软件动态分析与信息系统安全 *

应凌云 杨 轶

（中国科学院软件研究所信息安全国家重点实验室 北京 100190）

摘要 信息系统的应用越来越广泛，软件被视为信息系统的灵魂，已经在金融、军事、交通、基础设施等领域扮演越来越重要的角色，软件安全性已经成为关系到国民经济平稳发展、社会稳定和国家安全的重要因素。本文分析了国内外软件安全性研究的现状，并对软件安全性分析的主要科学问题和当前我国的重要需求进行了剖析，提出在信息系统安全保障能力建设中，应以加强软件安全性分析能力为导向，以提高软件的安全性分析水平为目标，以软件动态分析为关键技术手段，加强软件安全性分析基础方法研究，加强信息系统安全性分析和保障的专业人才队伍建设，为保障我国信息系统安全和网络空间主权提供技术支撑。

关键词 软件动态分析，恶意代码分析，漏洞挖掘，信息系统安全

DOI：10.3969/j.issn.1000-3045.2011.03.009

应凌云博士

1 引言

随着信息技术的不断普及，软件应用已经渗透到社会生活的方方面面，从网络通讯到交通调度，从证券交易到电网控制，从武器装备到家用电器，软件在各个领域都扮演着重要的角色。因此，软件的安全和可控已经成为关系国家安全和社会稳定的重要因素。由于历史原因，我国软件产业的发展与国际领先水平还存在一定差距，国外软件产品在操作系统、数据库、工业控制系统等信息系统的关键和核心技术方面占主导地位，由于软件系统普遍应用于金融、电信、民航等具有战略意义的国民经济重要行业和国家要害部门，这些软件是否安全，其中是否存在漏洞和后门，是否可能被敌手攻击和利用，都是需要密切关注和亟需解决的问题。

2010 年爆出的“Stuxnet”蠕虫（或称之为“震网”、“超级工厂”）入侵伊朗核电站的计算机系统事件，更是凸显了软件安全问题的重要性。“Stuxnet”综合利用了微软 Windows 操作系统和西门子 WinCC SCADA 系统中的多个软件漏洞，通过复杂和巧妙的攻击过程，将恶意代码植入了伊朗核电站的控制系统，进行远程控制和破坏[1]。

* 收稿日期：2011 年 3 月 30 日

“Stuxnet”打破了人们对计算机软件安全和网络攻击的传统认识，因为“Stuxnet”感染的工业设施横跨传统计算机平台和可编程逻辑控制平台(Programmable Logic Controllers, PLCs)，而且两个平台协同工作的关系十分复杂并且难以预知，因此需要大量资金投入和高超技术支持，不是一般的蠕虫制造者可以实现的。“Stuxnet”被精心设计出来，其最终目的是入侵伊朗核电站的控制系统，寻找核心设施控制部件并破坏其关键部分，它已经不是传统的蠕虫或间谍软件，是一种直接面向现实世界中工业程序的网络攻击，已然成为软件武器，被用于攻击敌方有重要价值的基础设施。

“Stuxnet”攻击事件提醒我们，信息系统的安全不仅需要关注软件设计环节的逻辑正确性、系统应对故障的健壮性等问题，更需要重视软件实现的安全性问题。尤其是在采用进口软件等商业软件、无法完全掌控软件开发的各个环节的情况下，对软件实现的安全性进行深入分析和严格评估是确保信息系统安全的重要手段。由于目前大多数软件都无法获得源代码，并且由于分析精度和软件规模的限制，难以开展有效的静态分析，因此，软件动态分析是目前软件安全性分析所采取的主要方法。

2 国内外研究动态

根据针对的目标不同，软件实现的安全性分析方法可分为针对软件源代码的方法和针对软件可执行代码的方法。由于绝大多数商业软件、进口软件等都不提供源代码，因此，针对软件可执行代码的方法是当前最主要的软件实现安全性分析方法。而根据分析过程中是否需要运行被分析软件，针对软件可执行代码的方法又可进一步分为静态分析方法和动态分析方法两大类。

静态分析方法通过静态反编译、模型检验等技术，分析软件可能产生的执行流程和可能到达的状态，实现对软件内部机理的解析，这类方法不需要执行被分析软件，具有分析开销较小、分析过程覆盖的代码较为全面的优点。由于从软件实现中重构的软件状态模型存在状态空间爆炸问题，静态分析难以全面分析软件的各种行为，并且静态分析无法处理软件中包含的自修改代码(Self-Modifying Code)等动态生成代码。

动态分析方法通过实际执行被分析软件，利用各种方式对软件执行过程进行监控，并在软件运行过程中提取各种数据，分析软件的各种行为和内部实现逻辑。在软件实现的安全性方面，动态分析方法主要用于挖掘软件实现缺陷导致的软件漏洞，检测软件隐藏功能导致的软件后门，以及检测恶意代码攻击引起的软件运行状态异常，其中主要涉及动态执行监控、符号执行、动态污点传播分析、Fuzz 测试等方法。

(1)动态执行监控。其主要以软件调试、虚拟化等技术为基础，通过在受控环境中执行被分析软件，利用系统提供的调试接口或直接分析虚拟硬件信息，获取程序的动态执行信息。基于调试技术的动态执行监控方法主要利用操作系统和硬件提供的调试接口实现，由于调试工具需要在分析时动态修改被分析软件的二进制代码，设置特定的系统标志位等，这类利用系统和硬件的调试接口的方法往往会在系统中留下痕迹，因此分析过程容易被分析目标察觉和反制[2]。基于虚拟化的分析方式通过在系统接口或虚拟硬件的层次构建分析引擎，在硬件层次提取信息，以此为基础还原程序执行的动态过程信息，具有透明性好、适用范围广泛、分析能力强、数据准确度高的特点[3]。

(2)符号执行。其是指在不执行目标软件的前提下，采用数值或逻辑公式表示软件代码指令的操作语义，然后通过对数值及逻辑公式进行推理和求解模拟软件执行过程

实现软件分析的技术[4]。该方法可以对代码的全部语义信息进行分析，也可以只对部分语义信息进行分析。符号执行包括构建符号化描述和模拟执行求解两个过程，符号化描述的构建方法由用户经验和分析目标决定，多采用逻辑公式；模拟执行求解通过制订推理规则，在符号化描述的基础上通过求解路径条件完成。符号执行方法在理论上面临路径状态空间的爆炸问题，其根本原因是静态分析方法无法准确确定程序执行时的实际状态，需要对路径分支进行穷举，因此在动态分析过程中往往作为辅助技术配合其他方法开展分析。

(3)**动态污点传播分析**。其是一种确定软件代码中指令与指令、指令与数据之间关系的有效手段，主要包括污点源标记、传播规则制订和污点传播计算三方面的内容[5]。污点源标记即确定被监控数据的起源，该数据往往是程序中的一段内存或函数的返回值；传播规则是根据程序指令和函数的语义，结合污点源数据的特点所制订的针对污点数据处理过程的推理规则；污点传播计算是在前面两方面工作的基础上，结合动态执行监控获取的动态过程信息，展开对于污点数据处理过程的分析，确定其中指令和指令、指令和数据之间的关系。动态污点传播分析被广泛应用于恶意软件分析、攻击代码检测等软件安全性分析研究中[6]。

(4)Fuzz **分析方法**。其通过向目标软件提供按照某种规则构造的外部输入，检测软件在处理这些输入时是否发生系统异常从而发现软件错误。传统的 Fuzz 分析方法并不猜测哪个数据会导致破坏，而是使用穷举的方式生成数据，通过将尽可能多的杂乱数据投入目标软件中以期触发潜在的程序异常[7]。由于这种穷举分析方法存在较高盲目性，分析效率较低，当前的 Fuzz 分析方法往往与符号执行、动态污点传播分析等方式结合，根据已有的软件分析结果，采用一定的规则指导后续测试数据的生成过程，从而提高分析效率和准确度[8]。

软件动态分析方法主要以动态获取的目标软件的各种数据为分析基础，由于目标软件容易检测到基于软件调试的分析方法，因此在具体的实现方式上，动态分析越来越多地采用基于虚拟化的方法。目前虚拟化方法可进一步细分为基于软件实现的虚拟化、基于硬件支持的虚拟化和硬件模拟器三大类。基于软件实现的虚拟化方法通过软件转换部分虚拟环境中的特权指令，其余指令直接在真实的 CPU 上执行，因而指令的执行过程和真实环境相比存在一定的差异，容易被检测。基于硬件支持的虚拟化则利用 CPU 内置的虚拟化功能，虚拟系统中的所有指令都直接在真实的 CPU 上执行，虚拟化过程对虚拟系统完全透明，但该方式基于真实硬件，无法虚拟没有真实硬件支持的其他各种设备[9]。硬件模拟器模拟的范围包括 CPU、内存、硬盘以及光驱等外围硬件，虚拟系统中的代码在模拟 CPU 上执行，具有与真实 CPU 一样的执行过程，并且能够模拟与底层物理设备不同的虚拟设备，因而具有更好的透明性和数据获取能力[10]，这种基于硬件模拟器的软件动态分析方法也是当前国内外研究的热点。

3 软件动态分析的国家需求

软件动态分析是在软件部署之前分析软件安全性是否符合要求的重要方法，也是在软件部署后监测软件系统运行状态的主要技术，同时还是在软件安全攻击事件发生后进行应急响应和数字取证的重要手段。由于我国大量采用进口软件等非可控来源的软件，因此为了确保各种重要信息系统的安全，我国在软件分析、尤其是软件动态分析领域的需求尤为迫切，主要表现在以下几个

方面：

(1)提高我国重要信息系统安全性的需要。虽然各级政府机关、军队等重要部门在采用外来软件时有严格的规定和限制，但网络连接、移动存储等各种信息流通渠道的存在，仍然使不安全的软件导致数据泄密等危害国家安全的网络攻击事件的发生成为可能，因此，在部署各种商业软件前需要对各种软件是否存在后门等进行分析，提高重要信息系统的安全性。

其次，随着开源软件种类的不断增多，开源软件的应用也越来越多，国内大量软件产品以开源软件为基础研发。由于可以获取软件源代码，人们普遍认为开源软件更加安全，然而，开源软件并不能防止软件漏洞的产生，甚至不能避免软件后门，如2010年就爆出FBI付费给开发商在OpenBSD中的IPsec协议栈中植入后门[11]。由于OpenBSD是第一个开发出供免费使用的IPsec协议栈，随后许多开源项目和软件产品都是直接采用该代码，其造成的影响难以估计。因此，开源并不等于安全，开源软件同样需要经过深入的安全性分析才能提高信息系统的整体安全性。

最后，由于一些我国还无法自主研制的进口武器装备、工业控制系统都配备了大量进口软件、硬件，这些关键设备和要害部门所使用软件的安全性，对于国家安全至关重要，一旦敌手通过软件漏洞对装备的正常运转造成干扰，甚至通过后门控制和破坏我方装备，将对国家安全造成巨大影响。因此，对组成这些重要信息系统的软件，需要进行深入和详细的动态分析。

(2)完善互联网安全保障体系的需要。我国是互联网大国，拥有超过4亿的网民，减少恶意软件数量、降低网络攻击危害对于维护互联网安全具有重要意义，而这需要大力提升软件运行监测、网络攻击检测和恶意代码分析等软件动态分析能力。而提升软件动态分析能力是提高网络攻击防御和恶意软件检测能力的基础。

目前的网络攻击检测方法主要依赖于特征匹配，无论是基于攻击代码指纹的特征还是基于恶意软件行为的特征，都难以检测不断出现的未知攻击代码，如针对零日漏洞的攻击、恶意代码变种的攻击等。通过动态软件分析方法，可以揭开网络攻击的漏洞利用过程的细节，能够获知攻击程序针对的目标软件，定位具体的软件执行路径和漏洞所在点，同时能够揭示攻击程序如何触发漏洞，注入攻击代码，并执行恶意软件。通过动态分析软件运行状态和恶意软件攻击过程，有助于研制基于攻击过程内在特征的网络攻击检测方法。

(3)保障传统基础设施安全的需要。“Stuxnet”蠕虫针对的西门子WinCC SCADA软件主要被用做工业控制系统，被广泛地应用于输油管道、发电厂、大型通信系统、机场甚至军事设施中。类似的系统在制造业、金融业、公用事业等传统基础设施中广泛应用，传统上这些系统普遍采用物理隔离的封闭运行方式，因此其中存在的漏洞、后门带来的威胁较小，导致人们长期以来对这些信息系统软件的安全性不够重视。

随着信息系统的不断深入应用，各网络环境互联互通的需求不断增加，手段不断发展，这种封闭的单一系统模式逐渐被打破，如企业需要将地理上广泛分布的工厂通过网络相互连接，通过总部的ERP系统进行统一调度，银行需要开放越来越多的网络服务以迎合用户的需求，提供越来越多的接口以满足电子商务发展的需要，因此，这些系统已经不再完全隔离。“Stuxnet”攻击事件表明，这类专用软件系统已经成为网络攻击的

新目标，对专用软件系统的安全性分析是对传统基础设施进行安全性评估的基础，是防御“Stuxnet”等攻击事件发生的关键。

4 对我国软件动态分析领域的发展建议

通过对软件动态分析领域的发展技术现状分析，和对我国信息化建设的现实需求剖析，我们建议在软件动态分析领域重点加强以下几方面工作：

(1)**重视软件分析基础方法研究**。路径约束问题求解、控制流图分析等软件分析理论和方法是软件动态分析的基础，当前主流的软件动态分析技术，如符号执行、污点传播分析等都是传统软件分析方法的发展和延伸。加强软件分析基本理论和基础方法的研究，对促进软件动态分析研究的发展和相关方法技术的进步具有重要的支撑作用。

(2)**提高在虚拟化和硬件模拟方面的研发能力**。虚拟化技术的发展是推动软件动态分析成为当前信息安全领域热点研究方向的重要因素。利用虚拟化技术和硬件模拟方法，研究人员可以对各种平台的软件进行深入、细致的跟踪分析，从而将软件动态分析的目标推广到计算机软件之外的软件系统，极大地扩展了软件动态分析的研究范围。因此，抓住当前虚拟化技术大发展的趋势，提高不同硬件的模拟能力，对于促进软件动态分析研究的发展，推进相关技术在不同软件系统安全性分析中的应用具有重要意义。

(3)**加强新型信息系统的软件安全性分析研究的支持**。随着智能手机等新型计算设备的迅猛增加，移动互联网、物联网、三网融合等新型网络的不断发展，这些新型信息系统的软件安全性需要得到足够的重视，避免出现当前计算机软件和计算机网络安全疲于应付的现状。因此，需要加强对新型信息系统的软件安全性分析研究的支持，鼓励研究人员深入发掘新型计算设备和新型网络系统的安全需求，开展针对智能手机、传感器、智能家电等不同平台的软件安全性分析研究。

(4)**加大支持力度，加强人才队伍建设**。软件安全性动态分析是信息安全与软件工程的交叉方向，我国在这个方向的研究队伍较为薄弱，专门从事这一方向研究的人员还很少，相关研究起步较晚。建议适当加大这一方向的支持力度，注重扶持年轻研究人员开展相关研究，着重培养和建设这一方向的专业研究队伍。

(5)**促进产学研用结合，鼓励应用导向型研究**。软件动态分析可以服务于不同领域、不同类型软件的安全性保障工作，建议针对当前我国学术、产业、国防等各个方面的通用/专用软件的安全性分析需求，在科技政策方面出台促进产学研用结合的相关法规，引导和鼓励研究机构针对不同领域存在的软件分析需求，开展有针对性的软件分析方法研究，充分发挥研究型机构在方法技术研发方面的长处，同时结合企业在应用服务方面的优势，形成应用需求驱动学术研究、学术研究满足应用需求的良性循环。

主要参考文献

1 Matrosov A, Rodionov , Harley D et al. Stuxnet Under the Microscope.Revision 1.2, ESET, 2010.

2 Kiriansky V, Bruening D, Amarasinghe S P. Secure Execution via Program Shepherding.Proceedings of the 11th USENIX Security Symposium, 2002: 191-206.

3 Bayer U, Kruegel C, Kirda E. TTAnalyze: A Tool for Analyzing Malware. Proceedings of the 15th Annual Conference of the European Institute for Computer Antivirus Research, 2006.

4 Yang J, Sar C, Twohey P et al. Automatically Generating Malicious Disks using Symbolic

Execution. Proceedings of the 2006 IEEE Symposium on Security and Privacy, 2006: 243-257.

5 Newsome J , Song D. Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software. Proceedings of the Network and Distributed System Security Symposium, 2005.

6 Egele M, Kruegel C, Kirda E et al. Dynamic Spyware Analysis. Proceedings of USENIX Annual Technical Conference, 2007: 233-246.

7 Sutton M, Greene A,Amini P. Fuzzing: Brute Force Vulnerability Discovery. 2009.

8 单锦辉, 王戟, 齐治昌. 面向路径的测试数据自动生成方法述评. 电子学报, 2004, 32(1):109-113.

9 Sharif M I, Lee W, Cui W et al. Secure In-VM Monitoring Using Hardware Virtualization. Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009:477-487.

10 Song D, Brumley D, Yin H et al. BitBlaze: A New Approach to Computer Security via Binary Analysis. Proceedings of the 4th International Conference on Information Systems Security, 2008, 5352:1-25,.

11 DeRaadt T. Allegations regarding OpenBSD IPSEC. http://article.gmane.org/gmane.os.openbsd.tech/22727, 2011-03-29.

Software Dynamic Analysis for Enhancing Information System Security

Ying Lingyun Yang Yi

(State Key Laboratory of Information Security, Institute of Software, CAS 100190 Beijing)

Abstract As information system is more and more widely used and software is taken as the soul of information system, it has been playing a more and more important role in finance, military, traffic, infrastructure and other sectors, and therefore security of software becomes a key factor of social stability and national security. In this paper, the authors present a survey of the present status of the software security analysis and research in China and foreign countries, and analyze the principal scientific problems of software security analysis and the important demand of China in this field at the present time. The authors propose that the basic method study of the analysis of security of information system should be enhanced; and professional talents contingent should be constructed, so as to offer technological support for ensuring the security of information system and network space sovereign rights of China.

Keywords dynamic analysis of software, malicious code analysis, finding out vulnerability, security of information system

应凌云 中国科学院软件研究所信息安全国家重点实验室助理研究员, 工学博士, 1982年出生。目前主要从事智能手机安全、僵尸网络检测等恶意代码分析与防范相关研究。
E-mail: yly@is.iscas.ac.cn

杨 轶 男, 中国科学院软件研究所信息安全国家重点实验室助理研究员, 工学博士, 1982年出生。目前主要从事恶意代码分析、网络攻击检测以及硬件虚拟化等相关研究。
E-mail: yangyi@is.iscas.ac.cn