基于拟态防御的管理信息系统

常啸林[1,2] 樊永文[1] 朱维军[1] 刘 洋[1]
(郑州大学信息工程学院 郑州 450001)[1]
(河南大学软件学院 河南 开封 475000)[2]

摘 要 管理信息系统(Management Information Systems,MIS)的安全性关系着众多企业和组织的正常运作。针对现有信息管理系统安全防护方法的不足,文中提出了一种基于拟态防御的管理信息系统(Mimic Management Information Systems,MMIS)。首先,为表示层、业务逻辑层、数据服务层构建冗余执行体集;然后,利用动态配置器对执行体集进行动态调度;最后,利用表决器对执行体集进行表决处理。仿真实验结果表明,与传统 MIS 相比,MMIS 具有更高的安全性。

关键词 管理信息系统,拟态防御,多样性,动态配置,拟态管理信息系统
中图法分类号 TP315,TP393 **文献标识码** A

Management Information System Based on Mimic Defense

CHANG Xiao-lin[1,2] FAN Yong-wen[1] ZHU Wei-jun[1] LIU Yang[1]
(School of Information Engineering,Zhengzhou University,Zhengzhou 450001,China)[1]
(School of software,Henan University,Kaifeng,Henan 475000,China)[2]

Abstract Safety management information system(MIS) affects the normal operations of many enterprises and organizations. In view of the shortcomings of existing security protection methods for information management systems,this paper proposed a management information system based on Mimic Defense(Mimic Management Information Systems,MMIS). Firstly,redundant execution set is constructed for presentation layer,business logic layer and data service layer. Secondly,execution set is dynamically scheduled by dynamic configurator. Finally,execution set is voted by voter. The simulation results show that MMIS has higher security than traditional MIS.

Keywords Management information system,Mimic defense,Diversity,Dynamic configuration,Mimic management information systems

1 引言

管理信息系统[1]凭借其特定的功能成为企业[2]、医院、政府等机构所使用的重要工具。但是,近年来信息安全问题层出不穷。例如英特尔“芯片门”丑闻,其芯片存在严重的技术缺陷,导致重大安全漏洞,黑客可利用此漏洞窃取设备的全部内存内容,威胁几乎所有电脑和移动设备用户的个人信息安全。而作为运行在该设备上的管理信息系统也不可避免地遭受着这些安全威胁。因此,MIS 系统的安全性问题显得尤为重要。

目前,MIS 系统多采用入侵检测[3-4]、数据加密[5]、防火墙[6]等安全防御技术,其在防御已知攻击时取得了良好的防御效果,但在面对不断涌现出的未知的攻击手段或漏洞时具有被动性和滞后性等缺点。邬江兴院士提出的拟态防御技术[7-8]正是一种可有效应对未知后门与漏洞、有效解决网络防御被动性和滞后性问题的新兴途径。在 2018 年举办的一次国际网络攻防邀请赛上,来自多个国家的 22 个黑客战队对拟态防御设备进行了多达 50 万次攻击,结果无一成功[9],这初步证实了拟态防御的威力。是否可利用拟态防御思想提升管理信息系统的安全性,降低系统被攻击的风险,是本文研究的问题。

2 基础知识

2.1 MIS 系统

管理信息系统是利用计算机硬件、软件、网络通信设备以及其他办公设备,进行信息的收集、传输、加工、储存、更新、拓展和维护的系统[1]。如图 1 所示,管理信息系统的实现过程是数据的处理、收集、分析和表达的过程。

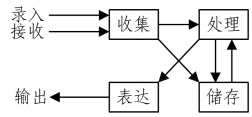


图 1 管理信息系统的处理过程

基于 B/S 模型的 MIS 系统是互联网时代的主流模式。因此本文主要以三层架构来搭建 MIS 系统。如图 2 所示,MIS 系统的安全构架可以按照表示层、商务逻辑层、数据服务层 3 个方面进行构建。

本文受国家自然科学基金项目(U1204608),国家重点研发计划项目(2016YFB0800100)资助。
常啸林(1998—),男,主要研究方向为网络安全;朱维军(1976—),男,博士后,副教授,CCF 高级会员,主要研究方向为信息安全,E-mail:zhuweijun76@163.com(通信作者)。

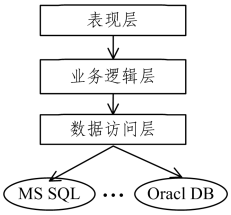


图 2　MIS 架构图[10]

2.2　拟态防御

主动防御技术是现在网络安全领域的研究热点[11]。相比被动防御技术，主动防御技术在面对攻击，尤其是未知的漏洞和后门时，表现出了具有更高的有效性和安全性的特点。目前入侵容忍[12]、移动目标防御[13]、拟态防御[7]是典型的 3 种主动防御技术。拟态防御(Mimic Defense，MD)较之于入侵容忍有性价比的优势，比移动目标防御更具安全性和可靠性[8]。拟态防御作为将二者融合的新型主动防御技术，以其优越的安全性和较高的性价比应用于多个领域，例如 Web 服务器[14]、DNS 框架设计[15-16]、工控领域[17]等。

动态异构冗余(Dynamic Heterogeneous Redundancy，DHR)结构[18]是拟态防御的核心架构，如图 3 所示。DHR 结构的原理描述如下[14]：首先根据动态选择算法从 m 个异构构件集合中选择出 $n(n\leqslant m)$个执行体构成执行体集，然后输入代理复制分发指令给各个执行体进行执行，最后表决器对每个执行体所执行的结果进行表决，将表决出的具有唯一性的近似正确结果输出。

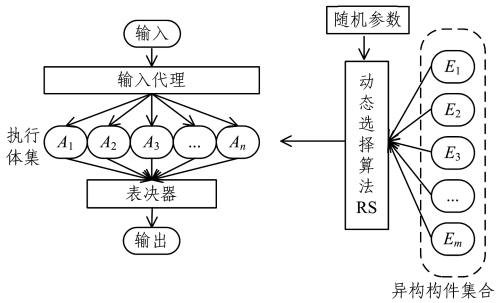


图 3　DHR 结构图[14]

3　基于拟态防御的管理信息系统

基于拟态防御的管理信息系统将拟态防御 DHR 架构中的动态、冗余等特性应用于 MIS 系统。

3.1　MMIS 系统的安全架构

如图 4 所示，MMIS 系统可由输入代理、异构构件集合、动态配置器、表决器和输出代理组成。

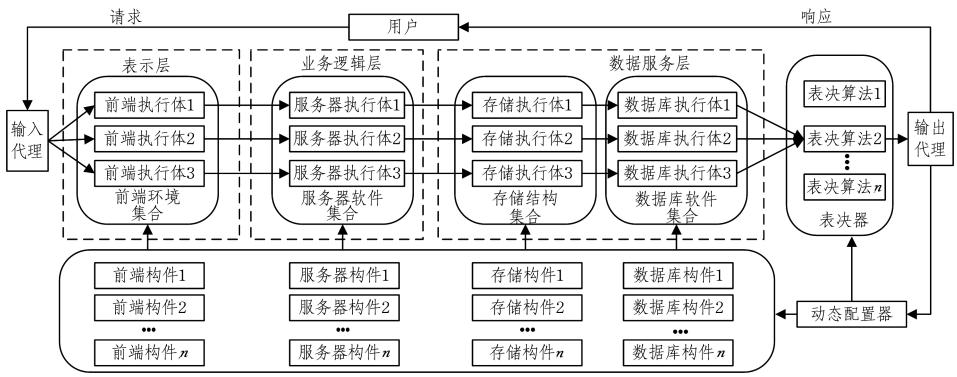


图 4　MMIS 架构图

(1)输入代理：与 HDR 结构中的输入代理相同，负责复制分发指令给表示层的执行体。

(2)异构构件集合：由动态配置器调度，从异构构件集合中随机挑选执行体，并分发给表现层、业务逻辑层、数据服务层中的执行体集合。如表 1 所列，经过动态配置器的调度，从执行体集合中随机地选出 3 个执行体组成存储结构集合。这些执行体集合接受输入代理或上层执行体集合派发的任务，执行后再交给对应的下层执行体集合或表决器。不同层的执行体采取一一对应的任务派发原则，避免了多次归一化的处理，可以有效地提高执行效率，缩短处理时间。

表 1　异构执行体资源池表

表现层	业务逻辑层			数据服务层	
前端框架	开发语言	后端框架	服务器软件	存储结构	数据库软件
Angular	PHP	Hibernate	Apache	顺序存储	MySQL
React	Python	Spring	Nginx	链式存储	SQL Server
Vue	ASP. NET	iBatis	IIS	索引存储	Oracle
...	...	...	...	...	...

(3)动态配置器：其动态性表现为定时触发和异常执行体处理两点[7]。定时触发是动态配置器根据其内置定时器所作出的、对执行体和表决器算法的调度操作。而异常执行体处理则是动态配置器根据输出代理所反馈的信息，做出隔离异常执行体的操作。

(4)表决器：相比拟态防御技术中的传统表决器，MMIS 系统使用 K/N(G)模型[19]构建表决器。如表 2 所列，根据 K 取值的不同，构建不同的表决方式加载到表决器中。图 5 给出了表决器的工作原理：首先切换器收到动态配置器的切换命令，切换表决方式，当切换器在接收到执行体的执行结果后，把结果交给当前切换到的表决方式进行表决，最后表决器经过采用当前表决方式的表决，将得到的唯一的、近似正确的结果和表决信息输出给输出代理。

表 2　$K/N(G)$表决方式表

$K/N(G)$	表决方式
$K=N$	全体一致性表决
$K=3N/4$	四分表决
$K=N/2$	大数表决
...	...

(5)输出代理：其功能有两个，分别为信息处理和结果标准化处理。信息处理可分为以下两种情况：1)若结果一致，则将结果输出；2)若结果不一致，则将异常的执行体标记，并反馈标记结果给动态配置器。结果标准化处理是指将表决结果做归一化处理，使其可以在异构的用户界面做出响应。

MMIS 系统的具体工作流程如图 6 所示。

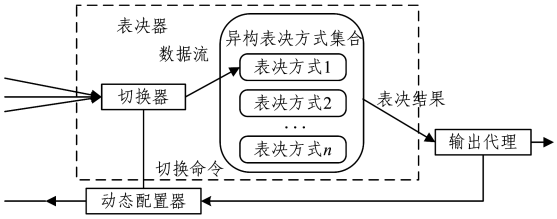


图 5 表决器工作原理图

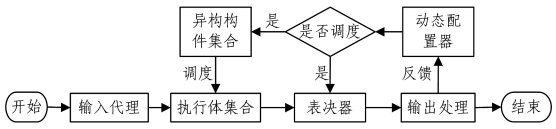


图 6 核心流程图

3.2 安全性分析

由于设计思想来自于拟态防御，因此 MMIS 系统继承了拟态防御的动态性、异构冗余性、多样性和随机性等特征，其以多样性、动态性为基础来提升系统的安全性。以这两点为基础的拟态防御技术，可放大入侵容忍和移动目标防御的优点，可减弱二者缺点造成的影响。在提升安全性的同时，降低其造成的时间成本和经济成本，是 MMIS 系统使用拟态防御技术的主要优势。

4 仿真实验

为了测试 MMIS 系统的安全性能和时间性能，本节将进行仿真验证。

4.1 实验平台

本文的实验环境如下：CPU 为 Intel(R) Core(TM) i7-4790 CPU @3.40 GHz；内存为 8.0 GB RAM；操作系统为 windows 7；采用 MATLAB R2014a 和 SQL Server 2008。

4.2 安全性仿真实验

根据 DHR 结构的性能评估[18]，本文同样假设攻击者的攻击能力随着时间的增加而增强。不采取拟态防御思想的传统静态 MIS 模型攻击的成功概率随时间的变化关系可表示为[18]：

$$P(t)=\int_t \lambda e^{-\lambda t} \tag{1}$$

其中，λ 代表攻击者的攻击能力，范围为(0,1)，在本次仿真实验中取 0.5。

MMIS 系统在周期时间内，在 t 时刻系统被攻击成功的概率为：

$$P(t)=R_{k/n(G)}\frac{m}{M}\sum_k^m C_m^k P_i^k (1-p_i)^{m-k} \tag{2}$$

其中，$\frac{m}{M}$ 表示从 M 个异构构件集合中选取 m 个执行体的概率($m \leqslant M$)。$R_{k/n(G)}$ 表示表决器判断出的 n 个执行体中至少有 k 个执行结果一样时，可以认为这个执行结果就是近似正确的结果的可靠度[20]。在本文仿真实验中，n 值相同时，k 不同的取值代表不同的表决方式。

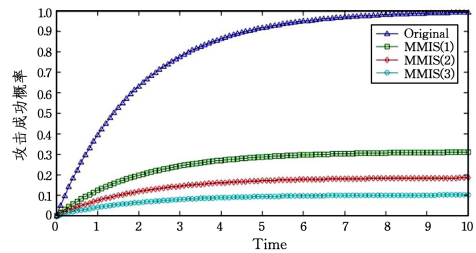
从文献[20]中可提取出如表 3 所列的数据，并按此数据进行安全性实验验证。

表 3 $k/n(G)$可靠性数据表

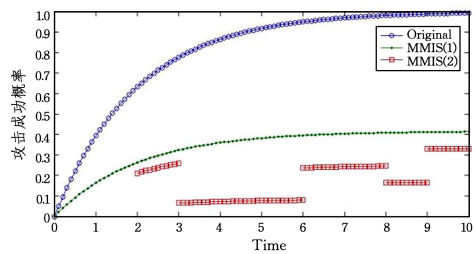
k/n	…	7/12	8/12	9/12	…
$R_{k/n(G)}$	…	0.416	0.247	0.135	…

如图 7(a)所示，假设 $\frac{m}{M}$ 固定，首先可以从实验仿真结果的曲线图中明显看出：具有拟态防御技术的 MIS 系统在面对相同攻击时，在同一时刻上攻击成功的概率明显低于传统 MIS 系统，可以认为 MMIS 系统由于采取了拟态防御技术，其安全性高于传统 MIS 系统。其次，MMIS(1)，MMIS(2)，MMIS(3)分别表示采用 7/12(G)表决方式、8/12(G)表决方式、9/12(G)表决方式时的攻击成功概率。由曲线图可以看出，表决方式对 MMIS 系统安全性的影响。可见采用 $k/n(G)$ 表决方式的 MMIS 系统的安全性高于传统 MIS 系统。

下面将讨论假设表决方式固定时，动态配置器对于系统安全性的作用。如图 7(b)所示，MMIS-1 表示采用 7/12(G)表决方式但没有采用动态配置器的攻击成功概率，MMIS-2 则表示采用 7/12(G)表决方式同时采用动态配置器的攻击成功概率。由图可知，采用动态配置器的 MMIS-2 系统的安全性高于 MMIS-1 系统，攻击 MIS 系统的成功率高于攻击 MMIS 系统的成功率。综上，动态配置器和表决器等拟态特征可以提升系统的安全性。



(a)不同表决方式安全性对比图

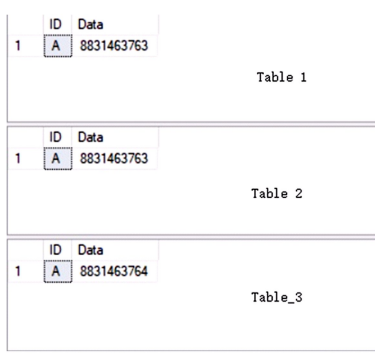


(b)MIS 安全性对比图

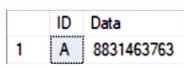
图 7 攻击成功概率图

4.3 可行性仿真实验

为简单起见，本节将使用 SQL Server 2008 验证 MMIS 系统的有效性。



(a)数据处理结果图



(b)表决结果图

图 8 执行结果图

本实验使用 3 种异构数据表：Table_1，Table_2，Table_3。其中 Table_3 的 Data 数据被入侵者篡改。如图 8(a)所示，Table_3 中的 Data 与 Table_1 和 Table_2 不一致。如图 8(b)所示，表决器使用 $K=N/2$ 表决方式，将多数结果作为最终结果输出，并将异常执行体隔离。这也说明了 MMIS 系统具有入侵容忍和威胁识别的能力，证明了 MMIS 系统的有效性。

4.4　时间性能仿真实验

为了测试 MMIS 系统的时间性能，利用 MATLAB R2014a 和 SQL Server 2008 做如下实验仿真实验。

假设现有 3 个执行体得出执行结果：Str1，Str2，str3。表决器为了得出近似正确的结果，调用表决函数，分别对 Str1，str2，str3 进行比较，函数处理时间即为表决时间。

针对系统执行一条命令，本文的实验结果如表 4 所列。由表 4 可知，MMIS 执行一条命令花费的时间短于 MIS 执行一条命令花费的时间。原因在于：后者系统只需执行该命令(简单起见，等同于执行 SQL 语句)，而前者系统既需执行该命令又需表决。因此，MMIS 系统需要更高的时间成本。

表 4　时间表

(单位：s)

系统名称	执行 SQL 语句时间	表决时间	总时间
MIS	0.006	—	0.006
MMIS	0.006	0.001	0.007

4.5　讨论

为了减少 MMIS 系统的时间成本、实现复杂性和经济成本，在具体实现过程中，不必采用所有层面的异构，采取单个或多个层面的异构即可。例如，某在线执行体集可在表现层采用相同架构，在业务逻辑层只对后端框架采取异构组合，在数据服务层只采取不同的异构存储方式即可。这种部分层次异构的 MMIS 系统减少了系统的复杂性、一定的经济成本和时间开销。当然，也可对 MMIS 系统的调度策略和表决方式进行优化，进一步降低了其运行时间成本。

结束语　针对 MIS 系统在设计上存在的根本性安全隐患，本文提出了一种基于拟态防御的管理信息系统。仿真实验证实了该系统可显著提升安全性，这是本研究的主要贡献。从已有的文献来看，这是第一个采用拟态防御思想的管理信息系统架构。

然而，新架构的不足之处在于：时间成本略高于传统 MIS 系统，而且由于部署相当数量的异构执行体，可以预见构建 MMIS 系统将带来经济成本的增大。可见，系统安全性与时间/经济成本是一对“鱼与熊掌式的矛盾”。为了提升系统安全性，付出如表 4 所列的微小时间成本代价以及适当的经济成本代价，对于国防、金融、电子政务等关键行业用户来说，其预期收益远远高于成本。

参 考 文 献

[1] 薛华成. 管理信息系统(第六版)[M]. 北京：清华大学出版社，2012.

[2] 张梦. 基于 C/S 结构的中小企业人事管理系统的设计与开发[J]. 计算机科学，2016，43(S1)：547-550.

[3] AROMS E. NIST Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)[M]. USA，CreateSpace，2012.

[4] ZHUANG R，QIAN D F，ZHANG W J. A Survey of Intrusion Detection Technology Research[J]. Journal of Chinese Computer Systems，2003，24(7)：1113-1118.

[5] WANG J，KISSEL Z A. Data Encryption Algorithms[M]. John Wiley & Sons Singapore Pte. Ltd，2009.

[6] CLINCY V，SHAHRIAR H. 2018 IEEE 42nd Annual Computer Software and Applications Conference(COMPSAC)- Web Application Firewall：Network Security Models and Configuration[C]// IEEE Computer Software & Applications Conference. IEEE，2018：835-836.

[7] 邬江兴. 网络空间拟态防御导论[M]. 北京，科学出版社，2017.

[8] 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.

[9] 多国顶尖“白帽黑客”对拟态防御网络设备和系统发起 50 余万次攻击测试无一次得手[EB/OL]. 新华网. http://m.xinhuanet.com/2018-05/12/c_129870684.htm，2018.

[10] 熊斌. 基于 B/S 三层架构 OA 系统的设计和实现[D]. 电子科技大学，2011.

[11] 仝青，张铮，邬江兴. 基于软硬件多样性的主动防御技术[J]. 信息安全学报，2017，2(1)：1-12.

[12] GARCIA M，BESSANI A N，GASHI I，et al. OS diversity for intrusion tolerance：Myth or reality[C]// IEEE/IFIP International Conference on Dependable Systems & networks. IEEE Computer Society，2011.

[13] 周余阳，程光，郭春生，等. 移动目标防御的攻击面动态转移技术研究综述[J]. 软件学报，2018，29(9)：2799-2820.

[14] 仝青，张铮，张为华，等. 拟态防御 Web 服务器设计与实现[J]. 软件学报，2017，28(4)：883-897.

[15] 王禛鹏，扈红超，程国振. 一种基于拟态安全防御的 DNS 框架设计[J]. 电子学报，2017(11)：2705-2714.

[16] CALLAHAN T，ALLMAN M，RABINOVICH M. On modern DNS behavior and properties[M]. ACM，2013.

[17] 魏帅，于洪，顾泽宇，等. 面向工控领域的拟态安全处理机架构[J]. 信息安全学报，2017，2(1)：54-73.

[18] 扈红超，陈福才，王禛鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报，2016，1(4)：40-51.

[19] 吴文青，唐应辉，兰绍军. 修理设备可更换的 $k/n(G)$ 表决可修系统[J]. 数学学报(中文版)，2016，59(6)：799-820.

[20] 柏仲干. 复杂系统 Bayes 可靠性评估方法研究及其应用软件的研制[D]. 长沙：国防科学技术大学，2003.