Gaming in the Glass Safe - Games, DRM & Privacy

Ferdinand Schober

Talk Overview

- Historical Development
  - Vintage Protection
- Copy Protection to DRM
- Current DRM systems
- DRM & Privacy
  - Case Study
- Messing with a gamer
  - Case Study
- Summary
- Q&A

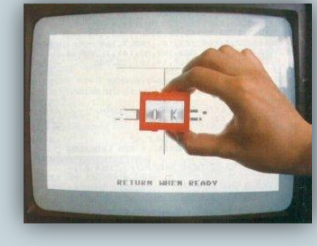
Historical Development

1980+

Disc Layout Protection

- Games distributed on floppy disc
  - Easy to duplicate
- Use Unique disc layout
  - E.g. change sector/track markings
  - Requires custom reading method
- Failure prevents loading
- Broken through nibble copy

1980s and 1990s

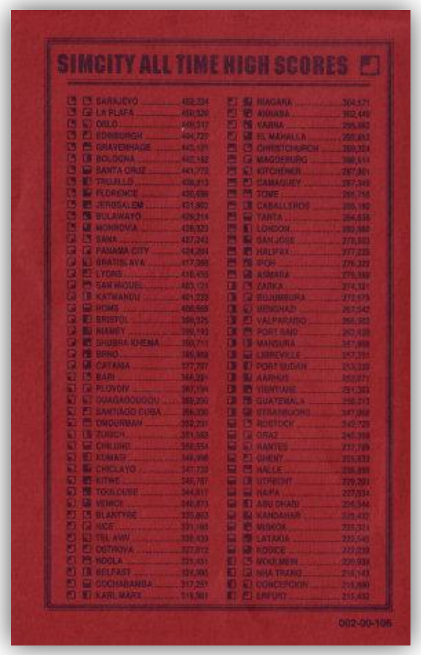


Physical Token Protection

- Use external token to confirm ownership
  - E.g. physical dongle
  - Failure prevents launching
  - Broken through game code modification
- Use user-based challenge/response
  - E.g. code wheel, handbook, etc
  - Failure stops game/changes behavior
  - Broken through (over time much less) painstaking token duplication

Vintage Game Tokens

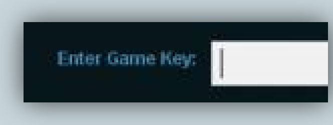
- Tokens could be nice game add-ons
- Effective as long as token is hard to copy
- Now outdated due to easy digitalization & Internet



Historical Development

1995+

1998+


Enter Game Key:

CD Layout Protection

- Games distributed on CDs
  - Same old problems
- Break Red Book standard
  - Broken sectors, oversized disc
  - Prevents standard copy procedure
- Failure prevents loading
- Broken through error-resilient hardware, advanced nibble copy

Registration Key

- Use of key value to confirm ownership
  - Derived through cryptographic algorithm
  - Required for installation, multiplayer features
  - Broken through reverse-engineering, online databases
  - Still the first defense

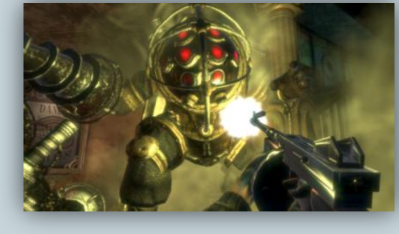
Historical Development

1980+, 2000+

Code Obfuscation

- All copy protection is useless if game code can be changed
- Obfuscate binaries
- Pre-2000 mostly custom solutions
- Post-2000 added as middleware (system components)
- De-obfuscation & patch possible (cracks)

2002+



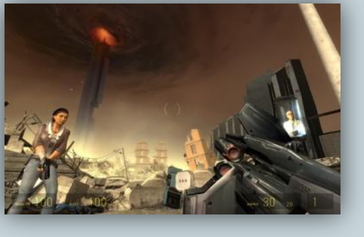
Advanced Copy Protection

- Cracks are surprisingly effective
- Combine disc layout, registration key, code obfuscation
- Added online registration requirement, often limits number of installs
- Can still be removed, but raises the bar

Historical Development

2003+

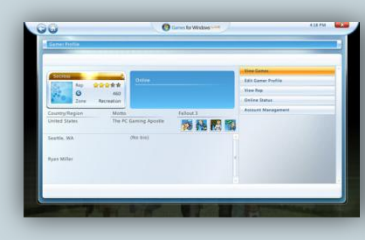
STORE LIBRARY NEWS COMMUNITY
Welcome to Steam, the world's largest gaming platform.
TORCHLIGHT
PORTAL
Play Portal Free On your PC or Mac
-50%
Now Available on Mac & PC



Content Delivery (DRM v2)

- Eliminates physical distribution, downloads only
- Copy protection built-in
- Adds:
  - user identity
  - payment information
  - social network
  - online requirement

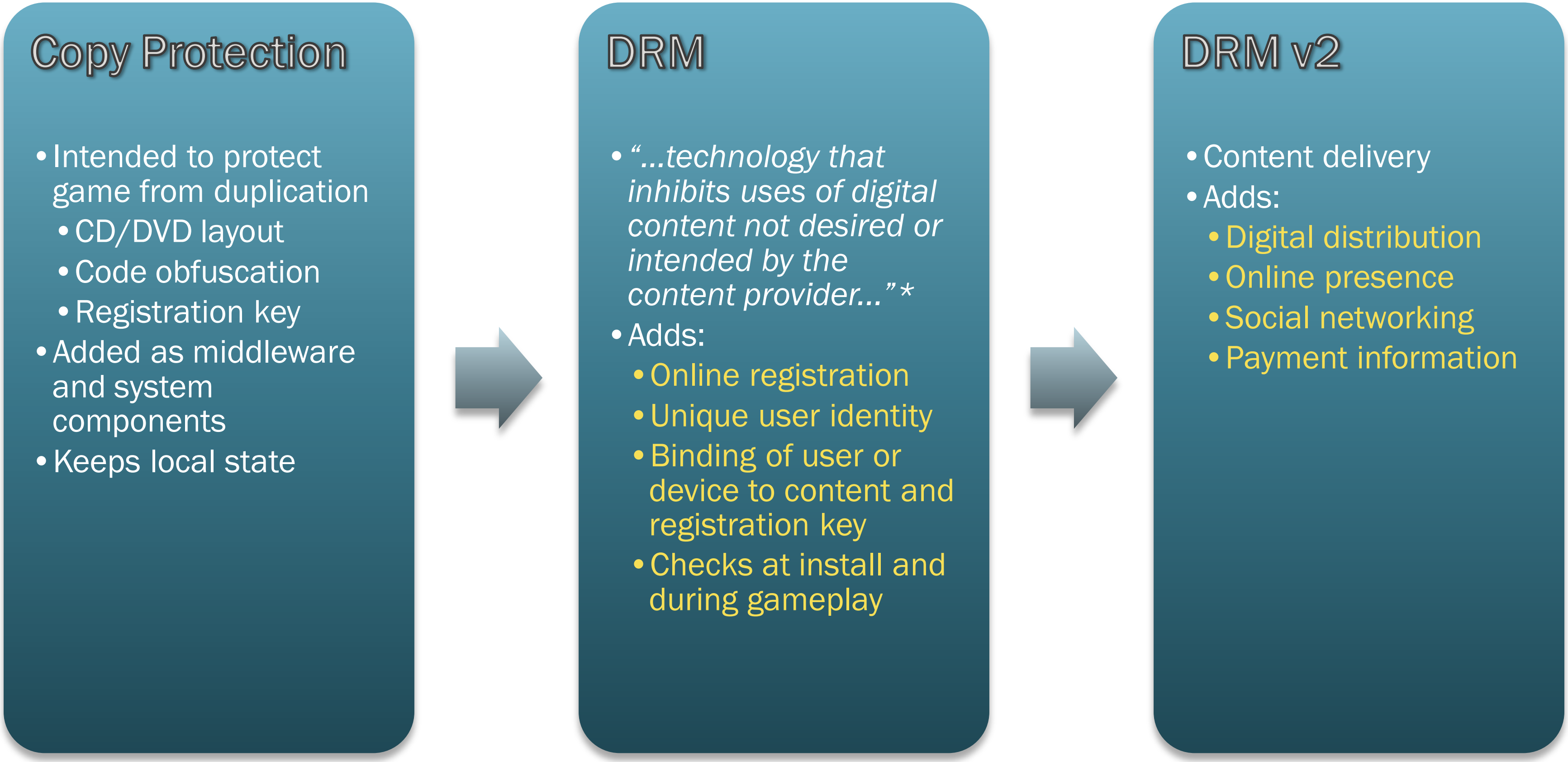
2006+



DLC

- Additional game content for purchase
- Tied to game registration and user account

Copy Protection to DRM



Copy Protection

- Intended to protect game from duplication
  - CD/DVD layout
  - Code obfuscation
  - Registration key
- Added as middleware and system components
- Keeps local state

DRM

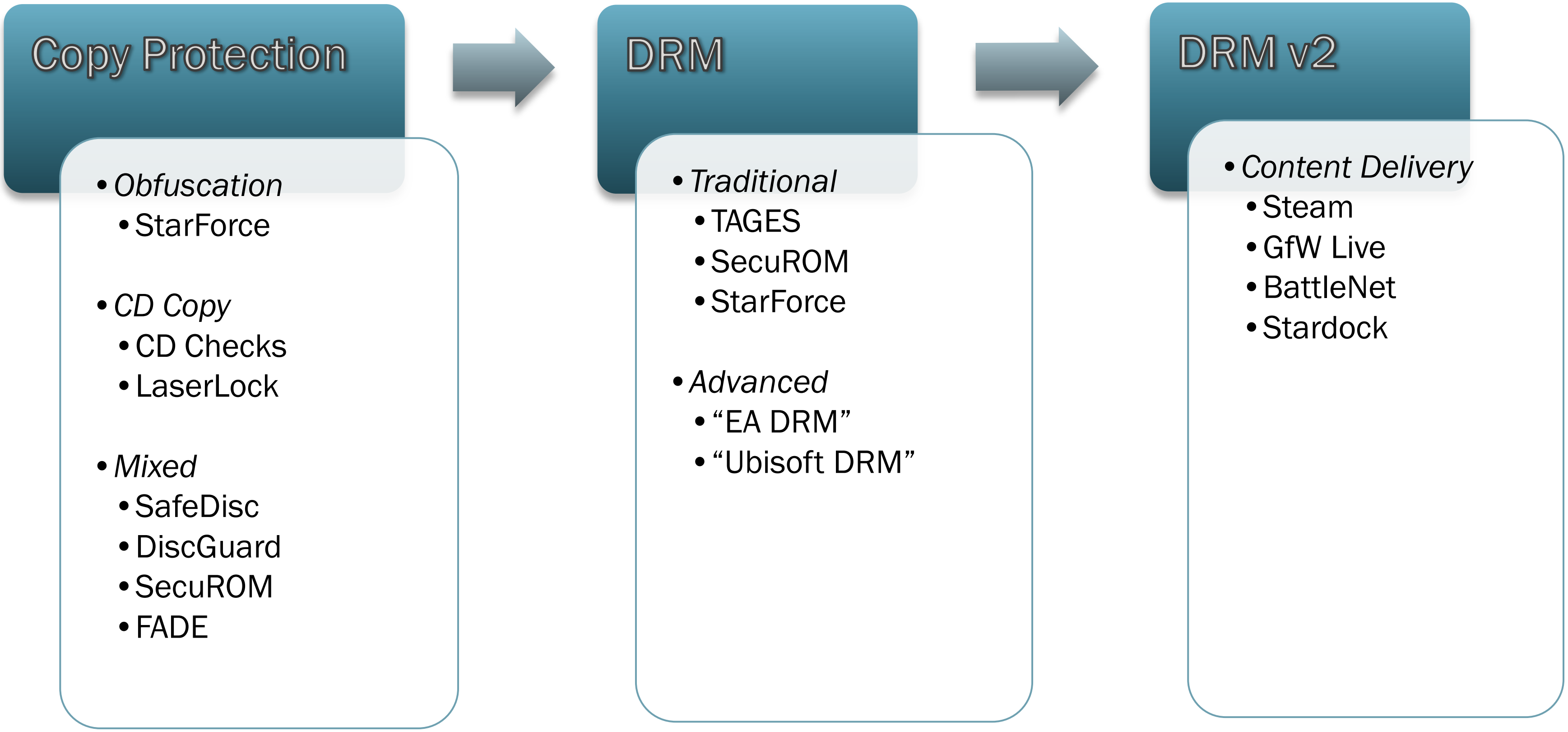
- *"…technology that inhibits uses of digital content not desired or intended by the content provider…"**
- Adds:
  - Online registration
  - Unique user identity
  - Binding of user or device to content and registration key
  - Checks at install and during gameplay

DRM v2

- Content delivery
- Adds:
  - Digital distribution
  - Online presence
  - Social networking
  - Payment information

**Wikipedia*

Copy Protection to DRM



Copy Protection

- *Obfuscation*
  - StarForce
- *CD Copy*
  - CD Checks
  - LaserLock
- *Mixed*
  - SafeDisc
  - DiscGuard
  - SecuROM
  - FADE

DRM

- *Traditional*
  - TAGES
  - SecuROM
  - StarForce
- *Advanced*
  - “EA DRM”
  - “Ubisoft DRM”

DRM v2

- *Content Delivery*
  - Steam
  - GfW Live
  - BattleNet
  - Stardock

Current DRM

E_FAIL Case 1: *SPORE*

- SecuROM DRM
  - Requires online registration on install
  - Installation limit – no uninstall tool (3x)
  - “Phones home”
- September 2008
  - "Most pirated Game ever”
    - Available on BitTorrent before release
    - downloaded >500,000 times
  - 90% 1-Star ratings on Amazon
  - DRM binaries remain on disc after uninstall
- December 2008
  - Uninstall tool released

Space Police

By kenuty

DOB: 9/11/2008

Description:
Ready to destroy consumers in all galaxies, 3 shots and you're dead. (credit to bkarsz logo,check out his space pirate)

Current DRM

- E_FAIL Case 2: S.TA.L.K.E.R.: Clear Sky
  - TAGES DRM
    - Requires online registration on install
    - Installation limit (5x)
  - December 2009
    - Servers overwhelmed by Steam sale
    - Most legal installations fail during the holidays

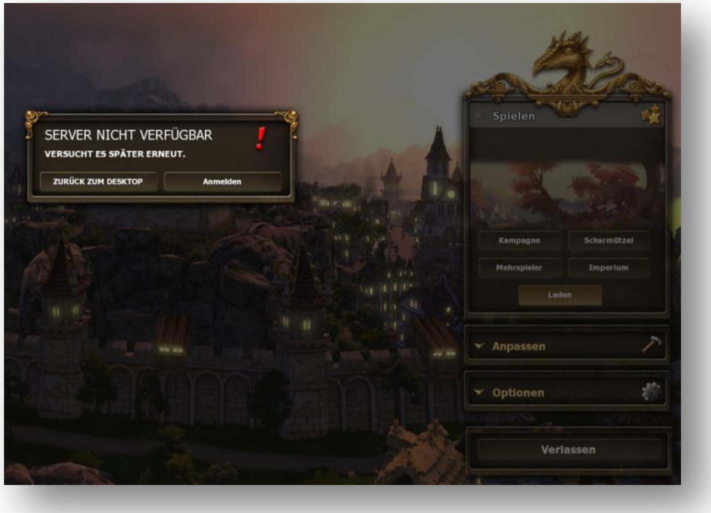
Current DRM

- E_FAIL Case 3: *Assassins Creed 2*
  - “Ubisoft DRM”
    - Requires permanent network connection
      - Reset to checkpoint on disconnect
    - Tied to user account
    - Stores saved games in the cloud
  - March 2010
    - Authentication server failures
      - 10+hrs offline
      - Single player users locked out
      - *“95% of players were not affected”*
    - Cloud saves often fail
    - Patched quickly
      - Resume gameplay after connection is restored
      - Local saves are allowed

WARNING ... DESYNCHRONIZATION IMMINENT... ...
... CONNECTION LOST ... ... ATTEMPTING TO RE-
ESTABLISH CONNECTION ... ... WARNING ...

Current DRM

- E_FAIL Case 4: Settlers 7
  - “Ubisoft DRM”
    - Requires permanent network connection
    - Tied to user account
    - Stores saved games in the cloud
  - April 2010
    - Authentication server failures
      - Players unable to run game
        - 50,000 posts in forum
      - MP reported nearly unplayable
    - Patched with little effect
  - June 2010
    - Australian players locked out at release time



SERVER NICHT VERFÜGBAR !

VERSUCHT ES SPÄTER ERNEUT.

Current DRM

- Futile Attempts
  - DRM of all previous games can still be removed!

Cracked in under 25hrs

DRM Privacy Impact

- Content Protection
  - Uniquely identify machine
    - Install limits (TAGES, …)
  - Uniquely identify user
    - User accounts (Steam, …)
- Runtime Protection
  - Identify when player is starting/installing game
    - Startup/install DRM checks
  - Identify when player is running game
    - Online DRM active all times (even single player)

DRM Privacy Impact

- User Account
  - Exposes
    - Machine history
    - Machine configuration
    - Running processes
    - Online Time
    - Personal information
      - Address, email, DOB, …
    - Payment information
    - Purchase history
      - Wishlist
    - Friend network

"Blind" Machine Account

User-specific Account

DRM Privacy Impact

- Exposes a bit too much information?

There is more…

Social Network Privacy Impact

- "Achievements"/"Badges"
  - Exposes
    - Game history
    - Gaming behavior profile
      - MP vs. SP
      - Casual vs. hardcore
      - …
    - Online Time
    - Gaming location

- Facebook Integration
  - Exposes
    - All personal data previously not accessible
      - Pictures, personal history, …

Case Study – Account Information

- BattleNet (RealID)
- Account needed for install
  - Naturally necessary World of Warcraft
  - Now for other games
    - StarCraft II
    - Diablo III
- Not needed for single player
  - But: *"…you don't get access a lot of the stuff."*
- Let's walk through the sign-up…

Case Study – Account Information

- Information needed
  - DOB (!)
  - Email Address
  - Full Name
  - Full Address
  - Phone Number
- Friend list
  - Friends of Friends are listed with real name (!)
    - *Optional*
- Game list

Glass Gamer

Case Study – Network Information

- “Ubisoft DRM”
- Persistent connection to Ubisoft DRM server
  - Port 80 (tunneling possible), TCP, encrypted
  - Required for single player
  - Failure when connection interrupted
    - High drop rate can be an issue
    - Unreliable routers
- Able to track all game usage
  - Especially on wireless networks

Glass Gamer

Messing with a Gamer

- DRM is an artificial point of failure
- Network connection can be limited
  - Anti-Virus and Firewalls can interfere
  - Connection bandwidth to small
  - Connection not reliable enough
- Can be directly attacked
  - Local network traffic saturation
  - Wireless traffic injection/interference
  - Server DDoS attack
    - See Ubisoft DDoS attack (March 2010)

Messing with a Gamer

- Registration keys are vulnerable
  - Steal registration key and post publicly
  - Worse: Key generator could generate valid key
    - Both lead to perma-ban (how to fight?)
- Accounts are vulnerable too
  - Passwords can be guessed
    - Security is improving
    - WoW players have become paranoid
  - Reset questions can be guessed
    - You linked to you Facebook profile, remember?
  - Can initiate false “my account has been compromised”
    - Will be painful…
  - Accounts can be compromised at the provider’s side
    - Not publicly admitted

Case Study – Gaming Denial

- “Ubisoft DRM”
- Local Method:
  - Saturate wireless network router/inject packets
    - Router failure is only a matter of time
  - Wireless dissasociation attack
    - Resets connection at the wireless layer
- Remote Method:
  - Dump traffic on remote target
    - Reduces bandwidth, router failure is likely
  - TCP reset attack
    - Resets connection at the TCP layer
  - SSL replay reset attack
    - Resets connection at the SSL layer
      - configuration dependent

Case Study – Gaming Denial

- Ultimate result:

Summary

- DRM developed gradually over time

- DRM is becoming more integrated
  - Easy to track gamers and their habits

- Content Delivery, Social Networks and DRM are merging
  - Exposes vast amount of personal information

- DRM is artificial, single point of failure
  - Can ruin your day…

Q&A