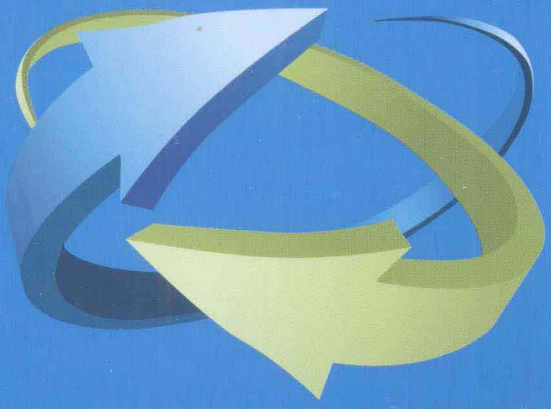
[美] Jason Andress

ELSEVIER
爱思唯尔

信息安全技术概论

The Basics of Information Security

孙建国 夏松竹 王让 译



国防工业出版社
National Defense Industry Press

信息安全技术概论

The Basics of Information Security

Jason Andress 著

孙建国 夏松竹 王 让 译

安徽大学图书馆 藏书 www.lib.ahu.edu.cn

国防工业出版社

·北京·

著作权合同登记　图字:军-2011-164号

图书在版编目(CIP)数据

信息安全技术概论/(美)安德斯(Andress,J.)著;孙建国,
夏松竹,王让译.—北京:国防工业出版社,2013.4
书名原文:The basics of information security
ISBN 978-7-118-08667-6

Ⅰ.①信...　Ⅱ.①安...②孙...③夏...④王...
Ⅲ.①信息安全-安全技术　Ⅳ.①TP309

中国版本图书馆 CIP 数据核字(2013)第 074658 号

Translation from the English Language Edition:
The Basics of Information Security by Jason Andress.
ISBN 978-1-59749-653-7
Copyright © 2011.
All fight reserved. This translation published under Elsevier Inc.. No part of this book may be reproduced in any form without the written permission of the original copyright holder.
本书中文简体版由 Elsevier Inc. 授权国防工业出版社独家出版发行。未经出版者书面许可,不得以任何方式复制或抄袭本书之部分或全部内容。

※

国防工业出版社出版发行
(北京市海淀区紫竹院南路23号　邮政编码100048)
北京嘉恒彩色印刷责任有限公司
新华书店经售
*
开本 710×960　1/16　**印张** 9¼　**字数** 161 千字
2013 年 4 月第 1 版第 1 次印刷　**印数** 1—3000 册　**定价** 24.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776
发行传真:(010)88540755　　发行业务:(010)88540717

关于作者

杰森·安德斯(信息系统安全架构专家，国际知名信息安全专家，费城环境网络顾问，道德骇客资格认证)是一位在学术和商业领域都有丰富经验的信息安全专业人士。他目前受聘于一家大型软件公司，该公司主要提供全球信息安全监督，并进行网络渗透测试、风险评估以及审计，以确保商业资产安全。

自 2005 年以来，杰森就开始教授本科生和研究生的信息安全课程。他拥有计算机学科的博士学位，从事数据安全保护领域的科学研究。他撰写了一系列刊物和书籍，内容包括数据安全、网络安全、渗透测试和电子取证。

关于技术编辑

拉斯·罗杰斯(国际注册信息安全专家,注册信息安全员,国际机械师协会智能能源管理理学博士),畅销书《骇客攻击恐怖网络》(桑格斯,ISBN 1-928994-98-9)的作者以及多部知名网络信息安全书籍的合著者,包括最畅销的《窃取网络:如何拥有一个大陆》(桑格斯,ISBN 1-931836-05-1)和《使用智能能源管理的国家安全局的网络安全评估》(桑格斯,ISBN 1-597490-35-0);曾担任《信息安全杂志》主编。目前,拉斯是一个联邦机构的渗透测试员,最高安全有限公司的创始人和首席执行官,这是一个资深的私有企业,其总部设在科罗拉多州斯普林斯。自1980年以来,拉斯一直从事信息安全技术工作,并担任了近20年的信息安全顾问。他曾与美国空军(USAF)、国家安全局(NSA)、国防信息系统局(DISA)和其他联邦机构合作。他是一个全球知名的信息安全专家、演讲者和作家,出席了世界各地的相关学术会议,包括阿姆斯特丹、东京、新加坡、阿布、迪拜和美国各主要城市。

拉斯已经获得先进科技大学信息技术科学荣誉博士学位、美国马里兰大学计算机系统管理硕士学位、计算机信息系统学士学位,空军社区学院应用通信技术准学士学位。他目前正在攻读位于科罗拉多州斯普林斯的科罗拉多大学的电气工程科学学士学位。他是国际社会保障协会和国际软交换协会(ISC)的成员。他还任教于先进科技大学,教授网络安全课程(http://www.uat.edu)。

拉斯想要感谢这么多年来一直支持他的孩子们,他的父亲和崔西。同时,他诚挚地感谢以下人员:克里斯·赫尔利、马克·凯里、罗布·巴瑟斯特、图丁、保罗·克里斯科洛、平·卢克、格雷格·迈尔斯、瑞安·克拉克、卢克·麦科米、柯蒂斯·奈森和埃迪·迈兹。

此为试读,需要完整PDF请访问: www.ertongbook.com

前 言

无聊、无聊、无聊。这难道不是我们阅读有关信息安全基本概念的书时立刻跳入脑海的感觉吗？单调的理论叙述、枯燥的技术细节、过于简略又不足以概括每个基本论题的叙述，即便你知道你永远不会受聘于国家安全局做一个专业级的密码员，但这仍然是无法容忍的。你可能仅仅需要一本让你每隔三十分钟就会睡着的书，但绝不能是五分钟。这难道是不可避免的“悲剧”吗？不，至少我的信息安全著作不会。

那么，诚实一些。难道你真的要从事信息安全的工作，而不仅仅是一种爱好吗？是否有其他的原因让你阅读这本书？和你们大多数一样，我并不知道（而且有时仍然好奇这一天的到来）自己长大后想做什么。那么，为什么要阅读这本书呢？是什么促使我对信息安全领域有如此大的兴趣呢？它能否帮助我学习基础知识并且推动我的事业走上正确方向呢？

当我儿子四岁时，我带他去了我家一条街以外的公园。在那里，有些小孩在打棒球，另一些孩子在丛林中追赶嬉戏，还有一些在爬攀岩墙。同时，他看到了在公园玩滑板的男孩子们。他自己也有一个滑板，但从来不知道可以那么玩。理所当然的，他立刻想试试那个滑板了。作为一个负责任的父亲，我不能让他仅仅是为了结束这种无意识的青春期冲动，就让他从一个六英寸的斜坡上滑下来。我可以做的是，要求他向我展示一下他会的那些基本动作，比如站在滑板上在我家车道上滑。作为回报，他可以去公园玩滑板。有一次，当他在车道上滑行时，他感到不那么舒服了，于是他坐着从斜道上滑下来。最终，他决定了自己的道路，制定了自己的目标，控制了达到目标的时间。

他的道路与那天在公园玩的孩子们都不一样。但是，想象一下，如果我们从没去过那个公园呢？如果他只看到一个被投掷的棒球和无止境的奔跑呢？如果他根本没看到那个滑板，更不用说那些小孩的空中技巧？知道什么是可能的，能够大大地改变一个人的命运。而且这个道理也适用于从事信息安全研究的

工作。

简单地想要一个信息安全方面的职位，不是具体地能够在一个如此与其他行业相接触的行业中传达所有的可能理念。安德斯博士所做的，除了给你稳定的理论基础之外，更是碰撞你的思想火花。正是那些火花可以拥有职业忠告的“计划内”结果。他是怎么做到的呢？他巧妙地融合、搜集、查阅了许多感性的课题（再次，诚实地，让大多数人首先接近和了解信息安全世界），同时向我们展示，它有空间能够容纳整个信息安全所覆盖的各类问题，而不只是坚持于那些经过试验的、实际的，用来表达信息并要求死记硬背的课堂知识。因此，他以对未来可能性的惊鸿一瞥来避免过多的繁缛，不再仅仅介绍所要求的理论知识，例如：

他第三章授权和访问控制中，将跨站请求、身份伪造、数据窃取的例子引入，以便讨论非常抽象的代理问题。

在第四章审计和责任承担中，他纵观各种评测，渗透测试以及二者之间的差异。这是一个在很多介绍信息安全的书籍中都不曾出现的重要概念。

第五章密码学主要是建议读者自己尝试着做分析机，破译第二次世界大战中德国的经典密码。

第八章网络安全和第九章操作系统安全，让读者不仅仅可以阅读到基本概念，而且会看到骇客工具的实际运行截图。例如，主界面的操作菜单、无线嗅探器、扫描器、图形界面等。

我不清楚为什么杰森会请我，一个网络骇客杂志的首席编辑来给一本有关信息安全方面的书做前言，而事实上是引言。但是，当我读了这本书并最终理解了上述例子后，我终于明白杰森不仅有想要分享他所掌握的信息安全知识的真诚愿望，而且想要传授一个骇客的思考模式。总之，骇客是一个什么事情都会独立完成的人。骇客会情不自禁想要对他关注的事物进行探索和获取，不管是一辆车、一个烤箱、一台计算机，或者是一个网络系统。如果你能够掌握杰森在书中展示的思维模式的一半，你在以后的路途上就可以走得更顺利。

令人兴奋!!! 在这条道路上的每一个脚步，杰森都用他宝贵的实践经验和知识加以点缀，使得那些基础课题闪耀出光芒。这样做，他不仅启发了读者，而且巧妙地帮助你确定了你的信息安全职业生涯之路。某些个案会吸引你的眼球，很多例子会使你加以记录并进行深入探索。更多的时候，你会感觉情不自禁地想要放下书，然后总结一下到底学习和掌握了些什么。如果杰森令你按照这本书所描述的某个知识点做了，请花点时间思考一下是什么令你思维活跃起来。

这是一个里程碑，这也许是一个事业即将来临的标志，请不要轻视它。我知道如果你同他在一个课堂学习的话，他不会让你那样做的。

那么，你们还在等什么呢？钻进这本书里，汲取你所需要的知识，找到属于你自己的骇客模式，同时发掘你的激情。

祝你们好运！

唐纳德 C. 唐扎

国际注册信息安全专家

微软系统工程师

国际注册信息安全专家

微软公司系统工程师

目 录

第一章　信息安全概述

本章信息

- 什么是信息安全
- 讨论安全问题的模型
- 攻击
- 纵深防御

引言

信息安全是一个在很大程度上几乎无处不在的计算技术，是一个与社会各个方面都息息相关的概念。在日常生活中，大多数人都用电脑为雇主工作，在家用电脑上玩游戏，接受远程教育，在网上买东西，带着笔记本电脑到咖啡店收发电子邮件，将智能手机放在裤兜里并使用它们来查询银行结余，用鞋中传感器跟踪记录运动情况，等等，循环往复。

虽然这项技术使生活能够更有效率，并且只需点击一下鼠标就可以访问主机信息，但它也带来了主机的安全问题。如果雇主或银行所使用的系统信息暴露给一个攻击者，其后果是可怕的。我们可能会发现自己资金突然丢失，在半夜资金从银行账户转移到另一个国家的某个银行账户上。雇主可能因为系统配置问题使攻击者轻而易举地访问到包含个人识别信息（PII）或专有信息的数据库，而为此造成数百万美元的损失，遭受法律诉讼，并且信誉受到损害。日常生活中，我们看到类似问题被媒体频繁地报道。

回顾30年前，这些计算机系统问题几乎不存在，这主要是因为当时技术水平低而且很少有人运用到位。尽管技术发展越来越快，并在一个看似日常的基础上得以具体实施，但存在争议的是：如何改变信息安全技术以慢得多的步伐变化，且没有始终保持与技术革新相一致。如果能够更好地认识信息安全基础，那么将拥有一个强大的环境以应付技术革新带来的挑战。

什么是信息安全？

根据美国法律[1]，信息安全被定义为“保护信息和信息系统不受未经授权

的访问、使用、披露、修改或破坏”。从本质上讲，它意味着保护数据和系统不被滥用。

在一般意义上，信息安全意味着资产得到安全保护，使其远离可能的攻击者对网络的入侵，避免自然灾害、介质损坏、电源故障、盗窃或破坏，以及其他不良状态。最终，考虑到系统的实际运行环境，要确保系统在最有可能的攻击条件下的信息安全，并达到最佳效果。

当仔细研究所需要保护的安全内容时，我们可能会看到一个范围更加广泛的潜在资产。此时，需要考虑那些想要保护的物质项目，例如，有价物品（如黄金），或那些对业务有价值的东西（如计算机硬件）；也可能需要保护一些虚拟项目，如软件、源代码或数据。在当今的计算机环境下，我们可能会发现，逻辑资产往往与实物资产一样具有不可替代的重要价值。此外，还必须保护业务所涉及的人，他们是最宝贵的资产，因为没有他们，就无法开展业务。我们可以复制虚拟和逻辑资产，保存他们的备份副本以避免不幸事件发生，但如果没有专业人员的维护，系统运行环境会迅速崩溃。

在保护资产的过程中，还必须考虑选择实施安全措施的后果。有一个著名的引述说道，“唯一真正的安全系统是那种已断电，浇筑在一个混凝土里，并密封在铅衬里，放入一个配备武装警卫的房间中，即使这样我仍有怀疑”[2]。虽然可以肯定地说，在这样一个状态下的做法可以被认为是相当安全的，但这肯定是不实用的。当提高安全水平时，我们通常会降低生产力水平。如引述中提到的系统，安全水平将非常高，但生产力水平则将接近于零。

此外，当保护资产、系统或环境时，还必须将安全水平同所保护项目的价值结合起来考虑。如果愿意适应性能下降，我们可以对所负责的资产采取安全性非常高的措施。可以建立一个被铁丝网包围的耗资 10 亿美元的设施，由武装警卫和凶猛的警犬巡逻，将资产精心放置在一个密封的地下室内……从而让妈妈的巧克力曲奇配方绝不受到伤害，但这没有太大的意义。然而，在某些环境中，这样的安全措施可能还不够。在计划提高安全水平的情况下，我们需要考虑到资产万一丧失的更换成本，并建立合理的保障水平，安全成本不应该超越其所保护资产的价值。

何时才是安全的？

准确界定什么是安全的确是一个挑战。如果系统被正确地修补了，就是安全的吗？如果使用强密码，就是安全的吗？如果与互联网完全断开，就是安全的吗？从一定的角度看，对所有这些问题都可以回答“不是”。

即使系统被正确地修补，也总是会有新的攻击使其变的脆弱。当使用强密

此为试读，需要完整PDF请访问：www.ertongbook.com

码时，攻击者还会有其他可以利用的途径。从互联网上断开，系统可以在物理上被访问或入侵。总之，要确定何时才真正安全是非常困难的。然而，我们可以反过来看这个问题。确定何时是不安全的，是一个容易很多的任务，并且可以快速列表，以显示不安全状态的项目：

- 不给系统打补丁。
- 使用弱密码，如“密码”或“1234”。
- 从互联网下载程序。
- 打开来自未知发件人的电子邮件附件。
- 使用不加密的无线网络。

我们可以创建这样一个列表，而且持续很长时间。好处是，一旦能够指出在环境领域内的不安全因素，我们可以采取一些措施来减轻这些问题。这个问题类似于不断地将东西对半切割，总是会剩下一些小部分需再次切割。虽然我们可能永远不会达到一个所谓的完美“安全”状态，但可以朝着这个正确的方向不断采取措施。

注意！

定义信息安全标准的法律机构，从一个行业到另一个行业，从一个国家向另一个国家颇有几分变化。在全球范围内运行的组织目前是很常见的，而且需要注意，在开展业务的过程中他们没有违反任何法律。审视美国和欧盟数据隐私法之间的差异时，我们可以清楚地看到这种情况。如有疑问，可以在实施前咨询法律顾问。

一些法律法规机构曾试图界定什么是安全，或至少一些确保“足够安全”的措施。我们拥有为使用信用卡付款的企业制定的支付卡行业数据安全标准（PCI DSS），为处理健康护理和病人病历的组织于 1996 年制定的健康保险便携性与责任法案（HIPAA），为许多美国联邦机构制定的定义安全标准的联邦信息安全管理法案（FISMA），等等。这些标准是否有效引起了许多讨论，但随之也出现了为很多需要进行身份授权的行业制定相应安全标准的需求。

讨论安全问题的模型

当讨论安全问题时，使用一个模型作为基础或基准往往是有益的。这能为信息安全专业人员，提供一系列的研究安全问题时可以参考的术语和概念。

保密性、完整性、可用性三元组

信息安全的三个基本概念是保密性、完整性和可用性，俗称保密性、完整性、可用性(CIA)三元组，如图 1.1 所示。保密性、完整性、可用性三元组提供了一个可以思考和讨论安全问题的模型，模型趋于非常注重安全性，因为它涉及到具体数据。

更高级的

保密性、完整性、可用性三元组的通用符号。在某些材料中，主要是由 ISC^2 发展而来的，我们可能会看到略微重新排列为 CAI。这一重排并没有隐含概念的变化，但对于那些没有事先了解它的人，可能会造成混淆。三元组的概念表达了他们的消极形式：披露、更改和拒绝(DAD)。

保密性

保密性是一个与隐私相似，但不完全相同的概念。保密性是隐私的一个必要组成部分，是指有能力保护数据并防止非授权访问。保密性是一个可以多层次实施的概念。

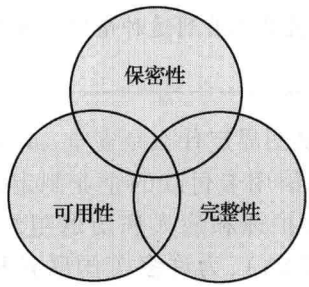


图 1.1　CIA 三元组

例如，考虑一个人从自动取款机取钱的情况，这个人可能会使用支持个人信息保密性的个体识别编码(PIN)，进而从自动取款机提取资金。此外，自动取款机业主则会希望确保账户数量平衡，以及其他任何使资金提取处同银行相联系所需信息的保密性。该银行将保持自动取款机交易，以及资金提取后账户余额变化的保密性。在任何时候，如果交易保密性被破坏，这一结果可能对个体、自动取款机所有者和银行均造成损害，并可能会产生安全领域的缺口。

保密性可能会因为一台笔记本电脑数据的丢失，键入密码时别人偷看，发送到错误地址的电子邮件附件，穿透系统的攻击或类似问题，而引起严重后果并使系统最终受到破坏。

完整性

完整性，是指保护数据不被未经授权或不良的方式改变的能力，即未经授权地更改或删除全部或部分数据的行为，或者经过授权但恶意地更改或删除数据的行为。为了保持完整性，不仅需要有方法来防止未经授权数据更改行为，也需要有能力恢复那些经过授权但因错误操作而引起的变更。

例如，一种控制操作系统中文件系统完整性的机制，如 Windows 和 Linux。为了防止未经授权的更改，这些系统往往实施许可证权限，以此来限制未经授权的用户对一个特定的文件能够执行什么样的操作。此外，一些类似的系统和许多应用，如数据库，可以阻止或回滚不符合要求的数据变更。

当决定为其他用户提供基础数据时，完整性显得尤为重要。例如，如果攻击者改变了包含医疗化验结果的数据，可能会产生导致病人死亡的错误治疗方案。

可用性

三元组的最后一个因素是可用性。可用性是指访问所需数据的能力。可用性的损失可能导致访问数据通路的各种缺口。这些问题可能是由于功率损耗、操作系统或应用程序、网络攻击、系统漏洞或其他问题造成的。当此类问题是由局外人如攻击者造成的，他们通常被称为拒绝服务(DoS)攻击。

保密性、完整性、可用性三元组与信息安全相结合

鉴于保密性、完整性、可用性三元组的联系，可以用一个非常具体的方式开始讨论安全问题。例如，那个承载一些敏感数据副本的、唯一现存的、未加密的备份磁带。如果在运输过程中失去磁带，我们将面临一个安全问题。从保密性角度来看，由于文件是不加密的，信息很可能被直接获取。从完整性角度来看，假设能够恢复一本磁带，但由于缺乏加密的文件，我们仍面临安全问题。如果恢复了磁带内容，而没加密的文件被修改了，结果不会立即显现。从可用性角度来看，因为没有文件的备份副本，除非磁带恢复，否则我们仍会遇到问题。

虽然可以相对精确地描述这个例子中使用保密性、完整性、可用性三元组的情况，但是可能会发现，该模型比我们需要的用以描述整个情况的要求更严格。另一种模式则更为广泛地存在。

帕科瑞六元组

帕科瑞六元组，由唐·帕克命名，并在他的著作《打击计算机犯罪》中予以介绍，为我们提供了一个经典的保密性、完整性、可用性三元组较为复杂的变化。经典三元组包括保密性、完整性、可用性，而帕科瑞六元组不仅包含这三个原则，同时还包括占有或控制、真实性和实用性[3]，共六个原则。如图 1.2 所示。

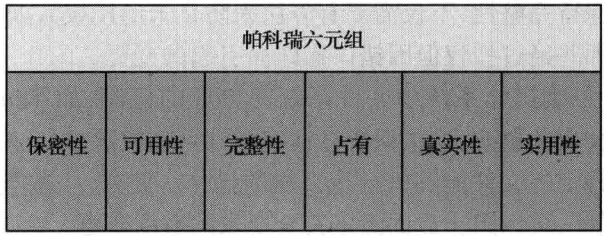


图 1.2　帕科瑞六元组

注意！

虽然它被有些人认为是更完整的模型，但帕科瑞六元组并不如保密性、完整性、可用性三元组那样被广泛认知。如果决定使用这个模型进行安全情况讨论，我们应作好向外行解释其区别的准备。

保密性、完整性、可用性

正如前边提到的，帕科瑞六元组涵盖保密性、完整性、可用性三元组的三个原则，与之前讨论的定义相同。帕克介绍完整性时有一些变化，他不认可“已授权但不正确的数据修改”，而是着重于数据本身的完整状态。

占有或控制

占有或控制，是指数据存储媒体的物理配置。这不涉及其他因素，如可用性，而仅讨论其物理介质中的数据丢失。在失去的备份磁带中，假设其中的一些数据被加密而另一些没有。依照占有的原则，能够更准确地描述事件的范围；很多数据被加密的磁带是一个占有问题而不是一个保密性问题，不加密的磁带在这两个方面都是难题。

真实性

真实性是指问题数据的适当归属，即雇主或创作者。例如，如果发送的电子邮件被改变了，那么该电子邮件显示的将不再是原地址，则电子邮件的真实性被侵犯了。通过使用数字签名，真实性可以被强制保护和验证，有关问题将在第五章进一步讨论。有一个相似但是截然不同的概念，就是认证，即防止有人采取相同行为发送电子邮件，但又否认这一行为。这一概念也会在第五章深入讨论。

实用性

实用性，是指数据的用途。实用性也是唯一的属于帕科瑞六元组中不由两部分组成的原则；可以定义多种实用性等级，这取决于数据及其格式。实用性是一个很抽象的概念，但它在研究信息安全领域的某些情况时确实非常有用。例如，在前面一个例子中，我们有一些备份磁带，其中一些加密而另一些没有。对于一个攻击者或其他未经授权人来说，加密的磁带很可能只有很小的实用性，因为数据无法读取。而未加密的磁带将有更大的实用性，因为攻击者或未经授权人能够访问数据。

攻击

可能会面临各种方法和方式的攻击。当研究攻击的构成时，我们可以根据它的类型、风险，并采用相应的控制和应对手段来加以防御。

攻击类型

对于可能面临的攻击类型时，可以大致将它们分为四类：拦截、中断、修改和仿制。每个类别可以影响一个或多个有关保密性、完整性、可用性三元组的原则，如图 1.3 所示。此外，攻击的类别及其特定效果之间的界限有点模糊。对于一个讨论的攻击，可能不止一种类型，或是多个类型叠加的效果。

拦截

拦截攻击是指未经授权的用户访问数据，应用程序或运行环境，主要是对保密性的攻击。拦截的形式可能有未授权查看或复制文件，窃听电话交谈或阅读电子邮件，还可以对静止或运动中的数据进行侦听。如果实施方法较好，拦截攻击很难检测。

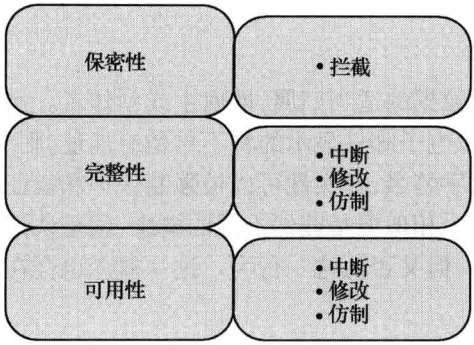


图 1.3　各种类型的攻击

中断

中断攻击则会导致资产临时或永久地无法使用或找到。中断攻击往往会影响可用性，但也可以是对完整性的攻击。如果邮件服务器的磁盘操作系统遭到攻击，会将其列为可用性攻击；当攻击者操纵数据库并进行数据访问时，由于可能发生的数据损失或破坏，这可能是一个完整性攻击或者两者的结合。这种攻击也可能被认为是修改攻击，而不是中断攻击。

修改

修改攻击涉及到篡改资产的问题。这种攻击主要被视为完整性攻击，但也可以视为可用性攻击。如果以未经授权的方式访问一个文件，并改变它所包含的数据，就已经影响到该文件中所包含数据的完整性。然而，如果考虑该文件是一个管理特定服务行为的配置文件，如指导网站服务器工作，这样如果改变了文件内容则可能会影响到服务的可用性。如果继续延伸概念，并且改变了网站服务器文件的配置，如改变服务器处理加密连接点的策略，则可以说这是一个保密性攻击。

仿制

仿制攻击涉及数据、程序、通信或其他类似的系统信息或行为。仿制攻击主要影响完整性，但也可以被认定为可用性攻击。如果在数据库中生成虚假信息，这将被视为仿制攻击。还可以生成电子邮件，也就是俗称的恶意传播软件，例如，系统可能会遭到蠕虫程序攻击。在遭到可用性攻击的情况下，如果产生大量的附加程序、网络流量、电子邮件或任何其他消耗资源的活动，将导致服务器无法处理合法用户的信息，甚至导致系统崩溃。

此为试读，需要完整PDF请访问：www.ertongbook.com