



拟态计算与拟态安全防御的原意和愿景

邬江兴

(信息工程大学 郑州 450002)

摘 要:以高效能和高安全性计算为目标,提出了以多维重构函数化体系结构与动态多变体运行机制为核心的拟态计算和拟态安全防御技术体系,并对二者的概念和机理从原意和愿景的角度进行了概略介绍,最后给出了需要进一步研究的主要科学与工程问题。

关键词:拟态计算;拟态安全防御;多维重构

doi: 10.3969/j.issn.1000-0801.2014.07.001

Meaning and Vision of Mimic Computing and Mimic Security Defense

Wu Jiangxing

(Information Engineering University, Zhengzhou 450002, China)

Abstract: To facilitate high-performance and high-security computing, a technology system based on mimic computing (MC) and mimic security defense (MSD) was proposed. The proposed system focused on both the multi-dimensional reconfigurable and functional architecture and the dynamic varied mechanism. An overview about the concept and mechanism of the MC and MSD was also introduced from the angles of meaning and vision. The science and engineering problems to be further addressed were given in the end.

Key words: mimic computing, mimic security defense, multi-level reconfiguration

1 引言

随着计算机技术的发展,原有的体系结构遇到了“功耗墙”、“存储墙”等一系列的瓶颈问题,追求高效能计算已经成为技术进步的关键问题之一。

以国家科学技术部“十二五”国家高技术研究发展计划(“863”计划)“部市合作”重点项目“新概念高效能计算机体系结构研究和原理样机研制”为依托,目前的国内研究以高效能计算为目标,从体系结构创新入手,对高性能计算在多个典型领域的应用、结构和效能关系进行了深入分析,揭示出“刚性不变的体系结构支持差异巨大的应用

是使计算效能低下的根本原因”,引入了“应用决定结构,结构决定效能”的理念,提出了基于多维重构函数化结构与动态多变体运行机制的拟态计算体系——拟态计算(mimic computing, MC)。

拟态计算固有的随机性、动态性和不确定性,自然中断了目前攻击技术所依赖的攻击链完整性。因此,基于拟态计算的信息系统具备内在的主动防御能力,称为拟态安全防御(mimic security defense, MSD)。相关分析和初步试验表明,MSD 有望成为改变网络空间游戏规则的革命性技术,有可能从根本上摆脱目前网络空间“易攻难守”的战略困局。

2 MC 的原意与愿景

2.1 MC 的原意

图灵—哥德尔—邱奇的可计算性理论^[1]和冯·诺依曼体系结构^[2,3]组成了当今计算机科学与工程的基础。可计算性理论只解决了可计算问题,并未考虑到计算效率问题;冯·诺依曼结构只解决了可计算理论的工程化和实用化问题,也未关心计算速度和效率问题。

自 20 世纪 40 年代第一台电子数字计算机问世以来,计算系统的速度得到了突飞猛进的发展,这一方面得益于器件技术的进步,另一方面则归结于体系结构技术的进步。随着流水线^[4,5]、并行技术^[6]等非冯结构的引入,尤其是大规模分布式并行计算及异构众核^[7,8]的发展,使得结构对计算速度的提升有了前所未有的成效。

然而,随着高性能计算机(high performance computer, HPC)的速度向着 E 级甚至 Z 级目标迈进,功耗问题正成为最大的拦路虎之一^[9]。尽管采用了多层次全方位的降功耗工艺和技术,目前 P 级 HPC 的运行功耗仍高达 10~20 MW。据预测,若没有更有效的低功耗和降功耗技术,未来 E 级 HPC 功耗有可能突破百兆瓦。在功耗成为工程实现难题的同时,应用的经济性问题也随之被提出,高效能计算已成为高性能计算机发展的新出路或新方向。

计算机应用实践表明,在硬件系统不变的情况下,通过软件算法的改进可获得运算速度和计算效能的等效提高,即一个问题往往存在多个不同的解决或实现方案;每个方案的不同阶段、不同时段存在多种可供选择的实现算法;每个方案的特点和属性不同,对计算环境和计算代价的要求也不同;每个方案的计算性能和运行效能也大不相同。若能在恰当的场合、恰当的时机、动态地选择恰当的实现方案(或称程序变体),就可能在限制条件下逼近计算效能的最优值。

硬件系统也可以设计成多种功能等价、效能不同的执行变体或计算环境方案,系统运行时硬件系统也能根据应用需求,在恰当的场合、恰当的时机,选择(或生成)恰当的方案。

这种包含了软件和硬件变体的多维重构函数化体系结构就是拟态架构(mimic structure),它能根据动态参数选择生成多种功能等价的可计算实体,实现拟态变换。对于一个确定的可计算问题,在拟态架构中可以由多种功能等价、计算效能不同的硬件变体和软件变体来实现,动态地选择与使用这些变体,计算效能可以达到最优化,这就是

拟态计算。实现了拟态计算的系统,运行效能无疑将会得到更为显著的提升。

2.2 MC 的愿景

MC 并不企图独立地构建高效能的计算系统,也不排除器件工艺进步和变频或资源管理等引入的降耗增益,更不拒绝优化软件算法提高计算效能的好处;而是借助“应用决定结构、结构决定效能”的思想,通过适时动态重构相应的系统运算结构或执行环境,达成提高运行效能的目的。

通过基于多维重构的函数化体系结构的呈现,应用问题可实时选择或定制相对理想的计算环境,包括计算和控制部件、存储部件、互连部件、输入输出部件等;任务或作业也可以根据不同资源情况、不同服务质量要求、不同处理负荷、不同同时段的运行效能等因素,在多种功能等价、效能不同的硬件执行变体(或环境)以及相关的多样化程序变体间做出调度,并能实现任务或作业的跨环境动态迁移。

传统计算系统的处理结构在总体上是确定的,且没有多少可变因素。所有应用必须基于这样一个刚性计算环境进行编程设计,这就是所谓的“应用适应结构”的可计算性取向,导致体系结构严重束缚运行效能的改善。

然而,硬件系统的结构变换也要受到器件技术、实现复杂性、结构变换开销和价格因素的限制,不可能做到任意变化。借用生物学的拟态概念来表征有限程度、有限规模的结构动态变化是合适的:一方面“结构适应应用”要求系统具有“形状”相似的能力,另一方面“结构动态变化”要求系统具有“行为”相同的能力。因此,拟态的相似性、相同性和有限性,正好刻画出拟态计算旨在通过基于多维重构的函数化(也可称为“拟态变换”)体系架构获得高效能计算的本质。此外,功能等价的多变体执行环境具有天然的冗余属性和内在的高可靠性、高安全性优势。

3 MSD 的原意与愿景

3.1 MSD 的原意

拟态安全防御是指在主动和被动触发条件下动态地、伪随机地选择执行各种硬件变体以及相应的软件变体,使得内外部攻击者观察到的硬件执行环境和软件工作状态非常不确定,无法或很难构建起基于漏洞(bug)或后门的攻击链,以达成降低系统安全风险的目的。

拟态安全防御的机理可以借用生物学拟态概念的四性——有限性、相似性、相同性和透明性来表征。在生物学



上,这四性主要表现在变化的有限性(有限场景、有限跨度、有限逼真度)、变化场景的相似性(“外观”相似)、变化形态的相同性(“行为”相同)以及由本体功能和性能的不变所体现出的透明性。在计算机的拟态体系结构中,这四性也有相应的体现。比如说,FPGA的可重构规模和粒度体现了有限性;所有通用机、专用机都可以等效为图灵机,有各种功能相似的操作系统,这些都是相似性的体现;同一源程序在不同运算平台应产生相同的执行结果体现了相同性;运算器、流水线和总线结构对源程序的透明则体现了透明性。

当前信息系统中,由数百万行代码组成的庞大软件仅仅需要一个漏洞或后门,就可能被数十行左右的脚本代码所完全“拥有”。同理,由数十亿晶体管组成的复杂片上系统(system on chip, SoC),仅仅因为一个设计漏洞或总量上可忽略不计的晶体管资源构成的后门,就可能被攻击者注入少量代码所完全“掌控”。所以,从防御者的角度来说,这些构成软件的数百万行代码和构成硬件芯片的数十亿只晶体管,必须得到完备的设计和整个安全链上诸环节、全要素的保护,才能防止一个漏洞或后门被利用;从攻击角度来说,只需要找到或留有一个漏洞或后门,就能破坏或掌控整个系统。攻击技术的发展使防御“疲于奔命”,从软件阶段拓展到硬件阶段,从数据层扩展到物理层,进而发展到更高级的软硬件协同持续(动态)攻击阶段。在未知漏洞或后门的利用和防护方面攻防双方成本空间的不对称性日益增加。

特别是近些年来,随着攻击技术从软件阶段拓展到硬件阶段,进而发展到更高级的软硬件协同持续攻击阶段。全球网络空间发生的众多标志性的信息安全事件都充分阐明,攻击者和防御者在成本空间的严重不均衡地位。

要从源头上解决信息系统的安全问题,必须实现“核心自主、逐步替代”的战略,但从现状来看,对设计和生产各个环节的完全自主依然任重道远,短期内很难解决整个安全链无后门、无漏洞的问题。从当前的主流防御技术来看,基于先验知识(特征或指纹)的被动防护,不能适时避免或缓解利用未知漏洞和后门的攻击问题。拟态安全防御就是要在被动的局面下实现主动的防御。

相比于传统信息系统的静态性、相似性和确定性,拟态计算系统具有视在的非持续性、非相似性和非确定性的基本属性,这与网络攻击所依赖的静态性、相似性和确定性正好相左。在动态持续攻击常态化背景下,在漏洞和后门以及可能驻留的病毒和木马信息缺位的情况

下,防御方通过动态化和随机化的内核结构与主动变化的安全机制,大幅度地增加未知漏洞和后门的利用难度,扰乱或破坏未知病毒和木马依赖的攻击链。与目前主流的基于加密认证和基于先验知识的病毒查杀等安全措施相比,拟态安全可以弱化利用未知漏洞、后门或病毒、木马的攻击威胁,可以弱化基于特征嗅探和状态转移的内外部攻击。所以,防御方基于拟态计算架构,并引入其他的动态化和随机化措施,不难构建起非对称的MSD系统,以应对网络空间的现实威胁,达到系统安全风险可控的目的。

MSD主要针对网络空间攻击成本和防御成本的严重不对称性,以及我国信息领域核心技术与产业基础严重滞后国家安全需求的严峻性而提出,它是一种改变游戏规则的创新性技术,力图扭转目前网络空间“易攻难守”的战略格局。

3.2 MSD 的愿景

一般说来,基于漏洞的攻击和防御有如下特点。

(1)漏洞层面

漏洞是软硬件设计导致的错误,可以被攻击者利用。理论上,就一个给定的检验规范,可以用形式化的正确性证明技术,找出并消除软硬件中所有的错误或漏洞。事实上,以现在的科学和工程技术水平,构建任何一个复杂的大型信息系统,既不能保证任何物理实现或逻辑实现无缺陷,也不能保证任何物理层或逻辑层的设计与工程化无漏洞。

(2)攻击层面

攻击者必须了解特定系统中的漏洞和基本的执行环境,才能利用这个漏洞,采取特定的攻击手段,或者使用确定的后门。其高度依赖传统目标系统的静态性、确定性和相似性,目标系统所暴露的时间越长,可供攻击者研究其运行规律、发现其弱点、创建和验证有效攻击方法的时间窗口就越大。

(3)防御层面

当前目标系统消除漏洞的方法主要有移除漏洞、打补丁和精确识别与阻断攻击3类。然而,这3类防御手段不是有完备性缺陷,就是阻止不了“零日漏洞攻击”抑或无法摆脱被动防御的困境。

作为攻防双方间的博弈,恶意软件开发者为了防止攻击被防御方从容地检测到,研发了具备动态变化攻击软件行为特征和手法的平台环境。所以,传统的基于某个物理(如CPU)或逻辑(如操作系统)实体安全可控性而建立的查毒、杀毒、堵漏和局部动态化、随机化的安全防御体系,都难以摆脱“漏洞攻击”和被动防御的困扰。为扭转这种不

对称优势,防御方也必须构建一个能够动态改变其视在特性和代码的系统,使攻击方同样没有足够的时间来从容发现和利用目标系统的漏洞。

尽管任何一种确定的结构或机制都很难证明或实现无漏洞或无缺陷存在,但是实时重构的体制和动态多样化机制的组合(乘法)运用,并不是试图完全消除缺陷或漏洞,而是通过大幅度增加漏洞的利用难度来降低攻击的实时性和有效性。同理,对于预先植入或预留的木马或后门的利用也会造成类似的难度和效果。

MSD 针对攻击链严重依赖静态系统架构和相关运行机制所特有的脆弱性,用多维重构技术和动态化随机化运行机制,试图联合其他各种安全防护技术,搭建起一个对构件级可控性不敏感的主动防御体系。这个体系的安全可控内核是由一个多维重构的执行环境和一个基于认知的动态化、随机化的运行机制构成的。在所创建的动态化、非确定和非相似的“迷局”中,允许使用“带毒含菌”的器件、部件或软硬件构件,并能将系统安全风险控制在防御方可接受的范围内。

MSD 并不试图一劳永逸地解决网络空间所有的安全问题,也不企图独立地构建完美的防御系统来阻止各种攻击,更不拒绝通过器件、组件、部件、软件和硬件等构件层面的自主可控途径获得的安全增益。而是试图在可接受的成本和复杂性代价条件下,为信息系统现有或将来可能发展出的安全技术,找到可以在不同层次、不同场景下均能持续获得高安全性的基础架构与安全机制。这样的基础架构和安全机制应能主动、动态且随机地改变防御方的视在特性和代码。相对于基于先验知识的被动防御聚焦于精确清除已知病毒和木马的方法,拟态安全致力于扰乱或阻断未知漏洞或后门利用的攻击链,极大地缩短外部攻击者和内网渗透者嗅探系统特征及规律的时间窗口,作为倍增器放大传统安全措施的功效。

值得注意的是,MSD 体系内核的安全性并不完全依赖自主可控、“零缺陷”设计与实现和非公开保密手段等因素,而主要通过基于认知的动态化、随机化的多维重组结构本身得到保护。运行中,结构函数的自变量取自当前系统负载情况、资源状况、服务质量、能效水平、安全状况和时间等动态参数,结构函数算法的公开并不会影响系统的安全可控性。即 MSD 的可信根不是任何物理或逻辑实体,而是动态化、随机化运行机制和多维重组结构本身。

MSD 系统的高安全风险可控性,不仅源自内核的

函数结构与动态化、随机化运行机制的组合运用,而且源自从内核直至应用层采用的已有(或未来可能发展出的)安全措施的深度组合(连乘)运用。换言之,MSD 能够自然地接纳各种安全防御技术,并可倍增甚至指数化增加攻击方的难度。

MSD 基于拟态计算理论,以提供运行环境的动态性、非确定性、异构性、非持续性为目的,通过网络、平台、环境、软件、数据等结构的主动跳变或迁移实现拟态环境,以防御者可控的方式进行动态变化,对攻击者则表现为难以观察和预测的目标变化,从而大幅度地增加攻击难度和成本,大幅度地降低系统安全风险。总之,一个具备 MSD 属性的系统能够在功能等价的条件下主动、随机地改变自身架构及执行环境,利用软硬件多样化、协同化、动态化地执行变体的伪随机性,在表象上给对手造成系统“攻击表面”不可预测的迷局。

3.3 拟态安全防御的特点和问题

从拟态安全防御的技术基础、基本原理和实现来看,它具有以下特点。

- 针对攻击链依赖传统系统架构和运行机制的特有的脆弱性,组合应用多维重构技术和动态化、多样化、随机化的安全机制,扰乱或阻断攻击链,增加攻击难度,实现不依赖先验知识的主动防御。
- 在所创建的动态化、非确定和非相似的“迷局”中,允许部分使用“带毒含菌”的器件、部件或软硬件构件,并能做到安全风险可控,可缓解自主产业能力不足的困境。
- 通过函数结构和动态机制的组合(乘法准则)应用,大幅度地降低漏洞或后门利用的可靠性。对于预先植入或预留的木马或病毒的利用,也会造成相似的难度。
- 内核的安全风险并不取决于“零缺陷”设计与实现或算法保密等外在因素,只取决于系统当前的资源状态、服务质量、运行效率、异常情况、流量特征和时间基准等非封闭动态参数的随机性。
- 能有机整合现有(或未来可能发展出)的安全防御手段,通过与拟态机制的深度组合(连乘)运用,构成主被动融合式防御体系,能够倍增甚至指数化地增加内外部攻击的难度。
- 拟态计算架构作为拟态安全防御的内核,具有高效计算的固有属性,可为防御的实时性需求提供强有力的系统结构层面的支撑。



- 拟态计算架构固有的冗余性,使拟态安全防御系统具有内在的可靠性。根据安全性需求,调整冗余度,可控制系统成本,权衡可靠性。
- 基于资源冗余配置的冗余资源应用模式,能够形成共生协同、 N 变体、等效多变体、异构环境迁移等特殊运行机制,为及时发现、抑制、阻断和清除病毒或木马提供了新空间、新视野。

拟态安全的主要问题有以下3个方面。

- 复杂性高:冗余资源和拟态能力的管理问题,软硬件多变体与作业、任务、进程异构环境迁移,环境快速清洗等都是工程技术上复杂性极高的问题。
- 功耗增加:软硬件多变体同时或同步运行时,功耗会显著增加等。
- 验证难:随机系统测试验证困难等。

4 MC 与 MSD 的实现基础及后续研究问题

4.1 MC 和 MSD 的实现基础

MC 是 MSD 的基础,拟态变换是两者共同的技术要点,但应用目的有所不同,前者是通过拟态变换追求高效能的计算,而后者则是通过拟态变换追求系统的低安全风险。因此,二者所依赖的技术基础有很多相同之处。主要用到的基础技术有仿生学技术、认知技术、可重构技术、信息安全技术、拟态计算技术、通信干扰技术等。

近年来相关理论和技术的进步,给 MC 和 MSD 技术的发展带来了可行性,主要包括:

- 集成电路工艺的不断进步;
- 多维可重构理论和技术的进步;
- 可编程器件技术的进步及应用领域的拓展;
- 异构多核及众核随机化技术;
- 虚拟化和异构环境负载迁移技术的发展;
- 以可重构智能互连为中心的系统架构技术;
- 二进制代码翻译技术;
- 基于 C 语言的 FPGA 高级编程工具;
- 动态多样化随机化技术;
- 基于即时编译器的多变体技术等。

4.2 MC 和 MSD 的后续研究问题

MC 和 MSD 的研究要重点关注以下3个领域。

(1)同步管理能力与实时性要求

有效管理各种“拟态安全”的能力,包括监测、建模、分析和理解系统本身以及网络空间与其交互的其他系统,还有应

对威胁环境的能力。防御对实时性要求很高,紧迫时限内要完成复杂分析须极大地提升分析速度,缩小反馈环路响应时间并尽可能消除人为因素的影响,如确实需引入人的因素,就必须提供一套信息表达、引导、分析导航方面的创新方法。

(2)重视自然灵感的解决方案

自然界有很多的生物系统远比人类的网空系统复杂,却极其稳健、灵活和高效。在抵御细菌和病毒入侵时启动的免疫系统能够很好地发挥作用,如分布式处理、病原体识别、多层保护、分散控制、多样性和信号表征等,都展示出大量具有启发性的机制,可用于形成解决网络空间安全问题的创意。

(3)持续关注理论、方法和工具研究

当在系统的不同层面、不同时机、不同阶段引入多样化、动态化、随机化因素后,传统的软硬件设计理论和支撑技术已不适应,需要发展新的理论体系及创新方法与开发新的工具技术。

需要重点开展的研究内容主要有:有关机制及有效性的科学论证与概念抽象;漏洞成因和利用机制的形式化描述方法,论证系统随机动态变化对攻击利用这些漏洞能力的影响;单个组件随机动态化对复杂系统性能的影响,尤其是系统弹性和规避威胁能力的影响;开发一种能够体现系统复杂性并实现系统有效性与弹性管理的控制机制;随着对系统行为理解的不断深化以及所面临威胁的不断演变,使“拟态安全”机制可持续发展。

作为新兴的技术方向,MC 和 MSD 仍有许多工程化甚至应用基础问题待解决,例如:

- 函数化结构系统的运行支撑技术和生态环境的构建;
- 软件兼容性问题;
- 实时可编程技术;
- 可重构高阶运算栈技术;
- MC/MSD 的一般性模型和评估评价方法;
- 基于动态化多样化基础架构的高级编译工具和系统开发工具;
- 跨平台即时编译工具;
- 自动多样化变体生成和编译技术;
- 异构环境进程或作业迁移技术;
- 动态改变管理系统和网络配置的自动化方法;
- 效能/安全性评估模型和定量分析;
- 相关量化评价方法与测试技术等。

5 应用前景展望

拟态安全产品技术可以按照先简后难、先高端后低端、先专用后通用的方式逐步完善,3 年内有望推出阶段性的商品化产品,5 年内有望形成规模化市场,10 年内有可能成为主流市场。

从核心方面,打造自主可控的国家信息通信核心网络,将拟态安全应用于核心路由器、边界路由器、汇聚路由器等;在企事业单位,将拟态安全应用于接入路由器、交换机、网关和防火墙等;在终端打造各种基于拟态安全的应用平台;在基础软件、支撑软件、工具软件等软件方面,全面引入拟态安全机制,以此全方位形成网络空间安全的新格局。这对于改变或缓解我国目前甚至今后相当长时期内,在自主可控领域面临的严峻形势具有重要的战略意义。

参考文献

1 Turing A M. On computable numbers, with an application to the entscheidungs problem. Journal of Math, 1936, 58(12): 345~363

2 Krishnaprasad S. Extending von neumann uniprocessor architecture to exploit result sharing. Proceedings of the IEEE Southeastcon, Charlotte, 1993

3 Bokor J, Nadai L, Rudas I J. Controllability of quantum bits from the von neumann architecture to quantum computing. Proceedings of the IEEE International Symposium on Computational Intelligence and Intelligent Informatics, Agadir, 2007: 9~12

4 Geiger G, Hazel T, Vogt D. Integrated SCADA-based approach for pipeline security and operation. Proceedings of Record of Petroleum and Chemical Industry Conference (PCIC), Record of Industry Applications Society, the 57th Annual Conference, San

Antonio, 2010: 1~8

5 Kock A A A, Etman L F P, Rooda J E. Effective process times for multi-server flowlines with finite buffers. IEEE Transactions, 2008, 40(3): 177~186

6 Kumm E T, Lea R M. Parallel computing efficiency: climbing the learning curve. Proceedings of IEEE Region 10's Ninth Annual International Conference, Singapore, 1994: 728~732

7 Sandrieser M, Benkner S, Pillana S. Explicit platform descriptions for heterogeneous many-core architectures. Proceedings of IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), Shanghai, China, 2011: 1292~1299

8 Kramer D, Karl W. Realizing a proactive, self-optimizing system behavior within adaptive, heterogeneous many-core architectures. Proceedings of IEEE Sixth International Conference on Self-Adaptive and Self-Organizing Systems (SASO), Lyon, 2012: 39~48

9 Phan D H, Suzuki J, Carroll R, *et al.* Evolutionary multiobjective optimization for green clouds. Proceedings of the Fourteenth International Conference on Genetic and Evolutionary Computation Conference Companion, New York, USA, 2012: 19~26

[作者简介]



邬江兴,男,中国工程院院士,信息工程大学教授、博士生导师,主要研究方向为交换技术、宽带信息网络、高效能计算。

(收稿日期:2014-06-22)

·简讯·

2014 年第 2 季度通信业主要通信能力

指标名称	单位	本季末到达	比上年末新增
光缆线路长度	km	18 837 559	1 386 379
其中:长途光缆线路长度	km	920 394	22 622
固定长途电话交换机容量	万路端	1 164	-106.3
局用交换机容量	万门	38 109.2	-2 943.0
其中:接入网设备容量	万门	21 371.0	-1 152.7
移动电话交换机容量	万户	201 466.8	4 921.5
互联网宽带接入端口	万个	37 892.1	1 919.7

(来源:工业和信息化部运行监测协调局)