第34卷 第21期 计 算 机 工 程 2008年11月
Vol.34 No.21 Computer Engineering November 2008
·安全技术· 文章编号：1000—3428(2008)21—0161—02 文献标识码：A 中图分类号：TP309.2

支持计算机取证的电子证据安全保护策略

赵小敏，郑河荣
(浙江工业大学软件学院，杭州 310014)

摘 要：计算机数据具有脆弱性，因此必须在计算机取证过程中对电子证据进行安全保护使其具有证据能力。该文提出一种基于 SHA-1, RSA 和 Rabin 容错算法实现的电子证据安全保护策略以支持计算机取证，对原始记录进行实时、安全的转移并分散存储，保证数据的真实性和完整性，能通过快速检测和还原对其进行有效性鉴定。

关键词：计算机取证；电子证据；安全保护

Secure Protection Policy for Electronic Evidence Supporting Computer Forensics

ZHAO Xiao-min, ZHENG He-rong
(Software College, Zhejiang University of Technology, Hangzhou 310014)

【Abstract】 It is essential to protect the electronic evidence for its admissibility in computer forensics due to the weakness of computer data. This paper presents a secure protection policy for electronic evidence supporting computer forensics, in which some algorithms of SHA-1, RSA and Rabin fault tolerance are used. It can transfer the original records in real time and securely, store them dispersively for the authenticity and integrality, and make validity assessment in fast check and recovery.

【Key words】 computer forensics; electronic evidence; secure protection

1 概述

随着电子商务、电子政务、网络虚拟财产转移等电子信息交互活动在现实生活中的不断深入，网络入侵、木马盗取账号等违法活动和相关的民事权利纠纷问题也日益突出。解决这些问题的有效办法就是电子证据的计算机取证，其关键是提取的电子证据是否具有法律认可的证明力[1]。电子证据由于数字化特性，具有易删除、易伪造、易篡改和篡改后易消除痕迹等特点，给司法和计算机科学领域带来了新的研究课题[2]。电子证据要具有法律认可的证据能力就必须是真实、可靠、完整和符合法律规定的[3]。因此，如何对电子证据进行安全保护，使其在计算机取证过程中具有证据能力显得尤为关键。目前，这方面的研究处于起步阶段，还没有建立一套完整的电子证据安全保护机制，相关的研究主要有文献[4]的一种日志文件的安全存储方法、文献[5]的电子证据可靠性保护方法、文献[6]的基于DSA数字签名机制实现电子证据完整性的一致性方案。

本文提出了一种支持计算机取证的电子证据安全保护策略，目的是确保所保存的信息与它们的原始状态一致，任何添加、篡改和删除原始记录的行为都将被有效证明，使得信息记录能够作为有法律效力的电子证据。该策略采用 SHA-1 散列算法、RSA 公开加密算法和 Rabin 容错算法来实现，并提供快速验证和还原的检测机制。

2 符号表示

为表述方便，规定以下符号：

(1)+，表示字符串的连接操作。

(2)$H(x)$，表示使用 SHA-1 算法对字符串 x 计算其单向散列值。

(3)XOR(x, y)，表示对字符串 x 和 y 进行异或操作，则由字符串异或运算的规则可知：

XOR(XOR(x,y),z)=XOR(x, XOR(y,z))

(4)$RSA_K(x)$，表示利用RSA算法并使用公钥K对字符串x进行加密。

(5)$ceil(x)$，表示对浮点数 x 取上整数，如 $ceil(1.1)=2$, $ceil(1.6)=2$。

(6)$IDA(n, m)$，表示信息分散算法(Information Dispersal Algorithm, IDA)[7]，运用矩阵运算的思想，将原始资料分成n份，仅须取回m份($m \le n$)即可还原资料。算法思路是：假设欲分散的原始资料D长度为L，分散的数值为n，还原所需数值为m，根据m值将D分散成$m \times ceil(L/m)$的资料矩阵，用n个两两独立的向量$(1 \times m)$进行叉乘运算，即可获得n份资料片断；还原时，任取m个资料片断，将其中的m个向量组成($m \times m$)的向量矩阵的逆矩阵，叉乘这m个资料片断组成的矩阵$m \times ceil(L/m)$，即可得到原始资料矩阵$m \times ceil(L/m)$，再分解还原成原始资料D。

(7)H_{id}，表示被取证主机标识符。

(8)D_i，表示需要安全保护的第i条证据信息记录，D_i'表示对该记录进行安全保护处理后的记录。

(9)V，表示经授权的电子证据完整性的验证者。

(10)FS，表示受到安全保护的取证服务器机群，FS_i表示第i个取证服务器主机。

3 安全保护策略

本文的安全保护策略是对原始信息记录进行加密保护并

基金项目：浙江省自然科学基金资助项目(Y106113)
作者简介：赵小敏(1976－)，男，讲师、硕士，主研方向：信息安全；郑河荣，副教授、博士研究生
收稿日期：2008-04-01 **E-mail：**zxm@zjut.edu.cn

分散存储于可信的 FS 中，包括信息记录的产生、还原和检测 3 个过程。与文献[4]的方法类似，这里有 2 个前提：(1)入侵者在执行入侵或违法活动时，必定有操作行为被主机所记录；(2)入侵者在执行入侵或违法活动后，至少有一条记录通过本方法保护后安全存储于 *FS* 机群，即入侵者在 *t* 时刻试图删除或修改自己留下的“痕迹”时，*t* 时刻前的记录已被加密保护并安全存储。

3.1 信息记录的产生

计算机和网络系统中的关键文件如系统安全日志、入侵检测日志以及各种重要进程或应用程序产生的缓存数据、安全记录或临时文件等都会记录用户的一些操作行为，可作为计算机取证的电子证据[1-2]。这些文件中的信息记录都是逐条产生的，入侵者成功入侵后往往会删除与其入侵过程有关的信息记录或直接删除相关文件。因此，计算机取证的关键在于相应关键文件的信息记录必须在产生之后尽快复制并加密保护，同时进行安全转移，使得这些信息记录真实、可靠且完整。为安全保护原始信息记录，本文提出信息记录产生的处理方法，将信息记录分散存储于*FS*中。信息记录产生的流程如图 1 所示。

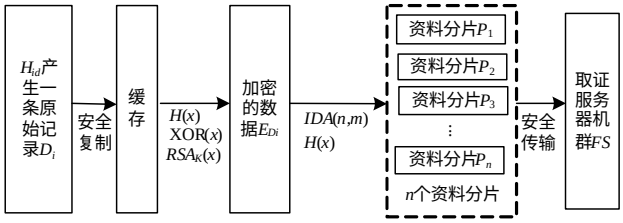

图 1 信息记录的产生流程

信息记录产生的详细步骤如下：

(1)H_{id}产生的原始记录D_i安全复制到缓存，当H_{id}产生一条新的记录D_i时，缓存中就会产生一份完全的拷贝。

(2)使用SHA-1 算法对缓存的原始记录进行散列运算，记为$H(D_i)$，供以后验证原始记录是否遭篡改。

(3)使用司法机关的公钥K，利用RSA加密算法计算得到$RSA_K(D_i+H(D_i))$，验证时采用司法机关的私钥进行解密，使资料具有可鉴别性。

(4)将前一条记录D_{i-1}和D_i的散列值进行XOR运算，产生验证码XOR($H(D_{i-1}),H(D_i)$)。

(5)产生加密的数据$E_{Di}=RSA_K(D_i+H(D_i))$+XOR($H(D_{i-1}),H(D_i)$)，其长度记为L。

(6)将E_{Di}进行IDA算法运算，得到分散的资料分片$C_1,C_2,\cdots,C_n$，其中，n为分散存储的取证服务器主机数；m可事先根据网络风险评估和带宽的参数确定，m/n的取值范围为1/2~1 时效果较好[7]。$IDA(n,m)$运算的具体过程如下：

1)任取n个两两独立的向量$\boldsymbol{A}_1=[a_{11},a_{12},\cdots,a_{1m}]$，$\boldsymbol{A}_2=[a_{21},a_{22},\cdots,a_{2m}]$,$\cdots$，$\boldsymbol{A}_n=[a_{n1},a_{n2},\cdots,a_{nm}]$，构建矩阵$\boldsymbol{A}_{nm}=[\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_n]$，其中，取$n$个独立向量的算法见文献[7]。

2)若$L \bmod m$为非 0，则在E_{Di}后面补 0，补 0 的个数为$m-(L \bmod m)$，然后分解成$m\times ceil(L/m)$的矩阵$\boldsymbol{B}$：

$$\boldsymbol{B}=\begin{bmatrix} b_1 & b_{m+1} & \cdots & b_{ceil(L/m)+1} \\ b_2 & b_{m+2} & & b_L \\ \vdots & & & \vdots \\ b_m & b_{2m} & \cdots & 0 \end{bmatrix}$$

3)由矩阵$\boldsymbol{A}$叉乘矩阵$\boldsymbol{B}$，得到$n\times ceil(L/m)$矩阵$\boldsymbol{C}$，对矩阵$\boldsymbol{C}$按行分解生成资料分片$C_1,C_2,\cdots,C_n$，其中，C_i为矩阵$\boldsymbol{C}$的第i行资料，长度为$ceil(L/m)$ Byte。

(7)使用SHA-1 算法对式(6)得到的资料分片C_i、对应的独立向量$\boldsymbol{A}_i$以及当前时刻T分别进行散列运算，即$H(T+\boldsymbol{A}_i+C_i)$，然后得到便于容错存储的$n$个资料分片：$P=P_1+P_2+\cdots+P_n$，其中，$P_i=T+\boldsymbol{A}_i+C_i+H(T+\boldsymbol{A}_i+C_i)$。

(8)将n个资料分片P通过信任的安全通道传输至各FS_i ($1\le i\le n$)中进行容错储存。

3.2 信息记录的还原

由验证者V从FS中取回超过m个同一时刻的资料分片P_i，分解P_i为T, $\boldsymbol{A}_i$, C_i和$H(T+\boldsymbol{A}_i+C_i)$4 项，对前 3 项进行SHA-1 运算并与第 4 项$H(T+\boldsymbol{A}_i+C_i)$作比较，以初步确定该资料是否遭篡改。

任取m个初步确认未遭篡改的资料分片P_i，分解资料，进行反IDA运算，过程如下：

(1)分解m个资料分片P_i，将各自的第 2 项$\boldsymbol{A}_i$和第 3 项C_i分别组成矩阵$\boldsymbol{A}$和$\boldsymbol{C}$，即$\boldsymbol{A}=(\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_m)$,$\boldsymbol{C}=(C_1,C_2,\cdots,C_m)$。

(2)根据 3.1 节对矩阵$\boldsymbol{A}$的假设条件，$\boldsymbol{A}_1$, $\boldsymbol{A}_2$,$\cdots$,$\boldsymbol{A}_m$是两两独立的，所以，可求出矩阵$\boldsymbol{A}$的逆矩阵$\boldsymbol{A}^{-1}$。

(3)矩阵$\boldsymbol{A}^{-1}$叉乘$\boldsymbol{C}$即可得矩阵$\boldsymbol{B}$，分解$\boldsymbol{B}$后即可得原始的加密数据：$E_{Di}=RSA_K(D_i+H(D_i))$+XOR($H(D_{i-1})$, $H(D_i)$)。

(4)司法机关利用RSA算法和私钥对$RSA_K(D_i+H(D_i))$进行解密，然后进行SHA-1 运算并比对，判断此m个同一时刻的资料分片P_i是否遭篡改。

若资料未篡改，便可产生法庭认可的电子证据；若资料遭篡改，则须经过信息记录的检测，找出入侵后修改记录的关键时间点，再对该时间点前后的资料进行解密，以加快检测速度。

3.3 信息记录的检测

直接对每条记录进行逐条检测将费时费力。假设有 n 条记录进行检测，关键时间点出现的概率为均分分布，则必须进行期望值为 $ceil((n+1)/2)$次解密、$ceil((n+1)/2)$次 SHA-1 散列运算和 $ceil((n+1)/2)$次比对才能得到关键时间点。

根据本文的前提假设，入侵者在进行入侵或违法操作时，至少有一条记录已被安全传送至*FS*。假设在第i-1 条记录中有入侵或违法操作的记录，入侵者于第i条记录产生前获得系统控制权，为掩盖入侵或违法操作行为，入侵者除了可以修改第i条及以后的记录，也可修改或删除还在内存中的第i-1 条记录中的散列值，即修改$H(D_{i-1})$值为$H'(D_{i-1})$。根据XOR的运算规则可知，第i-2 条记录中的散列值$H(D_{i-2})$与第i条记录的验证码XOR($H(D_{i-1})$, $H(D_i)$)及第i条记录中的散列值$H(D_i)$进行XOR 运算便可得到第i-1 条记录的验证码XOR($H(D_{i-2})$, $H(D_{i-1})$)。但$H(D_{i-1})$被修改为$H'(D_{i-1})$后，经过以上异或运算产生的验证码肯定与已传输至FS的第i-1 条记录的验证码不相等。检测时，最后一条记录先自行检查有无错误，然后依据以上检测方法，再进行二分法检测。根据二分法算法的平均查找长度，若有n条记录，则仅需 $1+(n+1)/n\times\text{lb}(n+1)-1\approx ceil(\text{lb}(n))$次就可完成检测。

由于每次检测需完成 1 次解密、2 次 XOR 运算和 1 次比对，因此利用本文对信息记录的保护方法，仅需进行期望值为 $ceil(\text{lb}(n))$次解密、$2\times ceil(\text{lb}(n))$次 XOR 运算和 $ceil(\text{lb}(n))$次比对即可得到关键时间点。

4 结束语

具有法律效力的电子证据必须是真实、可靠、完整和符

（下转第 189 页）