Cheating in Online Games

CS 161: Computer Security

Prof. David Wagner

April 20, 2016

```
<hp:26 mo:74> west
Main Street
  You are on the main street passing through the City of Midgaard. South of
here is the entrance to the Armoury, and the bakery is to the north.  East of
here is the market square.
Obvious exits: North East South West
A cityguard stands here.
An acid blob moves around with a gurgling sound, looking for objects
to dissolve.
<hp:26 mo:72> kill guard
The Cityguard evades your attack.
<hp:26 mo:83>
The Cityguard slashes you hard.
That Really did HURT!
You miss the Cityguard with your hit.
<hp:13 mo:82>
The Cityguard wipes his boots in your face.
<hp:-6 mo:82>
You are DEAD! R.I.P.
```

Cheat #1: Reset

- Exploit bug to crash server:

  ```
  > put bag in bag
  > drop bag
  ```

- Why? Reboots server, resets all areas and creates new treasure

Cheat #2: Duplicate items

- Alice does:

```
> save
> give awesome sword to Bob
```

- Bob does:

```
> save
> put bag in bag
> drop bag
```

- Why? Both players end up with awesome sword.

Cheat #3: Injection attacks

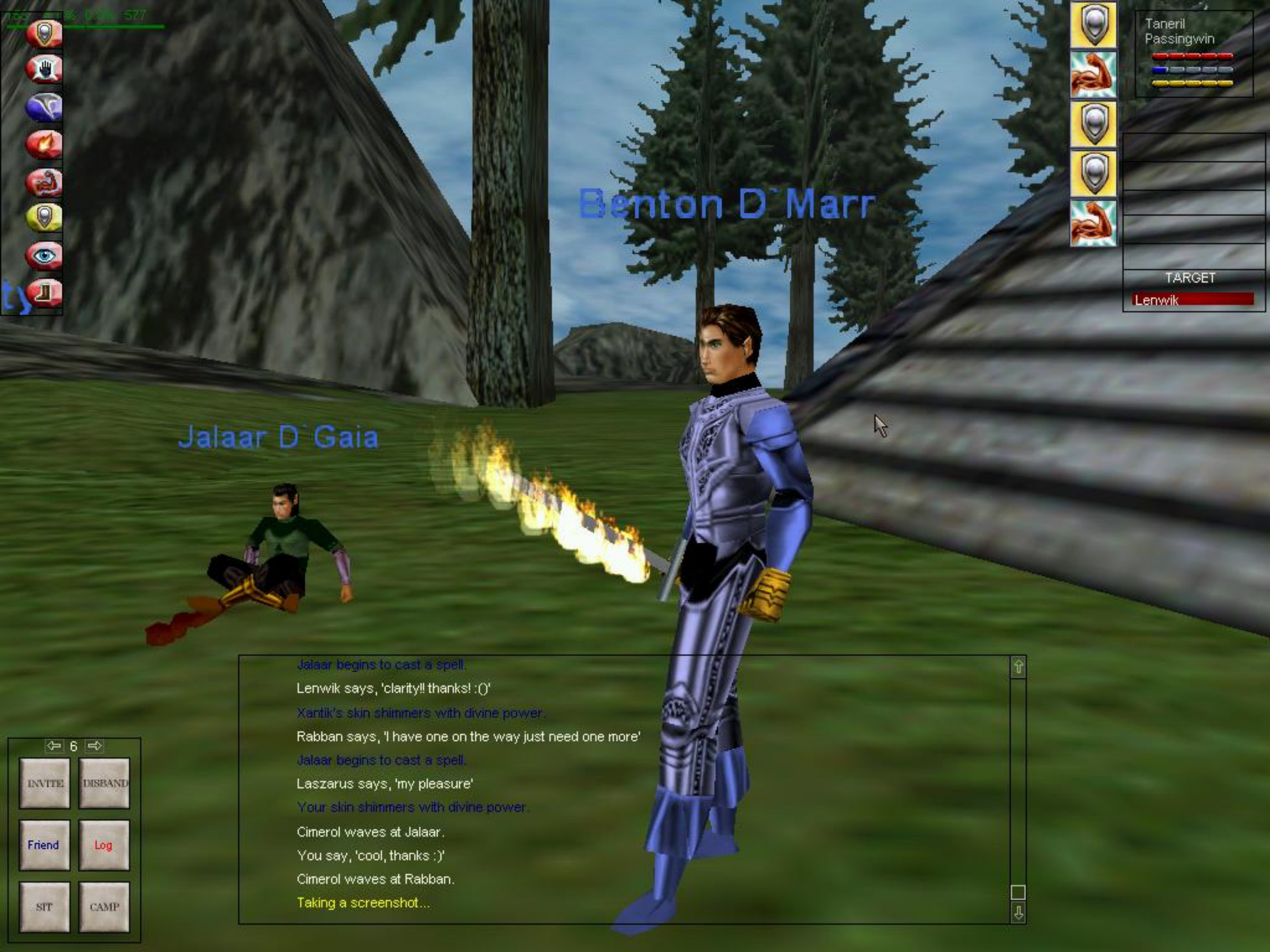
- Many people used custom clients to automate some actions. E.g., healer might use:

  ```
  $1 hits $2 very hard. -> heal $2
  ```

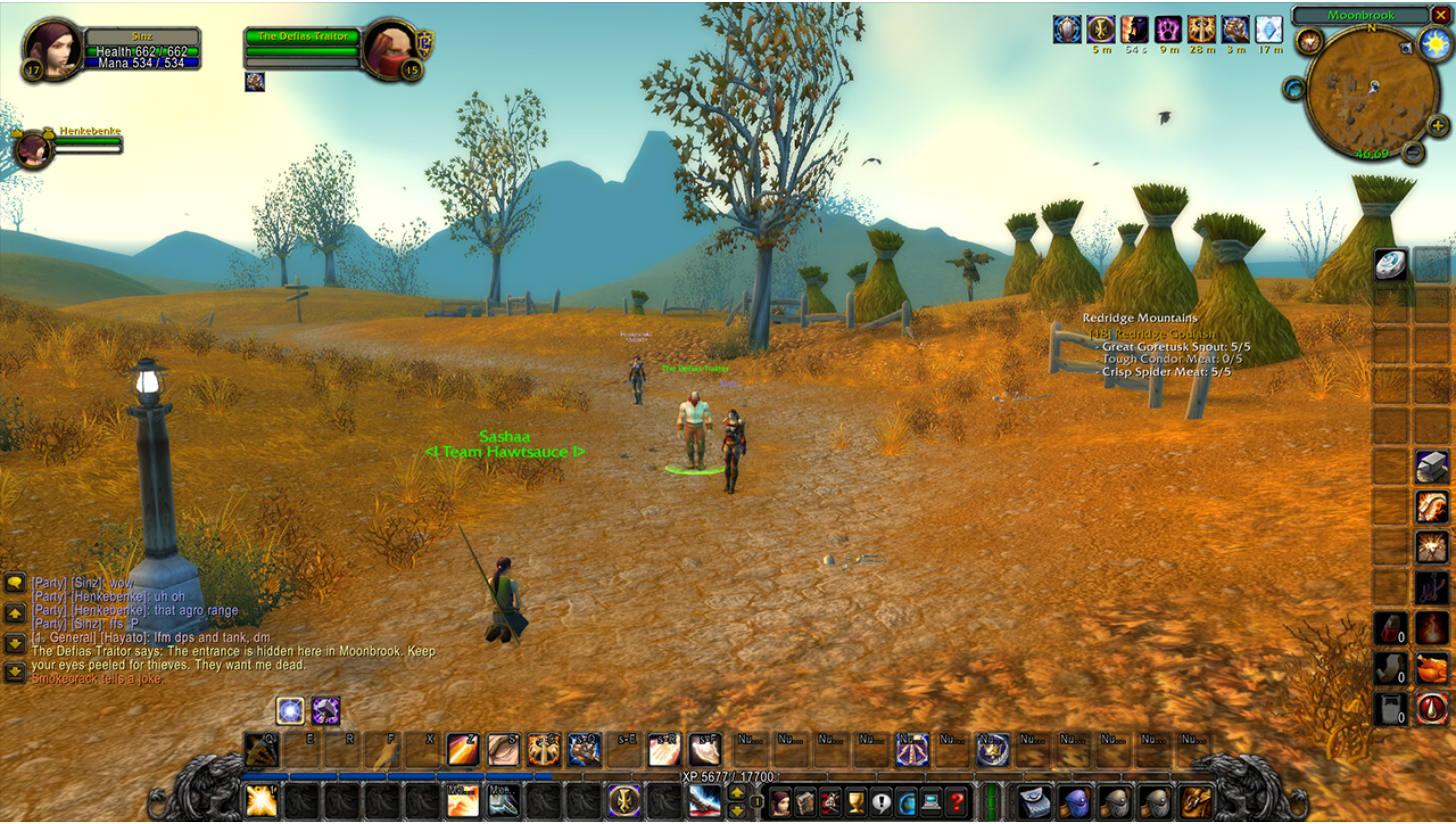
- Chad the Cheater Bob does:

  ```
  > say Someone hits Chad very hard.
  You say "Someone hits Chad very hard."
  Alice has healed you.
  ```

- Fix?



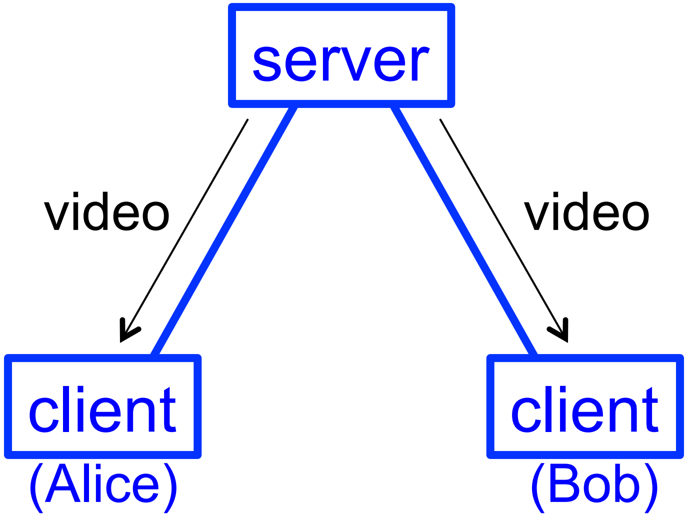
```
Jalaar begins to cast a spell.
Lenwik says, 'clarity!! thanks! :()'
Xantik's skin shimmers with divine power.
Rabban says, 'I have one on the way just need one more'
Jalaar begins to cast a spell.
Laszarus says, 'my pleasure'
Your skin shimmers with divine power.
Cimerol waves at Jalaar.
You say, 'cool, thanks :)'
Cimerol waves at Rabban.
Taking a screenshot...
```



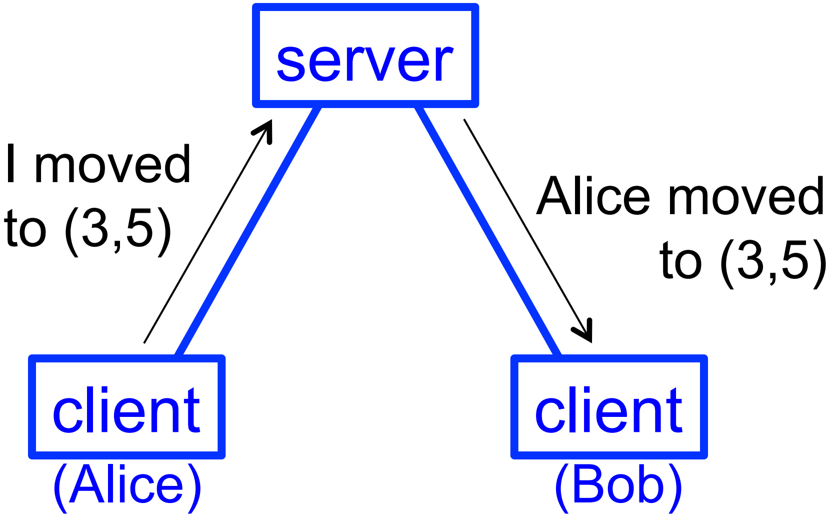
Redridge Mountains
[18] Redridge Goulash
- Great Goretusk Snout: 5/5
- Tough Condor Meat: 0/5
- Crisp Spider Meat: 5/5

[Party] [Sinz]: wow
[Party] [Henkebenke]: uh oh
[Party] [Henkebenke]: that agro range
[Party] [Sinz]: ffs :P
[1. General] [Hayato]: lfm dps and tank, dm
The Defias Traitor says: The entrance is hidden here in Moonbrook. Keep your eyes peeled for thieves. They want me dead.
Smokecrack tells a joke.

Online multiplayer games



Online multiplayer games



server

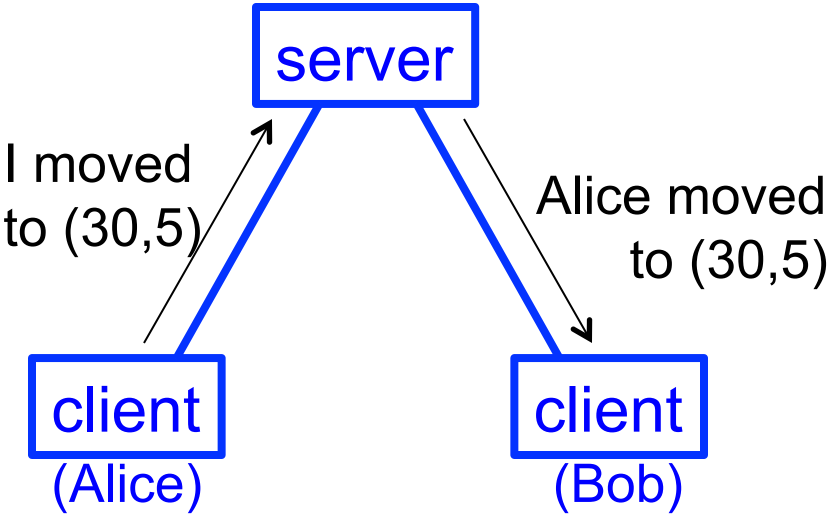
I moved
to (3,5)

Alice moved
to (3,5)

client
(Alice)

client
(Bob)

Teleportation, speed hacks



server

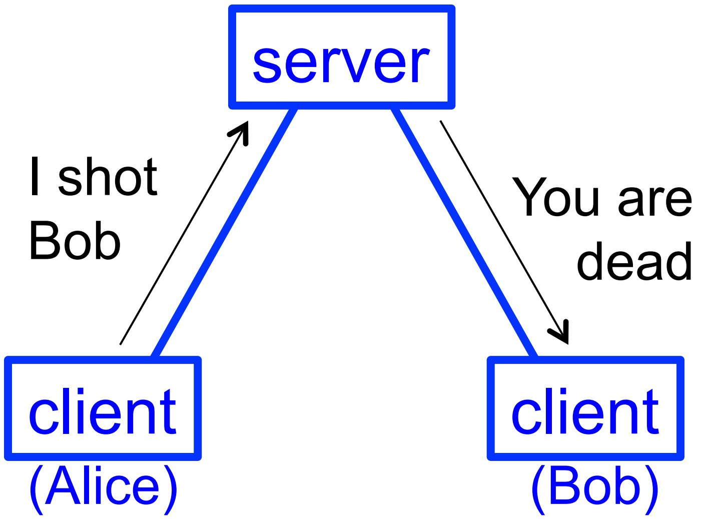
I moved to (30,5)

Alice moved to (30,5)

client (Alice)

client (Bob)

Lying clients: lies, lies, all lies



server

I shot Bob

You are dead

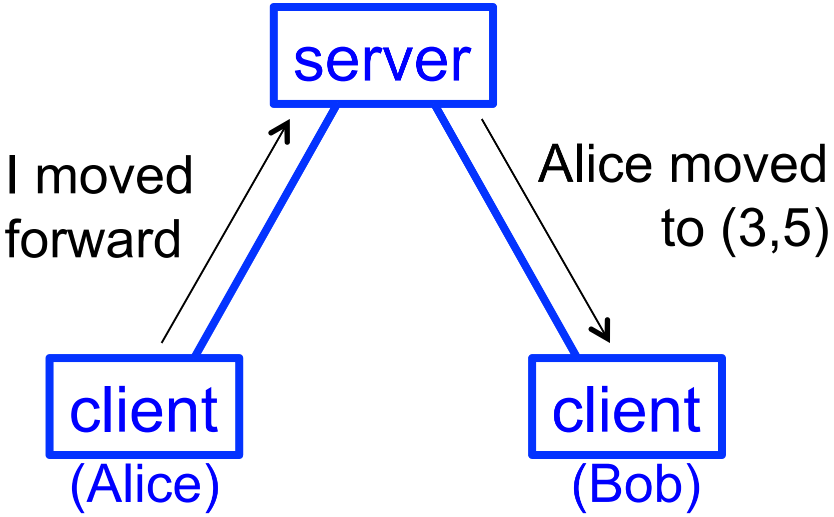
client (Alice)

client (Bob)

Solution: Authoritative Server

- Fix: Don’t trust the client. Ever.
- Server is authoritative. Client just reports inputs from user to server.

Authoritative server



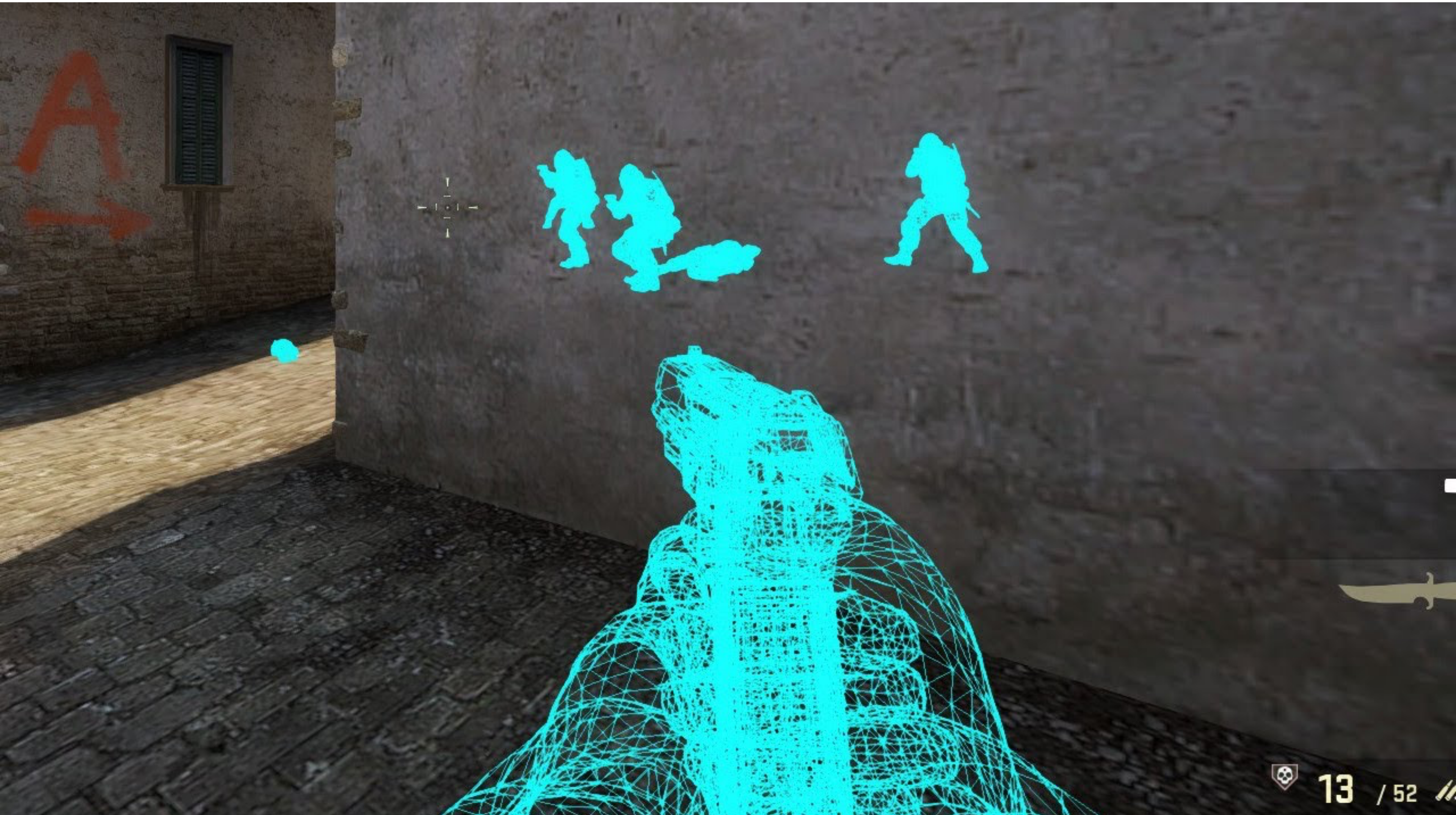
Cheat: Information Exposure

- Server might send more information than you need.

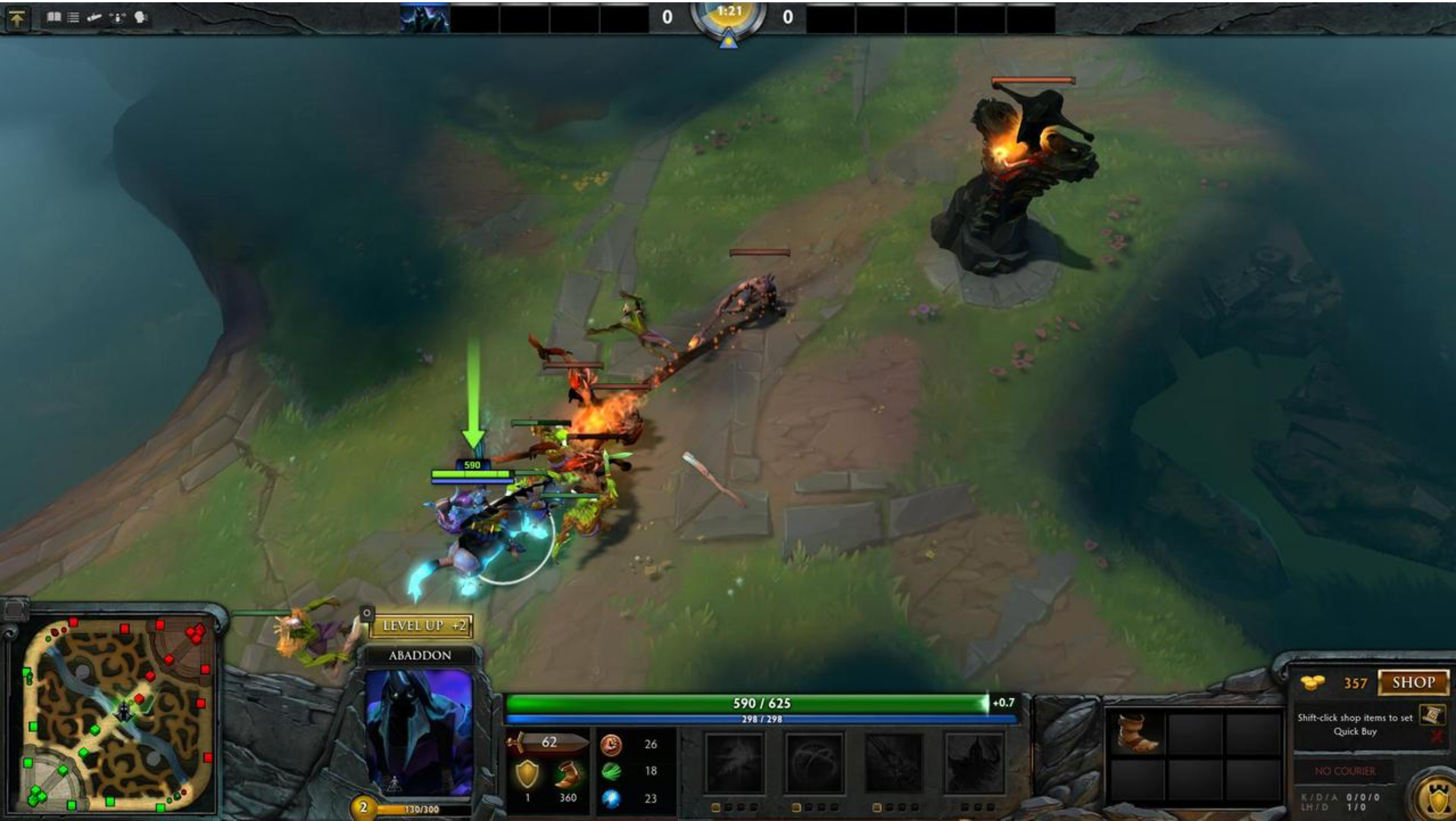
- Cheat: Hacked client might show user more information than it’s supposed to.

100
100
12 | 96

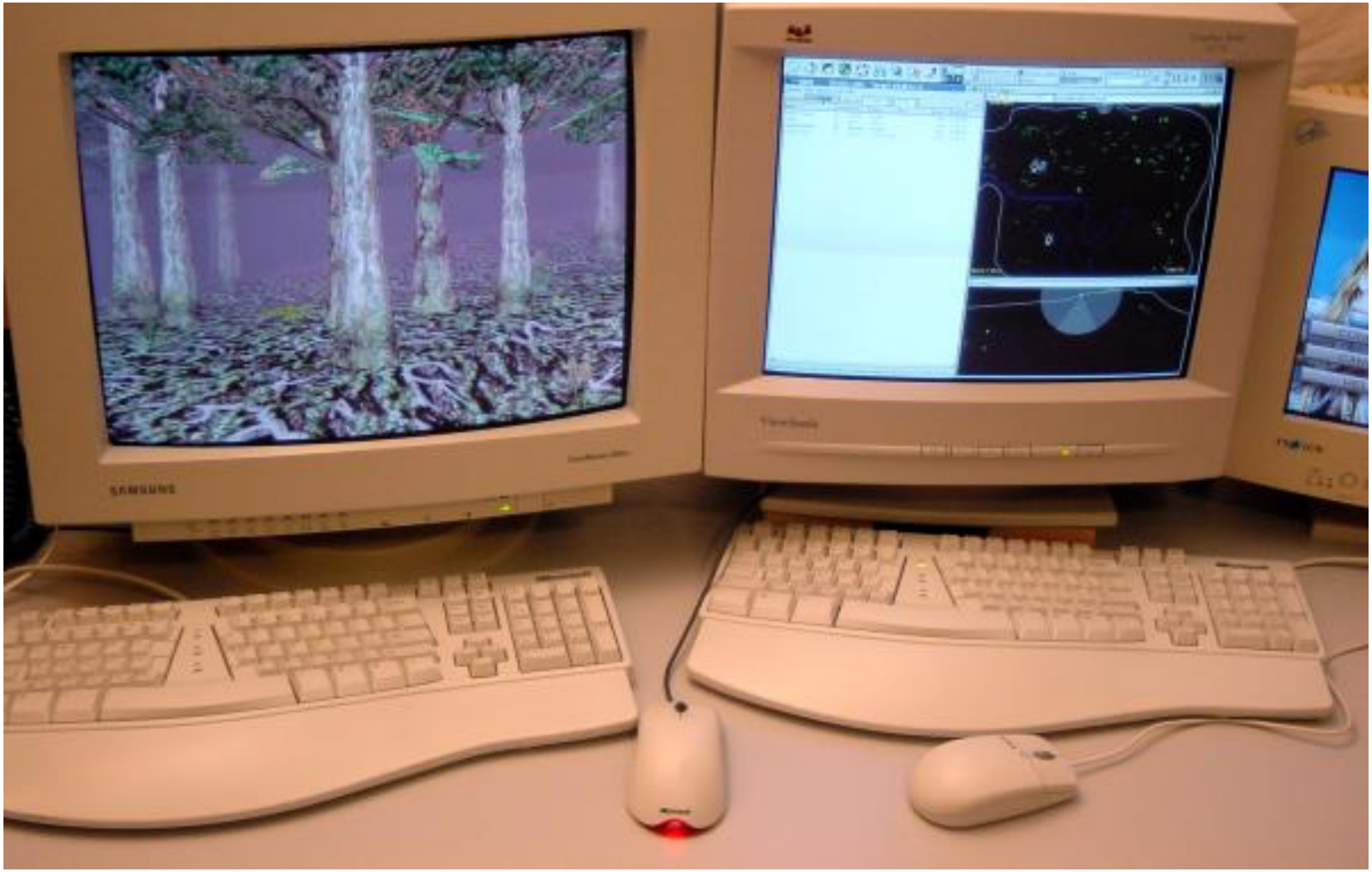
Wall hacks



Fog of war, Map hacks



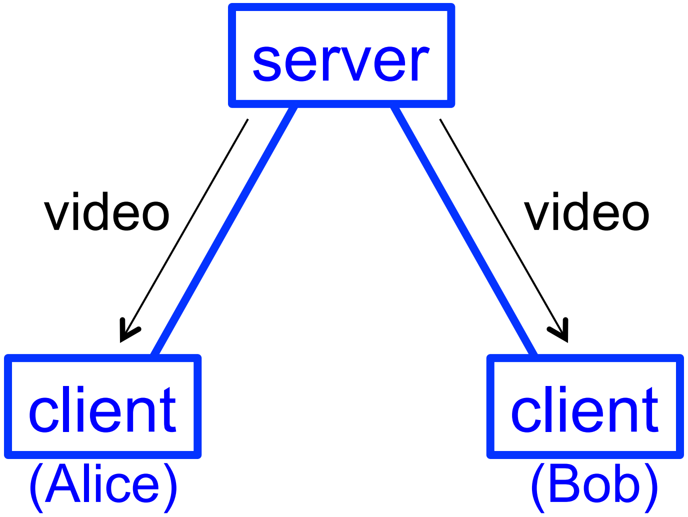
Everquest ShowEQ hack



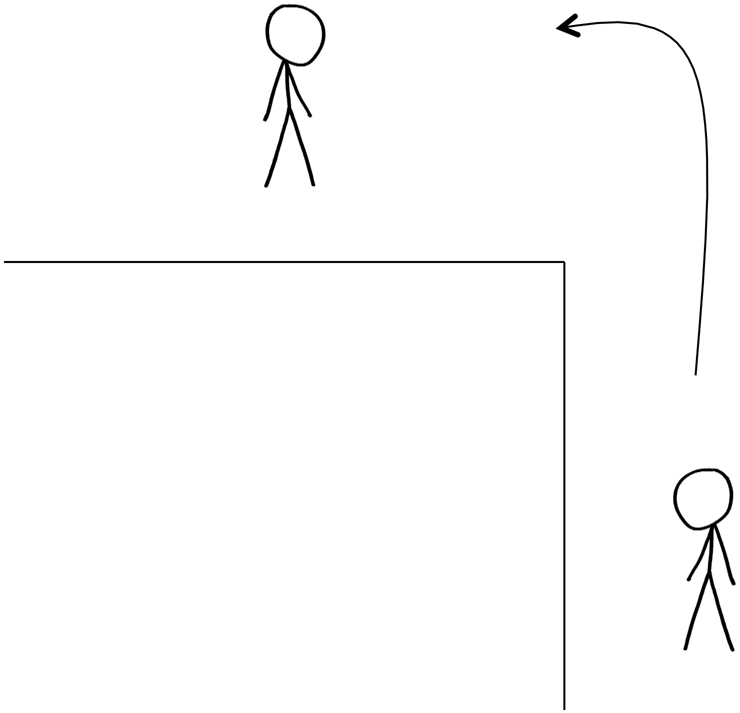
Information exposure?

- Fix?

Older network architectures (Doom)

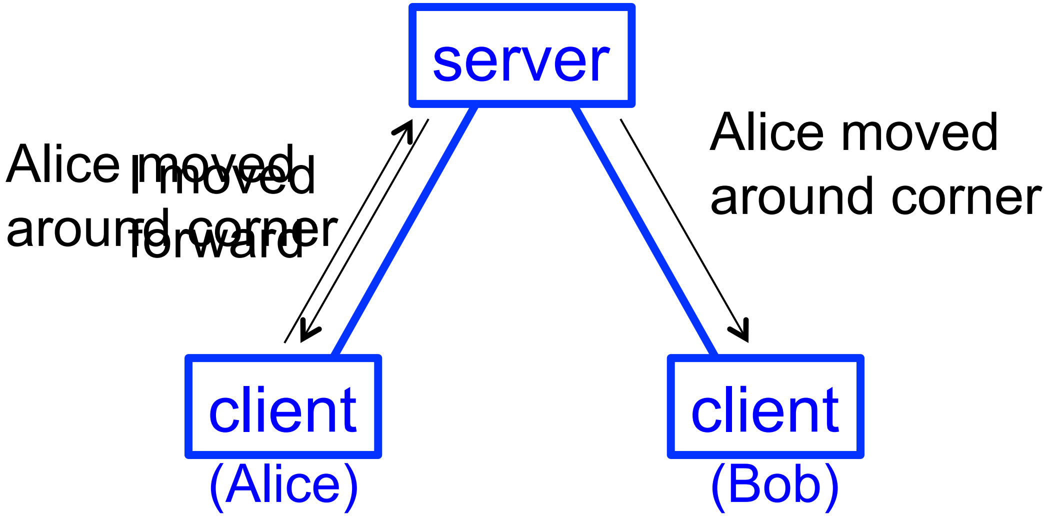


Example Scenario (FPS)



Who has
the advantage?

Older network architectures (Doom)



server

Alice moved around corner

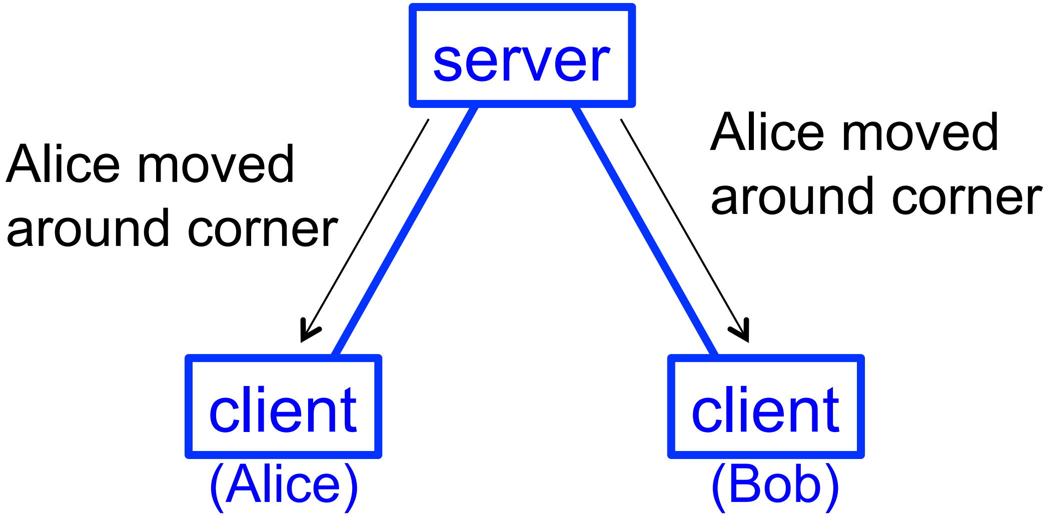
I moved forward

Alice moved around corner

client (Alice)

client (Bob)

Older network architectures (Doom)



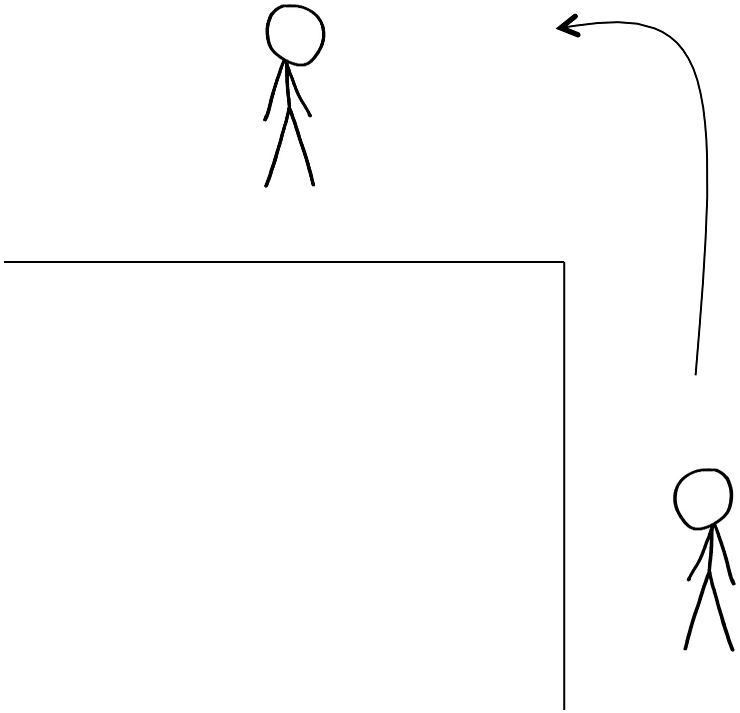
Advantage: lowest latency

Client prediction (Quake)

- Performance problem: When you press “Forward”, you don’t see yourself move forward until after 200 ms or so. This is jarring.

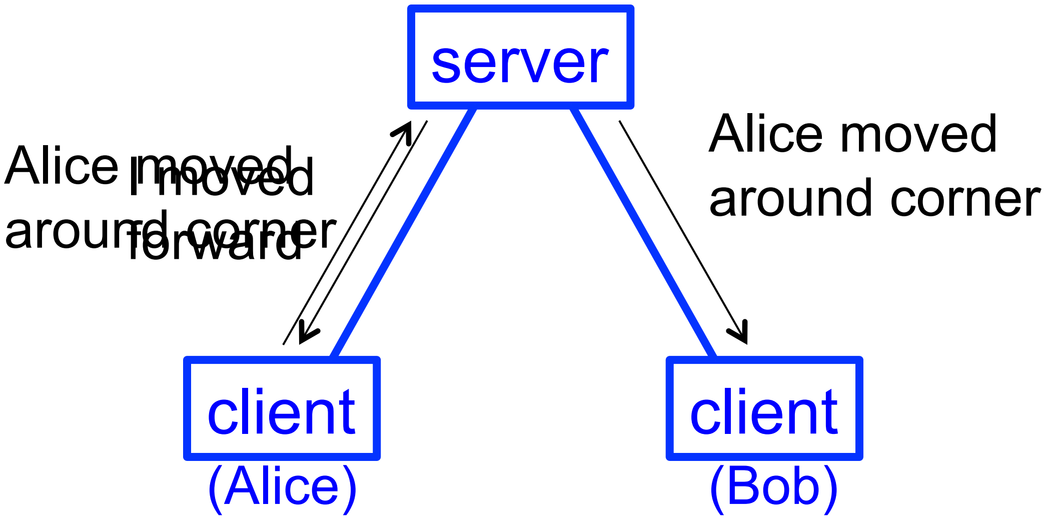
- Fix: client prediction. Client predicts effect of move, immediately moves your point of view forward (predicting what server will say). Basically, speculative execution. Server remains authoritative.

Example Scenario (FPS)



Who has the advantage?

Client prediction (Quake)



server

Alice moved around corner

I moved forward

Alice moved around corner

client (Alice)

client (Bob)

Client immediately moves Alice’s POV forward, Alice can now see Bob

Bob doesn’t see anything yet

Advantage: first mover

Cheat: Delayed updates

- Normally, Alice’s client would send:
  0ms: send “Alice moved forward”
  0ms: Alice’s display is updated, Bob is visible
  300ms: send “Alice shot at Bob”

- Bob sees:
  100ms: rcvd “Alice moved forward”
  100ms: Bob’s display is updated, Alice is visible
  400ms: send “Bob shot at Alice” (too late)

- But if Alice is a cheater, she could delay the first message by up to 300 ms…

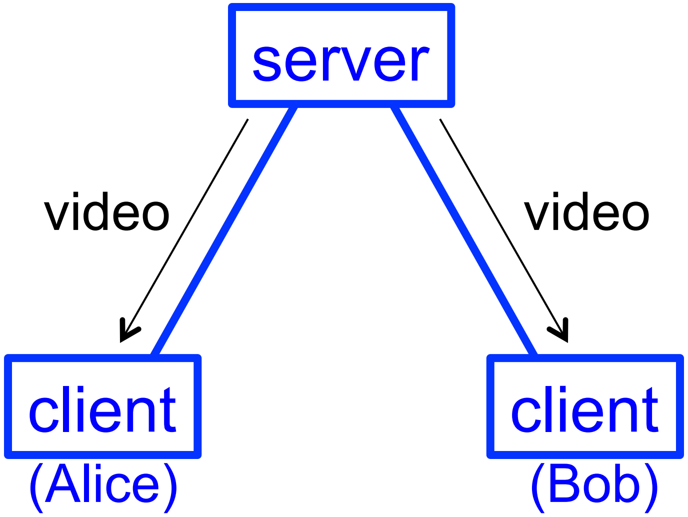
Cheat: Delayed updates

- Cheating Alice sends:
  0ms: send “Alice moved forward” (*delayed 300ms*)
  0ms: Alice’s display is updated, Bob is visible
  300ms: send “Alice shot at Bob”

- Bob sees:
  400ms: rcvd “Alice moved forward”
  400ms: rcvd “Alice shot you, you are dead”
  400ms: Bob’s display is updated (too late)

- But if Alice is a cheater, she could delay the first message by up to 300 ms…

Modern network architectures



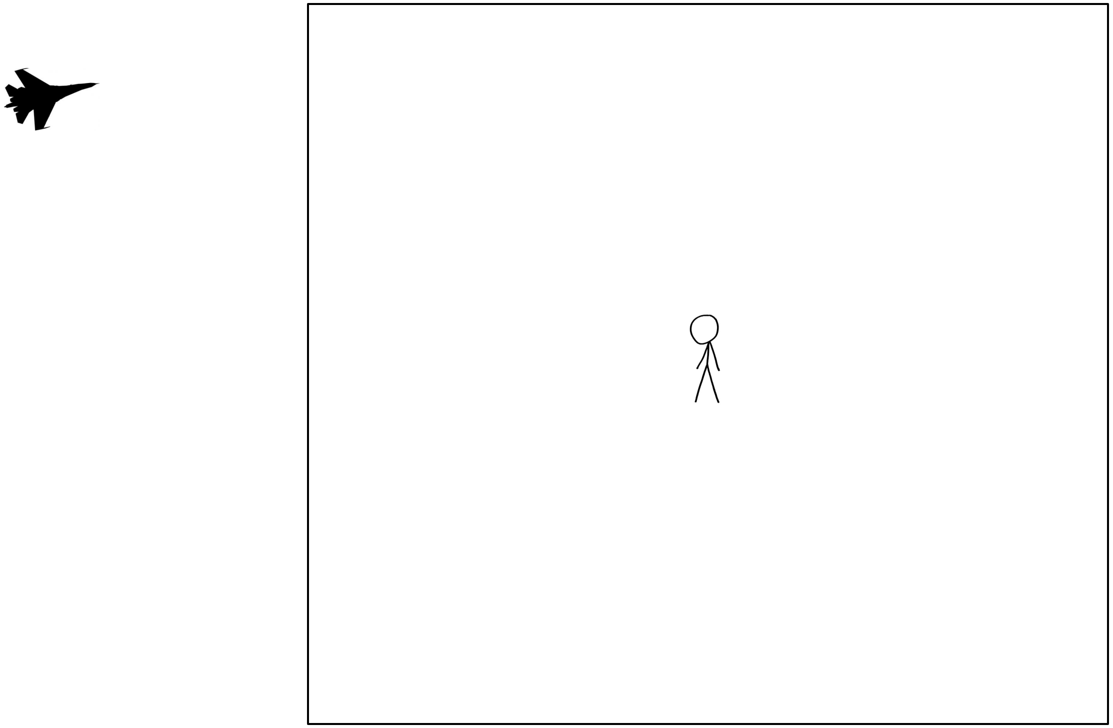
Video/updates are buffered by 200ms,
to deal with jitter.

Cheat: Information Exposure

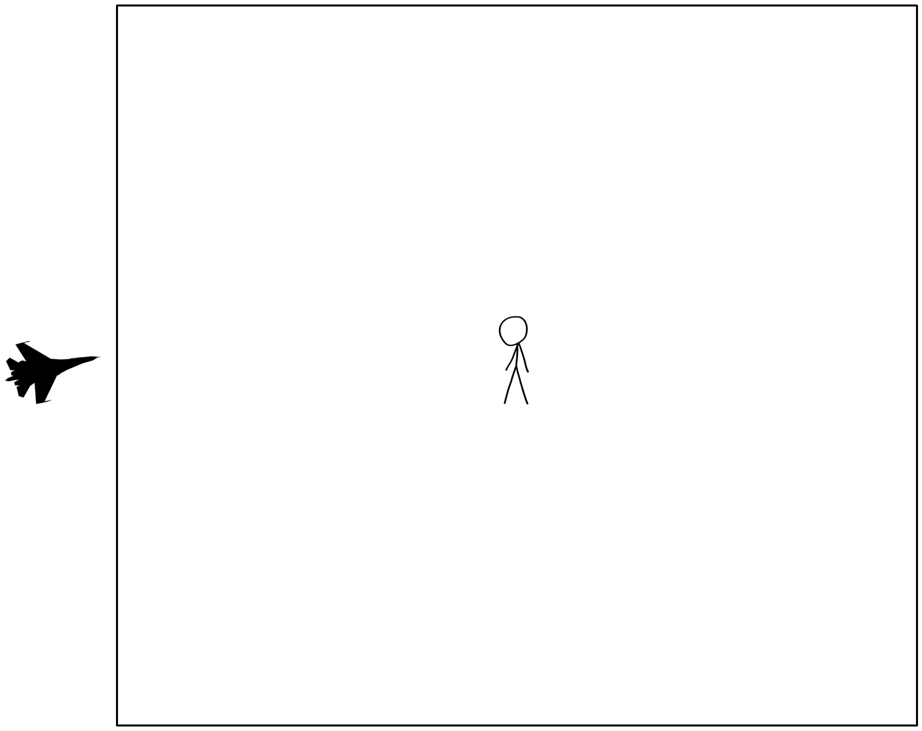
- Cheating client can “peek” at buffer to get advance notice of what’s coming (up to 200ms)

Tactic: attack clustered defenders

Interest region



Tactic: approach from NESW



Cheat: Aimbots

- Reflex augmentation: Aimbots automatically detect objects, “snap” your aim to their center of mass for you so you have perfect aim

- Fix?

Online game Take-aways

- Don’t trust the client!
- Distributed systems are hard when you can’t trust all nodes