·计算机工程与应用·

网络取证日志分布式安全管理

戴江山[1]，李向阳[2]，张增军[2]，肖军模[2]

(1. 总参谋部第61研究所 北京 丰台区 100039; 2. 解放军理工大学通信工程学院 南京 210007)

【摘要】提出了一种网络取证日志分布式安全管理方法，通过日志代理和管理网关将分散的异构的日志收集并存储到多个管理节点。该管理节点采用信息分配算法IDA将日志记录分散为n份，计算所有分片单向散列值，并同该节点相应存储分片关联存储。取证分析时，管理节点根据网络入侵事件多特征关联性，利用任意m(m＜n)个节点提取相关日志记录分片重建原有信息。由于每个分片携带所属日志记录所有分片的单向散列值，通过验证可以保证重构日志记录的完整性。

关 键 词 分布式; 日志; 网络取证; 网络安全
中图分类号 TP393.08 文献标识码 A

Distributed Security Management of Network Forensic Log

DAI Jiang-shan[1]，LI Xiang-yang[2]，ZHANG Zheng-jun[2]，XIAO Jun-mo[2]

(1. The 61st Research Institute of PLA General Staff Headquarter Fengtai Beijing 100039;
2. Institute of Communications Engineering, PLA University of Science & Technology Nanjing 210007)

Abstract A distributed security management method of network forensic log is proposed and designed in this paper. The log agents and management gateway collect and forward the log records to the multi-management nodes. The log records are respectively dispersed into n shares by information dispersal arithmetic in the node, and the node stores the corresponding share and the hash values of all shares. The management node can reconstruct the log records through corresponding information in m (m<n) random nodes and validate the integrity of the log records through the hash values of all shares.

Key words distributed; log; network forensics; network security

证据能力，即证据资格，是指证据资料在法律上被允许作为证据的资格[1]。数字证据资料由于其数字化特性，具有易删除、易伪造、易篡改和篡改后易消除痕迹等特点，因此其证据能力需要专门的技术手段和严格的取证程序加以保证。日志是网络取证中重要的数字证据资料，但目前其结构多样，存储分散，缺乏安全性和完整性保护，使网络取证的证据能力很容易遭到质疑，而且不利于证据的提取和分析。

针对以上问题，本文提出和建立了一种基于证据能力保证的网络取证日志分布式安全管理方法，该方法采用日志代理和管理网关收集分散的异构日志记录并存储在多个管理节点。管理节点采用信息分配算法(Information Dispersal Arithmetic，IDA)、单向散列函数和入侵事件多特征关联性对日志记录进行分布式安全存储、完整性验证和分析重构。

1 安全日志管理方法体系结构

分布式安全日志管理方法体系与结构如图1所示，图中n为管理节点个数。分布式安全日志管理方法体系结构主要由日志代理、管理网关和多个管理节点组成。

网络取证日志通常包括主机日志、网络日志(如入侵检测日志)和边界设备日志(如防火墙日志、路由器日志)。日志代理根据取证日志的重要性分别采用实时或定时抽取方式将日志发送到管理网关。对于记录网络攻击者入侵过程的主要证据来源主机和网络日志，日志代理采用实时抽取传送方式，即当日志记录产生后，除在本地按照原有策略存储外，日志代理向管理网关发送连接请求，并将日志记录加密和数字签名后发送到管理网关；对于重要性相对较低、安全性相对较好的边界设备日志，日志代理

收稿日期：2005－03－28
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，工程师，主要从事网络与信息安全方面的研究.

则可以采取定时抽取传送方式。

管理网关由安全防护、接收发送代理、安全监测、系统维护、管理控制模块和临时数据库等组成，主要完成日志的正确接收，以及将其安全可靠转发到各管理节点。安全防护通过防火墙、入侵检测系统、访问控制等手段严格限制和过滤进入管理网关的数据包，以保证系统安全。接收发送代理负责接收和向各管理节点转发日志代理发送的日志记录。日志记录被接收后，经过安全检测中的数字签名验证，被存储在临时数据库，然后由接收发送代理负责转发到各管理节点。为满足网络取证需要，日志往往需要长期保存，因此管理网关和管理节点均设有系统维护模块，协作运行以随时发现和纠正系统出现的问题，如节点系统发生故障，数据完整性遭到破坏等。管理控制负责整个系统检测、设置和安全管理。

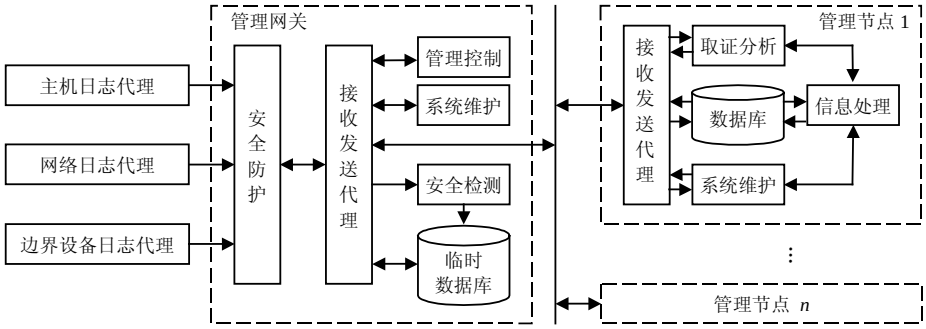

图1 分布式安全日志管理方法体系结构

管理节点由信息处理、取证分析、接收发送代理、系统维护模块和数据库等组成，具有日志的分布式安全存储、完整性验证和取证分析等功能。信息处理模块实现日志记录解密、信息分配算法IDA和单向散列计算，能够对日志记录进行分片和重构，以及计算分片的单向散列Hash值。取证分析根据网络入侵事件多特征关联性，通过接收发送代理从多节点数据库中收集相关信息，利用信息处理模块实现日志记录的完整性验证和重构。

2 安全日志管理方法实现

2.1 日志收集与传输

日志传输过程如图2所示。日志传输分为两个阶段，一是日志代理同管理网关间的日志传输，传输空间为非安全传输域；二是管理网关同管理节点间的日志传输，传输空间为安全传输域。运行优先级前者高于后者。

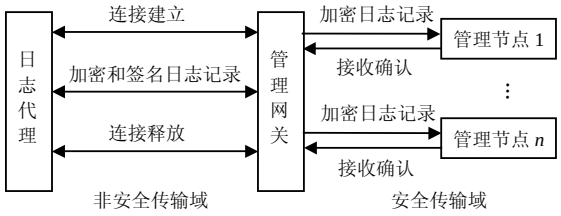

图2 日志传输过程图

日志代理同管理网关间的日志传输，首先由日志代理对待发送日志记录进行内容加密(如对称加密算法DES[2])和数字签名(如公开密钥数字签名算法DSA [2])，然后采用TCP协议向管理网关发送连接请求并完成可靠传输。管理网关内建有日志代理数字签名公钥表，对接收到的日志记录经过数字签名验证后存储到临时数据库。

管理网关同管理节点间的日志传输，由管理网关采用UDP协议将临时数据库内的日志记录同时发送给所有管理节点。在UDP数据包头后增加固定标识头(标识、类型、时间、IP地址、MAC地址)，管理节点根据数据包标识头识别和正确接收日志记录后发送接收确认。管理网关在规定时间内接收到所有节点发送的接收确认后，删除该日志记录并发送下一条，否则对未接收到确认的节点在设定阈值范围内重发。

2.2 日志分布式存储

管理节点将接收日志记录解密后，采用信息分配算法IDA[3]将日志记录分散为n份，计算所有分片的单向散列Hash值(如安全散列算法SHA[2])，并同该节点相应存储分片关联存储。另外，由于不同类型取证日志数据的结构差别较大，为减少存储空间的冗余度，管理节点内分别建有面向主机日志、网络日志和边界设备日志的多个数据存储结构。

信息分配算法IDA的基本思想是将长度为$L=|D|$的数据信息D分散为n份，其中任意m(m为重构信息所需最小数，$m\leqslant n$)份可以重组原有信息，针对某条日志记录算法过程如下：

(1) 在有限域GF(2^8)内将日志记录D划分为长度

为m的数据分组序列，不足位由0填充。$D=D_1, D_2, \cdots, D_i, \cdots = (d_{1,1}, d_{1,2}, \cdots, d_{1,m}), (d_{2,1}, d_{2,2}, \cdots, d_{2,m}), \cdots$，其中$|D_i|=m$。

(2) 在有限域GF(2^8)内利用$m\times n$矩阵$\boldsymbol{T}$实现D_i的m输入n输出的线性变换，即输入$D_i=d_{i,1}, d_{i,2}, \cdots, d_{i,m}$，输出$O_i=D_i \cdot \boldsymbol{T}= o_{i,1},o_{i,2},\cdots,o_{i,n}$。

(3) 同理，对D中其他数据分组进行同样处理得$O=O_1, O_2, \cdots=(o_{1,1},o_{1,2},\cdots,o_{1,n}), (o_{2,1},o_{2,2},\cdots,o_{2,n}),\cdots$。取序列$P_i=o_{1,i}, o_{2,i},\cdots(i\leqslant n, |P_i|=L/m)$作为日志记录$D$的第$i$个分片，存储在编号为$i$的管理节点。

其中，转换矩阵$\boldsymbol{T}=(t_{ij})_{m\times n}$，必须满足任意$m$个列向量线性无关，其选取有多种方法[3]。如设$n$=5，$m$=3，可取$\boldsymbol{T}=\begin{bmatrix}1&0&0&1&1+x\\0&1&0&1&x\\0&0&1&1&1\end{bmatrix}$，$\boldsymbol{T}$中任意3个列向量线性无关。$x$多项式表示有限域GF($2^8$)上的元素，通过模运算有限域GF(2)上不可约多项式$x^8+x^6+x^5+x^4+1$得到。

2.3 日志分析重构

取证分析时，首先根据网络入侵事件空间、时间和攻击类型特征，管理节点从m个节点(包括自身节点)提取收集相关日志记录分片。网络攻击中，攻击数据包发送源端口通常是随机选择，因此源地址、宿地址和宿端口是取证分析的主要空间特征。时间范围是取证分析基本的时间特征。此外，一次网络攻击通常是一个事件流产生一个日志记录序列，因此日志记录固定时间间隔也是取证分析重要的时间特征。设日志记录序列为$(r_1,r_2,\cdots,r_n)$，相邻记录时间间隔为$(\tau_1,\tau_2,\cdots,\tau_{n-1})$，则在满足空间特征和基本时间特征关联的条件下，当且仅当$\tau_i<c(1\leqslant i\leqslant n-1$，$c$为设定时间时隔阈值)日志记录序列$(r_1,r_2,\cdots,r_n)$对应相同攻击。相同攻击类型日志通常对应相同攻击，因此在满足时空关联的条件下，根据攻击类型可进一步确定取证分析所需日志记录。

管理节点采用UDP协议向所有n个节点同时发送收集条件，当接收到m–1个节点的数据返回时，则拒绝继续接收。针对某条日志记录，当收集到所需相关分片后，对分片携带的所有分片单向散列Hash值对应比较，如果全部相同则表示重构日志记录是完整的，否则发出完整性告警。

对通过完整性验证的m个日志记录分片利用IDA算法重新构建出原有日志记录。为表述方便本文假设接收到编号为1～m个管理节点的返回数据(如果含有其他编号管理节点如$m<i\leqslant n$，则只需使用其存储的数据分片和转换矩阵T中对应的列向量)。针对某条日志记录，管理节点获得分片$P_1,P_2,\cdots,P_m$，其中，$P_i=o_{1,i},o_{2,i},\cdots(1\leqslant i\leqslant m)$。算法过程如下：

(1) $O'=O_1', O_2', \cdots$，其中$O_j'=(o_{j,1},o_{j,2},\cdots,o_{j,m})$是由所有分片$P_i(1\leqslant i\leqslant m)$第$j$个分组组成的序列。

(2) $\boldsymbol{T}$中相对应的1至m列向量组成$m\times m$矩阵$\boldsymbol{T}'=(t_{ij})_{m\times m}$，如前假设$n$=5,$m$=3中，$\boldsymbol{T}'=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$。由于$\boldsymbol{T}'$中列向量线性无关，即$D_i\cdot\boldsymbol{T}'=O_i'$，因此在有限域$GF(2^8)$上有$D_i= O_i'\cdot\boldsymbol{T}'^{-1}$。

(3) 同理，对O'中其他分组进行同样处理，得$D=D_1, D_2, \cdots, D_i = (d_{1,1},d_{1,2},\cdots,d_{1,m}), (d_{2,1}, d_{2,2}, \cdots, d_{2,m}),\cdots$，即恢复出原有日志记录。

2.4 系统维护

系统维护采用固定时间轮值和时间滑动窗口方法维护管理节点安全性和日志完整性，如图3所示。

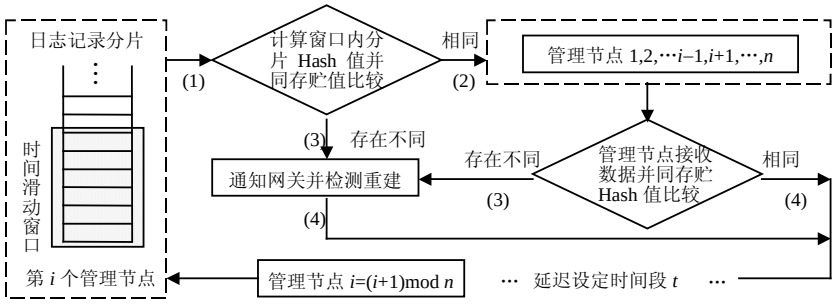

图3　系统维护过程图

维护管理步骤为：(1) 管理节点内建有所有管理节点地址表，轮值节点i计算本节点最近某时间滑动窗口(如一个月)内存储的日志记录分片的单向散列Hash值，然后同存储的相应Hash值相比较。如果全部相同，则转到(2)，否则转到(3)；

(2) 采用UDP协议向所有节点发送同滑动窗口内分片关联的所有分片Hash值。管理节点接收到轮值节点i发送的数据后，同本节点内存储的相应值比

较，如果全部相同，转到(4)，否则转到(3)；

(3) 通知管理网关停止发送新的日志记录。管理节点利用m个其他有效节点(不包括自身节点)数据检测和重新构建该日志记录，然后采用IDA和SHA重新计算和存储相关日志信息。转到(4)；

(4) 经过设定时间段t，管理节点编号i=i+1，转到(1)。

系统维护是以固定时间为间隔，因此经过时间段t所有管理节点没有接收到相应轮值节点发送来的信息，管理网关也没有接收到日志信息维护要求，则轮值节点系统可能发生故障。

3 安全日志管理方法性能分析

在非安全传输域，系统采用加密和数字签名方式防止日志记录被伪造、篡改和利用Sniffer监听、收集。管理网关设有安全防护并且通过严格的安全策略设置，保证系统运行安全性。日志被分散存储在n个管理节点，攻击者要破坏日志至少要侵入n–m+1(m为重构信息所需最小数)个管理节点，而这极大增加了攻击者入侵的难度和被发现的概率。由IDA算法可知，攻击者控制任意k<m个节点无法重新构造和获取原有日志。即使控制k>m个节点，也只有在网络取证授权条件下才能收集重构日志内容，这就保证了日志内容的安全性和隐私性。

日志代理同管理网关间采用TCP协议，以及管理网关同管理节点间采用UDP加接收确认的协议保证日志记录传输的完整可靠性。管理节点存储有日志记录所有分片的单向散列Hash值，系统维护以及取证分析利用这些信息可保证日志长期存储的完整性，以及取证分析日志的证据能力。

网络取证通常是入侵事件发生后对长期收集日志的综合性分析，因此对取证分析的实时性要求并不太高。该方法在取证分析时，由于管理节点需要对相关日志进行收集、完整性验证和重构，因此所需系统时间相对较长，但网络取证中证据资料的完整性要求往往比取证分析的时间性要求更为重要。

4 结 束 语

本文提出并建立了一种网络取证日志分布式安全管理方法，该方法采用分布式存储、信息分配算法以及单向散列函数保证网络取证日志的安全性、完整性、隐私性以及便于取证分析。日志代理时间同步、日志取证分析是该方法有待进一步深入研究的内容。

参 考 文 献

[1] 齐爱民, 刘 颖. 网络法研究[M]. 北京: 法律出版社, 2003.

[2] SCHNEIER B. 应用密码学: 协议、算法与C源程序[M]. 第2版. 吴世忠, 祝世雄, 张文政, 译. 北京: 机械工业出版社, 2000.

[3] RABIN M. Efficient dispersal of information for security, load balancing, and fault tolerance[J]. Journal of the ACM, 1989, 36(2): 335-348.

[4] GARAY J, GENNARO R, JUTLA C, et al. Secure distributed storage and retrieval[C]//In: proceedings of the 11th International Workshop on Distributed Algorithms. London: Springer-Verlag, 1997: 275-289.

[5] AWERBUCH B, SCHEIDELER C. Consistent an compact data management in distributed storage systems[C]//In: Proceedings of the 6th Annual ACM Symposium on Parallelism in Algorithms and Architectures. New York: ACM Press, 2004: 44-53.

编 辑 刘文珍