文章编号:1001 - 893X(2010)05 - 0099 - 05

网络信息安全综合测试与仿真验证技术*

雷 璟,王冬海

(中国电子科学研究院,北京 100041)

摘 要:提出采用信息安全模拟仿真、安全综合测试、系统级安全评估技术实现的网络信息安全综合测试与仿真验证系统的技术框架、关键技术及解决途径。此系统可对军工信息系统建设方案、安全技术、管理手段进行测试与评估。

关键词:军工信息系统;网络信息安全;综合测试;仿真验证

中图分类号:TN918;TP393.08 **文献标识码**:A doi:10.3969/j.issn.1001 - 893x.2010.05.022

Network Information Security Synthesis Test and Simulation Validation Technology

LEI Jing, *WANG Dong-hai*

(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: The technology framework, key technology and solution of network information security synthesis test and simulation validation technology system are presented, which is realized based on information security simulation, security synthesis test and system security evaluation technology. The system can test and evaluate the construction scheme, security technology, management means of military industry information system.

Key words: military industry information system; network information security; synthesis test; simulation validation

1 引 言

信息技术和信息系统的迅猛发展正在促进社会形态和战争形态的转变,推动了社会信息化和新军事变革浪潮[1]。与此同时,对信息和信息系统的非法入侵和破坏活动也正以惊人的速度在全世界蔓延,几乎达到了防不胜防的地步,信息系统正面临着前所未有的安全威胁。尤其是针对军工信息系统的攻击活动,使其面临的威胁日益严重,已经成为影响国家安全和军事安全的战略因素。

随着军工信息系统的建设规划和武器装备信息化的发展[2],一些军工大系统在信息安全总体技术研究和网络信息安全综合测试与评估方面缺乏验证手段,迫切需要验证技术手段支撑。现代科研开发和重大工程运作一般都将模拟仿真作为重要的前期验证手段,如果完全依靠真实的安全验证环境来测试验证,一方面需要投入大量的资金和设备来建立安全验证环境,实现起来有一定的难度;另一方面从技术上讲,对一些有特殊需求的安全产品和安全技术,通过真实的安全验证环境可能无法实现测试和验证。因此,通过仿真手段可达到节约资金,满足技术要求的目的。

为了解决军工信息安全技术试验验证条件不足的问题,我们实现了一个网络信息安全综合测试与仿真验证系统,即通过建立一个综合测试与评估的模拟仿真平台,对复杂的网络环境、应用环境和安全环境进行模拟,对各种攻击对抗手段进行仿真。对军工信息系统的建设方案、采用的安全技术、管理手段等方面的安全性进行测试与评估,最终形成适合

* 收稿日期:2009 - 12 - 11;修回日期:2010 - 03 - 31

军工信息系统自身特色的网络信息安全综合测试与评估管理规范,为军工信息化建设和测评提供参考、指导和示范,也可对未来的大型军工信息系统的研制提供网络信息安全支撑。

2 主要技术

网络信息安全综合测试与仿真验证系统是根据军工信息化应用的实际需求,搭建分布式的、半实物的网络信息安全模拟仿真试验环境[3],构建信息安全测试与验证综合集成平台,对信息安全技术进行验证、仿真、测试与集成。在此平台上开展多种网络渗透场景、业务场景模拟仿真,通过获取信息安全测试数据对信息系统的安全性进行系统级、一体化、自动化的综合分析与评估,从而评价验证各种安全理论模型、安全攻防手段、安全防护产品、系统级的安全体制等,利用仿真与可视化技术进行网络信息安全防护效用评估、分析与验证。同时,研制网络信息安全验证系统,对管理方面的安全性利用技术手段进行综合测试与评估,对应用信息系统的安全性进行测试与评估。

2.1 信息安全模拟仿真技术

模拟仿真技术采用半实物仿真手段实现应用业务、运行场景、网络环境等模拟仿真,并可实现与实物系统的信息与行为的交互。

随着面向服务架构和虚拟计算基础设施的出现和应用,军工信息系统网络环境、应用环境和安全环境变得相当复杂,构建一个同目标网络完全一致的真实网络环境周期长、成本高、难拓展、难调整;而采用全部由仿真方法来评估现有网络时,仿真网络与目标网络的差异性会对评估结果准确性产生影响。因此,采用虚实结合的半实物仿真方式,在模拟仿真中引入真实设备并导入部分真实流量,可以更快捷、更真实地对网络环境进行模拟。

搭建由仿真模型和实物组成的安全模拟仿真环境,通过仿真网络基础平台、部分安全防护功能仿真模块以及实物中的安全功能样机构建完整的安全防护体系,为仿真业务数据及导入的真实的业务数据流提供运行环境。同时,该仿真网络环境可以作为相关的网络渗透、综合测试及系统级评估的对象。

2.2 安全综合测试技术

安全综合测试技术是在测试知识库的支持下,可以合理地集成相关测试方法或技术到系统测试过程,生成参考测试方案;提供测试方法的最优选择组合,分析测试数据;同时结合历史经验,为测试活动调整和测试评估等提供定量决策依据;获取并保存有用的测试经验与知识。

通过安全综合测试技术可以提高管理部门的技术检测水平和能力,也可以提高第三方检测机构对军工信息系统安全性进行综合测试的现场检测效率。

2.3 系统级安全评估技术

系统级安全评估技术是在现有安全评估标准基础上,分析目标信息系统中各子系统、设备、策略和措施等组成要素相互之间及其与系统整体安全性之间的复杂关系,提炼总结出系统级安全评估指标体系,将安全性分解、落实到子系统、设备一级;建立系统级安全评估知识库及推理机制,通过子系统/设备安全相关参数发现系统的脆弱性并给出相应的解决方法。

此项技术的实现需要构建安全评估模型[4],建立一套既可以反映系统整体,又可以落实到具体设备/子系统的系统级的信息安全评估指标体系,建立系统级安全评估知识库。

3 系统组成

本文提出的网络信息安全综合测试与仿真验证系统组成图如图 1 所示。

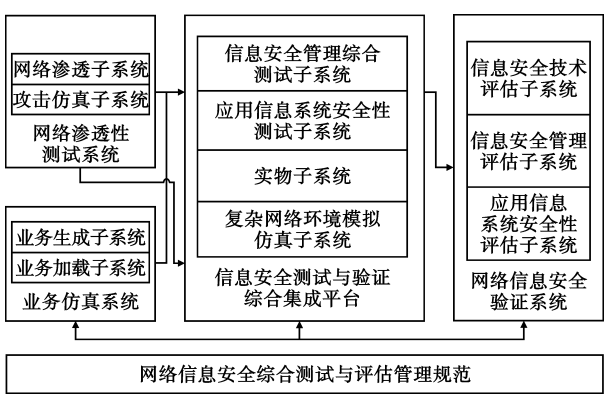

图 1 网络信息安全综合测试与仿真验证系统组成图

Fig.1 The composition of network information security synthesis test and simulation validation system

按照系统功能,系统可分为信息安全测试与验证综合集成平台、网络渗透性测试系统、业务仿真系统、网络信息安全验证系统四大组成部分。

信息安全测试与验证综合集成平台由信息安全管理综合测试子系统、应用信息系统安全性测试子系统、实物子系统、复杂网络环境模拟仿真子系统组成。此平台主要完成对复杂网络环境的模拟仿真,对管理因素和应用信息系统的安全性提供测试手段和集成平台。

网络渗透性测试系统由网络渗透子系统、攻击仿真子系统组成。此系统通过网络渗透性测试和攻击仿真手段来验证信息安全测试与验证综合集成平台的安全性。

业务仿真系统由业务生成子系统和业务加载子系统组成。业务生成子系统负责将实际业务抽象成仿真系统所需的业务背景,通过业务加载子系统将业务想定按照时间序列、动态地加载到仿真系统中。

网络信息安全验证系统由信息安全技术评估子系统、信息安全管理评估子系统、应用信息系统安全性评估子系统组成。此系统主要从技术、管理、应用角度完成对信息安全测试与验证综合集成平台的验证评估,并根据评估结果给出安全解决方案。

4　关键技术及解决途径

网络信息安全综合测试与仿真验证系统采用了以下关键技术,如图 2 所示。

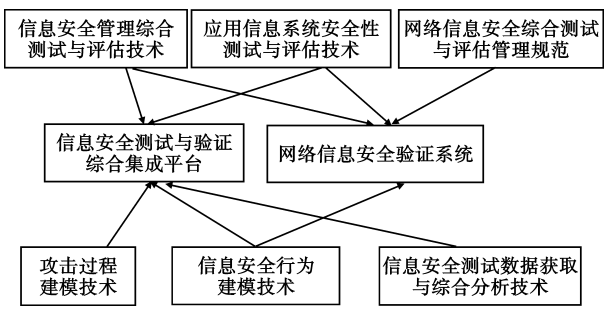

图 2　网络信息安全综合测试与仿真验证关键技术组成图
Fig.2 The key technologies composition of network information security synthesis test and simulation validation

4.1　攻击过程建模技术

攻击过程具有对应不同环境、不同后续反应而有多维度变化的特性,且行为之间也会有相互作用,准确描述此种变化对仿真可信度有很大影响。

攻击过程建模利用基于 HLA 的分布式代理灵活地把攻击加载到系统的内部或者外部,可以相应实现内部的攻击或者是外部的主动攻击。同时,对攻击的过程进行建模,在进行攻击仿真时,一般先将攻击进行分类,然后选择每种类别中典型的攻击方法进行仿真试验。选择好攻击类型后,在仿真时根据攻击的步骤进行仿真。在构造攻击数据时还要注意新式攻击、隐秘方式的攻击[5]、并行攻击等方面,因为相对于旧式攻击、显式攻击以及串行攻击而言,这些攻击方式能更好地检验信息系统的安全性,对测试评估结果有更大的影响。

4.2　信息安全行为建模技术

信息安全行为是测试系统脆弱性和风险的重要手段,其影响结果是安全评估的重要依据,目前还没有针对信息安全行为进行建模仿真的成熟技术。

信息安全行为建模在理论层面深入研究仿真建模的方法和技术,特别运用系统科学及复杂性研究方面的成果,从系统级对网络环境中的信息安全行为要素及信息安全保障要素进行数据模型构建和建模技术研究,形成高可信度的信息安全行为要素及信息安全保障要素数学模型。以理论研究成果为基础,基于构建的相关数学模型,提供信息安全正常行为仿真模型、信息安全异常行为仿真模型和安全保密设备仿真模型,为整体的系统仿真环境提供信息安全行为及信息安全保障要素模型。

4.3　信息安全测试数据获取与综合分析技术

研究如何快速、准确地获取所需要的各种信息安全数据,研究将基于内部网络协议直接从军工信息化网上采集或下载信息的信息采集方式与策略,实现高效、准确地从网络、通信传输收集数据,为后续信息综合分析、处理提供数据和素材。

各种信息安全测试产生的大量记录和系统参数数据不便于分析,因而需要将信息安全测试效果进行可视化显示,提供更为直观的统计趋势图、系统受渗透后系统自身状态变化趋势图和系统关联状态变化图等图表进行可视化显示。

4.4　信息安全管理综合测试与评估技术

由于管理部门对用户部门的信息安全保密监管技术难度大、操作复杂、缺少有效的技术手段,为此需研发灵活多变、操作简单的信息安全检查、综合测试与评估管理系统,以提高管理部门的技术检测手段。

技术解决途径是针对信息系统主要涉及需要保护的资产,各单位对于信息系统管理的手段、管理目标和管理方法,以及所需要的保障程度构建的信息安全管理系统开展漏洞检查、综合测试与评估技术

的相关研究。研发一套信息安全管理综合测试与评估系统从物理安全、运行安全、信息安全保密等方面自动化地启用一些网络安全漏洞扫描工具、计算机终端保密检查工具、电磁泄漏发射防护检测工具、其它专用检测工具等对信息系统安全进行综合测试与评估,提高现场检测的效率。

4.5 应用信息系统安全性测试与评估技术

此项关键技术重点针对基于 Web 应用系统的安全性检测与评估。军工信息系统包含多种 Web 应用系统,Web 应用系统上承载了各种涉密信息,因此 Web 应用系统的安全保密性直接决定整个军工信息系统的安全保密性,而对 Web 应用系统进行全方位的安全性检测与评估是保障 Web 应用系统安全性的重要手段之一。

技术解决途径将从 Web 应用程序、部署具体 Web 应用程序的 Web 容器和提供 Web 服务的服务器主机等 3 个方面研究 Web 应用系统面临的安全漏洞,搭建 Web 应用程序安全威胁模型、Web 容器安全威胁模型、服务器主机安全威胁模型,并针对这些安全漏洞进行 Web 应用程序渗透入侵、Web 容器渗透入侵、服务器主机渗透入侵,深层次地检测与评估 Web 应用系统的安全性。

4.6 网络信息安全综合测试与评估管理规范

此项关键技术通过搭建的信息安全测试与验证综合集成平台,对军工信息系统网络环境、应用环境和安全环境等进行全方位的模拟、综合测试与评估,形成适合军工信息系统自身特色的网络信息安全综合测试与评估管理规范,建立军工信息化网络信息安全保障支撑能力。

5 技术应用示范

网络信息安全综合测试与仿真验证系统可以将军工信息化网络作为演示验证示范平台,应用示范框架如图 3 所示。其中,信息安全仿真平台针对军工信息化网的典型应用业务、运行场景进行模拟仿真,并采用半实物仿真手段,实现与实物系统的信息、行为交互。信息安全综合测试平台通过完善、集成现有的测试手段,对目标系统展开综合测试,为系统层级的评估提供数据支撑。系统级安全评估系统以仿真验证和测试集成为基础,从系统层级对军工信息化网的整体防护效能进行评价,并发现其中的脆弱点,提出改进建议。

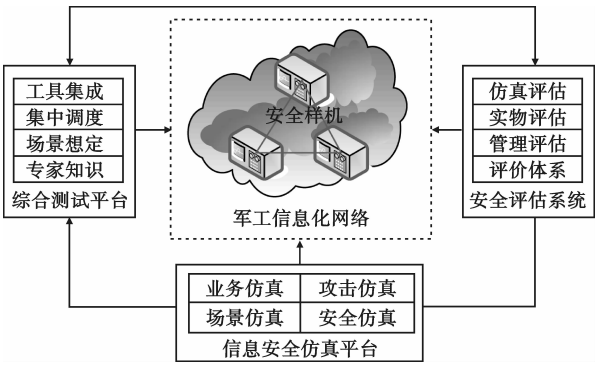

图 3 网络信息安全综合测试与仿真验证系统应用示范图

Fig.3 The application demonstration of network information security synthesis test and simulation validation system

网络信息安全综合测试与仿真验证技术具有以下应用示范性:

(1)搭建信息安全仿真平台,为军工信息系统安全防护效能评价提供仿真手段和决策支撑。针对军工信息系统安全防护效果的测试、评估、验证需求,运用模拟仿真技术,对安全环境、安全行为等进行仿真,搭建信息安全仿真平台,提升信息系统的安全防护水平,为军工信息系统安全防护效能评价提供仿真手段和决策支撑;

(2)提供自动化的综合测试手段,提升军工信息系统安全测试的科学性和效率。通过集成各种安全保密测试技术、工具,提供自动化的综合测试手段,可以解决测试工具相互独立、效率低,结果主观性强、不够科学,安全保密测试技术、工具分散,评估结果不具可比性,难以形成一致的综合结果的问题,提升军工信息系统安全测试的科学性和效率;

(3)建立评估指标体系,提升军工信息系统安全防护效用的评价水平和能力。构建系统级安全评估指标体系,开发数据采集、安全评估软件,从技术、管理、应用信息系统安全方面进行综合评估,提高安全评估结论的客观性和可信性。从系统层级提升军工信息系统整体安全防护效用的评价水平和能力;

(4)建设网络安全攻防演练靶场,提高网络安全攻防能力。通过网络信息安全综合测试与仿真验证系统建设网络安全攻防演练靶场,模拟实战环境,进行对抗进攻与对抗防御的有效演练[6],提高网络安全攻防能力,是十分必要的。例如,美国国防部为了提高自身信息安全保障与攻击水平,于 2008 年斥巨资建造了“国家网络靶场”系统,进行信息安全攻防作战模拟仿真,以实现网络攻击能力的重大突破。

6　结束语

通过网络信息安全综合测试与仿真验证技术研究而构建的网络信息安全测试与仿真验证系统,能够为安全产品和系统的测试评估提供良好的仿真环境、信息安全测试与验证综合集成平台,可用于开展技术验证、方案推演、测试技术效果分析、被测系统模拟等。同时,又能够为信息安全新技术的研发提供支撑平台,带动我国信息安全模拟仿真技术的发展,提升我国信息安全技术研发水平,并通过多个网络安全靶场的建设,最终互联形成国家信息安全靶场,成为我国信息安全技术研发的关键基础设施,为我国信息安全技术的发展提供有效支撑。

参考文献:

[1] 蔡红柳,何新华.信息安全技术及应用实验[M].北京:科学出版社,2004:50 – 51.
CAI Hong-liu, HE Xin-hua. Information security technology and application test[M]. Beijing: Science Press, 2004:50 – 51.(in Chinese)

[2] 吴伟仁.军工制造业数字化[M].北京:原子能出版社,2005:65 – 66.
WU Wei-ren. The Digitalization Technology of Military Industrial Manufacturing Enterprises[M]. Beijing: Atomic Energy Press, 2005:65 – 66. (in Chinese)

[3] 张锰.分布式交互仿真中的网络安全平台的设计与实现[J].计算机应用,2002,22(2):91 – 92.
ZHANG Meng. The Design and Implementation of a Network Security Platform in Distributed Interactive Simulation [J]. Computer Applications, 2002, 22(2):91 – 92. (in Chinese)

[4] 刘恒,吕述望.基于模型的安全风险评估方法[J].计算机工程,2005,31(9):159 – 162.
LIU Heng, LV Shu-wang. Research in the Models of the Security Risk Assessment Technology [J]. Computer Engineering, 2005, 31(9):159 – 162. (in Chinese)

[5] 周海刚,刘军,肖军模.网络反攻击技术的研究[C]//网络安全体系结构高级研讨班论文集.武汉:中国电子学会教育工作委员会,2001:250 – 254.
ZHOU Hai-gang, LIU Jun, XIAO Jun-mo. Research on network Anti-attack technologies[C]//Proceedings of High-level Seminar on Network Security Framework. Wuhan: Chinese Institute of Electronic Commission of Education, 2001: 250 – 254. (in Chinese)

[6] 李广文.强意识,抓防护,全面提高网络攻防能力[C]//网络安全体系结构高级研讨班论文集.武汉:中国电子学会教育工作委员会,2001:301 – 304.
LI Guang-wen. Strong consciousness, snatch at defense, improve the ability of network attack and defense entirely[C]// Proceedings of high-level seminar on network security framework. Wuhan: Chinese Institute of Electronic Commission of Education, 2001:301 – 304. (in Chinese)

作者简介:

雷　璟(1977 –),女,湖北武汉人,2003 年于华中科技大学计算机应用技术专业获工学硕士学位,现为工程师,主要研究方向为信息安全、信息网络安全建设、网络安全仿真评估;

LEI Jing (female) was born in Wuhan, Hubei Province, in 1977. She received the M.S. degree in Huazhong University of Science and Technology in 2003. She is now an engineer with the M.S. degree. Her research interests include information security, information network security construction, network security simulation and evaluation.

Email: leijanet@163.com

王冬海(1968 –),男,北京人,高级工程师, 主要研究方向为仿真技术、网络安全、系统集成、测试评估。

WANG Dong-hai(male) was born in Beijing, in 1968. He is now a senior engineer. His research interests include simulation technology, network security, system integration, test and evaluation.