Broadcast Encryption Research Project
- Proposal -

-

Department of Computer Science
University of Calgary

Abstract

This paper examines *Broadcast Encryption*, particularly its motivation, requirements and implementation. Further, this paper examines in depth the motivation and implementation issues relevant to *Traitor Tracing* and *Digital Rights Management*. A specific emphasis is placed on the failure of current DRM schemes and examines the question of whether DRM systems could be feasibly implemented on user accessible systems.

Key words: Broadcast Encryption, Cryptography, Internet, Network Security

1 Introduction

As research and production of digital technology advances, this technology becomes ever more integrated into our society. The advent of High Definition Television and dedicated Multimedia Centres is evidence of the extent to which this integration has progressed. Along with the technology for displaying digital content comes the necessity of transporting that content to the end user. The process of getting content to the end user is further complicated by the ease with which digital content can be eavesdropped and replicated without any loss of information. Broadcast encryption is a technology being developed to address this problem. In essence, it is a means by which information can be delivered to multiple end users simultaneously while managing a mutable list of authorized users[2]. The intention is for this technology to enable content control by the transmitting party regardless of the medium, it is intended for use on CD/DVD physical mediums as well as electronic mediums such as dedicated cable networks and the Internet[7]. All of these mediums have the common property that the data on the medium can be accessed by unauthorized parties and in unauthorized ways, it is the goal of broadcast encryption to establish control over this property[8].

1.1 Literature

Broadcast encryption is still very much an open problem and is seeing a large number of papers currently published on the topic. One of the first papers to appear on the topic was called "How to Broadcast a Secret" in which Berkovits introduced the problem and proposed several solutions[4]. The scope and terminology of the problem was established by Naor and Fiat in 1993[2]. Since then, many papers have been published describing various schemes and additional problems with respect to specific areas of broadcast encryption such as *digital rights management*[8], *key management* [9] and *traitor tracing*[11]. Several schemes for implementing broadcast encryption have been proposed, such as *ID based encryption*[10], *short key and transmission schemes*[3], *collusion resistance*[5], and the *Layered Subset Difference* scheme proposed by Shamir and Halevy[6]. All of these papers examine particular elements of broadcast encryption, each illuminating a particular part of the problem.

1.2 The Paper

This paper will be primarily an overview of broadcast encryption and the current state of its development. As such the paper will begin with the general elements of broadcast encryption and then move on to a specific recent implementation, *The LSD Broadcast Encryption Scheme*[6]. In addition to the general topic of broadcast encryption, this paper will examine in more detail the concepts of *Traitor Tracing* and *Digital Rights Management* [8]. In particular DVD copy protection and the failure of *CSS* [1] will be examined in the context of the question: Can there exist true copy protection on user accessible electronic mediums?

1.3 General Outline

- Abstract
- Introduction
- Detailed description of broadcast transmissions
  - Properties of senders
  - Properties of receivers
- Requirements for broadcast encryption
  - Motivation for Broadcast Encryption

  - Key Management concepts
- The LSD Broadcast Encryption Scheme
  - Stateless Receivers
  - Subset Difference Scheme
  - Layered Subset Difference Scheme
- Traitor Tracing Techniques
  - Motivation for Traitor Tracing
  - Collusion detection
- DRM and DVD Copy Protection
  - Motivation for DRM
  - General DRM Concepts
  - Breaking CSS DVD Copy Protection
  - CPPM DVD Copy Protection
  - Bottom Line DRM issues
- Conclusion
- Bibliography

2 Time Line

This research paper will be completed by the assigned deadline of April 15, 2005.

3 Conclusion

Broadcast encryption is an emerging area of technology that touches the heart of many current social issues. As such, the technology is quickly growing in two directions, one direction to enhance security and the other to defeat it. This pattern ensures that both streams of technology must competitively attempt to outpace each other, and as such presents interesting and difficult academic challenges.

References

[1] Andre; Adelsbach and Jorg Schwenk. Key-assignment strategies for cppm. In *MM&Sec '04: Proceedings of the 2004 multimedia and security workshop on Multimedia and security*, pages 107–115. ACM Press, 2004.

[2] Moni Naor Amos Fiat. Broadcast encryption. *Advances in Cryptology - CRYPTO '93 Proceedings, Lecture Notes in Computer Science*, 773:480–491, 1994.

[3] Nuttapong Attrapadung and Kazukuni Kobara. Broadcast encryption with short keys and transmissions. In *DRM '03: Proceedings of the 2003 ACM workshop on Digital rights management*, pages 55–66. ACM Press, 2003.

[4] S. Berkovits. How to broadcast a secret. In D. W. Davies, editor, *Advances in CD, cryptology, EUROCRYPT'91, Lecture Notes in Computer Science*, volume 547, pages 535–541. Springer Verlag, 1991.

[5] Dan Boneh and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. Cryptology ePrint Archive, Report 2005/018, 2005.

[6] Dani Halevy and Adi Shamir. The LSD Broadcast Encryption Scheme. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, pages 47–60. Springer-Verlag, 2002.

[7] Jeremy Horwitz. A survey of broadcast encryption. Manuscript, 2003. http://math.scu.edu/ jhorwitz/pubs/broadcast.pdf.

[8] Pestoni F Lotspiech J, Nusser S. Anonymous trust: digital rights management using broadcast encryption. In *Proceedings of the IEEE, Vol.92, Iss.6, June 2004*, pages 898– 909, 2004.

[9] Avishai Wool. Key management for encrypted broadcast. *ACM Trans. Inf. Syst. Secur.*, 3(2):107–134, 2000.

[10] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 354–363. ACM Press, 2004.

[11] T. Yoshida, M.; Fujiwara. An efficient traitor tracing scheme for broadcast encryption. In *Information Theory, 2000. Proceedings. IEEE International Symposium on*, pages 463–, 2000.