第33卷 第10期 计 算 机 工 程 2007年5月
Vol.33 No.10 Computer Engineering May 2007
·安全技术· 文章编号：1000—3428(2007)10—0128—03 文献标识码：A 中图分类号：TP393.08

计算机网络安全应急响应技术的分析与研究

刘宝旭[1]，马建民[2]，池亚平[3]
(1. 中国科学院高能物理研究所计算中心，北京 100049；2. 中国科学院研究生院，北京 100049；3. 北京电子科技学院，北京 100070)

摘 要：结合实际工作经验和研究成果，在分析安全应急响应技术发展动态的基础上，对网络入侵检测、事件隔离与应急恢复、取证、网络陷阱及诱骗等应急响应关键技术进行了分析和研究。构建了一个网络安全应急响应系统，并对系统的工作机制进行了分析。
关键词：应急响应；事件隔离；入侵检测；取证；陷阱

Analysis and Research About Computer and Network Security Emergency Response Technologies

LIU Baoxu[1], MA Jianmin[2], CHI Yaping[3]
(1. Computing Center, Institute of High Energy Physics, Chinese Academy of Sciences, Beijing 100049; 2. Graduate School, Chinese Academy of Sciences, Beijing 100049; 3. Beijing Electronic Science and Technology Institute, Beijing 100070)

【Abstract】 Based on the analysis of the development trend about computer network security emergency response technologies, this paper researches the emergency response key technologies such as intrusion detection, incident isolation, emergency restore, forensic, networked trap and entrapment technology, and draws relevant conclusion. An emergency response system is designed and its work mechanism is analyzed.
【Key words】 Emergency response; Incident isolation; Intrusion detection; Forensics; Trap

美国计算机紧急响应小组(US-CERT)发布的数据显示，2005年安全研究人员共发现了5 198个软件漏洞，与2004年相比增长38%。这些软件漏洞被黑客、病毒等利用，造成大量安全事件和严重损失。据CERT的报告，计算机安全事件从1988年的6次飞速增加到2003年的137 529次，增加了20多万倍。2004年底，CNCERT/CC发现了一个被黑客通过网络蠕虫集中控制的、近10万个节点的僵尸网络(Bot net)，对网络构成了严重威胁。

因此，如何使人们正确面对并消除网络威胁成为一个迫切需要解决的问题，各类网络安全应急响应技术也应运而生。

1 网络安全应急响应技术的发展

信息安全应急响应技术的出现，源自于1988年的“莫里斯蠕虫事件”。该事件的发生，催生了世界上第1个计算机应急响应小组CERT的建立，从此也开始了每年一度的世界级网络安全事件响应技术论坛(FIRST 年会)，网络安全防护技术的研究也逐渐从注重静态防护向注重动态防护转变。截至2005年，CERT/CC共处理了2 031 678 封E-mail，23 768个热线电话，收到了319 992份安全事件报告、2 437起漏洞报告，帮助了80多个CERT组织的建设，在计算机应急响应领域发挥了很大的作用。到了20世纪90年代中期，美国防部提出了信息保障的概念，并给出了PDRR动态防护模型。从此，应急响应研究得到了较为广泛的发展。到目前为止，全球已有数百个应急响应组织。国内由于信息技术发展相对落后，应急处理和响应机制距世界先进水平还有差距。

2 网络安全应急响应技术

计算机网络安全应急响应是一门综合性的技术学科，技术要求较高，是对突发安全事件进行响应、处理、恢复、跟踪的方法及过程，几乎与计算机网络安全学科内所有技术有关。主要包括：

(1)操作系统加固优化技术

操作系统是计算机网络应用与服务的基础，只有拥有安全可靠的操作系统环境才能确保整体系统的安全稳定运行，操作系统的加固优化可通过两种途径实现：1)将服务和应用建立在安全级别较高(如B1级)的操作系统上；2)不断完善现有的操作系统，通过自我学习、自我完善，不断修正操作系统中被发现的漏洞，加强对重要文件、重点进程的监控与管理，增强操作系统的稳定性和安全性。

(2)网络陷阱及诱骗技术

网络陷阱及诱骗技术是近期发展起来的一种网络安全动态防护新技术，它通过一个精心设计的、存在明显安全弱点的特殊系统来诱骗攻击者，将黑客的入侵行为引入一个可以控制的范围，消耗其资源，了解其使用的方法和技术，追踪其来源，记录其犯罪证据。不但可研究和防止黑客攻击行为，增加攻击者的工作量和攻击复杂度，为真实系统做好防御准备赢得宝贵时间，还可为打击计算机犯罪提供举证。

蜜罐(HoneyPot)、蜜网(HoneyNet)是当前网络陷阱及诱骗技术的主要应用形式。因为蜜罐蜜网并没有向外界提供真正有价值的服务，所以所有对蜜罐蜜网进行连接的尝试都被视为可疑的。采用的主要技术有：

1)网络欺骗技术。是指在一个严格控制的环境中，利用各种手段，诱骗攻击者对虚构的系统进行攻击，并为攻击者

基金项目：北京电子科技学院开放研究基金资助项目；“973”计划基金资助项目(G1999035806)
作者简介：刘宝旭(1972－)，男，博士、副研究员，主研方向：网络信息安全；马建民，硕士生；池亚平，副教授
收稿日期：2006-05-13 **E-mail：**liubx@ihep.ac.cn

提供其认为可信的对话信息，从而保护实际运行的系统免受攻击，并实现数据收集功能。

2)端口重定向技术。其主要应用方式为：在工作系统中模拟一个非工作的服务功能，将恶意的、未经授权的活动重定向到蜜罐系统中，如在 Web 服务器上，模拟并将 FTP 服务重定向到蜜罐系统中去，从而在网络中虚拟出该工作系统对外提供 FTP 服务。当蜜网网关发现非预期流量、已知攻击或发现被监控主机上有未授权的活动时，便将有关流量重定向到对应的蜜罐中。

3)数据控制技术。是指对蜜罐系统的连接控制和路由控制。防火墙实现连接控制：允许所有外部数据包进入蜜罐，但对蜜罐主机的对外连接进行追踪限制；路由器实现路由控制：防止基于蜜罐主机 IP 的跳转攻击。

4)数据捕获分析技术。获取黑客的所有活动，如攻击者键盘操作、屏幕信息以及曾使用过的工具等，并分析攻击者所要进行的下一步活动。难点在于如何获取尽可能多的数据而又不让攻击者发觉。捕获到的数据也不能存放在蜜罐主机上，应进行异地存储。实现这些要求的关键是分层捕获数据。

(3)阻断技术

主要有 3 种阻断方式：

1)ICMP 不可达响应：通过向被攻击主机或攻击源发送 ICMP 端口或目的不可达报文来阻断攻击；

2)TCP-RST 响应：也称阻断会话响应，通过阻断攻击者和受害者之间的 TCP 会话来阻断攻击。这种机制是目前使用最多的主动响应机制；

3)防火墙联动响应：当入侵检测系统检测到攻击事件后向防火墙发送规则，由防火墙阻断当前以及后续攻击。

(4)攻击抑制技术

在计算机网络应急响应手段中，一种及时主动的应急响应技术就是攻击抑制技术。对于已经发生的信息安全事件，必须立即采取攻击源隔离等有效措施，对其进行抑制，以防止不良后果的继续扩大。攻击抑制是指通过各种技术手段限制攻击的范围，或是在被保护的信息系统在遭受攻击时，采取各种技术手段，有效减少破坏行为。

抑制的目的是限制事件造成影响的范围和程度。是在事件发生的第 1 时间对故障系统或区域实施有效隔离和处理，或根据所拥有的资源状况和事件等级，采用临时关闭受影响系统并将业务切换到备份系统等措施降低损失、避免事件扩散和对受害系统的持续性破坏。抑制一般分为物理抑制、网络抑制、主机抑制和应用抑制。

研究抑制技术有助于在发生突发安全事件时降低或解除攻击的影响，其水平的高低也决定了应急响应效率的高低。主要涉及事件优先级认定、完整性检测和域名切换等技术。

(5)紧急恢复技术

在发生灾难性网络安全事件后可以通过紧急恢复技术进行系统恢复、数据恢复和功能恢复等工作，保持系统为可用状态或维持最基本服务能力。传统方法是采用磁盘镜像或数据备份技术以提高系统的可靠性。主要包括系统攻击可容忍性、网络结构的冗余容错和动态切换、计算机网络系统恢复、计算机远程恢复、计算机网络自修复等方面的研究。

通过应急恢复可以在遭受攻击后实现网络结构修复和重组、主机和服务器的恢复、数据库数据的安全恢复、网络配置的动态备份和快速恢复、网络受损分析与评估。

典型的恢复技术包括漏洞修补、业务连续性保障和灾难恢复等。常用工具有 Networker、ADSM、NetBackup、ARCserver 等。

(6)网络追踪技术

网络追踪技术是指通过收集分析网络中每台主机的有关信息，找到事件发生的源头，确定攻击者的网络地址以及展开攻击的路径。其关键是如何确认网络中的所有主机都是安全可信的，在此基础上对收集到的数据进行处理，将入侵者在整个网络中的活动轨迹连接起来。网络追踪技术可分为主动追踪和被动追踪。

主动追踪技术主要涉及信息隐形技术，如在返回的 HTTP 报文中加入不易察觉并有特殊标记的内容，从而在网络中通过检测这些标记来定位网络攻击的路径。国外已有一些实用化工具，如 IDIP、SWT 等，但基本还处于保密阶段。

在被动式追踪技术方面，已经有了一些产品，主要采用网络纹印(Thumb printing)技术，其理论依据是网络连接不同，描述网络连接特征的数据也会随之发生变化。因此通过记录网络入侵状态下不同节点的网络标识，分析整个网络在同一时刻不同网络节点处的网络纹印，找出攻击轨迹。

(7)取证技术

取证技术是指对存储在计算机系统或网络设备中潜在电子证据的识别、收集、保护、检查和分析以及法庭出示的过程，通常是对存储介质、日志的检查和分析。计算机取证包括物理证据获取和信息发现两个阶段。在应急响应中，收集黑客入侵的证据是一项非常重要的工作。取证技术不但可以为打击计算机、网络犯罪提供重要支撑手段，还可为司法鉴定提供强有力的证据。

1)物理证据获取技术。是指在计算机犯罪现场寻找并发现相关原始记录的技术，是取证工作的基础。在获取物理证据时最重要的工作是保证获取的原始证据不受破坏。关键技术是无损备份和删除文件的恢复：

①无损备份技术。直接在被攻击机器的磁盘上进行取证操作，可能会损坏原始数据，因此，要用磁盘镜像复制的办法，将被攻击机器的磁盘原样复制一份，然后对复制的磁盘进行取证分析。常用工具有 SafeBack、Ghost 等；

②删除文件的恢复技术在目前使用的操作系统中，即使将存储在硬盘的数据进行了删除操作，并清空回收站，数据仍然保留在硬盘上，只要该文件的存储位置没有被重新写入数据，原来的数据就可以恢复出来。常用工具有 Easy Recover、Recover My Files 等。

2)信息发现技术。是指对获得的原始数据(文件、日志等)进行分析，从中寻找可以用来证明或者反驳什么的证据。具体手段有：

①日志分析技术。通过日志分析可以获得某时段 CPU 负荷、用户使用习惯、IP 来源、恶意访问提示等重要信息。常用工具有 NetTracker、Logsurfer、Netlog 和 Analog 等。

②数据捕获分析技术。在发现网络攻击行为后，通过截获和分析入侵者终端发出或者被入侵主机发出的网络数据包，可获得攻击源的地址和攻击的类型方法。常用工具有 TcpDump、WinDump、SNORT 等。

③解密技术。越来越多的计算机犯罪者使用加密技术保存关键文件，隐藏自己进行攻击的记录和操作。为了取得最终的攻击证据，取证人员应能将已发现的文件内容进行解密。

3 网络安全应急响应系统的研究

网络安全应急响应技术是信息安全中较为前沿的一个研究领域。随着研究的深入，突破了原 PDRR 模型的设想，将“响应”和“恢复”两种安全机制有机地结合起来，成为一个较为完善的应急响应系统。本文在继承这种观点的基础上，

提出综合利用上述应急响应技术，充分发挥管理与机制在其中的作用，并不断改进相关规则来构建一个更为理想、完善的应急响应系统。该系统有机地实现了各类安全应急响应技术的联动。其示意图如图 1 所示。

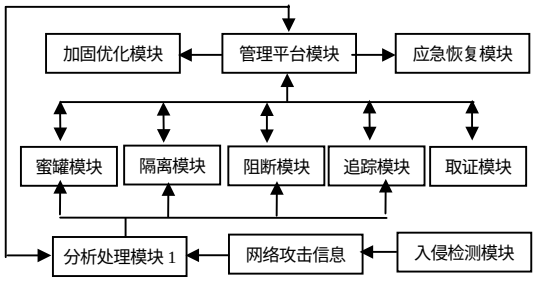

图 1 网络安全应急响应系统示意图

(1)攻击信息分析。由入侵检测模块发现网络攻击，用分析处理模块对收集到的攻击信息进行分析整理，根据预先设定的策略和事件处置规则，在对攻击的危害程度和紧急程度作出基本判断的基础上，形成初步处置方案，并将处置方案和攻击信息通报管理平台。

(2)简单情况处置。依据情况处置方案，对简单的网络扫描或危害性不高的攻击，系统自动启动阻断或隔离模块进行处理，防止发生进一步的网络攻击行为。对危害程度较高的攻击行为，则在启动阻断或隔离模块的同时，将攻击行为引入蜜罐模块中，避免攻击者对真实系统造成危害，并由蜜罐系统记录攻击者的攻击操作，同时调用追踪模块对攻击源进行追踪调查，收集并确定攻击信息。

(3)综合分析处理。管理员通过分析管理平台、蜜罐模块和追踪模块收集到的信息，对自动防护方案进行调整，并可采取进一步的措施，如通过取证模块对攻击现场进行取证，调用加固优化模块及时修补导致攻击的漏洞来防止类似事件的发生，调用应急恢复模块对已被破坏的系统进行各类恢复操作等。

(4)防护规则更新。事件处理完毕后，由管理员对此次的攻击行为及采取的应急防护措施进行综合分析，进一步完善分析处理机制，设定更为合理的防护规则，确保应急防护系统可以对下一次同样的攻击采取更为有效、及时的防护措施。

4 结束语

随着信息化的不断发展，网络安全威胁越来越凸现，为更好应对各种网络攻击、病毒破坏，提高应急响应的及时性和有效性，新的应急响应技术与工具都在不断发展与改进，但实际仍是挑战大于机遇。因诸多非技术层面的问题(如法律、协同响应等)要远大于技术本身的困难，所以，建立一个实时高效的应急响应系统还有许多政治和法律方面的问题需要研究和解决。

参考文献

1 CERT/CC. CERT/CC Statistics for 1988 Through 2005[Z]. http://www. cert.org/stats/cert_stats.html.

2 Cohen F. Simulating Cyber Attacks, Defense, and Consequences[Z]. 1999-03. http://www.all.net/journal/ntb/simulate/simulate.html.

3 Noordin M. Honeypots Revealed[Z]. 2004.11.05. http://www.securitydocs.com.

4 北京市信息化工作办公室. 北京市国家机关信息安全应急响应工作指南[R]. 2005-01-14.

5 曹爱娟, 刘宝旭, 许榕生. 网络陷阶与诱捕防御技术综述[J]. 计算机工程, 2004, 30(9): 1-3.

(上接第 127 页)

协商 Agent 在收到协商提议后，可以有几种响应方式：接受提议，给出反提议，拒绝提议并给出解释，单方终止协商。图 3 给出被请求方协商 Agent 的协商流程。

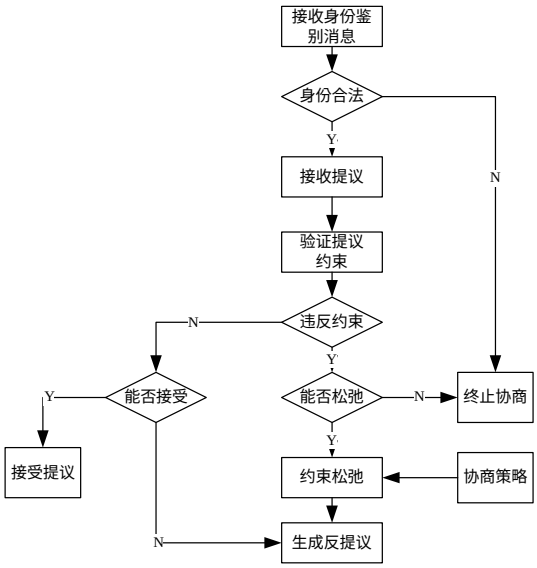

图 3 协商流程

被请求方 Agent 首先对请求方的身份进行鉴别，鉴别通过后，被请求方 Agent 根据自己所代理的用户定义的安全能力属性及约束信息，检查收到的提议请求的属性约束和属性间约束。发现违反约束时，被请求方 Agent 应用协商策略进行约束松弛。然后根据请求提议的属性约束、自己安全能力属性要求和约束生成反提议发给请求方协商 Agent。请求方协商流程与图 3 所示的协商流程类似，只是使用的约束、协商策略不同，不再赘述。

4 结束语

本文提出了一种适应多安全域环境的基于 Agent 的安全能力自动协商机制。该机制包括了一种基于 Agent 的安全能力协商模型、适用于该模型的协商 Agent 和协商流程。通过区分应用协商 Agent 和域协商 Agent，不仅实现了安全能力协商的自动化，也增强了多安全域环境下的系统安全性，简化了应用协商 Agent 并提升了它的执行效率。通过系统验证，该机制能较好地完成安全能力的协商工作。

参考文献

1 曹元大 孙 宁. 电子商务中的自动协商[J]. 计算机工程, 2002, 28(3): 182-183.

2 王 斌, 张尧学, 陈松乔. 一种基于黑板模型的多 Agent 系统通信方法[J]. 小型微型计算机系统, 2002, 23(11) : 1355-1358.

3 杨 明, 嘉 莉, 邱玉辉. 基于增强学习的多 Agent 自动协商研究[J]. 计算机工程与应用, 2004, 40(33) : 98-100.

4 ISO/IEC 15408-2002 Common Criteria for Information Technology Security Evaluation(Part 2): Security functional Requirements[S]. 2002.

5 GB 17959-1999 计算机信息系统安全保护等级划分准则[S]. 1999.

6 GA/T 390-2002 计算机信息系统安全等级保护通用技术要求[S]. 2002.