WANGLUO NEIBU WEIXIE YU FANGYU JISHU

网络内部威胁与防御技术

王 辉◎著

河南人民出版社

网络内部威胁与防御技术

王　辉◎著

河南人民出版社

图书在版编目(CIP)数据

网络内部威胁与防御技术 / 王辉著. —郑州 : 河南人民出版社, 2015. 4
ISBN 978-7-215-09451-2

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络-安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 084796 号

河南人民出版社出版发行
(地址:郑州市经五路 66 号　编辑邮箱:313137877@qq.com　电话:65788050)
新华书店经销　　郑州市今日文教印制有限公司印刷
开本 787 毫米×1092 毫米　1/16　印张 21.5
字数 450 千字
2015 年 4 月第 1 版　　2015 年 4 月第 1 次印刷

定价 : 86.00 元

王辉　1975年生，汉族，九三学社社员，博士（后），河南理工大学计算机科学与技术学院副教授，硕士生导师，主要从事计算机网络及网络安全、无线传感器网络等方面的研究。主持或参与完成国防科工委、解放军总装备部等省部级以上科研项目6项，地厅级科研项目5项。目前，承担国家自然科学基金研究项目2项，省部级科研项目1项，地厅级科研项目2项，地厅级精品课程研究1项。荣获省部级科技成果二等奖1项，省教育厅应用成果奖3项，省创新软件设计大赛创意奖1项，省教育厅科技论文奖2项。发表论文50多篇，其中被SCI/EI收录近30篇，主编教材1部。

前　言

随着计算机网络技术的不断发展，计算机给人类经济、文化、军事和社会活动带来更多便利的同时，也带来了相当巨大的安全挑战。信息技术的日益普及和信息安全问题日益发生，这对矛盾问题也越发突出，现代企业信息系统面临着各种各样的安全威胁，包括来自系统外部的攻击，以及来自系统内部的威胁。列宁曾经说过，堡垒最容易从内部攻破。世界头号黑客凯文·米特尼克提出的社会工程学方法也正是通过利用、影响和蒙骗内部人员实施攻击的。

和比较成熟的外部攻击检测技术相比，网络内部威胁的分析与检测技术仍处于研究阶段，尚无成熟的产品出现；现有用来保护信息系统免受外部威胁攻击的控制方法与安全工具对于网络内部威胁收效甚微。日前，如何对信息系统的网络内部威胁进行检测和预防，已引起了信息安全领域专家的高度重视，成为了一个新的研究热点。

本专著由国家自然科学基金项目“采用属性基代理重加密机制的敏感数据安全管理关键技术研究”（项目编号61300216），国家教育部重点实验室开放基金项目“军事信息网络中的内部威胁及防御技术研究”（项目编号421060711421），河南省教育厅自然科学基金项目“基于内部威胁的安全体系结构关键技术研究”（项目编号2011B520015），河南省社科联项目“信息资源安全保障研究”（项目编号SKL－2012－849）和河南理工大学博士基金项目“内部威胁安全体系结构及关键技术研究”（项目编号B2010－61）的研究成果凝练而成。

本书从基础篇、理论篇和技术篇三部分循序渐进地分析了网络内部威胁理论知识和防御技术。基础篇通过深入分析国内外官方发布的信息安全调研报告的有关资料和数据，给出了网络内部威胁相关的认识和感悟，并对代表性 Insider Threat 分类和典型模型进行剖析。理论篇从 Insider Threat 安全防御体系结构、Insider Threat 安全策略、Insider Threat 安全需求工程与风险管理三个角度进行了分析研究，并给出有关研究成果。

技术篇主要介绍攻击图和贝叶斯理论有关的技术方法来预防网络内部威胁，对网络内部威胁的技术检测机制进行了有益的探索，着重分析贝叶斯推理技术来检测威胁，并给出自己有关的研究成果。

本书由河南理工大学王辉独著，著者及其相关团队紧密配合，深入研究，在许多国内外热点和前沿研究问题上，勇于面对挑战，攻克了许多难点，取得了一系列创新型研究成果。为此，衷心感谢研究团队在研究项目中所做出的学术贡献，也感谢河南理工大学计算机科学与技术学院领导对本书的出版给予了大力支持。

作为新兴领域的一部专著，难免有疏漏之处，敬请读者指正。

王　辉

2014 年 12 月

于河南理工大学计算机科学与技术学院

目 录

基 础 篇

理　论　篇

技　术　篇

基　础　篇

第一章 绪 论

第一节 研究背景

计算机网络的飞速发展大大改变了人们的生活方式，并使人类进入了信息时代。人们通过计算机网络可以方便地存储、交换及搜索信息，给工作、生活带来了极大的方便。然而因为计算机信息有共享和易于扩散等特性，它在处理、存储、传输和使用上有着严重的脆弱性，很容易被干扰、滥用、遗漏和丢失，甚至被泄露、窃取、篡改、冒充和破坏，因此使得网络安全问题日渐突出，而且情况也越来越复杂。

媒体连篇累牍的关于黑客入侵的报道，在引导人们增强信息安全意识的同时，也把人们的注意力强烈地导向到重视防范来自外部的信息安全威胁。这固然是重要的，但却是片面的。对信息安全保障的威胁，只来自“内”“外”两个方面，而且外因通过内因起作用，“堡垒”最容易从内部攻破。①

近几年，来自网络内部的安全事件不断见诸报端，如公司的职员或前雇员由于遭到解雇，工作未得到认可，职位未得到升迁，或者被降职等原因引发网络内部攻击；内部人员安全意识淡漠，如可能违反公司规定，私自绕过防火墙玩网络游戏、浏览网页等，不知不觉中为黑客打开了后门，破坏了网络安全；甚至还有高层管理人员，试图带着公司重大机密数据跳槽。无论是有意还是无意，危害内网安全都可能会造成损失，如个人隐私泄漏、金融资产损失、国家机密泄漏等。特别是来自组织内部人员的恶意攻击，由于他们对组织内部情况了解甚多，熟知内部系统存在的安全弱点，因此所造成的损失往往也

① 赵战生、左晓栋：《“攘外”勿忘“安内”——谈 insider 威胁研究(上)》，《网络安全技术及应用》2001 年第 9 期。

是致命的。最近,在美国联邦调查局和计算机安全协会对企业和政府机构的调查中,90%的被调查者称,过去12个月中计算机安全系统遭受过破坏。这些破坏给80%的受访者造成财务损失。根据权威市场调查机构Gadner Research的调查,损失金额在5万美元以上的攻击中,70%都涉及网络内部攻击。[①] 英国高技术犯罪研究中心进行的类似调查也显示,有38%的金融诈骗案是由内部安全隐患所引起的。

列宁曾经说过,堡垒最容易从内部攻破。世界头号黑客凯文·米特尼克[②]提出的社会工程学方法也正是通过利用、影响和蒙骗内部人员实施攻击的。2007年,法国兴业银行(Societe Generale)的前厅交易员杰洛米·科维尔利用职权使用伪造的账户秘密进行投机交易,最终导致该银行损失约71.6亿美元。随着企业将安全防御系统构筑得越来越强大,通过拉拢内部人员来窃取敏感数据必然比创建新的恶意软件要更容易,这也进一步加快了网络内部威胁(Insider Threat)的增长速度。2010年的Verizon数据泄漏调查报告[③]显示,内部原因造成的数据泄漏较上一年增加了两倍多,达到46%。该报告预计这种趋势在2011年将会保持下去,网络内部威胁将会成为下一个重要的攻击来源。

随着Insider Threat的日益加剧,它已经逐渐体现出了危害大、难抵御、难发现的特点。

(1)内部人员最容易接触敏感信息,并且他们的行动最具有针对性,危害的对象往往是机构最核心的数据、资源等。

(2)一般说来,各机构的信息安全保护措施都是针对防外设计的,而不是针对内部设计的,比如很多公司赖以保护其安全的防火墙,对内部人员的攻击毫无作用,形同虚设。

(3)内部人员对一个机构的运作、结构、文化等情况非常熟悉,导致他们活动时不易被发觉,事后也难以发现。

(4)现实中很多企业即使发现内部人员犯罪,一般也会从公司的声誉着想,对其犯罪员工要么重金收买,要么将其辞退,很难从根本上制止网络内部威胁的发生,甚至纵容其进一步的发展。

对于企业组织而言,一方面,Insider Threat问题将作为一个无法回避的问题永远存在;另一方面,它还涉及经济价值问题,还关乎企业的名誉和形象工程。然而,Insider Threat的研究尚处于起步阶段,针对网络内部威胁的这些特点,如何建立完整的网络内

---

① 刘国玉:《内部安全威胁》,《中国信息界》2004年第20期。

② K. D. Mitnick, W. L. Simon, S. Wozniak. "The Art of Deception", *John Wiley & Sons*, 2002.

③ W. Baker, M. Goudie, A. Hutton, et al. "2010 Data Breach Investigations Report", Tech. rep., *Verizon RISK Team in cooperation with the United States Secret Service*, 2010.

部威胁检测和响应机制，如何对网络内部威胁进行定性和定量分析，如何能够实时掌握网络内部威胁的态势都是我们迫切需要解决的问题。

和比较成熟的外部攻击检测技术相比，网络内部威胁的分析与检测技术仍处于研究阶段，尚无成熟的产品出现；现有用来保护信息系统免受外部威胁攻击的控制方法与安全工具对于网络内部威胁收效甚微。目前，如何对信息系统的网络内部威胁进行检测和预防，已引起了信息安全领域专家的高度重视，成为了一个新的研究热点。

第二节 网络内部威胁的有关概念

在内部威胁研究领域中，提出了许多相关术语的定义，如 Insider、Insider Attack、Insider Misuse、Insider Threat。这里，除了探讨相关定义外，还将探讨它们之间的联系。特别声明的是，目前尚没有官方统一的定义，所探讨的定义均为相关领域专家、学者们所提出的。

在探讨术语“Insider Attack”“Insider Misuse”和“Insider Threat”之前，很有必要先来解释一个基本概念，什么是“Insider”。“Insider”中文意译为内部用户。Magklaras 在他的论文中，给出了“Insider”的解释。“Insider”是指这样一类人，他们是通过合法的途径，被授予访问一个或多个 IT 基础设施组成部分的访问权限，并能通过一个或多个验证机制的确认。[①] 这里，要特别注意一个特殊词汇——“合法”，它强调了内部用户与外部的解密入侵者之间的区别。

术语“Insider Attack”的含义是什么呢？参照中文词汇，“Insider Attack”可以意译为内部攻击。Tugular and Spafford[②] 给出了相关解释，内部攻击者是这样一类人，他们能够凭借所赋予的授权级别使用计算机系统，但是却在做违反自身企业组织安全策略的事情。依据 Schultz and Shumway 提出的定义，内部攻击是指那些被认为有意地误用或滥用计算机和网络的合法授权用户。[③] 依据 Einwechter 的观点，内部攻击者就是被信任并有访问权限的人们，他们不是履行所分配的职责，而是对所操纵的系统访问权限进

---

① G. B. Magklaras, S. M. Furnell. “A preliminary model of end user sophistication for insider threat prediction in IT systems”, *Computers and Security*, Vol24, No. 5, 2005.

② T. Tuglular, E. H. Spafford. “A Framework for Characterization of Insider Computer Misuse”, *Purdue University*, 1997.

③ E. E. Schultz, R. Shumway. “Incident response: A strategic guide for system and network security breaches”, Indianapolis: New Riders, 2001.

行利用,如进行破坏和信息的窃取等。①

术语“Insider Misuse”指的是什么呢?“Insider Misuse”在本文中意译为内部滥用。“Insider Misuse”与“Insider Attack”相似点在于,它们的主体都是企业组织中拥有计算机和网络使用权限的合法授权用户,都是被信任并有访问权限的内部人员。不同点在于,它们的动机是不同的,“Insider Attack”是一种有意识地误用、滥用或攻击,而“Insider Misuse”是一种无意识地误用或滥用。

现在,来探讨一下术语“Inside Misuse”的定义,“Insider Threat”对应中文词汇可以意译为内部威胁。内部威胁就是指威胁来自于对信息系统(IS)具有访问权限并滥用或误用(Misuse)这些权限,因而违背了组织安全策略的人。② 逻辑上,“Insider Threat”覆盖了“Insider Attack”和“Insider Misuse”两层含义,是两者的并集,如图 1 - 1 所示。

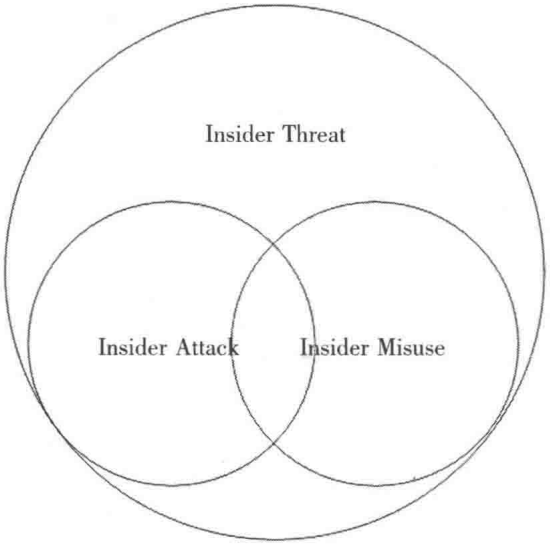

图 1 - 1 Insider Threat 与 Insider Attack、Insider Misuse 关系图

然而,实际上“Insider”的含义是十分复杂的。“Insider”通常包括自身企业的员工、合同工、顾问、临时员工,甚至包括第三方的商业伙伴以及他们的合同工、顾问等等。并且随着外购软件或设备的发生,在“Insider”和“Outsider”之间,越来越难保持一个快速和严格的区分。例如,如果一个攻击事件是由以前的员工利用原先的授权发起的,那么

① N. Einwechter. “Preventing and detecting insider attacks using IDS”, *Security Focus*, 2002.

② M. Theoharidou, S. Kokolakis, M. Karyda, et al. “The insider threat to information systems and the effectiveness of ISO17799”, *Computers and Security*, Vol. 24, No. 6, 2005.