异构冗余系统的安全性分析

王 伟 杨本朝 李光松 斯雪明

(信息工程大学数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 随着互联网技术的发展和普及,漏洞和后门已经成为导致网络安全问题的主要因素。冗余技术可以很好地解决系统的可靠性问题。受拟态防御思想的启发,分析了异构冗余技术对基于漏洞和后门的网络攻击进行安全防御的有效性。在一些假设前提下,以系统攻击成功率表征系统的安全性,建立了基于马尔科夫过程的异构冗余系统的安全性评估数学模型,给出了系统攻击成功率的表达式。最后对3模异构冗余系统进行了求解和分析,计算结果与直观预期相符。

关键词 拟态防御,异构冗余,漏洞后门,马尔科夫

中图法分类号 TP309.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.09.030

Security Analysis of Heterogeneous Redundant Systems

WANG Wei YANG Ben-chao LI Guang-song SI Xue-ming

(State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China)

Abstract With the development and popularization of Internet technology, vulnerability and backdoor problems have become the main factor of network security problems. The redundancy technology can solve the reliability problem of system. Inspired by the idea of the mimicry defense, this paper analyzed the effectiveness of the heterogeneous redundant technology against the security defense based on the vulnerability and backdoor network attack. On some assumptions, this paper established a security model of heterogeneous redundant system based on Markov process. System security was characterized by the success rate of system attack, and the expression of success rate of system attack was given. At last, triple-redundant heterogeneous system was solved and analyed. The experimental results are in accordance with the intuitive expectations.

Keywords Mimic defense, Heterogeneous redundancy, Vulnerability backdoor, Markov

1 引言

20世纪90年代以来,互联网呈现出异乎寻常的指数增长趋势,同时各种信息安全事件层出不穷,且愈演愈烈,严重影响到人类社会活动和发展的方方面面。作为当前网络信息技术发展的重要组成部分,信息系统软硬件中的安全漏洞成为直接影响系统安全性的决定性因素[1]。实践证明,绝大部分信息安全事件都是攻击者借助软硬件漏洞发起的,随着攻击者技术水平的快速提升,漏洞后门的危害越来越大。

被广泛接受的关于漏洞的定义为[1]:软件系统或信息产品在设计、实现、配置、运行等过程中,由操作实体有意或无意产生的缺陷、瑕疵或错误,它们以不同形式存在于信息系统的各个层次和环节之中,且随着信息系统的变化而改变。然而,针对软硬件设计缺陷导致的漏洞问题,目前在理论和技术上尚无有效的解决办法,试图从根本上杜绝也违背了人类认知时空局限性的客观规律。这就意味着无论从技术上还是经济上都不可能彻底保证网络空间构成环境内无漏洞后门,即"无毒无菌"。如何在网络空间"有毒带菌"的条件下实现有安全保障的"沙滩建楼",缓解"已知的未知"风险和"未知的未知"威胁挑战,便成为了一个亟需解决的很自然的科学问题。

基于此,我国科学家邬江兴院士提出了拟态防御思想[2-4],旨在为解决网络空间不同领域内相关应用层次上的基于未知漏洞、后门或病毒木马等的不确定性威胁,提供具有普适性的创新防御理论和方法。概括来说,拟态防御试图跳出传统"亡羊补牢"式的修复防御思维定式,使得核心设备的安全性不再过度依赖软硬件设计、制作、运行和管理环节的"自主可控"程度与安全水平,而是要使信息系统能够在一定程度或约束条件下包容软硬构件层面"有毒带菌"的现状。

基于上述认识,通过一种功能等价的异构冗余构造,使得攻击者对目标系统的漏洞或后门的可视性和可达性成为挑战性问题。文中首先介绍了冗余技术的应用及对解决网络安全问题的思考;在一些基本前提和相关定义下建立了基于马尔科夫过程的异构冗余系统的安全性评估模型;然后对3模异构冗余系统进行了求解和有效性分析;最后分析了该模型中

到稿日期:2017-08-01 返修日期:2017-11-17 本文受国家重点研发计划(2016YFB0800101),国家自然科学基金(61602512)资助。

王 伟(1984-),男,硕士,讲师,主要研究方向为拟态安全、区块链,E-mail:ntfyllyj@aliyun.com(通信作者);**杨本朝**(1982-),男,硕士,讲师,主要研究方向为拟态安全;**李光松**(1977-),副教授,硕士生导师,主要研究方向为信息安全、密码协议;**斯雪明**(1966-),男,教授,硕士生导师,主要研究方向为拟态安全、大数据。

存在的一些问题和下一步的工作方向。

2 冗余技术

冗余技术又称储备技术,它是利用系统的并联模型来提高系统可靠性的一种手段,即通过增加多余的同等功能的执行体,并通过一定的冗余逻辑使它们协调地同步运行,从而使系统的应用功能得到多重保证。冗余技术被广泛用于解决随机发生的物理性故障或由于设计缺陷引发的不确定性故障。然而,实践中人们发现在同构冗余(isomorphism redundancy)模式下,也就是使用完全一致的电路、结构、材料等参数的构件作为并联组件时,某些条件下容易因为单个特定的故障冲击作用导致多个并联组件同时失效,这种现象被称为共模失效(common mode failure),会极大地降低同构冗余系统的可靠性。为了有效降低共模失效的概率[5-6],人们又发展了异构冗余(heterogeneous redundancy)模式,即并联使用多个功能或性能等价的异构组件。典型的异构冗余模型如图 1 所示。

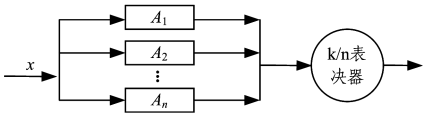

图 1 异构冗余结构图

Fig. 1 Heterogeneous redundancy architecture

图 1 中,A_i 表示异构冗余系统(以下简称系统)的各个执行体,各执行体是功能等价的异构体,对于每一个输入 x,各个执行体会独立运算得出结果 $f_i(x)(i=1,2,\cdots,n)$。对于这 n 个运算,由表决器基于择多原则得到系统的最终输出。

作为一种合理推测,既然冗余技术可以有效抑制自然发生的不确定性故障(无论是差模还是共模故障)对目标系统可靠性的不良影响,那么自然有以下设想:能否借助其基本机理来应对网络空间人为的基于目标对象未知漏洞后门等的不确定威胁;或者说在满足什么样的条件下,抗攻击问题或网络安全问题能够归一化为可靠性问题来处理。

文献[7-8]对同构冗余引发的共模失效问题进行了相关讨论。但对于软硬件人为设计缺陷导致的漏洞或后门,同构的冗余处理空间在机理上是不可能有效应对的。这是因为冗余空间内的所有软硬件都具有完全相同的设计和功能以及非常相似的性能,也包括可能存在的任何设计缺陷都会原封不动地复制到冗余空间内的各个组件上。在相同的输入激励条件下,冗余空间内各组件的计算应当具有一致性,包括一致的正确结果(正常情况下属于大概率事件)和一致的错误结果(正常情况下属于小概率事件),当相同设计缺陷引发共模故障时,同构冗余因为难以做出正确研判而失去基于架构的容错功能。

文献[9-10]对异构冗余系统的安全性做了相关分析,但其是在入侵检测的基础上而做的一系列分析,即该分析是在获得先验知识的前提下进行的容侵分析。借助“同一问题通常有多种解决方法,同一功能往往有多种实现结构”的公理,异构冗余从机理上可以避免同构冗余面对未知设计缺陷无能为力的难题。解决问题和实现功能的思路、方法、工具、条件等的不同,甚至不同实现者或工程团队的阅历和文化背景的差异,都会使解决问题的算法选取或方法创造以及满足功能要求的结构设计在具体实现上存在诸多的不同,甚至可能采取完全不同的技术路线[11],这就保证了在功能等价和计算结果大概率一致的前提条件下,即便是设计实现中存在的缺陷或错误,也都具有差异化的属性和表现,使得异构冗余空间出现多数或完全相同错误的概率很低。

但是,从统计意义上说,多数表决判定的结果也可能是错误的,即当多数或全部输出矢量出现完全相同错误的情形。也就是说,多数表决机制也会出现把异常判定为正常的情况,我们称之为表决“逃逸现象”(escape phenomena)。

在异构冗余架构内,每个功能等价的异构执行体尽管都可能存在未知的漏洞后门甚至木马、蠕虫等病毒,但是相异性设计和环境条件使得它们很可能各不相同,而且漏洞等的触发机制或内外通联的方式及信息内容也不尽相同。理论上,只要确保异构冗余执行体间是独立的,即不存在任何相关性或协同性,那么就很难用相同或不同的攻击手段同时作用于所有的异构冗余执行体并产生完全一致的异常输出。也就是说,不论什么样的攻击,只有造成“全部或多数异构执行体的输出出现完全一致的错误”的状况才能够达成攻击“逃逸”。对于一个由多次内外交互操作组成的攻击行动,若要达成最终攻击任务的目的,必须保证涉及表决环节的所有操作都能实现非配合条件下的协同逃逸,且在整个过程中“不允许试错”,因为一旦某个环节出现不一致,通过对同一执行体进行时间维度上的重复计算,或者对不同执行体进行空间维度上的相同计算,就可以从多次或多路计算结果的对比中发现由于攻击导致的异常部位,从而锁定被攻击位置。因此我们用成功“逃逸”的概率作为系统安全性的度量,该概率越小,说明系统越安全。为了从理论上分析逃逸概率的大小,首先给出一些前提假设和相关概念符号。

3 前提假设与符号说明

为了突出异构冗余架构的容侵特性,考虑到网络攻击过程的复杂性,我们做了一些合理的假设。

1)攻击指基于执行体中的漏洞或后门对系统发起攻击,其他的攻击不在本文讨论的范围内。

2)攻击成功后必然导致输出矢量发生改变,即攻击成功后的执行体运算结果与正常执行体的运算结果相异。

3)系统的输入与输出是一一对应的,即输入和输出之间存在函数关系。

4)执行体之间是独立工作的,且表决器是安全的。

定义 1(攻击成功) 对单个执行体而言,当攻击者利用执行体中的漏洞成功控制该执行体时,认为执行体被攻击成功。对系统而言,若攻击者利用 n 个执行体中的漏洞发起攻击,导致某些执行体输出一致但与正常输出不一致,且这种异常输出通过了表决器表决,认为系统被攻击成功。

定义 2(集合的分拆) 称 $\{E_1,E_2,\cdots,E_k\}$ 为集合 E 的 k 分拆,若满足 $E_i\neq\emptyset,E_i\cap E_j=\emptyset(i\neq j),\bigcup_{i=1}^{k}E_k=E$。

集合 E 的 k 分拆集为 $PA(E,k)$,即为 E 的所有 k 分拆组成的集合,其元素个数记为 $S(n,k)$,n 为集合 E 中元素的个数。

集合 E 的分拆集为 $PA(E)=\bigcup_{k=1}^{n}PA(E,k)$,其元素个数记为 $S(n)=\sum_{k=0}^{n}S(n,k)$,规定 $S(0)=1$。

相关符号:p_i 为单位时间内执行体 A_i 被攻击成功的概率。从统计意义上讲,该概率表示在单位时间内,执行体 A_i 被攻击成功的次数和总攻击次数的比值。ε_{ij} 为执行体 A_i 和 $A_j(i,j=1,2,\cdots,n)$被攻击成功且运算结果一致的概率(简称协同输出一致)。$A=\{A_1,A_2,\cdots,A_n\}(n\geqslant 3)$表示执行体集合。

4　模型的建立

在利用马尔科夫过程建立数学模型前,首先要确定系统的状态和转移速率矩阵 Q,根据系统中被攻击成功的执行体集合和协同输出一致的执行体集合可以将系统划分为不同的状态。

1)状态$\langle V,Partion\rangle$

①$V\subseteq A$,$Partion\in PA(V)$,其中 V 表示执行体被攻击成功的集合,$Partion$ 表示执行体被攻击成功且协同输出一致的集合。

②状态总数为 $N=\sum_{i=0}^{n}C_n^iS(i)$,$n$ 为执行体的总个数。

③将 N 个状态编号为 0 到 $N-1$,状态 0 表示 0 个执行体被攻击成功,称之为初始状态。

建立所有 N 个状态到编号集$\{0,1,2,\cdots,N-1\}$的一一对应映射 g:

$$(V,Partion)\overset{g}{\mapsto}\{0,1,\cdots,N-1\}$$

由于系统状态的转移是由于系统中某些执行体被攻击成功而导致的,基于假设,各执行体被攻击成功是独立的。由状态的定义可知,系统将要处于的状态只与当前状态有关,而与系统如何到达当前状态即过去无关,因此系统满足马尔科夫特性。根据各个状态,可列出系统状态转移速率矩阵:

$$\begin{pmatrix} q_{0,0} & q_{0,1} & \cdots & q_{0,N-1} \\ q_{1,0} & q_{1,1} & \cdots & q_{1,N-1} \\ \vdots & \vdots & \vdots & \vdots \\ q_{N-1,0} & q_{N-1,1} & \cdots & q_{N-1,N-1} \end{pmatrix}$$

其中,q_{ij} 表示系统从状态 i 转移到状态 j 的速率,且

$$q_{ii}+\sum_{\substack{j=0\\ j\neq i}}^{N-1}q_{ij}=0,i,j=0,1,\cdots,N-1$$

根据矩阵 Q,可以得到系统在时刻 t 处于状态 i 的概率 $p_i(t)$。令 $P(t)=(p_0(t),p_1(t),\cdots,p_{N-1}(t))$,$\frac{dP(t)}{dt}=(\frac{dp_0(t)}{dt},\frac{dp_1(t)}{dt},\cdots,\frac{dp_{N-1}(t)}{dt})$,则有:$\frac{dP(t)}{dt}=P(t)Q$。

对微分方程组求解,可得到系统在时刻 t 处于状态 i 的概率 $p_i(t)(0\leqslant i\leqslant N-1)$,若$\lim_{t\to\infty}p_i(t)$存在,则称之为系统的平稳分布。该极限说明了系统的稳定状态分布,对于不同的状态,系统所处的威胁程度也不一样,这样只需对系统安全性受到威胁的状态加以分析。将系统稳定在这些威胁状态的概率之和作为系统安全性的度量。

2)系统被攻击成功的概率

择多输出是指当有不少于$\left[\frac{n}{2}\right]+1$个执行体的输出相同时,系统的输出为这些多数执行体的输出。对于系统某个状态$\langle V,Partion\rangle$,若$|Partion|\geqslant\left[\frac{n}{2}\right]+1$,则称状态$\langle V,Partion\rangle$为欺骗态,因为此时攻击者可以达成"逃逸",则系统最终稳定在欺骗态的概率就是系统被攻击成功的概率。记所有欺骗态组成的集合为 D,则系统被攻击成功的概率 $P_t=\sum_{i\in D}p_i(t)$。

5　模型的简化与求解

考虑到基本模型过于复杂,求解困难,且其在各执行体是独立工作的,可将攻击时的系统输出看作独立均匀分布的。在此情形下对模型进行简化:

1)假设单位时间内对各个执行体攻击成功的概率都相同,记为 p。

2)任意两个执行体协同输出一致的概率相同,记为 ε,则任意 3 个执行体协同输出一致的概率为 ε^2。

3)只考虑执行体从正常状态向攻击成功状态转移,即不考虑执行体的恢复率。

基于以上简化,对 $n=3$ 时的系统进行求解分析,此时可以将 3 个执行体的异构冗余系统分为以下 7 个状态。

0 状态:3 个输出一致(3 个正常一致)。

1 状态:3 个输出一致(3 个协同输出一致)。

2 状态:2 个输出一致(2 个正常一致,另一个攻击成功)。

3 状态:2 个输出一致(2 个协同输出一致,另一个正常)。

4 状态:2 个输出一致(2 个协同输出一致,另一个攻击成功)。

5 状态:3 个输出不一致(2 个攻击成功,另一个正常)。

6 状态:3 个输出不一致(3 个攻击成功)。

根据各状态的定义,可得出矩阵 Q 为:

$$\begin{pmatrix} q_{00} & p^3\varepsilon^2 & 3p(1-p)^2 & 3p^2(1-p)\varepsilon & p^3\varepsilon & 3p^2(1-p) & p^3 \\ 0 & q_{11} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & q_{22} & 2p(1-p)\varepsilon & p^2\varepsilon & 2p(1-p) & p^2 \\ 0 & p\varepsilon & 0 & q_{33} & p & 0 & 0 \\ 0 & 0 & 0 & 0 & q_{44} & 0 & 0 \\ 0 & 0 & 0 & 0 & p\varepsilon & q_{55} & p \\ 0 & 0 & 0 & 0 & 0 & 0 & q_{66} \end{pmatrix}$$

从而可列出微分方程组:

$$p_0'(t)=(-p^3\varepsilon^2-3p(1-p)^2-3p^2(1-p)\varepsilon-p^3\varepsilon-3p^2(1-p)-p^3)p_0(t)$$

$$p_1'(t)=p^3\varepsilon^2p_0(t)+p\varepsilon p_3(t)$$

$$p_2'(t)=(-2p(1-p)\varepsilon-p^2\varepsilon-2p(1-p)-p^2)p_2(t)+3p(1-p)^2p_0(t)$$

$$p_3'(t)=(-p\varepsilon-p)p_3(t)+3p^2(1-p)\varepsilon p_0(t)+2p(1-p)\varepsilon p_2(t)$$

$$p_4'(t)=p^3\varepsilon p_0(t)+p^2\varepsilon p_2(t)+pp_3(t)+p\varepsilon p_5(t)$$

$$p_5'(t)=(-p\varepsilon-p)p_5(t)+3p^2(1-p)p_0(t)+2p(1-p)p_2(t)$$

$$p_6'(t)=p^3p_0(t)+p^2p_2(t)+pp_5(t)$$

根据微分方程的解法和初始条件 $p_0(0)=1$，$p_i(0)=0$ $(i\neq 0)$可解得 $p_i(t)$。根据 7 个状态的定义可知，1，3，4 状态为欺骗态，其他状态对于系统来说不是威胁，因此只需求解 1，3，4 状态的稳定情况即可。利用 Mathematica 软件，求解和模拟得到：

$$p_1(t)\xrightarrow{t\to+\infty}\frac{-p\varepsilon^2(p\varepsilon-2p+3)}{(\varepsilon+1)(-p^2\varepsilon^2+2p^2\varepsilon-3p\varepsilon-p^2+3p-3)}$$

$$\approx p\varepsilon^2,\text{当 } p,\varepsilon \text{ 较小时}$$

$$p_3(t)\xrightarrow{t\to+\infty}0$$

$$p_4(t)\xrightarrow{t\to+\infty}\frac{\varepsilon(2+p(-2+p+3\varepsilon+p(1+p)\varepsilon^2))}{(1+\varepsilon)(1+\varepsilon+p\varepsilon)(1+p(-1+p+\varepsilon+p\varepsilon^2))}$$

$$\approx cp\varepsilon,c\in(0,1)$$

从而系统被攻击成功的概率为：

$$P_t=p_1(t)+p_3(t)+p_4(t)\approx p\varepsilon^2+cp\varepsilon,t\to\infty$$

根据通用安全脆弱点评估系统 CVSS(Common Vulnerability Scoring System)的推荐[12]，对于未定义漏洞，取 $p=0.71$，当 $\varepsilon=10^{-4}$ 时，$p_i(t)(i=0,1,\cdots,6)$的趋势如图 2－图 8 所示，其中横坐标为 t，纵坐标为 $p_i(t)$。

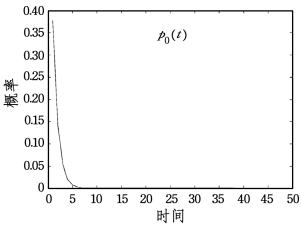

图 2 0 状态的概率趋势图

Fig. 2 Probability trend graph in state 0

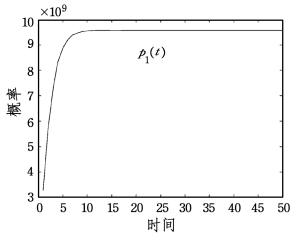

图 3 1 状态的概率趋势图

Fig. 3 Probability trend graph in state 1

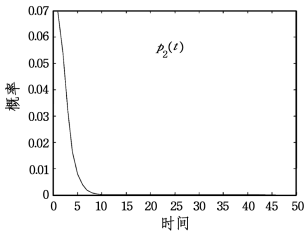

图 4 2 状态的概率趋势图

Fig. 4 Probability trend graph in state 2

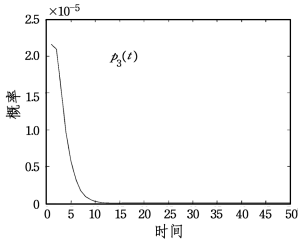

图 5 3 状态的概率趋势图

Fig. 5 Probability trend graph in state 3

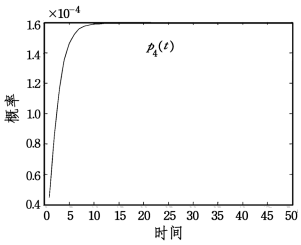

图 6 4 状态的概率趋势图

Fig. 6 Probability trend graph in state 4

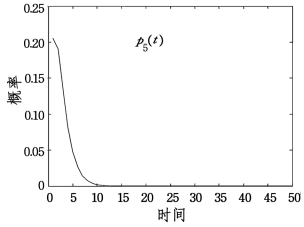

图 7 5 状态的概率趋势图

Fig. 7 Probability trend graph in state 5

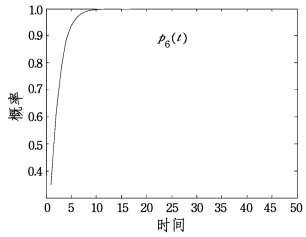

图 8 6 状态的概率趋势图

Fig. 8 Probability trend graph in state 6

观察图 2－图 8 可以发现，当 $t\to\infty$ 时，系统最终基本稳定在 1，4，6 状态，并且以很大概率稳定在 6 状态，而稳定在其他状态的概率为 0。这是因为随着时间的推移，最终各个执行体都会被攻击成功($t\to\infty$)，即为 6 状态；而在 0，2，3，5 状态中含有正常执行体，故稳定概率为 0。被攻击成功且逃逸的状态只有 1，4，由 1，4 状态的稳定分布表达式可知，$p_1(t)$，$p_4(t)$的大小与 ε 相关，这是因为 1，4 状态要求协同输出一致，ε 越小，则稳定在 1，4 状态的概率也越小，即系统被攻击成功的概率越小，系统越安全。而 6 状态对系统是没有威胁的，因为 3 个执行体输出都不一致，从而无法“逃逸”，这时异构冗余系统可采用其他策略进行表决，比如带权重表决、基于历史信息的大数表决等。

由系统攻击成功概率 P_t 的表达式可以看出，系统的安全性由单个执行体的安全性(p)和执行体之间的协同输出一致概率(ε)所决定。单个执行体越安全，攻击者利用该执行体也就越困难，从而系统也就越安全。当然，系统也可能发生“逃逸”情况，而“逃逸”是由于协同输出一致而引起的，即由 ε 所决定。对于 ε 来说，该参数实际上反映的是两异构执行体之间的异构性的强弱，很显然，异构性越强，则 ε 越小；异构性越弱，则 ε 越大，当异构性弱到同构时，$\varepsilon=1$。

结束语 异构冗余架构是解决系统可靠性的一种很好的方法，本文研究了其是否可以增强系统的安全性。根据异构冗余架构的特点，文中分析了该架构对系统的安全增益为“非配合条件下的多元目标协同一致的攻击难度”。基于此，利用连续时间马尔科夫链对系统进行建模，给出了该“难度”的定量描述——系统攻击成功概率 P_t，并分析了执行体的安全性和协同输出一致概率对 P_t 的影响。

表决机制迫使攻击者必须在非配合条件下破解对多个不同类型的目标实现协同一致攻击效果的难题，正如欧氏空间三角形的几何稳定性取决于其 3 个内角之和等于 180°，异构冗余架构的容侵效应也源自其基于表决的异构冗余构造和机制，即异构冗余系统的安全有效性来源于系统的架构特性(异构冗余)，不依赖于任何先验知识，因此该安全性是系统内生的。

文中对异构冗余架构抗网络攻击的有效性做了初步分析，但仍有其他问题值得探讨，如 ε 的显性表达式如何定义，系统的异构性如何度量，异构冗余架构抗增量式攻击的效果如何等，这些都是下一步需要解决的问题，以便更有效地指导工程实践。

(下转第 194 页)

[13] MALEK B, MIRI A. Combining attribute-based and access systems[C]// International Conference on Computational Science and Engineering. 2009:305-312.

[14] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// ACM Conference on Computer and Communications Security. 2006:89-98.

[15] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]// IEEE Symposium on Security and Privacy. 2007:321-334.

[16] DAN B, FRAKLIN M. Identity based encryption from the Weil pairing: Advances in Cryptology[J]. Lecture Notes in Computer Science, 2003, 32(3):213-229.

[17] XIA C, ZHOU J S. Research on cloud manufacturing resource-aware and access technology using RFID[J]. Journal of Harbin Institute of Technology, 2014, 21(3):101-110.

[18] LIU Z, CAO Z F. On efficiently transferring the linear secret-sharing scheme matrix in ciphertext-policy attribute-based encryption [J/OL]. http://www.iacr.org/cryptodb/data/paper.phb?pubkey=23275.

[19] BEIMEL A. Secure schemes for secret sharing and key distribution[D]. Israel: Technion-Israel Institute of Technology, Faculty of Computer Science, 1996.

[20] NARUES T, MOHRI M, SHIRAISHI Y. Provably secure attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating[J]. Human-centric Computing and Information Sciences, 2015, 5(1):1-13.

[21] ZHANG Y H, CHEN X F, LI J, et al. Anonymous attribute-based encryption supporting efficient decrypyion test[C]// Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. 2013:511-516.

[22] PHUONG T V X, YANG G, SUSILO W. Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions [J]. IEEE Transactions on Information Forensics & Security, 2015, 11(1):35-45.

[23] JIN C, FENG X, SHEN Q. Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size[C]// International Conference on Communication and Network Security. ACM, 2016:91-98.

(上接第 186 页)

参 考 文 献

[1] 吴世忠,郭涛,董国伟,等. 软件漏洞分析技术[M]. 北京:科学出版社,2014.

[2] WU J X. Meaning and Vision of Mimic Computing and Mimic Security Defense[J]. Telecommunications Science, 2014, 30(7):2-7. (in Chinese)
邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7):2-7.

[3] WU J X. Mimic Security Defense in Cyber Space[J]. Secrecy Science and Technology, 2014(10):4-9. (in Chinese)
邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014(10):4-9.

[4] WU J X. Research on Cyber Mimic Defense[J]. Journal of Cyber Security, 2016, 1(4):1-10. (in Chinese)
邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4):1-10.

[5] MARVIN R. System Reliability Theory: Models, Statistical Methods, and Applications (Second Edition)[M]. Beijing: National Defend Industry Press, 2011. (in Chinese)
MARVIN R. 系统可靠性理论:模型、统计方法及应用(第 2 版)[M]. 北京:国防工业出版社, 2011.

[6] SUN H Y, LIU B, CAO X L. Research on reliability and security of vote redundancy system[J]. Journal of Electronic Measurement and Instrument, 2011, 25(7):661-664. (in Chinese)
孙怀义, 刘斌, 曹晓莉. 表决冗余系统可靠性与安全性研究[J]. 电子测量与仪器学报, 2011, 25(7):661-664.

[7] LI C Y, CHEN X, YI X S, et al. Analysis of k—out-of-n:G systems subject to common cause failures based on Markov process [J]. Systems Engineering and Electronics, 2009, 31(11):2789-2792. (in Chinese)
李春洋, 陈循, 易晓山, 等. 基于马尔可夫过程的 k/n(G)系统共因失效分析[J]. 系统工程与电子技术, 2009, 31(11):2789-2792.

[8] LIU Y, LI R Z, ZHANG G B. Reliability analysis of k/n(G) Markov system with non-homogenous units[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2015, 43(3):17-21. (in Chinese)
刘英, 李荣祖, 张根保. 非同型单元 k/n(G)马尔可夫系统可靠性分析[J]. 华中科技大学学报(自然科学版), 2015, 43(3):17-21.

[9] YIN L H, FANG B X. Security Attributes Analysis for Intrusion Tolerant Systems[J]. Chinese Journal of Computers, 2006, 29(8):1505-1512. (in Chinese)
殷丽华, 方滨兴. 入侵容忍系统安全属性分析[J]. 计算机学报, 2006, 29(8):1505-1512.

[10] MADAN B B, GOSEVA-POPSTOJANOVA K, VAIDYANATHAN K, et al. A method for modeling and quantifying the security attributes of intrusion tolerant systems [J]. Performance Evaluation, 2004, 56(1-4):167-186.

[11] ZANG H W, HAN W, GAO D Y. Dissimilar redundancy computer system and reliability analysis[J]. Journal of Harbin Institute of Technology, 2008, 40(3):492-494. (in Chinese)
臧红伟, 韩炜, 高德远. 非相似余度计算机系统及其可靠性分析[J]. 哈尔滨工业大学学报, 2008, 40(3):492-494.

[12] YE Y, XU X S, JIA Y, et al. An Attack Graph-Based Probabilistic Computing Approach of Network Security[J]. Chinese Journal of Computers, 2010, 33(10):1987-1996. (in Chinese)
叶云, 徐锡山, 贾焰, 等. 基于攻击图的网络安全概率计算方法[J]. 计算机学报, 2010, 33(10):1987-1996.