高等院校信息技术规划教材

网络安全

邱仲潘 洪镇宇 编著

清华大学出版社

高等院校信息技术规划教材

网络安全

邱仲潘 洪镇宇 编著

清华大学出版社
北京

内 容 简 介

本书深入浅出地介绍网络安全的来龙去脉，二十年来发生的网络安全大事件及其背后的技术因素；介绍国家、企业与其他组织和个人可能面对的信息与网络安全威胁、各种防范措施及其适用范围和效果；从 TCP/IP 模型的各个层次介绍网络的攻击与防守；最后介绍当前主要的网络安全解决方案供应商及其各种产品的大致工作原理、接入方法和性价比评估。

本书既可以作为领导干部学习网络安全知识的读物，也可以作为专业人员转入网络安全领域的指南；既可以作为大中专院校不同专业同学了解网络安全的校选课教材，也可以作为信息安全专业同学的入门读物。

图书在版编目(CIP)数据

网络安全/邱仲潘，洪镇宇编著. —北京：清华大学出版社，2016
高等院校信息技术规划教材
ISBN 978-7-302-42812-1

Ⅰ. ①网… Ⅱ. ①邱… ②洪… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 028261 号

责任编辑：白立军　李　瞻
封面设计：常雪影
责任校对：时翠兰
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：14　　**字　　数**：321 千字
版　　次：2016 年 6 月第 1 版　　**印　　次**：2016 年 6 月第 1 次印刷
印　　数：1～2000
定　　价：29.00 元

产品编号：065800-01

前言 foreword

我们所处的时代是信息时代，移动互联、大数据和云技术使信息与网络越来越成为人们日常工作、生活的一部分，组织和企业的资源越来越集中到网络上，网络安全成为组织健全发展的必要条件。作为领导者，不可能花太多时间钻研技术细节，但必须对信息与网络面临的威胁、各种防范措施的适用范围和效果有足够了解，才能掌控局面，防患于未然，立于不败之地。

我们知道，网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。网络运行的管理者希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。安全保密部门希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，给国家造成巨大损失。因此计算机安全问题，应该像每家每户的防火防盗问题一样，做到防患于未然。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等发展到基于复杂的内部网(Intranet)、企业外部网(Extranet)、全球互联网(Internet)的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断地提高。但在连接能力信息、流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理的安全等。

本书深入浅出地介绍网络安全的来龙去脉，二十年来发生的网络安全大事件及其背后的技术因素；介绍国家、企业与其他组织和个人可能面对的信息与网络安全威胁、各种防范措施及其适用范围和效果；从 TCP/IP 模型的各个层次介绍网络的攻击与防守；最后介

绍当前主要的网络安全解决方案供应商及其各种产品的大致工作原理、接入方法和性价比评估。

本书一方面注意系统性与科学性，另一方面注意实用性和趣味性，由具有丰富教材编写经验和网络安全经验的教师编写，面向领导者，深入浅出，通俗易懂，同时照顾到技术要领，使领导者很容易提纲挈领，抓住网络安全问题的本质，有效开展工作。

编者

2016 年 2 月

目录 Contents

第1章 chapter 1

网络安全的来龙去脉

1.1 网络安全概述

1994年中国互联网与国际互联网全面对接之后，中国互联网发展日新月异。现今我们所处的时代是信息时代，移动互联、大数据和云技术使信息与网络越来越成为日常工作、生活中不可或缺的重要组成部分。而21世纪重要的特征就是网络化、数字化和信息化，因此网络毫无疑问是信息时代的核心。由于网络较强的技术性，网络安全成为网络中无法回避的问题。计算机网络的种种特点，如交互性、开放性等，导致它很容易受到攻击和干扰。我们所做的关于网络安全方面的努力，都是为了确保网络、系统中的信息达到保密、真实、完整、可用、可控等要求。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学和信息论等多种学科的综合性学科。它所涉及的场景很多，大到涉及国家的传统安全及非传统安全，小到商业企业的商业机密信息防护，甚至包括互联网上不良信息的传播或个人信息的泄露。

在互联网空前发达的今天，每年发生的网络信息安全事件不计其数，直接或间接地造成了巨大的损失。网络安全也呈现出了多元化的趋势，在不同平台上不停泛化且分布越来越广，如Windows平台、主机外设、Linux及其他类UNIX系统、智能设备、智能家庭、智能穿戴、智能交通和工控系统及社会基础设施都存在着不同程度的网络安全威胁。但网络安全主要威胁的途径还是通过信息泄露、黑客攻击和病毒入侵等。

但安全领域存在着各种挑战，各种因素交织在一起，错综复杂。

首先，人们对于安全这个概念有误解。我们可以先体会一下这句话：安全不是一件产品，它是一个过程。当人们遇到棘手的事情时，通常会选择避开这些麻烦。如果是无法避免的事情，人们往往会期望一劳永逸地解决它，但很明显这是不现实的。安全并不是配备了多么精良的设备，运用了多么高深的技术就能实现的。大多数人认为仅依靠设备就能实现安全，这是一种虚假的安全感。

其次，对于安全的投入并没有办法立即看见成效。事实上很多攻击发生后，很多管理人员总会庆幸对于安全方面的大力投入。很多时候，对于安全的投入与可能造成的损失相比算不了什么。但大多数人还是倾向于这是一件无利可图的事。

再次，安全问题并不像看上去那么简单。有些安全要求似乎很直观，但大多数重要的安全服务都要有个精确无误的词来描述。然而要了解这些专业词汇我们可能需要很多

积累。这需要我们潜心研究，没有办法一蹴而就。

然后，当一种新的算法或安全机制被开发的时候，需要考虑潜在的安全威胁。大多数情况下，攻击往往采用我们最意想不到的方式。就像中国的一句老话：千里之堤毁于蚁穴。因此，我们应从多角度、多方面来精心设计它们，而不是仅仅满足于特定的安全服务要求。应在不同的场合采取适合的安全机制或算法，有针对性地来解决不同的安全服务要求。

最后，计算机和网络安全实际上是攻击者与管理员或设计师之间的一场较量。有这么一句话说得好：互联网本来是安全的，自从有了研究安全的人后，互联网变得不安全了。出于种种目的，也许是利益，也许是炫耀技术，也许只是生活太过于平淡，总有些人企图发现一些漏洞来制造麻烦。但不同的是攻击者只要发现一个漏洞，管理人员则需要做好对攻击者行为的防范、中止和修复，要发现与修堵所有漏洞来保证安全。

另外，大多数人认为强调安全性对于系统或信息使用的易用性或有效性有影响。但实际上安全性大部分情况下是基础，对于安全性的强调完全是值得的。

1.1.1 网络安全的定义

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改和泄露，系统连续、可靠、正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。但网络安全涉及的内容不单是软硬件技术方面的，管理方面同样重要。技术方面侧重于防范外部的入侵，管理方面则侧重于内部人为因素的管理。安全领域普遍认为“最大的漏洞就是人”。例如，社会工程学就是黑客利用人为因素来达到自己预想的目的，且社会工程学认为安全链中最薄弱的环境就是人为因素。因此只有做到人防、物防、技防合一，才能真正实现安全这个目标。

1.1.2 网络安全的要素

既然安全方案的设计与实施是一个持续的过程，我们需要找到一些切入点来展开工作。把握住安全方案设计的思路与方法，就能够设计出优秀的算法或安全机制。要全面的认识网络安全问题，我们需要知道网络安全是由哪几种属性组成的。经过前人无数次的实践与总结，计算机网络安全大体包含有 6 个要素，即保密性、完整性、可用性、可控性、真实性和可审查性，其中保密性（confidentiality）、完整性（integrity）和可用性（availability）被称为 C-I-A 三元组，它是最基本的组成要素。

1. 保密性

保密性指的是非授权的用户、实体或过程对于信息无访问权限，从而保证涉密信息不被盗取或利用的特性。例如，一个软件需要访问数据库，该数据库的密码是进行加密之后存储在一个受保护文件中的，因此该软件若是需要访问数据库，需要算法、加密密钥、受保护文件提供的解密密钥、加密密码。

2. 完整性

完整性指的是信息在存储或传输的过程中防止信息被未经授权的篡改、删除、丢失和毁坏的特性。对于完整性的要求包含验证数据来源、检测数据更改、判断数据来源是否已经改变。

3. 可用性

可用性指的是可被授权实体访问并按需求使用的特性。高可用性应该具备以下属性：无单点故障、无单点修复、故障隔离出故障组件、故障遏制以防止故障传播、提供备用或恢复模式。

4. 可控性

可控性指的是对信息的传播及内容具有自主可控的能力，信息安全风险在可控的范围内。

5. 真实性

真实性指的是信息内容及信息行为主体具备真实性。

6. 可审查性

可审查性指的是对信息内容及信息行为可核查、可追溯。

保密性、完整性、可用性是最基本的组成要素。虽然后面扩充了可控性、真实性、可审查性、不可抵赖性等要素，但在设计安全方案的时候，要以最基本的安全3要素为出发点来全面的考虑问题。

1.2 网络安全的主要内容

1.2.1 物理安全

网络的物理安全是整个网络安全的前提。一般情况下，物理安全主要包含：火灾、洪水、地震等环境因素造成的事故；电源故障；人为操作因素；设备、线路被盗、被毁坏；电磁干扰等。因此在设备安置与防护时要充分考虑上述因素，防止设备遭到破坏，并采用一系列身份验证技术来控制接触设备的人员。

1.2.2 产品安全

网络最基本的元素是各式各样的信息技术产品，作为用户最常接触到的产品和大多数人连接互联网的入口，其安全性的要求之高不言而喻。通常信息技术产品包含有漏洞或者其他安全风险则会给整个网络造成巨大的破坏。我们一般指的信息技术产品包括

有计算机及软件、电信产品、半导体与半导体生产设备、科学仪器等产品，想要保证这些信息技术产品的安全主要是体现在对这些产品的控制力。对其关键技术的掌握程度、对其漏洞和后门的测试能力、发现能力与控制能力都是产品安全中所必须要强调的。

1.2.3 网络传输安全

网络传输是指线路经过电路的调整变化依据网络传输协议来通信的过程，是信息传递、交换、共享的必要手段。其需要传输介质来进行传输，还需要传输协议让计算机之间的相互通信共同遵守一定的规则。网络传输安全的主要任务就是确保信息资源在传输过程中的安全性，使信息资源符合网络安全的六个要素，做到信息资源不被非法获取、篡改、破坏等，从而实现传输安全。

1.2.4 网络运行系统安全

信息系统是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的，以处理信息流为目的的人机一体化系统，它需要做到的是为用户提供安全可靠的服务。但随着技术不断发展，信息系统现在不止面临着种类繁多的外部攻击，自身也包含着许多危害性极大的内部漏洞。为了确保信息系统的安全以及系统服务持续可用，一般需要定期对系统进行安全评估、异常任务排查、补丁升级、维护维修等技术手段。

1.2.5 网络系统设计与实施的安全

网络安全只保证网络运行系统安全是不够的，其最初的设计与实施则是很多人忽视的方面。不合理的设计与不规范的实施都会造成不同程度的安全威胁，且此类安全威胁对后期的影响比想象中的要大许多。对于设计与实施服务提供商应尽可能考虑多方面的因素并使系统符合相关国家法律法规和规范标准。而用户所用系统也应由具备相应安全资质和服务能力的机构设计与实施。

1.2.6 管理安全

正如之前网络安全定义中所讲的，网络安全不光指技术层面，也包含管理部分。而从以往经验来看，网络安全最大的风险都是来自于内部。为了实现内部人为因素的安全，部门与单位应制定完善的安全管理制度与法规，以此规范内部人员的行为、操作等，避免信息泄露、篡改或破坏，使攻击者无机可乘。

1.3 威胁建模

我们将可能造成危害的来源称之为威胁，把可能出现的损失称之为风险，风险一定与损失是相关联的。因此威胁分析和风险分析两个阶段并不同，但联系得很紧密。

威胁建模有许多方法，例如，头脑风暴法。当然也有比较科学的方法，比如对威胁进行建模。威胁建模有五个主要步骤。应当通过重复执行步骤二至步骤五逐步细化威胁建模。威胁建模的五个步骤如下。

步骤一：确定安全目标。目标清晰有助于将注意力集中在威胁建模活动上，已经确定后序步骤要做多少工作。

步骤二：创建应用程序概述。逐条列出应用程序的重要特征和参与者，有助于在步骤四中确定相关威胁。

步骤三：分解应用程序。全面了解应用程序的结构可以使用户更轻松地发现更相关、更具体的威胁。

步骤四：确定威胁。使用步骤二和步骤三中的详细信息来确定与用户的应用程序方案和上下文相关的威胁。

步骤五：确定漏洞。检查应用程序的各层以确定与威胁有关的弱点。使用漏洞类别来帮助用户关注最常出现错误的区域。

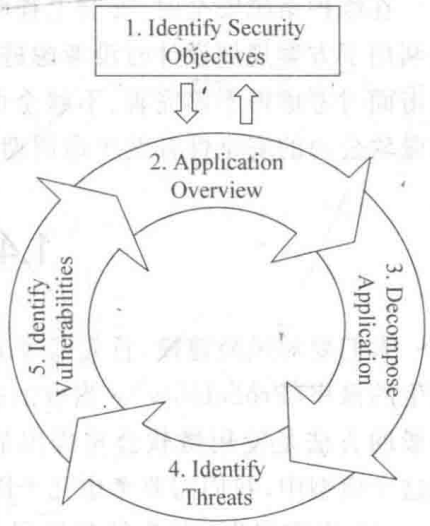

图 1.1 威胁建模

威胁建模如图 1.1 所示。

一般情况下需要考虑哪些威胁与安全性属性呢？我们可以采用微软公司提出的 STRIDE 模型。STRIDE 是 Spoofing（假冒）、Tampering（篡改）、Repudiation（否认）、Information Disclosure（信息泄露）、Denial of Service（拒绝服务）和 Elevation of Privilege（提升权限）的字母缩略词。分别对应的定义与安全属性如下。

（1）假冒的定义为冒充他人身份，对应的安全属性为身份验证。

（2）篡改的定义为修改数据或代码，对应的安全属性为完整性。

（3）否认的定义为否认做过的事，对应的安全属性为认可。

（4）信息泄露的定义为机密信息泄露，对应的安全属性为机密性。

（5）拒绝服务的定义为拒绝服务，对应的安全属性为可用性。

（6）提升权限的定义为未经授权获得许可，对应的安全属性为授权。

我们可以用数据流图来说明系统部件与相关的威胁。系统流图包括 4 个元素：数据流、数据存储、进程和交互方。而对于威胁建模，应另外增加一个元素为信任边界。数据流表示通过网络连接、命名管道、邮件槽、RPC 通道等移动的数据；数据存储表示文件、数据库、注册表项以及类似项；进程指的是计算机运行的计算或程序；交互方指的是系统的端点，即人、Web 服务和服务器。通常，他们是数据提供方，或处于系统范围之外但与系统相关的用户。信任边界表示可信元素与不可信元素之间的边界。STRIDE 模式提供了一个表格来说明这些元素可能涉及的威胁，如表 1.1 所示。

表 1.1 STRIDE 模式

元 素	假 冒	篡 改	否 认	信息泄露	拒绝服务	提升权限
数据流		√		√	√	
数据存储		√		√	√	
进程	√	√	√	√	√	√
交互方	√		√			

在维护系统安全时，安全工程师花费很多时间与精力实施安全方案，但攻击者却往往利用了方案规划设计时没考虑进去的漏洞，从而轻而易举地完成入侵。这就是在确定攻击面时考虑得不够完善、不够全面导致的。建模时也可以采用一些工具进行辅助，比如微软公司的安全性开发生命周期(SDL)威胁建模工具。

1.4 风险建模

人们要对风险建模，首先需要知道风险是由哪些因素组成的。一般情况下，风险＝发生的概率(Probability)×潜在的损失(Damage Potential)。如何更科学地衡量风险呢？一般的方法是使用微软公司提出的 DREAD 模型，DREAD 是几个单词首字母的缩写。在这个模型中，我们需要考虑几个因素。

(1) 潜在损失：如果缺陷被利用，损失有多大？

(2) 重现性：重复产生攻击的难度有多大？

(3) 可利用性：发起攻击的难度有多大？

(4) 受影响的用户：用粗略的百分数表示，有多少用户受到影响？

(5) 可发现性：缺陷容易发现吗？

按上述公式表明，特定威胁造成的危险等于威胁发生的概率乘以潜在的损失，这表明了如果攻击发生将会对系统造成的后果。可以用等级 1～10 来衡量概率，这里 1 表示威胁非常不可能发生，而 10 表示几乎肯定发生。同样，可以用等级 1～10 来衡量潜在的损失，这里 1 表示最小的损失，而 10 表示大灾难。用这种方法，发生概率低但潜在损失大的威胁造成的危险等于潜在损失有限但非常有可能发生的威胁所造成的危险。例如，if Probability＝10 and DamagePotential＝1，then Risk＝10×1 ＝ 10. If Probability＝1 and DamagePotential＝10，then Risk＝1×10＝10。这种方法导致分为等级 1～100，可以将这些等级分成高、中、低危险三级。在 DREAD 模型中有这么一个评价表，我们可以从中判断一个威胁的风险程度，如表 1.2 所示。

询问完上述问题后，计算给定威胁的值(1～3)，结果范围为 5～15。这样就可以将总分 12～15 的威胁评价为高度危险；8～11 的威胁评价为中度危险；5～7 的威胁评价为低度危险。例如，攻击者通过监视网络获得身份验证凭据。可做出如下评价，如表 1.3 所示。

表 1.2 DREAD 模型

评 价	高(3)	中(2)	低(1)
潜在的损失 (Damage Potential)	攻击者可以暗中破坏安全系统,获取完全信任的授权,以管理员的身份运行程序,上传内容	泄露敏感信息	泄露价值不高的信息
重现性 (Reproducibility)	攻击每次可以重现,而且不需要时间间隔	攻击每次可以重现,但只在一个时间间隔和一种特定的竞争条件下才能进行	攻击很难重现,即使很了解安全漏洞
可利用性 (Exploitability)	编程新手在短时间内就可以进行这类攻击	熟练编程人员可以进行这类攻击,然后重复进行这些步骤	这类攻击需要非常老练的人员才能进行,并对每次攻击都有深入的了解
受影响的用户 (Affected users)	所有的用户,默认配置,主要客户	一些用户,非默认配置	极少的用户,特点不明确,影响匿名用户
可发现性 (Discoverability)	公开解释攻击的信息;可以在最常用功能中找到的缺陷,非常明显	产品中很少使用部分的缺陷,只有少量的用户可能遇到。判断是否是恶意使用需要花费一些心机	错误不明显,用户不可能引起潜在的损失

表 1.3 DREAD 模型例子

D	R	E	A	D	总 计	得 分
3	3	2	2	2	12	高

以上说的是 DREAD 模式。但在许多实例中,综合的风险建模会消耗大量的时间,且效率低下。因此一些公司或组织会选择一种风险评估流程用于专注他们的项目业务。大体有以下几个步骤:

(1) 定义系统中所有数据类型,包括保密性、完整性和可用性(CIA)上的需求——信用卡数据、身份验证、用户联系信息等。

(2) 定义所有有风险的人员——外部恶意黑客、内部恶意黑客、活动分子、企业级间谍行为等。

(3) 定义所有有用实例——创建账号、下订单等。

(4) 对每个用户实例,定义应用流程如何在系统组件中进行。组件可以是高层次的(物理服务器)或是低层次(设计层的构建)——商业逻辑层,展现层等。并且记录哪些数据将在该用户实例中调用,以及相应的 CIA 需求。

(5) 对于每种操作,罗列所涉及的攻击载体,并查看这些载体在您的系统中是否存在。比如,如果一个用户实例包含数据库连接,那么 SQL 注入是一种很可能的攻击载体。您可以参考外部资源,即 OWASP ASVS、WASC 风险分类,或以 SANS/CWE 的前 25 位风险为参考建议。

(6) 评估每种潜在风险的危险性并定义策略,比如使用存储过程来防止 SQL 注入。

(7) 在一份统一报告中记录所有这些内容，并在程序员开始编码前提交给他们。

尽管更科学的风险的优势显而易见，但执行一个开销如此之大的活动，通常一个开发团队并不愿意承担风险建模的重担。因此对于一般情况，敏捷风险建模可能是更好的选择。例如，便捷式风险分析流程(Facilitated Risk Analysis Process，FRAP)，快速威胁建模(Threat Modeling Express，TME)等方法。

1.5 安全事件分类

由我国参与编制的国际标准 ISO/IEC 27035《信息技术、安全技术、信息安全事件管理》于 2011 年 7 月 12 日通过了国际标准编制最终阶段 FDIS 的投票表决，并于 9 月 1 日正式发布。该标准在原国际标准 ISO/IEC TR 18044:2004《信息技术、安全技术、信息安全事件管理》的基础上增加了我国国家标准 GB/Z 20986-2007《信息安全技术、信息安全事件分类分级指南》的内容。我国专家作为该标准项目的共同编辑，参与了标准制定的全过程。

2008 年 4 月，ISO/IEC JTC1 SC27 提出了 ISO/IEC 27035 新工作项，其主要内容是将技术报告 ISO/IEC TR 18044:2004 转化为国际标准。2008 年 4 月 SC27 WG4 京都会议上，在全国信息安全标准化技术委员会的组织下，我国代表基于我国国家标准 GB/Z 20986-2007，向 SC27 提交了《信息安全事件分类分级指南》的新工作项目提案，得到与会各国代表的认可，作为研究项目立项。同年 10 月 SC27 WG4 塞浦路斯全体会议决定将我国提案纳入 ISO/IEC 27035 项目，建议由日本专家和我国专家共同担任该项目的编辑，在 2009 年 5 月 SC27 北京全体会议上，该建议得到 SC27 的正式确认。这是我国第一次在信息安全领域将国家标准转化为国际标准。

经过 3 年的努力，ISO/IEC 27035 的编制工作已经顺利完成。该国际标准与 ISO/IEC TR 18044:2004 的最大区别在于引入了基于我国提案的信息安全事件分类分级内容。其中 GB/Z 20986-2007 对信息安全事件进行了分类。

1.5.1 有害程序事件

有害程序事件(Malware Incidents，MI)是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序。有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，影响信息系统的正常运行。其中包括如下 7 个子类：

(1) CVI——计算机病毒事件(Computer Virus Incidents)。

(2) WI——蠕虫事件(Worms Incidents)。

(3) THI——特洛伊木马事件(Trojan Horses Incidents)。

(4) BI——僵尸网络事件(Botnets Incidents)。

(5) BAI——混合攻击程序事件(Blended Attacks Incidents)。

(6) WBPI——网页内嵌恶意代码事件(Web Browser Plug-Ins Incidents)。

(7) OMI——其他有害程序事件(Other Malware Incidents)。

1.5.2 网络攻击事件

网络攻击事件(Network Attacks Incidents,NAI)是指通过网络或其他技术手段,利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击,并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件。其中包括如下7个子类:

(1) DOSAI——拒绝服务攻击事件(Denial of Service Attacks Incidents)。

(2) DBAI——后门攻击事件(Backdoor Attacks Incidents)。

(3) VAI——漏洞攻击事件(Vulnerability Attacks Incidents)。

(4) NSEI——网络扫描窃听事件(Network Scan & Eavesdropping Incidents)。

(5) PI——网络钓鱼事件(Phishing Incidents)。

(6) II——干扰事件(Interference Incidents)。

(7) ONAI——其他网络攻击事件(Other Network Attacks Incidents)。

1.5.3 信息破坏事件

信息破坏事件(Information Destroy Incidents,IDI)是指通过网络或其他技术手段,造成信息系统中的信息被篡改、假冒、泄露、窃取等而导致的信息安全事件。其中包括如下6个子类:

(1) IAI——信息篡改事件(Information Alteration Incidents)。

(2) IMI——信息假冒事件(Information Masquerading Incidents)。

(3) ILEI——信息泄露事件(Information Leakage Incidents)。

(4) III——信息窃取事件(Information Interception Incidents)。

(5) ILOI——信息丢失事件(Information Loss Incidents)。

(6) OIDI——其他信息破坏事件(Other Information Destroy Incidents)。

1.5.4 信息内容安全事件

信息内容安全事件(Information Content Security Incidents,ICSI)是指利用信息网络发布,传播危害国家安全、社会稳定和公共利益内容的安全事件。其中包括如下4个子类:

(1) 违反宪法和法律、行政法规的信息安全事件。

(2) 针对社会事项进行讨论、评论,形成网上敏感的舆论热点,出现一定规模炒作的信息安全事件。

(3) 组织串连、煽动集会游行的信息安全事件。

(4) 其他信息内容安全事件。