SELF-PROTECTING DIGITAL CONTENT

Paul Kocher
President & Chief Scientist
Cryptography Research, Inc.

Joint work with Benjamin Jun, Carter Laren, and others at Cryptography Research.

RSA 2004 – February 27, 2004 – 9:00am

About Cryptography Research

- Primary business:
  - —Develop & license new security technologies
  - —Major R&D focus
- Industries served:
  - — Financial Services
  - — Wireless / Telecommunications
  - — Pay Television
  - — Internet
  - — Entertainment

Products incorporating CRI technology secured over $50 billion in 2003

Motivating Question

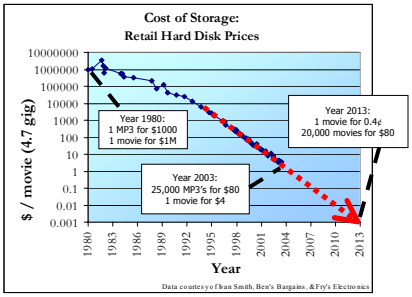
How should the anti-piracy features be designed for an optical disc format (like DVD)?

Complex, technically-challenging, controversial question.
(Many participants with conflicting objectives.)

One thing is clear, however: CSS is not the answer.

Too Important to Ignore

- Real-world problem:
  - CE/IT products need HD content on optical media
  - HD content owners require security
- Real-world challenges:
  - Piracy is growing with Moore's Law
  - DVD protection is broken
  - DRM market is dysfunctional
  - Piracy isn't a "solvable" problem
- Something will be done – but what's best?



• Ripping and burning of DVD movies cost film reportedly cost studios ~$3 Billion in 2002 DVD sales*
• 600,000 copies of films are reportedly downloaded illegally every day*

* BusinessWeek – July 14, 2003

Difficult requirements

- Must withstand concerted attacks
  - — Many motivated attackers
  - — Many implementations available to target
- Must fix the economics of security
  - — CE companies don't want to pay for security that doesn't help them
- Must be friendly to all participants
  - — CE, IT, studio, consumer…
- Must be renewable
  - — Must deal with unexpected threats
  - — Must adapt to new technologies
  - — Must be able to recover from attacks

[And the list goes on…]

User-friendly
- — Insert a disc & it plays
- — Minimize restrictions on legit use
- — Discourage piracy (casual + pro)
- — Support off-line playback
- — Respect privacy

Studio needs
- — Minimize piracy rates
- — Avoid irrecoverable failures

Player-maker requirements
- — Easy to implement
- — Low cost
- — Enables added-value features

RSA Conference 2004

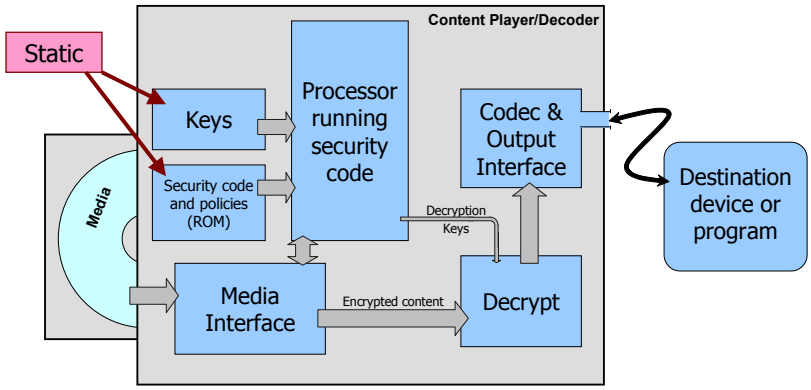
Background:
Anti-Fraud/Piracy Approaches

- Pay television security
  - — Anti-cloning and revocation technologies
- Copy control watermarking
  - — Embedding copying rules in audio or video
- Digital forensics
  - — Used to trace leaks of screeners and demos within studios
- Encryption
  - — Used to limit decryption to devices with valid keys
- DRMs
  - — Mechanisms for defining and implementing usage rules for content
- Financial risk management software
  - — Used to detect fraudulent transactions

RSA Conference 2004

Legacy Media Player Architecture

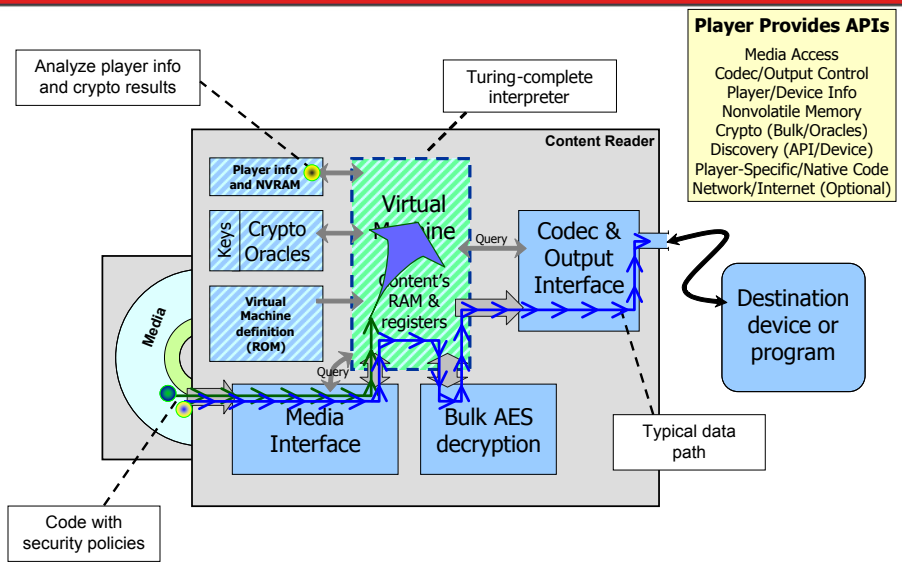
(DVD video, DVD audio, etc.)



RSA Conference 2004

Self-Protecting Content Architecture

(Simple player for decoding physical media)



Comparison

Traditional approach:

- — Content is passive
  - At most, carries flags/policies for player to detect
- — Player is responsible for security
  - May have great security or none (the content can't tell)

Static: Security upgrades require player replacement

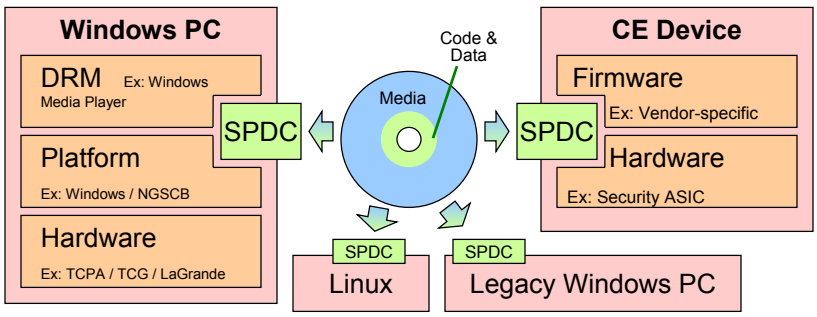
Self-protecting content:

- — Player provides a simple processing environment
  - Provides interpreter, environment info, crypto/security support, drive access, and codec/output
- — Content carries its own security logic
  - Can have great security or none (content decides)
- — Complementary to most other approaches
  - Key management, watermarking, physical disc features…
- — New security can be delivered with each released disc

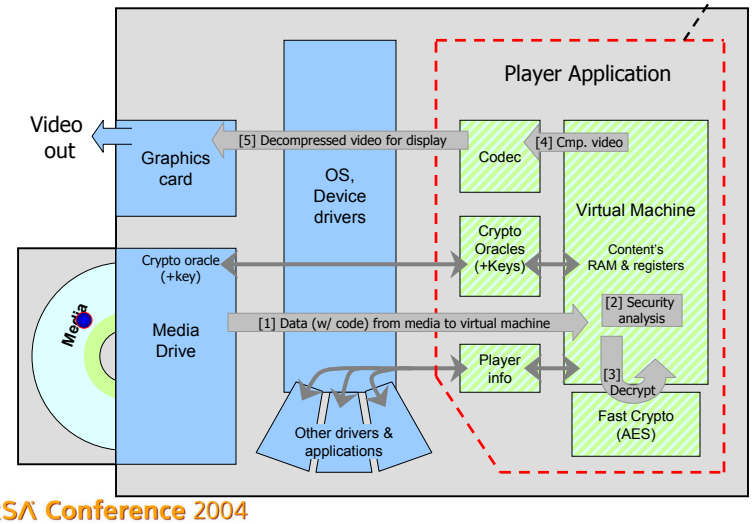
True renewability: Content provides its own security

Compatibility and Security: Heterogeneous playback environments

- VM can be simple and inexpensive to implement in a variety of devices
- Media format must be standardized, but players will be diverse
  - — Example: Some PCs will have TCPA / LaGrande / NGSCB (Palladium)
    - But general media format cannot mandate Palladium…
  - — Content needs benefits of platform-specific security features
    - Programmability standardizes playback process without making security static
    - Security should be as good as possible on each platform
    - Less secure platforms will need more updates & support fewer features



Example PC Implementation



RSA Conference 2004

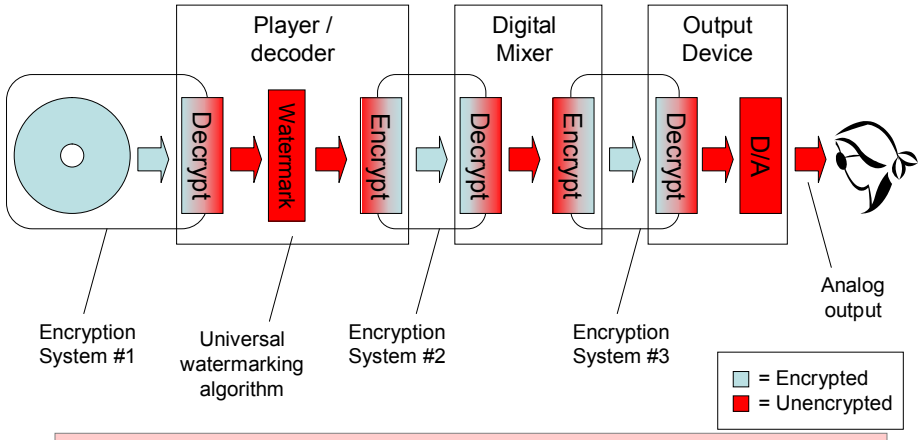
Implementation

- Hardware-based (CE box)
  - —VM: 35K gates, 0% CPU
    - < 2 Mb RAM
  - —Plus AES / RSA in hardware (~20K gates)
- Software-based (PC)
  - —VM: < 4% of a 2.4 GHz PC
  - —Plus decryption time (needed anyway)

RSA Conference 2004

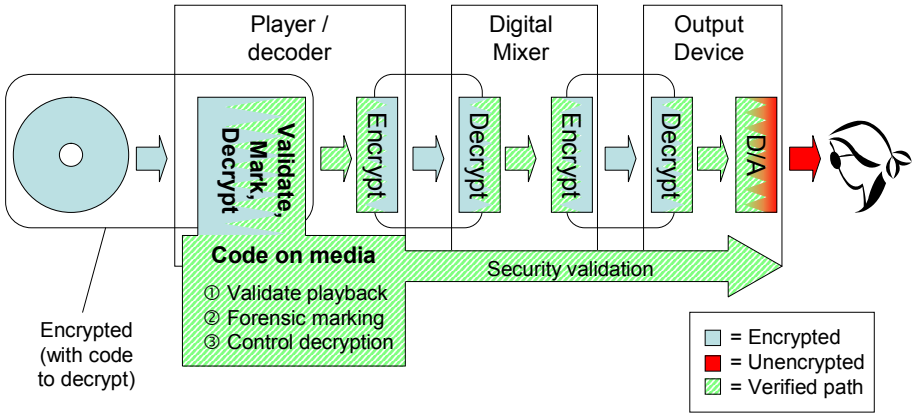
Link Encryption (Point-to-Point Security)

[How existing systems handle speakers, displays, etc.]



Any failure downstream from the decoder results in a permanent, irrecoverable system-wide loss of security

End-to-End Security

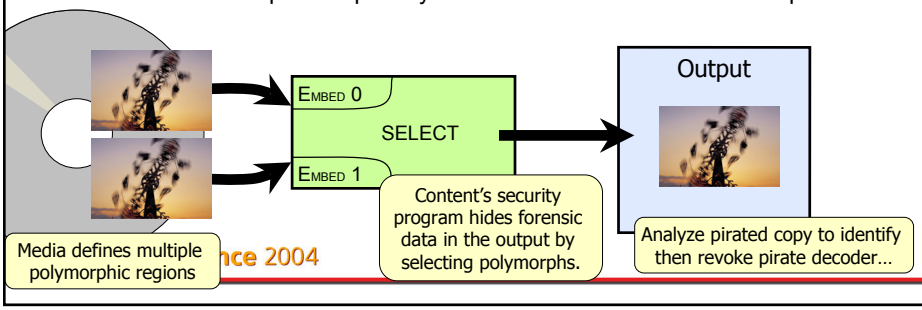


Content's code can identify downstream risks and take appropriate action

Forensic Marking

Provided by reprogrammability

- Risk management requires knowledge and control.
- Forensic marking: Knowing what went wrong.
  - — Player can allow content program to modify the output.
    - Modifications may be unique to player, output devices, user, keys.
  - — Addresses anonymity of piracy.
    - No impact on privacy of users who don't redistribute copies.



Marking: Security & Efficiency

- Marks can be extremely compact to encode
  - — Difference between version "A" and "B" can be a single byte
    - Enables virtually unlimited number of variations on a 25 gig disc
  - — Marks can be introduced prior to codec
    - Modifying content code submits different data to codec
  - — Marks can be introduced after codec
    - Mark drawn as an overlay
- Three important characteristics for forensic marks
  - ① Plausibility: Resistant to identification in a single copy
  - ② Durability: Resistant to degradation (e.g., tape from TV screen)
  - ③ Artistic Acceptability: Does not noticeably impair content
  - — Can easily exceed reasonable thresholds for all three with SPDC
- Content author controls everything
  - — Chooses marking rules & anti-collusion codes
  - — Selects variations in video
  - — Controls mark recovery & analysis

"Stalemate" Security Problems

- Last mover advantage.
  - — Unpredictable, evolving threats.
    - Must present a moving target.
  - — Many other security problems like this:
    - Credit card fraud, SPAM filtering, piracy, virus detection.

- No static solution
  - — Best hope: Avoid checkmate
  - — Must turn checkmates into stalemates

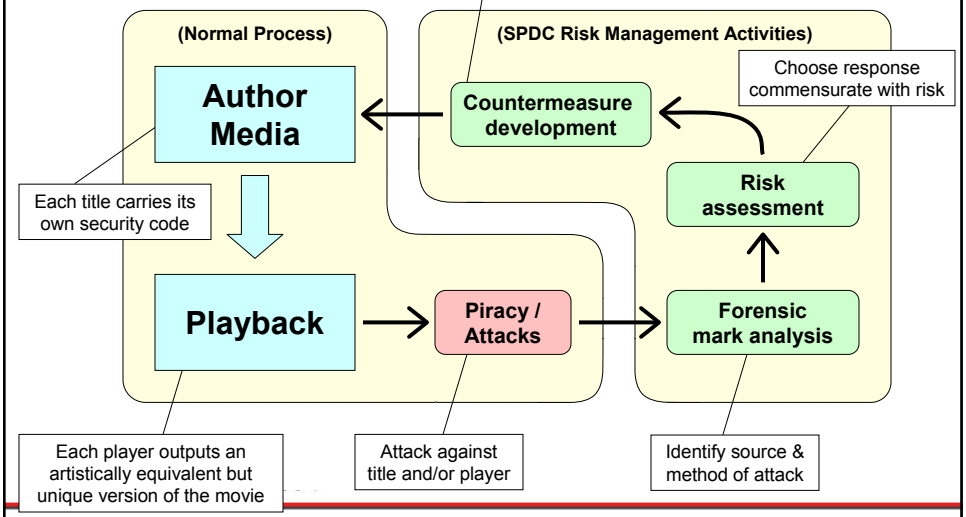
  (Practical countermeasure to every attack)

RSA Conference 2004

Risk Management Cycle

Goal: Reduce piracy rates & preserve release window

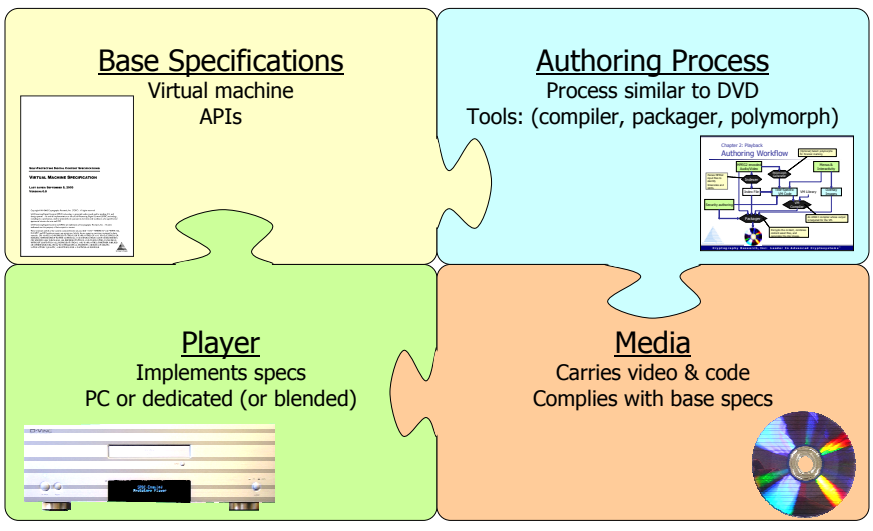
Wide range of options, e.g.:
- Extra player validity checks
- Signed native code on media
- Download PC software update
- Perform user auth step
- Check player history/NVRAM
- Limit output to DVD quality
- Embed extra forensic marks
- Display piracy warnings [etc…]



Guiding Principles

- Security architectures reflect basic design principles as well as specific requirements & objectives.
  - **Free market economics**
    - Technology should enable market-based solutions to problems
    - Studios should have control and responsibility over their own risks
    - Avoid requiring new laws or policies
  - **Risk management**
    - Piracy must be controlled since it cannot be eliminated
    - Must provide information about attacks & practical responses
    - Security must be renewable and effective, even after many attacks
  - **Security best practices**
    - Must be designed, reviewed by experts seeking to reduce piracy
    - Based on strong cryptography and good design principles
    - Integrates with other security technologies

Components

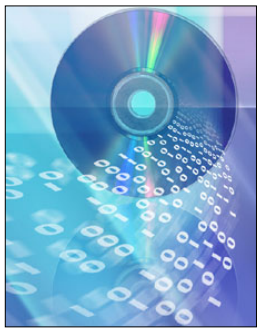


Reasons for titles to carry their own security

- Allows market forces to shape security
  - Security "menu" is not restricted in advance
  - Ensures that spending on security matches studio's risk
  - Frees CE companies from expensive & messy tasks
  - Allows market to respond to user demands
  - Reduced need for lobbying & regulatory solutions
- Forensic marking provides knowledge about piracy
  - Privacy-friendly way to gather information
  - Allows responses to be tailored to specific problems
- Renewable: Respond to piracy without player revocation
  - Work around player security bugs without affecting legitimate users
  - Security logic is not a static target
- Better interactivity & User experience
  - Work around player menu bugs, etc.
  - Enables interactive features (programmable environment…)
- Internet integration
  - Develop synergies with on-line assets

Conclusion

- Piracy is a real threat that needs research attention
  - It would be a tragedy if piracy ruins the movie industry
    - Threat is extremely serious
    - Impediments due to file size are going to go away
  - Today's technological choices will determine piracy rates in 3-7 years



- SPDC philosophy:
  - The problem is too complex to solve today
    … so we avoid committing to a static design
    … and build tools for managing the risk

For papers & more information, please visit:
www.cryptography.com/spdc

Contact Information

Paul Kocher

President & Chief Scientist
Cryptography Research, Inc.

paul@cryptography.com

We're Hiring!

Want to join an exciting, profitable company specializing in solving important real-world security problems?

www.cryptography.com/jobs

RSA Conference 2004