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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

A Design Proposal for Protecting Digital Distributions using Hash Code Pattern

Dr. G.M. Kadhar Nawaz[1], S.K. Indumathi[2]

Director, Department of M.C.A., Sona College of Technology, Salem, india[1]

Assistant Professor, Department of M.C.A., Dr. Ambedkar Institute of Technology, Bangalore, India[2]

ABSTRACT: The problem of protecting digital content data from illegal redistribution by an authorized node is the focus of considerable industrial and academic effort. The project introduces digital signets – a process for protecting digital content from illegal redistribution. The work motivates the study of the previously unexamined class of incompressible function, analysis of which adds a cryptographic twist to communication complexity. It introduces a data obscure methodology to overcome the data security without permission.

Keywords: Digital Water Marking, CSS, End-to-End Security, Tethered Security mode, Hash code, Cryptography

I. INTRODUCTION

The problem of protecting digital content data from illegal redistribution by an authorized node is the focus of considerable industrial and academic effort. In the absence of special-purpose tamper-proof hardware, the problem has no cryptographically secure solution: once a legitimate user has purchased the content, the node, by definition, has access to the material and can therefore capture it and redistribute it. A number of techniques have been suggested or are currently employed to make redistribution either inconvenient or traceable. We introduce digital signets, a technique for protecting digital content from illegal redistribution. The work motivates the study of the previously unexamined class of incompressible functions, analysis of which adds a cryptographic twist to communication complexity.

II. SURVEY

The various risk management strategies allows us manage security problems but are not very promising. For example, the credit cards used by the majority of people has its technology based on the magnetic strip which have proved to be not effectively protected. And similarly, our computer systems have been a victim to security flaws that are sometimes manageable and otherwise not. But with the help of risk management tools, the users of these resources have managed to surpass these challenges.

A. *Conventional Techniques*

There are numerous products and technologies that propogates as solutions to the problem of data leak or data piracy. But since these solutions work in limited deployments with predefined attacks, they tend to fail during unknown attacks. Thus there is a need to introduce a effective content protection system that can adapt to new threats without any compromises. The cryptographic systems which enables encryption of digital content can provide a long-term deterrent solution to avoid mishandling of data during content distribution.

1) *Digital Water Marking:* This has been proposed as a way to control and detect copying. It is to embed some information in a digital form which can be used to verify the authenticity of the data. But sometimes the technology allows the attacker to remove the mark if the watermarking technique is interpreted. And the current watermarking proposals are complicated making them expensive to embed and also to detect, and thereby requiring a improvised robust and effective technology to rely on. The challenge is to develop ever more invisible, decodable and permanent watermarking methods to meet more demands. At present, with the emergence of more sensitive applications non-invertible and non-extracting watermarking techniques are in the urge.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

2) *CSS:* Content Scrambling System (CSS) is a data encryption and authentication method used to protect digital versatile movies from being illegally copied, distributed, and viewed from other devices, such as computer hard drives. CSS is one of several copy-protection methods currently used in today's DVDs. The CSS provides a simple, fixed security policy for all contents. The content is compressed, encrypted and then put on read-only media and the player contains the keys to decrypt the contents. But the cryptographic algorithms have been proved to be weaker and easy to break.
3) *Smart Content:* The end-user devices have some APIs installed which authenticate security features and validate the user actions and also specify some device-specific controls. The actions on the documents can be controlled under suspicious environment. But the system cannot evolve with new attacks or threats that appear later after the implementation of the APIs and data-recovery is almost impossible in case of attacks.

B. *Design Challenges*

There are various issues to be considered as minimal requirements for an effective content protection system. These issues had to be reviewed for any technology which boasts of protecting the movement of digital data documents.

1) *Security Hierarchy:* The contents had to be secured from the source of the data till the destination and throughout the distribution channel in case of a point-to-point security system. For instance, each device has to receive the encrypted data, decompress it and use it and in case of further transmission it has to be re-encrypted and forwarded to the next device. But this system works well until all the devices and protocols are secure. The other system, end-to-end security system provides the required security mechanisms only at the source and destination systems. This system has been accepted to provide better risk management facilities than the former method.

2) *Controlled Execution:* The user must not be allowed to do any operations that might compromise the security aspects during data transmission. For example, the system should be able to identify anything unusual or tampering techniques being tried on the nodes or data.

3) *"Insecure" crypto-algorithms:* Though there is a lengthy collection of cryptographic algorithms, all supposed to be secured algorithms have been proved to be insecure at one or the other instant. Hence they are usually subjected to intense testing process by the cryptographic community before being implemented. This reluctance in accepting the cryptographic systems has been a challenge even which cryptographers had been facing.

4) *Design Independent:* As the implementation is to be reverse engineered, the security provided should be a part of the external system design and should not be a part of the system design.

5) *Security by Obscurity:* Most of the systems depend on the security by obscurity means which can promise security from only those what they expect to be a threat. This provides a false sense of security to those who rely on these systems for protecting their valuable content.

6) *Cost:* The cost of procuring and implementing the security codes should be minimal as it should not affect the overall cost of the master content.

7) *Reestablishment:* It must be easy to re-establish the security once a product or its design has been declared to insecure or is found to be vulnerable. This reestablishment should not affect the data or its path.

8) *Tethered and Untethered mode:* The untethered mode is where the key generated is kept with the data and hence is vulnerable as it might be possible to break or tamper the key. Whereas the tethered mode keeps the generated keys in a server and is transferred to the client when required. The tethered mode is difficult to design but has been proved to be better.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

III. PROPOSED SYSTEM

Carefully implemented cryptographic techniques with correctly implemented strong encryption algorithms can assure us that effective conversion between cipher text and plaintext without access to the key is computationally infeasible. Thereby the proposed system employs a strong encryption to eliminate the possibility that an attacker can remove the protection without first recovering the key. Protecting the encryption key presents a tremendous challenge on an open architecture.

A. Design Overview

We introduce new theoretical measures for the hash code pattern assessment of encryption schemes designed for broadcast transmissions. The goal is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing RKG key management related transmissions. We present a scheme that allows a center to broadcast a secret to any subset of privileged servers. It requires every nodes to store RKG keys and the sender to broadcast Binary messages regardless of the size of the privileged set.

We also present a scheme that is resilient with probability O against a subset repeats the same task based on n times foe the appropriate user. The problem of protecting digital content data from illegal redistribution by an authorized nodes, is the focus of considerable industrial and academic effort. In the absence of special purpose tamper-proof hardware, the problem has no cryptography secure solution: Once a legitimate user has purchased the content, the node, by definition, has access to material and can therefore capture it and redistribute it. The NI(Node Interface) is the RKG key for node and uploaded data are managed using the NI to create the encrypted data. Based on the verification, user can get uploaded data in readable format.

The figure 1 presents a diagrammatic flow of the proposed hash code pattern of encryption scheme between server nodes.

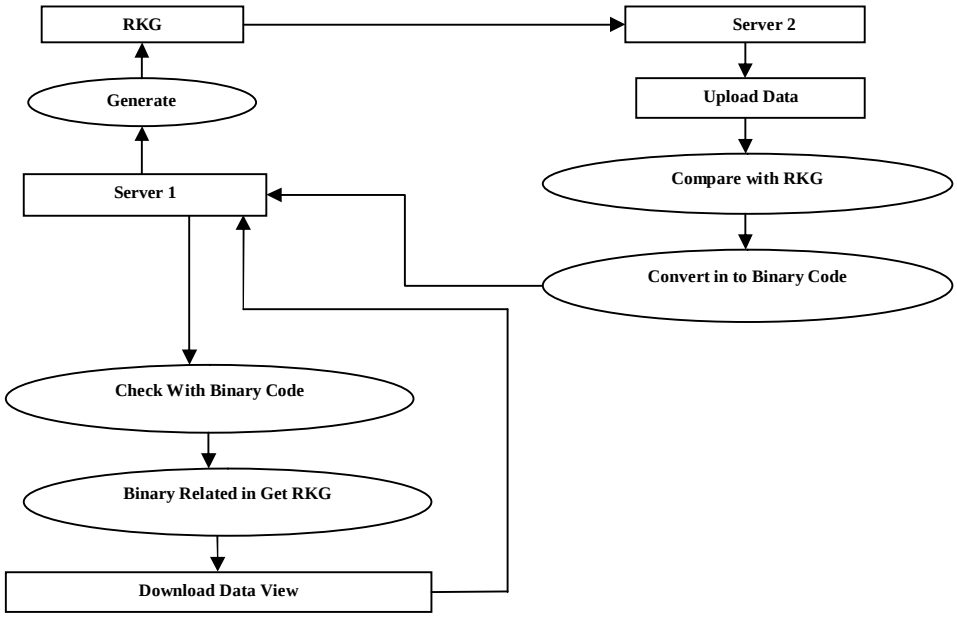

Fig 1 A sample overview of the proposed Hashcode Security pattern

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

B. Define Service Points to handle security:

We identify the service points where one node generates a random key for the data that is provided to it. This information is sent to another node that has been identified as the single service point to handle the security implementations. Here the code is divided into characters and converted into keys. These keys are associated with values which are converted into byte array. This is again converted into binary codes and transferred to the first service point. The second service point takes care of the data security and receives an acknowledgement from the first service point. The type of service that is to be provided depends on the acknowledgement that is provided by the requesting server. Some data are merely dropped without incorporating the security codes if the requesting node decides that the data is of lesser priority. The reverse mapping is also done by the same service point that was implemented initially.

C. Challenges Enforced

The proposed system has taken some of the issues that had long been a challenge to protect the digital data from being tampered or redistributed.

1) Security:
The system provides an end-to-end security where the data is protected throughout the distribution path and does not allow eavesdropping related activities. Though the data is sent through validated path the source determines the pattern of data downstream.

2) Reestablishment:
The code updates could be implemented whenever the system faces an illegal threat or is damaged during its data transmission. This helps to avoid redesigning of the entire system.

3) Uniqueness:
The Key Management System is unique for each access even between the same set of nodes. This does not complicate the design of the system but definitely makes it tougher for an attacker to break the security system.

4) Tethered Mode: The system uses a tethered mode where the key is generated and kept on a server and is sent to the client only when the data is to be transferred. After each access of the key, the key is discarded and a new key is generated. Hence the keys are only briefly exposed and is not available with the data. This makes the system invulnerable.

IV. CONCLUSION

Cryptography has been presumed to provide insufficient protection, but employing a strong encryption with a well-protected key can assure digital content protection. The architecture protects the digital content through encryption and key management techniques that work as two independent layers. Combination of these two techniques provides a data obscure method with a robust and mature cryptographic theory. The paper discusses the challenges that are faced in designing a cryptographic system and also lists out the challenges that had been enforced in the architecture. In conclusion, programmable systems provide better security than the conventional static approaches as they cannot withstand unusual and unexpected threats.

REFERENCES

1. Chen M.S and Yu P.S. (2004), 'Data Mining: An Overview from a Database Perspective', IEEE Transactions on Knowledge and Data Engineering, Vol. 8, 866-883.
2. Thulasimani Lakshmanan and Madheswaran Muthusamy 'A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes', The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012
Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi , 'Secure Digital Signature Schemes Based on Hash Functions' International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013.
3. M. Bellare, and P. Rogaway ,"Entity authentication and key distribution". In Advances in Cryptology — CRYPTO'93, pp. 232-249, 1994.
4. Gunjan Gupta and Rama Chawla, 'Review on Encryption Ciphers of Cryptography in Network Security', International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X