Watermarking and Traitor Tracing

Captain Bastien and
Quartermaster Théo

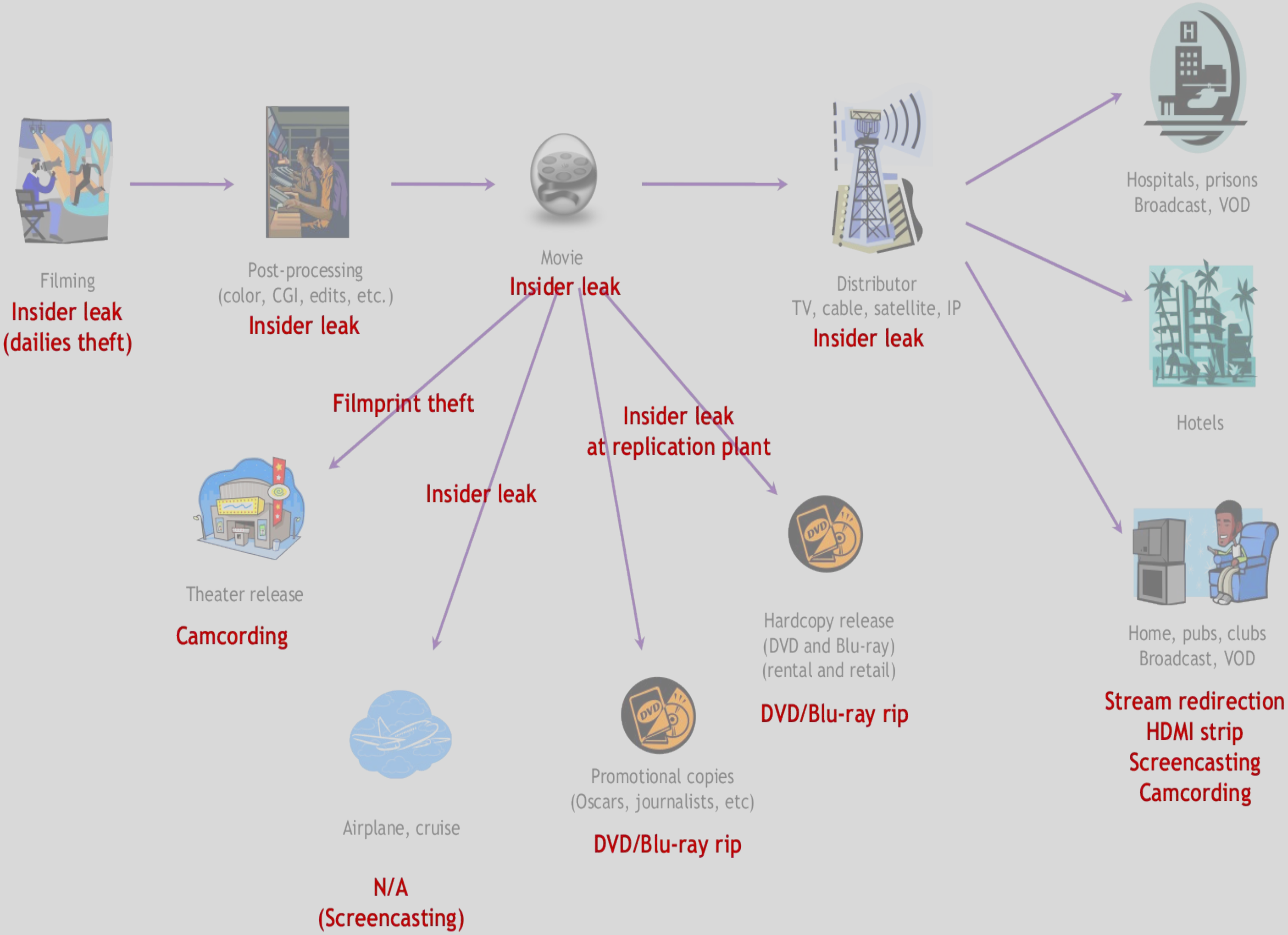
DRMs?

Consumer frustration

Intrusive

Easy to bypass

Mixed effects



Filming

Insider leak
(dailies theft)

Post-processing
(color, CGI, edits, etc.)

Insider leak

Movie

Insider leak

Distributor
TV, cable, satellite, IP

Insider leak

Hospitals, prisons
Broadcast, VOD

Hotels

Filmprint theft

Insider leak

Insider leak
at replication plant

Theater release

Camcording

Hardcopy release
(DVD and Blu-ray)
(rental and retail)

DVD/Blu-ray rip

Home, pubs, clubs
Broadcast, VOD

Stream redirection
HDMI strip
Screencasting
Camcording

Promotional copies
(Oscars, journalists, etc)

DVD/Blu-ray rip

Airplane, cruise

N/A
(Screencasting)

Threat Analysis in the multimedia business

Complementary strategies

- Interoperability across DRM platforms
  - Content can flow freely regardless of the underlying DRM technology

- Discreet protection technologies
  - Content fingerprinting and traitor tracing
  - They **don't** prevent piracy
  - Permit enforcement of a damage control policy

Content fingerprinting

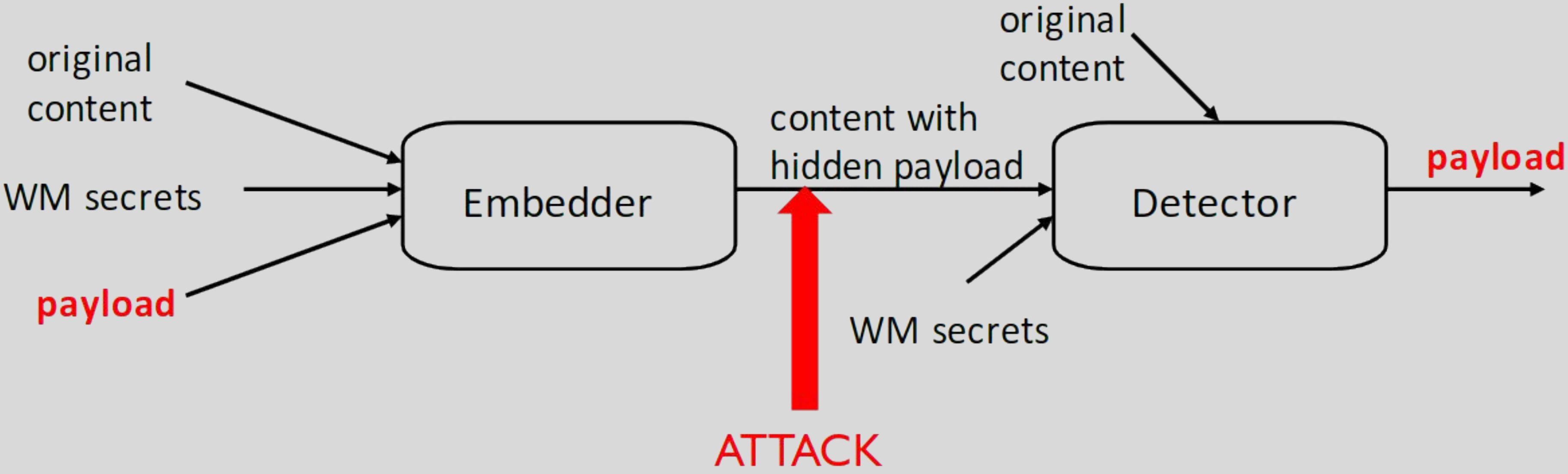
- **Content fingerprinting** efficiently **locates copyrighted material** that has been illegally published on the Internet
- But they don’t show **who** put the content

Traitor Tracing (a.k.a forensic watermarking)

- Aims to **pinpoint the origin of a leak** in a distribution framework

- **Incidence response** mechanism
- Can be view as a **dissuasive weapon**

- **Active forensic technique**
    - Prepares and **manipulates** the keys or content **upfront** to enable tracing



The payload is a secret code identifying the user/device

A real world example would be the **IBM’s sequence-key** which is part of the Advanced Access Content System (**AACS**), the **Blu-ray disc protection standard**.

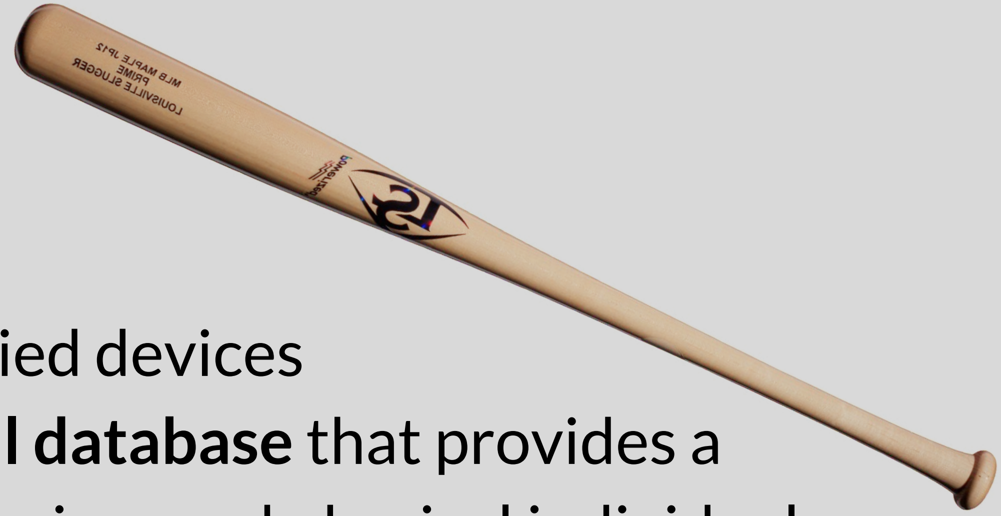
Arbitrary information can be embedded in the decryption key

Traitor tracing requirements

- A **traitor tracing code** that assigns a unique identifier to each user
- A **binding technology** that **irreversibly attaches** the identifier to the content in a **robust way**
- **Robustness** and **Imperceptibility** are key factors

Aims of traitor tracing

- Tracing ability to **identify pirates** (coalition of dishonest consumers) who may have leaked protected material
- Basis to **take further legal or business actions** against identified individuals



Response strategies:

- **Revoke** the identified devices
- Rely on an **external database** that provides a **pairing** between devices and physical individuals

Anticollusion codes

- Traitor tracing is **trivial when pirates are isolated**
- Dishonest users forge a pirated version by **mixing their copies**
- **Reliably identify** at least one pirate
- Most codes were based on **Error Correction Codes** (ECCs)
- In 2003, **Gabor Tardos** presented his optimal probabilistic fingerprint codes
    - Tardos codes are generated randomly but with a **specified statistical structure**
    - One of the most powerful tools to fight against collusion

Thank you!

References

- Tracing Pirated Content on the Internet: Unwinding Ariadne's Thread
- Watermarking-based Traitor Tracing to Deter Piracy of Entertainment Content
- Security issue and collusion attacks in video watermarking
- Multimedia Fingerprinting Forensics for Traitor Tracing
- Traitor tracing in content distribution: state of the art
- Anonymous Traitor Tracing: How to Embed Arbitrary Information in a Key

Active researcher in the field: Gwenaël Doërr

Lots of patents issued in this domain (~ 3500)