计算机动态取证技术的研究

Study of computer dynamic forensics technology

刘东辉　（长春吉林公安高等专科学校 130117）

摘要：本文首先介绍了计算机动态取证的概念、原则和步骤，然后主要介绍了计算机动态取证的关键技术，最后分析了计算机取证的发展趋势。

关键词：计算机取证　动态取证　静态取证

1　计算机动态取证的概念

计算机动态取证是将取证技术结合到防火墙、入侵检测技术以及密罐技术中，对所有可能的计算机犯罪行为进行实时数据获取和分析，智能分析入侵者的企图，采取措施切断链接或诱敌深入，在确保系统安全的情况下获取最大量的证据，并将证据鉴定、保存、提交的过程。可见，动态取证在及时获得全面、真实的证据的同时，能够分析犯罪手段、动机、从而得出正确的应对方略，指导相应防火墙及入侵检测系统做出实时响应，形成计算机取证与入侵检测、防火墙的互动；同时系统通过对自身网络结构的修改以及备份措施等来保障网络安全中的各个方面，从防外到防内，初步构成一个安全体系。计算机动态取证能记录系统工作、尤其是黑客入侵的全过程，截取入侵工具，对黑客入侵方法进行技术分析，通过分析和研究，牵制和转移黑客的攻击，取得最新的攻击技术的资料，产生防御攻击的方法。

2　计算机动态取证的原则

因为计算机取证过程涉及到电子证据的问题，所以它的要求很严格，必须遵循如下的原则：

（1）保持数据的原始性：取证分析的数据是被分析机器上数据的原始逐位比特的复制。

（2）保持数据在分析和传递过程中的完整性：分析软硬件环境不会改变分析的数据，数据传递过程中数据没有改变。

（3）保持证据连续性：如果确实需要改变数据，必须保证证据连续性，即在证据被正式提交给法庭时，必须能够说明在证据从最初的获取状态到在法庭上出现状态之间的任何变化。

（4）取证过程的可认证性：也就是说，整个过程是受到监督的，由原告委派的专家所作的所有调查取证工作都应该受到由其他方委派的专家的监督。

（5）取证过程和结论的可重现：由于电子证据的特殊性，任何取证分析的结果或结论可以在另外一名取证人员的操作下重现。

3　计算机动态取证的关键技术

在动态取证中，取证主要包括如下的环节：数据的获取、数据的分析、证据鉴定、证据保存及证据提交，下面就对每一步所使用的关键技术做一简要的介绍。

3.1　数据获取技术

在数据获取阶段，获取的数据量是非常大并且数据是不断更新的，一个网站每天可能产生上千万条的事件记录，即使是基于主机的取证，从整个系统中获取的历史数据加上实时数据的数据量也是相当惊人的。这些数据主要有：系统日志；IDS、防火墙、FTP、WWW 和反病毒软件日志；系统的审计记录；网络监控流量；Email；Windows 操作系统和数据库的临时文件或隐藏文件；数据库的操作记录；硬盘驱动的交换分区、slack 区和空闲区；软件设置；完成特定功能的脚本文件；Web 浏览器数据缓冲；书签、历史记录或会话日志、实时聊天记录等等。对这些海量数据的获取，我们可以考虑把网络数据获取部分做成专用的硬件，类似于飞机上的黑匣子。网络数据获取的流程如图 1 所示。

网络数据获取系统首先将网卡设为混杂模式，从

而可以对经过该网段的数据进行监听。然后接受每一个数据包，读取其包头信息，并跟相应的规则进行匹配，如果满足获取条件就将其存放到网络数据文件中，否则将其丢弃。网络数据文件以二进制的格式按照时间间隔进行存放，以利于后续的分析。

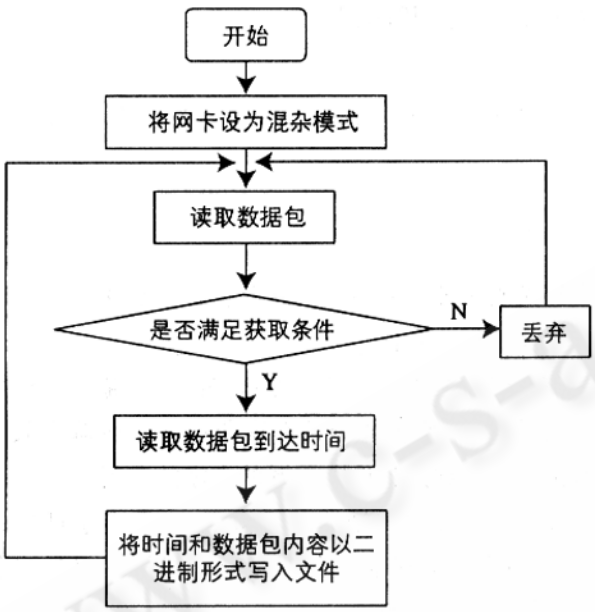

图 1　网络数据获取系统流程

3.2 数据传输技术

采用光缆以 RS－232 为接口进行异步传输数据，将所记录的数据从目标机器安全地转移到取证分析机上。由于计算机取证的整个过程必须具有不可篡改性的要求，因此，数据在传输过程中不仅要具备抵抗黑客非法入侵的能力，还要提高对远程数据传输的保密性，避免在传输途中遭受非法窃取。采用加密技术，如 IP 加密、VPN 加密、SSL 加密等协议标准，保证数据的安全传输。另外，通过使用消息鉴别编码（MAC）保证数据在传输过程中的完整性，MAC 算法同时也被认为是加密算法，即从目标机器发送一列所支持的 MAC 算法，取证系统在返回的 Hello 消息中标出所选的算法。

3.3 数据分析技术

通过计算机取证的数据获取软件来收集了大量的数据后，实施动态取证的关键是如何从海量的数据中挖掘有效信息，审查判断出与案件相关的、反映案件客观事实的、法庭接受的电子证据。因此，数据分析是动态取证的关键环节。在动态取证的数据分析阶段通常运用专用的辅助分析软件工具对数据进行筛选，根据数据确定犯罪实施的过程，包括入侵时间、使用 IP 地址、修改的文件、增加的文件、删除的文件、上载和下载的文件等。动态取证不同于静态取证的根本方面是它是事前就进行实时数据获取，即使是犯罪嫌疑人对原始数据进行更改、删除，原始数据、篡改数据及篡改操作都会被记录下来。这样就使动态取证面临一些技术难题：取证的实时要求、取证的有效性、可适应性和可扩展性要求。这就要求动态取证不但要从海量的数据中及时分析出具有计算机犯罪常见特征的数据，而且还要对具有新特征的数据进行分析判断，使动态取证过程智能化。将数据挖掘技术应用到动态取证的数据分析中，则有助于解决上述主要问题。数据挖掘的方法很多，在动态取证系统里，主要用到如下几种方法：

（1）关联分析。运用关联规则提取犯罪行为之间的关联特征（特征可能是经过预处理的统计特征），挖掘不同犯罪形式的特征、同一事件的不同证据间的联系，将审计数据和网络数据整理到数据表中（每一行为一条数据记录，每一列为一种系统特征）。在动态取证的数据分析阶段，通过用户行为与关联规则库中的规则匹配来判断当前用户行为是否合法、是否具有犯罪特征或与某一犯罪事件相关，并将可能成为犯罪证据的数据提取出来，一方面通过保全技术加密传送到证据库中；另一方面将入侵数据反馈到入侵检测系统中。将关联规则分析技术应用于海量的数据分析，提高数据分析的速度，有助于解决动态取证的实时性问题。

（2）分类分析。在动态取证的数据获取阶段收集了用户或程序足够的、海量的“正常”和“异常”的数据，在取证的数据分析阶段，应用分类算法来判断用户或程序是否非法，找出可能的非法行为，将非法用户或程序的入侵过程、入侵工具记录下来，作为犯罪证据及犯罪动机分析的依据。同时，应用分类样品数据来训练数据分析器的学习，使之具有标识或预测正常类型或异常类型数据的新特征的能力，预测一些未知的数据是否犯罪证据，提高数据分析的智能性。

（3）联系分析。运用联系分析算法来分析程序的执行与用户的行为之间的序列关系，分析常见的各种计算机犯罪行为在作案时间、作案工具及作案技术等方面的特征联系，发现各种事件在时间上的先后关系和联系，建立用户异常模型，将异常模型加入到知识库

中，保证系统可根据网上数据的变化实时地更新知识库。异常模型运用于动态取证的数据分析上，提高数据分析的准确性和有效性。如从系统日志文件中挖掘规则，对规则进行联系分析，得出异常数据模型，用异常数据模型判断当前用户行为的合法性，这种方法特别适合于对逻辑炸弹类型的计算机犯罪分析。

3.4 数据保存技术

证据在被鉴定出来后，就要对证据进行保存，以防内部或外部非法人员的篡改和删除，因此要使用加密技术。磁盘加密的主要方法有固化部分程序、激光穿孔加密、掩膜加密和芯片加密等，还可利用修改磁盘参数表如：扇区间隙、空闲的高磁道来实现磁盘的加密。另外，还可采用堆栈溢出保护技术，防止黑客使用堆栈溢出的方法对系统进行攻击。

3.5 其他的一些相关技术

动态取证除了使用上述一些技术以外，还经常使用如下一些技术：

(1) 对比分析与关键字查询。将收集的程序、数据、备份等与当前运行的程序、数据进行对比，从中发现篡改的痕迹；对所做的系统硬盘备份，用关键字匹配查询，从中发现问题。

(2) 文件特征分析技术。利用磁盘按簇分配的特点，在每一文件尾部都会保留一些当时生成该文件的内存数据，这些数据称为该文件的指纹数据，据此可得出文件最后修改的时间从而判断作案时间。

(3) 残留数据分析技术：文件存储到磁盘后，由于文件实际长度要小于等于实际占用簇的大小，在分配给文件的储存空间中，大于文件长度的区域会保留原来磁盘存储的数据，可以利用这些数据来分析磁盘中储存的内容。可以利用这些数据来分析磁盘中储存的内容。

(4) 磁盘储存空闲空间的数据分析技术：磁盘在使用过程中，会对文件要进行大量增、删、改、复制等操作。经过上述操作的文件会重新向系统申请存储空间，再写入磁盘，这样经过一次操作的文件写入磁盘后，在磁盘中就会存在两个文件，一个是操作后实际存在的文件，另一个是修改前的文件，但其所用的空间已被释放，随时可以被新的文件覆盖。利用这个特性，可进行一定程度的数据恢复，对于被删除、修改、复制的文件，可追溯到变化前的状态。

(5) 记录文件的分析技术：一些系统软件和应用软件对已操作过的文件有相应的历史记录，如系统日志、防火墙日志、word 最近使用文件列表等，被记录的文件名或网址可以提供一些线索和证据。

4 结束语

本文当中所提到的将数据挖掘技术应用于计算机动态取证的数据分析阶段，提高了数据分析的能力，有助于解决动态取证的实时、准确有效和智能化问题。虽然计算机动态取证已经有一定的研究成果，但是还不够完善。随着网络技术的飞速发展、计算机犯罪技术手段的不断提高、反取证技术的出现，计算机动态取证仍将面临新的挑战。结合入侵检测系统，以及人工智能、机器学习、神经网络和数据挖掘等技术开发新的动态取证工具或软件，使取证工具能有效地挖掘出潜在的信息，使计算机取证更加智能化，是计算机取证今后研究的方向之一。另外，利用无线局域网和手机、PDA、传真等无线终端设备进行计算机犯罪的案件逐年递增，如何在无线环境中进行取证分析也是今后的研究方向。

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，2002 年第 9 期。

2 杨泽明、许榕生、曹爱娟，网络取证与分析系统的设计与实现，计算机工程，2004 年第 13 期。

3 钟秀玉、凌捷，计算机动态取证的数据分析技术研究，计算机应用与软件，2004 年第 9 期。

4 Ranmu, Marcus J. Network Forensics and Traffic Monitoring. Computer Security Journal, 1997,12.

5 Robbins, Judd. An explanation of computer forensics.
http://www.computer forensics.net/forensics.htm