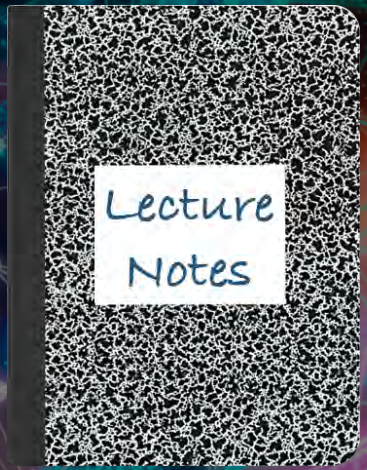
CS 419: Computer Security

Week 13: Part 4
Content Protection



Paul Krzyzanowski

Content protection

- **Digital content is simple to copy and distribute**
  - Software, music, video, documents
- **That's not always good**
  - How do software companies & artists make a living if their content is freely distributed on a large scale?
    - Maintain revenue streams
    - Enforce distribution rights (e.g., video available in the U.S. first)
  - How do organizations keep their documents secure?
    - Enforce confidentiality & protect trade secrets?

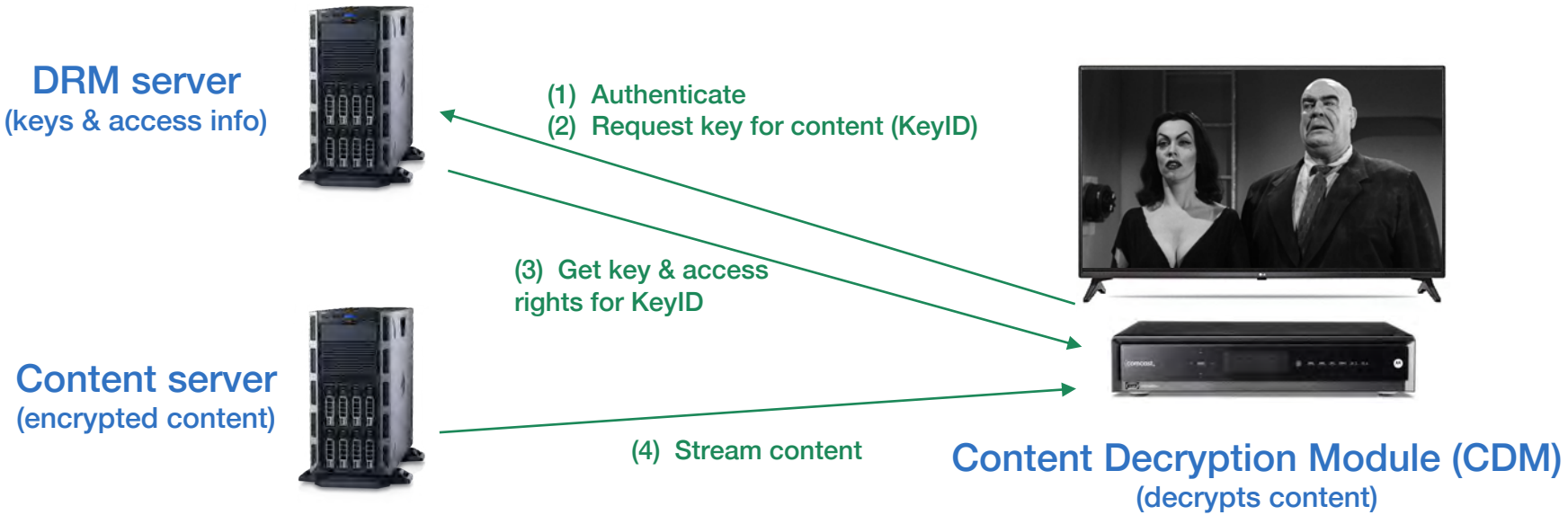
How can we make illegal content access difficult?

DRM

- **Content industry (movies, music, documents) asked for technical solutions to the content distribution problem**
- **This led to digital rights management (DRM)**
  - Protection of content
  - Definition on how it can be played and copied
- **Not just documents, music, & movies:**
  - Printer cartridges
  - Keurig coffeemakers
    - RFID connections enforce use of Keurig-branded K-cups
  - John Deere tractors

Basic DRM concepts

- To deliver content securely, encrypt it
- Store the keys on a DRM server along with access rights



Video Decode & Playback

- **The CDM needs to be trustworthy**
  - Don't leak the decryption key
  - Enforce playback rules
  - Don't leak the content

- **CDMs are closed-source**
- **Need direct path to hardware**
- **Key rotation just in case**

Content Decryption Module (CDM)
(decrypts content)

Use of the Trusted Execution Environment (TEE)

- **Software can decrypt content but**
  - It can be inspected
  - Modified
  - Output can be redirected
- **DRM decryption is usually done in hardware – in the TEE**
- **Content providers may alter content based on the playback device**

Widevine Content protection

Three security levels

- **L1: Most secure – used by most streaming services**
  - Requires TEE
- **L2: TEE only performs cryptographic operations**
- **L3: All operations are done outside the TEE**
  - Usually allows only 480p or lower resolution playback

Content isn't really protected

How do you use open source players (e.g., VLC) to play encrypted Blu-ray content?

People built databases of media keys – so no need to decrypt the media key

- Do a google/bing search for **AACS KEYDB.cfg**
  - http://fvonline-db.bplaced.net
- Individual keys for all each film
  - 20,231 VUK (volume unique key) entries
  - 111,347 legacy entries (contact server to get key)
- Processing keys
  - Work for all content
  - But can be revoked!
    - Newer discs can revoke old processing keys

There's also the analog hole

Legal barriers: DMCA

Digital Millennium Copyright Act

Criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (DRM) that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself.

Without DMCA, anyone would be able to build a set-top box to decode video signals

- Just crack HDCP (High Definition Content Protection)

Also

- Licensing agreements (EULAs)
- EU's Copyright Directive

The End