Game Security Software

Corbin Modica & Johnathan Butler


ELIMINATED BY CARTERLOL
AS HANZO
1:48 ESCORT THE PAYLOAD
RESPAWN IN
5
MATCH TIME: 1:39
KILL CAM
PRESS H TO CHANGE HERO

Threat Model

Assets and vulnerabilities

Assets

- The Platform (network, servers, online store)
- The Game’s competitive integrity and balance
- The Company’s image, player perceptions and experience
- The In-game economy
- The Identity and personal information of players
- The Game’s source code and assets

Vulnerabilities

Wide Attack- Surface

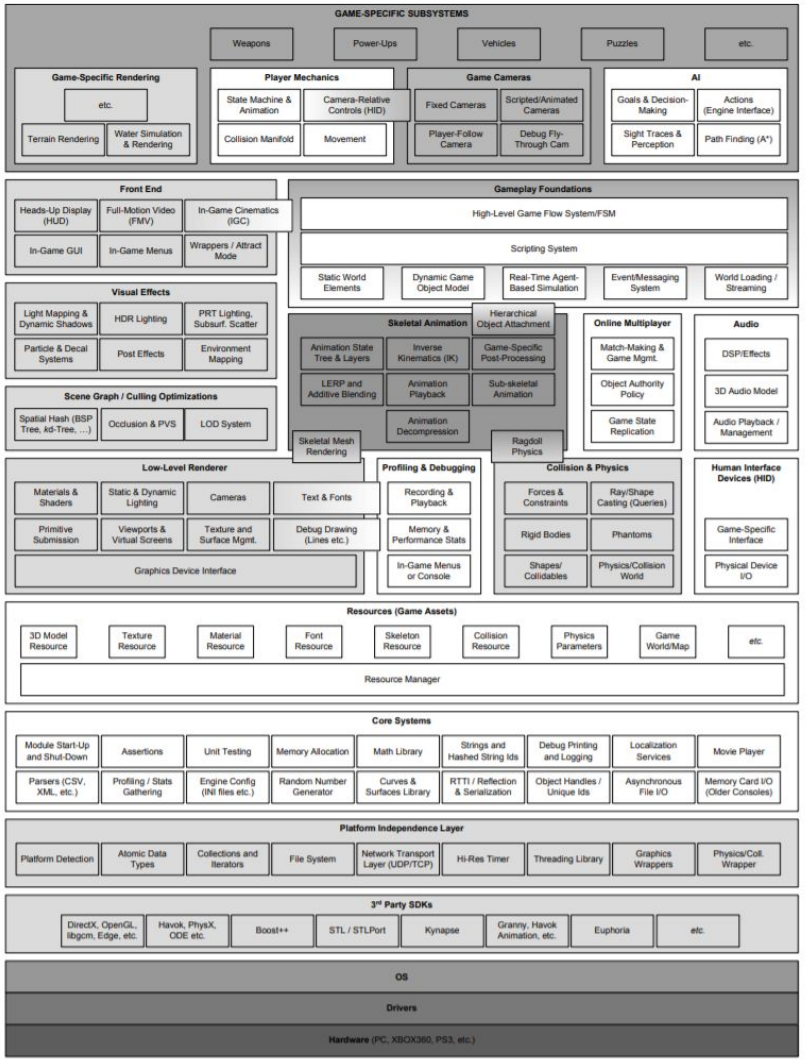


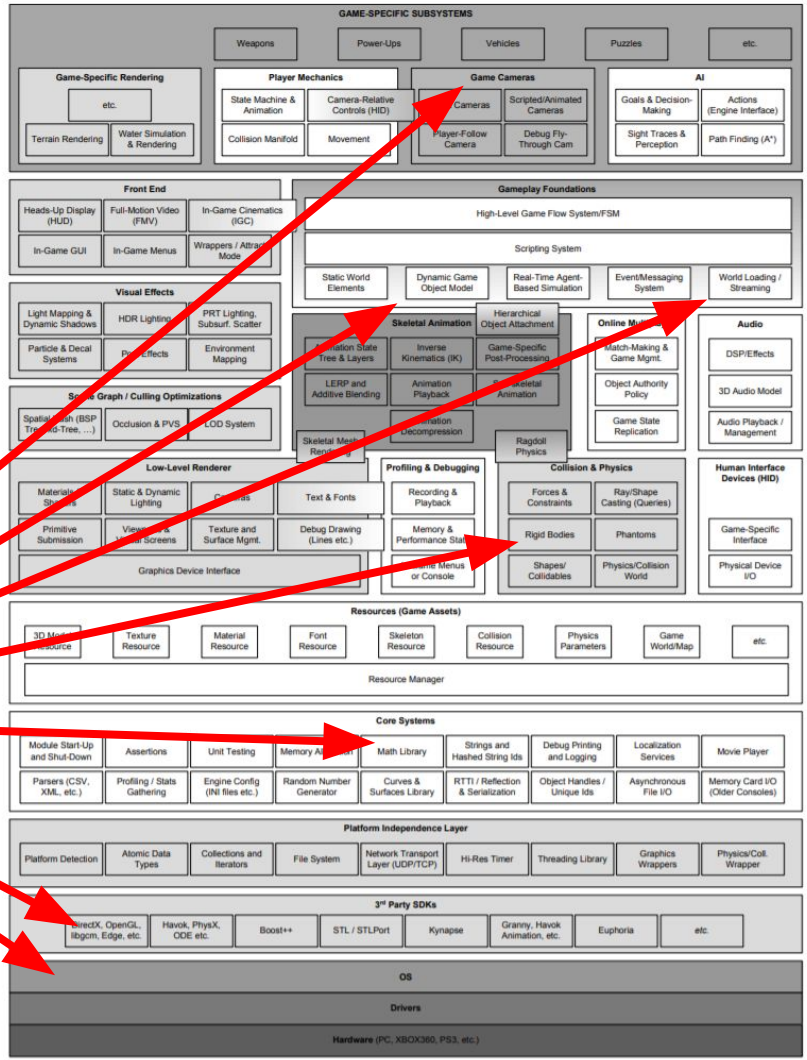
Image: Jason Gregory
Game Eng. Architecture

[x]

Vulnerabilities

Wide Attack- Surface

Exploitation of these systems & libraries



Leads to this:

Snoop on object lists to find the coordinates of enemy players, use the DirectX library to draw unauthorized interface
They can port hacks or pieces of hacks from game to game, especially those that share libraries / engines

Threats

Game Developers **cannot control the client system.**

Cheaters will:

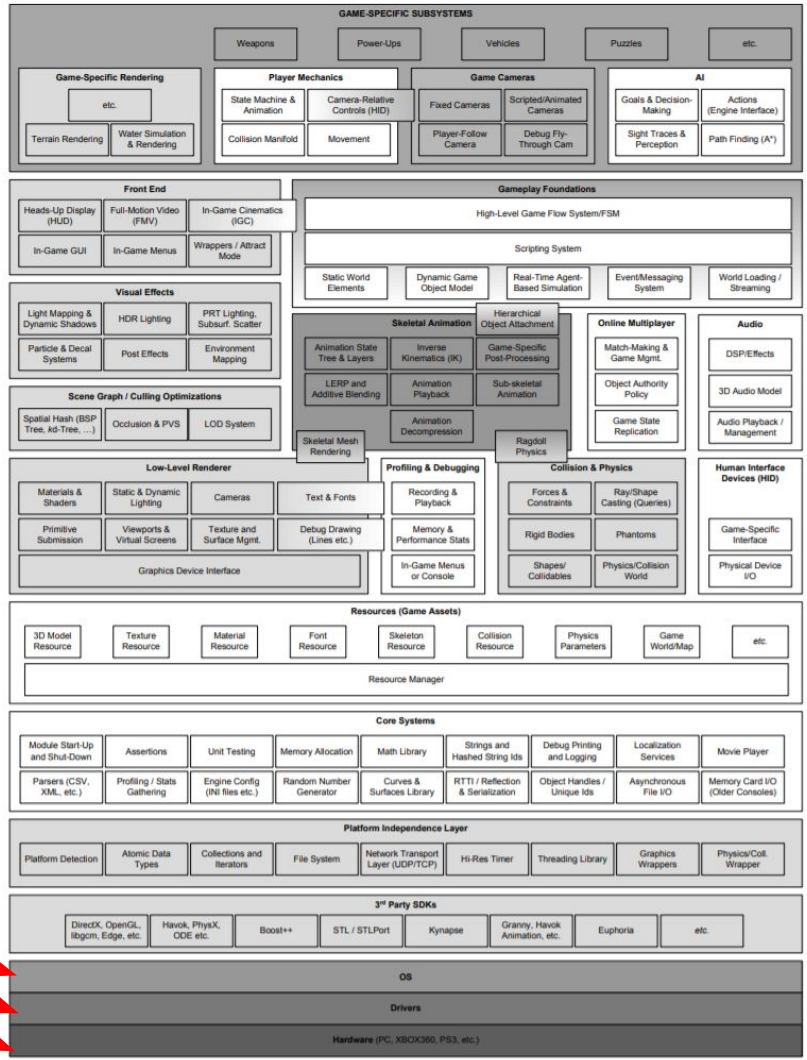
- Read/change process memory, control of execution
- Modify OS to change behavior of functions

Vulnerabilities

Reliance on Host OS

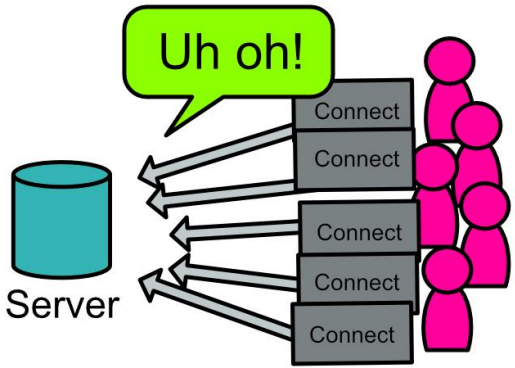
- Can’t trust memory
- Can’t trust the kernel

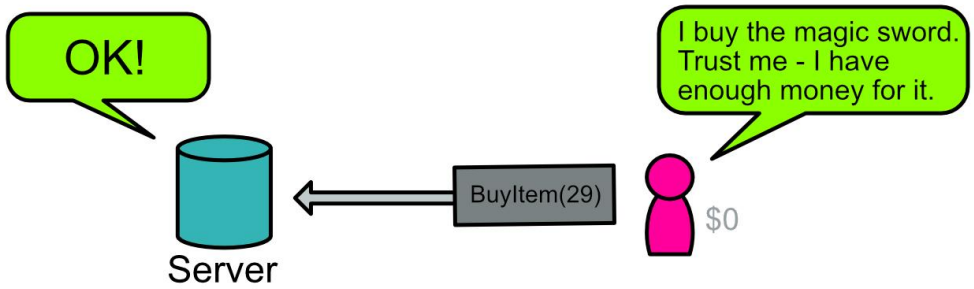
A malicious host can tamper with these.



More Threats

- Overwhelm routers with connection requests (DDOS)
- Send falsified game-state/messages to fool server





Even More Threats

- Decrypt and steal game assets and source code
- Supplement human capabilities via peripherals, scripts
- Search for bugs in failure-likely game systems

Vulnerabilities

Failure-Likely Systems

Attacking state synchronization and object instantiation over the network

ie. Animal Crossing Item Duplication

Asset under attack is the in-game economy.

Exploiting vulnerability doesn’t require modifying the game.

Network programming is difficult, need to synchronize the state of both players. Vulnerable to issues with bad-interleavings, similar to a data race.

Responding to the Threat

Cheat Detection

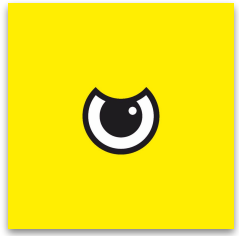
Examples

PunkBuster

Valve Anti-Cheat

Easy

Vanguard



BattleEye

Signature-based Detection

- Detection software scans running processes
- Running processes are compared to a set of known cheats and their binary signature
- If a signature match is found, action can be taken (like reporting or banning)

Problems with Signature-based Detection

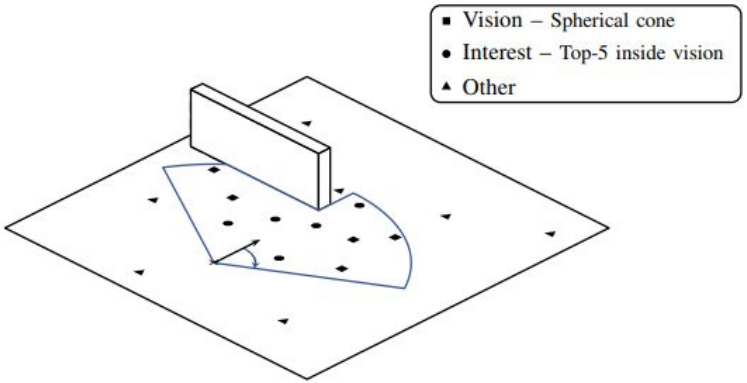
- Developers have to discover cheats manually
  - To build the signatures, they have to obtain and flag cheat binaries
  - Some binaries are kept within private forums and circles
- This can lead to bad behavior, like false positives
  - Example:
    - Binary code of a cheat posted in a discord server
    - Members of the server get banned by the anticheat running on their machines because
      it recognized the signature in an open process

Anomaly-based Detection

- Determine what a clean client looks like when it is running
- Audit the running client
  - Look for unexpected memory access or execution
- Anomalies are potential cheating
- Advantageous compared to signature-based detection
  - Don’t need a signature! Cheat agnostic
  - Just need to know what a clean client operates like

What might it look like?

- Example from a research paper showing the field of view, objects the player can see, and object they can’t
- This is tracked by the server
- Player actions and movement can then be judged based on this snapshot of what they should have known



Source: AntiCheat: Cheat Detection and Prevention in P2P MOGs

Learning-based Detection

- New! Demoed at GDC (Game Developers Conference) 2018
- Train a system using known examples of cheating, and telemetry like server logs
- Server can learn to recognize bad behavior, and point it out when monitoring live matches
- Think “Naive Bayes” project from CSE 312, where we statistically identify spam based on training data
    - Similar idea: identify cheats based on examples of cheats and cheating behavior

Comprehensive Example: Valve Anti-Cheat

- Rolled out by Valve in 2010
- Uses anomaly-based detection
  - Routinely sends “challenges to client”
    - Contains code for the client to run
  - A clean client will return a passing response within the time limit
  - Challenges are encrypted, dynamic and polymorphic, so they are very difficult to read or reverse-engineer
- Also uses server-side checking as a fall-back
  - Sanity checks as part of an “Authoritative Server”

Authoritative Server Pattern

- Client machines just cannot be trusted.
- Enforce invariants at the server, which is the only entity permitted to modify true game state.
- All client actions are verified applied to game state.
- Techniques like client-side prediction can alleviate the issue of clients needing to hear back from the server as quickly as possible to get updated game state.
- Discrepancies between client and server beliefs could be because of de-sync, not always a sign of cheating.

Responses to Cheating

Banning and Lawsuits

Why Ban?

- Increase cost of cheating (money & time)
- Dissuade players from cheating
  - Risk their account, in-game items, time invested
- Instill trust that competition is fair
  - Important for companies selling competitive games!

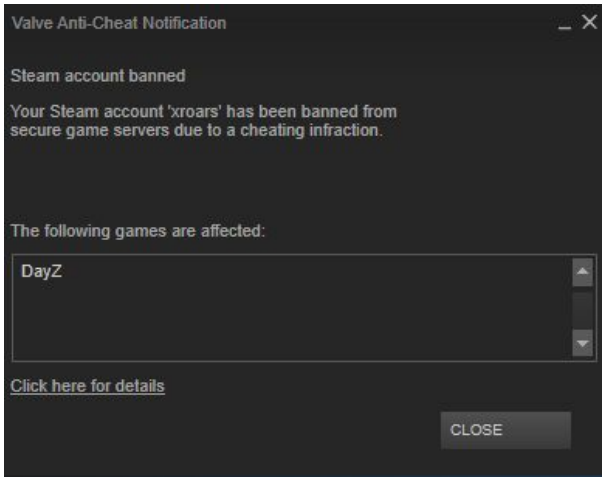


Image: VAC Ban Notification

Types of Bans

- Batch bans
  - Flag accounts and ban all-together in a “wave”
  - Lets detector run, flag accounts w/out alerting cheaters
  - Generally publicized, seen as a publicity stunt
- Account bans (email, phone no.)
- IP bans
- Hardware ID bans
- Identity/professional bans

Examples of Ban Technology: Punkbuster

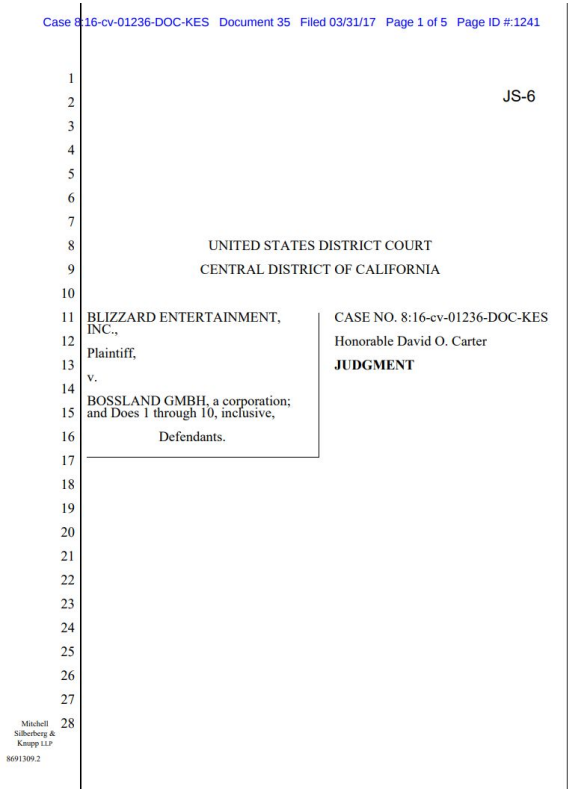
- The Punkbuster anti-cheat service implemented a ban-system based on hardware ID's (sidenote: Punkbuster uses signature-based detection)
- Punkbuster scans the system it is running on and generates a unique, digital fingerprint for it
    - All info is run through multiple one-way hashes so that identifying information (hardware serial numbers, ect) are not collected, stored, or made part of the signature directly
- When cheating is detected, that hardware ID is uploaded to a remote server
- Any game using Punkbuster automatically checks hardware ID when users log in, and denies access to users with banned IDs
- Punkbuster boasts that this new identifier will require cheaters to buy a whole new computer to keep cheating (as opposed to a new license/account)

Legality of Banning

- License to use a platform, not ownership of a game
- Bug exploits, bots, hacks, stealing code/assets, selling in-game items for profit, account boosting, account trading, advertising, cloud-computations, data mining, trading, harassment, platform disruption (including DDOS) all legal grounds for bans or a lawsuit after signing most Terms of Service.
- However, the Terms of Service as a legally binding contract is possible to dispute.

Why sue?

- Similar reasons to banning; game developers have a vested interest in protecting the integrity of their services
    - Players prefer experiences where competition is seen as “fair”
- Game developers, especially the large ones, have the resources to pursue legal action as deterrent or punishment for cheating
- Generally, targeted at companies that sell cheats, not individuals



Case 8:16-cv-01236-DOC-KES Document 35 Filed 03/31/17 Page 1 of 5 Page ID #:1241

JS-6

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

BLIZZARD ENTERTAINMENT, INC.,

Plaintiff,

v.

BOSSLAND GMBH, a corporation; and Does 1 through 10, inclusive,

Defendants.

CASE NO. 8:16-cv-01236-DOC-KES

Honorable David O. Carter

JUDGMENT

Mitchell Silberberg & Knupp LLP

8691309.2

Image: Example of a lawsuit by Blizzard Entertainment

Lawsuits: Do they work?

- Lawsuits have been won by game developers
  - Example:
    - German company Bossland sold software for Blizzard Entertainment's game Overwatch
    - The software was a "bot." It played the game for players
    - Blizzard argued that the software violated terms of service, and infringed on their IP by being an unauthorized reverse-engineering and modification of their game
    - Bossland was ordered to pay $8.6 million to Blizzard in damages for lost revenue
- It is debated whether they work
  - Going back to the example above, Bossland is still operating in Germany
    - Their website is blocked in some countries, like the UK, following the ruling
    - However, they are still distributing and selling their cheats

Sources

Research Papers

https://patents.google.com/patent/US8302199B2/en (Valve Client Challenge Patent)

https://dl.acm.org/doi/abs/10.1145/1653662.1653695 (Fides Anomaly Detection)

https://espace.curtin.edu.au/handle/20.500.11937/32304 (P2P/“Serverless” Referee)

https://dl.acm.org/doi/pdf/10.1145/1517494.1517497 (General survey of how to detect all sorts of intrusions)

Dev-blogs, Cheat Authors, Forums

http://onwarden.blogspot.com/ (Hacker analysis of Blizzard Warden)

Conference Videos

https://www.youtube.com/watch?v=hI7V60r7Jco (Easy Anti-cheat)

https://www.youtube.com/watch?v=SnRgW54EWwA (VACNET)

Additional References

A Message About Vanguard From Our Security & Privacy Teams

/dev/null: Anti-Cheat Kernel Driver - League of Legends

/dev: Anti-Cheat in LoL (& More)

Riot Games' Vulnerability Disclosure Policy

https://web.archive.org/web/20150620083446/http://www.evenbalance.com/index.php?page=announce04.php

https://www.google.com/amp/s/www.bbc.com/news/amp/technology-39490317