基于自学习多维参数可信安全度量模型研究*

蔡庆玲[1]，詹宜巨[1]，杨 健[2]
（1. 中山大学工学院，广东 广州 510275；
2. 广东工业大学自动化学院，广东 广州 510006）

摘 要：针对可信度量现存问题，依据软件安全保护原则提出通过融合多方度量因子建立综合的可信度量模型——随机抽取划分序列策略模型。该模型兼顾了软件安全度需求系数、软件安全度评估系数及软件执行所需资源开销系数等多方因素，摒弃了传统单一的度量方法，建立了综合性的可信度量策略及构造方法，兼顾了多方面安全需求问题，并且实现了细粒度完整性检验，降低了可信度量的运算开销。

关键词：可信计算；可信度量；完整性检验
中图分类号：TN915.04 **文献标志码**：A **文章编号**：0529－6579（2014）04－0021－04

Trusted Measurement Model of Multidimension Parameter Based on Self-learning

CAI Qingling[1], *ZHAN Yiju*[1], *YANG Jian*[2]
（1. School of Engineering, Sun Yat-sen University, Guangzhou 510275, China;
2. Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China）

Abstract: To solve trusted measurement, a trusted measurement model of multidimension parameter (called Random Division Sequence Model, D^R) is given through the integration of multi-factor based on the software security protection principles. D^R takes into account software security level factor, software security assessment factor and the required resources of software operation factor, which abandons the traditional single measurement methods and establishes a comprehensive trusted measurement model by giving consideration to various security requirements. D^R achieves a fine-grained integrity measurement, and reduces operation costs.

Key words: trusted computing; trusted measurement; integrity measurement

可信计算是目前信息安全领域的研究热点[1－2]。可信度量是可信计算的关键技术之一[3－4]。而目前可信度量的方法主要采用单一的软件完整性检验。其存在缺陷主要有[2,4－6]：软件完整性检验的计算量过大问题；难以有效解决动态环境下完整性检验的实时更新问题；难以实施动态环境下完整性检验计算端与验证端的同步问题；对资源受限的设备如移动终端细粒度完整性检验实现的策略问题。

为此，本文依据软件安全保护原则提出一种综合的可信度量的建模方案——随机抽取划分序列策略模型（Random Division Sequence Model, D^R）[7]。

1 可信度量模型相关问题研究

1.1 可信度量模型问题分析

可信计算环境的建立依靠着可信根、可信链的建立和传递，可信链的建立和传递又离不开可信计算的关键技术——可信度量。目前可信度量的方法

* **收稿日期**：2013－11－08
基金项目：国家自然科学基金资助项目（61071038，61102034，61172156）；广东省教育部产学研结合资助项目（2011A090200128）；广东省自然科学基金资助项目（9151027501000076）
作者简介：蔡庆玲（1966 年生），女；**研究方向**：网络与信息安全；E-mail：caiqingl@mail.sysu.edu.cn

主要采用单一的软件完整性检验，即将整个软件进行哈希摘要形成参考完整性值作为该软件完整性检测的安全依据。

可信计算环境又可分为静态可信计算环境和动态可信计算环境。其中静态可信计算环境中，采用单一的软件完整性检验还可以勉强胜任，但在动态可信计算环境下，随着用户开启的应用程序不同，系统完整性是动态变化的。因而，必须实时地更新系统的完整性信息，如操作系统内核、用户动态进程，还要兼顾着各进程的运行参数、堆栈区及数据区域的完整性检验。实时的、全面彻底的动态完整性计算，虽然提高了计算平台安全可信的可能性，但必然会导致系统整体性能的下降，这对资源有限的设备问题就尤为突出。另一方面更因为动态环境下安全性已不仅仅依赖于执行单一软件的完整性检验，其情况极为复杂多变，如计算平台常驻内存代码（如操作系统中的系统调用、服务器进程等）仅在加载文件时进行完整性度量，必然会造成完整性度量的盲区，遗留安全隐患。此外还有程序的运行参数、堆栈区及数据区域的不断地更新等都无法作到完整性检验的实时、全面彻底不留有漏洞。

由此可见，一方面，软件完整性检验的计算量大，尤其是动态环境下完整性的复杂多变，其目标完整性值需要实时更新，对资源受限的计算设备难以胜任。另一方面，传统单一软件完整性检测方案，难以解决动态环境中完整性检验计算端与验证端的同步实施问题。需要一种兼顾多方面安全需求低耗高效的、综合性的可信度量策略及构造方法，才能解决动态环境中完整性检验有效实施的多项难题。

1.2 软件安全原则及保护机制

目前，信息安全领域被广泛认可的原则主要有[7]：等级保护原则、适度安全原则、动态安全原则及全过程安全原则。

等级保护原则：对信息系统的安全特性进行等级划分，应按标准进行建设、管理和监督。

适度安全原则：信息系统安全措施的强度与该系统承担的业务职能和系统的重要性紧密相关。采用适度安全原则，有效的控制浪费和不足。

动态安全原则：网络环境的动态变化，攻击手段的更新，安全解决方案也需随之变化。安全框架应随威胁和网络环境的变化而不断调整。

全过程安全原则：当安全防护在任何一个环节出现漏洞，风险都将会在此点发生，并渗透到其它环节。故应采用全过程安全原则对风险实施安全监控。

2 多维参数可信度量模型设计

系统软件与应用软件的可信度量对构建安全体系至关重要。本文依据软件安全保护原则提出一种综合的可信度量的建模方案——随机抽取划分序列策略模型 D^R（R, K_r, K_e, K_c, L_D）。该方案将软件安全度需求系数 K_r 以及软件安全运行的动态调整参数——软件安全度评估系数 K_e 引入模型 D^R，同时兼顾为执行该软件所需资源开销系数 K_c 的适度安全原则。该方案首先对软件 P 的代码进行划分，生成等长的基本划分序列 L_R（见图 1）。然后按照模型 D^R，计算出相应的抽取序列，抽取相应部分的划分，再进行摘要，其运算量可降低为 $O(\frac{8}{27}\cdot N)$，同时解决了抽取端与验证端同步的难题。

设计思想：

计算端将软件按照摘要划分单元长度 l（本文哈希函数使用 MD5，l 选为 512bits）进行划分，对每一个划分进行哈希摘要，计算端和验证端共同保存作为验证 RIM_i 值序列（见图 2）。可信度计算验证时，验证端按照模型 D^R 抽取相应的若干划分进行摘要计算和验证。

图 1 随机数 R 为 1 的位表示将被抽取的划分序列

Fig. 1 1 bit of random number R indicates that the sequence will be extracted

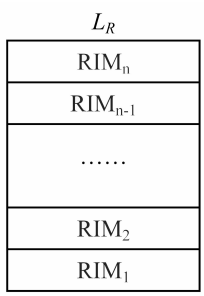

图 2 软件 P 的基本划分序列 LR

Fig. 2 The basic division sequence LR for the software P

软件 P 模型：

软件 P 模型表示为：元组 P（L, K_r, K_e, K_c, L_R），其中 L_R =（RIM_1, RIM_2, …, RIM_n）

L：为待检测的软件长度；

K_r：为该软件安全度需求系数；

K_e：为该软件安全度评估系数；

K_c：为执行该软件所需资源开销系数；

RIM_i：为划分 i 的完整性验证参考值。其中 RIM_n 长度 < l 时，在 RIM_n 的尾部补 0。

随机抽取划分序列策略模型：

随机抽取划分序列策略模型表示为：元组 D^R（R, K_r, K_e, K_c, L_D），

其中 L_D = （L_1, …, L_i, …, L_{n-1}, L_n）

R：高熵随机数，用于确定摘要所抽取的划分（见图 1）；

l：摘要划分基本单元长度；

N：为该软件所具有的划分数，$N = [\frac{L}{l}] + 1$；

K_r：软件安全度需求系数，软件安全要求越高则 K_r 越大，$0 \leqslant K_r \leqslant N$。

$K_r = N$ 时，表明该软件每一个划分都必须进行完整性检验；

$K_r = 0$ 时，表明该软件都不需要进行完整性检验。

K_e：软件安全度评估系数，依据该软件执行的评估结果动态调整，$0 \leqslant K_e \leqslant N$。

$K_e = N$ 时，表明该软件每一个划分都具有可信安全性；

$K_e = 0$ 时，表明该软件每一个划分都不具有可信安全性。

K_c：执行该软件所需资源开销系数，软件执行时间及所需资源越多则 K_c 越大，取值为：$0 < K_c \leqslant 10$。

$K_c = 10$ 时，表明该软件执行时间及所需资源等级为最高；

$K_e = 0$ 时，表明该软件执行时间及所需资源等级为最低。

抽取的划分序列 L_D 表示为：（L_1, …, L_i, …, L_{n-1}, L_n）

$L_i = 1$ 时，则表明序列号为 i 的划分块被抽取，参与完整性检验；

$L_i = 0$ 时，则表明序列号为 i 的划分块未被抽取，不参与完整性检验。

$|L_D|$：为序列中元素为非 0 的个数；

随机抽取划分序列执行过程：

模型 D^R（R, K_r, K_e, K_c, L_D）用于生成抽取划分序列 L_D，其中 R 为一高熵随机数，其格式见图 1。用于随机地确定初时抽取的划分块。K_r, K_e, K_c 共同对 R 值的进行修正。因此 L_D 是由 R, K_r, K_e, K_c 四个参数共同决定，最终确定的完整性检验所抽取的划分。具体执行算法如下：

1）随机选取高熵随机数 R，R 为 1 的位表示将被抽取的划分序列号。

2）K_r 为该软件安全度需求系数。在系统运行中，K_r 值保持不变。K_r 越大表示该软件安全要求越高。初始时由系统根据软件的安全度需求进行赋值，其取值为 $0 \leqslant K_r \leqslant N$，如操作系统等为最高安全度需求 $K_r = N$。K_r 用以调整 R 取值，表示为：$\sum K_r \cdot R$。依据等级保护原则，K_r 取值越大，则 R 取 1 的位越多，表明抽取划分的越多；K_r 取值越小，则 R 取 1 的位越少，表明抽取划分的越少。

3）K_e 为软件安全度评估系数。在系统运行中，随软件执行后安全信誉的变化进行动态调整。K_e 值越大表示该软件执行后的安全信誉越高，其取值为 $0 \leqslant K_e \leqslant N$。$K_e$ 用以调整 R 取值，表示为：$\Gamma \frac{1}{K_e} \hat{} R$。依据动态安全原则，$K_e$ 增大，则 R 取 1 的位减少，表明抽取划分的越少；K_e 减小，则 R 取 1 的位增加，表明抽取划分的越多。当程序执行结果为安全，则 K_e 增加，最高为 N；当程序执行结果为为非安全，则 K_e 减少，最低为 0。

4）K_c 为执行该软件所需资源开销系数。在系统运行中，K_c 值保持不变。K_c 越大表示为执行该软件所需资源开销越高。初始时由系统进行赋值，其取值为 $0 \leqslant K_c \leqslant 10$。$K_c$ 用以调整 R 取值，表示为：$\Delta \frac{1}{K_c} \check{} R$。依据适度安全原则，$K_c$ 取值越大，则 R 取 1 的位越少，表明抽取划分的越少；K_c 取值越小，则 R 取 1 的位越大，表明抽取划分的越多。

因此模型 D^R 参数之间的关系可表达为

$$\prod [\frac{1}{K_e} \hat{} \frac{1}{K_c} \check{} K_r] \cdot R$$

定义：$\prod [\frac{1}{K_e} \hat{} \frac{1}{K_c} \check{} K_r]$

5）当 $|L_D| > |L_R|$，需要抽取的更多划分，执行如下程序：

（a）如果 $|L_D| > |R|$，再生成随机数 R'；

（b）计算：$R = R$ or R'；

（c）计算：$\prod [\frac{1}{K_e} \hat{} \frac{1}{K_c} \check{} K_r] \cdot R$，得到序列 L_D = （L_1, …, L_i, …, L_{n-1}, L_n）；

（d）判断是否满足：$|L_D| \leqslant |R|$；

（e）如果不满足，则重复操作（a）－（d）；

（f）如果满足，则按照 L_D 序列抽取相应的划分。

随机抽取划分序列策略模型性能分析：

假设 $K_r = N$ 时，抽取序列数为：$\frac{2}{3} \sim 1$；

$K_r = \left[\frac{N}{2}\right]$ 时，抽取序列数为：$\frac{1}{3} \sim \frac{2}{3}$；

$K_r = 0$ 时，抽取序列数为：$0 \sim \frac{1}{3}$。

假设 $K_e = \mathrm{N}$ 时，抽取序列数为：$0 \sim \frac{1}{3}$；

$K_e = \left[\frac{N}{2}\right]$ 时，抽取序列数为：$\frac{1}{3} \sim \frac{2}{3}$；

$K_e = 0$ 时，抽取序列数为：$\frac{2}{3} \sim 1$。

假设 $K_c = 10$ 时，抽取序列数为：$0 \sim \frac{1}{3}$；

$K_c = 5$ 时，抽取序列数为：$\frac{1}{3} \sim \frac{2}{3}$；

$K_c = 0$ 时，抽取序列数为：$\frac{2}{3} \sim 1$。

因此，综合抽取序列概率为：$O(\frac{8}{27} \cdot N)$。

系统运行后，其中 K_r，K_e，K_c 参数通过自学习、自适应不断调整最终得到优化，并趋于稳定。

3 结 论

本文提出的随机抽取划分序列策略模型 D^R 融合了多方位参数，摒弃传统单一度量方案，建立了综合性的可信度量策略及构造方法，兼顾了多方面安全需求问题，实现了细粒度完整性检验，为可信度量的建模提出了新的思路。

参考文献：

[1] 2012 年度国家有关“可信软件基础研究”重大研究计划科技项目指南[R]. http://www.ecas.cn/xxkw/kbcd/201115_85123/ml/xxhjsyjcss/201202/t20120216_3441065.html.

[2] 刘昌平. 可信计算环境安全技术研究[D]. 成都:电子科技大学, 2011.

[3] 蔡红云, 田俊峰, 李珍. 何莉辉基于信任领域和评价可信度量的信任模型研究[J]. 计算机研究与发展, 2011, 48(11): 2131 – 2138.

[4] 王丹, 卢彦, 赵文兵,等. 基于变量间依赖关系的软件可信度量模型[J]. 华中科技大学学报：自然科学版, 2013, 41(1): 41 – 45.

[5] 杨蓓, 吴振强, 符湘萍. 基于可信计算的动态完整性度量模型[J]. 计算机工程, 2012, 38(2): 78 – 81

[6] 刘孜文, 冯登国. 基于可信计算的动态完整性度量架构[J]. 电子与信息学报, 2010, 32(4): 875 – 879.

[7] 计算机信息系统安全保护等级划分准则 GB17859 – 1999[S]. http://www.docin.com/p – 396913971.html.

（上接第 20 页）

[10] WATTS D J, STROGATZ S H. Collective dynamics of ‘small world’ networks [J]. Nature, 1998, 393 (6684): 440 – 442.

[11] BARABáSI A L, ALBERT R, HAWOONG J. Mean-field theory for scale-free random networks [J]. Physica A, 1999, 272(1): 173 – 187.

[12] YANG J M, LU L P, WANG D X, et al. On competitive relationship networks: a new method for industrial competition analysis [J]. Physica A, 2007, 382(2): 704 – 714.

[13] 万阳松,陈忠. 上海 A 股市场股价波动相互影响能力实证研究[J]. 上海管理科学, 2006, 4: 29 – 30.

[14] LIU X R, SUN H Y. The leading nodes analysis of the consumer price volatility based on complex network[C]//2012 IEEE fifth International conference on Advanced Computational Intelligence, nanjing, jiangsu China, 2012: 28 – 31.

[15] 孙红英,刘向荣. 消费品价格波动的关联效应分析—基于价格波动网络主导节点的实证研究[J]. 价格理论与实践, 2012, 2:41 – 48.

[16] 刘向荣,杨建梅,孙红英,等. 基于符号动力学的中国工业产品价格传导复杂网络分析[J]. 工业工程, 2013,16(4): 49 – 55.

[17] 广东省统计局. 2007 年广东省 135 部门价值型投入产出表[EB/OL]. (2010 – 03 – 08) [2013 – 10 – 15] http://www.gdstats.gov.cn/tjzl/tjfx/201003/t20100308_77821.html.