大规模互联网络的入侵检测[1]

龚俭　陆晟

（东南大学计算机系　南京 210096）

摘要：介绍了大规模互联网络入侵检测技术的发展现状；对网络入侵检测的体系结构，异常检测技术，响应技术，入侵检测的协同技术，网络基础设施的保护技术等热点问题进行了侧重讨论，指出了该领域的一些发展重点。

关键词：入侵检测系统，异常检测，入侵响应，协同检测，入侵追踪，网络安全。

1. 引言

随着 Internet 使用的进一步发展，Internet 网络安全变得日益相互依赖，例如从 DDOS(分布式服务失效攻击)可以看到，一个网络的安全状态会影响其他网络的安全状态，2001 年 5 月份爆发的红色代码病毒在 13 个小时之内就迅速感染了 39 万台主机。小到一个独立的局域网，大到整个国家的网络基础设施，其内部的依赖关系日益紧密，网络的边界、拓扑和用户成分越来越复杂，各级 Internet 自治系统安全控制的难度日益提高，所以对大规模互联网络入侵检测的研究引起了人们的高度重视。

虽然真正意义上的网络攻击从八十年代末才出现，但是网络的入侵检测研究较早就开始了。SRI 早在 1983 年就开始 Intrusion Detection Expert System (IDES)的研究，James P. Anderson 更早在 1980 年就有相关论文发表。二十世纪九十年代前后入侵检测的单项技术研究有了很大的发展，新的检测技术和各种检测系统不断涌现，其中比较有代表性的有：1989 年出现异常检测的概念，1990 年出现通过网络监听进行入侵检测的系统，1991 年出现分布式入侵检测体系。九十年代中后期入侵检测的体系结构的研究又有了许多发展，例如 Mark Crosbie 和 Gene Spafford 的自治代理概念被广泛接收[1]。目前被各种商业入侵检测系统和其他实用系统所采用的检测方法主要包括：特征分析、模式匹配、安全状态分析、统计分析等，此外还有许多支持技术，如会话还原、日志存贮技术等也得到了发展。

和入侵检测技术不同，网络攻击的响应技术直到近年来才逐渐得到重视，SRI 在 1997 年的 EMERALD 项目中开始提到响应问题，而且在其目标中是监测和响应技术是并重的[3]；同时美国南加州大学信息科学学院也开始将 IDS 系统中某些独立成分视为专门的响应者，并且试图建立检测者和响应者之间的交换协议。此后，在 1999 和 2000 年 DARPA 有近十个项目直接研究响应问题，相关研究则更多。

本文介绍了大规模互联网络入侵检测技术各领域的发展现状，对其中的一些热点问题进行了侧重讨论。

2. 入侵检测的体系结构

早期入侵检测系统的保护对象是单台服务器或某个局域网（或园区网），没有协同的需求和概念，因此也没有关于体系结构方面的研究讨论，各个系统有其不同的实现模型。但大规模互联网络的入侵检测研究所面临的首要问题就是监测体系结构问题，由当前 Internet 的大规模和高速的特性所决定，目前被广泛使用的商业化以及共享的入侵检测系统实现模型无法满足多点协同监测的需要，因此研究和设计新的入侵检测系统体系结构是实现对大规模网络安全检测的基础。

对大规模互联网络入侵检测的研究开始于美国加州大学戴维斯分校（UC Davis）的

[1] 本文受国家自然科学基金重点项目 90104031 资助

GrIDS 系统，S. Staniford-Chen 等的论文[2]在 1996 年对所采用的方法加以了说明，即通过采用图论的方法对安全事件的相关性和危害的蔓延情况进行分析。此后，UC Davis 提出了通用入侵检测框架 CIDF(Common Intrusion Detection Framework) [3]的概念来试图建立通用的入侵检测体系结构，并引发了相关的研究。目前针对大规模网络的监测一般都采用分布式结构，主要为基于主机的分布式代理结构和分布式监听结构，此外也存在综合以上两种方式的分布式监测结构。例如美国普度（Purdue）大学的 COAST 小组研究各种监测和日志技术，并采用了基于主机的代理结构[4]。UC Davis 的 GlobalGuard 项目则主要使用基于网络分布监听的方式，而 UC Santa Barbara 的 NetSTAT 项目则混合了以上方法[5]。

但是，若需要建立完整的大规模分布式安全监测体系，目前并没有公认的体系结构，因为人们对大规模网络入侵检测的功能覆盖范围和检测方法认识尚不统一，各个研究小组在研究入侵检测系统的体系结构时都有明显的单项技术侧重点。例如，波音公司的 IDIP[6]瞄准了入侵检测后的响应信息交换和响应决策；IETF 入侵检测工作组（IDWG）的 IAP 与 IDMEF 的目的则是建立通用的安全检测信息交换方式[7]。另外还有一些相关的研究活动涉及大规模网络安全监测各方面的问题，比较著名的有：美国北卡州微电子中心（MCNC）关于建立可靠安全域的研究与路由基础设施保护的研究；美国加州大学圣巴巴拉分校（UC Santa Barbara）关于分布式的基于状态变迁的安全检测方法研究[8][9]；以及美国康乃尔大学关于可靠的安全信息交换协议的研究等[10]。

3. 入侵检测技术

最初的网络入侵检测方法都是基于攻击特征的，通过对这些攻击特征进行识别和归纳来得出安全结论。但由于现有的网络系统存在安全性方面的先天缺陷，而且人们对攻击的认识总跟不上攻击的发展，所以基于这种思路来完全杜绝网络入侵是不可能的。因此美军在上世纪九十年代末提出了容忍入侵（Intrusion-tolerance）系统的概念，这种系统可以在存在入侵攻击的情况下继续正常工作并能及时地提供预期的用户服务（但系统性能和其他功能可能会受到影响）。这种系统可以检测到那些突破了外层防御措施的攻击，并采取必要的响应行动，这些响应措施可以从限制可疑代码或数据的使用到重新配置软硬件资源。因此目前大规模网络入侵检测技术方面的研究重点转向了异常检测，即发展检测和抵御未知类型攻击的能力。例如美国新墨西哥（New Mexico）大学和Odyssey Research Associates, Inc.都试图采用免疫学的方法进行大规模网络的安全研究[11]，同时也研究计算机免疫学的相关技术，该技术属于异常检测和滥用检测的混合类型。美国Carnegie Mellon大学、Purdue大学、Columbia大学、UC Davis和MCNC等都在进行新的异常检测技术的研究，这些研究包括采用数据挖掘、神经元网络、可能性图分析、代价分析、元学习、特征发现、统计等不同的技术方式。虽然上述的研究活动提出了多种异常检测方法，但是由于其过高的误报率，严重影响了实际推广和使用，在商业领域的应用很少，因此今后的研究重点是使误报率能够下降到在可接受范围内的方法。MIT的林肯实验室和美国空军研究实验室从1997年开始研究对IDS的评测问题，他们构造了一组标准的测试数据，并定义了一个接收者运行特征(ROC)曲线的概念来描述IDS的测准率和误报率。

另外随着网络拓扑和应用复杂度的增加，针对网络基础设施本身的攻击也在增多，而网络中的基础设施组件，例如路由器，交换机等，作为防御前沿却缺乏保护措施。目前针对网络基础设施安全性的研究主要集中在协议层进行，通过统计和逻辑分析网络路由和管理协议来检测入侵，或对现有协议进行改进以增强检测和抵御攻击的能力。比较典型的是由 MCNC 研制的 JiNao 系统和由 BBN 公司研制的外部路由入侵检测系统(ERIDS)。JiNao 基于对网络路由协议的统计与逻辑分析，通过内嵌的网络管理功能提供针对 OSPF 网络入侵的防范、检测、响应和重配置能力，并通过 JiNao 之间的协同工作覆盖整个被保护的网络[12]。系统包

含本地检测子系统和基于 SNMP 的远程管理应用子系统，后者支持对前者的查询和重配置。本地检测子系统由三个模块组成：基于规则的防范模块，它起关守的作用，基于一个小的规则集拦截和过滤所有到达的报文，这些规则表达了基本的安全要求或特殊的安全政策；基于协议的检测模块，它对协议操作作逻辑分析，并对协议状态机出现的异常状态进行报警；统计分析检测模块实现对路由协议行为的分析，它统计并学习路由协议的正常行为并产生一个特征文件（profile），如果发现了异于特征文件规定的行为，则进行报警。前两个检测模块都是基于已知知识，因此响应时间比较短，而统计检测需要一段观测期（observation window），因此不能实时响应。

ERIDS 可以使网络运行管理中心发现由于恶意攻击或配置错误而导致的 BGP 异常操作[13]。ERIDS 具有 BGPv4 协议信息的收集能力，能够对报文的数据进行解码分析，将采集的路由数据与路由政策数据库中的路由信息进行比较，发现可能存在的攻击行为。进一步地，可在 ERIDS 中加入入侵检测引擎，它使用分布式的检测探头来收集 BGP 报文，将它们压缩并传递到中央的检测引擎作分析处理。这个检测引擎使用路由数据库访问工具获得路由政策定义，将收集到的路由信息与管理员确定的自治系统路由政策进行分析比较，并对所发现的攻击事件作出响应和报警。

对基础设施软件的框架结构进行研究和改进是一种新的思路，它试图建立新的基础软件架构，以能够处理大范围的错误。例如美国 TIS 和 NAI 公司在多种系统平台上研制的软件阻隔（wrapping）技术[14]，可以大大提高由标准软件组件（COTS-commercial off the shelf，包括应用系统和操作系统）构成的大型软件系统的安全性和可靠性。通用软件阻隔器将拦截组件之间的交互，并把这些交互绑定到实现实际的安全（如限制、过滤）和可靠性（如冗余、崩溃数据的恢复）政策的功能上。这种阻隔器可作为一个软件模块嵌入运行环境，不需要对嵌入系统的源码进行修改。它通过阻隔器定义语言 WDL 来描述轻型可移植的软件阻隔器在安全性和可靠性方面的功能和性质，并利用阻隔器支撑界面 WSI 提供所有需要的操作系统服务，包括从操作系统内核到命令解释器。阻隔器中内嵌了一组基于 CIDF 概念的入侵检测功能，从而可发展成为入侵检测阻隔器 IDW，它们使用的检测技术包括基于特征规范的技术（例如可以检测对 IMAP 的栈溢出攻击）、状态转换分析技术、和基于序列的技术（自动学习合法的调用序列并只允许合法的调用序列被执行）。事实表明，在进行入侵检测时，使用软件阻隔器比使用系统日志更为有效，因为前者有更好的访问、过滤和动态探测系统状态的能力，因此有更丰富的输入数据，和更好的数据选择能力。

对检测信息进行综合处理算法的研究呈多样化的趋势，例如基于图论的方法，基于性能模式的方法，基于权重的代价分析方法，基于分布式计算中的错误处理的方法等。但到目前为止尚无公认的综合处理算法，因此对于入侵检测的汇总决策问题仍需要进一步研究。

4. 检测的响应技术

无论大规模网络监测所采用的结构如何，网络中的安全系统一般均分为监测者(Detector)和响应者(Responder)，它们分别用于对网络攻击进行检测和响应处理。关于响应的研究大致可分为响应政策研究和响应机制研究两类。

有关响应政策的研究侧重两个方面：响应的自适应性和响应政策的形式化技术。响应的自适应性研究目前主要有以下两个手段：1)自适应网络安全管理架构的建立[15]，用于构造对政府和商用信息系统的保护系统，这种自适应性使系统不仅具备对安全攻击的实时检测能力，而且具有使网络设施自动适应以阻止进一步攻击的能力，呈现出端系统保护的典型特征；2)试图将响应政策的评估和执行机制集成进入侵检测与响应系统，着重于研究一种机制来协调跨服务器的系统范围内的应用层响应，通过要求应用服务器嵌入支持攻击条件自适应的访问控制系统来达到目的，例如美国南加州大学信息科学学院开发的 DEFCN（Dynamic Policy

Evaluation for containing Network Attacks）系统。

在响应政策的形式化技术方面，研究的重点是使用高级语言为大规模互联网络定义安全政策，并开发相应的工具来处理、验证和将其转换成为中间语言表示，从而可以向网络组件提供安全政策信息；或者转换成其他特定于某些应用的形式（例如报文过滤语言）；或者通过信任关系的形式化描述，建立信任管理系统。这方面比较著名的成果是 Bell 实验室提出的 Keynote 语言[16]，它可用一种符号语言来描述系统之间的信任关系，通过密钥的交换将信任关系映射为允许或不允许的动作。这种方法的新颖性在于可以将高级安全政策表达为元 Keynote，进而可以转换为 Keynote 表达式，因此 Keynote 被集成到 IPsec 和防火墙中，允许对一组 IP 路由器按特定的安全政策实现自动的配置。

针对目前响应机制的低效和基本依赖人工处理的问题，关于响应机制的研究热点是新的响应方法和追踪方法，其中比较著名的是作为 DARPA 信息生存(Information Survivability)计划的一部分，由 Boeing 牵头进行的实时响应研究活动。通过开发 IDIP(Intruder Detection and Isolation Protocol)建立动态的协作的边界控制，并可追踪对系统部分攻击的入侵者[17]。IDIP 采用的是基于代价的分析处理模式，并考虑了性能影响、拓扑限制、系统的副作用、对攻击进行围堵的保障、局部自治与全局控制的关系、政策机制对不同攻击场景的适应性、以及各个网络组件在入侵追踪和围堵中的作用与角色等多种因素。这个名为 Dynamic Cooperating Boundary Controllers 的系统的响应总体策略是首先实施实时响应，其反应程度可能超出实际需要，但确定此响应的计算开销小，响应的有效期短，响应成功的可能性高；然后再提供一个全局优化的、更合理的响应。实时响应由响应组件根据本地信息和简单模型确定并实施（如防火墙、路由器过滤等），而后续的响应由中央管理部件（IDIP discovery coordinator）根据全局信息和一组代价模型作出，然后分布到各有关响应组件去执行。第一级快速而短暂的响应为第二级优化响应提供了决策时间，在防止攻击造成的危害继续扩大的同时，允许系统作出一个全局优化的合理响应。系统的代价模型使用 NASA 提供的 CLIPS - C Language Integrated Production System 系统开发。

UC Davis 的研究思路基于他们提出的 CIDF，以协同的方式来检测、分析、和响应大规模网络中因大范围攻击(包括未知攻击)或操作错误所产生的问题，其重点是提高响应的效率和自动程度，降低误报率。SRI 研制的 NIDES 系统采取的响应动作可以包括对入侵检测系统本身进行重新配置以获得更多对受影响的主机和网络的详细检测数据；激发管理动作关闭某种服务；孤立受攻击的部件；或激活备用资源等等。一个值得注意的动向是基于主动网络技术的入侵检测、跟踪、响应和发现机制的研究。由于主动网络技术提供了高度定制的结构以允许用户对路由器、交换机和其他设备重新编程和定制，因此在主动网络中有可能开发出具有更大灵活性、适应性，功能强大，高效率的入侵检测和响应机制。

5．入侵检测的协同技术

大规模互联网络的入侵检测靠单点是无法完成的，需要各个检测系统之间的协同工作。由于检测技术的多样性，而且入侵检测的管理与网络管理有很大的联系，同样受管理域的约束，因此入侵检测的协同技术研究重点放在了大范围检测信息的安全传递和开放接口上。这方面最著名的成果是由 UC Davis 的安全实验室提出的 CIDF，它定义了一种通用入侵说明语言（CISL）[18]，可以对事件、分析结果、响应指示等作通用的表示。CIDF 把入侵检测系统从逻辑上分为面向任务的组件(component)，并试图规范一种通用编码方式以表示在组件边界传递的数据。CIDF 还定义了入侵检测协同的六种场景形式，即分析、互补、互纠、核实、调整检测和响应，并分别为这些场景定义了语义。

IETF 的 IDWG 工作组的工作重点是定义在大规模互联网络中进行安全的检测信息交换的标准，包括为入侵检测和响应系统以及可能需和它们交互的管理系统所感兴趣的共享信息

定义数据格式和交互过程。到目前为止他们完成的工作包括：

(1) IETF/IDWG 的安全监测框架模型；

(2) IDMEF（Intrusion Detection Message Exchange Format）：描述了用来表示入侵检测系统的输出信息的数据模型；

(3) IAP（Intrusion Alert Protocol）：用于入侵检测组件、特别是监测器/分析器和管理人员间的入侵警报数据交换；

(4) IDXP（Intrusion Detection Exchange Protocol）：用于入侵检测实体间交换数据，该协议支持基于面向连接协议双向鉴别，完整性和机密性。该协议支持 IDMEF（入侵检测消息交换格式）消息、非格式化文本和二进制数据的交换。

但以上工作均未成为正式的 RFC，因此标准的制定工作仍旧在进行中。另外美国国防部也在试图将众多安全研究中所产生的一些相关结果，包括 CIDF、EMERALD、IDIP 和 GrIDS 等，统一到其 Advanced Information Technology Services Reference Architecture(AITS RA)中，以期在安全检测信息的规范化表示方面取得突破性的进展，但该项工作到目前为止还并未完成。按 CIDF 的观点，入侵检测系统的协同可分为三个层次：配置互操作（网络中的 IDS 可相互感知并可建立通信联系），语法互操作（IDS 之间具有统一的数据表达方式，因此交换的数据是可识别的），和语义互操作（IDS 之后的检测数据具有统一的语义，从而在响应上是可协同的）。第一层次的互操作对于协同没有太多意义；第二层次的互操作对于检测数据的交换有意义，在一定程度上可支持检测的协同；第三层次的互操作可实现 IDS 的完全协同，但现阶段的工作主要还是针对前两个层次的互操作，对标准语义的研究还没有什么比较满意的进展。

6. 入侵的追踪技术

入侵追踪的最初目的是试图发现攻击者的位置，通常表现为攻击者的 IP 地址。由于攻击者会使用地址欺骗技术来隐藏自己的真实位置，因此入侵追踪技术的研究重点就逐渐转为如何发现攻击者的真实地址和传输路径，或对其作出尽可能真实的定位。网络入侵的追踪是对网络入侵正确响应的重要前提。由于入侵响应会造成网络服务的损失，所以对入侵的正确定位有助于降低服务损失，例如对服务失效攻击的响应。入侵追踪技术包括传输日志、报文标记、链路测试、和 ICMP 追踪等方法[19]。

传输日志方法在报文传输路径上的一些重要路由器中对过往的报文作日志记录，并使用数据挖掘的方法来分析报文传输的真实路径。例如美国 BBN 公司设计开发的 SPIE（Source Path Isolation Engine）系统可以可靠地追踪攻击源点至其特定 AS 的入口点，这要求在沿途的路由器中置入特殊软件来记录和缓存每个报文转发事件的信息摘录，以供追查[20]。BBN 与 Avici 公司合作开发了支持这种功能的路由器，并定义了 SPIE 的请求与响应信息格式。由于路由器的存储资源有限，因此这种方法只能支持较短时间周期内的源点追踪。

报文标记方法要求转发报文的路由器采用随机或固定的模型对经过的报文进行标记，通常是在报文中记录下自己的地址（如使用 IP 报文的选项字段）。这样，当网络节点发现遭受攻击时，它可以通过寻找标记过的报文来确定攻击的源点。这种追踪方法相对来说管理开销比较小。

链路测试方法包括输入检测和受控泛洪两种形式。输入检测方法要求被攻击的系统向网络管理员提供攻击特征，网络管理员据此检测网络各端口以确定攻击的来向，并以此回朔直至源点。这种方法需要很大的管理开销和各个 ISP 之间的协同合作，因此在实现有一定的难度。受控泛洪方法要求对路由器各端口作短暂的突发流量传输，并观察它们对攻击的影响。因为对攻击来向端口的泛洪传输要暂时阻断攻击的继续，因此回朔地使用这种方法对检测服务失效攻击的真实源点有一定的效果。

ICMP 追踪方法要求路由器以一个很小的概率（如 1/20000）抽取转发的报文，并将其报头信息封装在 ICMP 追踪报文中发送给终点地址，接收者可以根据这些 ICMP 报文重构报文的真实传输路径，并发现报文的真实源点。这种方法虽然实现简单，但也容易受到假的 ICMP 追踪报文的干扰，而且许多网络管理域对 ICMP 报文的穿越是有限制的，因此实际可操作性较低。

入侵追踪的完成通常需要多点之间的合作协同，因此一个标准的合作框架对于入侵追踪的协同操作是必不可少的，波音公司和 NAI 公司在 DARPA 的资助下联合研制的 CITRA（Cooperative Intrusion Traceback and Response Architecture）系统是这方面的典型代表[17]。遵从 CITRA 框架的各个 ISP 之间通过边界网关构成相邻关系，并通过 IDIP 实现相互的交互。这些边界网关提供入侵追踪功能和入侵响应功能以实现对入侵者的定位和系统边界控制（如隔离入侵者的访问活动），同时仍然维持正常网络活动的进行。整个框架中存在一个或多个协调中心（称为 Discovery Coordinator），它通过接收各个边界网关的报告和响应政策来确定一个最佳的响应方案，并通知有关的边界网关执行，因此这是一个集入侵追踪与响应于一体的系统。

7. 结论

从总体上看，目前对于大规模互联网络入侵检测问题主要的研究热点大致集中在网络入侵检测的体系结构，异常检测技术，响应技术，入侵检测的协同技术，网络基础设施的保护技术等方面。由于网络节点之间的安全相关性越来越强，所以入侵检测问题必须从宏观的角度，在大规模的网络范围内来研究和解决，这就使得入侵检测系统的体系结构问题变得十分重要，因为检测的协同与响应都与此有关。另外当前的实用 IDS 仅仅能够检测已知的周知事件中的一个小集合，而已经存在的异常检测技术的误报率都比较高，应用并不广泛，所以无论是单点异常检测技术还是分布式异常检测都还是研究的热点。在响应方面，现有的技术不支持安全事件的自动响应，大量地靠专家人工干预，成本太高。因此，提高响应的自动化程度和处理效率是对于 IDS 的广泛应用具有十分重要的意义。

Internet 的核心技术是 IP，它最初的设计原则是争取最大的可用性（availability），考虑的是自治网络组件的行为因素。但构成 Internet 的不仅仅是 IP，还包括应用系统和使用者。因此在 Internet 已经成为全球一个重要的基础设施之后，仅仅考虑可用性是不能满足实际需要的，新的设计原则应当是可生存性（survivability），即要考虑网络中所有对象的行为因素，这其中包括可能的攻击对网络的影响。这种需求的变化使得对网络入侵检测的研究从仅仅针对孤立主机的攻击发展到面向大规模互联网络，也导致对网络基础设施如路由和域名[21]等的可用性的研究也便得比较活跃。

参考文献

[1] Jai Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, E. H. Spafford, Diego Zamboni, "An Architecture for Intrusion Detection using Autonomous Agents", Coast TR 98-05, 1998.

[2] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, D. Zerkle, "GrIDS -- A Graph-Based Intrusion Detection System for Large Networks". The 19th National Information Systems Security Conference. 1996.

[3] http://www.gidos.org/ "Common Intrusion Detection Framework (CIDF)" 相关文档

[4] Diego Zamboni, E. H. Spafford, "A prototype for a distributed Intrusion Detection System", Coast TR 98-06; 1998.

[5] G. Vigna and R.A. Kemmerer, "NetSTAT: A Network-based Intrusion Detection System,"

Journal of Computer Security, 7(1), IOS Press, 1999.
[6] http://seclab.cs.ucdavis.edu/projects/idrds/summary.html IDIP 执行摘要
[7] http://www.ietf.org/html.charters/idwg-charter.html IDWG 相关文档
[8] S.T. Eckmann, G. Vigna, and R.A. Kemmerer, "STATL: An Attack Language for State-based Intrusion Detection," in Proceedings of the ACM Workshop on Intrusion Detection, Athens, Greece, November 2000.
[9] G. Vigna, S.T. Eckmann, and R.A. Kemmerer, "Attack Languages," in Proceedings of the IEEE Information Survivability Workshop, Boston, MA, October 2000.
[10] Robbert van Renesse, Yaron Minsky, and Mark Hayden., "A Gossip-Based Failure Detection Service", September 1998. June, 1998. In Proc. of Middleware '98. England.
[11] Marceau, Carla "Characterizing the Behavior of a Program Using Multiple-Length N-grams," Proceedings of the New Security Paradigms Workshop 2000, Cork, Ireland, Sept. 19-21, 2000.
[12] S. F. Wu, H.C. Chang, F. Jou, F. Wang, F. Gong, C. Sargor, D. Qu, R. Cleaveland, JiNao: Design and Implementation of a Scalable Intrusion Detection System for the OSPF Routing Protocol, Journal of Computer Networks and ISDN Systems, 1999.
[13] http://www.net-tech.bbn.com/projects/erids/erids-index.html, ERIDS 项目主页
[14] Timothy Fraser, Lee Badger, Mark Feldman, "Hardening COTS Software with Generic Software Wrappers," in the proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 1999.
[15] D. Schnackenberg, K. Djahandari, and D. Sterne, "Infrastructure for Intrusion Detection and Response", to be published in DARPA Information Survivability Conference and Exposition (DISCEX), Hilton Head Island, SC., January, 2000.
[16] Matt Blaze, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis, The KeyNote Trust-Management System Version 2, RFC2704, 1999.9.
[17] D. Schnackenberg, K. Djahandari, and D. Strene, Harley Holiday, Randall Smith, "Cooperative Intrusion Traceback and Response Architecture (CITRA)", Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEXII), June 2001.
[18] Rich Feiertag, Cliff Kahn, Phil Porras, Dan Schnackenberg, Stuart Staniford-Chen, Brian Tung, A Common Intrusion Specification Language (CISL), http://www.isi.edu/~brian/cidf/drafts/language.txt, 1999.6.
[19] S. Savage, et. al., Network Support for IP Traceback, IEEE/ACM Transaction on Networking, Vol.9 No.3, June 2001
[20] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer., Hash-Based IP Traceback, Proceedings of the ACM/SIGCOMM 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 3-14, San Diego, CA, August 2001.
[21] S. Cheung and K.N. Levitt. 2000. "A Formal-Specification Based Approach for Protecting the Domain Name System." Proceedings of the International Conference on Dependable Systems and Networks, New York City, New York, June 25-28, 2000, pp.641-651.

Intrusion Detection in Large-Scale Network[2]

Jian Gong　Sheng Lu

（Computer Department, Southeast University　Nanjing 210096）

Abstract：The security is getting more dependent among inter-connected networks, so that the effective intrusion detection must be done in a large scale. The state-of-art of intrusion detection technology in a large-scale network has been introduced in the paper, some hot topics, such as the architecture of IDS, abnormally detection, response technology, coordinated detection, and the technologies used to protect network infrastructure are discussed in detail. Some future trends are mentioned as well.

Key Words：Intrusion Detection System，Abnormally Detection，Response to Intrusion，Coordinated Detection，Intrusion Trace-back，Network Security。

[2] The paper is supported by NNSFC, grant number 90104031.