

DRM

Presenter: Vladimir Dzhuranyuk
Computer Security Seminar

What is the biggest lie ever?



What is the biggest lie ever?

I have read and agree to the terms of use

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

Digital Rights Management



Digital Rights Management

Digital Restrictions Management

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

What might be bad about DRM?

The image features a solid blue gradient background. In the bottom right corner, there are several white, parallel diagonal lines that create a sense of motion or a modern design element.

2 types of protecting DRM:
technical measures and legal
solutions

The background is a solid blue gradient. On the right side, there are several white diagonal lines of varying lengths and thicknesses, creating a modern, abstract design element.

Technical measures

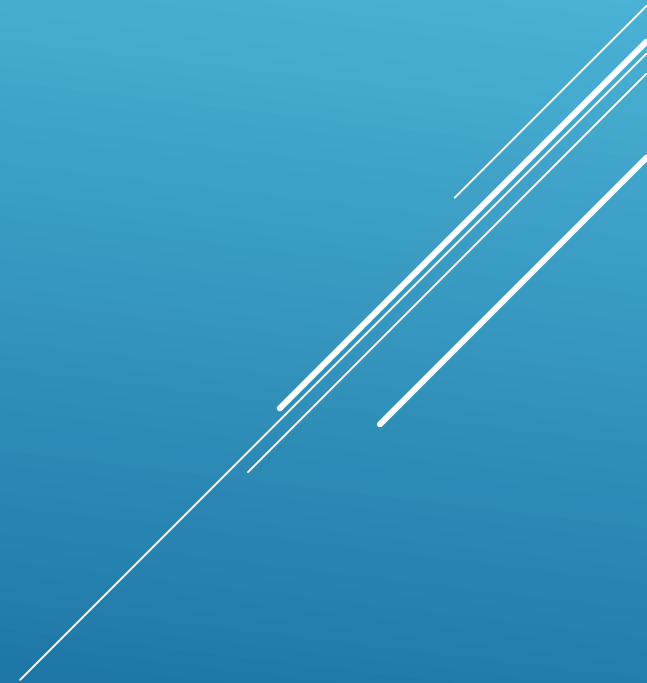


Software

Video

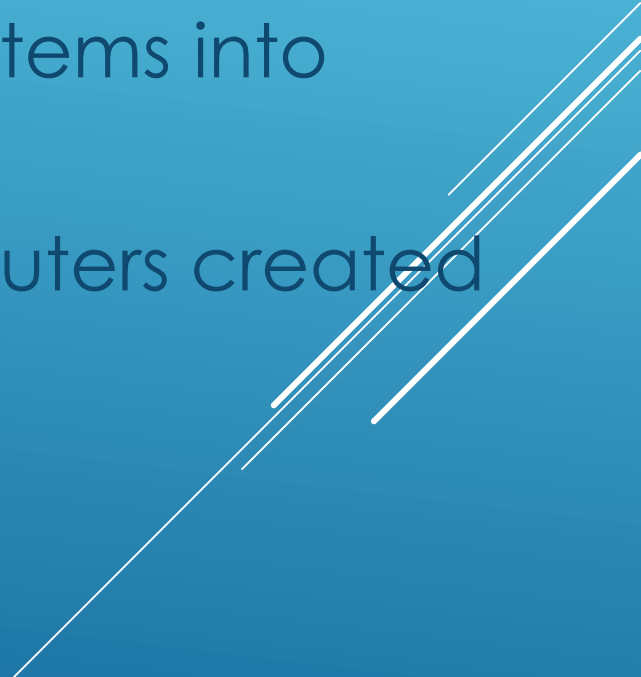
General platforms

Information hiding






SOFTWARE

- 1960's – arrival of minicomputers; software costs started to become significant.
 - By the mid-1970's some of vendors had turned systems into packages; software birthmarks
 - Late 1970's – early 80's – the arrival of microcomputers created mass market
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

3 APPROACHES AGAINST UNLICENSED COPYING

1. The standard way to add hardware uniqueness was a **dongle**
 2. A cheaper and more common strategy was for **software to install itself on the PC's hard disk** in a way that was resistant to naïve copying
 3. Average PC has **many unique identifiers**; you can use it to tie a software to a given machine
- 

SOME PSYCHOLOGICAL TECHNIQUES WHICH WERE USED BY THE VENDORS

- Embed the registered user's **name and company on the screen**
- Stories of organizations that **didn't pay** and thus **didn't get crucial updates**
- If early Microsoft software detected a debugger it would put up the message '**The tree of evil bears bitter fruit. Now trashing program disk.**'

SOFTWARE

- In the mid- to late-1980's, the market split:
- **The games market** -> hardware protection -> games console products
- **Business software vendors** -> stopped trying to protect products using predominantly technical means
- The industry then swung to legal solutions
- Eventually it became clear that **both technical and legal measures** should be used



VIDEO

DVD(Digital Video Disk, Digital Versatile Disk)

DVD was introduced in 1996

DVD has **region coding**: it divides world into regions

Vendors didn't like it

They made sure everyone knew how to turn it off in their player

VIDEO

DVD(Digital Video Disk)

CSS(Content Scrambling System)

It is based on stream cipher. There are 2 shift registers
Each successive keystream bit is obtained by adding two outputs

Each player has at least one key

Each disk has a disk key k_d

The content is protected under keys derived from k_d

VIDEO

HD-DVD and Blu-ray

2 successors to DVD

Similar in many ways

Both of them use a content encryption system called AACCS

Blu-ray adds extra mechanism called SPDC

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

VIDEO

AACS(Advanced Access Content System)

The encryption is done using AES

Basic idea: to give **each user** a number of **different keys** in such a way that **any two of them** will have some **subset of keys in common**

VIDEO

AACS(Advanced Access Content System)

Each decoder has **256 device keys**

Data on the disk tells the decoder **which keys** to use and how, for creating **Processing Key**

This mechanism is called **Media Key Block(MKB)**

The **Processing Key** protects a **Volume Unique Key(VUK)**, which protects a **title key**, which protects the content

VIDEO

AACS(Advanced Access Content System)

Idea: different **processing key** for a different **set of disks**

The goal is to be able to **revoke single devices**

When a decoder is revoked, a **new MKB** can be distributed

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

VIDEO

AACS(Advanced Access Content System)

Did it work well?

It is possible to read VUKs from the memory, which enables to decrypt the disk's content

Processing keys were extracted and published too

In theory, publishers should have used different processing keys, but many were using a single key for all disks

VIDEO

Blu-ray and SPDC

SPDC (Self-Protecting Digital Content): each player contains a virtual machine that can run content-protection code

The studios write this code and can change from one disk to the next

A decorative graphic consisting of several parallel white lines of varying lengths and orientations, located in the bottom right corner of the slide.

GENERAL PLATFORMS

Windows Media Rights Management

A store wanting to sell digital media:

- encrypts each item
- puts the encrypted files on a **media server**


To use this system, the customer must first **personalize** his media player

GENERAL PLATFORMS

Peer-to-Peer File-Sharing Systems

Became very popular

The United States Copyright Office defines peer-to-peer systems as networks where computers are linked to one another directly rather than through a central server

Three parallel white lines of varying lengths and positions, slanted diagonally from the bottom right towards the top right, serving as a decorative element.



Hiding



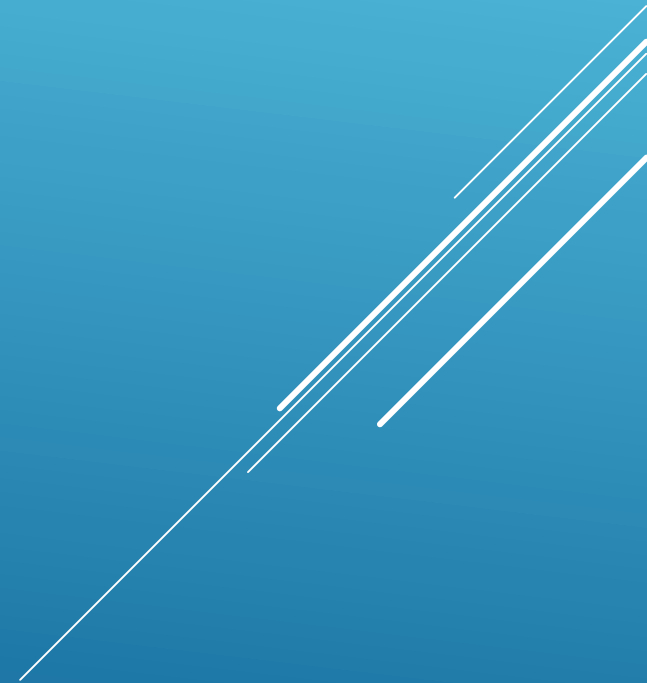
INFORMATION HIDING

Copyright Marks

There is a need in good mechanisms to hide copyright marks in media


Two general types:

- watermarks: hidden copyright messages
- fingerprints: hidden serial numbers




INFORMATION HIDING

General Information Hiding Techniques

- Hiding marks or secret message in the least significant bits of audio or video signal
 - Direct-sequence spread-spectrum technique. You have a number of secret sequences, each coding a particular symbol
- 
- A decorative graphic consisting of several parallel white lines of varying lengths and orientations, located in the bottom right corner of the slide.


INFORMATION HIDING

General Information Hiding Techniques

- Using characteristics of particular media, such as moving text lines up or down, or adding extra echoes to music below the threshold of perception
- 
- A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

INFORMATION HIDING

Attacks On Copyright Marking Schemes

- Many marks are simply additive, which might make them vulnerable
 - There have been various attempts to develop a marking equivalent of public key cryptography
- 
- A decorative graphic consisting of several parallel white lines of varying lengths and thicknesses, arranged diagonally from the bottom right towards the top right of the slide.

INFORMATION HIDING

Attacks On Copyright Marking Schemes


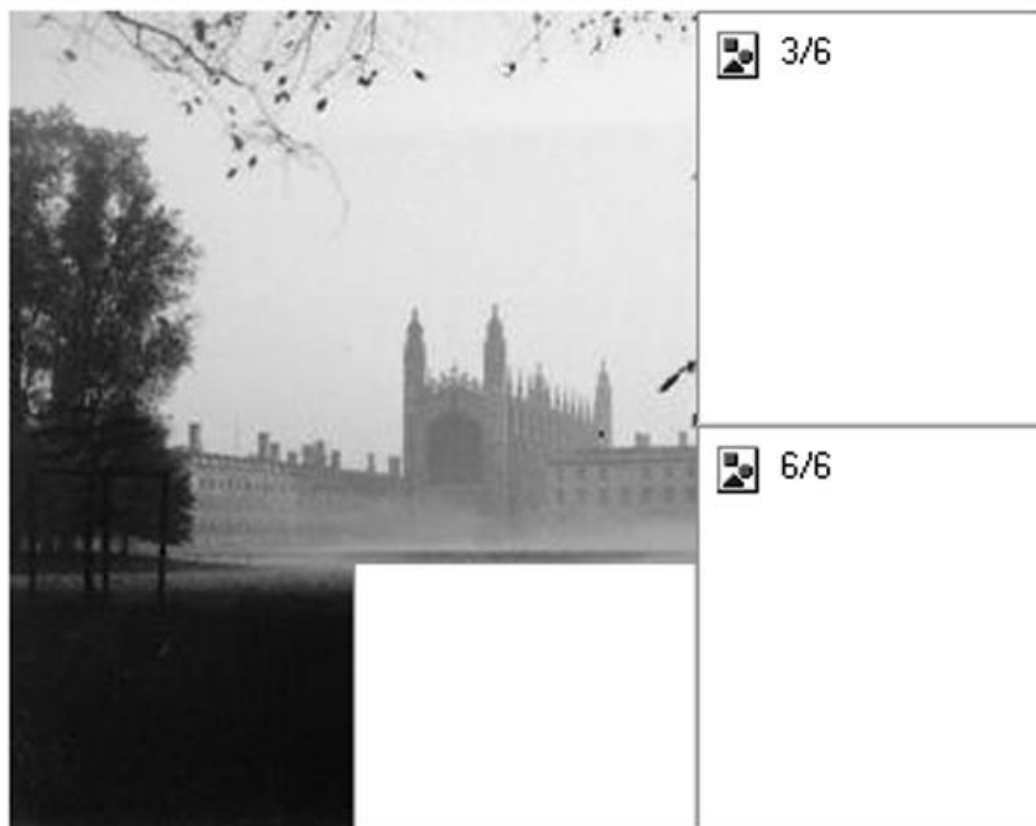
- Sometimes mark is added by increasing or decreasing the luminosity of the image
- Digimarc supplied tools to let picture owners embed invisible fingerprint

INFORMATION HIDING

Attacks On Copyright Marking Schemes

- Also Digimarc created 'Marc spider', a bot which crawled the web looking for marked pictures and reporting them

How to defeat it: typical web browser presents a series of images by displaying them one after another. A marked image can often be divided to smaller images, which together look just like an original

Address  http://www.cl.cam.ac.uk/~fapp2/watermarking/image_watermarking/2mosaic/

King's College Chapel, courtesy of John Thompson, JcpPhotographic, Cambridge. In some cases downloading the mosaic is even faster than downloading the full image! In this example we used a 350x280-pixel image watermarked using PictureMarc 1.51.

Legal solutions





DMCA

Social networks



POLICY

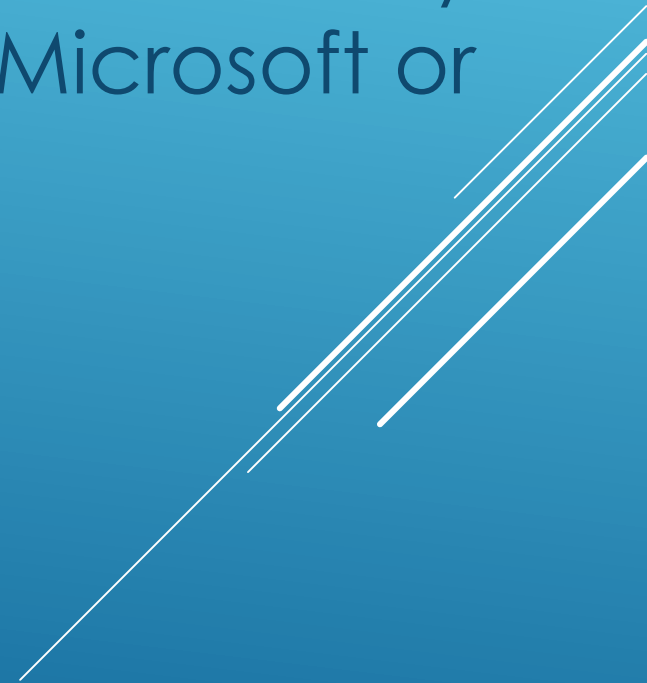
In 1998 the DMCA (Digital Millennium Copyright Act) was signed. It shifted power to the owners of 'intellectual property'



POLICY

More and more material becomes electronic and thus many controls become technical controls

As a result, copyright regulations are no longer made by lawmakers, but by programmers working for Microsoft or Apple



POLICY

Copyright law has become relevant to people who download music, movies, etc.

Privacy concerns: the move to the downloads means that DRM license servers have a record of what people watch and listen to

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, set against a blue gradient background.

POLICY

At some point the IP lobby was trying to strengthen it's rights through Brussels, by a document called IP Enforcement Directive

This would have further ratcheted up the penalties on infringers

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

POLICY


For example, the IP folks tried to compel every country in Europe to make patent infringement a crime

IP lobby have seriously overreached



POLICY

Some of the sequences of the DMCA:

- Weakening security for all computer users
 - Deterring innovation and competition
 - Threatening to displace “computer intrusion” and “anti-hacking” laws
 - Restricting personal, non-commercial use
- 
- A decorative graphic consisting of several parallel white lines of varying thicknesses, slanted diagonally from the bottom right towards the top right, set against a blue background.

POLICY

Social Networks


By default: it is prohibited to copy a work



POLICY

Social Networks

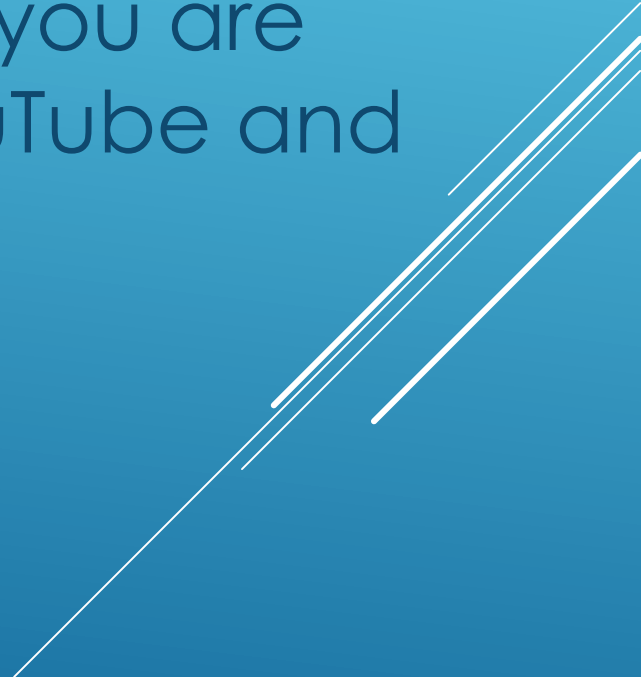
Exception 1: Facebook. From Terms of use 2(4) : When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

POLICY

Social Networks


Exception 2: YouTube. From Terms of use 7.2: You retain all of your ownership rights in your Content, but you are required to grant limited licence rights to YouTube and other users of the Service

A decorative graphic consisting of several parallel white lines of varying lengths, slanted diagonally from the bottom right towards the top right, located in the lower right quadrant of the slide.

POLICY

Who benefits?

In economic theory a technical link between two industries would usually benefit the more concentrated industry (for example, car makers). The platform industry is more concentrated than the music industry

A decorative graphic consisting of several parallel white lines of varying lengths, slanted upwards from left to right, located in the bottom right corner of the slide.

BIBLIOGRAPHY

Ross Andreson "Security Engineering"

<http://www.pc.co.il/editorial/177528/>

<http://www.pc.co.il/editorial/177641/>

<https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca>

<https://www.mishpati.co.il/article/1840>

<http://www.geektime.co.il/sdarot-website-is-down/>

<http://www.rcip.co.il/useful-info/israel-intellectual-property-laws/>