

分布式计算机取证模型研究

周 敏, 龚 箭

(重庆理工大学 计算机科学与工程学院, 重庆 400054)

摘 要: 在计算机犯罪发生后对现场信息进行事后的收集, 难以确保证据的真实性、可靠性和完整性. 提出了一个分布式的计算机取证模型, 设计了其中的主要模块, 实现了基于该模型的计算机取证系统. 实验表明, 提出的模型、设计的系统是高效可行的.

关键词: 分布式; 计算机取证; 取证模型; 网络监测

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)02-0040-04

Study on the Distributed Computer Forensics Model

ZHOU Min, GONG Jian

(School of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China)

Abstract: If the data was collected after the computer crime had occurred, it was difficult to ensure that the evidence were authentic, accurate and complete. A distributed computer forensics model was presented in this paper. The main parts of the model were designed, and a computer forensics system based on this model was implemented. Experiments indict that the model presented and the system designed in this paper are efficient.

Key words: distributed; computer forensics; forensics model; network monitor;

1 引言

计算机取证是将计算机调查和分析技术应用于对潜在的、有法律效力的证据的确定与获取上^[1], 包括了对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档^[2]. 目前, 网络入侵已成为最主要的攻击手段, 针对网络入侵的计算机取证大致分为两种: 一是事后的静态取证, 是在案发后、使用技术手段对相关计算机进行取证, 主要是对损坏的文件进行恢复和分析, 同时提取相关的信息; 二是实时的动态取证, 是在网络中随时监测、记录被保护计算机的状态数据, 一旦发生入侵行为, 便可通过对记录的数据进行分析, 并提取相关的信息、确定攻击源, 依法打击入侵者. 由于入侵攻击技术的不断变化, 入侵者在成功入侵系统后, 往往会将相关数据删除或篡改, 从而使事后的静态取证无法获得完整准确的入侵数据^[3]. 有效地监测、记录网络的数据

包, 是发现入侵行为、进行动态取证的重要手段^[4]. 文章提出一种分布式动态取证模型, 运用了动态取证、分布式证据收集技术, 构建了包括网络数据收集、客户机信息收集、数据分析等模块, 以及客户机与取证服务器之间的数据传输模块在内的分布式动态取证系统, 并在 Windows 平台上进行了实现, 测试表明, 系统既提高了证据的获取能力, 又保障了数据的安全性.

2 系统设计

分布式动态计算机取证系统包括实时数据收集、安全证据保护、证据分析和提取、证据处理等功能, 并且要保证数据安全存储和传输, 保障数据完整性. 分布式动态取证模型采用 C/S 结构, 有以下几个组成部分: (1) 分布式信息收集器, 进行证据的分布式收集; (2) 集中的证据存储中心, 进行证据的集中存储; (3) 专用的通信协议, 保证证据传输的安全

收稿日期: 2011-05-29; **修回日期:** 2011-08-03

基金项目: 重庆市自然科学基金项目(2009BB2340)

性和完整性;(4)证据分析中心,对收集到的证据进行分析,并向用户提供有效的证据;(5)系统接口,方便用户对系统的管理.系统模型如图1所示.

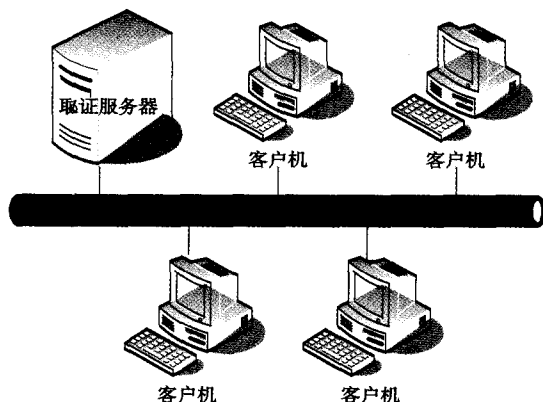


图1 计算机取证模型图

客户机的信息收集器用于收集包括重要文件访问、篡改等系统信息,并将其发回取证服务器.取证服务器的主要功能是实时地获取网络数据和客户机的各种重要信息并进行存储,同时对数据进行分析得出最终结论.取证服务器是系统的核心,包括:1)网络数据收集模块,用于获取网络数据源,监测网络中的全部活动;2)客户机数据接收与存储模块,用于接收、保存来自客户机信息收集器的各种信息;3)数据分析模块,用于根据记录分析入侵行为,并得出结论.

取证系统的主要功能模块如图2所示,下面阐述其中主要模块的原理.

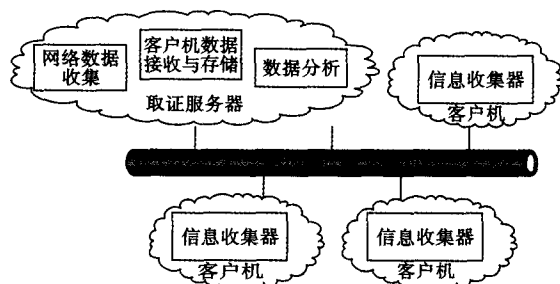


图2 取证系统主要功能模块图

2.1 信息收集器模块

客户机上的信息收集模块收集的取证信息各有特征,如果不加处理就发送给取证服务器,取证服务器的负担会较重,所以,信息收集器应有一定的信息分析处理功能,能按照取证信息的来源,将证据分类、简单处理后再发送,也可以根据需要重点收集某些信息,如:重要文件的信息、重要进程的信息等.

2.2.1 重要文件的信息收集

黑客攻击的对象往往是一些重要文件,如对网站的攻击经常集中在对网页文件的篡改上,因此,对重要文件的信息收集是动态取证的关键.收集器应及时发现重要文件的篡改情况,并将信息发回取证服务器.可以采用 MD5 报文摘要算法对重要文件进行完整性校对,通过 CPU 时钟控制对重要文件的扫描时间,随时获取重要文件的信息,并与以前的相关信息进行比较,一旦发现改动便将信息传回取证服务器.

2.2.2 重要进程的监测

这部分模块的功能主要是监测客户机上的重要进程是否被恶意关闭或打开,在上述情况发生时将相关信息传回取证服务器.信息收集器定时对系统进程拍摄快照,并将进程快照与重要进程列表比较,如果有变化发生,便立即通知取证服务器.

2.2 网络数据收集模块

网络数据收集模块主要采用网络监听技术,通过有效捕获网络数据包并对数据包进行解析来发现入侵,是实现动态取证的基础.将网卡设置为混杂模式时,主机工作在监听模式下,它将接收所有经过的数据包,也就是说,无论数据包中的目标地址是什么,只要经过主机的网络接口都将被接收,即所有的数据帧都将被交给上层协议软件处理.

数据包的捕获步骤是:(1)获取本地设备信息:寻找系统中可用的网络接口设备,返回一个表示网络适配器的字符串;(2)打开设备开始监听会话;(3)设置过滤条件:编辑过滤字符串,设置过滤器,制定要捕获的主机、协议等,可以有效的捕获指定类型的数据;(4)执行捕获循环:每捕获一个数据包后就调用用户的回调函数对数据包进行处理.可通过调整用户级缓存、设置严格的过滤条件、设置内核缓存等几个措施来提高监听模块的性能,通常,设置较大的内核缓存可以取得较好的性能.

捕获后的数据帧经过解析才能得到有用的信息.对数据帧的解析过程是将数据帧中的数据按照不同协议进行分析、提取的过程,如提取数据帧的源地址、目的地址、协议类型等信息.

2.3 客户机数据收集与存储模块

客户机数据收集与存储模块的功能是接收与保存大量来自不同客户机的数据,包括对证据的存储、查询、导入与导出等,为数据分析做准备.

2.4 数据分析模块

数据分析模块通过有效分析取证数据来确定入

侵权行为,常用的方法有两种:第一种是模式匹配法:通过收集非正常操作的行为特征,建立相应的数据库,如果收集到的用户或系统行为与数据库中的记录相匹配,就认为这是入侵行为.模式匹配法的优点是只需要收集相关的数据,既减轻了系统负担,又提高了检测的准确率、降低了误报率.不过,这种匹配方法不能检测出攻击的细微变化,也不能检测出从未出现过的攻击手段.第二种是统计分析法:首先根据系统对象的活动情况,产生能刻画这些活动的行为框架.每一个框架能保存记录主体的当前行为,并定时地将当前的框架与存储的框架合并.然后通过比较当前的框架与事先存储的框架来判断异常行为,并检测出网络的入侵行为.该方法的实际使用效果受制于人工智能技术的发展速度^[5-8].

3 关键技术

3.1 收集器进程状态监测

如果客户机上的信息收集器进程发生意外中断,或被入侵者恶意中断,就会失去监测能力,收集器进程状态监测模块必须及时发现这种情况并记录下来.方法是:收集器定时向取证服务器发送特定信息,如果在一定时间段内,取证服务器没有接收到来自某客户机的信息,就说明该客户机上的收集器进程已停止运行或是通讯中断,取证服务器将立即记录这种情况,并将通过自动学习,生成网络中运行收集器进程的客户端列表,随时记录其变化情况.

3.2 客户机与取证服务器间的数据传输

收集器必须及时将收集到的数据发回取证服务器,具体操作步骤如下:(1)客户机为要传送的数据计算校验信息,采用循环冗余校验法;(2)将数据和校验信息用 MD5 加密算法进行加密;(3)将加密后的数据发送给取证服务器;(4)取证服务器对收到的数据进行解密;(5)用与第(1)步相同的方式,为解密后的数据计算校验信息,并与收到的校验信息进行比较,如果两者一致,说明数据在传输的过程中没有发生错误或被恶意篡改,可以将收到的数据集中存储,否则,就要通知客户机重传并报告取证工作人员.

3.3 证据存储

采用 SQLSERVER 数据库对证据进行分类存储,通过构造不同的查询语句就能方便、高效地进行证据的插入、删除、修改等操作.证据是一个包含多个域的记录,不同的证据类具有不同的域成员,某类证据的组成如表 1 所示.

表 1 某类证据的组成

域名	域的数据类型	域的含义
evidence_class	整型	证据的类别
fd	整型	发生变动的重要文件描述符
time	时间型	变更时间
operation	字符串	变更的操作
bytes	无符号整型	变更的字节数
client	字符串	客户机 MAC 地址
...	...	...

3.4 系统实现方法

将动态取证程序及组件安装在取证服务器上,组件使用系统的组件服务管理器进行安装,其客户端代理安装在客户机上.在客户机上配置好重要文件列表文件,将要保护的重要文件写入其中,另外,将要监测的重要进程添加到重要进程列表文件中,便可启动客户机上的信息收集程序了.

4 实验分析

根据文中设计的模型,在 Windows XP 操作系统下,用 VC 6.0 开发了一个分布式动态取证系统,并进行了取证能力的测试.实验表明,通过取证服务器上的网络数据收集程序可以看到网络中数据帧的情况;客户机上的任何重要文件的变动或重要进程的启动、停止都可以被系统检测到,并按时间顺序记录到取证服务器上的日志文件中;当重要文件或重要进程的非法入侵来自于内部人员而非通过网络时,也可通过记录的时间和其他相关资料确定入侵者.在测试中为了模拟网络入侵,将架设在某客户机上的网站的访客记录文件加入重要文件列表中,当访问该网站时,引起了访客记录文件的变化,取证服务器上立即记录了这个变化,同时,访问的网络数据包也被取证服务器捕获.

5 结束语

与其他取证模型相比,分布式动态取证模型将信息收集分布至系统中的客户机上,避免了取证服务器的性能瓶颈,有效提高了系统的处理速度和能力.模型在对网络中的入侵行为进行监控的同时,对网络数据进行同步记录,实时获取入侵证据,解决了事后证据收集的困难,提高了证据的证明能力.采用 FCM 算法进行数据分析,增加了证据的可信度,提

高了证据的有效性。

参考文献:

- [1] Judd, Robbins. An explanation of computer forensics [EB/OL]. [2010-07-10]. <http://www.computerforensics.net/forensics.htm>.
- [2] 殷联甫. 计算机取证技术[M]. 北京:科学出版社, 2008.
- [3] 鄢喜爱,杨金民,常卫东. 基于蜜罐技术的计算机动态取证系统研究[J]. 微电子学与计算机, 2010, 27(1): 135-137.
- [4] 王素芳,高美真,苏继斌. 基于涉密网的计算机取证模型研究[J]. 微电子学与计算机, 2010, 27(5): 202-205.
- [5] 陈龙,麦永浩,黄传河. 计算机取证技术[M]. 武汉:武

汉大学出版社, 2007.

- [6] Catalin Grigoras. Applications of ENF criterion in forensic audio, video, computer and telecommunication analysis [J]. Forensic Science International, 2007 (167):136-145.
- [7] Claire LaVelle, Almudena Konrad. FriendlyRoboCopy: a GUI to robocopy for computer forensic investigators [J]. Digitalinvestigation, 2007(4):16-23.
- [8] Farmer D, Venema W. Computer forensics analysis class handouts [EB/OL]. [2010-07-05]. <http://www.fish2.com/forensics/class.html>.

作者简介:

周敏 女, (1971—), 硕士. 研究方向为信息安全.

(上接第 39 页)

- [4] Zheng WeiMou. Kneading plane of the circle map[M]. Chaos, Solitons & Fractals, 1994, 4(7):1221-1233.
- [5] 张慧档,贺昱曜. 基于混沌序列的 SVM 参数选择及其在笔迹鉴别中的应用[J]. 计算机应用, 2007, 27(7): 1961-1963.
- [6] 袁冬根,刘晓东. 基于混沌蚁群算法的 BP 神经网络训练研究[J]. 微电子学与计算机, 2009, 26(4): 11-14.

作者简介:

韩萍 女, (1973—), 教授, 硕士生导师. 研究方向为模式识别及智能方法.

张慧档 女, (1971—), 博士研究生, 副教授. 研究方向为智能优化.

孙福艳 女, (1979—), 博士研究生. 研究方向为混沌系统.

潘昊 男, (1964—), 教授, 博士生导师. 研究方向为智能方法及智能系统.