An Analysis of BD+ and Other Major Schemes of DRM

Urvi Tank
Upendarreddy Mamidi
Sangamitrareddy Katamreddy
Agenda

• Three techniques of digital right copy protection
• Content Scrambling System (CSS) and attacks on CSS
• Advanced Access Control System (AACS) and attacks on AACS
• BD+ and attacks on BD+
Content Scramble System (CSS)

- Protects DVD video disc from copying.

**Diagram:**

- DVD CCA
- 409 Player keys
- Manufactures (pay fees)

DVD Copy Control Association (DVD CCA)
What DVD Contains?

Mark Barry (June 2004); “Cryptography in Home Entertainment” [online]; Available: http://www.math.ucsd.edu/~crypto/Projects/MarkBarry/
Decryption Process

\[
K_{DISK} = D_A(D_{K(N)}, K_{PLAYER(N)})
\]

\[
K_{DISK} = (\text{hash}, K_{DISK})
\]

Equal

Yes, valid disk key

\[
K_{TITLE} = D_B(tk, D_{KDISH})
\]

\[
\text{DATA\_OUT} = D_C(IN, K_{SECTOR}, K_{TITLE})
\]

Sector key (Unencrypted)

2048 bytes sector

Movie Data

Disc

Decryption of keys (key mangling stage)

<table>
<thead>
<tr>
<th>Mode</th>
<th>LFSR 17</th>
<th>LFSR 25</th>
<th>Seed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disc key $D_A$</td>
<td>-</td>
<td>-</td>
<td>Player key</td>
</tr>
<tr>
<td>Title Key $D_B$</td>
<td>-</td>
<td>Invert</td>
<td>Disk Key</td>
</tr>
</tbody>
</table>

Decryption of data


<table>
<thead>
<tr>
<th>Mode</th>
<th>LFSR 17</th>
<th>LFSR 25</th>
<th>Seed Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data $D_C$</td>
<td>Invert</td>
<td>-</td>
<td>(Sector key) XOR (Title key)</td>
</tr>
</tbody>
</table>
 Attacks on CSS

• Brute force attack can be possible since the key length is 40 bits – 5 bytes.

• LFSR Cipher attack ($2^{16}$ attack) (attack with 6-bytes of LFSR) was attempted.
Evolution of AACS

- Checking with the revocation list on both drive and host side
- Signature verification by ECDSA and bus key sharing
AACS
Encryption and Decryption of Pre-Recorded Media

Kevin Henry et al., “An Overview of the Advanced Access Content System (AACS)”, David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.
Encryption and Decryption of Recordable Media

Kevin Henry et al., “An Overview of the Advanced Access Content System (AACS)”, David R. Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, N2L 3G1, Canada.
Broadcast encryption and analogy to AACS

U - Universal set of users
R - Revoked set of users
P - Privileged set of users
P = U/R = \{S1, S2, S3, ..., SN\}

<table>
<thead>
<tr>
<th>Broadcast Encryption</th>
<th>AACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index of each subset</td>
<td>UV number and U mask in explicit subset difference</td>
</tr>
<tr>
<td>Long lived keys</td>
<td>Processing key produced after finalising the device key</td>
</tr>
</tbody>
</table>
MEDIA KEY FORMAT

Example Media Key Block Format Records

UV-subtree Data

Media Key Data

Every device key is associated with a uv number.

Uvnumber = pathnumber//vmask and umask

Path number denotes the path of the device from the root node and umask and vmask denotes depth of unode and vnode from root A respectively.
ATTACKS ON AACS

• The process of AACS is captured from the program running in PC
• The keys are published
• Renewal of keys- took very short time to break it
• BD+ is based on Self-Protection Digital Concept.
• The virtual machine embedded in authorized players runs title specific code provided from BD-ROM discs.
• Re-secure compromised environments without revoking the player.
• Copying of content is restricted by the ROM-MARK on the disc

EVOLUTION OF BD+

BD+ Overview
Virtual Machine functionality

- Perform security check by matching BD+ keys with the certificate.
- Checks player’s playback environment by checking memory footprint.
- Begin Play back after above checks are complete.
BD-ROM Content Protection Environment

Deriving the BD-ROM Title Key

BD+ Media Transform Process

**BD+ PHASES**

- Transformations – Alter content stream before decoding
- Basic Countermeasures – Respond to attacks
- Advanced Countermeasures – Execute native code

**ATTACKS ON BD+**

- Along with the attacks the process and techniques of BD+ are changing challenging the attacks
- POINT to POINT security to END to END security
- PUBLIC WATERMARKING to FORENSIC MARKING
Thank You
TIME FOR QUESTIONS