基于TPM的视频安全远程取证

马 强[1,2]，马建国[2]，邢 玲[2]

(1. 中国工程物理研究院电子工程研究所 四川 绵阳 621900; 2. 西南科技大学信息工程学院 四川 绵阳 621010)

【摘要】为了保证视频内容被合法用户接收，且接收到的视频内容没有受到帧丢弃、帧重组等恶意攻击，对接收到的视频内容安全信息进行远程取证。提出了基于可信平台模块TPM的视频安全远程取证，对该远程取证的结构和过程进行了分析。为防止中间人伪造远程取证响应，提出了基于Fourier-Mellin的视频内容哈希算法，采用TPM对视频帧的特征进行认证；同时为提高远程取证的效率，提出了用于视频安全远程取证下的可区分粒度的取证模式，分析了如何能够有效地在粒度下视频序列中寻找不可信视频帧。通过实验证明了该视频哈希算法的有效性，并验证了可区分粒度取证模式的特点。

关 键 词 远程取证； 可信计算； 可信计算模块； 视频哈希； 视频安全

中图分类号 TP393 **文献标识码** A doi:10.3969/j.issn.1001-0548.2012.05.020

TPM Based Remote Attestation of Video Security

MA Qiang[1,2], MA Jian-guo[2], and XING Ling[2]

(1. Institute of Electronic Engineering, China Academy of Engineering Physics Mianyang Sichuan 621900;
2. School of Information Engineering, Southwest University of Science and Technology Mianyang Sichuan 621010)

Abstract In order to ensure the video can be received by the legal client without attack of frame dropping, frame rearranging, and so on, a remote attestation protocol of video security based on Trusted Platform Module (TPM) is proposed. The architecture of the remote attestation protocol is explained in detail. Video content hash algorithm which is based on Fourier-Mellin is put forward to authenticate the video frame contents in order to prevent the man-in-the-middle from fabricating the response of remote attestation. To improve the efficiency of remote attestation, an attestation mode of differentiable granularity is developed. The experiments prove the effectiveness of the video hash algorithm and also demonstrate the characteristics of the proposed attestation mode of differentiable granularity.

Key words remote attestation; trusted computing; trusted platform module; video hash; video security

视频服务已成为互联网中的主要应用，根据中国互联网信息中心最新的报告，视频业务已占到了网民网络应用行为的62.1%[1]。伴随着视频服务的大量普及，视频内容的安全性问题越来越突出。一方面，视频内容容易被非法用户获取；另一方面，互联网体系的开放性容易造成视频内容被第三方篡改，使得传输到接收方的视频内容被修改，视频内容不再可信。因此，视频内容的可信计算已成为目前视频应用开发与安全领域迫切需要解决的问题。

传统的用于认证接收方身份的用户名、密码方法，由于接收方可能受到攻击或注入木马行为而显得无能为力。在保证视频内容的安全性方面，对视频内容进行简单的加密、解密方法，会明显地降低视频传输效率，增加计算复杂度和视频内容的冗余[2]。由可信计算组织(trusted computing group，TCG)提出的可信计算方案给视频内容的安全研究提供了新的方向。TCG制定了关于可信平台模块TPM(trusted platform module)、可信网络连接TNC (trusted network connect)以及可信存储等一系列技术规范[3]。TCG中规定信任模型以TPM硬件模块为基础，由该硬件中的信任根为出发，对系统中的其他组件或程序进行认证。TPM中拥有RSA、SHA1等算法，也具有可信远程取证、可信报告的功能。

目前，国内外围绕可信计算已开展了大量的研究工作，主要分为对可信计算协议本身的安全性研究和对可信计算的应用研究两大类。前者的研究主

收稿日期：2011－07－05； 修回日期：2011－11－02
基金项目：国家自然科学基金重点项目(60932005)；国家自然科学基金(60902021)
作者简介：马强(1982－)，男，博士生，主要从事视频语义处理、视频可信计算方面的研究.

要是对可信计算平台信任链规范中信息流安全问题的建模分析[4]，采用基于马尔可夫过程对TNC架构安全问题的量化分析方法[5]，对可信计算硬件模块可配置性与灵活性问题进行研究[6-7]；后者的研究主要是采用具有数据恢复功能星型信任链的PDA可信计算平台系统结构和安全机制的研究[8]，利用TPM的完整性测试、存储和报告功能，基于可信状态的多级安全模型[9]，基于可信计算的嵌入式智能摄像机的安全性与隐私保护进行研究[10]。可信计算的应用通常是利用TPM提供的信任链机制对应用程序或者服务进行认证，并且认为TPM提供的信任根是可信的，不会受到攻击。

本文利用可信计算的概念对视频安全问题进行研究，可以直接应用到视频监控系统、VOD点播系统、视频会议系统等。为了保证视频接收方平台的可信，采用TPM对平台的启动过程进行认证，利用信任链的关系将信任根的信任传递给视频接收处理应用程序。采用基于Fourier-Mellin的视频哈希算法，以防止攻击者对远程取证过程中伪造视频接收方对远程取证的响应。为提高远程取证效率，提出了可区分粒度的远程取证模式，研究了在可区分粒度下如何有效地处理不可信帧，最后通过实验证明了视频哈希算法的有效性以及可区分粒度远程取证模式的特点。

1　远程取证结构和过程

视频内容是从视频服务方VS (video server)下载或传输到视频客户方VC (video client)。为了验证视频内容的安全性，采用基于TPM的远程取证过程实现。为此，在VC端采用了虚拟技术[11]以实现视频内容的可信计算与视频内容下载到本地、播放或存储的过程相分离，从而保证可信计算运行环境的相对独立性。远程取证系统结构如图1所表示。其中，运行于VC的播放虚拟机PVM (player virtual machine)负责从VS端获取视频内容，分析、提取视频帧特征并将视频帧特征提交给可信计算虚拟机TVM (trusted computing virtual model)。TVM完成VC端的视频内容安全远程取证功能，负责收集VC的运行环境、视频帧特征，并且处理来自VS的取证请求。在VC运行过程中，PVM与TVM之间的交互工作由虚拟机器监视器VMM (virtual machine monitor)完成。VMM是运行在硬件机器设备上的软件代码层，提供PVM对TPM操作的功能接口。

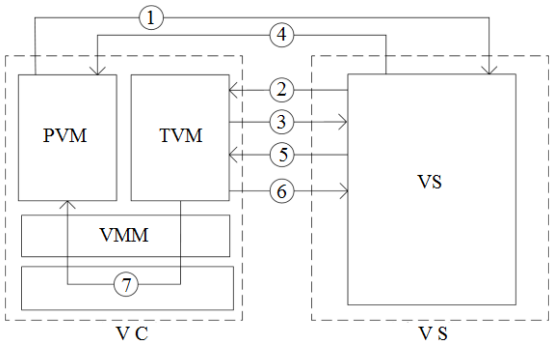


图1　远程取证结构

远程取证的过程主要按照以下步骤进行：

1) VC中由PVM向VS发出获取视频内容链接请求。

2) VS接收请求，要求VC提供本地可信证明，VS向TVM请求链接，并且传送随机数nonce_s，以防止重复攻击行为。

3) TVM接收来自VS请求，通过VMM获得PVM运行环境可信信息，PVM运行的可信证明存储在TPM中的PCR_0；TVM执行命令Quote(0x00, Key_s, nonce_s)，返回结果Quote_0，其中执行命令参数分别表示PCR的标识号、VS方提供的用于取证的密钥、VS方提供的随机数；PVM同时执行CreateAIK命令，获得用于视频帧特征提取的密钥AIK_1、AIK_2。TVM将返回给VS的信息格式为{nonce_c, Hash{Quote_0, nonce_c}、Ekeys{AIK_1, AIK_2}}。其中Hash{·}表示对其中的内容采用SHA1算法，由TPM的SHA1Start命令完成，Ekey_s{·}表示对其中的内容采用密钥key_s进行加密，由TPM的Bind命令完成，密钥Key_s由PrivacyCA机制通知VC[12]

4) VS对TVM返回的信息进行可信性分析，利用自己的密钥key_s和随机数nonce_s、nonce_c得到Quote_0，对比可信环境下VC的值Quote_0^-，判断VC是否可信；VS同时获得AIK_1和AIK_2。若判断VC环境可信，VS将向VC传输视频内容，否则终止可信连接的初始化过程。可信环境下VC的值Quote_0^-由PrivacyCA机制提供给VS。VC对接收到的视频一方面进行播放或者存储，一方面完成对视频帧特征的提取。

5) VS向TVM发起远程取证的请求，传送待取证帧序号f_{id}和随机数$\text{nonce}_{s'}$。

6) TVM通过VMM访问PVM，与初始化过程类似，执行Quote命令得到结果Quote_0'，并且回传给VS的信息格式为：{$\text{nonce}_{c'}$,Hash{ Quote_0', $\text{nonce}_{c'}$}}；VS将比对视频帧可信的特征，从而判断在VC端的视频内容是否可信。

VC可能受到攻击代码的注入，或者隐藏在VC系统中的木马将对视频内容的安全构成威胁，采用基于TPM视频安全远程取证的初始化过程，将保证VC的可信。在VC启动过程时，将采用信任链的方式对载入内存的代码进行完整性认证。TPM中测试可信的核心根CRTM (core root of trust for management)固化在TPM芯片中，TPM认为CRTM是系统认证的开始，并且保证不会受到外界的攻击。视频安全信任关系的传递如图2所示。

信任链可以分为VC的初始化过程和视频帧的可信计算过程。由CRTM对BIOS中的配置进行验证，计算其Hash值，判断BIOS是否经过恶意篡改；若BIOS完整性正确，系统按照其设置装载配置。以同样的方式，BIOS执行后，系统在将控制权转交给Bootloader之前，也将验证Bootloader的完整性。依次类比，VC将保证PVM可信，而PVM的可信是视频内容安全的前提。

为了认证视频内容在空域和时域的完整性，对视频帧内和帧间的可信同时进行认证。在视频帧内，提取该帧的特征作为VS与VC之间确认帧完整性的依据，而视频当前帧的可信将用于认证视频的下一帧。PVM接收到视频内容，首先对第一帧视频帧Frame_1的完整性进行认证，视频的特征将对视频帧的攻击具有敏感性；Frame_1的可信是视频帧Frame_2可信的基础，以此类推，视频安全信任链将对视频所有的帧进行认证。

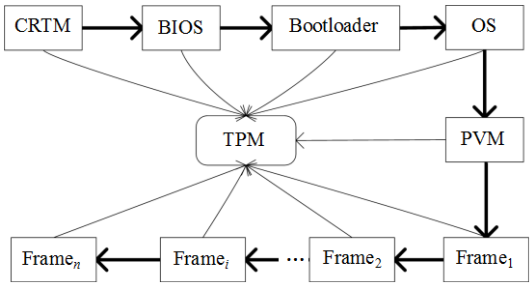


图2 视频安全信任链

2 视频内容哈希算法

2.1 Fourier-Mellin方法

在选取视频帧的特征时，采用了Fourier-Mellin方法[13]。设视频帧中像素点用$p(u,v)$表示，对视频帧进行Fourier变换，得到$P(f_u,f_v)$，并计算其模的大小为$|P(f_u,f_v)|$。对变换后的Fourier变换采用对数极坐标表示，即 $f_u=\mathrm{e}^{\rho}\cos\theta$，$f_v=\mathrm{e}^{\rho}\sin\theta$，$\rho\in[0,1]$，$\theta\in[0,2\pi]$，此时模大小表示为$\left|P(\rho,\theta)\right|$。定义$h(\rho)$为$\left|P(\rho,\theta)\right|$在$\theta$轴的投影，即大小为$\rho$的模对所有的$\theta$值取积分：

$$h(\rho)=\int_0^{2\pi}\left|P(\rho,\theta)\right|\mathrm{d}\theta \tag{1}$$

$h(\rho)$体现了在频域范围内视频内容的特点，用作视频帧的特征。

2.2 视频帧特征提取

首先对视频帧图像进行RGB到YCbCr颜色空间的转换，在提取其特征时，仅考虑Y分量空间中视频帧的特征。对Y分量进行Fourier变换后，在对数极坐标中对$\left|P(\rho,\theta)\right|$沿$\theta$轴等分为$K$个点，即$\theta\in\{0,2\pi/K,\cdots,(K-1)2\pi/K\}$。

由TPM生成的AIK_1、AIK_2用于视频帧中特征的随机化处理，并且AIK_1和AIK_2在VS与TVM之间远程证明初始化过程中已通知双方。AIK_1负责生成$\left|P(\rho,\theta)\right|$的伪随机半径候选集$\Xi$，将$h(\rho)$对$\Xi$中的半径上的取值进行线性组合，其中线性组合系数$\beta_\rho$为伪随机系数，由$\text{AIK}_2$负责生成，得到的视频帧特征具有以下关系：

$$h=\sum_{\rho\in\Xi}\beta_\rho\sum_{i=0}^{K-1}\left|P\left(\rho,\frac{i}{K}2\pi\right)\right| \tag{2}$$

由最大熵原理，在生成伪随机系数时为了使得视频帧特征拥有较大的熵，β_ρ服从正太分布。

2.3 视频哈希算法

为了使得视频哈希算法能够有效地体现出视频帧序列之间的有序关系，采用TPM中extend方法对连续的两帧视频特征进行处理，以提高算法对视频帧丢弃、重组方面的攻击。设PCR_0中当前存放视频帧特征h_i的哈希值为Q_i，则哈希算法具有以下关系：

$$Q_i=\text{extend}(Q_i\,|\,h_i) \tag{3}$$

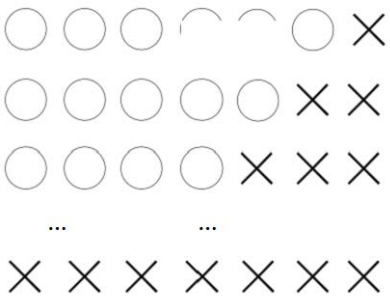
Q_0为PVM载入内存执行时PCR_0中的取值，反映了PVM整个启动过程的可信。TVM在视频安全取证初始化过程中将Q_0通知VS方。

3 远程取证模式

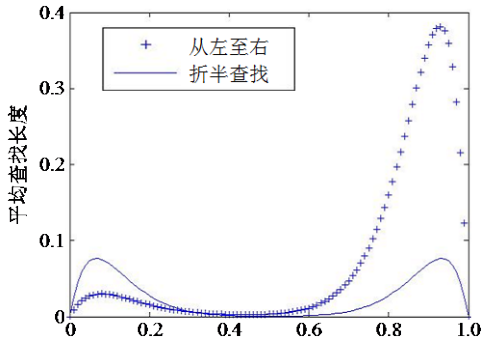
VS对VC获取的视频内容进行安全远程取证时，视频内容特征序列$H=\{h_1,h_2,\cdots,h_i,h_{i+1},\cdots,h_n\}$，经过视频哈希算法后相应的有哈希值序列为$Q_i=\{Q_1,Q_2,\cdots,Q_i,Q_{i+1},\cdots,Q_n\}$，其中元素$h_i$为第$i$个视频帧的特征，$Q_i$为第$i$个视频帧的哈希值。由于视频哈希算法考虑到帧间的完整性，所以Q_i实际上体现了前i帧视频帧的可信与否。为此，在VS对视频安全的取证时，为了提高取证的效率，提出可区分粒度的视频取证模式，用D表示粒度，$D\in[1,2,\cdots,n]$。VS向TVM请求待取证的视频帧序号

为f_{id}，下一次待取证的视频帧序号为max(f_{id}+D,n)。显然，如果序列号为f_{id}与f_{id}+D的视频帧哈希值正确，则序列号为f_{id}+1, f_{id}+2,…, f_{id}+D–1的视频帧都是可信的。

在粒度为D的取证模式下，若下一次的视频帧是不可信帧，此时需要判断区间大小为D的视频帧序列中是哪一帧首次出现了不可信，从而导致了后面帧的不可信，实现粒度的可区分性。图3a中列出了D=7，视频帧序列中有1帧、2帧、3帧和7帧不可信的情况，其中○表示可信帧，×表示不可信帧。在对该视频帧序列进行查找时，有从左至右查找和折半查找两种方法。若令视频帧可信的概率为p，则视频帧不可信的概率为1–p，视频帧可信概率分布服从独立同分布。易知，按照从左至右的查找方法，需要的平均查找次数为$\sum_{i=1}^{n-1} p^{n-i}\times(1-p)^{i}\times(n-i)$，按照折半查找的方法，平均查找次数为：$p^{\lfloor n/2\rfloor}\times(1-p)^{n-\lfloor n/2\rfloor}+\sum_{i=2}^{\lfloor\log_2 n\rfloor}(p^{n-\lfloor n/2^{i}\rfloor}\times(1-p)^{\lfloor n/2^{i}\rfloor}+p^{\lfloor n/2^{i}\rfloor}\times(1-p)^{n-\lfloor n/2^{i}\rfloor})\times i$，两者在最好的情况下，查找次数都是1，在最坏的情况下，两者的查找次数分别是n–1和$\lfloor\log_2 n\rfloor$，其中$\lfloor A\rfloor$表示取不大于A的最小整数。



a. 视频帧序列中出现不可信帧的情况



b. 两种查找算法的比较

图3　取证模式分析

采用从左至右和折半查找算法的描述如下：

输入：视频帧序列f_{id}+1, f_{id}+2,…, f_{id}+D。

输出：序列中首次出现不可信帧序列号s。

从左至右查找算法步骤为：

1) 取temp=1；

2) 判断f_{id}+temp可信，若不可信，则s=temp，程序结束；否则，执行步骤3)；

3) temp=temp+1，转到步骤2)。

折半查找算法步骤为：

1) 取temp=$\lfloor D/2\rfloor$；

2) 判断f_{id}+temp可信，如不可信，转到步骤3)；否则转到步骤4)；

3) 判断f_{id}+temp–1是否可信，若可信，则s=temp，程序退出；否则转到步骤5)；

4) temp=temp+temp/2，转到步骤2)；

5) temp=temp–temp/2，转到步骤2)。

两种算法平均查找长度的比较结果如图3b所示，从图中可以看出，当视频帧的可信的概率p较小时，从左至右算法优于折半查找，因为p越小，表明长度为D的视频帧序列中不可信帧数量较多，可信帧较少，从图3a可以直观上理解采用从左至右查找可以快速的找到目标帧；当p较大时，视频帧序列中含有较多的可信帧，不可信帧较少并且集中在视频序列的尾部，采用折半查找可以较快速的找到目标帧；而p介于两者之间时，两种算法的差别不大。因此，实际当中可以根据需要选择不同的查找算法。

如果在视频帧序列f_{id}+1, f_{id}+2, …, f_{id}+D–1中查找到首次出现不可信视频帧f_{id}+i后，VS将向VTM取证视频帧f_{id}+i+1的可信度量值，并且采用$Q_{f_{id}+i+1}$=extend($Q_{f_{id}+i-1}|h_{f_{id}+i+1}$)的方式进行重新计算后续帧的可信值，即此时视频安全的信任链由原先的Frame$_{i-1}$→ Frame$_i$→Frame$_{i+1}$变为了Frame$_{i-1}$→Frame$_{i+1}$。若视频帧f_{id}+i+1也非可信，则将取证视频帧f_{id}+i+2，直到后续某可信帧出现，此时视频帧取证粒度D实际上变为1。

4　实验分析

4.1　实验环境

实验验证过程中VC与VS的硬件配置内存为2 G，CPU为Intel(R) Core2 Duo CPU，TPM版本为1.2。VC与VS均采用了Linux kernel 2.6.30的Fedora-11系统，利用了Xen-4.10开源软件来实现VMM的管理操作功能[14]。VC的可信启动过程利用Tboot过程实现，Tboot是可以在Xen中使用的认证Kernel启动过程的开源代码。TPM的实现利用了MIT可信计算项目开发的面向对象的TPM/J-0.3，它封装了底层TPM的命令，提供了对TPM操作的API[15]。视频安全远程取

证采用了Java语言进行开发。PVM中设计了视频接收处理模块vRPM (video receiving and processing module)，用于接收视频内容，提取视频帧特征并计算视频哈希；TVM中设计了远程取证响应模块RM (remote attestation responding module)，以处理VS发送给VC的取证请求，并且通过Xen访问PTM。在VS中视频远程取证功能由取证模块AM(attestation module) 完成，VS中还包含视频提供模块vPM(video providing module)，响应VC的视频请求，从数据库中获取视频并传输给VC，vPM与AM之间存在的交互过程如图4所示。

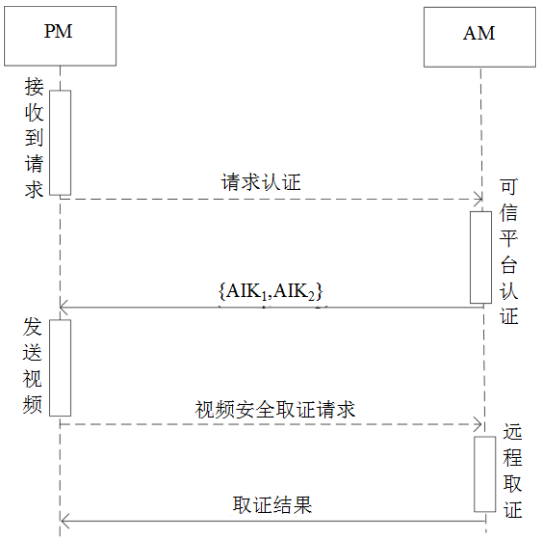


图4 vPM与AM之间交互过程

在实验中执行攻击型视频内容操作，定义A={Dropping, Modifying, Rearranging}，分别表示对视频帧进行丢弃、内容修改和重组操作，选择用于A中某操作的目标视频帧序号随机生成，定义对视频内容无操作为B={}，即视频帧在B的情况下，其特征值应该保持不变；同时定义A'与B'分别为远程取证过程中识别视频帧经过A与B操作。

4.2 实验结果

为研究视频内容哈希算法的正确性，定义$P(A'|A)$为在对视频帧进行攻击的情况下，能正确地识别该帧被攻击的概率，定义$P(B'|B)$为没有对视频帧进行攻击的情况下，能正确地识别该视频帧是可信帧的概率。

实验中对10个视频进行了视频哈希算法的测试，测试结果如图5所示。从图中可以看出，该视频哈希算法对于对视频帧进行的攻击行为都可以正确地识别检测，因此，该算法可以认为是对视频帧安全具有较好的认证特性。但对于在没有对视频帧进行攻击情况下，有极少的帧被认作是经过攻击的，说明算法对于对视频的非攻击行为操作(如噪声)具有敏感性，导致这一原因在于该视频哈希算法对于视频前后帧的特征采用了TPM中extend方法的关联，而extend需要完成SHA1算法。

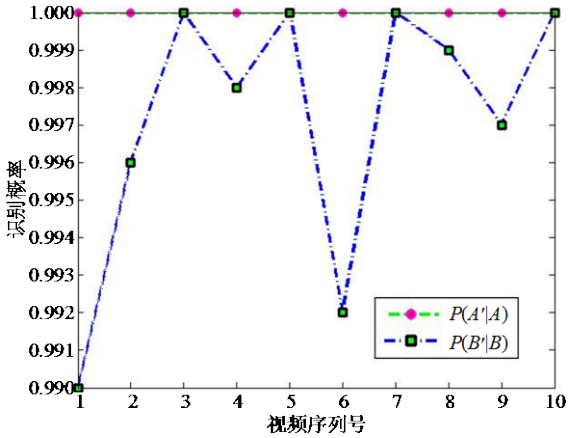
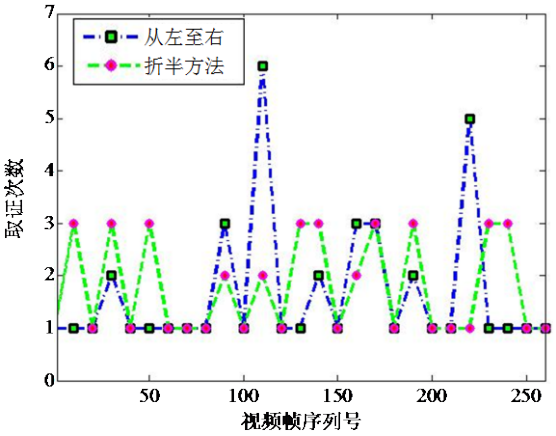
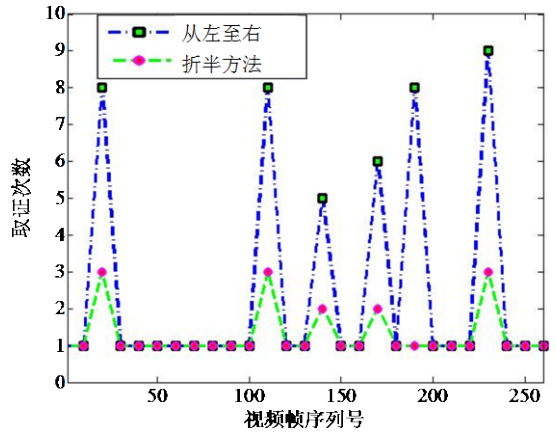


图5 视频哈希算法测试结果

对于可区分粒度取证模式的实验，选用了粒度D=10，分别在视频帧可信概率P为12%和98%情况下，分析在长度为10的视频帧序列中查找到首次出现的不可信视频帧时，所需要进行的远程取证次数，如图6所表示。从图6a中可以较清晰地看出，采取从左至右方法优于折半查找方法，而在图6b中采用折半查找方法则优于从左至右方法，其原因已在第3节进行了阐述。



a. P=12%的情况



b. P=98%的情况

图6　可区分粒度内视频安全取证次数

5　结　论

本文提出了基于TPM的视频安全远程取证，对视频的安全采用了信任链的方式加以认证。在远程取证结构中，利用虚拟机技术实现了可信计算模块与视频接收、播放或存储应用相互隔离，为远程取证提供可信的计算环境。视频内容哈希算法基于Fourier-Mellin方法，充分利用了视频帧的序列关系，可以有效地防止攻击者获得视频帧特征，伪造VC的远程取证响应。本文提出的可区分粒度的取证模式，提高了远程取证的效率，并且对取证的协议进行了安全分析，指出了该协议具有安全性，不会受到中间人的攻击。实验过程证明了该视频哈希算法的正确性，并验证了可区分粒度的取证模式特点。

视频安全是未来网络应用中重要的研究领域。将可信计算引入到视频安全研究，可以有效地解决视频内容在语义以及安全方面的问题，具有重要的应用前景。未来将研究具有鲁棒性的视频哈希算法，以提高视频安全认证的效果；同时将研究分布式网络环境下视频安全的可信计算问题。

参　考　文　献

[1] 中国互联网信息中心.中国互联网络发展状况统计报告[R]. 北京: 中国互联网信息中心, 2011.
CNNIC. Statistical report on internet development in china [R]. Beijing,: CNNIC, 2011.

[2] 廉士国, 孙金生, 王执铨. 几种典型视频加密算法的性能评价[J]. 中国图象图形学报, 2004, 9(4): 483-490.
LIAN Shi-guo, SUN Jin-sheng, WANG Zhi-quan. Quality analysis of several typical MPEG video encryption algorithms[J]. Journal of Image and Graphics, 2004, 9(4): 483-490.

[3] TCG. TPM main level 2, version 1.2, revision 116 [EB/OL]. [2011-03-20]. www.trustedcomputinggroup.org.

[4] 徐明迪, 张焕国, 赵恒, 等. 可信计算平台信任链安全性分析[J]. 计算机学报, 2010, 33(7): 1165-1176.
XU Ming-di, ZHANG Huan-guo, ZHAO Heng, et al. Security analysis on trusted chain of trusted computing platform[J]. Chinese Journal of Computer, 2010, 33(7): 1165-1176.

[5] 罗安安, 林闯, 王元卓, 等. 可信网络连接的安全量化分析与协议改进[J]. 计算机学报, 2010, 33(5): 887-898.
LUO An-an, LIN Chuang, WANG Yuan-zhuo, et al. Security quantifying method and enhanced mechanism of TNC[J]. Chinese Journal of Computer, 2010, 33(5): 887-898.

[6] EISENBARTH T, GÜNEYSU T, PAAR C, et al. Reconfigurable trusted computing in hardware[C]//ACM STC'07. Alexandria, Virginia, USA: ACM, 2007.

[7] ENGLAND P, TARIQ T. Towards a programmable TPM[J]. Lecture Notes in Computer Science, 2009, 5471: 1-13.

[8] 赵波, 张焕国, 李晶, 等. 可信PDA计算平台系统结构与安全机制[J]. 计算机学报, 2010, 33(1): 82-92.
ZHANG Bo, ZHANG Huan-guo, LI Jing, et al. The system architecture and security structure of trusted PDA[J]. Journal of Chinese Computer, 2010, 33(1): 82-92.

[9] 张晓菲, 许访, 沈昌祥. 基于可信状态的多级安全模型及其应用研究[J]. 电子学报, 2007, 35(8): 1511-1515.
ZHANG Xiao-fei, XU Fang, SHEN Chang-xiang. Research on multimedia security model based on trustworthy state and its application[J]. Acta Electronic Sinica, 2007, 35(8): 1511-1515.

[10] WINKLER T, RINNER B. Securing embedded smart cameras with trusted computing[J]. EURASIP Journal on Wireless Communications and Networking, 2010, 2011: 1-20.

[11] ROSENBLUM M, GARFINKEL T. Virtual machine monitors: current technology and future trends[J]. Computer, 2005, 38(5): 39-41.

[12] PIRKER M, TOEGL R, HEIN D, et al. A PrivacyCA for anonymity and trust[J]. Lecture Notes in Computer Science, 2009, 5471: 101-119.

[13] SWAMINATHAN A, MAO Y, WU MIN. Robust and secure image hashing[J]. IEEE Transactions on Information Forensics and Security, 2006, 1(2): 215-230.

[14] ANDERSON M, MOFFIE M, DALTON C, et al. Towards trustworthy virtualization environments: Xen library OS security service infrastructure[R]. Bristol: HP Research, 2007.

[15] MIT Trusted Computing. TPM/J: Java-based API for the trusted platform module (TPM), version 0.3[EB/OL]. [2010-06-10]. http://projects.csail.mit.edu/tc/tpmj/.

编　辑　税　红