ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 553-557
doi: 10.18178/wcse.2017.06.095

Video Authentication Protocol

Alex X. Galloway and Qingzhong Liu [+]

Department of Computer Science, Sam Houston State University, Huntsville, TX 77382, U.S.A.

Abstract. Video watermarking and fingerprinting can be enhanced by combining them with a video authentication protocol (VAP) that utilizes cryptographic hardware and metadata to indicate ownership, origin and device identity. While watermarking and fingerprinting provide significant protection against third party attackers, they neglect standardization, protecting against a malicious user, and device-specific origin questions that VAP answers.

Each time a video is recorded, VAP automatically creates and sends encrypted metadata to the manufacturer that created the video recording device. Then, another device may verify the video's authenticity by sending a verification request to the manufacturer via a web service. To analyze the viability of this new technology, three areas are examined: the storage requirements, the relative CPU time performance of its functions, and a comparative attack analysis.

Keywords: video authentication, watermarks, video fingerprinting, cryptographic hardware, video security.

1. Introduction

Just the production of movies in the United States is a 34 billion dollar industry, according to market research [1]. This does not take into account the growing amount of streaming television and movie services that came about since the dawn of YouTube and Netflix. Even Apple, traditionally a hardware platform and smartphone company, has decided to focus on offering streaming services.

Nearly all of these companies and video-based industries rely on the security of videos and protecting them against various threats from multiple attackers. In particular, one common security technique is authenticating a video, making sure it is the authentic and authorized form of a video that came from a legitimate source. While many useful algorithms have been created to analyze videos or protect their distribution and copyright laws, these methods tend to ignore the root of the authentication issue, which is providing a simple, protected authentication record produced by the video recording device. The closest commercial technologies to achieving this on their own use watermarking, fingerprinting and digital signature methods [2, 3, 4, 5, 6, 7, 8, 9].

Another proposed method is called the video authentication protocol (VAP). By remotely storing cryptographically-protected metadata, a video can be recorded and later verified as being an authentic, original video from a specific device. The various technologies at play in the video authentication protocol are not new, but combine together in a framework that can be compared against the traditional methods of video security.

The purpose of designing the video authentication protocol is to automate and improve video copyright protection and video origin evidence by unifying the benefits of video security with modern cryptographic technologies. There are primarily six security end goals with information. They are confidentiality, availability, authentication, authorization, integrity and non-repudiation [2]. They can be summarized in Table 1. In addition, there are several general goals that influence the various video security goals and technologies. Most of these are directly related to specific industries and organizations [3].

[+] Corresponding author. Tel.: + 001 936 294 3569.
E-mail address: liu@shsu.edu.

Table I: Information Security Goals

Defense Goal	Strategy	Attacker's Goal	Strategy
Confidentiality	Secure data	No confidentiality	Publish data
Availability	Provide access.	Not available	Disrupt access
Integrity	Secure creation and modification.	Unreliable data	Tamper
Non-repudiation	Track changes.	Fraud	Change data secretly
Authentication	Identify Proof	Spoof	Authenticate fake ID
Authorization	Division of roles and access controls	Unauthorized access	Break access controls

Since the proposed Video Authentication Protocol relies on the confidentiality of cryptographic keys, it is important to briefly review the technologies available. This is summarized in Table 2. The most relevant aspects to note is that current cryptography technology allows for hardware protection of cryptographic keys. Though each key is typically accessible for use by the local user, there are certain functions like remote attestation specifically designed for use only by a remote user [10]. VAP requires a key and camera hardware protection scheme for a remote user, the manufacturer. This is proposed in VAP as a Manufacturer Cryptography Control Chip (MCCC) [11], it can be summarized as doing the following in VAP: 1) Isolating and securing the video creation process; 2) Generating metadata; 3) Encrypting the metadata, using an encryption key unavailable for use by the user; 4) Digitally signing the metadata and providing a public key; and 5) Communicating the encrypted metadata to the manufacturer's cloud, receiving only requests from the manufacturer's cloud, and rejecting any requests by the user or other third parties.

Table II: Cryptographic Hardware

Hardware	Description
TPM	Trusted Platform Module is both a specification and hardware add-on or built-in that protects cryptographic keys and functions. Typically, only Windows mobile devices use TPM.
TrustZone	A virtualized co-processor that isolates and secures processes and is common in some ARM processor tablets and phones.
TEE	Trusted Execution Environment is a framework used with TrustZone and TPM for creating and implementing cryptographic functions.
Remote Attestation	This is a cryptographic function in use by TPMs and TEE that allows a remote user, like a manufacturer, to verify platform integrity.

2. Video Authentication Protocol

To build a VAP simulated prototype, an open source Android app was constructed with a NodeJS and MySQL server. VAP can be described functionally in four stages between three entities: the manufacturer and their cloud service; the camera device with the installed MCCC; and the third parties requesting that a video is verified, shown in Figure 1.

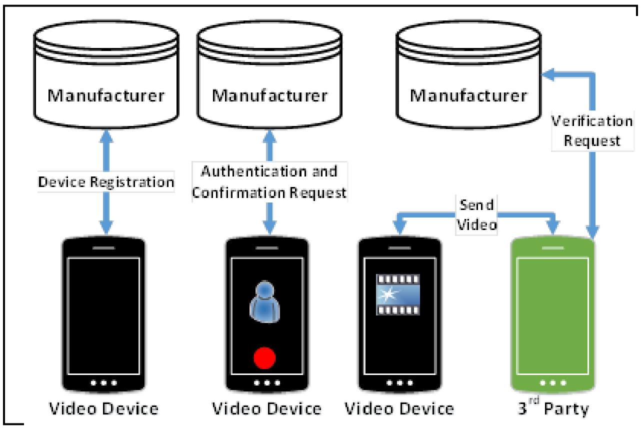

Fig. 1: The four stages of VAP

2.1. Four stages of VAP

The four stages include device registration, authentication, confirmation and verification, consisting of the following actions:

1) Device registration: an Internet-connected camera device is built by the manufacturer; The device is loaded with a digital signature key pair, not viewable except for the public key, but useable by the device user; The device is primed with an encryption asymmetric key, token and secret device ID, unknown and unavailable to the user; The manufacturer may store the above data with device-specific metadata in order to further verify and communicate with the device later.

2) Authentication: The user records a video; The hardware chip receives the video; The hardware chip analyzes it and stores at least a hash of the video metadata and of the file; The hardware chip digitally signs the data; The hardware chip encrypts the data payload with the necessary token, metadata and device identifiers using the encryption key; and The encrypted data payload sends to the manufacturer.

3) Confirmation: The manufacturer decrypts the request and verifies the secret device ID and token; It saves the video metadata, generates a new token, and sends an encrypted confirmation request to the device; The confirmation request includes the old token, a new token, and a hash of the metadata; The hardware chip receives the encrypted message and decrypts it with the encryption key; If the old token matches, the new token replaces the old token. Otherwise, the message is ignored; Then, the hashes received are checked against the hardware chip's stored hashes; If it matches, the device sends an encrypted confirmation; and finally, the manufacturer responds by annotating the video's data as confirmed and sends a new token to the device for the next communication.

4) Verification: The device sends the video and necessary verification data to another device; The second device checks the digital signature in the verification data and forwards it to the manufacturer's cloud address; and The manufacturer checks the database for a matching video and digital signature. If it is there, it returns true and additional corroborating metadata.

3. Comparing Video Authentication Protocol (VAP) to Other Methods

To compare VAP to other methods, three general attributes were examined, its storage requirements, the CPU time by the different parts of the VAP process, and methods of attack on the system. Lengthy descriptions of methodology and data are available in online supplemental documentation [11].

3.1. Storage requirements

This is important because VAP data is added to the video and sent with it. To analyze VAP storage requirements, three tasks were completed. First, the size of VAP data was measured in relation to the video size, and the same was done for a published fragile watermark called OpenPuff [12]. Second, an equation was formulated relating VAP data size to video size. There is no relation, so the resulting equation is:

$$VAP\ Data\ Size\ (S) = Fixed\ Size\ (c) \tag{1}$$

Then, it was speculated by looking at the fragile watermark measurements, fingerprint and other watermark algorithms, what would be their resulting storage size equation in general. The fragile watermark measurements show that some watermarks are size neutral, however, fingerprinting, and possibly some watermarks, must grow with the size of the video, since something is inserted in or extracted from every frame, groups of frames or groups of features. These other algorithms that grow linearly by frame would likely follow this equation:

$$Size\ (S) = Data\ to\ Video\ Ratio\ (b)*\ Video\ Size\ (V) + c \tag{2}$$

Finally, VAP, like fingerprints, must store data in a database. Using YouTube statistics from 2014 and estimating a 100 KB VAP data size, it was calculated that to implement VAP for all the new YouTube videos in 2014, approximately two hundred terabytes of storage would be needed [1].

3.2. CPU time

Android Studio allows for functions within an app to be relatively compared. The inclusive (Incl) CPU time counts the method itself and all methods called in order to execute the method. The exclusive (Excl) CPU time merely counts the time executed in the method. When an asynchronous request is called, that seems to add in to the time measurement as well. As can be seen in Table 3, the processing of the VAP data and cryptographic functions combined is minimal. Much of the resources for VAP are dedicated to communication requests to the manufacturer.

TABLE III: Top Level CPU Time of VAP Functions (Unitless)

VAP Function	Incl CPU Time	Excl CPU TIme
Verify Signature	0.325	0.021
Digitally Sign	2.025	0.061
Get Key Pair	4.198	0.050
Make Metadata	6.312	0.035
Process Confirm Request	11.119	0.059
Make File Hash	15.700	0.471
Process Authentication Request	54.069	0.201
Confirm Request	62.873	0.178
Record Video	124.408	4.653
Authenticate Request	139.311	622.353

3.3. Attack analysis

For the generic attack analysis, voluntary attacks were presumed. Attacks methods were first identified generically and categorized by their attacker, the user of the technology, a third party, or the manufacturer of the technology. Second, it was divided by security category, authentication, integrity or non-repudiation. The results of the analysis are summarized in Table 4. An unlikely perfect design is presumed, where all security risks would be low. “Trusted” means it is designed to trust the attacker, and no risk means the design precludes any advantage obtained by the attack method. Also, in the analysis, it is assumed the fingerprint database (DB) is used with a video upload service like YouTube.

- The second device checks the digital signature in the verification data and forwards it to the manufacturer’s cloud address.
- The manufacturer checks the database for a matching video and digital signature. If it is there, it returns true and additional corroborating metadata.

Table IV: Attack Analysis Risk Summary

Attack Method	Digital Security Type	Attacker	VAP	Watermark	Fingerprint DB
Spoof ownership	Authentication	User	Low Risk	Trusted	Trusted
Spoof origin.	Authentication	User	Low Risk	Trusted	Trusted
Spoof ownership	Authentication	3rd party	Low Risk	Low Risk	Low Risk
Spoof origin	Authentication	3rd party	Low Risk	Low Risk	Low Risk
Tamper Video	Integrity	3rd party	No Risk	Low Risk	Low Risk
Man-in-the-middle	Integrity	Multiple	Low Risk	No Risk	Low Risk
Deny Ownership	Non-repudiation	User	Low Risk	Low Risk	Trusted
Deny Origin	Non-repudiation	User	Low Risk	Low Risk	Trusted
Database Attack	Multiple	Multiple	Low Risk	No Risk	Low Risk
Insider Attacks	Multiple	Manufacturer	Low Risk	Low Risk	Low Risk

4. Discussions

In identifying attacks across VAP, watermarking and fingerprinting indeed showed VAP protects against a user spoofing origin and ownership information, whereas watermarks and fingerprints are not designed for that. As VAP prototype only concerns itself with the original video, tampering with the video is outside its scope, a scope handled by watermarks and fingerprints. As for most third party and manufacturer attacks, the three technologies tend to be integrated.

InformaCam is a software alternative to VAP, but there are three main differences which make InformaCam fall short of the VAP model, automation, hardware protection and a trusted authority. InformaCam is an open source software-only solution, meaning that it is implemented at the application level. The simplest attack at the application level is to use the open source to produce spoofed metadata. In addition, this means the origin of the video is not directed tied into the hardware, but into the software, losing any automated hardware-origin benefit that could have been obtained.

VAP’s hardware presents both advantages and disadvantages. Very little data is processed, and the cost of server storage is demonstrably small for the VAP given the 100KB size. Scalability to handle all the requests would present a more significant cost. This cost may be remediated by performing useful analytics on the customer’s data, or by having a paid service for more advanced multimedia security services.

Also, many mobile manufacturers are hesitant to add cryptographic hardware into mobile devices, as they are tiny and want the lowest price for the customer in order to be competitive. Adding more hardware makes mobile devices bigger and cost slightly more. This may be solved by identifying how the VAP may be implemented within TrustZone and TEE already used in mobile, or TPM in the case of Windows devices.

5. Conclusions

To reap all of the benefits of the VAP, watermarking and fingerprinting, they could be combined into a standardized VAP, which calls proprietary methods as designed by the manufacturer. For instance, when recording a video, a fingerprint method could be called, followed by a watermark method, and finally the VAP process. The fingerprints could be stored with the VAP information or in a separate more searchable database.

Reducing the protocol to its simplest form, to allow a variety of commercial applications, would mean having one standard verification request method and data format to send and receive. Each manufacturer’s methods could be rated against another’s methods more easily, as the rate of fraudulent videos to authentic videos could be obtained by an auditor who simply attempts to attack their VAP implementation. By having a standardized protocol, the industry may more easily trade to gain security advantages without exposing proprietary methods.

6. References

[1] “Movie & Video Production in the US Market Research | IBISWorld.” [Online]. Available: http://www.ibisworld.com/industry/default.aspx?indid=1245. [Accessed: 05-Mar-2017].

[2] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Amsterdam ; Boston: Syngress, 2011.

[3] E. Diehl, Securing digital video: techniques for DRM and content protection. Berlin: Springer, 2012.

[4] Saurabh Upadhyay and Sanjay Kumar Singh, “Video Authentication: Issues and Challenges,” International Journal of Computer Science Issues, no. 1, p. 409, 2012.

[5] J. Li, X. Guo, Y. Yu, Q. Tu, and A. Men, “A robust and low-complexity video fingerprint for multimedia security,” 2014, pp. 97–102.

[6] “InformaCam: Verified Mobile Media | The Guardian Project.”

[7] Bong-Joo Jang, Suk Hwan Lee, Sanghun Lim, Ki-Ryong Kwon, “Biological Infectious Watermarking Model for Video Copyright Protection,” Journal of Information Processing Systems, vol. 11, no. 2, pp. 280–294, Jun. 2015.

[8] T. M. Thanh, P. T. Hiep, T. M. Tam, and K. Tanaka, “Robust semi-blind video watermarking based on frame-patch matching,” AEU - International Journal of Electronics and Communications, vol. 68, no. 10, pp. 1007–1015, Oct. 2014.

[9] DaYou Jiang, De Li, and JongWeon Kim, “A Spread Spectrum Zero Video Watermarking Scheme based on Dual Transform Domains and Log-Polar Transformation,” International Journal of Multimedia and Ubiquitous Engineering, no. 4, p. 367, 2015.

[10] J.-E. Ekberg, K. Kostiainen, and N. Asokan, “The Untapped Potential of Trusted Execution Environments on Mobile Devices,” IEEE Security & Privacy, vol. 12, no. 4, pp. 29–37, Jul. 2014.

[11] “VAP Project Documentation,” Google Docs. [Online]. Available: https://docs.google.com/document/d/1U5X8R0J6hqfxfSocqD25XGrh5vDxPb3Ddg62irJVoeA/edit?usp=sharing.[Accessed: 20-Mar-2017].

[12] ‘OpenPuff - Steganography & Watermarking.” [Online]. Available: http://embeddedsw.net/OpenPuff_Steganography_Home.html. [Accessed: 20-Mar-2017].