自动入侵响应系统的研究[1]

丁勇 龚俭 虞平
（东南大学计算机科学与工程系，南京，210096）
(江苏省计算机网络技术重点实验室)

【摘要】攻击手段的复杂化和自动化给网络造成了日益严重的威胁，自动入侵响应系统能够及时地采取响应措施阻止攻击的延续和降低系统的损失。本文综合分析了理想的自动入侵响应系统应当满足的要求，给出了自动入侵响应系统的一般结构，总结了可能的响应方式作为研究的前提和基础，并重点介绍了成本敏感模型、意图识别技术和自适应技术，这些响应技术的结合有助于实现一个合理的、及时的、自适应的自动入侵响应系统，文末还对应用于大规模网络的响应协同技术进行了介绍。
【关键词】自动入侵响应；成本敏感模型；意图识别；自适应；协同。

1. 引言

随着计算机网络的不断发展和普及，安全问题日益严重，已成为当今研究的重点。从CERT每年的安全事件报告可以看出，安全事件的数量从1989年的6例上升到1999年的8268例[1]，计算机网络的安全问题引起了广泛的关注。另外，攻击技术也由简单的攻击发展为复杂的攻击，如组合式攻击和协同攻击。1998 年 CERT 的报告[2]指出越来越多的攻击者开始使用脚本进行攻击，即大量的攻击工具集成在一起，能在短时间内自动完成多种复杂攻击。因此，入侵检测系统对保护系统的安全性显得尤为重要，而且攻击复杂化和自动化的出现对入侵检测系统的响应功能提出了更高的要求，要求响应系统能够及时地做出响应以减少攻击成功的机会和对系统造成的损失。

对于入侵响应系统来说，响应的及时性尤为重要。Cohen[3]通过模拟的方法研究了响应的时间与攻击者成功概率之间的关系。他的研究结果显示：如果熟练的攻击者被发现后仍留给他们 10 小时的时间，他们将有 80％成功的机会；如果留给他们 20 小时的时间，则成功的机会达到 95％；如果留给他们 30 小时的时间，则攻击者几乎很少失败。

Curtis [4]将入侵响应系统按其响应速度分为 3 类：报警型响应系统、手工响应系统、自动响应系统。报警型响应系统只是发现了安全事件后简单地给管理员发送通知，具体决定如何响应以及响应措施的实行由管理员负责。这类响应系统的缺点在于它使攻击发现和响应之间的时间窗口过长，从而给攻击者提供了充足的时间窗口实现攻击意图。手工响应系统提供了一些预先编制好的用来响应的程序，并能指导管理员选择适当的程序进行响应。这类系统加快了响应的速度，但仍然留给了有经验的攻击者足够的时间窗口。自动响应系统是最理想的能有效保护网络安全的一类系统，它能自动进行响应决策并及时地对攻击做出响应，从而留给攻击者尽量短的时间窗口。

目前的 IDS 的大部分研究还是集中于入侵的检测，对入侵的响应并未予以足够的重视，现有的入侵响应系统只有少数属于自动响应系统，而且它们做的仍不够理想。本文在第 2 节中对自动入侵响应系统的要求进行了分析，第 3 节介绍了自动入侵响应系统一般采用的体系结构，第 4 节总结了可能的响应方式作为研究自动响应的前提和基础，第 5 节讨论为了达到自动入侵响应系统的要求而采用的多种技术，第 6 节介绍了响应协同技术。

2. 自动入侵响应系统的要求

自动入侵响应系统应当满足以下一些要求：

[1] 国家自然科学基金重点课题（No.90104031）资助

（1） 安全性：这个要求的必要性在于入侵响应系统也会受到攻击，如 DOS 攻击，这样的 IDS 显然失去了保护系统的作用。安全性的要求使入侵响应决策不能只做成简单的静态决策表，而是要有一定的智能。

（2） 合理性：入侵检测系统应该以最小的代价换取最大的安全目标，即响应应当在最适当的位置，以最适当的方式进行；当响应的代价大于攻击持续所造成的损失时，就不需要进行响应；极端的情况就是受攻击系统对检测到的攻击免疫，例如 Unix 系统遇到针对 NT 系统的攻击，那么就不需要采取任何响应措施。目前的入侵检测系统试图对所有检测到的攻击进行响应，这显然不能有效地利用有限的资源达到尽可能高的安全级别，采用基于成本模型的决策可以将有限的资源集中在潜在危害高的入侵行为上。

（3） 及时性：入侵响应系统的目标就是及时地采取措施以尽量降低入侵对系统造成的危害，所以这需要入侵响应系统尽可能地缩短入侵发现和响应实施之间的时间窗口。这一方面要求响应决策和响应执行的计算复杂度不能太高，另一方面要求系统有预测攻击者意图的能力。

（4） 自适应性：实际环境中有许多不确定的因素（如入侵检测系统本身就有一定的误报率），因此响应系统不能做成静态的形式，而是能不断适应环境的变化。例如，响应系统应当避免对可信度低的攻击做出严厉的响应，响应方式也应当能随着攻击的进行不断地调整。

（5） 灵活性：不同的机构可能有不同的响应政策（如法律约束或安全级别的要求）。因此，入侵响应系统应当有适应不同的响应政策的能力。

目前还没有一个 IDS 能够完全满足以上的要求，但已经有多种技术被提出并用来解决这些问题，这些将在第 5 节中分别介绍。

3. 自动入侵响应系统总体结构

自动入侵响应系统的总体结构如图 1。响应决策模块根据响应决策知识库，决定对入侵检测系统检测出的安全事件做出何种响应；响应策略应当由一种中间语言描述，由响应执行模块解释执行，并调用响应工具库中预先编制好的工具。其中响应决策是系统的核心，因为合理的、及时的响应是降低系统损失的关键。

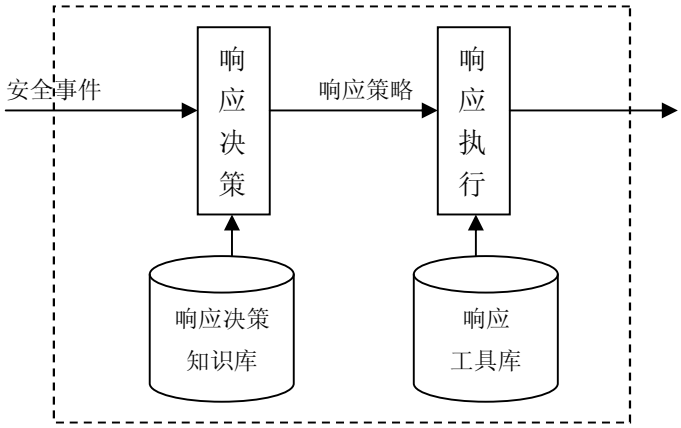

图 1 自动入侵响应系统总体结构

4. 响应方式

Curtis 在他的论文中[4]对响应的可能方式进行了枚举，响应方式可以分为基于主机的和基于网络的响应方式。

基于网络的响应方式主要有以下几类：

（1）记录安全事件：将安全事件记录下来有利于管理员的事后追查。
（2）产生报警信息：在控制台产生报警，或发送邮件给管理员。
（3）记录附加日志：为了能更好的分析攻击，有时应当不仅限于记录发现攻击的报文，如对于栈溢出攻击，记录栈溢出之后的一些报文对管理员了解攻击者的意图是非常有帮助的。
（4）激活附加的入侵检测工具：入侵检测系统为了将有限的资源集中于更多的攻击，一般使用计算复杂度较低的测度进行检测，当发现攻击者对系统的潜在危害上升时，可以触发更细致的检测，这种检测一般使用计算复杂度较高的测度，但检测精度更高。
（5）隔离入侵者 IP：当发现攻击者对系统的威胁到达一定程度时，可以配置防火墙将攻击者从受保护网络隔离，这种响应措施的选择需要慎重考虑，特别是对于伪造 IP 的攻击，这种响应会伤害合法客户的利益。
（6）禁止被攻击对象的特定服务：通过配置防火墙实现，但这种响应将伤害其他合法客户的利益。
（7）隔离被攻击对象：这种措施实际上禁止了所有外网对被攻击对象的访问。
（8）警告攻击者：通过发警告消息给攻击者。
（9）跟踪攻击者：找到尽量接近攻击发起的位置。
（10）断开危险连接：对于 TCP 连接发送 RST 报文将连接断开。
（11）攻击攻击者：最严厉的响应措施。

可以看出，1 至 4 的响应措施比较温和，8 至 11 的响应措施比较严厉，5 至 7 的响应措施介于两者之间。其中 1 至 4 的响应措施属于被动方式，其它的属于主动方式。8 至 11 的响应方式一般受到法律等因素的约束，而 5 至 7 的方式能有效地阻断攻击，但错误的响应甚至正确的响应可能伤及合法用户的利益，因此也需要慎重考虑。

基于主机的被动响应方式与基于网络的被动响应方式基本相同，但它们的主动响应方式却有所不同。基于主机的主动响应方式包括：提供附加的认证措施、暂停用户任务的执行、中止用户的会话、锁住用户的帐户、关闭被攻击主机。

5. 响应决策技术

自动入侵响应系统的核心是响应决策，其目的就是根据检测出的攻击及相应的一些属性（如可信度等），决定对当前攻击做出什么响应。当前已有多种技术被提出并应用，Wenke Lee 在他的论文中[5]提出成本敏感模型作为响应决策的基础，使入侵响应系统满足合理性要求；Christopher 和 Robert[7]介绍了意图识别技术在入侵响应中的应用，从而增强了入侵响应系统的实时性和合理性；Curtis[10]介绍了他们开发的入侵响应系统 AAIRS，该系统能够满足自适应性要求。

5.1 成本敏感模型

Wenke Lee 将入侵检测和响应中涉及的代价分为 3 类：

（1） 损失代价（Damage Cost）：即在 IDS 不采取任何响应措施的情况下，攻击对系统造成的损失，记为 DCost；
（2） 响应代价（Response Cost）：即 IDS 对攻击做出响应所付出的代价，记为 RCost；
（3） 检测代价（Operational Cost）：即 IDS 为了检测出攻击所付出的代价，记为 OpCost。

对于检测到的入侵行为，如果其损失代价大于响应代价，即 DCost > RCost，则有必要采取响应措施；反之，如果 DCost < RCost，则不进行响应。使用该模型的关键在于损失代价和响应代价的估算。

Wenke Lee 分别阐述了如何计算两种代价。损失代价可通过两个指标衡量，即重要性（criticality）和致命性（lethality）。重要性是指被攻击目标的价值或重要程度，如防火墙、

路由器或 DNS 服务器的重要性最高，邮件或 Web 服务器次之，接着依次是 UNIX 工作站和 Windows 工作站。致命性指攻击本身的危害程度，如获取根权限攻击的危害程度要高于获取本地用户权限攻击的危害程度。因此攻击的损失代价可用下面公式计算：DCost ＝ criticality ×lethality。响应代价主要根据响应方式的类型，同时考虑安全政策和环境因素进行计算，响应代价应该包括响应实施本身所消耗的资源以及响应给合法用户可能带来的额外损失。

表 1 是 Wenke Lee 根据 Lindqvist 和 Jonsson 的攻击分类[6]对每类攻击的损失代价和响应代价的估算。

表 1 攻击分类及代价估算

一级分类	描述	二级分类	描述	DCost	RCost
ROOT	非法获取根权限	Local	通过先以合法用户登录再获取根用户实现	100	40
		Remote	从远程主机直接获取根用户	100	60
R2L	从外界获得非法访问	Single	通过单一步骤实现	50	20
		Multiple	通过多步骤实现	50	40
DOS	拒绝服务	Crashing	通过单一事件实现	30	10
		Consumption	通过大量事件实现	30	15
PROBE	获取目标系统的信息	Simple	短时间内大量的扫描	2	5
		Stealth	分布式，并且慢速的扫描	2	7

该代价模型存在两个缺点：

（1） 在代价的衡量中都是以单个攻击为粒度，在实际情况中攻击者经常采用协同攻击，而协同攻击的损失代价并不是组成该攻击的各单步攻击的损失代价之和，另外应当采取的响应方式也不一定相同。

（2） 损失代价和响应代价的估算都是静态的，而实际环境中的代价估算应当体现出动态和自适应的特点。

5.2 意图识别技术

Christopher 和 Robert 在他们的论文中[7]提出了将意图识别（Plan Recognition）应用在入侵检测及响应领域。他们的主要思想是：将 IDS 检测出的一系列原始安全事件流作为意图识别模块的输入，意图识别模块推断出攻击者的意图，从而使系统能够尽早地做出适当的响应。

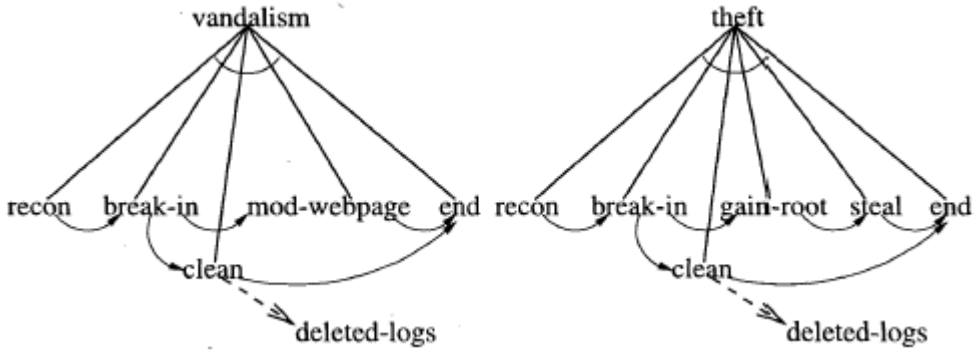

图2 攻击者意图表示举例

关于攻击者意图的知识可以用语义网络来形式化描述，图 2 是攻击者意图描述的例子。一次恶意攻击（vandalism）的可能步骤是：侦察（recon）、攻破（break-in）、修改网页（mod-webpage）、结束（end）；一次窃取攻击的可能步骤是：侦察（recon）、攻破（break-in）、

获取 root 权限（gain-root）、窃取信息（steal）、结束（end）。

Henry A. Kautz[8]提出了意图识别技术的正规理论，但是该理论的一些假设限制了意图识别的应用，网络安全领域对入侵者意图识别提出了许多新的要求：

（1） IDS不可能检测到所有安全事件，因此攻击者的有些攻击步骤可能不能被IDS发现，即意图识别应当能容忍不完整的信息；

（2） 攻击者为完成某一攻击意图采取的攻击步骤不一定有严格的先后顺序，这些步骤之间在时间上往往呈现偏序关系；

（3） 攻击者一段时间的行为往往有多重攻击意图，各种攻击意图对应的行为交错进行；

（4） 攻击者的单个行为可能用来达到多种意图。

Christopher 和 Robert [7]提出了改进的意图识别算法，能够适应以上这些新的要求。

将意图识别技术应用到入侵检测和响应系统有以下两点好处：

（1） 攻击者意图识别有助于入侵响应系统做出更合理的响应。比如检测到 DOS 攻击，可能入侵者的意图就是使攻击对象服务失效，也可能攻击者想对信任受害主机的其它主机进行 IP 地址欺骗攻击，对于这两种攻击意图，响应方式是截然不同的。

（2） 攻击者意图识别能够尽快地发现或预测攻击者的意图，从而尽早到地做出响应，减少系统的损失。

5.3 自适应技术

响应决策不应当只是一种静态的形式，它应当有一定的自适应性。Curtis 在他的论文[9]中介绍了他们研制的 AAIRS（Adaptive Agent-based Response System）系统是如何处理各种不确定因素，以达到系统的自适应性。

不确定因素有以下两方面：

（1） 入侵检测系统的不确定性。IDS 检测出的原始安全事件有一定的误报率，IDS 将给每一个产生的安全事件赋予一个可信度，每一个安全事件可以有多种响应方式，对于可信度大的安全事件可以选择较严厉的响应方式，而对于可信度小的则选择较温和的响应方式。

（2） 入侵响应系统的不确定性。响应系统接收到安全事件报告后，必须能够判断该事件是已在进行攻击的一部分，还是一个新的攻击的开始，对于这两种情况的响应方式有可能是不同的；而且由于响应措施执行的成功与否不确定，入侵响应系统必须时常检测响应措施是否成功，及时更换响应方式的实现甚至是响应方式本身。

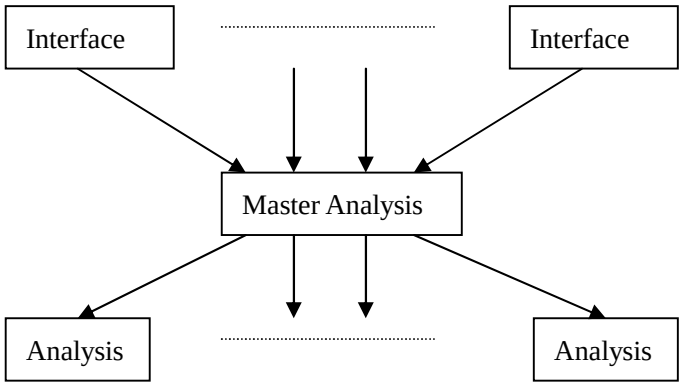

图 3 AAIRS 处理不确定性的方法

为了解决以上的不确定因素，AAIRS 采用了图 3 的体系结构。其中 Interface Agent 将不同 IDS 的安全事件报告转化为统一的格式，并赋予安全事件一定的可信度，可信度由专家赋值，并在检测过程中采用自学习的方式动态更新。Master Analysis Agent 的作用是判断当前收到的安全事件是一个新的攻击的开始，还是已有攻击的继续，若是新的攻击的开始则创

建一个新的 Analysis Agent 进行分析，否则将安全事件送给已有的 Analysis Agent。Analysis Agent 的作用是对当前收到的安全事件，结合考虑该事件对应的攻击的历史状态做出合理的响应决策。该 agent 还检查以前做出的响应是否成功，如果失败则采用同种响应方式的其它实现版本，如果其它实现也失败则更换响应方式。Curtis 提出可以用三种尺度结合的方法判断安全事件是属于已有攻击还是新的攻击的开始，即时间尺度（安全事件之间的时间间隔）、会话标识尺度（如 IP 地址和用户名等）、攻击类型尺度。

Curtis 在他的论文[10]中介绍了 AAIRS 的体系结构，AAIRS 的优点在于它良好的自适应性，而且在响应决策中考虑了环境因素的影响。但是 AAIRS 的响应决策没有基于成本模型，这使得系统可能产生过多的不必要的响应措施。

6. 响应的协同

现有的响应系统都是根据本地的安全事件信息，进行局限于本地的响应，而对于大规模网络而言，各响应系统之间有必要进行协同。这主要有以下两点好处：

（1） 各响应系统之间安全事件信息的共享有助于对攻击者行为做出更精确的判断，从而做出更合理的响应；

（2） 各响应系统之间响应措施的协同可以使总的损失代价达到全局的最小，如在离攻击者最近的边界控制器将攻击者 IP 隔离可以减小该响应措施对其他正常用户带来的额外损失。

IDIP[11]是在 DARPA 的资助下，由波音公司、NAI 实验室和加州 Davis 分校计算机安全实验室共同研究的应用协议，它能将各种网络基础设施（如边界控制器、入侵检测系统、基于主机的响应器等）有机地集成在一起，从而实现以下功能：

（1） 协同追踪攻击源，并在最接近攻击源的边界控制器隔离攻击者 IP；

（2） 使用独立于设备的追踪和阻塞指示消息；

（3） 集中的报告和入侵响应的协同。

IDIP 系统被组织成两级的结构。第一级为 IDIP 团体（community），每一个 IDIP 团体是一个管理域，该域内所有的入侵检测和响应系统被发现协调点（Discovery Coordinator）管理；团体由多个邻居（neighborhood）组成，边界控制器（Boundary Controller）是连接相邻邻居的设备，每个邻居内都有入侵检测和响应系统，入侵追踪就是从一个邻居通过边界控制器追踪到另一个邻居。对于一次攻击，每个邻居的 IDIP 节点会做出本地的响应，IDIP 将追踪攻击源，在攻击路径上的各 IDIP 节点都将做出响应，发现协调点综合各邻居的 IDIP 节点的信息，协调和纠正各 IDIP 节点的响应措施，从而达到全局最优的响应。

COMON 系统是国家 863 计划通信主题重大项目资助下，由东南大学等高校研究和开发的分布式高速 IP 网络入侵监测系统。该系统的协同功能主要分为三个层次，最底层是一个通用安全传输平台，可以进行身份的鉴别、数据的加密传输、数据的完整性保护，秘钥的分配采用 PKI 机制。安全传输平台的上层是一个通用协同平台，它支持各协同点之间的基本协同操作，并提供了访问控制策略对各协同点之间的相互访问进行约束。协同平台之上是安全事件的综合和追踪功能，其中安全事件追踪通过向相邻协同点查询相关安全事件可以追溯到最接近攻击源的边界控制器，从而隔离攻击者 IP。试验表明，协同功能的引入大大增强了系统对入侵的检测和响应能力。

7. 总结

随着攻击的复杂化和自动化，自动入侵响应系统将在保护系统安全、降低攻击对系统造成的损失方面起着重要的作用。自动入侵响应系统在成为实用的系统之前，必须具备安全性、合理性、实时性、自适应性和灵活性，但目前还没有一个 IDS 产品能达到所有这些要求。本文重点介绍了多种应用在自动入侵响应系统中的技术，其中成本敏感模型应当作为入侵响

应决策的基础，意图识别技术和自适应技术增强了自动入侵响应系统的功能。这些技术的结合使我们能够构造一个功能强大、实用的自动入侵响应系统，从而为系统提供更有力的保护。

8. 参考文献

[1] C. C. Center. CERT/CC Statistics for 1988 through 1998. http://www.cert.org/stats/cert_stats.html, 2000

[2] C. C. Center. CERT Coordination Center 1998. http://www.cert.org/annual_rpts/cert_rpt_98.html, 2000

[3] F. B. Cohen. Simulating Cyber Attacks, Defenses, and Consequences. http://all.net/journal/ntb/simulate/simulate.html, 1999

[4] Curtis A. Carver. Intrusion Response Systems: A Survey. http://faculty.cs.tamu.edu/pooch/course/CPSC665/Spring2001/Lessons/Intrusion_Detection_and_Response, 2000

[5] Wenke Lee. Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, Volume 10, Issues 1/2, 2002

[6] Ulf Lindqvist, Erland Jonsson. How to Systematically Classify Computer Security Intrusions. IEEE Symposium on Security and Privacy, 1997

[7] Christopher W. Geib, Robert P. Goldman. Plan Recognition in Intrusion Detection Systems. IEEE, 2001

[8] Henry A. Kautz. A Formal Theory of Plan Recognition and its Implementation. University of Rochester, 1987

[9] Curtis A. Carver. Limiting Uncertainty in Intrusion Response. IEEE, 2000

[10] Curtis Curtis A. Carver. A Methodology for Using Intelligent Agents to provide Automated Intrusion Response. Proceedings of the IEEE Systems, 2000

[11] Dan Schnackenberg, Kelly Djahandari, Dan Sterne. Infrastructure for Intrusion Detection and Response. Proceedings of the DARPA Information Survivability Conference and Exposition, 2000

A Study of Automated Intrusion Response Systems

Ding Yong, Gong Jian, Yu Ping

（Dept. of Computer Science and Engineering, Southeast University, 210096 Nanjing）

（Computer network technology key laboratory, Jiangsu）

【Abstract】The emergence of automated and complex attacks imposes great threat on the network. The automated intrusion response system is able to take timely countermeasures to stop the attacks and decrease the loss of systems. This paper analyzes the several requirements of an ideal automated intrusion response system, introduces the general architecture of automated intrusion response systems, summarizes the possible countermeasures that make the basis of the research, and focuses on the introduction of three important techniques, including cost-sensitive model, plan recognition, and the self-adaptive technique. The combination of these techniques helps to construct a reasonable, timely, and self-adaptive automated intrusion response system. In the end of this paper, we make a brief introduction of the cooperation techniques that is used in large scale networks.

【Keyword】automated intrusion response, cost-sensitive model, plan recognition, self-adaptation, cooperation