间间隔将运行时间划分为连续的时间片:$T^{(0)}$, $T^{(1)}$, …, $T^{(i)}$, …,这里 $T^{(i)}$ 为第 i 个时间片。

定义 1 n 个共享服务器 $S=\{S_1, S_2, \cdots, S_n\}$ 存在多样性构造。如果 S 满足:

(1)服务器 S_i 有各不相同的口令、份额和证书等秘密信息;

(2)运行于服务器 S_i 的软件系统采用多版本程序设计;

(3)组成每个服务器 S_i 的硬件系统是异构的。

共享服务器的多样性构造是保证 ASPSS 系统安全的一个基本要求,它使得移动攻击入侵每个服务器可能采取的方法是互不相同的,从而有效保证了每个服务器具有同等的入侵难度,避免了移动攻击者成功入侵某个服务器后,能够以相同的方法在短时间内迅速入侵更多的服务器。

自适应控制器是 ASPSS 系统的关键部件,它由环境风险评估器、系统安全评估器、安全策略库和事件执行器等 4 部分组成。如图 1 所示:

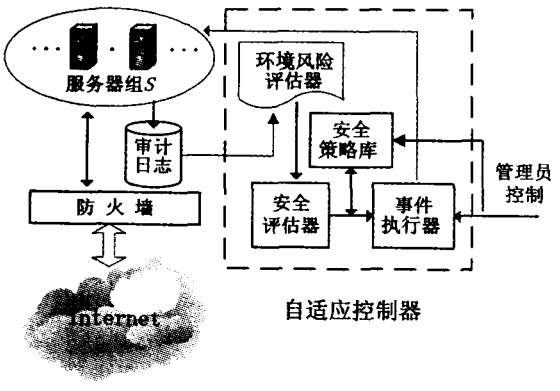


图 1 自适应安全先应秘密共享系统模型

审计日志:记录各服务器的异常信息,其中包括系统身份认证机构不能确认的身份、与访问安全等级不相符合的数据、对系统运行产生重要影响的动作及其它与安全相关的动作等。安全审计记录应包含如下信息:事件发生的日期、时间、事件类型、主题标识、执行结果、引起此事件用户的标识等。

环境风险评估器:它是自适应控制器的输入部件,其输入信息由系统的审计日志获得。审计日志反映了当前一段时间入侵攻击的危害程度,从中环境风险评估器可定量获得当前的网络入侵风险程度。文[11]给出了审计日志格式和评估方法。

安全评估器:根据入侵风险程度和当前系统的状态,采用随机建模方法定量评估系统的安全性,为事件响应器提供决策依据;

安全策略库:定义了系统的安全性与安全策略之间的映射关系。存储系统管理员制定的安全策略和在线学习功能形成的新策略。策略包括系统配置参数调整,报警策略等。在门限方案中,配置参数与系统性能是相互关联的,一方面,参数的选取需满足安全性要求,另一方面,它们要受到诸如系统成本、规模及设计复杂程度等多种因素的制约。针对不同的应用,策略库是综合多方面因素的折衷。

事件执行器:事件执行器完成相应的决策命令发布。其输入信息有两个来源:安全评估和安全策略库、管理员控制。在这两种信息中,管理员控制命令发布具有优先执行权。

3 ASPSS 系统的响应过程

ASPSS 系统对于入侵威胁程度变化的自适应安全响应过程分为变化检测、安全性评估和事件响应 3 个阶段。

3.1 安全风险变化检测

通过审计日志能够获得安全风险程度及其变化趋势。尽管,常用的安全检测系统存在一定的缺陷,但环境风险评估器不必要严格判断攻击者、攻击类型等细节,仅需从中统计出当前入侵的活跃程度信息和变化情况。Jonsson[11]将入侵攻击划分为三个阶段:试探期(learning phase)、标准攻击期(standard attack phase)和创新攻击期(innovative attack phase),其中,标准攻击时间远大于其它两个时间。在标准攻击阶段,服务器被入侵的概率最大,并且被入侵概率符合指数分布。由此,服务器 S_i($1\leqslant i\leqslant n$)在时刻 t 被入侵的概率可表达为:$P(t)=1-e^{-r_i t}$,式中 r_i 为指数分布参数,在此称为入侵率(intrusion rate)。r_i 反映了攻击者入侵的能力,若某个攻击者入侵能力强,r_i 值则大,反之,r_i 值则小。在现实世界中,尽管入侵攻击的手段千差万别,并且攻击者个体之间存在巨大差异,但让风险评估器定量刻画每个攻击者的入侵能力是不必要的,风险评估可忽略这种差异,将具有最强破坏能力的入侵率 r 作为分析的基准,显然从安全角度看,如此简化是合理的。因此,为保证秘密信息 X 的机密性,参数 $T^{(i)}$、k 分别可看作是 r 的函数。

3.2 安全性评估

3.2.1 共享服务器组的状态转移 随着共享服务器组中被入侵服务器数量的增加,系统将由 $T^{(i)}$($i=0,1,\cdots$)时刻的起始安全态向入侵态逐渐转移。令 m 为 $\tau=T^{(i)}+t$($0\leqslant t<T^{(i+1)}-T^{(i)}$)时刻系统中被入侵的服务器总数,这里,$m$ 与 t 相关,而与 $T^{(i)}$ 之前的状态无关。以系统中被入侵服务器的数量表示系统的状态,则系统的状态集合可以表示为有限状态集 $F=\{F_0, F_1, \cdots, F_m, \cdots, F_n\}$。由于服务器组的多样性构造保证了移动攻击的入侵方法和过程是无关的,并且,指数分布满足无记忆性(memoryless),因此,状态集合 F 可看作是一个连续时间的 Markov 链(CTMC),并且,所有的状态转移只会发生在相邻的两个状态之间。即,对时间 $0\leqslant t_0<\cdots<t_m<\cdots<t_n$ 和状态 $F_0, \cdots, F_m, \cdots, F_n\in F$,有条件概率

$$p_m(t)=P\{C(t_m)=F_m \mid C(t_0)=F_0, C(t_1)=F_1, \cdots, C$$

$(t_{m-1})=F_{m-1}\}=P\{C(t_m)=F_m|C(t_{m-1})=F_{m-1}\}$ (1)

由于某个服务器一旦被入侵,那么,它将始终处于失效状态,所以系统在时间片$[T^{(i)},T^{(i+1)}]$上的状态转移是一纯生过程。其转移过程如图2所示:

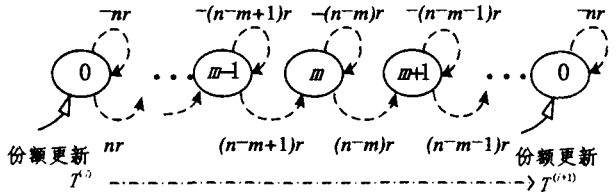


图2 $[T^{(i)},T^{(i+1)}]$时间片服务器状态转移强度

3.2.2 *共享服务器组的安全性评估* 由图2可得服务器组状态转移强度矩阵Q为:

$$Q=\begin{bmatrix} -nr & nr & & & & & \\ & -(n-1)r & (n-1) & & & & \\ & & \cdots & \cdots & & & \\ & & & -(n-m)r & (n-m)r & & \\ & & & & \cdots & \cdots & \\ & & & & & -r & r \\ & & & & & & 0 \end{bmatrix} \quad (2)$$

$Q=(q_{ij})_{(n+1)\times(n+1)}$为二对角矩阵。事实上,由于入侵率$r$值有界,且$\sup_{i\in F}|q_{ij}|<\infty$,则$Q$为有界保守矩阵。以$P(t)$表示服务器组状态转移概率矩阵,那么,Kolmogorov微分方程成立:

$$P'(t)=P(t)Q,\ t\geqslant 0 \quad (3)$$

由于$P(0)=I$(单位矩阵),所以有:

$$P(t)=e^{Qt} \quad (4)$$

考虑到$T^{(i)}(i=0,1,\cdots,)$时刻,服务器组是安全的,则系统初始概率分布:

$$p(0)=(p_0(0),\ p_1(0),\cdots,\ p_n(0))=(1,0,\cdots,0) \quad (5)$$

由(4),(5)可得:

$$p(t)=p(0)P(t)=p(0)e^{Qt},t\geqslant 0 \quad (6)$$

在$p(t)=(p_0(t),\ p_1(t),\cdots,\ p_n(t))$的分量中,$p_0(t)$,$p_1(t),\cdots,\ p_{k-1}(t)$为服务器组安全态转移概率,$p_k(t)$,$p_{k+1}(t),\cdots,\ p_n(t)$为失效态转移概率。

定义2 设运行时刻t,(k,n)门限ASPSS系统处于状态$F_i(0\leqslant i\leqslant n)$的概率为$p_i(t)$,系统的安全性为被入侵服务器总数小于$k$的概率之和,即

$$A(t)=\sum_{i=0}^{k-1}P_i(t)$$

系统运行时刻t,如果$A(t)$不低于某个安全阈值,那么自适应控制器可以认为此时系统是安全的,反之,系统则是不安全的。自适应控制器通过动态调整$T^{(i)}$,门限k等配置参数维持系统的安全。

3.3 事件响应

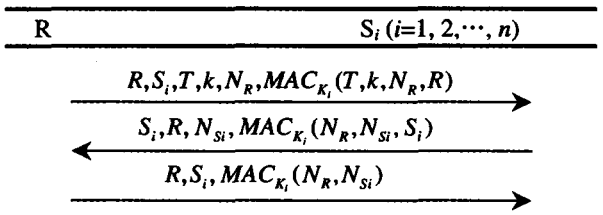
3.3.1 *控制命令传送* 审计日志中入侵风险的变化触发事件响应器对运行系统的安全性进行定量评估,从而得到系统最佳的参数配置。系统获取最佳参数配置的方法有两种:安全评估及策略自适应、系统管理员根据秘密信息的重要程度调整系统的参数配置。这里,管理员控制方式具有优先响应权。先应秘密共享协议设计及实时调整门限值的方法可参见文[1~3]和文[12,13]。

事件响应自适应命令传送有如下要求:

·正确性:确保每个共享服务器接收命令来自事件响应器,而不是假冒的;

·完整性:确保共享服务器接收命令未被恶意服务器篡改、重放或延迟。

为此,事件响应器与每个共享服务器间执行如下双向认证协议:



这里,R和$S_i(i=1,2,\cdots,n)$分别代表事件响应器和共享服务器S_i的标识,N_R和N_{Si}分别为R及S_i为完成命令传送生成的两个一次随机数。MAC为单向杂凑函数(如MD4、MD5、SHA等),用于消息认证,保证传输命令的真实性和完整性,K_i为R和S_i共享会话密钥。在R与S_i信息交互过程中,如果R不能确定S_i的可靠性,可采取向管理员实时报警、切断链路、甚至关闭所有主机等安全控制措施。

3.3.2 *振荡现象* 在自适应安全系统中,系统振荡(oscillation)[14]会导致系统拒绝服务。产生系统振荡的原因是:当环境安全风险发生变化时,自适应系统随之调整其工作模式,但是,如果调整过程太频繁,且不受控制,那么,系统将不能稳定于一个正常运行状态。在ASPSS系统中,自适应控制器不与外部网络直接连接,其输入信息由审计日志统计获得。由于审计日志是相对较长一段时间入侵攻击危害程度的数据记录,那么,攻击者将无法利用一般自适应安全系统存在的振荡特性发动拒绝服务攻击。

4 应用实例与分析

4.1 入侵率与安全性的关系

图3为(4,7)门限ASPSS系统的安全性与入侵率之间的关系,这里r的取值分别为0.01、0.02、0.04和0.08。

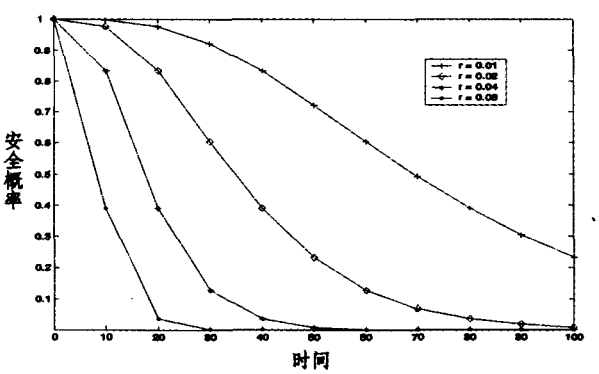


图3 (4,7)门限ASPSS系统在不同入侵率下的安全概率比较

由图3可以看出,随着一个时间片内系统运行时间和入侵率增加,安全性将降低,在一定入侵率下,保持系统的安全性水平可通过减小更新周期间隔获得。

4.2 门限值与安全性的关系

设r为0.02,如图4所示为不同门限与安全性之间的关系曲线。

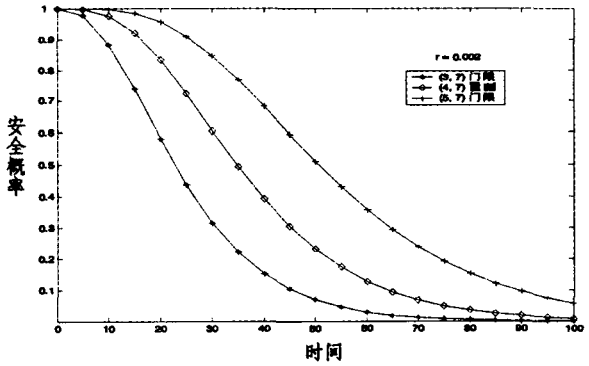


图 4　不同门限时 ASPSS 系统安全概率比较

由图 4 可见，提高门限有利于系统的安全，但门限值提高的同时会造成系统计算及通信负荷的增加，图示关系为选取恰当的门限值提供了有价值的参考依据。

4.3　入侵率变化与更新周期的关系

给定某个安全阈值后，如果环境入侵风险波动，自适应控制器通过调整更新周期维持系统的安全性水平。图 5 为(4，7)门限 ASPSS 系统分别在不同安全阈值下，更新周期随入侵率的变化关系。

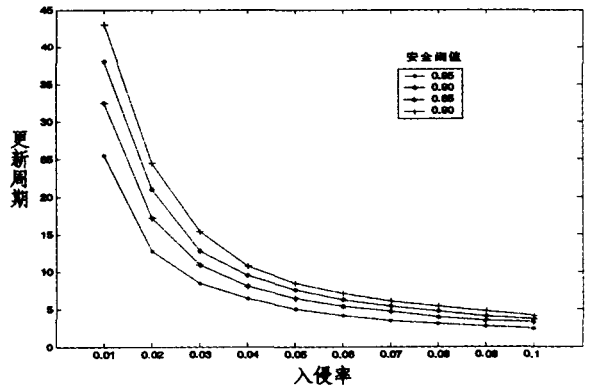


图 5　不同安全阈值下入侵率与更新周期之间的关系

图中安全概率阈值分别取 0.95、0.90、0.85 和 0.80。由图 5 可以看出，随着入侵率增大，为维持一定的系统安全阈值，自适应控制器应动态地减小系统的更新周期。

结论　本文将系统安全检测技术与先应秘密共享方案相结合，通过分析系统运行的安全日志，在定量评估环境安全风险的基础上，提出了自适应安全的先应秘密共享系统结构和响应方法。本文分析了移动攻击下，系统的共享服务器组由安全向失效转移的渐进过程，建立了系统的安全状态转移模型，给出了系统的安全性的定量分析和评估方法。据此，通过比较不同门限配置、入侵率和安全阈值下系统的安全性，给出了维持系统安全的一般步骤和方法。通过动态调整系统的运行配置，实现系统安全的自适应安全管理。尽管本文针对先应秘密共享体制，但文中提出的自适应安全结构和分析方法，对于其它分布式系统(如分布式计算、Byzantine 协商等系统)同样具有重要的参考意义。

参 考 文 献

1　Herzberg A, Jarecki S, et al. Proactive secret sharing or: How to cope with perpetual leakage. Advances in Cryptology-Crypto '95. Lecture Notes in Computer Science, Springer-Verlag, 1995, 963:457～469

2　Ganetti R, Gennaro R, et al. Proactive security: long-term protection against break-ins. CryptoBytes, 1997, 3(1):1～8

3　Frankel Y, MacKenzie P, Yung M. Adaptively-secure optimal-resilience proactive RSA. Advances in Cryptology-Asiacrypt '99, Lecture Notes in Computer Science, Springer-Verlag, 1999, 1716:180～194

4　Shamir A. How to share a secret. Comm. ACM, 1979, 22(11): 612～613

5　Research Z. The economic impacts of unacceptable web-site download speeds: [Technical Report]. 1999. http://www.webperf.net/info/wp_downloadspeed.pdf

6　Canetti R, Damgaard I, et al. On adaptive vs. non-adaptive security of multiparty protocols. Advances in Cryptology-EUROCRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, 2001, 2045: 262～279

7　Rabin T. A simplified approach to threshold and proactive RSA. Advances in Cryptology -Crypto '98, Lecture Notes in Computer Science, Springer-Verlag , 1998, 462:89～104

8　Canetti R, Gennaro R, Jarecki S, et al. Adaptive security for threshold cryptosystems. Advances in Cryptology-CRYPTO 99. Lecture Notes in Computer Science, Springer-Verlag, 1999, 1666:98～115

9　Lysyanskaya A, Peikert C. Adaptive security in the threshold setting: From cryptosystems to signature schemes. Advances in Cryptology-ASIACRYPT2001, Lecture Notes in Computer Science, Springer-Verlag, 2000, 2248:331～350

10　Jarecki S, Lysyanskaya A. Adaptively secure threshold cryptography: introducing concurrency, removing erasures. Advances in Cryptology-EUROCRYPT 2000. Lecture Notes in Computer Science, Springer-Verlag, 2000, 1807:190～206

11　Jonsson E. A quantitative model of the security intrusion process based on attacker behavior. IEEE Transactions on Software Engineering, IEEE press, 1997, 23(4):1～10

12　Martin K M, Pieprzyk J, et al. Changing thresholds in the absence of secure channels. Australian Computer Journal, 1999, 31(2):34～43

13　Maeda A, Miyaji A, et al. Efficient and unconditionally secure verifiable threshold changeable scheme. In: Proc. of ACISP2001, Lecture Notes in Computer Science, Springer-Verlag, 2001, 2119:403～416

14　Bryant S, Wang F. Aspects of Adaptive Reconfiguration in a Scalable Intrusion Tolerant System. Complexity, 2004, 9(2): 74～83