LOIS

信息安全国家重点实验室

信息安全丛书

Information System
Incident Response

信息系统安全事件响应

李德全　苏璞睿　编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

信息系统安全事件响应

李德全　苏璞睿　编著

国家自然科学基金资助项目(项目编号:60273027)
国家杰出青年基金资助项目(项目编号:60025205)
国家重点基础研究发展规划 973 项目(项目编号:G1999035802)

科学出版社
北京

内 容 简 介

本书是《信息安全国家重点实验室信息安全丛书》之一。本书主要介绍了与信息系统安全事件响应相关的关键技术和一些管理措施，以及在处理信息安全事件过程中的主要工作内容。书中主要内容包括：各种攻击技术介绍；如何进行日常安全管理，降低安全事件的发生；如何检测入侵事件，及时发现问题；如何组建应急响应小组，防患于未然；应急响应技术与工具介绍；事件响应过程中各个阶段所要完成的主要工作等。

本书可作为计算机、信息安全、管理信息系统等专业的高年级本科生、研究生的教学参考书，也可供相关领域的科研和工程技术人员，尤其是安全管理人员和应急服务人员参考。

图书在版编目(CIP)数据

信息系统安全事件响应/李德全，苏璞睿编著. —北京：科学出版社，2005
(信息安全国家重点实验室信息安全丛书/冯登国主编)
ISBN 7-03-015537-8

Ⅰ. 信… Ⅱ. ①李…②苏… Ⅲ. 信息系统-安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2005)第 048399 号

责任编辑：鞠丽娜 /责任校对：柏连海
责任印制：吕春珉/封面设计：王 浩

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

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2005 年 6 月第 一 版 开本：B5 (720×1000)
2005 年 6 月第一次印刷 印张：14 3/4
印数：1—4 000 字数：295 000

定价：24.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

销售部电话 010-62136131 编辑部电话 010-62138978-8002 (BI06)

《信息安全国家重点实验室信息安全丛书》编委会

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了非常漫长的岁月。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾御技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人和社会等因素，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系、操作系统安全、数据库安全，网络安全、无线网络安全、网络攻击、密码技术、PKI 技术、信息隐藏、安全协议、安全事件应急响应、量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

2003 年 7 月

前　言

随着计算机网络的广泛应用，政府、企业和教育等组织机构的日常工作对计算机的依赖性越来越大。计算机网络已经渗透到了社会的方方面面，已经在政治、经济、教育等方面发挥出愈来愈大的作用。计算机已经逐步成为政府和商业活动的主要工具。计算机的大量应用既带来了利益也带来了风险，大量网络安全事件的发生引起了各国政府和广大网络用户对网络安全的广泛关注。

计算机网络技术的飞速发展已使得现有的网络系统越来越复杂，管理难度越来越大，而层出不穷的安全漏洞也为入侵者提供了源源不断的入侵机会。Internet的发展给人们带来越来越多便利的同时，也使网上黑客迅猛增加，这些都使得今天的计算机网络面临更大的威胁，从而使得确保网络系统的安全性变得越来越困难。由于绝对的安全是不可能的，也是不必要的，当现有的安全防范措施没能阻止安全事件的发生时，应急响应就成为了减少损失的重要手段。在著名的PDRR（保护、检测、响应和恢复）模型中，响应成为了信息安全保障中极为重要的一环。

随着信息系统重要性的增加以及信息安全事件的增加，人们对应急响应服务的需求也在逐渐增加。目前，国内陆续地有一些公司提供应急响应服务。然而，相比国际上一些先进国家而言，国内在应急响应方面还存在着较大的差距，国内大多数公司提供的应急响应多是低层次的和不规范的。同时，国内应急响应方面的参考书较为缺乏。因此，我们特组织有关人员编写了这本书，一方面希望能供广大读者借鉴和参考；另一方面也希望能抛砖引玉，期待着出版更多更好的应急响应方面的参考书。

本书主要介绍了与应急响应相关的关键技术和管理措施，并详细论述了应急响应过程。书中介绍了应急响应队伍的建设和相关的日常管理措施，对应急响应队伍的构成、培训、管理等多方面进行了论述，并在附录中提供了事件报告模板以供用户参考。本书将应急响应过程进行了分解，分为前期准备、中期处置和后期总结三个阶段，详细说明了各个阶段具体应该完成的工作以及涉及的关键技术，对于开展实际应急响应工作具有重要指导作用。书中还介绍了大量的应急响应工具，以便用户在实际工作中参考。由于应急响应工作必须跟踪最新的技术进展，为了便于读者随时了解最新动态，我们在附录中还提供了丰富的网上资源。这些资源都是目前业内人士广泛关注的站点，它们提供了丰富的最新技术动态，可供从事应急响应工作的有关人员学习参考。

本书是几位同仁通力协作的结晶，在具体写作过程中，我们也各有侧重。其中，

第1章和第4章由苏璞睿执笔，第2章、第5章、第9章、附录A、附录B由李德全执笔，第3章、第6章、第8章由徐一丁执笔，第7章由钱秀槟执笔。冯登国老师审阅了全书。

本书在出版过程中得到了科学出版社各位老师的大力支持和帮助，鞠丽娜老师、刘亚军老师更是为此付出了大量的心血和辛勤的劳动。在本书的写作过程中还得到了众多信息安全专家的指导和帮助，在此一并表示感谢。

由于作者水平有限，疏漏之处在所难免，欢迎广大读者批评指正。

作　者

于北京中关村

2005.2

目　录

第1章 概 述

随着计算机网络的广泛应用，政府、商业和教育等机构的日常工作对计算机的依赖性越来越大。据统计，Internet 上的主机，截至 2001 年 1 月是 1 亿 1 千万台，2002 年 1 月是 1 亿 5 千万台左右，2003 年 1 月是 1 亿 7 千万台左右。据中国 Internet 络信息中心调查显示，截至 2004 年 6 月底，我国上网用户约为 8 700 万，上网计算机数约为 3 630 万台，在 CN 下注册的域名数约为 382 216 个，WWW 站点的域名数约为 626 600 个，国际出口带宽达到了 53 941Mb/s。这些数据反映出我国的网络化建设正在高速发展，计算机网络已经渗透到了社会的方方面面，并已经在政治、经济、教育等方面发挥出愈来愈大的作用。

随着网络的快速发展，计算机已经逐步成为政府和商业活动的主要工具。但计算机的大量应用既带来了利益也带来了风险，大量网络安全事件的发生引起了各国政府和广大网络用户对网络安全的广泛关注。

虽然人们对网络安全的关注与投资与日俱增，但是安全事件的数量和影响并没有因此而减少。图 1.1 是 CERT/CC (Computer Emergency Response Team/Coordination Center) 接到的安全事件报告的统计，而向 CERT/CC 报告的安全事件还只是所有安全事件中很少的一部分。

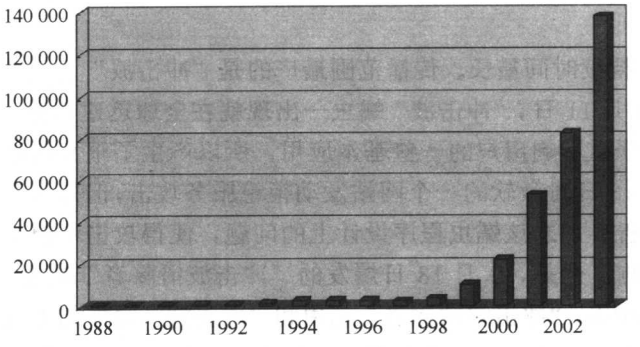

图 1.1 CERT 接到的安全事件报告的统计

1988 年 11 月蠕虫爆发，造成 6 000 多台计算机崩溃。两周后，由美国国防部资助在卡内基·梅隆大学建立了应急响应小组 (CERT)。这是全世界第一个完全意义上的应急响应组织，后来发展为应急响应协调中心 (CERT/CC)。美国能源部也随之建立了计算机事故咨询委员会 (Computer Incident Advisory Capability,

CIAC）以处理相关计算机安全事故。

随后，世界各地各种各样的计算机安全事件响应组织纷纷成立。由于语言、地域和标准的差异，最初各个应急响应组织之间交流不多。1989 年 10 月，Wank 蠕虫的爆发让大家发现了应急响应组织间交流合作的重要性。1990 年，成立了第一个全球应急响应和安全小组论坛（Forum of Incident Response and Security Team，FIRST）。截至 2004 年 6 月，全球已有 200 多个应急响应组织，其中加入 FIRST 的就有 150 多个。这也从另外一个侧面反映了应急响应越来越多地受到重视。

1.1　为什么需要应急响应

由于各类信息安全事件产生的严重损失已被媒体曝光，各组织机构越来越关注自身的信息安全建设。据美国联邦调查局(FBI)和计算机安全研究所(Computer Security Institute) 2004 年度《计算机犯罪与安全调查》显示，在被调查的对象中，99%采用了反病毒软件，98%应用了防火墙。可是在过去的 12 个月中，仍有 78%受到攻击，这还不包括 22%不清楚自己安全情况的。CERT 收到的安全事件报告的数量也迅速增长，1998 年是 3 734 起，2001 年猛增到 52 000 起，2002 年增加到 82 094 起，而 2003 年记录在案的安全事件已达到了 137 529 起，是 2000 年的 6.5 倍。

2001 年，“红色代码”蠕虫在 Internet 上的大规模蔓延给全世界带来的经济损失高达 20 亿美元，而这与“求职信”、“情书”等蠕虫相比，则是小巫见大巫，它们所造成的损失分别为 90 亿美元和 88 亿美元。每年由病毒所造成的损失达上千亿美元。

2003 年，持续时间最长、传播范围最广的是“冲击波”及其变种“冲击波清除者”蠕虫。8 月 11 日，“冲击波”蠕虫一出现就在全球迅速传播，并且由于遭受该蠕虫感染会严重影响用户的一些基本应用，所以产生了很大的社会影响。该蠕虫设定于 8 月 16 日对微软的一个网站发动拒绝服务攻击，但是由于微软撤销了该网站的域名解析，加之该蠕虫程序设计上的问题，使得攻击不但未成功，蔓延速度反而受到影响。但是，8 月 18 日爆发的“冲击波清除者”蠕虫，却给 Internet 带来了更大的冲击。“冲击波清除者”利用和“冲击波”同样的方式入侵网络中存在特定漏洞的主机，因此在技术上相当于原来“冲击波”蠕虫的一个变种。虽然该变种主要的动作是给感染“冲击波”蠕虫的主机下载补丁程序，但它的探测和蔓延方式，却导致了网络带宽的严重消耗，事实上造成了部分区域网速的大幅下降。根据 CNCERT/CC 对采样数据的分析，全世界至少有 2 000 多万台主机感染“冲击波”或“冲击波清除者”蠕虫，其中我国至少有 600 多万台。

美国黑客保险业的繁荣从另一个方面反映了网络安全形势的严峻。据预测，美

国的“黑客保险”市场有望从2003年的1亿美元增加到2005年的9亿美元。目前，Internet上的黑客攻击事件每天都有发生，其中一些涉及盗窃信用卡号、公司商业机密和电脑病毒攻击等。越来越多的保险公司开始要求客户为黑客袭击可能造成的损失额外支付保险费，否则对这部分损失不予理赔。

“9·11”事件则告诉了人们，再好的防火墙、防病毒软件也防不住这种出人意料的恐怖袭击。“9·11”事件造成的直接经济损失达上千亿美元，而一些公司由于没有相应的应急措施，没有采取完备的灾难备份，造成整个公司业务瘫痪，甚至公司破产。

由此可以看出，现有的安全防范措施并不能完全保证我们的网络系统绝对安全，仍然不可避免地会有一些意外事件发生，而原因是多方面的。

1. 应用越来越复杂，管理难度增加

根据泰钠的推论，技术上的每一次努力都意在提供对现实问题的解决办法，但同时也暗藏着反噬自己的种子。自从电子计算机时代的来临，对电话和计算机的攻击行为就没有停止过。从一开始，数据安全机制就是与计算机操作系统密不可分的一部分，直到20世纪80年代中期，攻击行为还只是局限在小范围内。此后，便宜的调制解调器把每台个人计算机都变成了潜在的终端，使它们可以同其他任何计算机进行交流，而不断扩展的Internet更促使通信与计算变得无所不在，几乎世界任何角落的不知名的用户都可能成为潜在的攻击者。

网络技术的推广应用，使组织对网络的依赖程度越来越大，如业务推广、内部日常管理、客户售后服务等都需要依靠网络来解决。组织机构的分散，使组织机构网络地域分布越来越广，组织内部网络也越来越复杂。网络解决方案既要考虑组织内部管理，又要考虑客户的需要。

网络中各种各样的网络设备及其上运行着的各种各样的操作系统、应用服务则让管理员伤透了脑筋。现在，一个大型网络中，通常会有多个操作系统同时运行。每个系统都有着各自不同的安全机制和配置管理方法；防火墙、路由器等网络设备各自有一套深奥难懂的配置方法，要保证各个设备之间策略的一致自然不是轻而易举的；大量的数据库服务器保存着各种各样密级的数据，必须分开管理；组织内部可能还有自己的电子商务/电子政务平台，上面的应用更是五花八门，包括Web服务、邮件服务、FTP服务等；还需要对各种各样的用户群的访问控制权限进行有效管理，如公司内部用户、客户、合作伙伴等。

最让人头疼的是这些设备、系统可能还会有各种各样的漏洞，它们会危及管理员的安全控制目标，因此还需要对它们打补丁。CERT/CC曾经做过一个调查，截至2002年，一共有5 500个漏洞发布。假设阅读一个漏洞的相关介绍，平均要花20分钟，那么一个管理员要熟悉所有漏洞，则一共需要229天。如果只有1%

的漏洞影响系统，需要安装补丁程序，且安装一个补丁程序只要1个小时的话，共需要69天。这样，仅仅是了解漏洞信息，安装补丁程序，需要的时间就是298天。阅读新发布的电子公告中的1%，每一篇文章花5分钟时间，至少需要65天。截至2003年，CERT/CC发布的漏洞数量是12 946个。当然，该分析是基于考虑所有漏洞信息这一假设，实际操作时，会更多地关注和自己有直接关系的漏洞信息，有选择地放弃一些信息，但这也从一个侧面反映出了网络管理员要确保系统安全的难度。

由于应用越来越复杂，涉及的协议越来越复杂，软件系统越来越庞大等原因已经造成软件开发难度加大，软件可靠性降低。随着网络应用的发展，网络将涉及越来越多的系统及应用，而各类系统、应用又会带来更多的漏洞。

从漏洞的发现到漏洞补丁、相应评估工具等安全措施发布之间的这一段时间，也为入侵者留下了很大空挡。一个漏洞一般要经历从高水平攻击者发现这一漏洞、粗糙的漏洞利用工具发布、新手广泛利用该工具、自动检测/利用该漏洞的工具发布、自动工具广泛传播五个阶段。网络管理员不能及时获取漏洞评估工具和补丁程序，不能在入侵者发现漏洞之前采取弥补措施，也为系统的安全管理增加了难度。

因此，网络与信息系统已变得越来越复杂，这使确保系统的安全性变得更加困难。

2. 来自 Internet 的威胁增加

在我们越来越难管理好我们的网络系统的同时，来自网上的威胁也在增加。随着网络技术的普遍应用，Internet 几乎触及到了世界的各个角落。我们在利用Internet的便利和世界各地的朋友交流的同时，也给入侵者提供了便利的条件。我们的潜在攻击者可能遍布在世界的各个角落。他们有着各种各样的动机，有的是为了金钱，有的是为了宗教信仰，而有的则仅仅是好奇，或者是为了吸引人的注意力，为了出名。入侵者有可能是十几岁的小孩，也有可能是竞争对手安排的工业间谍，有可能是敌对国家组织，也有可能是公司内部员工发泄对领导的不满。1999年12月，Saint Diego的超级计算机中心曾经做了一个试验，他们在一个机器上安装Redhat 5.2，没有打任何补丁，连接到Internet上。8小时后，即有人开始扫描，寻找该机漏洞；21天后，即有20多人次试图利用Telnet、RPC、IMAP等方面的漏洞入侵该主机；40天后，该主机被攻破，攻击者还在该主机上安装了rootkit和sniffer。Internet上的潜在攻击者数量在激增，随时都在寻找新的目标。

随着网络技术的发展，黑客攻击方法也发生了很大变化。1988年，黑客攻击主要采用破解口令和利用已经公开的漏洞。如今黑客可以利用的攻击技术已经越来越全面，攻击方法也朝智能化和大规模方向发展。网络上的黑客大都是狂热的网络技术爱好者，他们对网络技术有着强烈的好奇心，并有着扎实的技术基础、充

裕的时间和精力，他们能够利用 Internet 上丰富的技术资料，很快地学习并掌握一些攻击方法。Internet 几乎成了黑客新手的学习园地，既有全面的学习资料，还有各类功能强大的免费工具，并可和不少同行交流。Internet 上各种层次的黑客攻击论坛数不胜数，而黑客技术更是吸引了不少电脑爱好者，他们不断涌向这个群体，互相交流，互相帮助提高。

根据 CERT/CC 的研究表明，在我们越来越难管理好我们自己的网络，攻击涉及的技术越来越复杂的同时，已有越来越多的高质量黑客攻击工具发布，攻击过程自动化程度越来越高，要成功地实施攻击对入侵者的要求越来越低。对于黑客团体来说，Internet 为他们提供了很好的交流方式。他们采用松散组织方式，代码共享，共同开发各类技术精湛、界面友好、易于使用的黑客工具，而 Internet 能让这些工具在短短几个月内在世界各地迅速传播开来。任何一个新手都可以很容易地掌握它，利用它在 Internet 上造成实质性破坏。

在 Internet 上很难追踪到攻击者，由于对攻击取证的困难以及其他一些相关法律问题，将网络入侵者绳之以法的难度较大，因此网络入侵者承担的风险很低。这也是造成如今网络入侵泛滥的原因之一。他们几乎可以毫无顾忌地利用一些机构的网络作为自己学习训练攻击技术的对象。

黑客活动的日益猖獗，促使各国政府设立专门机构、增加经费投入、加紧培养网络安保人才及完善相关法制建设等。2000 年 10 月，美国国会通过了《计算机安全加强法》，把网络安全纳入了法制化管理的轨道。世界各国也在加强合作，共同对付黑客犯罪。2000 年，100 多个国家和行业的网络专家聚集德国柏林，共同商讨如何联手打击计算机犯罪问题。包括美国在内的 40 多个国家将加入欧盟委员会制定的《打击计算机犯罪公约》，该公约是为了对计算机犯罪采取统一的国际政策，防止针对计算机系统、数据和网络的犯罪活动。但由于种种原因，这些法律、相应机构还没有对 Internet 犯罪构成足够威慑。黑客群体仍在迅速膨胀，与黑客的对抗仍然任重道远。

3. 对信息技术依赖增加，风险增大

《经济观察报》2003 年曾刊登一篇题为《一场伟大的争吵：IT 不再重要?》的文章。该争吵由《哈佛商业评论》上的《IT 不再重要》引起。该文认为，“由于信息技术的能力和普及性已经达到成熟阶段，它的战略重要性降低了，公司处理信息技术投资和管理的方式必须彻底变革。”该文认为信息技术已经和铁路、电力和其他基础设施一样，已经变得如此普及，对公司来说它不可缺少，但它已经不能提供战略性竞争优势。我们且不讨论目前信息技术是否能为企业带来战略性竞争优势，但 Internet 及相关的信息技术已经成为众多企业、组织的“必需品”，它已经成了一种基础设施，这是一个不争的事实。整个社会对其依赖性已经越来越大，