Lecture 31

Networking: Security
## Game Networking Issues

### Consistency
- Do our games agree?
  - Where do I see objects?
  - Where do you see them?
  - Who is authoritative?
- How to force agreement?
  - Do I wait for everyone?
  - Do I guess and fix errors?

### Security
- What cheats are possible?
  - View hidden data
  - Enter invalid states
  - Improve player skill
- How do we cheat proof?
  - Technical solutions?
  - Community policing?
Network Communication

• In order to communicate
  • Must agree on expected *order* of messages
  • Must agree on expected *meaning* of messages

• **Example**: Asking for the time
  • **Successful Exchange**
    • Hi … Hi … Got the time? … It’s two o’clock.
  • **Aborted Exchange**
    • Hi … Don’t bother me. XXX
  • **Communication Mismatch**
    • Allo … Hello … Quelle heure a’til … XXX <blank stare>
Protocols

- Getting the time is an example of a protocol
  - Defines the *format* and the *order* of messages exchanged between communicating entities
  - Defines the actions expected to be taken on the receipt or the transmission of a message
- Protocol are customized to the application
  - All web browsing uses the http protocol
  - Every game will have a unique protocol
## Protocol Design

### What is Sent?

- Entire state of the game?
  - This will be slow
  - But it is easy to program

- Changes to an object?
  - Problems if we miss packets
  - Can resend with timestamps

- Only user inputs?
  - Missing packets very bad
  - Context depends on state

### When is it Sent?

- When the player requests?
  - Asynchronous web games
  - Game needs to poll a server

- At periodic intervals?
  - Turn-based strategy games
  - Game must open a socket

- At arbitrary times?
  - Real-time strategies
  - Requires multi-threading
Protocol Cheats

- Sixth-sense cheats
  - See hidden information
  - e.g. See through walls

- Rule-bending
  - Ignore game restrictions
  - e.g. Walk through walls

- Superhuman cheats
  - e.g. Auto-aim, auto-position

- Game-state editing
  - e.g. Increase resources
Protocol Cheats

- Sixth-sense cheats
  - See hidden information
  - e.g. See through walls
- Rule-bending
  - Ignore game
  - e.g. Wall
- Superhuman cheats
  - e.g. Auto-aim, auto-position
- Game-state editing
  - e.g. Increase resources

Requires packet interception!
Intercepting Network Data

- Packets can be intercepted
  - Game must see data to work
  - If can be seen, can be copied
  - Modify with other programs

- **Can intercept in the OS**
  - Networking uses a library
  - Replace it with new library

- Preventing this is difficult
  - Game must monitor your OS
  - Sony rootkit controversy
Intercepting Network Data

- Packets can be intercepted
  - Game must see data to work
  - If can be seen, can be copied
  - Modify w/other programs

- Can intercept in the OS
  - Networking uses a library
  - Replace it with new library

- Preventing this is difficult
  - Game must monitor your OS
  - Sony rootkit controversy
Intercepting Network Data

- Packets can be intercepted
  - Game must see data to work
  - If can be seen, can be copied
  - Modify w/other programs

- **Intercept at local router**
  - Home routers can be hacked
  - Newer ones run Linux

- Very difficult to prevent
  - Impossible to detect this
  - Encryption is only defense
Intercepting Network Data

- Packets can be intercepted
  - Game must see data to work
  - If can be seen, can be copied
  - Modify w/other programs
- Intercept at local router
  - Home routers can be hacked
  - Newer ones run Linux
- Very difficult to prevent
  - Impossible to detect this
  - Encryption is only defense
Preventing Protocol Cheats

• Information to display ≠ information to play

• **Example**: Object location
  • Need exact geometric positioning to draw
  • But if you have this information, can auto target
  • Greater the discrepancy, more you can cheat

• **Solution**: Give the client as little as possible
  • Server-side computation for anything important
  • P2P MMOs are unpopular for this reason
Learning this the Hard Way
The Division: Protocol of Fail

- Recall **World** v. **Local** State
  - Equipment is all local
  - Stored in a file when quit
  - File can easily be edited
- Player state is **authoritative**
  - No protocol verification
  - Server accepts edited state
  - No need to modify packet
- *The Division* is screwed
  - Fix needs new architecture
Consistency Cheats

- Cheats all have a similar feel
  - Abuse consistency algorithm
  - See opponent’s future moves
  - Modify past moves to cheat

- **Look-a-head cheat**
  - Pretend connection is slow
  - Others act as you “catch up”

- **Suppress-correct cheat**
  - Claim your move was lost
  - Use it to “undo” a bad move
Consistency Cheats

- Cheats all have a similar feel
  - Abuse consistency algorithm
  - See opponent’s future moves
  - Modify past moves to cheat

- Look-a-head cheat
  - Pretend connection is slow
  - Others act as you “catch up”

- Suppress-correct cheat
  - Claim your move was lost
  - Abuses Dead Reckoning
Look-A-Head Cheats

Player 1 is Honest

Player 2

0 50 100 150 200 250

0 50 100 150 200 250

t=0 t=50 t=100

Actual 150ms to Player 2

Player 1

0 50 100 150 200 250

0 50 100 150 200 250

t=0 t=50 t=100

Claims 150ms to Player 2

Player 1

0 50 100 150 200 250

0 50 100 150 200 250

t=0 t=100 t=150

Actual 50ms to Player 2

Networking: Security
Recall: dead reckoning
- If moves lost, predicts them
- If move received, correct
- Use correction to advantage

Example:
- Pretend lost at $t = 0, 50, 100$
- Look at opponent $50 - 150$
- Fake moves for $0 - 100$
- Consistent move at $150$
Exploits

- Cheats due to a bug
  - Due to poor architecture
  - Hard to find until release

- Typical causes
  - Insufficient refactoring
  - Multiplayer a later addition
  - Patch adds untested features

- What to do?
  - Patch, patch, patch
  - But see above

Examples

- **Duping**
  - aka Item duplication
  - Distorts game economy

- **Griefing tactics**
  - Stealing player items
  - Ambush abilities

- **Denial of service**

- **Account theft**
Item Theft: *Ultima Online*

- “Overload scam”
  - Character has a limit to how much can carry
  - Player picks up too much weight/items
  - *UO* forced the player to drop something
  - Grab it and run

- **Solution**: Don’t pick it up in the first place
  - Check item limit before grabbing item
  - But does not solve all problems…
“Black bag scam”
- Scammer initiates trade
- Bag is dyed black (*hard to see*) in trade window
- When trade completes, player is at item limit
- When unequip an item, pack cannot contain it
- Item falls to ground (*and is stolen*)

This is a **user interface exploit**
- Solutions?
Item Duping

• **Example**: Selling sword to vendor
  • Sword added to vendor’s inventory
  • Sword taken from player’s inventory
  • What if server crashes in the middle?
  • What if I know how to crash server?

• **Solution**: Database Transactions
  • But databases are too slow…
  • And designers cannot script them
Account Theft

- Account theft usually a matter of **phishing**
  - Player gets request for username and password
  - Gives it up, thinking request is official

- Phishing in *Ultima Online*
  - *UO* only has “bubble chat”
  - “Chat Window” is for system messages
  - Scammers hacked into the chat window
  - Sent out official looking messages
Account Theft

• Trojans are another possibility
  • Download a program to cheat
  • Program steals username/password

• Account theft is a big deal
  • Your character has items worth real money
  • Scammer will pick your character clean
  • Organized crime launders money this way
And Even More Cheats

- This is just skimming the surface
  - There are many more cheats than can list
  - Could probably devote a course to it
  - Requires detailed knowledge of networking

- Cheating is an “arms race”
  - The minute you learn about a cheat, it is old news

- Keep up to date on what hackers are doing
  - Search for hacks of various games
  - Read gamer/hacker forums
Community Policing

- Limited technical options
  - Eventually cheats will form
  - Can only stop them so long
- Must police community
  - Actively seek out cheaters
  - Ban them from playing
  - “Terms of Service”
- Can affect architecture
  - Player servers allowed?
  - How does policing work?
Games and Analytics

- Monitor game data for cheats
  - Check for *superhuman* players
  - Use logs to verify complaints

- **Analytics** becoming popular
  - Stream state to analytic server
  - Data mine state for information
  - Standard procedure for MMOs

- Game data is precious!
  - Game companies want it all
  - More valuable than technology
  - Another reason for online play

Networking: Security
Summary

• Cheating is a severe problem
  • Can use knowledge of the protocols
  • Can use knowledge of consistency algorithms
  • Exploits take advantage of software bugs

• Cheating is an “arms race”
  • Technical solutions are limited
  • Community policing becoming common

• Policing requires data monitoring