Enhancing Authentication Protocol from Unauthorized Access

M.Muthuselvi, P.Jeevananthini, B.Vijayakumar

Dept of CSE, Sri vidya college of Engineering and Technology,TN,India
Dept of CSE, Sri vidya college of Engineering and Technology,TN,India
Dept of CSE, Acharya College of engineering, TN, India

Abstract
More web-based services involve distribution of content like digital video, audio, software, online games, stock quotes, from online stream presentations, and online live news feeds through distributed networking technologies, like Content Distribution Networks (CDN's), multicast networks, and peer-to-peer networks. So protect delay sensitive streams against malicious attacks, modification of content security mechanisms and auditing mechanisms need to be designed to efficiently process for user.So here propose a novel signature amortization technique based on trapdoor hash functions for authenticating each and every individual data blocks in the stream. So technique provides for each and every intermediate blocks in the stream Communication overhead should be minimized, prevent the content from unauthorized person.

Key Words:
Stream authentication, cryptography, content distribution network, trap door functions.

1. INTRODUCTION

In this paper, focus on the problem of efficient stream authentication and stream verification and auditing using digital signatures. The goal is to provide integrity, origin authentication, and non repudiation and auditing each and every individual data blocks that comprise digital stream. The problems faced by efficient authentication of stream poses several challenges:

The first problem faced by authentication of delay sensitive streams requires more verification rates for verify each and every individual data block in the stream.

The second problem faced by stream authentication for signature and other hash value mechanisms require high excessive bandwidth utilization and require high and more size for transmitted signed streams.

The third Problem for stream authentication for transmission of stream using unreliable transmission protocols like User Data Gram protocol leads to loss of datagram's during transmission.

In Existing approach the problems faced by stream authentication should be solved for one sender and receiver. Each sender and receiver must agree on a secret code with message authenticating code (MAC) to ensure authenticate each and every packet. In case of the multiple receivers it is harder to solve the symmetric approach either sender or receiver wants to any one holding a key. In order to avoid this proposed system use digital signature for sender to sign each and every packet with its private key.

In stream authentication security problems are even harder with many receivers this leads to loss in the data.

So want to ensure the authenticity of the data in the loss of high packets. In Existing paper for stream authentication they proposed different schemes,

The first scheme is TESLA (Timed Efficient Stream Loss-tolerant Authentication) and it offers authentication for the sender, provide high scalability and minimal overhead. Using symmetric cryptographic primitives for a pseudorandom Functions (PRFs) and message authentication codes (MACs) and it based on release of keys for the sender by time to time.

The second scheme is EMSS (Efficient Multi-chained Stream Signature) and it offers origin of non repudiation and it provides high loss resistance and it provides the cost of slightly delayed verification. It is used to signing a limited number of special packets in a data stream. Each and every packet should be linked as a signed packet via multiple hash chains. This can be achieved by appending the hash of each packet and also include the appending hashes of previous packets to the number of subsequent packets.

2. RELATED WORK

2.1 Trapdoor hash function

A trapdoor hash function is a special type of hash function. Trapdoor hash function is provided with a (public, private) key pair, and also referred to as a (trapdoor, hash) key. A trapdoor hash function is a probabilistic hash function, such that collisions are difficult to generate when only hash key is known, but easy to generate when trapdoor is also known. Collisions are very difficult to find without knowledge of trapdoor key pair Collisions resistance depends on the knowledge of trapdoor key(hash, trapdoor).The technique for signature amortization using concepts derived from application of trapdoor hash functions in building online/offline signature schemes [1]. Trapdoor hash functions provide the unique capability to

Manuscript received January 5, 2015
Manuscript revised January 20, 2015

find collisions between hashes of different messages using a secret trapdoor key.

2.2 Stream authentication

Stream (or flow) authentication that aims at reduces per-block communication and computation overhead, signature-based stream authentication techniques with securing each and every individual blocks in a stream. Leonid Reyzin et al [8], to design a stream authentication scheme with small communication overhead and fast authentication of each packet. Its complexity is the time required signing a message, authentication scheme itself no need modifications at all if asignature scheme, Stream signing is even faster than verifying. The only known key exposure-free trapdoor hashing schemes that prevent computation of additional collisions given a collision producing message pair is those by Harn et al. [5], Chen et al. [3], [4], [6] and one scheme by Ateniese and de Medeiros [2]. However, as will see in the next section, these schemes are computation expensive is high or unsuitable for use in building efficient stream authentication schemes.

2.3 Content Distribution

A Content Distribution Manager provides usage tracking service that enables logging of content usage. Caching service that implements content temporary storage from a media server. Content processing service through the requested content from the media server (or stores content into the media server), splits the media file into several blocks (or packet flows), and transmits the blocks to other edge caches or to clients. Request content processing service that provides navigation of the CDN to locate the content.

The number of users and devices connected by the Internet is growing [7] which increase the load on the servers that can handle only a limited number of clients. More servers will need to be deployed to cope with the growing number of clients [10], distributed leading through additional costs and overheads. Moreover, servers need to generate signatures when new stream content is uploaded, and for authenticating content in real time and dynamic content whose signatures cannot be cached. As the amount of content being distributed grows [9], servers will need to generate more signatures that can add up to significant processing overhead. In a problem is authentication generated only one sender and one receiver but rather to generate the authentication with multiple sender and receiver in multiple blocks.

3. Signature Amortization Technique

Distribute the content using distribute technology like Content Distribute Network. Sometimes it's designed with large group of user. Suppose if it is send a malicious means its goes to affect a client devices, to protect such delay sensitive streams against malware attacks like virus worms, here security mechanisms need to be designed to efficiently process for stream authenticate. So propose a novel signature amortization technique based on trapdoor hash functions for authenticating individual data blocks in a stream. To allow users to be timely and accurately informed about their usage of data, so distributed logging mechanism is complemented by an innovative auditing mechanism. Support two complementary auditing mechanism modes: Pull mode and push mode. During pull mode allows auditors to retrieve the logs anytime when they want to check the recent access to their own data. During push mode the logs are periodically pushed to the data owner.

- The advantages of the proposed technique:
- Communication overhead should be minimized.
- Prevent from modification of the content.
- Protect from unauthorized person

4. System Architecture Overview

Fig 1 shows system architecture of content distribution network. The components include the core data center, web cache and it serving the multiple clients and the back end of the content distribution network is internet or wan and the data centers. The caches should be distributed widely and serving the requested clients. Both the core data centers and web caches contains media server and the content distribution manager. The media content should be stored in the media servers and it should serve the content in both the real time as well as on demand users

3.1 Content Uploading

Server should upload the multimedia content was given by the content provider and store in a media Server. The client can also be allowed to upload the multimedia content after the registration process is done

3.2 Stream Authentication

Stream authentication can help prevent some type of attacks by providing the ability to sign and verify each block in the stream content. All stream content originates at the core data center and the stream signing mechanism is implemented at the core CDM as part of its content processing service. So assume the existence of a public key infrastructure (PKI) responsible for generating certificates

for the core Content Distribution Manager, and distributing the public key and certificate of the core Content Distribution Manager to all verifying entities. When a request arrives at the core Content Distribution Manager, the content processing service retrieves the content from the media server. The core Content Distribution Manager then splits the content it into a stream of blocks, signs each block (using a suitable signature amortization technique), places the authentication signed stream of blocks to the requesting entity.

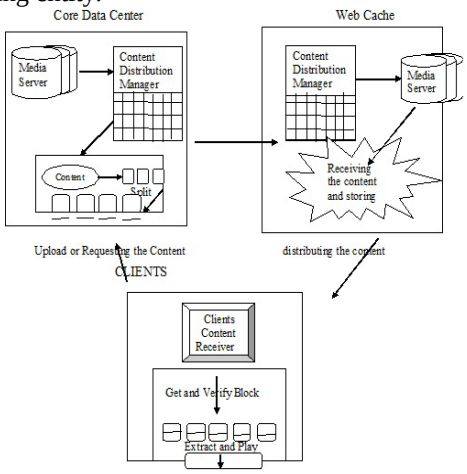

Fig 1: System Architecture Overview

If the stream content is not generated in real time from a core data center, the content processing service stores the signed stream at the media server to prevent redundant signing operations when subsequent requests arrive for the same content

3.3 Stream Verification

Threats involved in distribution of content include: Compromising malicious attacks, where an attacker takes control of legitimate content providing hosts (edge cache/core data center/third-party provider) to inject malicious content, and Man-in-the-middle attacks, where an attacker performs modification of content during transmission from core data center to the edge cache or from the edge cache to the client or from the core data center to the client.

Verification of signed streams at edge caches ensures that packets failing verification are not forwarded to the requesting client, through by preventing unnecessary usage of bandwidth and processing time at the client machine. When a signed content stream arrives at the client machine, the requesting application content verifies each block in the stream and removes the authenticating information placed inside the block before beginning playback of the media content.

5. Feature of Authentication of Online Digitized Technique

Thus a security and performance merits of the authentication of online digitized signature for the authentication of the stream. The packet loss should be robustness and the verification of each and every blocks should be depends on the of the stream. The arbitrary loss should be tolerated and the blocks containing signature should be reliably delivered to the receiver. Computation cost should be constant for the sender as well as receiver. The communication overhead should be constant and there are no multiple copies of the authenticating materials in the multiple blocks. The modification of the stream should be prevented and the forgery signature should be avoided.

6. CONCLUSIONS

The authentication flow in the content distribution network prevents malicious modification or threats in the middle of the data transmission. The challenging task is to verification and signing for the on demand content and the tolerance against the transmission loss and the communication overhead should be small per block. So present the authentication of online digitized signature using trap door hash function method the authentication flow in the content distribution network prevents malicious modification or threats in the middle of the data transmission. The challenging task is to verification and signing for the on demand content and the tolerance against the transmission loss and the communication overhead should be small per block. So Present the authentication of online digitized signature using trap door hash function method that challenges that meet real time streaming in content distribution and provide efficient authentication of delay sensitive streams. The authentication of online digitized signature method by authenticating from initial blocks in the stream using signature on the trap door hash function and by authenticating subsequent blocks in the stream.

REFERENCES

[1] Shamir and Y. Tauman, “Improved Online/Offline Signature Schemes,” CRYPTO ’01: Proc. 21st Ann. Int’l Cryptology Conf.,pp. 355-367, 2001.

[2] G. Ateniese and B. de Medeiros, “Identity-Based Chameleon Hash and Applications,” Proc. Eighth Int’l Conf, Financial Cryptography (FC), pp. 164-180, 2004.

[3] X. Chen, F. Zhang, W. Susilo, H. Tian, J. Li, and K. Kim, “Identity-Based Chameleon Hash Scheme without Key Exposure,” Proc. 15th Australasian Conf. Information Security and Privacy (ACISP), R. Steinfeld and P. Hawkes, eds., pp. 200-215, July 2010.

[4] X. Chen, F. Zhang, W. Susilo, and Y. Mu, “Efficient Generic Online/Offline Signatures without Key Exposure,” Proc. Fifth Int’l Conf. Applied Cryptography and Network Security (ACNS), J. Katz and M. Yung, eds., pp. 18-30, 2007.
[5] L. Harn, W.-J. Hsin, and C. Lin, “Efficient Online/Offline Signature Schemes Based on Multiple-Collision Trapdoor Hash Families,” The Computer J., vol. 53, no. 9, pp. 1478-1484, 2010.
[6] X. Chen, F. Zhang, H. Tian, B. Wei, W. Susilo, Y. Mu, H. Lee, and K. Kim, “Efficient Generic Online/Offline (Threshold) Signatures without Key Exposure,” Information Sciences, vol. 178, no. 21, pp. 4192-4203, 2008.
[7] K.Skaugen,“Cloud2015,”Proc.Interop,http://www.interop.com/lasvegas/2011/presentations/free/136-kirk-skaugen.pdf, 2012.
[8] L. Reyzin and N. Reyzin, “Better Than Biba: Short One-Time Signatures with Fast Signing and Verifying,” Proc. Seventh Australian Conf. Information Security and Privacy (ACISP), L.M. Batten and J. Seberry, eds., pp. 144-153, 2002.
[9] Cisco, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011-2016,” White Paper http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ ns705/ns827/white_paper_c11-520862.pdf, 2012.
[10] D. Grabham, “Intel: New Server Needed for Every 120 TabletsSold,”Techradar,http://www.techradar.com/news/computingcomponents/ processors/intel-new-server-needed-for-every-120-tablets-sold-1069