基于 Windows 平台的动态取证系统①

文少勇[1]，王 箭[1]，李 剑[2]

[1](南京航空航天大学 计算机科学与技术学院，南京 210016)
[2](南昌陆军学院 战斗实验室，南昌 330103)

摘 要：针对目前一些动态取证模型的不足，在分布式网络取证模型的基础上设计了一个基于 Windows 平台的动态取证系统，能够实现网络中的计算机作为作案目标和作案工具双重角色时的取证，具有实时获取多种数据源、取证过程隐秘、取证分析算法可扩展等特点。介绍了动态取证系统中各功能模块设计，并阐述了系统设计中涉及到的关键技术，最后通过模拟测试表明该系统能够在 Windows 网络下实现动态取证。

关键词：计算机取证；动态取证；获取技术；隐秘技术

Dynamic Forensics System Based on Windows Platform

WEN Shao-Yong[1], WANG Jian[1], LI Jian[2]

[1](College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)
[2](Battle Laboratory, Nanchang Army College, Nanchang 330103, China)

Abstract: In view of the shortages of some dynamic forensics model at present, this paper designs a dynamic forensics system in distributed network forensics model based on Windows platform, which can realize obtaining evidence on the computers that plays a dual role on the network as crime goals and crime tools, and have the characteristic of real-time accessing various data sources, forensics process secretive, forensic analysis algorithm extensible etc. This paper introduces the designing of each function module in the dynamic forensics system at first. Second, it lays out the key technology that appears in the design process of the system. Finally, simulation test indicates that the system can realize dynamic forensics in Windows network.

Key words: computer forensics; dynamic forensics; acquire technology; hiding technology

1 引言

计算机技术与网络通信技术的发展，在给人们带来便利的同时，发生在计算机领域中的各种犯罪（如计算机诈骗、商业机密信息的窃取与破坏、电子商务纠纷、对政府、军事网站的破坏等）在逐年剧增。研究如何打击计算机犯罪、提取和分析计算机犯罪证据并证明该证据是原始的、完整的、合法的、有效的新型学科——计算机取证学由此应运而生。

在计算机犯罪案件中计算机扮演着作案目标和作案工具双重角色，无论作为哪种角色，计算机系统中都会留下大量的与犯罪有关的数据。因此给出的计算机取证(computer forensic) 的定义是“计算机取证就是对计算机犯罪的证据进行获取、保存、分析和出示，它实质上是一个详细扫描计算机系统以及重建入侵事件的过程”[1]。根据取证时证据的特性，计算机取证可以分为静态取证和动态取证。静态取证又称为事后取证、被动取证，随着网络犯罪技术的提高，事后取证已无法适应要求，解决方案是进行实时取证，也称动态取证。

目前常见的动态取证系统有基于入侵检测的动态取证系统[2]、基于入侵容忍的蜜罐网络取证系统[3]、基于 Agent 的分布式网络取证系统[4]、基于人工免疫动态取证系统[5]等，但这些系统还存在着一些不足，比如基于入侵检测的动态取证系统仍然存在着误报率和

① 收稿时间:2011-05-24;收到修改稿时间:2011-06-10

漏报率高的问题；利用蜜罐取证的缺陷是只能捕获到入侵者进入蜜罐区的攻击行为，而不能捕获进入应用区的攻击，对这样的系统获得的信息是否能作为法律认可的证据，仍是一个有争议的问题；对动态取证中获取的海量数据如何高效地分析出具有计算机犯罪特征的数据还面临一些技术难题。此外，目前大多数动态取证系统把重点放在来自于外部入侵者的犯罪行为的取证上，而忽略了内部人员犯罪行为的取证。由于内部人员熟悉网络的结构和取证系统的运行机制，他们实施犯罪活动（如军队内部人员利用军网泄密或者个人利用公司网络发布违法言论等）时，往往能绕过取证系统，使取证系统失效。所以设计出一个既能对外部入侵行为取证，又能对内部人员犯罪行为取证的系统已经成为一个迫切需要。

本文针对目前一些系统中存在的不足，在分布式网络取证模型的基础上设计了一个基于 windows 平台的动态取证系统，该系统具有证据获取效率高、取证过程隐秘、取证分析算法可扩展等特点，主要解决网络中的计算机作为作案目标和作案工具双重角色时的取证。

2　基于windows平台的动态取证系统

2.1 关键需求分析

首先要考虑两方面的取证工作：一方面是来自网络外部的以计算机系统为攻击目标的犯罪行为，另一方面是来自网络内部的以计算机为工具的犯罪行为，所以需要取证过程具有隐秘性。

其次考虑到电子证据的可靠性，需要实时、高效地采集多种数据源。

第三是考虑到网络中各主机的数据量非常大，要完全依靠人工进行分析，其工作量将不可接受，所以还需要一种对计算机取证获取的信息进行自动分析的方法。本系统将数据挖掘技术应用到计算机取证分析中，它能从海量的数据中发现有价值的知识和信息。

此外在平台的选择方面，考虑到 Windows 系统是目前使用最多的操作系统，针对该系统发生严重的计算机犯罪案件比较多，研究 Windows 系统下的计算机取证不但具有理论价值，也具有重大的现实意义。本文选择对 Windows XP 系统网络环境下的各个主机进行动态取证。

2.2 取证系统结构

本系统分为取证服务器端和取证客户端，如图 1 所示。取证客户端安装了入侵检测系统（IDS），分布于网络中的各个主机实现分布式入侵检测。取证客户端将所采集的电子数据证据加密后传送到安全的服务器端进行统一的收集，经过数据预处理后按照统一的格式存入数据库以方便后续的查询与分析活动。对于已经获取的电子数据证据由证据分析模块进行分析产生规则库并对具有犯罪嫌疑的证据进行提取，加密签名后存入证据库。产生的新规则又反馈给客户端的入侵检测系统，使其具有学习功能，进而能检测出新的异常行为。而整个系统的统一管理则由管理控制模块实现，确保系统稳定运行。

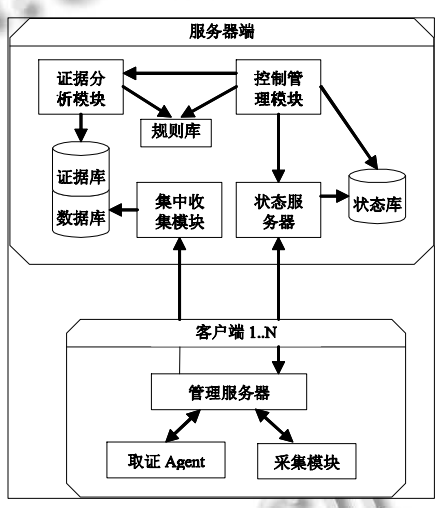

图 1　系统总体框图

2.3 系统功能模块和结构设计

我们假设网络中有 N 台主机，则有 N 个客户端。客户端安装在网络中的每一台主机上，分别负责监测每一个主机的活动，它由以下几个模块组成：

① 取证 Agent：在该模块中引入了 IDS，负责分析主机上的活动，当监测到某种可疑事件时，立即触发数据采集模块按照特定的策略采集数据。

② 数据采集模块：负责采集主机上的各种数据源，包括：日志文件、注册表、正在运行的程序、键盘操作记录、网络数据包等。

③ 管理服务器：接收来自服务器的命令，管理取证 Agent 和数据采集模块，并把采集到的数据进行分类，加密签名后发送给服务器端。

④ 服务器端安装在一个专门的有安全保障的服务器上，负责收集从各个主机上采集到各种数据，并

将数据进行预处理后存入数据库，以便进行随后的证据分析。它由以下几个模块组成：

⑤ 集中收集模块：接收各个主机传来的数据，解密并验证签名后按分类信息将数据分类存入数据库。我们采用了 mysql 数据库对收到的数据进行存储与组织，可以很方便高效地实现证据的各种删除、插入、修改操作。

⑥ 状态服务器：接收和保存各个客户端的工作状态，并将各状态信息存入状态信息库。

管理控制模块：给网络管理员提供一个管理整个取证系统的用户界面，主要包括监测各客户端的运行状况（通过查询状态信息库），修改生成的规则库或自定义规则，设置取证 Agent 或给取证 Agent 更新规则库，管理采集模块、证据查询、证据导出等。

⑦ 证据分析模块：利用数据挖掘算法对收集到的数据进行分析，产生规则，并提取犯罪证据，存入证据库。管理人员可以导入不同的分析算法，或者对分析算法进行修改、更新。同时管理人员可以根据取证经验自定义犯罪行为规则或者修改、删除分析算法生成的一些无用规则，使分析模块具有很好的扩展性。

3 构建系统的关键技术

3.1 证据获取技术

因为要获取多种数据源，采集模块采用多线程技术对各种数据进行实时收集，主要实现对系统日志、注册表、辑过的文档信息、浏览过的网页信息、正在运行的进程、键盘操作记录，网络数据包等数据源的收集，并且可以根据取证的要求增加线程数，即增加采集器，实现更多数据源的采集。在实现数据采集时，我们借鉴了文献[6]中给出的日志信息、编辑过的文档信息、浏览过的网页信息、运行过的程序采集实现方法和文献[7]中利用 winpcap 进行网络数据包捕获的方法。键盘操作的记录可利用系统勾子实现[8]，但是由于用户在进行键盘操作时，可能录入的是汉字，所以我们不仅需要利用系统钩子获取到录入的键盘字符，还需要考虑录入的是不是汉字。所以我们还需要安装一个类型为 WH_GETMESSAGE 消息钩子，然后在消息处理程序中判断消息标识符是否为 WM_IME_COMPOSITION，即编码状态改变标识，如果是，则先调用 ImmGetContext(hWnd) 获取当前正在输入的窗口的输入法句柄，再用 ImmGetCompositionString（）方法从输入法数据区中获取字符串。

需要采集的另一个重要数据源是系统注册表。windows 操作系统的注册表(Registry)是一个数据文件的集合，包含了很多的有关计算机的硬件、软件和用户的信息。但是一个完整的注册表难以读懂，对动态取证分析意义不大，我们关心的只是注册表在系统运行过程中的改动情况，从而方便地分析出系统在什么时候安装了什么软件、用户增加、修改或删除了哪些目录和文件等，因此获取注册表的改动历史对取证分析意义更大。

本文提出了一个监控注册表的实现方案。该方案首先在初始时备份一份在正常情况下的注册表，然后监测特定的子键或键值是否有改变，如果有改变立即对注册表进行了备份，最后通过对新备份和原备份进行比较，从而获得注册表中改变的位置和内容。

当监控注册表变化时我们使用到一个 API 函数：RegNotifyChangeKeyValue （ HKEY hKey, BOOL bWatchSubtree, DWORD dwNotifyFilter, HANDLE hEvent, BOOL fAsynchronous）

当函数成功返回后，应用程序可通过 WaitfForSingleObject 来等待发生改变的通知。WaitForSingleObject（hchange，dwmilliseconds）中 hchange 为创建的事件句柄，dwmilliseconds 为等待时间值。在事件响应程序中，对注册表进行备份，然后通过与原备份进行比较，最后得出注册表修改的位置和内容，并给出修改时的时间。最后在结束监视程序之前用 FindCloseChangeNotification (hchange) 来关闭句柄。

如要监测预定目录下文件的变化，可通过两个 API 函数实现：FindFirstChangeNotification()、FindN0extChangeNotification()。实现过程与监控注册表变化类似，在这里省略之。

3.2 获取策略

为了高效地获取各种数据，减少采集到海量的无用数据，以便减轻网络通信压力和后面的数据分析压力，就需要制定一个有效的数据获取策略。

我们在各个客户端的取证 Agent 集成了基于误用检测模型的 IDS，对各自的主机的活动进行监测，所有的取证 Agent 可实现一个分布式的 IDS，可检测网络中单机无法检测的协同攻击。同时按照定义的规则库发现主机上有异常行为发生时，立即向管理服务器发出警报，并发布危险等级。危险等级可以根据规则

的危险程度分为正常、警告、危险三个等级。将规则库分为犯罪特征库和异常规则库，而两个库之间的关系为：犯罪特征库异常规则库，即计算机犯罪行为有一定的异常表现。当行为符合犯罪特征时，则发出危险等级；当行为符合异常规则时，则发出警告等级；否则为正常等级。管理服务器则按照相应的危险等级触发采集模块按照一个合适的时间隔采集数据，并根据异常类型有针对性地采集特定数据。采取这种策略能有效减少采集到海量的无用数据。

3.3 取证过程隐秘技术

取证过程隐秘的目的是为了取证活动不被主机用户感知和终止，达到对主机作为作案目标和作为作案工具两种情况下的取证目的，主要涉及到自动加载技术、进程隐藏技术和文件隐藏技术。

(1) 自动加载技术

自动加载目的是在被取证主机运行时，能自动启动取证客户端程序，典型的方法有修改注册表启动项、添加 Windows 任务计划、注册为系统服务。前两种方法操作比较简单，但容易被用户修改，隐藏性较低。在 Windows 2000/XP/2003 系统中，为了节省系统资源，微软把很多服务做成共享方式，交由 svchost.exe 进程来启动。svchost 进程只作为服务宿主，并不实现任何服务功能，只是提供条件让其它服务在这里被启动。注册为系统服务的程序运行稳定，并且在后台运行，在“进程管理器”中不可见，有一定的隐藏性。

(2) 进程隐藏技术

进程隐藏目的是在被取证主机上实施取证工作时，取证进程不被被取证机用户感知。目前具有代表性的进程隐藏技术主要有：Hooking API 技术、远程线程插入技术、动态链接库插入技术等[9]。本系统使用了 Hooking API 技术，它基本思想是：通过特殊的编程手段截获 windows 系统调用的 API 函数，使其他调用这些 API 函数的程序转向 Hook 函数，在 Hook 函数中将需要隐藏的进程信息去掉，然后返回给调用程序，就达到进程隐藏的目的。

(3) 文件隐藏技术

文件隐藏目的有两个，一是隐藏取证程序文件，二是采集到证据之后，在把证据文件传输到取证服务器之前，为了不被用户发现和破坏，隐藏证据文件。在 windows 平台可利用基于文件过滤驱动实现文件隐藏和利用流文件实现文件隐藏等。基于 ADS 的文件隐藏方法就是一个利用流文件实现文件隐藏的有效方法[10]。ADS 即 NTFS 备份数据流（alternative data streams，简称 ADS），是 NTFS 的一个数据流属性，将用户数据存入 ADS 其大小和内容往往对用户是不可见的。

4 系统实现和测试

综合以上技术，我们用 C++编程实现了各个功能模块，系统服务器端的主界面如图 2 所示。

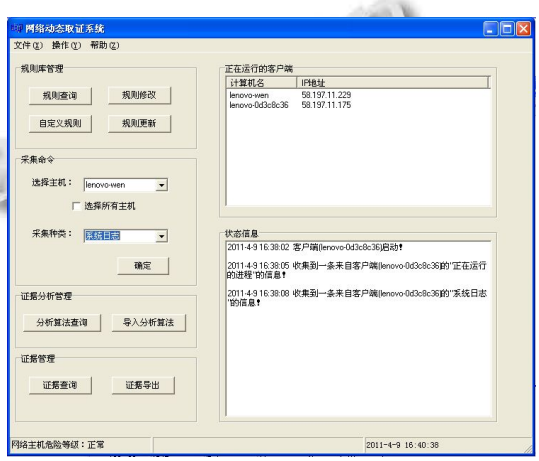

图 2　系统主界面

我们在一个局域网中进行了下列测试：

① 被保护系统上的取证信息范围

证据收集器能够采集各种可能的证据信息。在动态取证系统运行一段时间后，可以在在取证服务器中查询到用户正在运行的进程信息、用户最近编辑过的文件信息、最近访问的网站信息、系统日志信息、注册表修改记录、键盘操作记录、网络数据包信息等。如图 3 所示。此外，这些取证信息的种类还可以通过证据收集器的添加实现扩展。

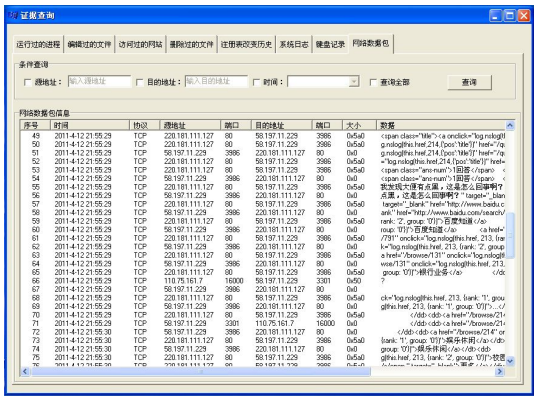

图 3　收集到的网络包信息

②同时对多台被保护主机的取证能力

在动态取证系统运行一段时间后，可以在取证服务器中查询到多台被保护系统的取证信息。这种同时对多台被保护主机进行取证的能力极大地提高了系统的适应性。

③ 客户端的隐秘性

因为已经把客户端程序注册为系统服务，所以客户端在操作系统开机时交由 svchost.exe 进程来启动，并且是在后台运行，在“进程管理器”中不可见，只是在任务管理器中多了一个 svchost.exe 进程，具有较好的隐秘性。

5 结束语

本文设计的基于 windows 平台的动态取证系统具有如下优点：

① 能高效地获取多种数据源。在客户端结合入侵检测系统，实时监控主机中多种数据源，并根据被取证主机的异常情况按照预定的策略收集数据，提高了数据获取的效率，减少了无用的数据。

②具有对网络中各主机在作为犯罪目标和犯罪工具时的动态实时取证能力。使用隐秘技术对取证过程进行了隐秘，在一定程序上避免被保护主机上的相关证据可能受到入侵者或者用户本人的篡改、删除。同时，把证据传输到取证服务器过程中进行了加密签名，保证了证据的安全性、完整性和抗抵赖性。

③ 具有取证信息的易扩展性和灵活的证据处理和分析方式。在本系统模型下可以根据应用环境和需要，对证据采集器的种类、证据分析的方式和分析算法进行调整，使取证系统具有可扩展性。

下一步的改进工作包括采用更多的信息采集技术以扩充取证模型，研究证据分析算法，使取证分析更准确、更高效等。

参考文献

1 王玲,钱华林.计算机取证技术及其发展趋势.软件学报,2003,14(9):1635–1644.
2 吴琪.基于 IDS 的计算机犯罪证据动态取证技术研究. 吉林:吉林大学,2007.
3 杨尚森,胡蓓.基于入侵诱骗技术的主动蜜罐系统的设计.计算机应用与软件,2008,25(1):259–260.
4 Ren W, Jin H. Distributed Agent-Based Real Time Network Intrusion Forensics System Architecture Design. Proc. of the 19th International Conference on Advanced Information Networking and Applications. San Francisco, California, 2005:177–182.
5 丁菊玲,刘晓洁,李涛,等.基于人工免疫的网络入侵动态取证.四川大学学报,2004,36(5):108–111.
6 黄小珊.计算机取证系统的研究与数据挖掘技术在其中的应用.成都:电子科技大学,2008.
7 蔡豪,李娜.基于 WinPcap 的网络数据包捕获的研究.电脑知识与技术,2010,(13):3330–3332,3347.
8 陈栋,林喜竹.基于钩子的计算机监控程序的实现.科技信息,2010,(8):228–228,230.
9 史国川,张璐璐.进程隐藏技术的研究和实现.合肥学院学报,2009,19(2):26–28.
10 陈欣,施勇,薛质,陈俊杰.一种基于 ADS 的文件隐藏技术研究.信息安全与通信保密,2009,(11):106–108.

（上接第 33 页）

造我国重要的战略性优质烟叶基地步伐，推进烟草农业现代化和信息化的跨越式发展。

参考文献

1 鲁韦坤,黄中艳,余凌翔,朱勇.“3S”技术在昭通市现代烟草农业示范区规划信息管理中的应用.中国烟草学报,2010,16(3):72–75.
2 吴孟泉,崔青春,张丽,赵娜.复杂山区烟草种植遥感监测及信息提取方法研究.遥感技术与应用,2008,23(3):305–309.
3 彭光雄,宫阿都,崔伟宏,明涛,陈锋锐.多时相影像的典型区农作物识别分类方法对比研究.地球信息科学学报,2009,11(2):225–230.
4 黄勇奇,赵追.3S 技术平台支持下的烟草轮作查询和规划研究.安徽农业科学,2007,35(11):3219–3221.
5 王晓敏.贵州植烟区土壤重金属污染状况及其对烟叶安全的影响评价.贵阳:贵州大学,2009.
6 陈益银.海拔等因素对鄂西南烟叶发育及品质影响的研究.郑州:河南农业大学,2008.
7 宋春桥,柯灵红,刘喆惠,游松财.基于 ArcGIS Server 的藏北草地资源信息共享平台的设计与实现.安徽农业科学,2010,38(17):9350–9353.
8 彭光雄,胡德勇,陈锋锐,郭继发,崔伟宏.基于空间信息的烤烟种植适宜性评价与轮作规划.地理研究,2010,29(5): 873–882.