DOI 10.15302/J-SSCAE-2016.06.015

拟态防御技术结合软件多样化在软件安全产业中的应用

庞建民[1]，张宇嘉[1]，张铮[1]，邬江兴[2]

（1. 中国人民解放军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；
2. 中国人民解放军信息工程大学国家数字交换系统工程技术研究中心，郑州 450002）

摘要：随着互联网的飞速发展，计算机软件全球化的进程不断推进。大量相同软件安装在数以万计的计算机中，容易导致黑客利用软件的漏洞，攻击安装了该软件的所有计算机。传统的软件安全措施是依靠对漏洞进行修补，其只能起到亡羊补牢的作用。软件多样化技术可以使这种情况得到缓解，但其并没有从根本上消除漏洞带来的威胁。本文提出将拟态防御技术与软件多样化技术相结合应用于软件安全产业，可以消除漏洞带来的威胁。

关键词：软件多样化；拟态防御；软件安全产业
中图分类号：TN915　　**文献标识码：**A

Applying a Combination of Mimic Defense and Software Diversity in the Software Security Industry

Pang Jianmin[1], Zhang Yujia[1], Zhang Zheng[1], Wu Jiangxing[2]

(1. State Key Laboratory of Mathematical Engineering and Advanced Computing, The PLA Information Engineering University, Zhengzhou 450001, China; 2. National Digital Switching System Engineering & Technological R&D Center, The PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: With the development of the Internet, the process of computer software globalization continues to push forward. For widely used software, anidentical binary code is installed on millions of computers; sometimes even hundreds of millions. This makes widespread exploitation easy and attractive for an attacker because the same attack vector is likely to succeed on a large number of targets. Traditional software security methods can only counter the threat temporarily, and cannot eliminate essential vulnerabilities. This paper proposes a scheme of combining software diversity with mimic defense in the software security industry.

Key words: software diversity; mimic defense; software security product

一、前言

我国早在“十五”规划中就明确指出发展信息产业的重要性，信息技术在国家经济和社会各领域的应用能够建设一条在信息化带动下的新型工业化道路。而近期的“十三五”规划又指出应该着眼于

收稿日期：2016-10-08；**修回日期：**2016-10-28

作者简介：庞建民，中国人民解放军信息工程大学数学工程与先进计算国家重点实验室，教授，博士生导师，主要研究领域为逻辑与推理、信息安全；E-mail: jianmin_pang@hotmail.com

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)
本刊网址：www.enginsci.cn

网络安全和信息化发展，其中提出了要保障国家网络基础设施、重要信息系统和数据资源等一系列关乎国家根本利益客体的安全性，提高网络治理能力，保障国家信息安全。为了解决网络安全这一国家发展的根本需求，发展规划中又提出应该在信息保护、信息管理、安全审查和自主可控等关键技术能够有所创新。软件安全产业作为网络空间安全产业中的基石和在未来对社会经济增长、国家发展具有重要推动力的产业，其标志着一个国家战略方向，同时也是指导国家经济的风向标，是一个国家在二十一世纪关键竞争力之一。在国际软件安全产业发展过程中，不同的国家采用了不同的发展道路和模式，经济学中产业发展的相关理论指出，产业的发展模式、模式选择以及影响因素等都会对未来该产业发展的道路产生深远影响，因此我国的软件安全产业的规划应该探索出一条适合我国的软件安全产业发展的道路，其直接影响着未来我国软件产业的兴盛。

拟态防御技术在这一关键时期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防御技术体系，其着重于高效能和高安全性计算。拟态防御技术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变革性技术，力图扭转目前网络空间“易攻难守”的格局。

二、我国软件产业的安全现状

（一）软件产业面临的安全问题分析

1. 针对软件漏洞进行攻击

2016 年 8 月 23 日，中国互联网络信息中心 (CNNIC) 发布的第 38 次《中国互联网络发展状况统计报告》显示，截至 2016 年 6 月，中国网民规模达到 7.1 亿，互联网普及率达到 51.7 %，半数中国人已接入互联网，越来越多的人接触到网络 [1]。软件作为互联网发展的重要载体，已经渗透到人们生活的各个领域，也因此成为破解者攻击的目标。这就意味着越来越多的人正受到软件安全的威胁 [2]。2015 年，丹麦安全公司 Secunia 的研究团队对来自 263 个软件供应商的 2 484 款软件进行漏洞扫描，结果发现总漏洞数量为 1 6081 个，相比较 2014 年总量增加了 2 %，相比较 2010 年总量增加了 39 %。进一步分析发现，大部分检测到的漏洞（45.6 %）是不重要的；而中等级别的危险漏洞占比为 25.5 %，高危安全漏洞占比为 13.3 %，占比为 0.5 % 极端危险的漏洞。在漏洞分类上，57 % 的缺陷是通过远程网络访问方式进行的，35 % 是通过本地网络进行的，还有小部分（8 %）需要攻击受害人的电脑来触发缺陷。IEEE729-1983 对缺陷有一个标准的定义：从产品内部看，缺陷是软件产品开发或维护过程中存在的错误、不足等各种问题；从产品外部看，缺陷是系统所需要实现某种功能的失效或违背。

2. 针对软件进行逆向破解

软件开发人员代码编写粗糙和不安全编程是计算机软件缺陷形成的主要原因。很多软件开发人员在设计和编写代码初期没有或者较少考虑软件的安全问题，而软件交付后用户的不恰当使用常常容易导致缺陷的出现。在当前开放性架构的计算系统中，用户可以完全控制自己的系统并且可以更改软件和进程。有些用户会试图分析软件保护机制，其常是带有纯技术以外的恶意目的。软件开发者为了保护未授权的软件拷贝或软件中的知识产权，通常需要防止软件被逆向。常用的加密算法，如 AES、RSA、ECC，其设计初衷是专为在“可信”的实体之间交换加密的消息。加密和解密的运算在黑箱中进行，黑箱内部是安全的。攻击者只存在于受信任的实体之间，无法知道加密、解密实体内部的信息和具体实现 。市场上有很多不同的代码保护技术，这些技术提供防止逆向工程和代码分析的功能。这些方案不管是否成功和复杂，大多数都无法对抗通用破解。所谓通用破解指的是一旦能够成功地破解某个软件实例，那么就可以把类似的破解应用于同样软件的所有实例上。这无疑给软件厂商造成了巨大的损失。通用破解的根本原因是目标软件的所有拷贝都有同样的二进制码，这样攻击者就可以成功地开发出通用的破解方案。

（二）解决软件安全问题的意义

从需求层面看，随着愈演愈烈的各种信息泄密、大量的 APT（高级持续性威胁）攻击等事件发生，

很多企业对信息安全的认识已经从“被动的防御”变成“主动的核心竞争力塑造”，尤其是新型的互联网金融、电商、云计算等都前瞻性地把安全当做市场竞争的重要砝码并寻求各种方法来不断提升其安全性。

软件产业不但自身能形成庞大规模，拉升国民经济指数，还能大幅度提高国家整体经济运行效率。随着信息经济的深入发展，软件产业将会成为衡量一个国家综合国力的标志之一。软件安全产业作为保障国家顺利发展的基石，从软件产业对其他行业的辐射拉动效应层面上看，发展软件安全产业的意义不仅在于软件产业发展，而且对传统制造业也有相同的辐射作用，对整个社会经济都具有很大的拉动作用。

三、软件安全问题的解决措施

（一）软件的自主可控

人们在考虑软件安全问题时往往只考虑其外部防护措施，例如防火墙、入侵检测和防病毒软件等，但对于软件自身存在的后门和漏洞，以上的安全措施可能完全无效。信息安全的本质是自主可控[3]，应该高度重视信息系统本身软硬件的安全问题，尤其是基础软硬件、核心设备等更是影响重大。自主可控主张如果能用国产软件就应该用国产的，但是国产化并不等于安全。信息安全的特殊性是一定存在一个“第三方”，即威胁方，他不是一成不变的。而且我国在软件产业发展的道路上与发达国家还存在一定距离，在 IT 领域有很多关键技术以及零部件往往受制于国外，在软件开发的质量和效率上还有很长的路要走，因此，实现完全的自主可控在中国还存在一定困难。

（二）软件多样化

Cohen 早在 1993 年就指出软件的一元化会对计算机安全带来潜在的威胁[4]。攻击者通过利用软件漏洞轻易地对部署了该软件的所有计算机进行攻击。软件多样化是指同一个软件的多个实例有不同的可执行二进制代码。其最早的应用是用于某些重要领域系统容错机制的实现，利用由多个可选版本程序来组成多样化系统。很明显软件多样化较单版本程序拥有更高的可靠性和安全性。多个可选版本程序的差别对于终端用户是透明的，其具有完全相同的功能，仅在功能的实现上有细微的差别。对于黑客来说，每个实例具有同样的功能，但它们具有不同的二进制代码以及运行流程。软件多样化可以防止黑客把从某个实例获得的信息应用于其他实例，这样黑客就很难开发出对整个软件所有实例都适用的通用漏洞利用和破解方案，每个软件实例必须要单独攻击或破解。软件多样化是应对通用攻击和破解的一个十分有效的技术。它能够大大增加对被保护的应用软件的攻击难度和破解所花费的时间。极端状况下，攻击者甚至必须要对每个客户端的二进制代码进行单独分析。软件多样化对于防止在开放环境下大量分发并安装的软件被攻击和破解是十分有效的手段。软件多样化的实现有很多方法，如利用不同编程语言（C/JAVA/Python/Object-C）的多版本编程、基于编译器的软件多样化和软件二进制代码重写等。

虽然软件多样化在一定程度上提高了攻击者对软件进行攻击和破解的门槛，但同时也增加了软件开发和维护的难度，且成本昂贵。对大规模部署的软件实施软件多样化，将使软件的维护更加复杂。

（三）拟态防御技术

虽然软件多样化在一定程度上增大了针对软件漏洞攻击与利用的难度，但并没有完全消除威胁，为了使系统达到更高的安全性和可靠性，不仅需要对软件采用各种不同的多样化手段，并且需要引入投票机制（大数表决机制）以产生相较于多版本程序集中单个执行体更加可靠的输出。在此基础上提出的拟态防御思想[5]，其核心就是基于多样化（异构性）的表决机制，其中必要的多样化可以包括软件和硬件等多个构件。

基于拟态防御技术的软件保护，不依赖于自身的保密性，而是通过软件多样化方法对待保护软件构造一个含有多个异构变体的集合，常用的方法是利用多样化编译生成变体集合。基于编译器的多样化技术，例如等价指令替换、控制流混淆和花指令插入等都在不同程度上改变了程序的目标代码，添加了新的无关指令或改变现存的控制流方向[6]。图 1 展示了依赖于多样化编译器的功能等价多变体的生成过程。对程序的所有输入将会被复制并分发给所有异构变体。多变体的异构性特征和与之采用

的多样化技术相关，当攻击特征与变体异构性特征相重合时，攻击产生的输出在不同变体上将会不同，通过比较变体的所有输出并对其进行表决，可以防御针对该异构特征的攻击，并能够识别出受到攻击的变体。基于拟态防御的设计框架见图2，变体A、B、C分别由多样化编译器针对同一软件源码编译生成。

从拟态防御的设计框架很容易看出，其将原本只需要一个程序执行的工作同时交给了三个变体，这样的设计框架带来的优点如下[7]：

（1）利用多样化的安全机制，扰乱或阻断攻击链，增加攻击难度。

（2）允许一定程度地使用“带毒含菌”的软件构件，并能够做到安全风险可控。

（3）软件运行机制的组合应用可以构成相当大的动态空间，以有效降低利用漏洞和后门进行攻击的可靠性。

（4）冗余获得的高可靠性，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。

（5）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的运行机制，可以为“容毒”运行和及时发现、抑制、阻断、清除木马及病毒提供创新方法空间。

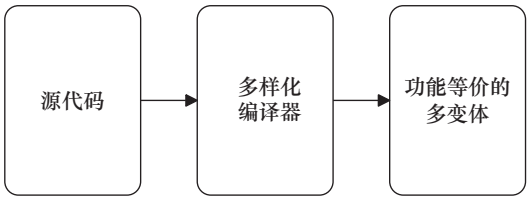

图 1　功能等价多变体的生成过程

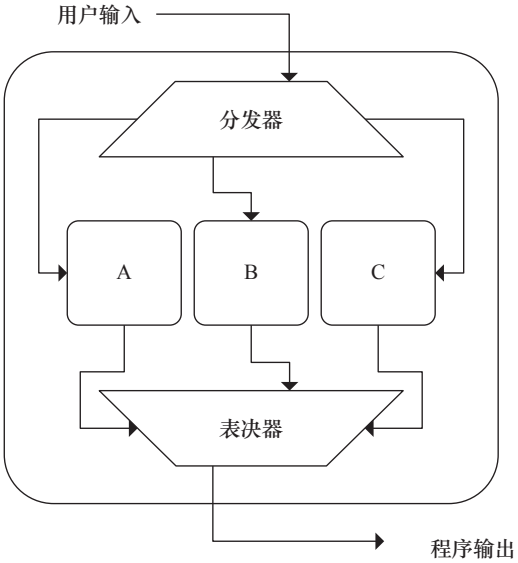

图 2　基于拟态防御的设计框架

四、结语

在网络空间安全形势和全球化背景下，国与国之间的产业合作日益紧密，而竞争也更加激烈。软件产业不仅在规模、创新性上有了更大的发展机遇和挑战，同时也面临着日趋复杂的安全性问题。解决软件安全不仅要综合利用已有安全技术，更需要理论创新的指导和技术创新的支持。新一代软件体系需要配合国家安全战略，一方面关注研发自主可控的软件体系；另一方面利用拟态防御等安全架构，实现基于非可信组件的可信系统，从各个环节实现软件安全发展。

拟态防御技术作为“网络空间再平衡战略”的有力抓手，能够为软件安全提供架构技术，解决软件安全面临的漏洞攻击和破解问题。在当今国内外软件安全产业市场份额不对等、安全地位不对称的情况下，拟态防御技术为解决组件级安全问题提供了一种新的解决思路，即通过安全架构技术解决软件内存在的漏洞和后门，尤其是未知漏洞和后门，在一定程度上，缓解了软件产业中由于技术劣势带来的软件安全威胁。另外，拟态防御技术是我国首次提出的主动防御技术之一，技术本身的自主可控为软件产业的安全问题提供了普适的解决方案，为解决信息系统软件安全问题提供了技术支撑，为推进国家安全战略部署提供了有利条件。

参考文献

[1] 中国互联网络信息中心. 第38次中国互联网络发展状况统计报告 [EB/OL]. (2016-08-03)[2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.
China Internet Network Information Center. The 38th statistical report on internet development in China [EB/OL]. (2016-08-03)[2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.

[2] Symantec Corporation. Internet security threat report 2016 [R/OL]. (2016-04-01) [2016-10-08]. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[3] 倪光南. 信息安全“本质”是自主可控[J]. 中国经济和信息化, 2013(5):18–19.
Ni G N. The Nature of information security: Autonomous and controllable [J]. China Economy & Informatization, 2013(5):18–19.

[4] Cohen F B. Operating system protection through program evolu-

tion [J]. Computers & Security, 1993, 12(6): 565–584.

[5] 邬江兴. 专题导读——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): 1–7.
Wu J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014, 30(7): 1–7.

[6] Jackson T, Salamat B, Homescu A, et al. Compiler-generated software diversity[M]//Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense. New York: Springer, 2011: 77–98.

[7] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014, 10(1): 4–9.
Wu J X. Mimic security defense in cyber space [J]. Secrecy Science and Technology, 2014, 10(1): 4–9.