# Session 4: DRM
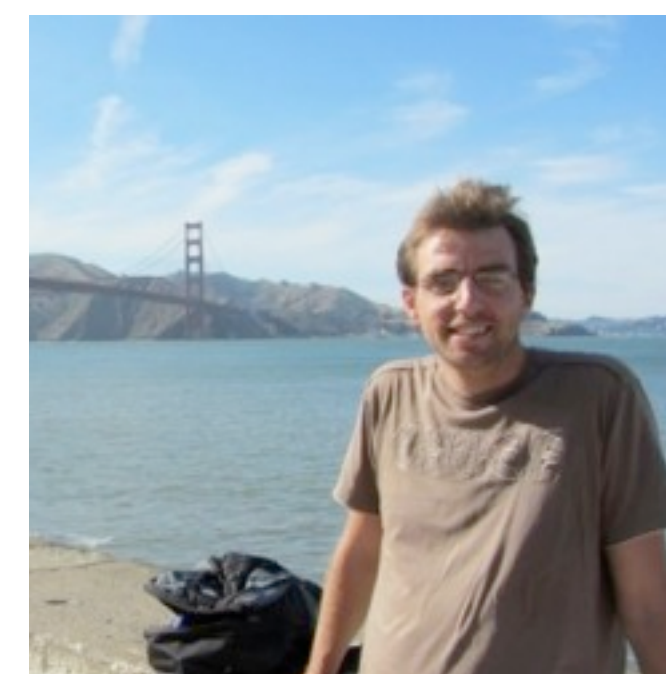
**Moderator:
Jim Dovey
Kobo**

**Minhyung Ko
Samsung**

**Gerardo Capiel
Benetech**

**Oliver Brooks
Valobox**

I'll talk about general tech
Minhyung will discuss performance issues
Gerardo will discuss watermarking— Social DRM
Oliver will discuss using DRM to identify purchases across discrete stores

**"DRM is not a selling point. There's no one who's ever bought a book because it had DRM."**

—Cory Doctorow

Don't forget: any DRM must fade into the background. Think minimal, or you'll lose out to someone else who does.

# Digital Rights Management

- Ideological wars
- RMS' "Digital Restrictions Management"
- Hackers & Crackers
- Insert your preferred [trollface.gif] here

Let's avoid all that…

Please no flame-wars. I would like us all to exit this workshop without anyone being bludgeoned by our hosts…

# Why *are* we here?

# *Not* to define some new DRM scheme

No, really. We're not forming a working group here.

# Discussing DRM's merits & failures?

Really?

# ~~Discussing DRM's merits & failures?~~

No. We're not Slashdot or Reddit either.

# Anyone can write a DRM scheme

W3C & IDPF are perfectly capable of doing this on their own, as is anyone. Let's face it— in the eBook Distribution business, we all have already.

# Underlying Technology

Let's instead look at what the tech underneath requires

# *Enabling* end-user features

Again, because it's important: if you get in users' way, they'll go elsewhere (or nowhere!). Focus on giving them things; Oliver can talk to this.

# Four Components

- User Authentication
- Device (Reading System) Authentication
- Content Authentication
- Action Authorization

# Two Components

- Authentication
- Authorization

These boil down to two concepts

# Authentication

- Guaranteed identity
  - Absolute requirement for any rights management
- Identifying a user — are they a purchaser?
  - The Prime Aim: guaranteed compensation
  - Secondary Aim: identifying Bad Actors
    - Watermarking— Benetech
- Identifying a Reading System or Device
  - Only to lock down actions of a particular purchaser

Authentication may involve user interaction. Remember the prime aim.

# Authentication

- Identifying content
  - Digital signatures
    - X.509 Certificates for signer's identity
  - Watermarking

Identifying content is simpler: we can prove it's been unchanged, and we can use X.509 to ensure the signer isn't some script kiddy.

# Authorization

- Action-by-action
  - "Read content" is an authorized action
  - "Excerpt", "Share", etc.
  - "Re-download" is an important one
    - Valobox
  - "Loan to a friend" anyone?

We authorize individual actions. There are lots of these. In the interest of not driving away your audience, a small number is recommended. Do NOT try to recreate the cumbersome nature of dead–tree books...

# Authorization

- Libraries
  - Loan out content
  - Specific time-frames
  - Differing authentication requirements?
    - Library-approved devices
    - Library account authentication

Should **never** need a different SKU/ISBN/ePub

Libraries have differing needs— but they shouldn't need special copies of books to work with. Publishers make one copy, and any DRM system needs to anticipate that a library may need to make alterations to authentication/authorization rules.

# Denying Authorization

- Encrypt your content
- Decrypt only upon authentication/authorization.

We'll see a technical suggestion for this later

# Identities

- Four things to identify:
  - The consumer i.e. the person reading now
  - The purchaser
  - The reading system
  - The content

# Watermarking

- Four things to identify:
  - ~~The consumer i.e. the person reading now~~
  - The purchaser
  - ~~The reading system~~
  - The content

Watermarking primarily wants to identify a purchaser, to 'name and shame'. Content identity is optionally required to detect tampering.

# Lightweight Content Protection

- Four things to identify:
  - The consumer i.e. the person reading now
  - The purchaser
  - ~~The reading system~~
  - The content

LCP adds the ability to ensure at read-time that content has been purchased; a reader might enter a password or similar. This may identify the purchaser only (assuming the purchaser isn't going to tell everyone their password), or a lendee. Content signatures again help prevent tampering.

# Strong DRM

- Four things to identify:
  - The consumer i.e. the person reading now
  - The purchaser
  - The reading system
  - The content

Strong DRM uses it all, and may even require an active internet connection to do all the validation in a remote location, or to allow remote revocation outside the realm of X.509 CRLs.

# Technology

- W3C has some components:
  - XML-ENC for encryption
  - XML-DSig for signing
- Private entities have some:
  - Adobe, Benetech
- IDPF has... thoughts
  - An interoperable Lightweight Content Protection standard.

IDPF LCP is a new initiative, not yet formalized, but which informs much of this presentation (and is the sole reason your humble moderator is here today…)

# W3C: XML-ENC & XML-DSig

- Benefits:
  - Widely available
  - Already implemented (libxml/libxmlsec, Java)
- Detriments:
  - Complex implementations
  - Many many algorithms
- Possibilities:
  - Limit the scope of each W3C standard in this use case.

23

IDPF can publish a 'lite' version which only defines use of a couple of algorithms.

# Everyone Else

- Those of us who make reading systems can:
  - Define authentication mechanisms
  - Define rights definition vocabularies

We all have these things internally already. There are some things already happening around the W3C in this regard too, e.g. ODRL.

# BUT:

- Don't forget that many eReaders are:
  - Low power
  - Low cost
- …and therefore low-performance
- Minimizing the technical effort required for DRM is a *must-have*

Minhyung Ko has something to say about all this.

# Beyond DRM

- Identity functions are widely applicable:
  - OCX file can use device identity to point to capability-based manifestations (individual OPF files)
  - JavaScript APIs & CSS '@-word-thingies' to provide access to identity/capability information inside content.
- Authentication too:
  - Authorization to purchase/download read-along info from within a book?

# **Remember:** Think of the *reader*. If they're not sold, neither are your products…