Protecting Digital Rights: Technical Approaches

CSH6 Chapter 42

Robert Guess, Jennifer Hadley,
Steven Lovaas, and
Diane E. Levine

1

Topics

- ➢Introduction
- ➢Software-Based Antipiracy Techniques
- ➢Hardware-Based Antipiracy Techniques
- ➢Digital Rights Management
- ➢Privacy-Enhancing Technologies
- ➢Political and Technical Opposition to DRM
- ➢Fundamental Problems

Introduction

- ➢The Issues
- ➢Digital Rights
- ➢Patent, Copyright, and Trademark Laws
- ➢Piracy
- ➢Privacy

3

The Issues

- ➢Continued exploitation of intellectual property
  - ❑July 2015: FBI reported 53% annual rise in theft of US trade secrets – 95% by China
  - ❑2014: US Dept Commerce est. total losses ~225B/yr in US alone; OECD est. ~$638B/yr globally
- ➢Effects of piracy
  - ❑Lost jobs, wages, tax revenue
  - ❑Potential barrier to success for startups
- ➢Privacy increasingly difficult to protect
  - ❑Rising identity theft
  - ❑Anti-piracy efforts can reduce privacy

4

Theft of Trade Secrets

Global Economic Crime Survey 2016

Adjusting the Lens on Economic Crime

Preparation brings opportunity back into focus

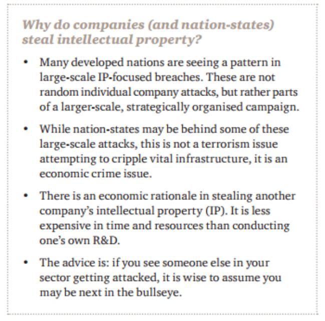
36% More than one in three organisations report being victimised by economic crime

32% Cybercrime climbs to 2nd most reported economic crime affecting organisations

44% Close to half the organisations surveyed believe that local law enforcement is not adequately resourced to investigate economic crime, leaving the responsibility for fighting economic crime on organisations

pwc

www.pwc.com/crimesurvey



Why do companies (and nation-states) steal intellectual property?

- Many developed nations are seeing a pattern in large-scale IP-focused breaches. These are not random individual company attacks, but rather parts of a larger-scale, strategically organised campaign.
- While nation-states may be behind some of these large-scale attacks, this is not a terrorism issue attempting to cripple vital infrastructure, it is an economic crime issue.
- There is an economic rationale in stealing another company's intellectual property (IP). It is less expensive in time and resources than conducting one's own R&D.
- The advice is: if you see someone else in your sector getting attacked, it is wise to assume you may be next in the bullseye.

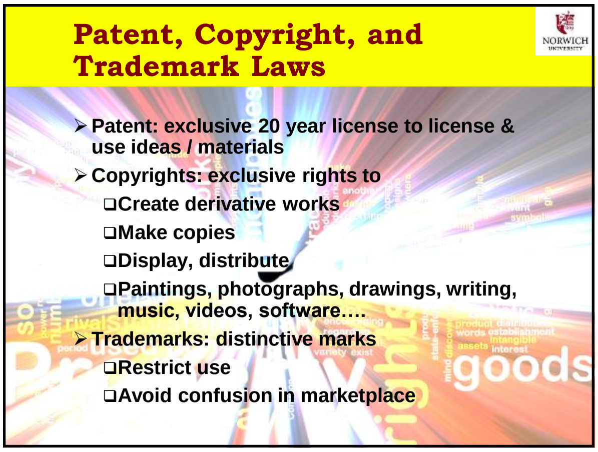
https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

5

Digital Rights

- ➢Ambiguous term
- ➢Producers mean intellectual-property rights
- ➢Privacy advocates mean personal privacy rights when using online services

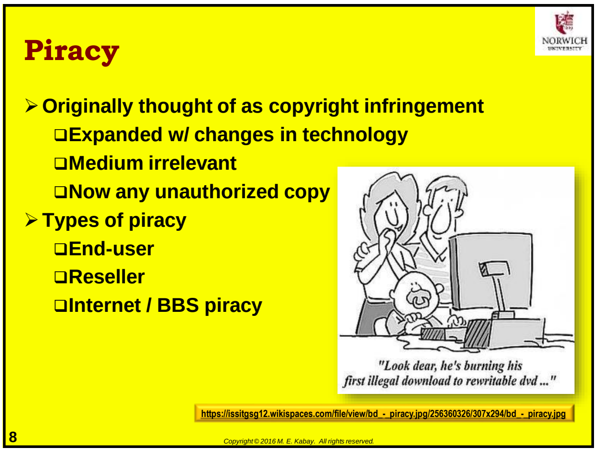
6



Patent, Copyright, and Trademark Laws

- **Patent: exclusive 20 year license to license & use ideas / materials**
- **Copyrights: exclusive rights to**
  - ❑ **Create derivative works**
  - ❑ **Make copies**
  - ❑ **Display, distribute**
  - ❑ **Paintings, photographs, drawings, writing, music, videos, software….**
- **Trademarks: distinctive marks**
  - ❑ **Restrict use**
  - ❑ **Avoid confusion in marketplace**

NORWICH UNIVERSITY
goods
rights



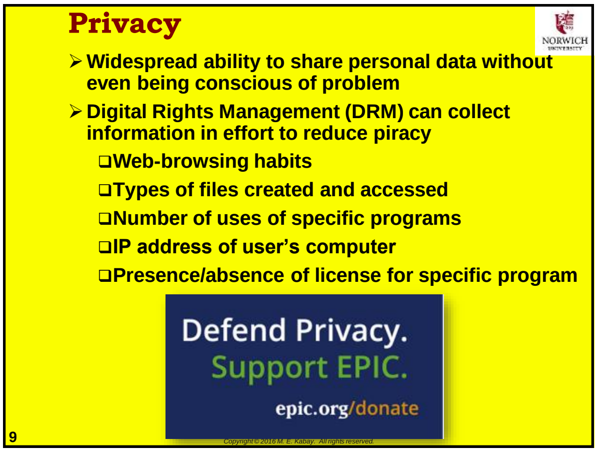
Piracy

- **Originally thought of as copyright infringement**
  - ❑ **Expanded w/ changes in technology**
  - ❑ **Medium irrelevant**
  - ❑ **Now any unauthorized copy**
- **Types of piracy**
  - ❑ **End-user**
  - ❑ **Reseller**
  - ❑ **Internet / BBS piracy**

"Look dear, he's burning his first illegal download to rewritable dvd ..."

https://issitgsg12.wikispaces.com/file/view/bd_-_piracy.jpg/256360326/307x294/bd_-_piracy.jpg

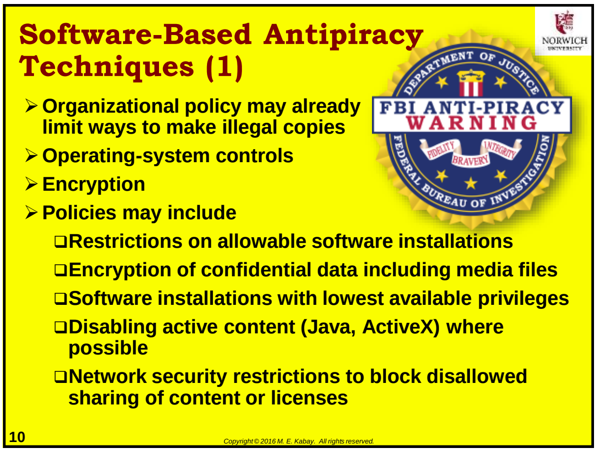
NORWICH UNIVERSITY



Privacy

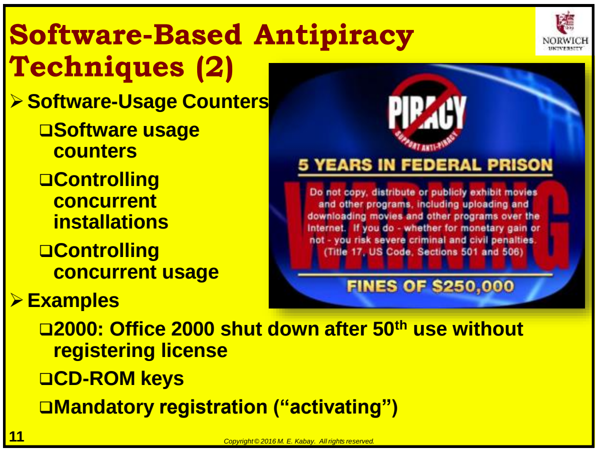
- **Widespread ability to share personal data without even being conscious of problem**
- **Digital Rights Management (DRM) can collect information in effort to reduce piracy**
  - ❑ **Web-browsing habits**
  - ❑ **Types of files created and accessed**
  - ❑ **Number of uses of specific programs**
  - ❑ **IP address of user's computer**
  - ❑ **Presence/absence of license for specific program**

Defend Privacy.
Support EPIC.
epic.org/donate



Software-Based Antipiracy Techniques (1)

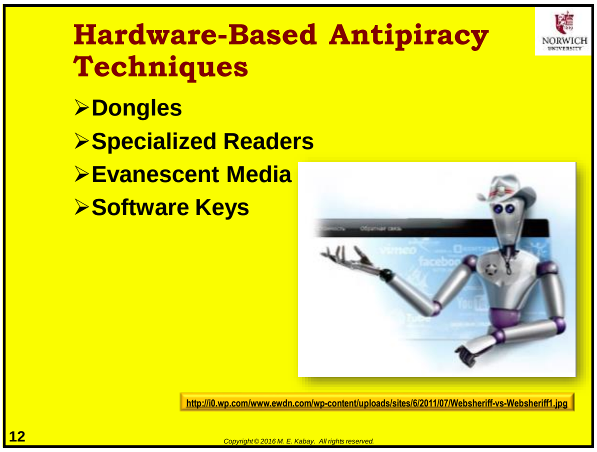
- **Organizational policy may already limit ways to make illegal copies**
- **Operating-system controls**
- **Encryption**
- **Policies may include**
  - ❑ **Restrictions on allowable software installations**
  - ❑ **Encryption of confidential data including media files**
  - ❑ **Software installations with lowest available privileges**
  - ❑ **Disabling active content (Java, ActiveX) where possible**
  - ❑ **Network security restrictions to block disallowed sharing of content or licenses**



Software-Based Antipiracy Techniques (2)

- **Software-Usage Counters**
  - ❑ **Software usage counters**
  - ❑ **Controlling concurrent installations**
  - ❑ **Controlling concurrent usage**
- **Examples**
  - ❑ **2000: Office 2000 shut down after 50th use without registering license**
  - ❑ **CD-ROM keys**
  - ❑ **Mandatory registration ("activating")**

Do not copy, distribute or publicly exhibit movies and other programs, including uploading and downloading movies and other programs over the Internet. If you do - whether for monetary gain or not - you risk severe criminal and civil penalties. (Title 17, US Code, Sections 501 and 506)



Hardware-Based Antipiracy Techniques

- **Dongles**
- **Specialized Readers**
- **Evanescent Media**
- **Software Keys**

http://i0.wp.com/www.ewdn.com/wp-content/uploads/sites/6/2011/07/Websheriff-vs-Websheriff1.jpg

NORWICH UNIVERSITY

Dongles (1)

- Hardware like USB flash drive
  - ❑Communicates with operating system
  - ❑Can provide authentic hashed identification
- History
  - ❑Originally used for printing – needed dongle to allow output
  - ❑Now can product all kinds of devices including recording (CD, DVD etc)

13

Dongles (2)

- Pro
  - ❑Easy to use
  - ❑Can require registration
  - ❑Can support encryption – need key
- Con
  - ❑Consumers hate having to use them
  - ❑Can be lost / stolen / fail
  - ❑May not be compatible with system
  - ❑Delays in replacement not good for high-availability uses
  - ❑Ending support for dongle can ruin software usability
  - ❑Encryption restricted in some countries

14

Specialized Readers

- Manufacturers tried to restrict copying by limiting distribution of hardware
- But current technology for copying data near-universal
- Audio theft widespread problem
- Video easily copied, uploaded & downloaded
- TV shows being stored and shared
  - ❑HDTV uses encryption
  - ❑Descramblers readily available
- Consumers resisting specialized readers
  - ❑But accessible & inexpensive legal sources will help (e.g., iTunes, Spotify, Amazon Music)

15

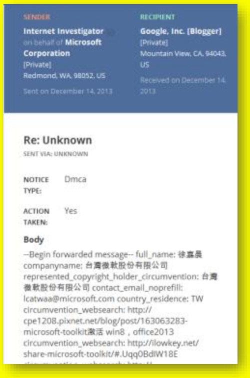
Evanescent Media

- Attempts to make data *evanescent*
  - ❑Not lasting long
  - ❑Disappearing soon
- E.g., Snapchat®
  - ❑"Snaps" can be viewed for 10 seconds or less
  - ❑But can be kept
    - ✓Screenshot
    - ✓External camera

16

Software Keys (1)

- String to unlock / activate software or equipment
- Malfunctions can cause trouble
- Some Websites provide cracked keys
  - ❑IP owners send DMCA Takedown notices



SENDER
Internet Investigator
on behalf of Microsoft Corporation
[Private]
Redmond, WA, 98052, US
Sent on December 14, 2013

RECIPIENT
Google, Inc. [Blogger]
[Private]
Mountain View, CA, 94043, US
Received on December 14, 2013

Re: Unknown
SENT VIA: UNKNOWN

NOTICE TYPE: Dmca

ACTION TAKEN: Yes

Body

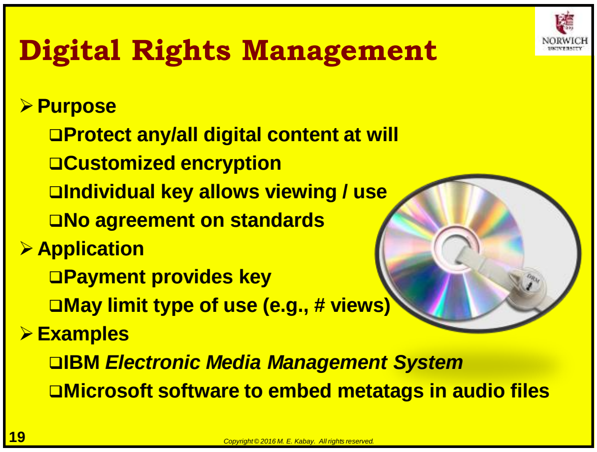
--Begin forwarded message-- full_name: 徐嘉晨 companyname: 台灣微軟股份有限公司 represented_copyright_holder_circumvention: 台灣微軟股份有限公司 contact_email_noprefill: lcatwaa@microsoft.com country_residence: TW circumvention_websearch: http://cpe1208.pixnet.net/blog/post/163063283-microsoft-toolkit激活 win8，office2013 circumvention_websearch: http://ilowkey.net/share-microsoft-toolkit/#.Uqq0BdlW18E

17

Software Keys (2)

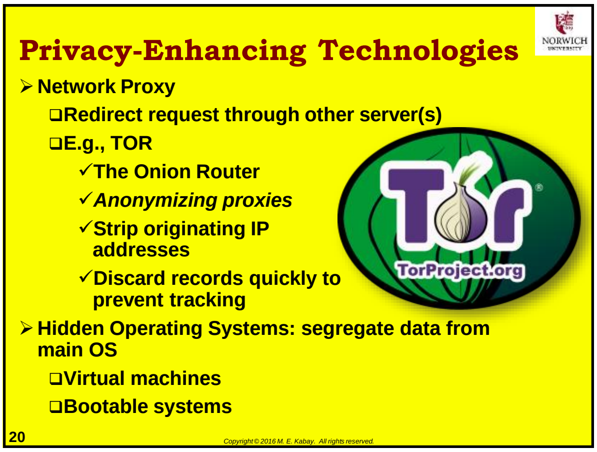
- Videocassettes vs copy machines
  - ❑Embedded codes interpreted by copying equipment to block copying
- DVD area encoding
  - ❑Region codes read by players
  - ❑Can switch to different region only once
- Watermarks
  - ❑Steganographic insertion of codes into data
  - ❑Identify origins / ownership
  - ❑Allow identifying illegal copies
  - ❑Issues of false positives / false negatives

18



Digital Rights Management

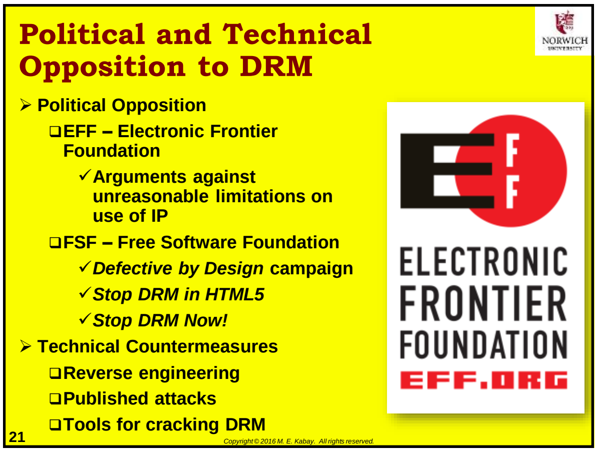
- Purpose
  - Protect any/all digital content at will
  - Customized encryption
  - Individual key allows viewing / use
  - No agreement on standards
- Application
  - Payment provides key
  - May limit type of use (e.g., # views)
- Examples
  - IBM *Electronic Media Management System*
  - Microsoft software to embed metatags in audio files



Privacy-Enhancing Technologies

- Network Proxy
  - Redirect request through other server(s)
  - E.g., TOR
    - The Onion Router
    - *Anonymizing proxies*
    - Strip originating IP addresses
    - Discard records quickly to prevent tracking
- Hidden Operating Systems: segregate data from main OS
  - Virtual machines
  - Bootable systems

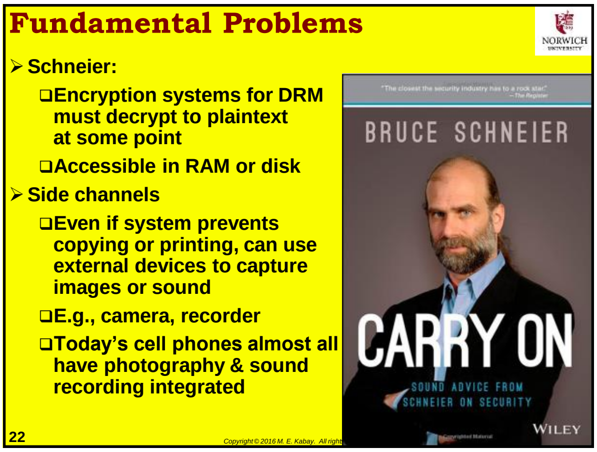
TorProject.org



Political and Technical Opposition to DRM

- Political Opposition
  - EFF – Electronic Frontier Foundation
    - Arguments against unreasonable limitations on use of IP
  - FSF – Free Software Foundation
    - *Defective by Design* campaign
    - *Stop DRM in HTML5*
    - *Stop DRM Now!*
- Technical Countermeasures
  - Reverse engineering
  - Published attacks
  - Tools for cracking DRM

ELECTRONIC FRONTIER FOUNDATION
EFF.ORG



Fundamental Problems

- Schneier:
  - Encryption systems for DRM must decrypt to plaintext at some point
  - Accessible in RAM or disk
- Side channels
  - Even if system prevents copying or printing, can use external devices to capture images or sound
  - E.g., camera, recorder
  - Today’s cell phones almost all have photography & sound recording integrated

"The closest the security industry has to a rock star." —The Register
BRUCE SCHNEIER
CARRY ON
SOUND ADVICE FROM SCHNEIER ON SECURITY
WILEY

Now go and study