Gaming in the Glass Safe - Games, DRM & Privacy

Ferdinand Schober

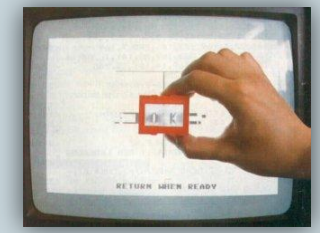
Talk Overview

- Historical Development
  - Vintage Protection
- Different DRM approaches
  - Privacy Study
  - Failure Cases
  - Case Studies
- Messing with a gamer
  - Case Study
- Why are games cracked?
- Q&A

Historical Development

1980+

1980s and 1990s



Disc Layout Protection

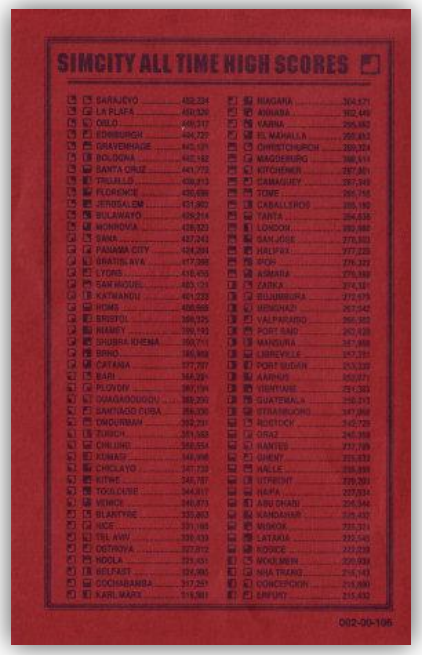
- Games distributed on floppy disc
  - Easy to duplicate
- Use Unique disc layout
  - E.g. change sector/track markings
  - Requires custom reading method
- Failure prevents loading
- Broken through nibble copy

"Feelies"

- 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

Feelies

- 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- Now outdated due to easy digitalization & Internet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+

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

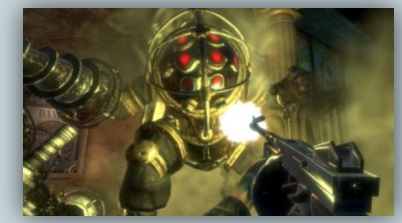
Registration Key

- 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+

2002+



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)

Networked DRM

- 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+

2006+

Social DRM

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

DLC

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

Copy Protection to DRM

Copy Protection

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

Networked DRM

- *Current*
  - TAGES
  - SecuROM
  - StarForce
- *Next-gen*
  - “EA DRM”
  - “Ubisoft DRM”

Social DRM

- *Content Delivery*
  - Steam
  - GfW Live
  - BattleNet
  - Stardock
- *Walled Garden*
  - iPhone
  - Xbox Live
  - PS Network

Privacy Study - Copy Protection

Copy Protection

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

- Keeps local state only
  - Intended to prevent local copies
  - Never leaves the local system
    - Might modify the local OS, install drivers, etc.
    - Stores data locally

Copy Protection

- E_FAIL Case:
  - Advances in computing and technology break copy protection
    - Digital Reproduction
    - Binary analysis technology
    - Hardware
    - Internet
    - …
  - Copy protection relies on error-case functionality
    - Removal is possible

Networked DRM Privacy

Networked DRM

- *"…technology that inhibits uses of digital content not desired or intended by the content provider…"**
- Combine disc layout, registration key, code obfuscation
- Online registration requirement, often limits number of installs

- Restricts usage
  - Intended to monitor proper usage
  - In terms of privacy:
    - Unique Machine Identification/User ID
      - Machine Fingerprint
    - Exposes usage over the network
      - Install/Startup: when is user starting a game?
      - Runtime: when is user playing a game?
    - Next big thing: content execution
      - All other security concerns

*Wikipedia

Networked 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

Networked DRM

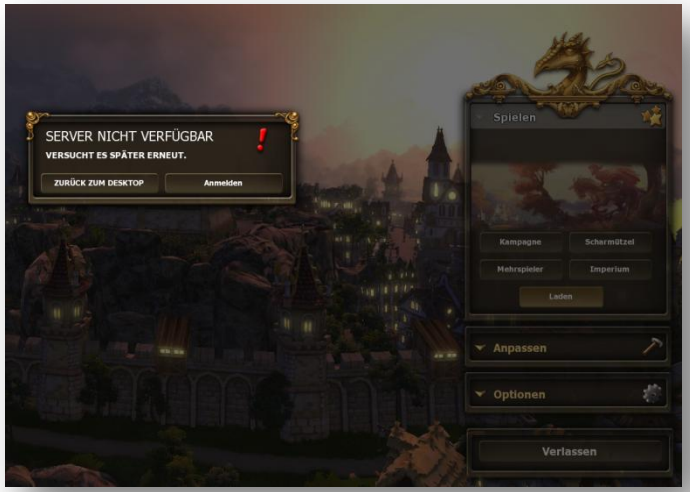
- E_FAIL Case 2: *S.T.A.L.K.E.R.: Clear Sky*
  - TAGES DRM
    - Requires online registration on install
    - Installation limit (5x)
  - December 2009
    - Servers overwhelmed by Steam sale
    - Most legal installations fail during the holidays

Networked 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

Networked 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



Networked DRM

- Futile Attempts
  - Games will continue being cracked

Cracked in under 25hrs

Privacy Case Study – Networked DRM

- "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

Social DRM Privacy

Social DRM

- *Social Network*
  - *"Achievements"*
  - *Game History*
- *Content Delivery*
  - *Payment*
- *Built-in content protection*

- Ties in all the social goodness…
  - Still intended to monitor proper usage
    - …but be social too
  - In terms of privacy:
    - All from before
    - User account information
      - Personal Information (address, DOB (!), …)
    - Payment information
      - Need to pay for this somehow…
    - Purchase history
      - Wishlist
    - Friend network

Social DRM Privacy (cont.)

Social DRM

- *Social Network*
  - *"Achievements"*
  - *Game History*
- *Content Delivery*
  - *Payment*
- *Built-in content protection*

- Ties in all the social goodness…
  - "Achievements"/"Badges"
    - Game history
    - Gaming behavior profile
    - MP vs. SP
    - Casual vs. hardcore
    - Online Time
    - Gaming location
    - …
  - Facebook integration
    - All other data not previously accessible
    - Pictures

Social DRM Privacy

- Exposes a bit too much information?

Privacy Case Study – Social DRM

- BattleNet (RealID)
- Account needed for install
  - Naturally necessary World of Warcraft
  - Now for other games
    - StarCraft II
    - Diablo III
  - Was also considered for official forum posts

- Not needed for single player
  - *But: "…you don't get access a lot of the stuff."*

- Let's walk through the sign-up…

Privacy Case Study – Social DRM (cont.)

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

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 too 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

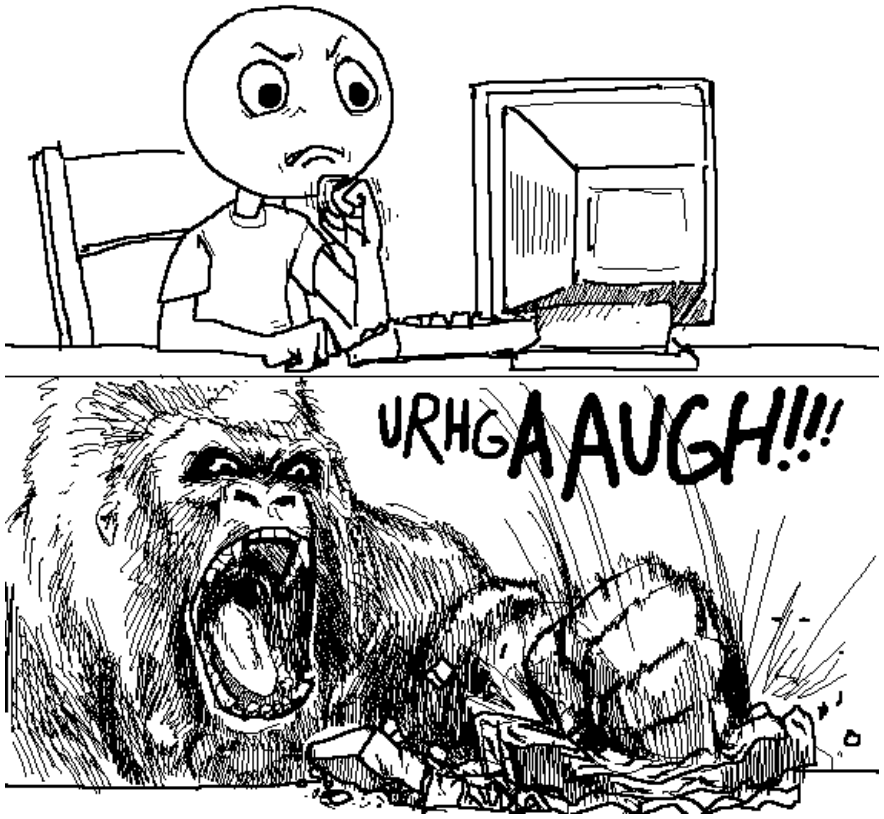
- Registration keys are vulnerable
  - Steal registration key and post publicly
  - Worse: Key generator could generate valid key
    - Both lead to perma-ban (how to fight?)
- Accounts are vulnerable too
  - Passwords can be guessed
    - Security is improving
    - WoW players have become paranoid
  - Reset questions can be guessed
    - You linked to your 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:



Why are games cracked?

- Quick answer:
  - Free stuff is always good
- It is more complex:
  - DRM can be a severe nuisance
    - Cracked games are often easier to use
    - Might not be able to play when I really want
  - Privacy/Policy concerns
    - This is making a lot of gamers worry…
  - What to do if DRM servers go offline for good?
    - Gamers like to play old games
    - Vintage gaming & emulators

Q&A