基于 Jini 的封闭式网络中攻击源追踪系统模型研究

彭云鹏　李　华　吴中福　张简政
（重庆大学计算机学院　重庆 400044）

摘　要　入侵检测系统是现有网络安全系统的重要组成部分。现有的入侵检测系统可以检测大多数基于网络的攻击，但不能对攻击源进行追踪。据此，结合 Jini 技术和现有入侵检测技术提出了网络攻击源追踪模型，简单介绍了 Jini 技术，阐述了该系统的设计思想、体系结构和各部分的主要功能。最后，从实用性和攻击精度等方面对系统可能存在的问题进行了分析。

关键词　Jini，入侵检测，攻击源追踪，网络监听

Study of a Framework of Network Attacker-Tracing System Based on Jini

PENG Yun-Peng　LI Hua　WU Zhong-Fu　ZHANG Jian-Zheng
(Dept. of Computer, Chongqing University, Chongqing 400044)

Abstract　Intrusion detection system is an important part of present network security system. The intrusion detection systems available can detect most network-based attacks, but can't locate the real attackers. On the basis of the existing techniques and Jini, this paper presented a framework of network attacker-tracing system. The paper then introduces Jini and provides the design idea , the architecture and the principal functions of this system. At last, it analyses the potential problems of this system, for example, pracpicability and precision.

Keywords　Jini, Intrusion detection, Attacker-tracing, Network monitoring

1　引言

现有的入侵检测系统可以实时地监控网络和主机系统的活动，实时地发现攻击行为并采取相应的措施，以避免攻击的发生或尽量减少攻击造成的危害。但为了从管理和法制上惩治攻击者的行为，在实际的安全保障系统中，除了需要提供入侵检测功能之外，更重要的是追查攻击的源头（如地址、标识等），从而为打击计算机网络犯罪提供取证。现有的入侵检测系统侧重于对攻击的发现与防范，尽管可以检测到大多数基于网络的攻击，但均不能提供对攻击的真正来源追踪。因为对于入侵的追踪比较难，攻击者为了避免身份的暴露，惯用的手法是首先攻破一个系统，然后利用它作为平台，使用网络跳转（HOP）的办法来攻击另一个系统，很多情况是经过多次跳转才到达真正的攻击目标。

本文提出的网络攻击源追踪系统旨在弥补这一缺陷，其基本原理是在一个可控或相对封闭的网络系统中的每个共享网段内，均安装一个或多个监听器，监听器将网中的入侵报警信息发送给局域网管理器。一旦某个监听器发现入侵，则可以通过局域网管理器之间的协同工作，确定攻击者所在的网段，甚至确定其攻击来源。而多个局域网管理器的互相协作是利用 Jini 来实现的。

2　Jini 分布式计算模型

Jini 是 SUN 公司于 1999 年 1 月 25 日正式公布的一种基于 JAVA 的全新的分布式计算模型，其结构如图 1 所示。其核心是其中的查找服务器。当整个系统中出现一个新的服务器 1 时，第 1 步，服务器 1 就会把一个与自己通讯的通讯接口发布到 Jini 系统中的查找服务器，该通讯接口包括了与服务器 1 通讯的规则，以及针对不同的失败形式提供的不同应对机制；第 2 步，凡是 Jini 系统中需要使用到服务器 1 的客户，如图中的服务器 2，只需要通过到查找服务器下载该服务器的通讯接口；第 3 步，服务器 2 通过该接口直接和服务器 1 通讯，并使用服务器 1。

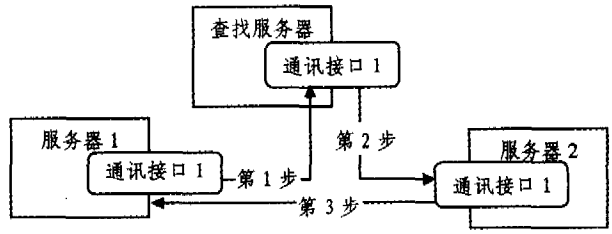

图 1　Jini 结构图

3　基于 Jini 的网络攻击源追踪系统的设计思想

3.1　设计思想

本系统应是一个分布式入侵检测与追踪系统，能够对攻击者的入侵行为进行识别与追踪。

系统的主要设计思想是：利用分布在网络中和服务器上的监听器对网络中传输的报文和服务器上的关键数据进行监听，识别并记录攻击行为或异常现象，对攻击的来源进行追踪、记录。

本系统的主要设计原则是：(1)将整个封闭系统中的跟踪

彭云鹏　硕士研究生，主要研究方向：计算机网络安全；**吴中福**　教授、博士生导师，主要研究方向：计算机网络安全；**张简政**　硕士研究生，主要研究方向：计算机网络安全。

系统按不同的局域网划分成几个小的系统，每个小的系统只解决本局域网内部的跟踪问题，使问题简化；(2)将各个局域网的入侵跟踪系统与该局域网本身划分开来，使局域网本身的性能不受入侵跟踪系统的影响，而跟踪系统的网络监听器对局域网本身是透明的，且网络监听器只负责监听，不在网络中发送任何信息，保护了入侵跟踪系统本身。

3.2 架构模型

本系统主要由多个监听器 ND、多个局域网管理器 SNM 和一个控制管理器 CM 组成，其总体结构如图 2 所示。

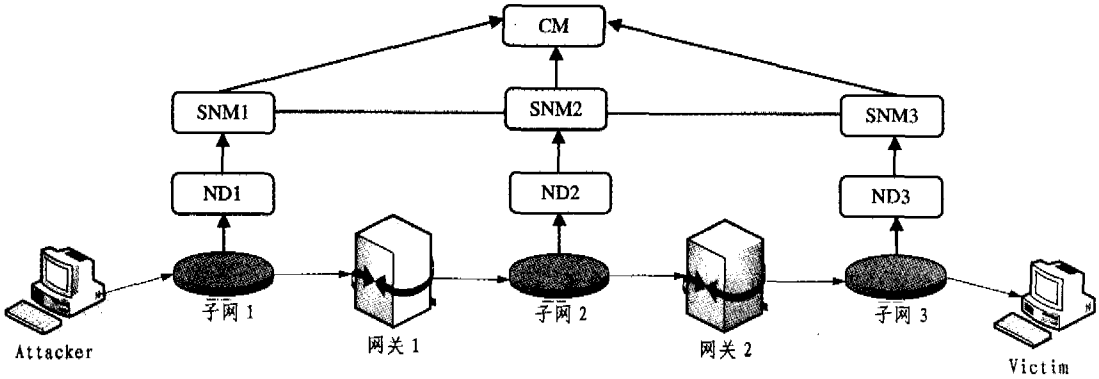

图 2 跟踪系统架构模型图

其中各个局域网管理器 SNM 之间、监听器 ND 与局域网管理器 SNM 之间、局域网管理器 SNM 与控制管理器 CM 之间的通信由 Jini 来实现。两个结点(包括：监视器 ND、局域网管理器 SNM、控制管理器 CM)之间要通讯的时候，只需通过到跟踪系统内部的查找服务器处下载该结点的通讯接口就可以实现通讯。这样，可以让整个系统变得更灵活，很容易地添加网络监听器及局域网管理器，使得当局域网内部网络拓扑改变和扩大跟踪系统监视范围的时候更加容易实现。

在图 2 中，攻击者(Attacker)通过网关 1 和网关 2 对攻击目标(Victim)发动攻击，此时 Victim 收到的攻击报文源地址是子网 3 的内网地址，ND1 在时刻 t_1 截获的攻击类型标识为 S 的攻击信息，ND2 在时刻 t_2 截获从网关 1 到网关 2 的攻击标识类型也为 S 的攻击信息，ND3 在时刻 t_3 截获从网关 2 到攻击目标的攻击标识类型同样为 S 的攻击信息。当 t_3 时刻 ND3 检测出该攻击时，SNM3 分析出该攻击来自于网关 2，于是通过与网关 2 连接的其他局域网管理器(图中为 SNM2)，经过 SNM2 在查找服务中提供的接口与 SNM2 协商，并由 SNM2 提供与当前跟踪相关的攻击信息。同样，SNM2 也要求 SNM1 提供相关信息，再通过 SNM2 最后返回给 SNM3，SNM3 把该攻击路径提交给 CM 处理。

4 基于 Jini 的网络攻击源追踪系统模型的组成与功能

4.1 监听器(ND)

ND 位于各子网内及服务器上，负责监听该网段的数据报文和服务器上关键数据的访问情况，将收集到的数据采样过滤，并将可疑攻击信息发送到 SNM。其重要特点是它们的存在对于网段中其他结点是不可见的，不影响信息的传输，对网络流量影响极小。一个局域网内可安置多个 ND，分别监听不同类型和不同源目的地址的报文，从而减少每个 ND 的负担。每个 ND 包括三个模块：

①监视探针：以“混杂”模式监听网络中的报文，根据监视策略提取出相应的攻击报文；

②监视策略：根据不同的要求和特点制定的监视计谋；

③监视载体：提供站点管理和设置监视策略，并负责将相关数据提供给 SNM；

当然，监视器可根据不同的要求采取不同的监视策略和不同的实现方法，但要求支持 Jini，且对外通讯采用统一的接口。

4.2 局域网管理器

局域网管理器负责记录和协调各个 ND 之间的工作，以实现局域网内的跟踪行为；各 SNM 之间协同工作，以实现整个封闭网络中的跟踪行为。有两种情况会触发跟踪行为：当本局域网内的 ND 向 SNM 发送“发现攻击信息”的消息；当别的局域网内的 SNM 向它发送“发现攻击信息”的消息。通过 SNM 对外提供统一接口，将两种情形统一起来，可以把其它局域网内的 SNM 简化成一个特殊的 ND。这个特殊的 ND 和一般的 ND 之间的区别在于前者要返回一条攻击路径而后者则不用返回。整个过程的流程图如图 3 所示，其中“是否有相关性记录”部分的判断条件有 3 个：

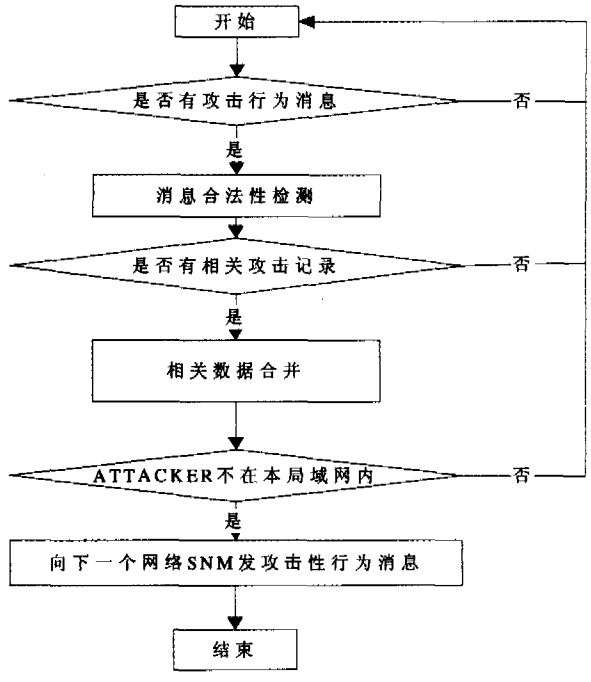

图 3 局域网管理器数据处理过程流程图

(下转封四)

(上接第 85 页)

①攻击类型相同;

②检测到的攻击时间间隔在一定范围内;

③一条攻击记录的目的源 IP 地址与另外一条攻击记录的源 IP 地址相同。

对于存在相关性的两条记录,系统将产生一条攻击链路并保存在数据库中。然后判断当前已知攻击路径的起点是否在本局域网。如不在,向该起点所在局域网的 SNM 发送"发现攻击消息"。如此反复,直至查到攻击源为止。最后,攻击路径层层返回到最开始发出"发现攻击消息"的 SNM,该 SNM 将该攻击路径保存到数据库后将攻击路径返回到 CM,由 CM 决定应当采取的相应措施。

4.3 控制管理器(CM)

控制管理器上运行 Jini 查找服务支持整个跟踪系统的运行,同时接收和保存各个 SNM 发来的攻击路径,并采取相应措施。另外,控制管理器还包括对各个 SNM 以及 ND 的控制管理功能。

4.4 问题分析

攻击源的追踪精度取决于监听器所处的网络位置。即如果监听器处于以太网段内,则可以确定攻击者所处的网段地址,此时在同网段的攻击者仍然可以假冒其他主机。如果监听器处于内部网络的出口处,则可以确定攻击者所处的内部网络地址,此时在同一网络内的攻击者仍然可以假冒其他主机。高明的攻击者普遍采用跳板的形式,先入侵某台机器,以其为跳板展开攻击。如安放一个定时发作的攻击程序,时间的跨度可以是几天甚至几个月,令相关性分析变得非常困难或几乎不可能。

结束语 入侵检测、应急反应与攻击源追踪是网络安全系统的重要组成部分,国内现有的研究工作和所开发的安全产品主要集中在前两个方面,而攻击源追踪技术尚未见到公开报道,更没有相应的产品出现。本文结合现有的入侵检测技术提出了基于 Jini 的网络攻击源追踪系统的模型,给出了利用相关性分析和各个局域网的跟踪管理器 SNM 协作对攻击者的攻击路径进行回溯的基本思想,为封闭网络中的攻击源跟踪提供了一个方案,并正按此为下一步试验做准备。

参 考 文 献

1 Denning D E. An Intrusion-detection model[J]. IEEE Transactions on Software Engineer, 1987, 13(2): 222~232

2 唐正军. 网络入侵检测系统的设计与实现[M]. 北京:电子工业出版社,2002

3 Edwards W K. Jini 核心技术. 北京:机械工业出版社

4 蒋文保,杨大鉴,任晓明. 宽带网络入侵检测系统的分析与实现. 计算机工程,2003

5 孙海军,徐良贤,杨怀银. 针对网络入侵检测系统的攻击与防御. 计算机工程与应用,2002

6 应向荣. 入侵检测(IDS)技术的发展. 信息技术与应用,2002

计算机科学

(1974 年 1 月创刊)

第 33 卷第 1 期 (月刊)

2006 年 1 月 25 日出版

ISSN 1002-137X

CN50-1075/TP

定价:30.00 元 国外定价:5 美元

邮发代号:78-68

发行范围:国内外公开

主管单位:国家科学技术部

主办单位:国家科技部西南信息中心

编辑出版:《计算机科学》杂志社

重庆市渝中区胜利路 132 号 邮政编码:400013

电话:(023) 63500828 E-mail:jsjkx@swic.ac.cn

网址:www.jsjkx.com

社 长:牟炳林

总 编:彭 丹

主 编:朱宗元

主编助理:徐书令

印 刷 者:重庆科情印务有限公司

总发行处:重庆市邮政局

订 购 处:全国各地邮政局

国外总发行:中国国际图书贸易总公司(北京 399 信箱)

国外代号:6210-MO