

CS 201P - Computer Security, Notes

Fall, 2021

Please find below lecture slide notes associated with the lectures for CS 201P, Computer Security.

Notes:

- **Introduction:**
 - [Introduction](#).
- **Physical Security:**
 - [Locks and Keys](#).
 - [Authentication Technologies](#).
 - [Direct Attacks](#).
- **Operating Systems Security:**
 - [OS Concepts](#).
 - [SetUID](#).
 - [Environment Variables](#).
 - [Buffer Overflow Attacks](#).
 - [OS Security](#).
- **Malware:**
 - [Malware](#).
- **Network Security 1:**
 - [Network models and ARP security](#).
 - [TCP/IP Security](#).
- **Network Security 2:**
 - [DNS security](#).
 - [Wireless Networks](#).
 - [Firewalls, Tunnels, and IDS](#).
- **Browser Security:**
 - [Web Security](#).
- **Cryptography:**
 - [Intro. to Cryptography](#).
 - [Modes of Operation](#).
- **Application Security:**
 - [Spam and Cybercrime](#).
 - [Digital Rights Management](#).

[Goodrich's Home Page](#).

Digital Rights Management

9/21/21

Digital Rights Management

1

Introduction

- Digital Rights Management (DRM) is a term used for systems that restrict the use of digital media
- DRM defends against the illegal altering, sharing, copying, printing, viewing of digital media
- Copyright owners claim DRM is needed to prevent revenue lost from illegal distribution of their copyrighted material

DRM Content and Actions

- There are many capabilities covered by DRM

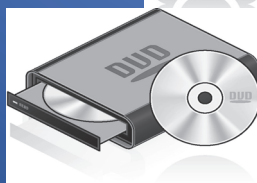
Digital Rights Management

Digital content:

- Videos
- Music
- Audio books
- Digital books
- Software
- Video games

Possible Actions and Restrictions:

- Play once
- Play k times
- Play for a set time period
- Play an unlimited amount
- Copy
- Burn to physical media
- Lend to a friend
- Sell
- Transfer to a different device



9/21/21

Digital Rights Management

3

Early U.S. Copyright History

- US Constitution, Article 1, Section 8
 - “The Congress shall have the Power ... To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries”
- Copyright Act of 1790
 - "the author and authors of any **map, chart, book** or books already printed within these United States, being a citizen or citizens thereof....shall have the sole right and liberty of printing, reprinting, publishing and vending such map, chart, book or books...."
 - Citizens could patent books, charts, or maps for a period of **14 years** – Could renew for another 14 years if you were alive
 - Non-citizens and works from other countries not protected
 - Other laws followed to change the Act slightly

Copyright Act of 1976

- Could copyright literary works, musical works, dramatic works, choreographic works, graphical works, motion pictures, and sound recordings (architectural works added in 1990)
- Copyright holders had exclusive right to reproduce, create derivative works of the original, sell, lease, or rent copies to the public, perform publicly, display publicly
- Could hold copyright for 28 years with a possible 28 year extension
- Rights of copyright holders are limited slightly by sections 107 through section 118 – Often referred to as Fair Use

Fair Use Doctrine

- Various purposes for which reproducing a particular work is considered fair use
 - Criticism, comment, news reporting, teaching, scholarship and research
- Four factors are considered when determining if it is fair use [17 U.S.C. § 106]
 1. The purpose and character of the use, including whether such use is for commercial nature or is for nonprofit educational purposes;
 2. The nature of the copyrighted work;
 3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
 4. The effect of use upon the potential market for or value of the copyrighted work

Sony vs. Universal Studios

- In the 1970s, Sony invented Betamax, a video tape recording format similar to VHS
- Could be used to record copyrighted broadcasts
- At the same time, some movie studios created DiscoVision which was a large disk that would disintegrate after a few plays
- In 1976 Universal Studios and Disney sued Sony for all the lost profits and tried to ban the use of Video Tape Recorders (VTR)
- District Court for the Central District of California rejected the claim on the basis that noncommercial use of VTRs was considered fair use
- Court of Appeals for the Ninth Circuit reversed the ruling and held Sony liable for aiding in copyright infringement

Sony vs. Universal Studios (cont.)

- In 1984, the Supreme Court had to decide on the issue – Is selling VTRs to the general public aid in copyright infringement of public broadcasts?
- The Supreme Court eventually ruled that “the sale of the VTR’s to the general public does not constitute contributory infringement of copyrights”
 - Concluded that most copyright holders who license there work for public broadcast would not mind having their broadcasts recorded on to a Betamax tape by viewers
 - Betamax was ruled that it fell under the Fair Use clause
- Case often referred to by future copyright lawsuits including the Napster case

Digital Millennium Copyright Act (DMCA)

- Signed into law by President Clinton on October 28th, 1998
 - Illegal to circumvent anti-piracy measures built into software
 - Unlawful to create, sell, or distribute devices that illegally copy software
 - Legal to crack copyright protection to conduct encryption research, assess product interoperability, and test computer security systems
 - Provides exceptions to nonprofit libraries, archives, and educational institutions in some cases
 - ISPs are not held accountable for transmitting information resulting from their customers infringements
 - Service providers are required to remove material when found
- Congress passed the law with almost no opposition
 - Congress held the impression that it was merely a technical issue and not one of impact to public policy
 - Highly lobbied by the industry

Dmitry Sklyarov and Ed Felten

- Dmitry Sklyarov
 - Worked for Elcomsoft in Russia and created product that converts Adobe secure eBook to unprotected PDF (legal in Russia)
 - While in the US, Sklyarov was arrested and placed in jail for DMCA violations
 - Eventually Elcomsoft was sued and Sklyarov was released
- Professor Edward Felten of Princeton
 - In 2000, the Secure Digital Music Initiative (SDMI) invited researchers to try and break their watermark technology
 - Felten and his team were able to remove the watermarks and wrote a paper to be presented at a conference
 - SDMI and RIAA threatened to take legal action against Felten
 - Felten withdrew from conference but talked about the threats
 - Felten with help of the Electronic Frontier Foundation sued RIAA and SDMI
 - SDMI and RIAA withdrew their threat
 - Felten eventually presented the paper at a different conference

Copy Protection Methods

- Dongle
 - Pluggable hardware device that contains a secret value required to run the software
- Product key
 - Required to be entered by installation software
 - Online check for duplicate use
 - Hardware and OS fingerprinting to bind license to machine
- Phone activation
 - Human-to-human interaction servers as deterrent

The Analog Hole

- Every copy protection mechanism is open to the risk of the “analog hole”, that is, recording the content as it is being played



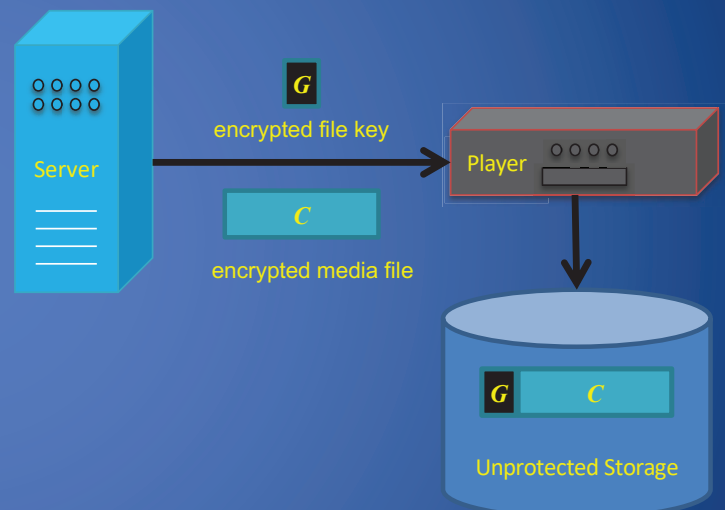
9/21/21

Digital Rights Management

12

DRM Media File Example

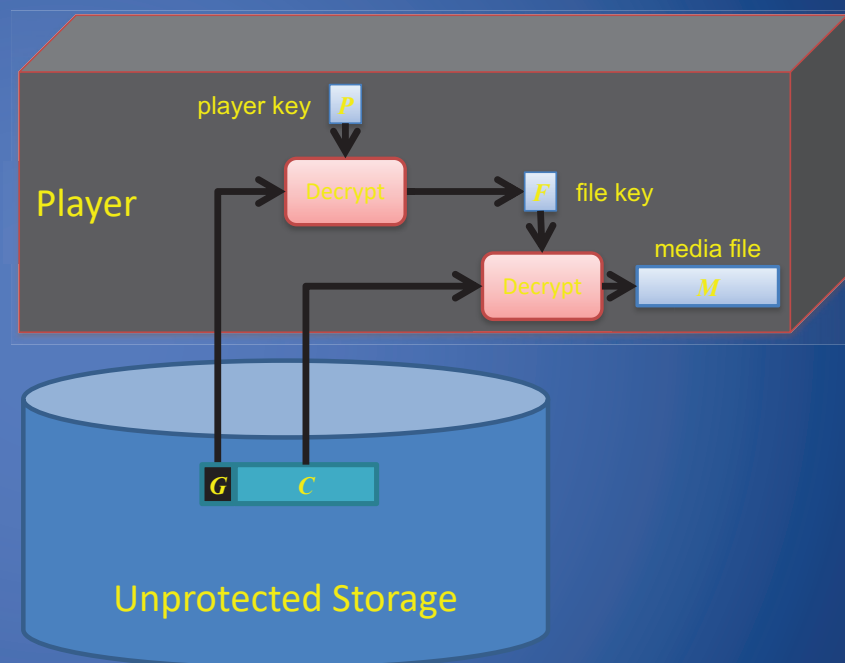
- Step 1:
 - A media server sends to the player the media file encrypted with the file key and the file key encrypted with the player key



9/21/21

DRM Media File Example

- Step 2:
 - The player first decrypts the file key using the player key and then decrypts the media file with the file key.

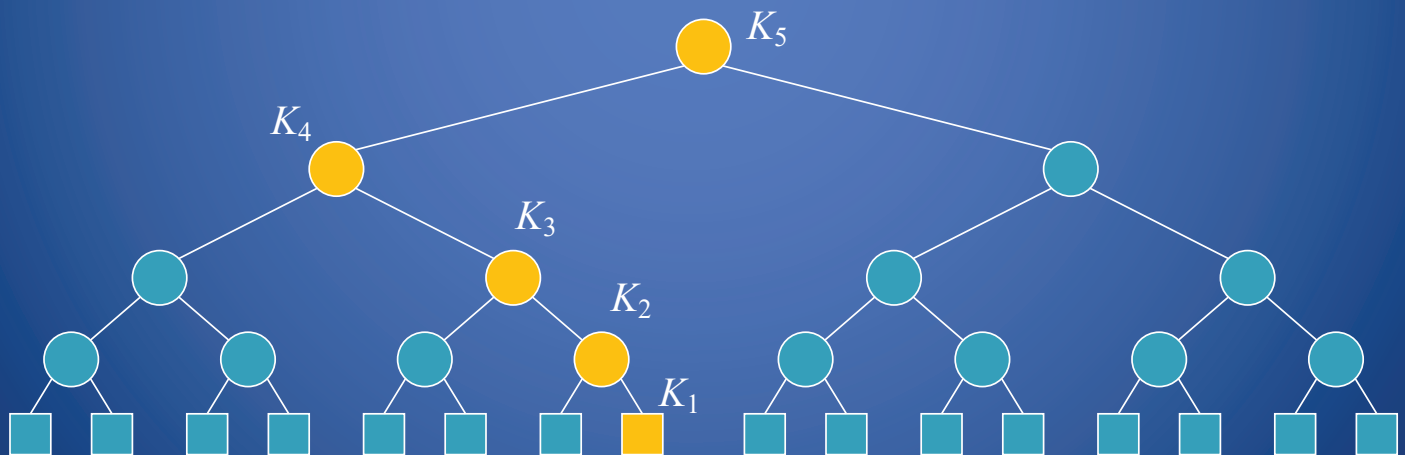


Traitors Tracing

- A controller distributes protected content to a collection of devices
- The devices share a common symmetric key with the controller
- Each content item is encrypted with the shared key and broadcast to all the devices
- Some devices (traitors) are cloned or used to illegally copy and distribute protected content
- Problems:
 - Identifying traitors
 - Revoking traitors

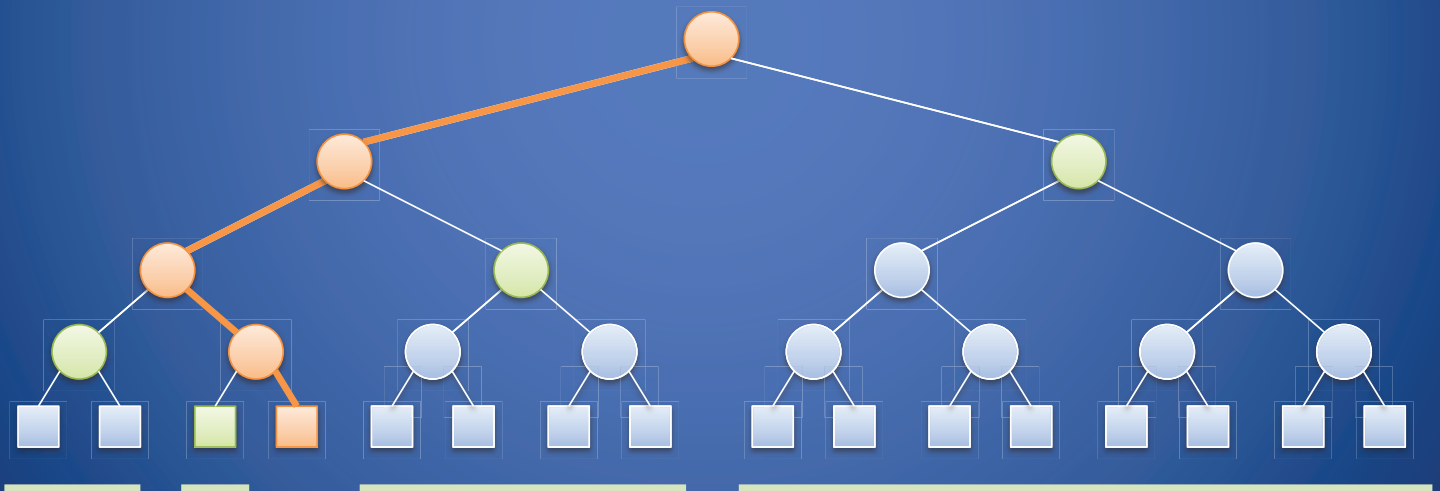
Logical Key Hierarchy

- Balanced binary tree of symmetric encryption keys
- Devices associated with leaves, each holding the keys on the path to the root
- Content encrypted with the key of a node v can be decrypted by all the devices in the subtree of v



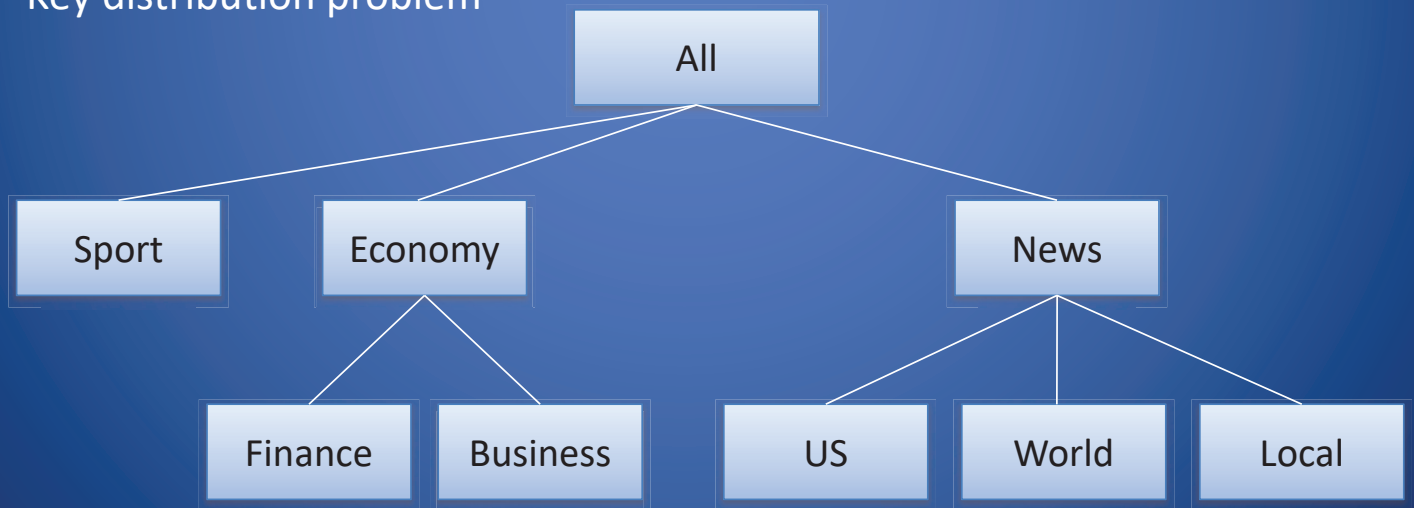
Revocation of a Device

- If a device needs to be revoked, the keys known to this device must be changed and the new keys must be distributed
- The distribution of new keys can be done with a logarithmic number of encrypted broadcast messages



Encrypted Broadcasts

- Content hierarchy with various subscription packages
- Each content item is encrypted with a single symmetric key before broadcasting
- Subscriber authorized to view item must have the key to decrypt the item
- Single key per node allows computation of keys of descendant nodes
- Key distribution problem



9/21/21

Digital Rights Management

18

CD/DVD Protection

- Most CD/DVDs are protected so they cannot be copied
- CDs are not indestructible and backups are required
- Legal to make backups of CDs you own in most countries – Not legal to sell
- Most protection technologies encrypt the files using a key that is added to the disc as a digital signature
- Almost every encryption technique has been cracked

CD/DVD Protection

- Technically, it is impossible to completely prevent users from copying media they purchase
 - Bit-by-bit copy of software
 - Recording of music using microphones
 - Recording of movies using cameras
 - Scanning of text media
- Given enough time and resources, any media can be copied
- Most companies realize they cannot stop “professionals” from duplicating but they try to stop the casual user from copying

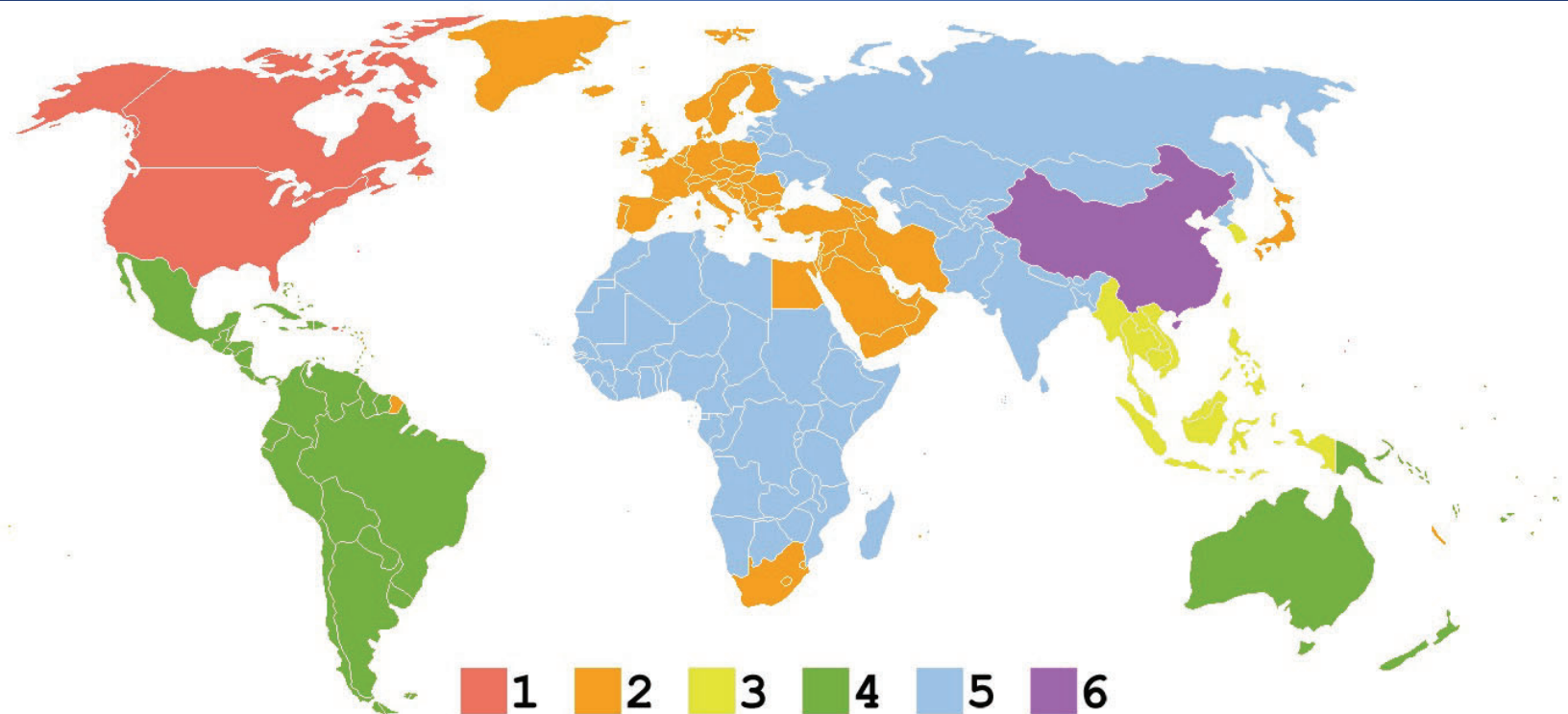
SafeDisc V1 and V2

- Copy protection created by MacroVision
- Games starting in 1999 were protected
- Based on having read errors on the original disc
 - CD burners had to be able to copy the errors exactly as is
- Version 2 Has bad sectors like version 1 but also has “weak” sectors
 - Weak sectors often become bad sectors when copying
 - Uniform bit-patterns are hard to write for many CD writers – Some people allege hardware manufacturers may have done this on purpose to aid CD copy protection
- Easy to break
 - 1:1 CD-Copy using several CD copy programs
 - SafeDisc Patches: Generic SafeDisc Patch, Daemon Tools
 - Executable UnWrappers: unSafeDisc, DumPlayerx

DVD copy protection

- Traditional recording media (e.g., audio tape, VHS tape) for audio and video are **analog** and used different **standards** NTSC, PAL, SECAM ...
- Piracy is not too big of a concern because quality degrades with each copy generation.
- With digital recording and high-resolution video, DVD copy protection was a big issue to the movie industry.
- In fact, it took about 2 years after the invention of DVD to put DVD movies on the shelf. Part of it is due to the development of a reasonable copy protection scheme.

How Studios Split our Planet



DVD Region Code Symbol

A region code byte is recorded on a disc

9/21/21

Digital Rights Management

23

DRM Architecture

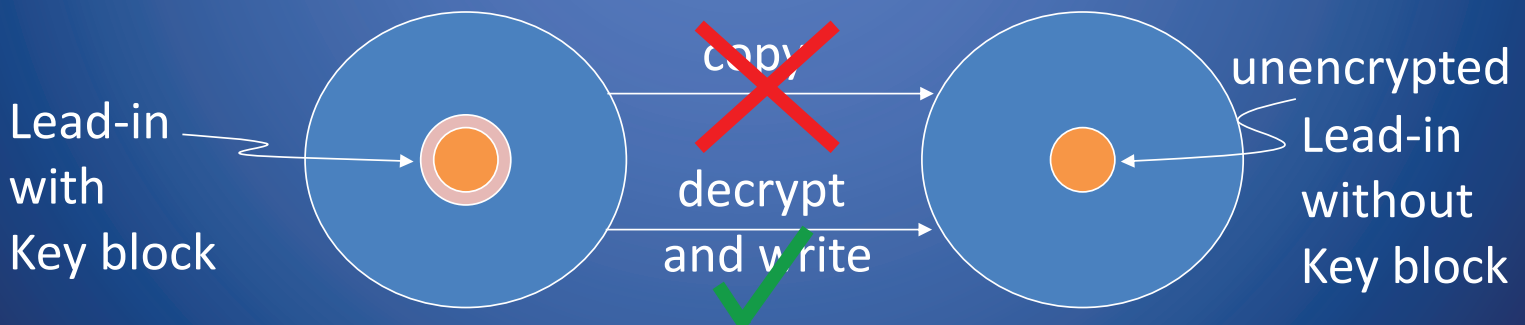
- Proposed by the Copy Protection Technical Working Group for DVD (CPTWG), IBM, Intel, Matsushita, Toshiba.
- Idea:
 - Alice sells Bob a video, in order for Alice to prevent Bob from re-disseminating the video to others, Alice tries to make sure that Bob only accesses the video data on a **trusted** (or compliant) device

Trusted Devices

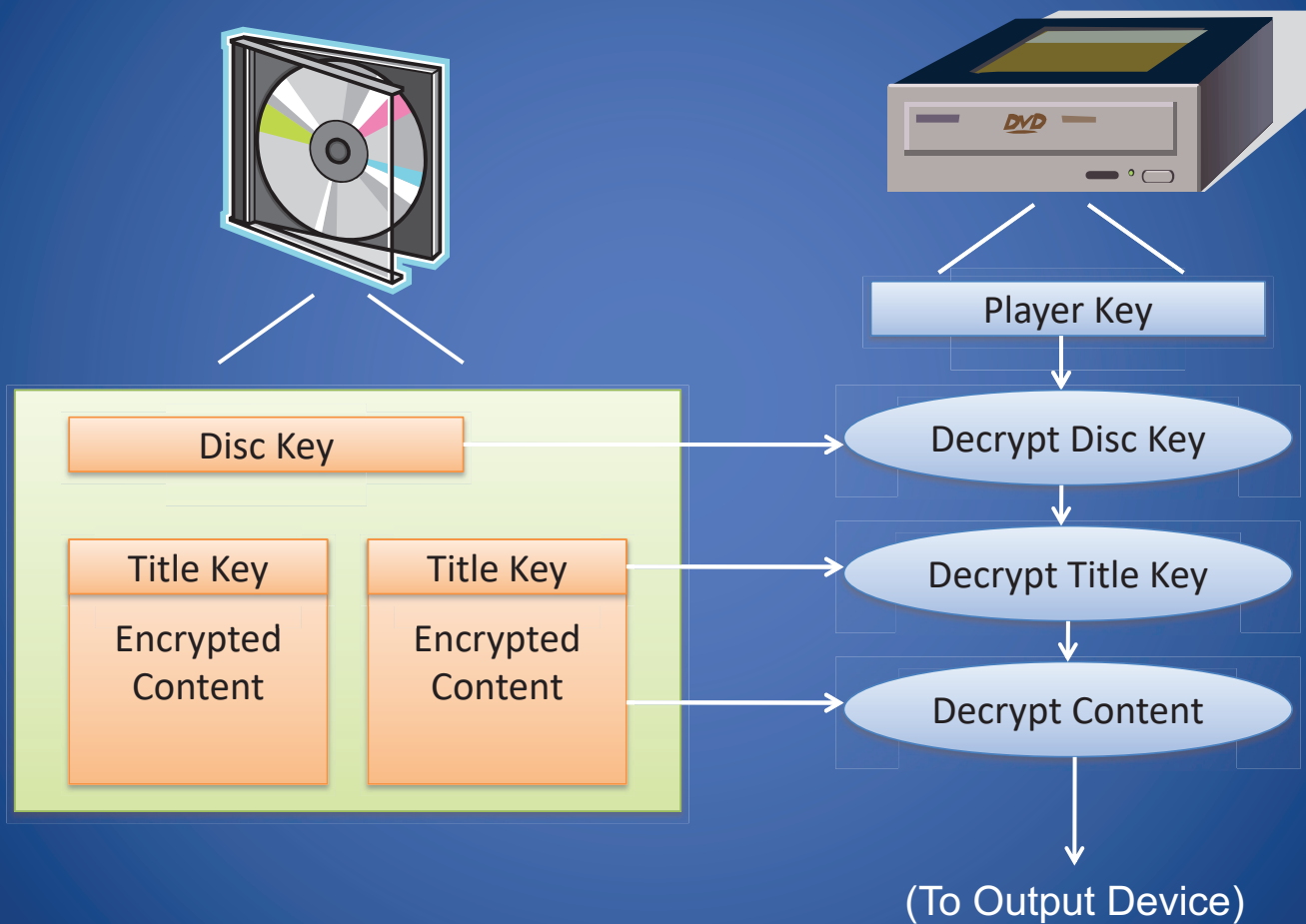
- A trusted device is manufactured by a trusted manufacturer.
- A manufacturer is trusted if it has joined the Copy Control Association (CCA)
- A trusted device is given a (secret) player key
- The trusted manufacturer has to sign an agreement with CCA, basically barring it from making devices that could undermine the copy protection mechanism.
- Since 2000, manufacturers must produce DVD ROM drivers compliant with=RPC 2 (Region Playback Control)

CSS: Content Scrambling System

- In most cases, a DVD (video disk) is protected by the CSS scheme. Intuitively, the video content is encrypted using a *disc key*, k .
- In the lead-in area of a CSS-protected DVD, the disk's key k is encrypted about 400 times, each using a different player key.
- A DVD player with the i^{th} player key will read the i^{th} entry of the key block. This entry is then decrypted using the player key k_i to obtain the disk key k .
- The video content is then decrypted on-the-fly while the movie is played.
- Using a normal DVD writer the copy will not have the key block and disk will not be playable
- if someone decrypts a video, with special tools (HW or SW), it is possible make pirated copies with the lead-in key block or without CSS (i.e., decrypted).



Viewing a DVD



CSS Keys

- Authentication Key
 - Used for mutual authentication
- Session/Bus Key
 - negotiated during authentication
 - encrypt title and disk keys before sending them over the unprotected bus
 - Prevent eavesdropping
- Player Key
 - Licensed by the “DVD Copy Control Association” to the manufacturer of a DVD player
 - Stored within the player
 - Authenticates the player
 - Used to decrypt disk key.
- Disk Key
 - Used to decrypt the title key
- Title Key
 - This key is XORed with a per-sector key to encrypt the data within a sector
- Sector Key
 - Each sector has a 128-byte plain-text header
 - Bytes 80 - 84 of each sector's header contain an additional key used to encode the data within the sector

DeCSS

- Created in 1999 by Jon Johansen
- Decrypts CSS and allows for copying files to hard drive
- At the time, little information known about CSS algorithm
- DeCSS came with the source code that showed how easy it was to crack CSS
- Technique used for creating open source DVD players that could run on Linux
- First in a long line of DVD decrypting programs
- Johansen was sued by the DVD-CCA but case was dropped
 - Mass pirating occurred far before DeCSS was published
 - DVD writers are unable to write to the region that CSS writes
 - Most DVD copies done using special equipment that copy bit by bit

Advanced Access Content System

- New standard for DRM that allows for limited sharing and copying of next generation DVDs
 - Developed by Microsoft, Sony, Disney, IBM, Matsushita, and Warner Brothers
 - Used in Blu-Ray
- Method
 - Based on broadcast encryption
 - Revocation of traitors