

Preventing multiplayer cheating

CMSC425.01 Fall 2019

Administrivia

- Midterm 2 – grades released, solution this evening
- Final demo schedule – this evening

Today's question

How to prevent cheating

Cheating ...

- Frustrates players
- Reduces in game purchases
- Causes players to quit
- Impacts paid player leagues

- Your experiences?

Consider more generally ...

- Always good to consider security
- How are games like
 - Online banking
 - Online retail
 - Social media
 - Anything networked

Cheating ...

- Frustrates players
 - Reduces in game purchases
 - Causes players to quit
 - Impacts paid player leagues
- Your experiences?
- How prevent?

Cheating ...

- Frustrates players
 - Reduces in game purchases
 - Causes players to quit
 - Impacts paid player leagues
- Your experiences?
- How prevent?

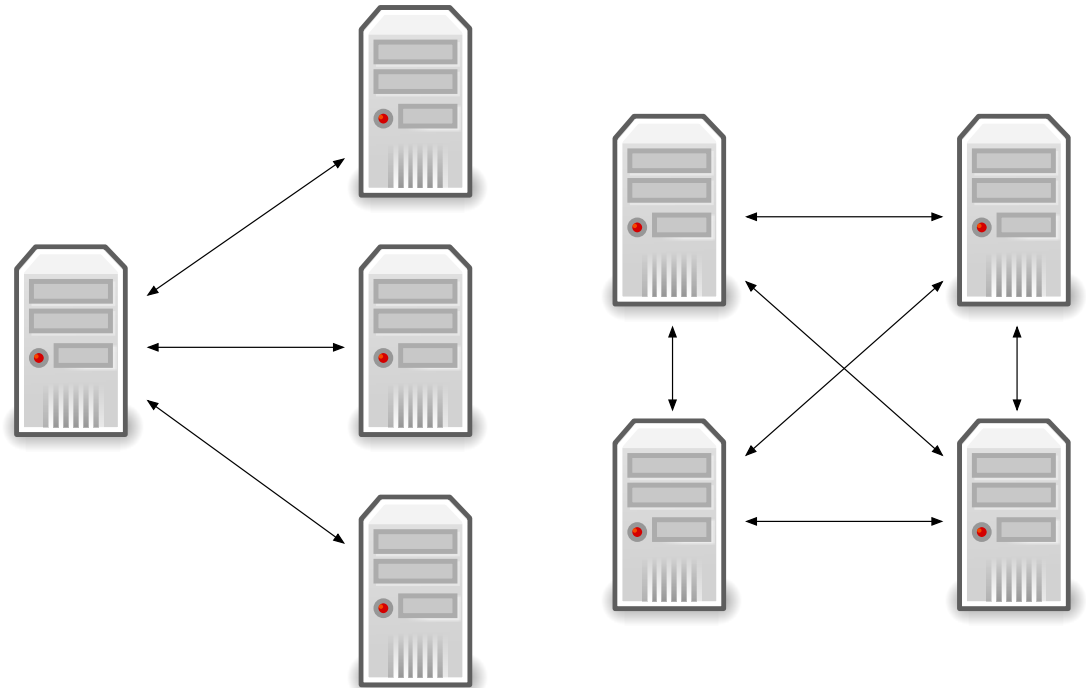
<https://www.aimforest.com/cheat-detail/call-of-duty-ghosts-hacks-aimbots-and-other-cheats>

Pritchard on Gamasutra

- If you build it, they will come to hack and cheat
- Hacking attempts increase as a game becomes more successful
- Cheaters actively try to control knowledge of their cheats
- Your game, along with everything on the cheater's computer, is not secure—not memory, not files, not devices and networks
- Obscurity is not security
- Any communication over an open line is subject to interception, analysis and modification
- There is no such thing as a harmless cheat
- Trust in the server is everything in client-server games
- Honest players would like the game to tip them off to cheaters

Network game models

- Client server
 - Client software
 - Server software
- Peer to peer
 - Identical vs. different clients
 - With or without lockstep
- Question
 - How is computation shared?



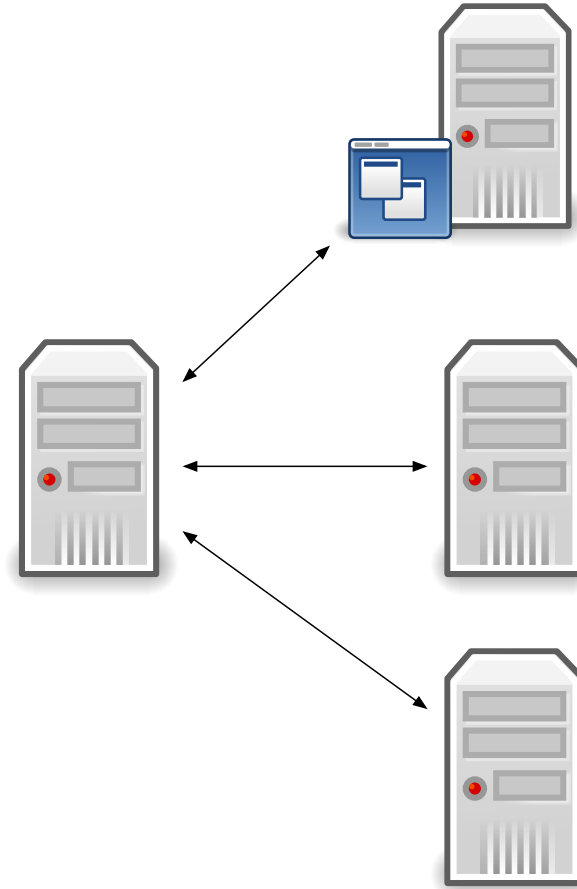
https://developer.valvesoftware.com/wiki/Source_Multiplayer_Networking

Cheating attacks

- **Reflex Augmentation:** Improve physical performance, such as the firing rate or aiming
- **Information Exposure:** Clients obtain/modify information that should be hidden.
- **Protocol cheats:** Clients capture and modify or delay packets
- **Authoritative Clients:** Although the server should have full authority, some online games grant clients authority over game execution for the sake of efficiency. Cheaters then modify the client software.
- **Compromised servers:** A hacked server that biases game-play towards the group that knows of the hacks.
- **Bugs and Design Loopholes:** Bugs and design flaws in the game are exploited. **Infrastructure Weaknesses:** Differences or problems with the operating system or network environment are exploited.
- https://en.wikipedia.org/wiki/Cheating_in_online_games

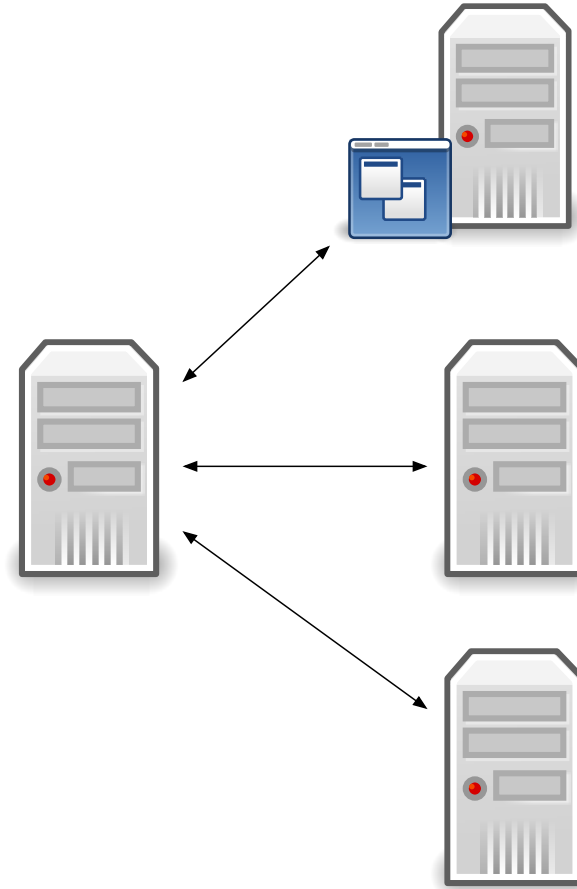
Reflex Augmentation

- Enhance client software
 - Externally capture packets
 - Modify client code
- Aimbot
- Reflex enhancer
- How detect?



Reflex Augmentation

- Enhance client software
 - Externally capture packets
 - Modify client code
- Aimbot
- Reflex enhancer
- How detect?
 - Check client executable
 - Analyze packet traffic



Information Exposure

- Access and use information not entitled to
 - Infrastructure-level cheats
- What might a cheat use?

Information Exposure

- Access and use information not entitled to
- What might a cheat use?
 - Key variables
 - Graphics hacks
 - Item properties
 - Physics behavior
 - Time (speed hack)
 - Ghosting

Key variables

- Lives, strength, health, etc.
- You have the executable – how find these variables?

Key variables

- Lives, strength, health, etc.
- You have the executable – how find these variables?
- Run program.
 - If num_lives=5, search for locations with 5
 - Get killed, find one that just decreased
- How prevent?

Key variables

- Lives, strength, health, etc.
- You have the executable – how find these variables?
- Run program.
 - If num_lives=5, search for locations with 5
 - Get killed, find one that just decreased
- How prevent?
 - Encrypt or protect key variables

Graphics hacks (removal of game elements)

- Change local graphics rendering
- Turn off rendering elements
- Eliminate fog, walls, etc



Item hacks

- Modify item properties
- Firing rate, accuracy, portion action, item frequency



Physics and speed hacks

- Change collider behavior
- Change physics engine behavior

- Control game clock

Ghosting

- Cooperation between two players
- One runs as spectator
- Informs actual player of location of other players, etc

Protocol cheats

- Interfere with network packets
 - Packets may be inserted, destroyed, duplicated, or modified
- *Suppressed update:*
 - Accept opponent packets, suppress own, to get advantage
 - Uses server policy of interpolating and backwinding
 - Prevent by monitoring patterns of packet delay

Protocol cheats

- Interfere with network packets
 - Packets may be inserted, destroyed, duplicated, or modified
- *Suppressed update:*
 - Accept opponent packets, suppress own, to get advantage
 - Uses server policy of interpolating and backwinding
 - Prevent by monitoring patterns of packet delay
- *Fixed delay:*
 - Delay all packets
 - Local players see info faster
 - Prevent by lockstep, analysis, sliding pipelines

Protocol cheats

- Interfere with network packets
 - Packets may be inserted, destroyed, duplicated, or modified
- Inconsistency: corrupt packets
- Time-stamp: post date packets
- Spoofing: sent out packets masquerading as other player

Detecting Cheating

- Signature detection - Detecting of certain patterns of bytes in memory, checked against a database
- Heuristic analysis - Statistical analysis of behavior
- User reports - Information provided by other users