ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Authentication of Online Digitized Content Using Trapdoor Hash Function Method

M.Muthuselvi[1], P.Jeevananthini[2]

ME, Dept of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, India[1]

Asst. Prof. Dept of CSE, Sri Vidya College of Engineering and Technology, Virudhunagar, India[2]

ABSTRACT- Web based services involve distribution of content like digital audio, video, software, games, stock quotes, streaming presentations, and live news feeds through distributed networking technologies, like Content Distribution Networks (CDN's), multicast networks, and peer-to-peer networks. We protect delay sensitive streams against malicious attacks, security mechanisms and auditing mechanisms need to be designed to efficiently process long sequence of bits. We propose a novel signature amortization technique based on trapdoor hash functions for authenticating each and every individual data blocks in the stream. Our technique provides for each and every intermediate blocks in the stream we want to avoid the transmission loss and we will provide constant memory requirements for sender as well as receiver and we want to authenticate and verify the stream to avoid unauthenticated user and to avoid malicious content.

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

I. INTRODUCTION

In this paper, we 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 a digital stream.

THE PROBLEMS: faced by efficient authentication of stream poses several challenges:

1. 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.
2. The second problem faced by stream authentication for signature and other hash value mechanisms requires high excessive bandwidth utilization and requires high and more size for transmitted signed streams.
3. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In stream authentication security problems are even harder with many receivers this leads to loss in the data streams. The data loss will be based on the bandwidth of the receivers. With high packet loss leads to low bandwidth. We want to ensure the authenticity of the data in the loss of high packets. We have to design the stream authentication without loss of data blocks for the receiver.

In Existing paper for stream authentication they proposed different schemes

1. The first scheme is TESLA (Timed Efficient Stream Loss-tolerant Authentication) and it offers authentication for the sender, provide high scalability and minimal overhead. It is 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.

2. 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.

II.PROPOSED AUTHENTICATION OF ONLINE DIGITIZED TECHNIQUE

Digital streaming Internet applications such as online gaming, multimedia playback, presentations, news feeds, and stock quotes involve end-users with very low tolerance for high latency, low data rates, and playback interruption. To protect such delay sensitive streams against malicious attacks, security mechanisms need to be designed to efficiently process long sequence of bits. We study the problem of efficient authentication for real-time and delay-sensitive streams commonly seen in content distribution, multicast, and peer-to-peer networks. We propose a novel signature amortization technique based on trapdoor hash functions for authenticating individual data blocks in a stream.

The advantages of the proposed technique:

- To tolerate the out of order arrival rates and the transmission losses should be resilient in intermediate blocks without affecting the remaining blocks in the stream.
- The transmitting stream should be minimizes for the block signing process and the block verification process.
- The communication overhead should be limited while sending the authenticated message and for each block in the stream.
- The bandwidth should be limited with multiple blocks by sending authentication information.

III. 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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. Clients can include laptops, tablets and mobile phones.

A content distribution manager has the following functionalities

- Tracking or auditing or monitoring the content usage by the clients and accounting the usage of their respective clients.
- The contents requested by the clients should be fetched from the media server and partition the file into multiple blocks and transmitting the requesting blocks into appropriate clients.
- If the client requested the digital media content the request should be sent to closest web cache of the client. If the web cache contains the request which will be ask by the client it should be fetched and transmits to the client.
- If the request is not in the web cache means the request should be forwarded to the core data center and fetches the data and should transmit to the appropriate client.

A. 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.

B. STREAM AUTHENTICATION:

Stream authentication can help prevent some type of attacks by providing the ability to sign and verify each block in the stream. All 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. We assume the existence of a Public Key Infrastructure (PKI) responsible for generating certificates for the core CDM, and distributing the public key and certificate of the core CDM to all verifying entities. When a request arrives at the core CDM, the content processing service retrieves the content from the media server. The core CDM then splits the content it into a stream of blocks, signs each block (using a suitable signature amortization technique), places the authentication information within the block, and transmits the signed stream of blocks to the requesting entity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

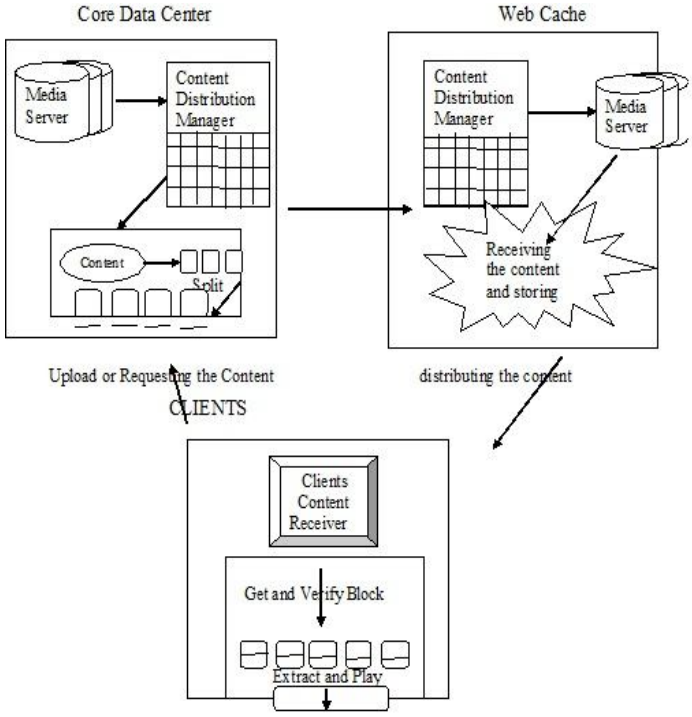

Fig1: System Architecture Overview

If the content is not generated in real time, 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.

C. STREAM VERIFICATION:

Threats involved in distribution of content include: Compromising attacks, where an adversary 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 adversary 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, thereby preventing unnecessary usage of bandwidth and processing time at the client machine. When a signed stream arrives at the client machine, the requesting application verifies each block in the stream and removes the authenticating information placed inside the block before beginning playback of the media content.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. FEATURES OF AUTHENTICATION OF ONLINE DIGITIZED TECHNIQUE:

We present 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 authentication 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.

V. FUTURE ENHANCEMENT OF AUTHENTICATION OF ONLINE DIGITIZED TECHNIQUE

To allow users to be timely and accurately informed about their data usage, our distributed logging mechanism is complemented by an innovative auditing mechanism. We support two complementary auditing modes:

1. Push mode,
2. Pull mode.

A. PUSH MODE:

In this mode, the logs are periodically pushed to the data owner (or auditor) by the harmonizer.

The push action will be triggered by either type of the following two events: one is that the time elapses for a certain period according to the temporal timer inserted as part of the JAR file, the other is that the JAR file exceeds the size stipulated by the content owner at the time of creation. After the logs are sent to the data owner, the log files will be dumped, so as to free the space for future access logs.This mode serves two essential functions in the logging architecture:

a. It ensures that the size of the log files does not explode
b. It enables timely detection and correction of any loss or damage to the log files.

B. PULL MODE:

This mode allows auditors to retrieve the logs anytime when they want to check the recent access to their own data. The pull message consists simply of an FTP pull command, which can be issues from the command line. For naive users, a wizard comprising a batch file can be easily built. The request will be sent to the harmonizer, and the user will be informed of the data's locations and obtain an integrated copy of the authentic and sealed log file.

VI. CONCLUSION

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

against the transmission loss and the communication overhead should be small per block. We 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. Our 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] B.M. Luettmann and A.C. Bender, "Man-in-the-Middle Attacks on Auto-Updating Software," Bell Labs Technical J., vol. 12, no. 3, pp. 131-138, 2007.

[2] Akamai, "Akamai Information Security Management System Overview: Securing the Cloud," White Paper, http://stag-wwwweb01.akamai.com/dl/whitepapers/Akamai_ ISMS.pdf?campaign_id=AANA-65TPAC, 2012.

[3] P. Bright, "Google, Microsoft Distribute Malware after Domain Name Trickery," Ars Technica, http://arstechnica. com/security/news/2010/12/google-microsoft-distribute-malware-after-domain-name-trickery.ars, 2010.

[4] A. Gonsalves, "YouTube Confirms Justin Bieber Hack Attack,"InformationWeek, http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID= 225702490, 2010.

[5] K. Skaugen, "Cloud 2015," Proc. Interop, http://www.interop.com/lasvegas/2011/presentations/free/136-kirk-skaugen.pdf, 2012.

[6] Cisco, "Cisco Visual Networking Index: Global Mobile DataTraffic Forecast Update, 2011-2016," White Paper, http://www. cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ ns827/-520862.pdf, 2012.

[7] 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-1069021, 2012.

[8] A. Shamir and Y. Tauman, "Improved Online/Offline Signature Schemes," CRYPTO '01: Proc. 21st Ann. Int'l Cryptology Conf.,pp. 355-367, 2001.

[9] G. Brassard, D. Chaum, and C. Cre´peau, "Minimum Disclosure Proofs of Knowledge," J. Computer and System Sciences, vol. 37,no. 2, pp. 156-189, 1988.

[10] H. Krawczyk and T. Rabin, "Chameleon Signatures," Proc.Network and Distributed System Security Symp. (NDSS), 2000.

[11] S. Even, O. Goldreich, and S. Micali, "Online/Offline Digital Schemes," CRYPTO: Proc. Ninth Ann. Int'l Cryptology Conf., pp. 263-275, 1989.

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