Tutorial on Content Protection

Nelly Fazio
IBM T.J. Watson Research Center
19 Skyline Drive
Hawthorne, NY 10532-1596, USA
+1-914-784-6284
nfazio@us.ibm.com

Dulce Ponceleón
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120-6099, USA
+1-408-927-1927
dulce@almaden.ibm.com

ABSTRACT
Devising effective Content Protection mechanisms and building satisfactory Digital Rights Management systems have been top priorities for the Publishing and Entertainment Industries in recent years. In this tutorial, we focus on protection tools and standards for entertainment content. We analyze the challenges of content protection systems, ranging from legal aspects and business models to cryptographic techniques. We discuss current technology licensing practices, describe state-of-the-art broadcast encryption mechanisms and forensic approaches, and present content protection standards such as 4C and AACS.

Categories and Subject Descriptors
E.3 [**Data Encryption**]: *Public key cryptosystems*; K.5.1 [**Hardware/Software Protection**]: *Copyrights, Licensing*; K.6.5 [**Security and Protection]:** *Authentication, Unauthorized access (e.g., hacking, phreaking).*

General Terms
Human Factors, Legal Aspects, Security, Standardization.

Keywords
4C, AACS, Blu-ray disc, Broadcast Encryption, Traitor Tracing.

1. INTRODUCTION
The future of digital distribution is *customization*. The media and entertainment companies have come together to define strategies and cutting-edge technologies focusing on tailoring content to the individual. The goal is to create innovative systems which will make experiencing and consuming digital content easier than ever, delivering you exactly what you want, when you want it.

Content creator, TV studios, movie studios networks are strategizing on how to survive this new trend in delivering digital content. The old way of packing the content and sending it to the market is now replaced with an interactive relationship with the consumers. The goal is to understand the preferences and behaviors of potential customers and offer a personalized and therefore enhanced user experience.

MM'08, October 26–31, 2008, Vancouver, British Columbia, Canada.
ACM 978-1-60558-303-7/08/10.

This tutorial starts off introducing the notion of content protection and describing the main components of a content protection system. Next, we define the relevant security notions and describe two essential cryptographic primitives: broadcast encryption schemes and traitor tracing techniques. A broadcast encryption scheme allows a content provider to encrypt the digital content in such way that only authorized receivers are able to recover the original data. A traitor tracing scheme is a mechanism capable of detecting the illegal redistribution of content or access keys. In particular, we describe the broadcast encryption scheme of Naor-Naor-Lotspiech, which achieves the best security guarantees among the schemes of wide practical adoption. We will also describe an extension to the NNL scheme, due to Dodis-Fazio. The extended scheme operates in the public-key setting, in which multiple content providers can share the cost of maintaining a single common infrastructure to deliver the content to its own set of authorized users.

We also describe the Content Protection for Recordable Media (CPRM) technology, along with its recent extension, the Secure Digital with Separate Delivery CPRM system (SDSD-CPRM). SDSD-CPRM adds the ability to independently maintain the encrypted content and the access keys used to decrypt it. This novel capability of the SDSD-CPRM enables various ways to move, distribute, restore and backup content between SDSD-CPRM compliant devices.

While cryptography remains an important component in the design and development of a DRM system, a complete solution to the DRM problem require efforts from many different area. We will go through the analysis of adequate business model to discourage privacy without putting to much burden on the side of customers. Next, we review the relevant legal issues which are centered around the problem of specifying the conditions under which legitimate users are authorized to make copies of purchased content. We will ground the discussion by describing several content protection standards, such as 4C and Advanced Access Content System (AACS).

2. ATTENDEES GOALS
The tutorial is targeted at a beginner to intermediate audience, i.e. no background on cryptography is assumed. Intermediate students will have the opportunity to get summary of existing content protection systems and emerging standards. Industrial practitioners will walk away with an understanding of challenges of real content protection systems, from design, legal issues, to adoption.

3. TUTORIAL OUTLINE

- Content Protection Overview
  - Definition
  - Components of Content Protection Systems
    - Conditional Access, Digital Rights Management, Copy Protection
- Legal Aspects
  - IP, Copyright, Licensing
  - Piracy and its Categories
- Security Concepts Overview
  - Cryptographic Objectives
  - Cryptographic Primitives
  - Cryptographic Protocols
  - Attack scenarios
- Secure Distribution of Content and Access Keys
  - Broadcast Encryption Schemes
    - Matrix-based: CPRM
    - Tree-based: NNL and DF
  - Forensic Technologies
    - Traitor Tracing Schemes
    - Watermarking and Fingerprinting Schemes
- Flexible Protection for Digital Content
  - SDSD-CPRM
- The Digital Home Network
  - HANA
- Open Standards
  - 4C and AACS
  - HD-DVD versus Blu-ray Disc Format
- Future of Content Protection and Challenges

4. SPEAKERS' BIOGRAPHIES

The authors bring expertise in cryptographic applications to Content Protection and first-hand participation in two standard bodies (4C and AACS) providing key technical support role (with licensees) and first-hand design, implementation and deployment of key generation and management systems.

4.1 Nelly Fazio

Nelly Fazio earned her M.Sc. ('03) and Ph.D. ('06) in Computer Science from New York University. During her studies, she also conducted research at Stanford University, École Normale Supérieure (France) and Aarhus University (Denmark). In 2003, she was awarded the NYU CIMS Sandra Bleistein prize, for "notable achievement by a woman in Applied Mathematics or Computer Science." Her Ph.D. thesis was nominated with honorable mention for the NYU J. Fabri prize, awarded yearly for the "most outstanding dissertation in Computer Science."

Dr. Fazio's research interests are in cryptography and information security, with a focus on digital content protection. Since July 2006, she is part of the Content Protection group at IBM Almaden Research Center, where she has been conducting research on advanced cryptographic key management, tracing technologies, and authenticated communication in dynamic federated environments. Currently, she is a visiting research scientist in the Security group at IBM T.J. Watson Research center, working on security issues of decentralized environments such as mobile ad-hoc networks (MANETs) and sensor networks.

4.2 Dulce Ponceleón

Dulce B. Ponceleón holds an M.S. and a Ph.D. degree in computer science from Stanford University. She worked in the Advanced Technology Group at Apple Computer, Inc., where she worked on information retrieval, video compression and audio compression technologies for QuickTime. She was a key contributor to the first software-only videoconferencing system. She is currently at the IBM Almaden Research Center, where she manages the Content Protection Competency Center. She has worked on multimedia content analysis and indexing, video summarization, applications of speech recognition, storage systems, and content protection. She contributed to the ISO MPEG-7 standardization efforts, specifically in Multimedia Description Schemes. She is an IBM technical representative in 4C and Advanced Access Content System (AACS). The 4C Entity has developed content protection standards for recordable and pre-recorded media (CPRM/CPPM).

Dr. Ponceleón is the Chair of the 4C Technical Group since 2004. AACS is a content protection standards for managing content stored on the next generation of pre-recorded and recorded optical media for consumer use with PCs and CE devices. Dr. Ponceleón has been on the Scientific Advisory Board of a leading NSF multimedia school, and a program committee member of ACM Multimedia, SPIE, SIGIR, IEEE, and several multimedia workshops. She has held workshops on multimedia standards (ACM MM 2000), panels on streaming video (ACM MM 2001), and multimedia information retrieval tutorials (SIGIR 2002, SIGIR 2005 and ICASPP 2006). She holds patents and numerous publications in video and audio compression, multimedia information retrieval, numerical linear algebra and non-linear programming. She holds several patents and numerous publications in video and audio compression, multimedia information retrieval, content protection, human computer interfaces, numerical linear algebra and non-linear programming.