FSEM 1111 Computer Security – from a Free Software Perspective

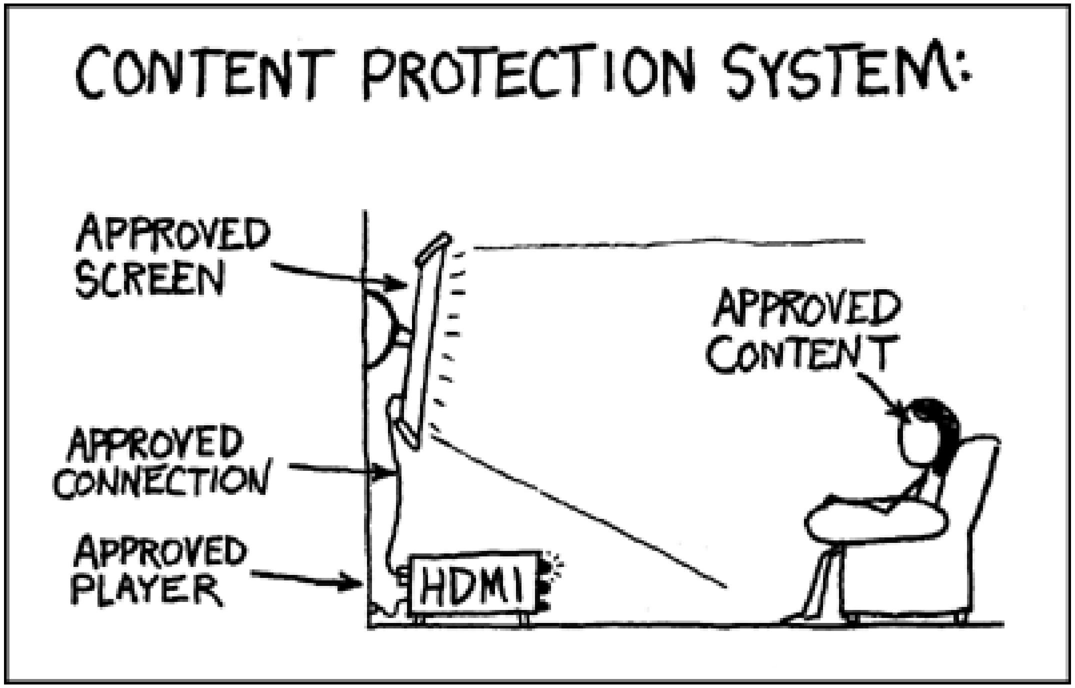
Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Digital Rights Management (DRM)

- Infrastructure to support "secure" promotion, sale and delivery of digital content
- "secure" means that restrictions on use are imposed on customers or the general public
- Stallman suggests to use the term "Digial Restrictions Management" instead

DRM illustrated[1]



[1] Thanks to xkcd.org

Essential Features

- Encryption – not just anyone can access the work
- Authentication – verify user or device is approved
- Secure Execution Environment – control content after decryption

Encryption

- Well understood
- Increases hardware costs slightly (similar to cost of decompression)
- Key distribution / management is incredibly hard
- Keys usually encapsulated in trusted devices

Authorization

- Trusted device containing keys only reveils keys after authorization

- Authorization primarily involves the player

- Authorization could also validate the content

⇒ Player software must be non-free

- Users can be authorized using Internet-based services (centralized accounting) or biometrics

Secure Execution Environment

- Ideally closed hardware running trusted software
- For PCs, embedded into trusted (non-free) operating system
- Execution environment operates in untrusted context (end-users!)

⇒ Every "secure" execution environment that has been widely deployed has been cracked!

How to “crack” SEEs?

- Emulate the hardware in software (qemu, xen, vmware) and use the emulator to inspect the execution, capture keys

- Take the hardware apart – drill deep enough to retrieve the keys directly from the hardware

- Key problem: in the end, the device must decode the content, at that point, crackers will have access

⇒ SEE’s raise costs for end-users who are not infringing on rights without seriously limiting actual infringement

Uses for DRM

- Prevent modification (for Forensics) – validate work has not been tampered with (sign work)
- Prevent unauthorized viewing (encrypt work)
- Prevent unauthorized reproduction (label work as non-copyable)
- Prevent unauthorized access (authenticate end-user)

Sample Restrictions

- Limit number of views
- Limit creation of copies
- Restrict viewing to particular time interval

DMCA

- DMCA prohibits technology that breaks “copyright protection mechanisms”
- Effective mechanisms need no such protection – that’s the definition of effective
- Ineffective mechanisms are presumably not protected
- In practice, “sophisticated” mechanisms are deemed protected

DMCA Consequences

- You can copy music from CD legally to disk
- You can copy video from VHS legally to disk
- You cannot copy music or video from an encrypted DVD legally to disk

DMCA and First-sale

- The DMCA makes it illegal to obtain devices that break copyright enforcement technology

- First-sale doctrine transfer of legitimately owned electronic works may require such technology

⇒ You have the right to transfer ownership of legitimately obtained copyrighted material

⇒ You do not have the right to obtain the technology required to do so!

Sony's Rootkit

- Rootkits are tools used by crackers to hide their activities inside of the OS
- Using rootkits (outside of research) is generally considered malicious and illegal
- Sony deployed a rootkit as part of their copyright protection program
- Does that mean that anti-virus/intrusion detection software is now illegal by DMCA?

Questions

?

Assignment 5

- This is a group project – start forming groups!
- The presentation must be done in LaTeX

⇒ FoliTeX

Slides with LaTeX

- LaTeX package for typesetting slides
- Anything LaTeX can do – for slides
- PPower4 can be used to add background colors and special effects
- `foils` itself is often sufficient
- Do not over-do effects!

Prerequisites

It is necessary to have

- java and PPower4 (available in the lab)
- pause.sty, background.sty, and pp4slide.sty

The commands needed to process example.tex are

```
pdflatex example
ppower4 example.pdf
xpdf example.pdf
```

Simple Slides

Ordinary LaTeX commands can be used to create slides. Each slide must begin with the command `\foilhead{`*foiltitle*`}` where `foiltitle` may be void. The following commands define a

```
\foilhead{simple slide.}
\begin{itemize}
 \item Ordinary \LaTeX commands
 \item {\bf  very} easy
\end{itemize}
```

PPower4 Extensions: Pauses

Placing the command `\pause` at appropriate places in a slide partitions the slide into "chunks" with increasing pauselevels.

For each subsequent page of the PDF document, chunks with one higher pauselevel are displayed or highlighted.

```
\foilhead{simple slide.}
\begin{itemize}
\item First only show this \pause
\item And then the second part
\end{itemize}
```

Headers and Footers

Headers and footers can be placed on each of the four corners of the slide. To place a logo on the bottom left of each page, with a small number on the bottom right of each page, enter the following in the preamble:

```
\MyLogo{\pauselevel{=1 +1}
        \includegraphics[scale=0.5]{logo.png}}
```

The \pauselevel is required with PPower4.

Grading Criteria

30% Demonstrated understanding of the material (be it technology, law and philosophical view points, including use of `subversion`)

20% Quality of the argumentation in terms of reasoning, structure and ambition

30% Typesetting quality (of the slides!)

20% Presentation style

Presentation Requirements

Presentations are due 11/08/2007

You can give your presentation as early as 10/30/2007

No more than 20 slides

No more than 15 minutes

Presentation Content

Present the legal case from:

- The point of view of the law
- The point of view of the general public
- The point of view of companies

Questions

?