SIGPwny

FA2023 Week 06 • 2023-10-08

Cracking DRM

Ojas Upalekar

Announcements

- Fall CTF challenge solutions were released (prizes soon)
    - some challenges in vault for points

ctf.sigpwny.com

sigpwny{l1c3ns3_t0_h4ck}

YOU NEED TO PAY EXTRA TO USE FEATURES
B M W
THAT ARE ALREADY IN YOUR CAR

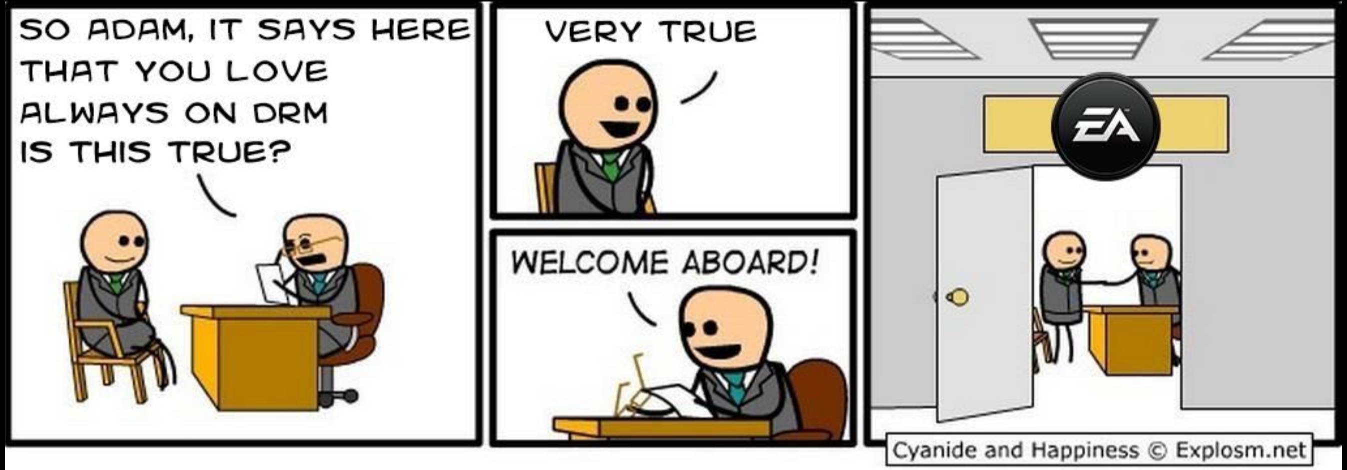

SO ADAM, IT SAYS HERE THAT YOU LOVE ALWAYS ON DRM IS THIS TRUE?
VERY TRUE
WELCOME ABOARD!
EA
Cyanide and Happiness © Explosm.net

Table of Contents

- What is DRM
- History of DRM
  - Early implementations
  - Denuvo
- Opposition to DRM
- How to Crack?

Consider

- Unable to cast a Netflix show through Zoom
- Jailbreaking iPhones
- Activation Codes for Games
- Even just simple password entry

What is DRM?

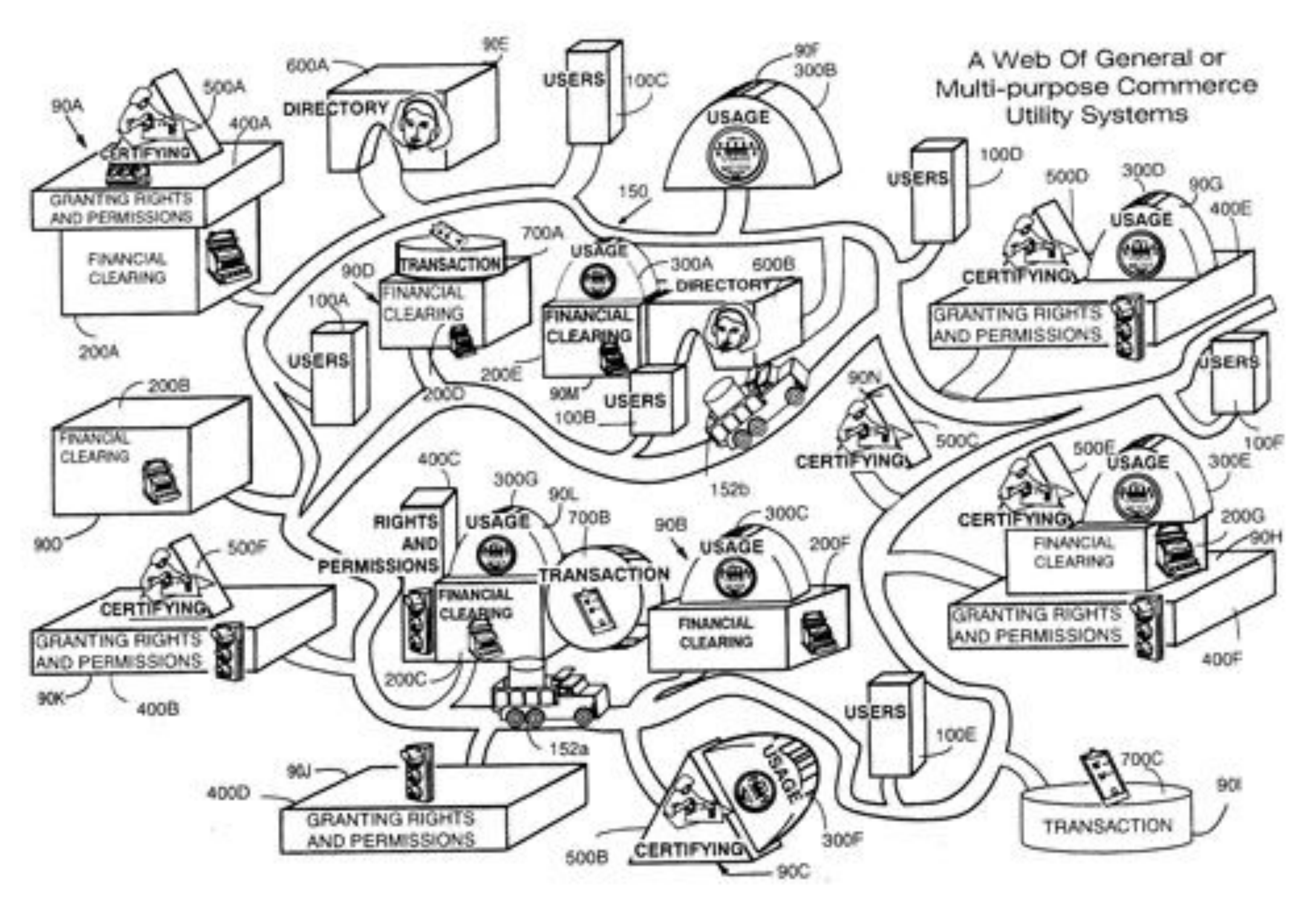
Digital Rights Management

- Management of legal access to digital content
- Protection of copyright
- Expanded beyond just software applications

History of DRM

- Developers wanted to develop a method that ensured that every person using their software legally purchased the service
- Piracy became prevalent in the 90s
- Began as Game Manuals
- First DRM: Software Service System (SSS) was developed by Japanese engineer Ryuichi Moriya
  - Encryption based system
- Libraries

InterTrust's Patents



History - contd.

- Combination of software and laws
    - US: DMCA
    - EU: Information Software Directive
    - Denuvo Anti-Tamper

Denuvo

- Most well-known and widely used DRM system in the video game industry.
- Developed in 2014
- Found in:
  - FIFA 15
  - Doom: Eternal
  - Assassin's Creed Origins

So, what’s the problem?

Oppositions

- The Ideology of the "Internet"
  - Open source
- User Convenience
  - People feel annoyed encountering DRM
- Examples of decreasing game
- Opposed by the ACM and the IEEE
- Issues about availability, usability and performance

Cracking?

Reverse Engineering

- Using tools like Ghidra, IDA to read source code
- Tools and Patches to exploit vulnerabilities
- Altering conditional branches, images, assets etc.
    - DeCSS
    - FairUse4WM

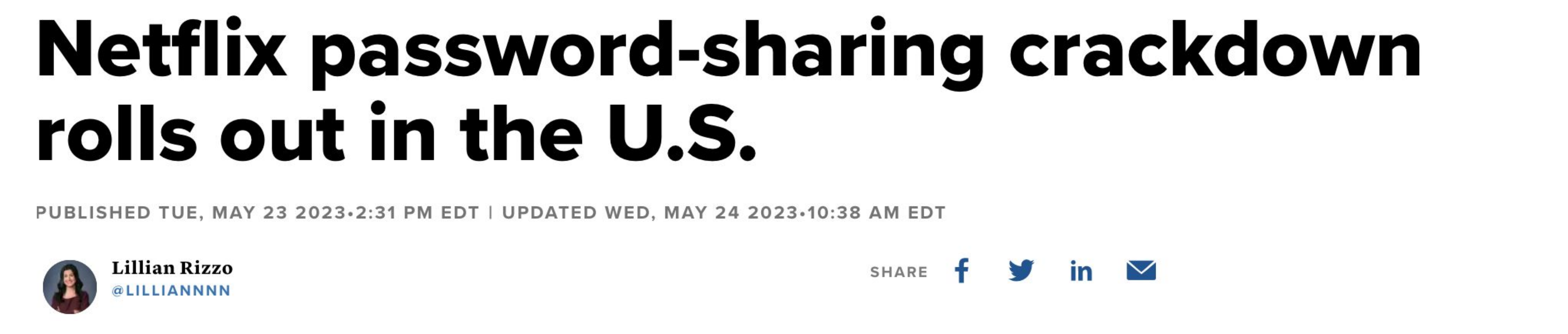
Key Generators

- Some applications require a verification/authentication code for access
- Key Generators have been used to create valid keys and licenses to bypass DRM systems.
  - Microsoft Word
  - Expansion Packs for Games (Destiny)

Emulation

- Some DRM systems verify software/hardware
- Emulation tricks that application into believing it is in a legitimate platform
- Works well with reverse engineering
  - Allows for frame by frame execution
  - Can see what block of memory is being executed
- Pokémon

Account Sharing



Netflix password-sharing crackdown rolls out in the U.S.

PUBLISHED TUE, MAY 23 2023•2:31 PM EDT | UPDATED WED, MAY 24 2023•10:38 AM EDT

Lillian Rizzo
@LILLIANNNN

The Empress

- Most famous DRM cracker
- Identify unknown
- "no one has liberated more high-profile games over the past year than Empress."
  - Grew to fame for cracking RDR2 and recently Hogwarts Legacy

https://www.wired.com/story/empress-drm-cracking-denuvo-video-game-piracy/

Demo/Challenge

- Simple "crackme" that resembles a user trying to authenticate their copy of a software
- Password cracking and reverse engineering

Next Meetings

`2023-10-12` • **This Thursday**

- Crypto I
- Learn the basics of Cryptography, and how to break it!

`2023-10-15` • **Next Sunday**

- Crypto II

ctf.sigpwny.com

sigpwny{l1c3ns3_t0_h4ck}

Meeting content can be found at sigpwny.com/meetings.

SIGPwny