大规模分布式系统脆弱性分析框架研究

况晓辉 赵 刚 温 研 许 飞 苗 青
(信息系统安全技术重点实验室 北京 100101) (北京系统工程研究所 北京 100101)

摘 要 随着大规模分布式系统在国家安全、经济运行、基础设施、社会生活等方面扮演的角色越来越重要,其脆弱性分析问题日益成为人们关注的焦点。将大规模分布式系统视为脆弱性分析对象,构建了大规模分布式系统的层次模型,分析了大规模分布式系统的脆弱性类型,提出了基于生命周期的多维度的大规模分布式系统脆弱性分析框架,从脆弱性分析阶段、生命周期以及脆弱性类型等方面系统地梳理了研究方向。

关键词 大规模分布式系统,脆弱性分析,生命周期
中图法分类号 TP393 **文献标识码** A

Research on Vulnerability Analysis Framework for Large-scale Distributed System

KUANG Xiao-hui ZHAO Gang WEN Yan XU Fei MIAO Qing
(Science and Technology on Information System Security Laboratory, Beijing 100101, China)
(Beijing Institute of System and Engineering, Beijing 100101, China)

Abstract As the large-scale distributed system plays an increasingly important role in such fields of national security, critical infrastructure and social life, its vulnerability analysis has become a growing focus nowadays. Regarding it as a vulnerability analysis object, a multi-layer model for large-scale distributed system was put forward first, and then a multi-dimension vulnerability analysis framework was proposed, which provided an overview of vulnerability analysis research area and method in three aspects, including vulnerability analysis phase, lifecycle process and taxonomy of vulnerability.

Keywords LDS, Vulnerability analysis, Lifecycle process

1 前言

大规模分布式系统(Large-Scale Distributed System, LDS)由广域部署的众多实体构成,它将高速互联网、计算机、数据库和应用软件融为一体,显著提高了资源共享和协同能力,在商业、军事和政府等领域的应用日益广泛,逐渐成为重要的关键信息基础设施[1],典型系统有网格、P2P系统、域名系统、GIG以及云设施等。由于LDS特有的广域分布、异构、层叠、动态以及无法集中监控等特点,其安全性面临严峻的挑战。

针对LDS的安全问题,最初的研究主要集中在其安全体系结构和传统安全机制方面,取得了大量成果。尽管如此,针对LDS的安全事件仍然不断出现[2],使人们意识到上述工作并不能保证系统的安全性,需要从攻击者的角度对LDS进行脆弱性分析,以发现在设计、实现和配置运行等方面可能存在的安全隐患,从而提出有针对性的解决措施。Andre L. Nash[3]分析了各类常见的针对P2P系统的攻击方式,包括文件注毒攻击、拒绝服务攻击、恶意代码攻击、身份标识攻击、垃圾信息攻击等,讨论了这些攻击的危害与形成原因,并初步探讨了其可能存在的防御方式。Baptiste Pretre[4]重点分析了4类P2P网络的攻击方式,即理性攻击、Eclipse攻击、女巫攻击和文件注毒攻击,讨论了可能的安全防范机制。Seung-Taek Park等人[5]从理论角度分析了Internet的脆弱性模型。Mudhakar Srivatsa等[6]分析了基于DHT的层叠网的脆弱性,重点研究了针对该类型网络的路由表与身份标识映射机制的攻击,并定量分析了这两类攻击的危害,探讨了可能采取的防御机制。同时,他们分析了这两类脆弱性对基于DHT的P2P网络可能造成的危害与相应的安全防范机制。Marling Engle和Javed I. Khan[7]从网络通信层、系统层和P2P应用层3个层面分析了P2P系统的脆弱性,讨论了针对这3个层次脆弱性的各种攻击方式,重点分析了理性攻击、女巫攻击、Eclipse攻击的攻击原理,并分析了目前针对这3种攻击可能的解决方案。Li Baiyan等人[8]通过形式化分析的方法,分析了网格安全基础设施(GSI)安全机制(包括认证、验证等)的有效性。Y. Demchenko等人[9]基于已有的安全脆弱性模型和分类对网格的脆弱性进行分析,提出了Web服务和网格相互作用的一个基础的安全模型,在基础Web服务中引入安全区的概念,以定位应用层的安全事件。Syed Naqvi等

到稿日期:2011-07-13 返修日期:2011-09-29
况晓辉(1975—),男,博士,副研究员,主要研究方向为计算机网络、信息安全;赵 刚(1969—),男,博士,研究员,主要研究方向为计算机网络、信息安全;温 研(1980—),男,博士,助理研究员,主要研究方向为信息安全、虚拟化技术;许 飞(1981—),男,硕士,助理研究员,主要研究方向为计算机网络,E-mail:xufei1023@126.com;苗 青(1970—),女,硕士,助理研究员,主要研究方向为信息安全。

人[10]对多种网格脆弱性模型进行了分析，提出了一种较为系统的威胁模型，把网格专有的威胁分为3大类：非重要数据和应用的威胁、重要数据和应用的威胁、来自网格资源自身的威胁。Lim H-W等人[11]对Globus Toolkit网格的传输层和应用层的GSI安全服务进行了脆弱性分析，指出其存在着证书的短期有效、可扩展性差等不足，提出了用户友好的网格安全架构和协议。Gui Xiao-lin等人[12]在建立安全架构的同时，从用户层、资源层、应用层、网络层等4个层次进行了网格脆弱性分析。Lieven Desmet等人[16]从Web服务模型分层的角度对Web服务脆弱性进行了分析，并给出了应对措施。Lai J-Y等人[17]从基于HTTP方法的Web攻击角度对Web服务的脆弱性进行了研究。Parrend等人[18]通过分析从基于组件到面向服务的各类软件系统，创建了Java脆弱性分类。N. Gruschka等人[19]研究了SOAP通信层的脆弱性。Yu等人[20]研究了基于SOAP的Web服务软件的脆弱性。Lutz Lowis等人[21]分析了传统的脆弱性和Web服务的脆弱性对SOA体制安全性的影响，指出了在BPEL和SOAP实现中可能出现的脆弱性，提出了针对SOA特有脆弱性的攻击手段。

已有的研究工作主要针对P2P、网格等特定LDS系统的具体脆弱性类型，未从将LDS作为通用的系统开展脆弱性分析，研究工作的系统性不强，研究进展缺乏普适性。针对上述问题，本文首先构建了LDS的层次模型，提出了LDS的脆弱性类型，并在此基础上提出了多维度的LDS脆弱性分析框架，为后续研究工作的开展奠定了基础。

2 LDS层次模型

LDS是指通过广域部署在大量独立计算机上的组件，它将高速网络、计算机、数据库和应用软件融为一体，以底层透明和位置无关的方式为用户提供服务。LDS的体系结构可用4层模型来描述，如图1所示。

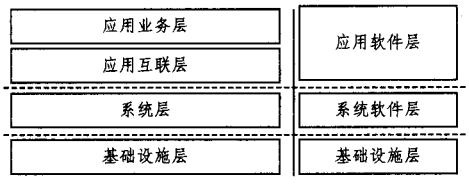

图1 LDS 4层体系结构模型

图中，基础设施层指构建LDS的网络和硬件平台，它屏蔽了物理网络的异构性，为系统层提供了统一的、基于TCP/IP协议栈的网络通信服务；系统层包括各类系统软件，主要是各类型的操作系统，为上层应用构建了统一的计算资源与网络通信的平台；应用互联层基于系统层提供了复杂多样的计算与通信接口，屏蔽了下层基础设施的异构性，为应用业务层提供了统一的定位和互联服务；应用业务层为终端用户提供了业务相关的各种功能，如资源、信息、服务的共享和交换等。

3 LDS脆弱性分类

LDS是一个动态、复杂的系统，其脆弱性分析面临特有的挑战。从广义上看，LDS脆弱性分析范畴涵盖图1的各个层次。然而，网络协议脆弱性分析、OS脆弱性分析以及软件脆弱性分析等领域已经进行了大量的深入研究。为聚焦LDS脆弱性分析的独特问题，限定LDS脆弱性分析包括以下3方面，即针对LDS实体广域分布、动态性、涌现性和体系结构的层叠性等特点，研究LDS系统性、整体性的脆弱性问题；针对LDS缺乏集中统一的管理和协作性等特点，研究广域分布的实体中应用互联层和应用业务层在交互过程中存在的脆弱性；针对LDS异构性、协作性等特点，分析应用互联层和应用业务层软件在设计、实现过程中引入的脆弱性。

已有的脆弱性分类法主要从脆弱性产生的根源、利用脆弱性造成的威胁、利用脆弱性的方法、引入脆弱性的阶段、脆弱性产生的位置等角度对操作系统、软件的脆弱性进行分类，尚未形成通用的、广泛适用的分类，因此难以直接应用到LDS脆弱性研究中。借鉴基于位置的脆弱性分类思想，从LDS层次结构的角度，可将LDS脆弱性分为结构脆弱性、交互脆弱性和组件脆弱性3类。

• 结构脆弱性

结构脆弱性是指LDS系统设计和应用过程中，组件间的拓扑结构以及各层次依赖关系的缺陷导致的脆弱性。它仅与实体间的依赖关系以及层次特性有关，不涉及具体的业务功能、安全机制等，如实体拓扑结构脆弱性、网络拓扑结构脆弱性等。

• 交互脆弱性

交互脆弱性指LDS系统中实体交互过程中存在的缺陷导致的脆弱性。它存在于应用互联层和应用业务层，缺陷包括应用层协议脆弱性、安全机制缺失导致的脆弱性等。如P2P系统中对节点互联缺乏有效的管理、认证等安全机制，导致女巫攻击、Eclipse攻击等可以破坏其可用性，这就属于因安全机制缺失而引入的交互脆弱性。

• 组件脆弱性

组件脆弱性指LDS应用互联层和应用业务层软件的脆弱性。组件脆弱性为软件脆弱性的子类，包括跨站脚本漏洞、SQL注入漏洞、缓冲区溢出漏洞、整数溢出漏洞等。

4 多维度LDS脆弱性分析框架

为了发现系统中潜在的、已知或未知的漏洞，在LDS脆弱性分类的基础上，提出多维度LDS脆弱性分析框架，如图2所示。

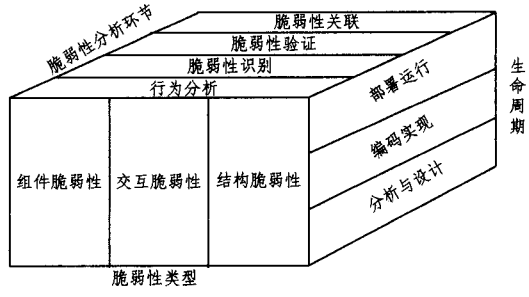

图2 LDS脆弱性分析框架

本脆弱性分析框架从脆弱性分析环节、脆弱性类型和LDS生命周期3个维度构建。

• 脆弱性分析环节

脆弱性分析环节确定脆弱性分析的基本流程，包括行为分析、脆弱性识别、脆弱性验证和关联分析4个步骤。

在LDS脆弱性分析环节的4个阶段中，行为分析阶段的

任务是获得 LDS 的组件特性、组件间依赖关系、运行流程、安全机制等信息，为后续步骤奠定基础；脆弱性识别阶段的目的是寻找已知或未知的脆弱性；脆弱性验证的目的是检测可利用的脆弱性在 LDS 中是否存在；脆弱性关联分析的目的是确定已知脆弱性被各类攻击方法利用的次序关系。4 个阶段相互关联，形成目标对象分析、脆弱性识别、验证和关联分析的完整流程。每个阶段的主要任务不同，需研究解决的问题也存在较大差异。

• 脆弱性类型

LDS 脆弱性类型界定了脆弱性分析对象的范畴。在 LDS 脆弱性分析框架中，脆弱性类型包括组件脆弱性、交互脆弱性和结构脆弱性 3 种类型。

LDS 的脆弱性分类对于分析方法具有较大的影响。LDS 脆弱性分析框架采用基于 LDS 层次结构的脆弱性分类方法，可指导脆弱性分析流程从宏观整体结构到微观实现细节，逐层全面分析 LDS 的脆弱性；同时，该分类方法将 LDS 分割为组件、交互和结构(整体)3 个相对独立的脆弱性分析对象，每类分析对象具有自身的特点，可聚焦脆弱性分析问题，研究特定类型脆弱性的分析方法；此外，引入组件脆弱性类型可将 LDS 的脆弱性分析和传统的软件脆弱性分析有机地结合起来，使组件的脆弱性分析技术可在已有软件脆弱性分析研究的基础上展开。

• 生命周期

LDS 在系统生命周期的每个阶段都可能引入脆弱性。在分析与设计、编码实现和部署运行等生命周期的各个阶段，脆弱性分析环境和条件存在较大差异，对脆弱性分析的方法和重点具有较大影响，因此在分析框架中引入生命周期维度，并将生命周期分为分析与设计、编码实现和部署运行 3 个阶段。

结束语 LDS 在国家安全、经济运行、基础设施、社会生活等方面扮演着越来越重要的角色。然而，LDS 的规模性、异构性、动态性、层叠性以及跨域性等特点，使其脆弱性分析技术面临新的挑战。本文把 LDS 作为一类专门的对象，在系统梳理已有研究工作的基础上，提出了多维度的 LDS 脆弱性分析框架，为后续研究工作的展开奠定了基础。

参 考 文 献

[1] Tanenbaum A S, Steen M V. 分布式系统原理与范型(第二版)[M]. 北京：清华大学出版社，2008：1-22

[2] CERT. CERT Statistics [R/OL]. http://www.cert.org/stats/cert_stats.html, 2009-09-06

[3] Andre L N. Attacking P2P Networks[J/OL]. http://wwwcsif.cs.ucdavis.edu/~nash/235/attacking_p2p_networks.pdf, 2010-08-24

[4] Pretre B. Attacks on Peer-to-Peer Networks[D]. Zurich: Swiss Federal Institute of Technology(ETH), 2005

[5] Park S-T. Static and Dynamic Analysis of the Internet's Susceptibility to Faults and Attacks[C]// Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, 2003, 3: 2144-2154

[6] Srivatsa M, Liu L. Vulnerabilities and Security Threats in Structured Overlay Networks: A Quantitative Analysis[C]// 20th Annual Computer Security Applications Conference(ACSAC). 2004: 252-261

[7] Engle M, Khan J. Vulnerabilities of P2P Systems and a Critical Look at their Solutions[R]. Kent: Department of Computer Science, Kent State University, 2006

[8] Gymnopoulos L, Dritsas S, Gritzalis S, et al. GRID Security Review [J]. Springer Lecture Notes in Computer Scien-ce, 2003, 2776: 100-111

[9] Demchenko Y, Gommans L, de Laat C, et al. Web Services and Grid Security Vulnerabilities and Threats Analysis and Model [C]// Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing. Washington: IEEE, 2005: 262-267

[10] Naqviand S, Riguidel M. Threat Model for Grid Security Services[J]. Lecture Notes in Computer Science, 2006, 3470: 1048-1055

[11] Lim H W, Lim H W, Mao Wen-bo. User-friendly Grid Security Architecture and Protocols[J]. Lecture Notes in Computer Science, 2007, 4631: 157-161

[12] Gui Xiao-lin, Xie Bing, Li Yi-nan, et al. A Grid Security Infrastructure Based on Behaviors and Trusts: GCC 2004 Workshop [C]// International Workshop on Information Security and Survivability for Grid. Berlin: Springer Berlin, 2004, 3252: 482-489

[13] Deubler M, Grünbauer J, Jürjens J, et al. Development of Secure Service-based Systems[C]// International Conference on Service Oriented Computing. New York: ACM Press, 2004: 115-124

[14] Bhargavan K, Fournet C, Gordon A D. Verifying policy-based security for web services[C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. New York: ACM Press, 2004: 268-277

[15] Nakamural Y, Satol F, Chung H-V. Syntactic Validation of Web Services Security Policies[J]. Lecture Notes in Computer Science, 2007, 4749: 319-329

[16] Desmet L, Jacobs B, Piessens F, et al. Threat Modeling for Web Services Based Web Applications[J]. IFIP International Federation for Information Processing, 2005, 175: 131-144

[17] Lai J-Y, Wu J-S, Chen S-J, et al. Research on Proposal Taxonomy of Web Attacks[C/OL]. http://security.nknu.edu.tw/psnl/publications/2009/10_LAI, JUNG-YING/JWIS2008.pdf, 2010-02-11

[18] Parrend P, Fr′enot S. Classification of Component Vulnerabilities in Java Service Oriented Programming(SOP) Platforms[C]// Conference on Component-based Software Engineering(CBSE'2008). Berlin: Springer Berlin, 2008, 5282: 80-96

[19] Jensen, Gruschka M, Herkenhoner N, et al. SOA and Web Services: New Technologies, New Standards-New Attacks[C]// Proceedings of the Fifth European Conference on Web Services. Germany: ECOWS, 2007: 35-44

[20] Yu W D, Aravind D, Supthaweesuk P. Software Vulnerability Analysis for Web Services Software Systems[C]// Proceedings of the 11th IEEE Symposium on Computers and Communications. ISCC, 2006: 740-748

[21] Lowis L. Towards Automated Risk Identification in Service-oriented Architectures[C]// Proceedings of the Multikonferenz Wirtschaftsinformatik(MKWI). 2008: 253-254