分布式网络实时取证系统研究与设计

戴江山，肖军模，张增军

(解放军理工大学通信工程学院 南京 210007)

【摘要】在分析目前网络体系中存在的不利于网络取证的问题的基础上，提出和设计了一种分布式网络实时取证系统。该系统通过不断监视和分析网络内部的运行情况，在保护网络安全的基础上，确定网络入侵者的行为是否已构成犯罪，然后提取和分析入侵者犯罪证据信息，并实现证据信息的完整性保护和验证。最后，通过时间线性化实时融合，生成入侵者犯罪证据。

关 键 词 网络安全； 网络取证； 分布式； 数字证据

中图分类号 TP309 文献标识码 A

Research and Design of a Distributed Network Real Forensics System

DAI Jiang-shan，XIAO Jun-mo，ZHANG Zeng-jun

(Institute of Communications Engineering, PLA University of Science and Technology Nanjing 210007)

Abstract Based on the discussion of the weakness of the network forensics in current Internet system, a distributed real network forensics system is proposed and designed. This system monitors and analyzes the state of the local network. When the Internet intruder is found, on the base of the security of the local network, the system confirms whether crime has happened, and then captures and analyzes the intruding evidence information, protects the integrity of them, finally, produces the intruding crime evidence.

Key words network security; network forensics; distributed; digital evidence

目前，在意识到单纯依靠技术手段已远远不能阻止网络入侵事件发生的情况下，人们开始考虑借助于法律手段去维护网络合法使用者的权益和对网络入侵者进行威慑和惩罚。网络取证就是为了揭露已经发生的入侵、破坏、危及系统安全的网络犯罪行为，采用科学的技术手段从多数据源收集、融合、鉴别、调查、分析和建立数字证据的过程 [1]。目前的网络体系对于实现网络取证还存在许多不足，如网络缺少收集、存储和转发证据信息的系统设计；网络和系统日志可靠性差，不能满足取证分析要求；网络流量的迅速增长和系统存贮空间局限的矛盾，使对证据信息的处理速度难以提高，对证据信息的存贮方式难以更新；数字证据容易消失；取证过程大多采用手工完成等。为此，本文提出并设计了一种分布式网络实时取证系统。

1 分布式网络实时取证系统结构

分布式网络实时取证系统包括网络取证控制中心ForCenter和网络取证用户代理ForAgent，如图1所示。

网络取证控制中心通过对内部网络数据流的捕捉和分析，对网络的运行情况进行实时监控。当发现入侵企图或入侵事件时，ForCenter将根据威胁等级确定是继续实施监控或是立即开始取证。如果确定开始取

收稿日期：2003 – 11 – 21
基金项目：国家自然科学基金资助项目(69931040)
作者简介：戴江山(1973 –)，男，博士生，主要从事网络信息安全方面的研究.

证，ForCenter将启动被入侵主机的网络取证用户代理ForAgent和自身相应的功能模块，开始收集和提取有关证据信息，并对证据信息进行完整性处理和存储，并实时融合生成入侵证据。

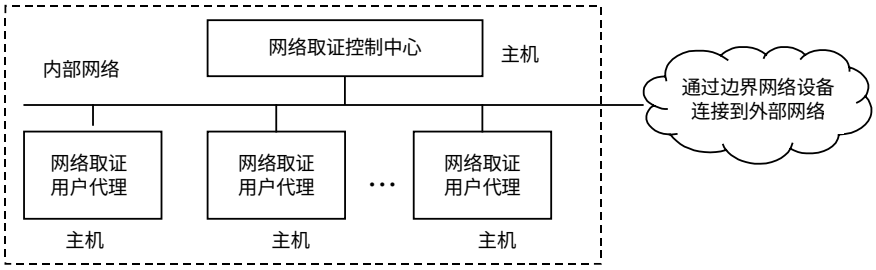

图1 分布式网络实时取证系统结构图

为掌握入侵者真实的入侵目的和获取入侵者确凿的犯罪证据，被入侵主机的网络取证用户代理ForAgent启动后，在保证系统安全的情况下，将允许入侵者在可控制范围内进行一定程度的操作。在此期间，ForAgnet记录入侵者在系统内的操作信息，并将提取、存储、规范和完整性处理后的证据信息，连同系统日志内的有关证据信息发送到ForCenter进行证据融合。ForAgent将对入侵数据包的内容进行阻止和清洗，以防止主机系统遭到破坏或敏感信息外流。此外，系统管理员也通过取证控制中心适时阻断入侵连接。

2 分布式网络实时取证系统组成

2.1 分布式网络实时取证控制中心**ForCenter**

分布式网络实时取证控制中心ForCenter包括入侵检测模块、入侵证据提取模块、证据信息完整性处理模块、通信模块、监视与控制模块、入侵命令解析模块、证据融合模块和证据信息库，如图2所示。

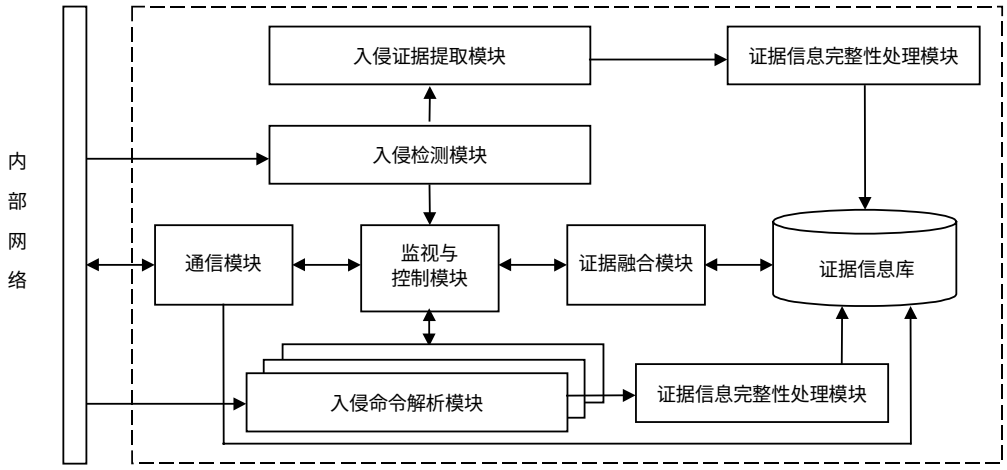

图2 分布式网络实时取证控制中心结构图

2.1.1 入侵检测模块

入侵检测模块通过对数据包的捕捉和分析，检测内部网络的运行情况。当发现网络出现异常行为时，入侵检测模块确定被攻击的目标主机，判断异常情况的威胁等级，并对有关信息进行日志记录。入侵检测模块采用基于规则的网络入侵检测系统snort，按系统要求进行配置和改造。

根据系统要求，首先对入侵检测日志记录进行配置，要求每条日志记录包括应用层在内的完整数据，并打上时间戳后记录到日志文件中。然后将规则库中的规则划为警告和危险两个威胁等级，将探测扫描、连接企图、缓冲区溢出企图等规则定为警告级；而将表明系统已被入侵的响应规则定为危险级。对于警告级，可由系统管理员通过监视与控制模块确定是否进行网络取证；对于危险级，表明已有入侵事件发生，系统自动启动入侵命令解析模块、入侵证据提取模块，并通过通信模块启动被攻击主机的取证用户代理。

2.1.2　证据信息完整性处理模块

证据的法律效力就在于证据的客观性和真实性。证据信息完整性处理模块能实现对证据信息的完整性保护，防止证据信息被删节、篡改和伪造，并能向第三方证明证据信息的完整性。证据信息完整性处理过程如图3所示，图中H_{id}表示被入侵主机标识符，A_j表示第j条证据信息记录消息鉴别运算密码，D_j表示需要完整性处理的第j条证据信息记录，H表示单向散列函数的安全散列算法(Secure Hash Arithmetic, SHA)[2]，消息鉴别码(Message Authentication Code, MAC)表示消息鉴别运算函数，采用三重数据加密标准(Three Times Data Encryption Standard, 3DES)加密[2]，以运算速度较快的SHA计算散列值。

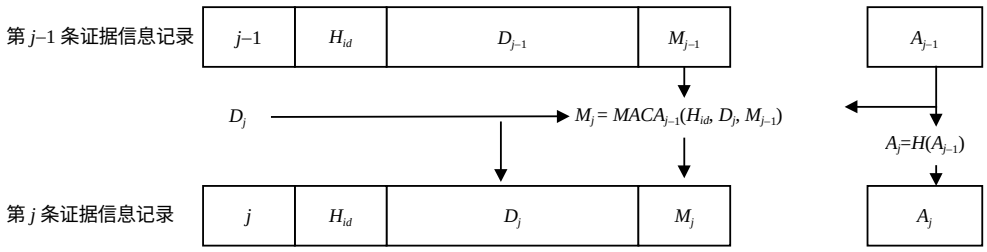

图3　证据信息完整性处理过程图

1) 分布式网络实时取证系统安装后，首先在司法机关认可的网上认证中心进行软件注册，并要求产生和保存随机的A_0，A_0对系统用户完全保密并定期更换。

2) 对于输入的第j条证据信息记录D_j，以A_{j-1}为密码，以H_{id}，D_j和第$j-1$条记录中的消息鉴别码M_{j-1}组成的序列为对象，经MAC运算后产生第j条证据信息记录的消息鉴别码M_j。M_j产生后，按照图3所示存储格式生成第j条证据信息记录并写入相应的证据信息文件。A_{j-1}经SHA运算后产生A_j，A_j作为产生下一条证据信息记录的消息鉴别加密密码，删除A_{j-1}。

鉴别密码A_j是整个安全策略的核心。初始鉴别码A_0由认证中心产生，并对系统用户保密，防止取证系统用户完全伪造证据信息文件。如果有人对证据信息文件的完整性提出质疑，可以请认证中心出示A_0，对证据信息文件进行验证。每次A_j产生后，要立刻删除A_{j-1}，防止任何人获得A_{j-1}后进行推导，伪造攻击。通过消息鉴别码M_j将相邻证据信息记录进行关联，可以防止证据信息记录被部分删节、篡改和伪造。

2.1.3　其他主要模块

入侵命令解析模块采用插件库的形式，根据被入侵主机的IP地址捕捉入侵数据包和解析入侵者入侵命令。内部网络在防火墙等边界网络设备的防护下，通常可选择性地提供ftp、telnet、http和e_mail等服务，因此建立各种服务的命令插件库并随时扩充。入侵命令解析模块捕捉到入侵数据包后，根据入侵检测模块识别出的入侵模式，调用相应的插件库如ftp命令库、telnet命令库等对捕捉到的入侵数据包进行匹配解析，得到入侵者入侵操作的命令，然后经证据信息完整性处理后发送到证据信息库中。

入侵证据提取模块从入侵检测模块日志中提取有关入侵证据信息，并经完整性处理后发送到证据信息库中。成功的网络入侵通常需要对目标进行长时间的探测和扫描，广泛收集目标的相关信息，建立该目标网络结构、网络访问能力以及安全情况的剖析图，围绕收集到的信息制定相应的入侵计划，入侵者才能利用获得的目标信息发掘系统配置的错误或漏洞，设法进入目标系统[3]。而入侵者对目标系统探测和扫描的信息往往被记录在入侵检测模块日志中。

通信模块负责网络取证控制中心与用户取证代理之间进行的命令和数据交互。取证控制中心通过通信模块向被入侵主机用户取证代理发送启动命令、阻断保护命令和负责接收用户取证代理发送来的证据信息，以及将该信息转发往证据信息库。

证据融合模块提取和融合证据信息库中存储的证据信息，实时构造出入侵者的入侵犯罪过程。证据信息库中存贮的证据信息包括来自于取证用户代理、入侵检测日志以及入侵检测模块的证据信息。此外，还可以包括来自于防火墙、路由器日志等虽没有经过完整性处理，但可以作为辅助证据的证据信息。证据融合模块根据入侵的通常过程，采用时间线性化的方法实时建立和显示入侵者犯罪证据。入侵犯罪证据内容

通常的顺序包括入侵者扫描探测的证据、获取主机shell权限的证据[4]、侵入系统后的上传下载文件或执行某些命令的操作证据等。对于必须进行信息交互而难以进行IP伪装的攻击，系统根据入侵数据包的IP地址识别出入侵者的位置。入侵犯罪证据生成后，系统可以申请网上司法部门认可的认证机构加盖时间戳以保护证据的完整性[5]。

2.2 分布式网络实时取证用户代理**ForAgent**

分布式网络实时取证用户代理包括证据信息提取模块、完整性处理模块、通信模块和过滤器。

证据信息提取模块实时监控和捕捉入侵者在系统内的操作，提取出相应的操作内容并经完整性处理后，通过通信模块发送到证据信息库。目前，随着加密技术的发展，攻击者可以非常方便地利用安全命令行界面远程登录(Secure Shell, SSH)，安全复制(Secure Copy, SCP)等加密手段与被入侵主机进行交互。企图通过解密的方法提取入侵者的操作内容是异常困难的，可以设法绕过解密方法，如在系统内核以New_read()函数替代原有read()系统函数，在加密数据刚被解密的情况下，将内容复制到相应缓冲区内以得到明文内容。

为了更加确凿地获得入侵者的犯罪动机和犯罪事实，在入侵者已经侵入主机系统后，对于流入和流出被入侵主机的数据流，系统并不是单纯地阻止，而是通过过滤器修改或扼杀攻击者行为，使入侵者只能够在可控制的范围内进行一定的操作，而这种操作不会对系统造成危害。例如在ftp连接中，入侵者通过某些命令，要求被入侵系统向外传输某些敏感文件，过滤器通过规则匹配鉴别和修改流经的入侵数据包数据内容，攻击者虽能看到已经登录到的目标系统，数据包也能有效返回，但不能获得应有信息，这样既能保护系统安全，又可以在一定时间内对入侵者进行更好的控制和取证。

过滤器采用阻止规则集和替代规则集两个规则集。阻止规则集主要针对流入数据包，作用是阻止流入数据包失去控制而对系统造成破坏，对于与阻止规则相匹配的危害系统安全的数据包，要立即阻止其流入和执行。替代规则集主要针对流出数据包，作用是防止系统的敏感信息外流和入侵者以该系统为跳板攻击其他系统。对于与替代规则相匹配的数据包，要根据规则清洗数据包内容，然后转发。

3 结 束 语

本文研究和设计了一种分布式网络实时取证系统。该系统实时检测内部网络运行情况，对于入侵企图和入侵行为，在保证系统安全的情况下，能够有效地实现对入侵犯罪证据的获取，并能保证证据信息的真实性和可靠性。目前，网络取证研究无论在理论还是在实现方面都还有许多工作要作，如世界各国之间达成对网络证据认可的标准；建立有利于网络取证的网络设备、网络系统和协议；建立司法机关认可的证据认证机构等等。可见，对网络取证的研究和实现还需要不懈的努力。

参 考 文 献

[1] Palmer G . A road map for digital forensics research[R]. Report From the First Digital Forensics Research Workshop (DFRWS), 2001

[2] Schneier B著. 应用密码学协议、算法与C源程序[M]. 吴世忠, 祝世雄, 张文政译. 北京: 机械工业出版社, 1996

[3] McClure S, Scambray J, Kurtz G著. 黑客大曝光[M]. 刘 江、杨继张、钟向群译. 北京: 清华大学出版社, 2003

[4] Howard J D. An analysis of security incidents on the internet 1989-1995[D]. Pennsylvania: Carnegie Mellon University, 1997

[5] Haber S, Stornetta W S. How to time stamp a digital document[J]. Journal of Cryptology, 1991, 3(2): 99-11

编 辑 熊思亮