The Identity-embedded Technology in the Application of the IPTV Regulatory Platform

Xu Lu[1,a],Hongwei Ding[2,b],Xiang Li[3,c],Yong Wang[4,d],Jia Guo[5,e],Haiying Deng[6,f]
[1]School of information Yunnan University Kunming, China
[2]School of information Yunnan University Kunming, China
[3]School of information Yunnan University Kunming, China
[4]Science and Technology Department Radio of Yunnan province Kunming, China
[5]Science and Technology Department Radio of Yunnan province Kunming, China
[6]School of information Yunnan University Kunming, China
[a]695683175@qq.com,[b]Dhw1964@163.com,[c]66704215@qq.com,[d]wangyong@126.com,[e]Gy@126.com,[f]Dhy@126.com

Keywords: IPTV regulatory platform; identity embedded technology; monitor
Abstract. The identity embedded technology is a method for monitoring the active network information. Other content would be prevented from tampering with any content from the source. This paper analyses the identity embedded technology in the application of the IPTV regulatory platform of Yunnan province.

Introduction

Safety supervision system of the IPTV can be achieved on the program source of legitimacy to identify, prevent the program source tampering and illegal insert and realize the traceability function. This paper introduced the identification (Content Monitoring Indicator, CMI) concept, is a method for monitoring the active network information content monitoring technique requires Publisher content that has been published with the data tags. According to the markings on the record about the information, information gateway determines the information content, then examination, judgment and filtering operation. This technology can avoid the information recognition and extraction of complex operations.

1 Embedded and inspection technology

Logo design take into account both the video content providers copyright protection requirements, but also take into account the content of the video SARFT effective monitoring. Identifies at least contain video content copyright information (owners, producers, etc.), as well as the issue of the video content publisher's unique identification number (when the video has security issues, Soft could trace the responsible units or responsible person) engaged IPTV service license. In order to facilitate future content management, logo also added content title, summary, content rating and other information.

IPTV-based content regulation of the three major demands: source control, tamper-proof, source authentication, content regulation logo should have the following characteristics:
(1)Carry operator information and content information. This allows you to identify the test equipment to extract real-time information, when detected illegal content, facilitate the extraction of operators and content information tracking illegal sources, so as to realize the source of supervision.
(2)Carry content hash value. Hash operation after the content, when the attacker to tamper with the contents, because the hash function calculation is indirection, weak collision free, strong collision free etc, so as to the content of the modified to hash operation after will get different hash value, so you can find the attacker to tamper with the content, so as to realize tamper-proof.
(3)Using cryptographic techniques to protect the identity of the content regulation. By the underlying security infrastructure support, users can identify the operator information, certification, making an attacker can-not masquerade as legitimate operators, in order to achieve the source certification.

In IPTV monitoring system, identify the inspection system, there are three treatment options:

© 2014. The authors - Published by Atlantis Press

(1)In the general set-top boxes based on embedded ASIC embedded into the user's set-top box, a direct detection of illegal content filtering. But the need to transform the set-top box, workload is too big.
(2)Put into the transmission distribution networks, specifically placed in the third to fifth grade regulatory front end, detected by the gateway filtering illegal content.
(3)Add to the client carry out sampling tests, the program will form suspected violation alarm information sent to the monitoring center, regulators after the second artificial audit program will be recognized as illegal broadcast control platform by integrating offline. In actual construction, the second and third programs are equipped with better feasibility, can be used in combination.

2 Embedded and inspection technology design

In order to realize the IPTV content of the regulatory requirements, reference broadcast technology, embedded in a content monitoring identifies the CMI content in IPTV stream, the label contains content feature information(content hash value, operator information, content information), and to protect the password technology. When the user receives the IPTV content filtering through the identification, review inspection equipment, no program content identification or identification errors will be filtered, guarantee the received user is the legitimate content.

Used to provide a mass of IPTV service can operate IPTV architecture is more complex, often have different ways of realization of each operator. But most of the IPTV architecture usually adopt reference model as shown below:

Content providers for each channel by streaming content sources, the use of real-time transport protocol RTP transmission to the IPTV service provider's streaming media server. User terminal server access via service access business, streaming media server content transmitted via the RTP protocol to the user terminal.

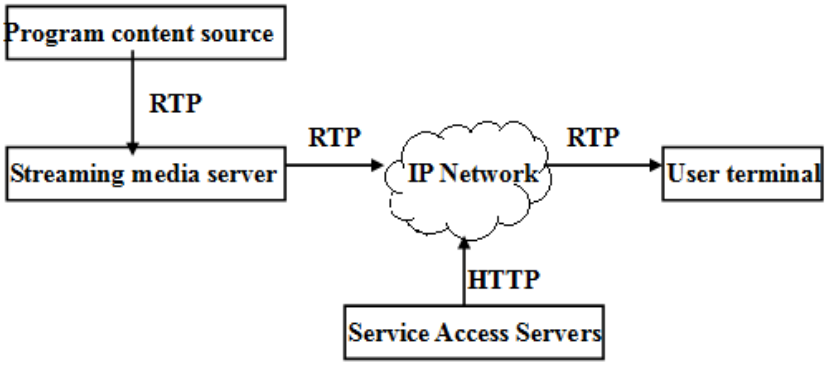

Figure 1 IPTV reference model

The introduction of IPTV content regulation reference model:
In the above reference model introduced content regulation, the reference model increases the logo embedded modules and identifies test module two functional modules. In every way the content provider via streaming content sources, first by identifying logo embedded module embedded content regulation, and then transmitted to the streaming media server. User terminal access service, the first test module by identifying regulatory identification test the legality of the content, and then play.

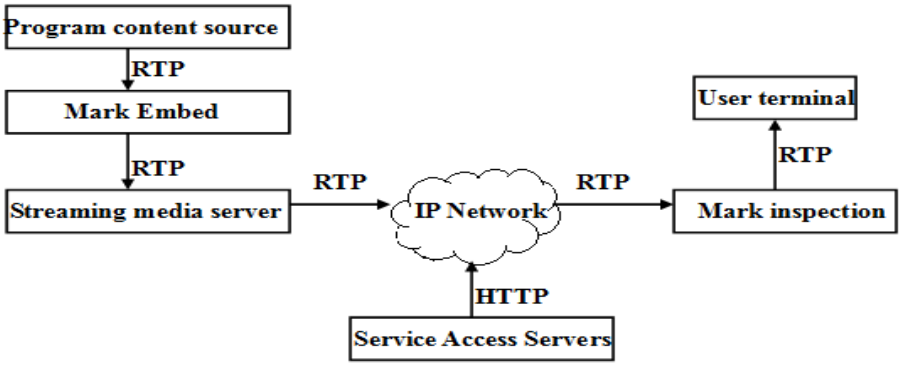

Figure 2 The introduction of IPTV content reference model identifies

3 Embedded and inspection technology process

Embedded in network television content stream CMI needs and content tightly bound, the attacker can-not replace the lawful content or illegal content disguised as legitimate content to spread illegal content; CMI requires tamper resistance, when the content is illegal tampering, by examining the CMI can effectively detect and alarm. Embedding process is as follows:

(1)Group: the CMI embedded module receives the RTP packet to packet, according to the Package Number value, divided into a number of RTP packages.

(2)Hash Algorithm: MD5 algorithm for each packet in RTP packet content hash operations, resulting in a 128 bit hash code MD1. According to the strong collision free nature of the MD5 algorithm, if the attackers tampering with the packet content, will produce a hash code for different values of the test module, which can detect attacks and corresponding treatment. But if the attacker packet content hash codes in tamper to calculate a new packet content and replace the original hash code value, test module will not be able to identify, so we need to improve the security of digital signature.

(3)Signature Process: the sender use private key of RSA algorithm to make the digital signature, MD1 receiver test using send the public key digital signature, thus to distinguish whether the hash code from the sender, so as to ensure the safe transport of the CMI. According to the previous analysis of the RSA algorithm, the encryption algorithm computation complex and long key length. So general choice for all packages of hash code all digital signatures, the result got a 1024 bits of the digital signature. Scatter hash code and digital signature to packages extension header, but due to the IPTV network conditions such as delay, packet loss phenomenon, cause the receiver cannot recover the data in the CMI. So still need to adopt fault-tolerant mechanism (FEC) in order to ensure reliable transmission of CMI.

(4)Error control on RTP. Increasing the coding redundancy,increase the minimum Hamming distance of the code to error detection and correction.

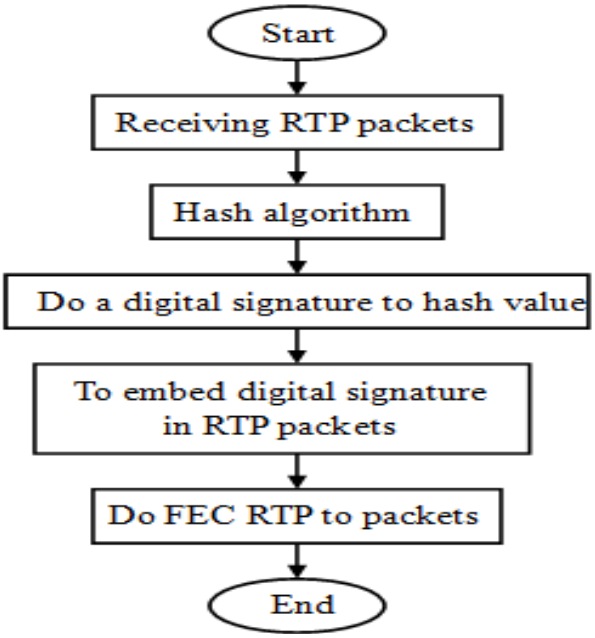

Figure3 The embedded process of CMI

After embedding, the RTP packet is transmitted to the receiver. The legitimacy of the user terminal via the CMI inspection module of CMI. The inspection process is as follows:

(1)Obtained from the receiving end of a smart card public key to verify the digital signature, if illegal the rule description grouped under attack, discard the packet.

(2)Get hash code MD1 and digital signatures, using FEC restore FEC Redundancy in the fields of all the hash code and digital signature.

(3)Get MD2: when the receiver to receive after RTP packets, use hash algorithm, MD5 algorithm to the package content do get hash code MD2.

(4)Compare MD1 and MD2 value due to a weak hash function collisions freedom, if the results are not equal, that the packet contents have been tampered with, discard the RTP.

(5)If digital signatures are equal in legal and MD1 and MD2 results, prove legal content, in the process of the transmission was not tampered with, the RTP packets sent to the user terminal playing module. Embedded and inspection technology Process chart is as follows.

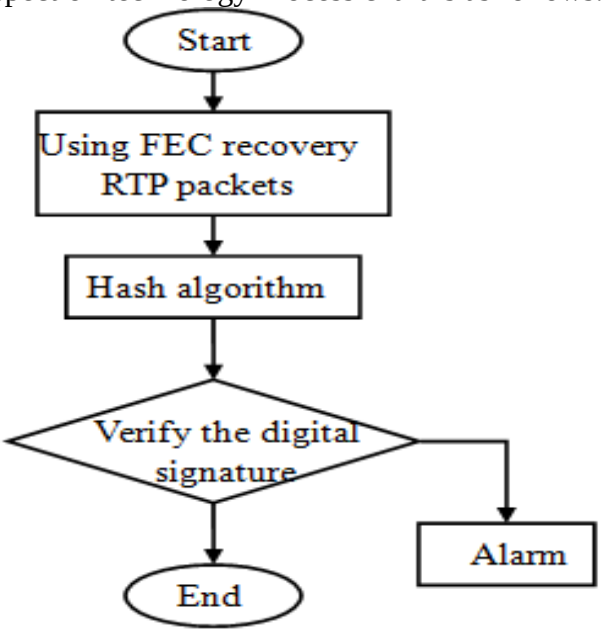

Figure4 The test process of CMI

Summary

As a network television hosted network IP network has the characteristics of openness, sharing, security problems inevitably. For IPTV may suffer from attack types using this method and the corresponding prevention attack capability analysis is as follows:

(1)Completely replace attack or replace packet payload attack

The attacker in the network television transmission process through completely replace the original RTP stream, or replace a packet payload way, trying to be legitimate content replacement for illegal content. In the user terminal through the test with or without CMI, the CMI hash codes and the calculated hash code, can find such attacks and alarm.

(2)Replace the package load, calculation and replace hash code, forge a digital signature.

Attacker by replacing the package load, according to the new package load calculation and replace the original hash code, according to a new hash code forged a digital signature or don't change the way a digital signature, trying to push the legal content is replaced with illegal content. Although the attacker recalculate and replace the hash code, but the attacker can-not obtain a content sender's private key for digital signature, enough key length makes it hard for attackers to forge the sender's digital signature content, the user terminal can recognize the illegal digital signature. Thus also makes replacement packet payload, and replace the hash code computing efforts become futile.

(3)Reverse operation, piecing together and replace packet payload attack.

Attackers don't change the hash code and digital signature, based on the hash code for reverse operation, piecing together and replace package loading way, trying to legal content is replaced with illegal content. The MD5 algorithm has the characteristics of indirection, the known hash code, package load is very difficult to solve, make the attacker attempts to not change the original hash code, solving out new, replace the contents of the attack is technically impossible.

Corresponding author

Hongwei Ding (1964 -), male, Professor of Yunnan University, PhD Degree. Mainly engaged in the research of random multiple access communication system, polling system, network communication engineering.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (61072079); Natural Science Foundation of Yunnan Province (2010CD023); Graduate Scientific Research Fund of Yunnan University (ynuy201047) financial support of Yunnan University(No.XT412004). This work was also supported by radio and Television Bureau of Yunnan province innovation platform project.

References

[1] Miyoung H, Shingak K. Mechanism for IPTV service discovery using SIP protocol[A]. The 9th International Symposium on Communications and Information Technology[C]. 2009. pp564-567.

[2] Froedroch O, Arbanowski S. Enhanced IPTV service control media delivery in next generation networks[A]. Conference on Internet Multimedia Services Architecture and Applications[C].2009.pp1-5.

[3] Wai L Y, Anh T H, Chen K T. On average packet delay bounds loss rates of network-coded multicasts over wireless downlinks[A].IEEE International Conference on Communications[C]. 2009.pp11-16.

[4] Sohrabi K,GaK J, Ailawadhi V, Pottle G J. Protocols for self-organization of a wireless sensor network. IEEE Personal Communications[J]. 2000, 7(5):16-27.

[5] Arisha K A, Youssef M A, Younis M F. Energy-aware TDMA—based MAC for sensor networks. In:Proceedings of IEEE Workshop on Integrated Management of Power AwareCommunications, Computing and Networking[C]. New York, USA: IEEE, 2002. 189-201.

[6] Wei,Heidemann J,Estrin D. An energy-eficient MAC protocol for wireless sensor networks. In: Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies[C]. New York, USA: IEEE, 2002. 1567-1576.

[7] Yang Zhijun, Zhao Dongfeng. QoS support polling scheme for multimediatraffic in wireless LAN MAC protocol. Tsinghua Science and Technology, 2008, 13(6):754-758.

[8] Liu Qianlin, Zhao Dongfeng, Zhao Yifan. An efficient priority service model with two-level-polling scheme[J]. High Technology Letters, 2011, 17(3):245-251.

[9] Qianlin Liu, Dongfeng Zhao, Dongming Zhou. An analytic model for enhancing IEEE 802.11 coordination function media access control protocol[J]. European Transactions on Telecommunications, 2011, 22(6):332-338.

[10] R Eckhom, H J Reitboeck, M Amdt Feature linking via stimulus-evoked oscillation: experimental results from cat visual cortex and functional implications from a network model[J]. Neural Networks, 1989, 1:723-730.