信息安全

漏洞分析基础

吴世忠 刘 晖
郭 涛 易 锦 著

科学出版社

信息安全漏洞分析基础

吴世忠　刘　晖
郭　涛　易　锦　著

科学出版社
北　京

内 容 简 介

本书共分三部分，第1部分为理论篇，主要介绍漏洞分析理论研究基础，内容包括漏洞的定义及产生、漏洞的状态及预测、漏洞的发展等；第2部分为方法技术篇，主要介绍漏洞分析的工作内容及方法，内容包括漏洞发现、漏洞发布、漏洞修复、漏洞预防；第3部分为管理篇，主要介绍漏洞分析管理工作的机制、模式及手段，从法律法规、基础设施、市场等方面，总结国内外漏洞分析管理工作的现状及存在的问题，并对漏洞市场的管理方式进行了有益的探索，最后从漏洞标识、漏洞补丁、漏洞信息等几方面总结和分析了国内外漏洞管理标准规范并提出了漏洞分析的准则框架。

本书可作为信息安全从业人员、黑客技术发烧友的参考指南，也可作为信息安全专业的研究生或本科生的指导用书。

图书在版编目(CIP)数据

信息安全漏洞分析基础/吴世忠等著. —北京：科学出版社，2013.4

ISBN 978-7-03-036832-4

Ⅰ.信… Ⅱ.吴… Ⅲ.①计算机网络-管理 ②计算机网络-安全技术 Ⅳ.TP393.07

中国版本图书馆CIP数据核字(2013)第039693号

责任编辑：杨 凯 / 责任制作：董立颖 魏 谨

责任印制：赵德静 / 封面制作：周 杰

北京东方科龙图文有限公司 制作

http://www.okbook.com.cn

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京佳艺恒彩印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2013年4月第 一 版 开本：B5(720×1000)

2013年4月第一次印刷 印张：21

字数：410 000

定 价：59.00元

(如有印装质量问题，我社负责调换)

序

在当前国内外日益严峻的信息安全大环境下，作为我国信息安全保障体系建设的基础性环节，漏洞分析工作在国家相关部门的大力支持下，持续稳步推进；在各行各业的共同努力和专业技术部门的有力支撑下，针对漏洞隐患的分析掌控能力以及面向重要信息系统威胁风险的应对能力得到了大幅提升；在学术界和产业界的共同努力下，漏洞分析的理论研究、产品工具研制以及服务体系正不断趋于完善。

信息安全漏洞分析是一项战略性很强的工作，同时也是极具挑战性和对抗性的艰巨工作。发达国家对此高度重视，在近年大国网络安全战略调整中，均把它作为战略级任务予以强调。国内的情况是，尽管经过几年的探索和尝试，在基础理论、技术工具、挖掘评估以及标准规范等方面积累了一定的经验和方法，但较之于急速发展的网络化时代和日趋严峻的信息安全形势，漏洞分析工作还需要提高认识和定位，还有待突破和创新。因此希望本书能为我国信息安全漏洞分析工作贡献一份微薄之力，抛砖引玉，吸引更多力量参与到这项工作中来，以助于增强我国信息安全保障的理论建构和实战能力。

1. 漏洞分析工作的意义

近几年来，国内外银行、购物、社交和游戏等网站，由于 SQL 注入、跨站脚本等漏洞被黑客入侵，导致数亿用户资料外泄和近亿美元的财产损失。2011 年，网络数据泄露事件呈现高发态势，成为网络生活的热点问题和信息安全的重大现实威胁。例如，HBGary Federal 公司数据库泄露，导致 6000 封机密电子邮件、公司主管社交媒体账户和客户信息泄露；SONY 公司数据库泄露，导致 1 亿客户的详细资料和 122 万个未加密信用卡号码泄露；中国最大的程序员社区 CSDN 数据库泄露，导致 600 万用户资料公开；广东出入境政务网数据库泄露，导致 400 万出入境人员相关信息泄露。如果说上述“泄密门”事件是黑客组织利用漏洞对网站发起的“软攻击”，那么 2011 年年底利用 4 个 0-day 漏洞的“震网”病毒事件，则是针对核设施、电力、通信、交通等重要基础设施发起的“硬摧毁”。该病毒直接针对德国西门子公司设计制造的计算机控制系统，导致伊朗核电站的部分离心机停止工作。针对伊朗核电站的攻击烟云未消，2012 年 4 月，综合利用了多个已知漏洞的“火焰”病毒，再次感染了中东地区的大量电脑。该病毒是迄今为止发现的最复杂的病毒，代码量达到了 65 万行，计算机一旦被“火焰”感染，就会被安装特定的任务模块，包括捕

捉键盘敲击、窃取密码、删除硬盘数据、窃听网络电话和聊天内容，甚至利用蓝牙功能窃取与电脑连接的智能手机、平板电脑中的内容，可以说“火焰”就是一个完整的网络情报收集系统。由此可见，漏洞不仅是网络安全事件的触发点，更是制造网络战新武器的要件。因此漏洞是网络战攻守双方的关注焦点和争夺对象，作为一种战略资源而受到格外关注。

传统的“黑客精神”正在被“利益驱动”所替代。早期的黑客发现漏洞或攻击服务器，其目的多出于兴趣、好奇、挑战心理或是对技术的钻研精神。而现在的黑客行为或网络安全事件的发生正越来越多地受利益驱动。首先，未公开漏洞成为一种商品。黑客通过技术手段发现漏洞之后，不再像以前一样报告安全组织，而是通过各种途径出卖，漏洞的价格也因其重要程度而价码攀升，少则几千元，多则几十万元。其次，漏洞利用代码等恶意程序成为多人参与、分工明确、快速完善的工业化产物，其制造、生产和流通逐步形成网络地下经济产业链。从“熊猫烧香”病毒的传播过程就可以看到，恶意代码的编写者、传播者通过发现漏洞、利用漏洞、编写恶意代码和买卖网络资源获利。网络地下经济的蓬勃兴起导致越来越多的网络终端受害，大量机密信息被窃取，敏感数据信息（包括用户的信用卡信息、借记卡信息、个人身份信息、游戏账号、网络账号等）在互联网上传播，并在黑市网站和聊天室中待价而沽。更为严重的是，通过漏洞和恶意代码，一些个人或团体有组织、有预谋地在一定范围内控制一群机器，通过特殊的控制信道和指令来掌握这些机器的行为，不但可以窃取这些机器中的机密信息，更可以发动大规模网络攻击。这种被称为“僵尸网络”的系统已经成为互联网的巨大威胁。由于互联网的广泛使用和快速传播特性，通过对信息系统的控制，有恶意目的的攻击者甚至具备了相当程度的信息影响和控制能力。由此可见，漏洞已成为网络地下经济产业链的源头，随着社会生活对信息系统依赖性的增强，漏洞危害已经成为关系国家安全的重要内容。

在“十二五”期间，我国将发展新一代信息技术产业作为抢占新一轮经济和科技发展制高点的重大战略。新技术新应用的安全漏洞，特别是基础核心系统的安全漏洞将成为制约新技术新应用发展的瓶颈。例如，云计算作为一种新型的信息利用模式和商业模式，得到了越来越多的重视。从技术和产业链上看，云计算是跨越硬件、软件、应用等多个领域的信息技术应用模式，它涉及虚拟化、云平台、分布式资源管理、海量分布式存储、云安全等大量核心技术，因此存在于底层和基础系统的安全漏洞将会给云计算带来更致命的安全隐患。2011 年以来，云安全事故频发，“云攻击”正在变为现实。例如，亚马逊服务器大面积宕机，云服务中断 4 天，恶意攻击者利用亚马逊弹性云计算盗取 9 家银行用户数据。此外，在物联网领域，由于我国在传感器、RFID 等核心器件产品种类不全，多为低端产品，且在该领域缺乏相关的技术标准体系，缺乏自主知识产权的产品，产业链不健全；更为重要的是，某些物联网关键基础设施由于集中应用国外技术和产品，如果存在人为设置的“漏洞”，将导致整个物联网产业受控于人的被动局面。由此可见，在新技术及新应用

中的基础系统安全漏洞及关键基础设施的人为预置漏洞将直接影响我国新一代信息技术产业发展的战略目标。

2. 漏洞分析工作的内容

通过分析漏洞对信息安全的影响可知，随着全社会对信息网络的依赖不断加剧，漏洞日益成为信息安全的无形杀手，由漏洞滋生的各种信息安全问题，对政府和行业信息安全所造成的危害程度高，冲击大。因此，中央高度重视信息安全工作，根据新的国际斗争形势，结合我国国情，适时部署和强化漏洞分析工作。

在本书中，我们将漏洞分析工作理解为：对信息技术安全漏洞的成因、机理和模型进行研究，从技术和管理两个角度，发现、修复并消减漏洞，为信息安全保障工作提供理论、方法、工具与手段。

具体来说，从技术角度出发，漏洞分析工作主要包括漏洞发现、漏洞发布、漏洞修复和漏洞预防等环节，其中，漏洞发现是漏洞分析的基础，漏洞发布和修复是漏洞分析的关键，漏洞预防是漏洞分析的目标。从管理角度出发，漏洞分析工作主要包括两个方面：一方面是漏洞管理的机制和模式，包括每个国家在政府、产业、学术、用户等几个层面建立相应的组织与机构，从战略和战术两个层面出发，通过法律法规、基础设施、市场、合作与交流等手段对漏洞资源进行管理，对漏洞分析工作进行指导；另一方面是与漏洞相关的国际标准规范的制定，信息安全漏洞相关准则和规范研究在管理漏洞方面起到了重要作用，可为国家在信息安全漏洞的管理措施制定、管理机制运行、管理部门协作等方面提供参考或依据，是行政管理的重要辅助手段之一。

3. 漏洞分析工作的现状

信息安全漏洞作为一种战略性资源和网络空间博弈的资本和武器被各国政府高度关注，纷纷采取行动，建立国家和地区级漏洞库。例如，美国于 2006 年为配合布什政府的国家网络安全战略，在原有“互联网可搜查漏洞索引 ICAT”的基础上，建立了美国国家漏洞数据库(NVD)，由国土安全部(DHS)研究部署并提供建设资金，由美国国家标准与技术研究院(NIST)负责技术开发和运维管理。欧盟于 2008 年启动“欧洲盾牌计划”，开展漏洞库服务，该计划注重漏洞模式的提取、模型研究和工具开发，以便于开展漏洞的检测和防范。在我国，2009 年 10 月 18 日，中国国家信息安全漏洞库(CNNVD)投入运营，目前由中国信息安全测评中心负责建设和运维。由此可以看出国家级漏洞库已成为国家信息安全保障的一项重要基础设施，因此，围绕漏洞资源展开的漏洞发现、漏洞发布、漏洞修复等漏洞分析相关的技术和管理工作已成为我国信息安全保障的基础工作。

当前网络空间博弈日益复杂和严峻。一方面西方国家不断开展漏洞挖掘和分析，实施网络攻防演练，大力提升网络对抗能力；另一方面，西方国家积极开发以漏洞利用为核心的网络战武器，备战网络空间，全球网络军事化的进程明显加快。我国相关部门已经认识到漏洞分析工作是国家信息安全保障的重要环节，由此开展

了相关理论研究和技术工具的研发。经过近几年的探索和实践，也逐步认识到漏洞分析工作是一项极具挑战性的课题。这主要体现在以下几个方面。一是漏洞分析在国际上被列为“高精尖”和“杀手锏”对抗性技术，西方发达国家均将相关研究项目和成果列为国家机密“严防死守”，严格限制出口，而国内研究者较少，整体水平非常有限，包括所用的大型、高端专用工具都需要从西方发达国家购买；二是漏洞分析本身是一项对个人素质要求极高、经验性很强的工作，且由于技术大量掌握控制在黑客层面，理论总结不够，也未形成独立成熟的学科领域，传承相对困难；三是随着新技术、新应用、新产品不断产生，网络和系统的复杂程度持续增加，同时云计算和物联网时代的到来将使未来的网络体系架构发生巨大变革，由此带来的基于复杂系统和新技术应用的信息安全风险评估手段和方法将越来越复杂，技术难度将越来越大。由此可见，漏洞分析工作涉及我国信息化工作的发展，更涉及我国国家安全，因此，我们需要把漏洞分析工作作为我国信息安全保障的关键和长期的工作来对待，切实有效地应对安全事件和网络对抗。

4. 本书结构

本书共分 3 部分，合计 11 章。

第 1 部分(理论篇)——漏洞分析理论研究基础。主要内容有：漏洞的定义、漏洞的产生、漏洞的分类、漏洞状态演变模型、漏洞数量预测模型、漏洞发展的态势分析。

第 2 部分(方法技术篇)——漏洞分析的工作内容及方法。主要内容有：漏洞的发现，包括对漏洞进行挖掘、检测、验证和危害评级；漏洞的发布，包括对漏洞信息进行收集、监测和发布；漏洞的修复，包括现状和安全补丁的类型、描述、修复模式、分析技术；漏洞的预防，包括从人员的教育和意识、开发过程、使用和维护过程三个方面开展漏洞的预防工作。

第 3 部分(管理篇)——漏洞管理的组织机构和标准规范。主要内容有：漏洞管理组织机构，包括组织机构类型、合作交流、管理机制、风险控制对策等；漏洞管理标准规范，包括从漏洞标识、漏洞补丁、漏洞信息等几方面总结和分析国内外漏洞管理标准规范，并提出漏洞分析准则框架。

5. 致　谢

本书对多年来漏洞分析工作的发展历程进行了系统、翔实的总结，在编写过程中得到社会各界人士特别是中国信息安全测评中心的高新宇、李守鹏、张涛、张晓菲、熊琦、吴润浦、王星、刘彦钊、张磊、张宝峰、刘洪梅、李婧、刘林、李娟、赵向辉、姚原岗、刘晴等同志的大力支持和帮助。在本书即将出版之际，对给予本书关心和帮助的各方面人士表示衷心的感谢。

本书得到中国信息安全测评中心“漏洞分析与风险评估”专项工程国家自然科学基金项目(90818021)的支持。

目 录

第 1 部分　理论篇

第 2 部分 方法技术篇

第 6 章 漏洞的发现

第 7 章 漏洞的发布

第1部分

理论篇

第1章　漏洞的定义

漏洞(Vulnerability)又叫脆弱性,这一概念早在1947年冯·诺依曼建立计算机系统结构理论时就有涉及,他认为计算机的发展和自然生命有相似性,一个计算机系统也有天生的类似基因的缺陷,也可能在使用和发展过程中产生意想不到的问题。20世纪80年代,早期黑客的出现和第一个计算机病毒的产生,软件漏洞逐渐引起人们的关注[1]。20世纪70年代中期,美国启动的PA计划(Protection Analysis Project)[2]和RISOS(Research in Secured Operating Systems)计划[3]开启了信息安全漏洞研究工作的序幕。在历经30多年的研究过程中,学术界、产业界以及政策制定者对漏洞给出了很多定义,漏洞定义本身也随着信息技术的发展而具有不同的含义与范畴,从最初的基于访问控制的定义发展到现阶段的涉及系统安全流程、系统设计、实施、内部控制等全过程的定义。

1.1　漏洞的概念

1.1.1　基于访问控制

1982年,Denning从系统状态、访问控制策略的角度给出了漏洞定义[4],认为系统的状态由三大要素集合$\{S,O,A\}$组成,其中:

(1) 操作主体集合S是模型中活动实体(Entity)的系列主体(Subject)。主体同时属于对象,即S属于O。

(2) 操作客体集合O是系统保护的实体的系列对象,每个对象定义有一个唯一的名字。

(3) 规则集合A是访问矩阵,行对应主体,列对应对象。

系统中主体对对象的访问安全策略是通过访问控制矩阵来实现。改变系统的状态就是通过改变访问矩阵的基本操作元素,从而改变操作系统的指令模型。访问矩阵的设置描述了主体能够做什么、不能做什么。这样,一个保护策略或安全策略就把所有可能的状态划分为授权的和非授权的两个部分。从访问控制角度讲,信息安全漏洞是导致操作系统执行的操作和访问控制矩阵所定义的安全策略之间相冲突的所有因素。

1.1.2　基于状态空间

Bishop 和 Bailey 在 1996 年对信息安全漏洞给出了基于状态空间的定义[5]，认为信息系统是由若干描述实体配置的当前状态所组成的，系统通过应用程序的状态转变来改变系统的状态，通过系列授权和非授权的状态转变，所有的状态都可以从给定的初始状态到达。容易受到攻击的状态是指通过授权的状态转变从非授权状态可以到达的授权状态。受损害的状态是指已完成这种转变的状态。攻击就是指到达受损状态的状态转变过程。

从状态空间角度来讲，漏洞是区别于所有非受损状态的容易受攻击的状态特征。通常地讲，漏洞可以刻画许多容易受攻击的状态。

1.1.3　基于安全策略

对大多数系统来说，基于状态空间定义漏洞的主要问题是由于状态和迁移的数量一般为指数级别，因此导致了状态空间“爆炸”，而不能有效地进行枚举或搜索。因此，研究者们提出了基于安全策略的漏洞定义方法。

给定一个系统，安全策略规定了其用户哪些操作是允许的，哪些操作是不允许的。其形式化的定义为：给定状态空间 $S=(M,T)$，安全策略是状态对，其中，$A\subseteq M$ 是系统允许的状态集合，$D=M-A$ 是系统不允许的状态集合。那么基于安全策略的漏洞定义为：漏洞是一个二元组 $V=(N,P)$。其中，N 是一个非空的条件集合，满足这些条件可导致违背某个系统 x 的安全策略 P。

在文献[6]中，提出了一个层次式安全策略模型，在该模型中，根据安全策略被实现的程度，展示了不同类型的安全策略。因此，对应于不同安全策略的违背，就形成了不同类型的漏洞。

由美国 MITRE 公司（一个由美国联邦政府支持的非营利性研究机构）在 1999 年发起，旨在为信息安全产业界提供通用漏洞与披露（Common Vulnerabilities and Exposures，CVE）的标准命名字典给出的定义也是基于安全策略的，即一个错误（Mistake）如果可以被攻击者用于违反目标系统的一个合理的安全策略，那么它就是一个漏洞。一个漏洞可以使目标系统（或者目标系统的集合）处于下列危险状态之一：允许攻击者以他人身份运行命令；允许攻击者违反访问控制策略去访问数据；允许攻击者伪装成另一个实体；允许攻击者发起拒绝服务攻击。

1.1.4　基于信息安全风险管理

1992 年，D. Longley 等[7]从风险管理角度把漏洞分成 3 个方面来描述：一是存在于自动化系统安全过程、管理控制以及内部控制等方面的缺陷，它能够被攻击者所利用，从而获得对信息的非授权访问或者关键数据处理；二是在物理层、组织、程

序、人员、软件或硬件方面的缺陷，它能够被利用而导致对自动数据处理系统或行为的损害；三是信息系统中存在的任何不足或缺陷。

1999 年，ISO/IEC 15408-1 给出的定义是：漏洞是存在于评估对象（TOE）中的，在一定的环境条件下可能违反安全功能要求的弱点[8]。2000 年美国发布的信息系统安全词汇表（NSTISSI No. 4009）给出的定义认为漏洞是指可被利用的信息系统、系统安全流程、内部控制或实施中存在的弱点[9]。2011 年美国国家标准和技术研究院发布的《关键信息安全术语词汇表》（NIST IR 7298）认为漏洞是指威胁源可以攻击或触发的信息系统、系统安全流程、内部控制或实施中的弱点[10]。依据同年出版的《信息安全字典》给出的定义，漏洞是系统安全流程、系统设计、实施、内部控制等过程中的弱点，这些弱点可以被攻击以违反系统安全策略；攻击或对威胁暴露的可能性特定于给定的平台。依据 2009 年 ISO/IEC SC 27 发布的国际标准《SD6：信息安全术语词汇表》中给出的定义：漏洞是一个或多个威胁可以利用的一个或一组资产的弱点，是违反某些环境中安全功能要求的评估对象（TOE）中的弱点，是在信息系统（包括其安全控制）或其环境的设计及实施中的缺陷、弱点或特性[11]。

1.2 本书的定义

信息安全漏洞是信息技术、信息产品、信息系统在需求、设计、实现、配置、维护和使用等过程中，有意或无意产生的缺陷，这些缺陷一旦被恶意主体所利用，就会造成对信息产品或系统的安全损害，从而影响构建于信息产品或系统之上正常服务的运行，危害信息产品或系统及信息的安全属性。也就是说，本书将漏洞研究的对象限制在信息技术、信息产品、信息系统等方面，未将人和管理流程作为主要研究目标；同时，明确了漏洞的产生环节，即需求、设计、实现、配置、运行等全生命周期过程中均可能存在漏洞；最后，指出了漏洞的危害特性。

信息安全漏洞是和信息安全相对而言的。安全是阻止未经授权进入信息系统的支撑结构，漏洞是信息产品或系统安全方面的缺陷。例如，在 Intel Pentium 芯片中存在的逻辑错误、在 Sendmail 中的编程错误、在 NFS 协议中认证方式上的弱点、在 Unix 系统管理员设置匿名 FTP 服务时配置不当、对信息系统物理环境、信息使用人员的管理疏漏等，这些问题都可能被攻击者使用，威胁到系统的安全。因而这些都可以认为是系统中存在的安全漏洞。

有时漏洞被称为错误（Error）、缺陷（Fault）、弱点（Weakness）或故障（Failure）等，这些术语很容易引起混淆。严格地讲，这些概念并不完全相同。错误是指犯下的过失，是导致不正确结果的行为，它可能是印刷错误、下意识的误解、对问题考虑不全面所造成的错误等；缺陷是指不正确的步骤、方法或数据定义；弱点是指难以克服的不足或缺陷，缺陷和错误可以更正、解决，但弱点可能永远也没有解决的办