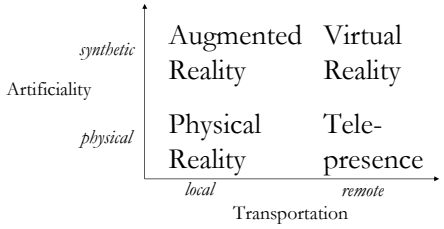
§6 Cheating Prevention

- traditional cheating in computer games
  - cracking the copy protection
  - fiddling with the binaries: boosters, trainers, etc.
- here, the focus is on multiplayer online games
  - exploiting technical advantages
  - exploiting social advantages
- cheaters' motivations
  - vandalism
  - dominance

Goals

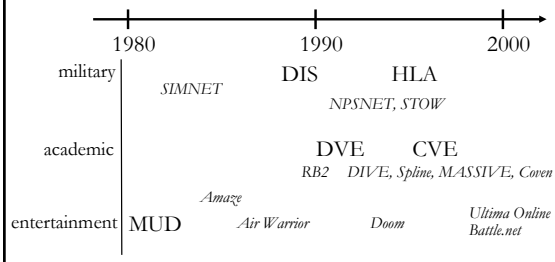
- protect the sensitive information
  - cracking passwords
  - pretending to be an administrator
- provide a fair playing field
  - tampering the network traffic
  - colluding with other players
- uphold justice inside the game world
  - abusing beginners
  - gangs

Shared-space technologies



(source: Benford *et al.*, 1998)

History and evolution



Massive multiplayer online games

Name	Publisher	Released	Subscribers
Ultima Online	Origin Systems	1997	250,000
EverQuest	Sony Entertainment	1999	430,000
Asheron's Call	Microsoft	1999	N/A
Dark Age of Camelot	Sierra Studios	2001	250,000
Sims Online	Electronic Arts	2002	97,000
Star Wars Galaxies	LucasArts	2003	N/A

(source: **www.mmorpg.com**)

Cheating methods

- tampering network traffic
- illicit information
- exploiting design defects
- collusion
- offending other players

Tampering network traffic

- reflex augmentation
- packet interception
- look-ahead cheating
- packet replay attack

Breaking the control protocol: Maladies & remedies

- *malady*: change data in the messages and observe effects
- *remedy*: checksums (MD5 algorithm)
- *malady*: reverse engineer the checksum algorithm
- *remedy*: encrypt the messages
- *malady*: attack with packet replay
- *remedy*: add state information (pseudo random numbers)
- *malady*: analyse messages based on their sizes
- *remedy*: modify messages and add a variable amount of junk data to messages

Illicit information

- access to replicated, hidden game data
  - removing the fog of war
  - compromised graphics rendering drivers
- cheaters have more knowledge than they should have → passive cheating
- compromised software or data
- counter measures in a networked environment
  - centralized: server maintains integrity among the clients
  - distributed: nodes check the validity of each other's commands to detect cheaters

Exploiting design defects

- what can we do to poor designs!
  - repair the observed defects with patches
  - limit the original functionality to avoid the defects
- client authority abuse
  - information from the clients is taken face-value regardless its reliability
- unrecognized (or unheeded) features of the network
  - operation when the latencies are high
  - coping with DoS and other attacks

Denial-of-service attack

- logic attack: exploit flaws in the software
- flooding attack: overwhelm the victim's resources by sending a large number of spurious requests
- distributed attacks: attack simultaneously from multiple (possibly cracked) hosts
- IP spoofing: forge the source address of the outgoing packets

Collusion

- imperfect information games
  - infer the hidden information
  - outwit the opponents
- collusion = two or more players play together without informing the other participants
- how to detect collusion in online game?
  - players can communicate through other media
  - one player can have several avatars

Analysing collusion

- tracking
  - determine who the players are
  - but physical identity does not reflect who is actually playing the game
- styling
  - analyse how the players play the game
  - requires a sufficient amount of game data
  - collusion can be detected only afterwards

→ no pre-emptive nor real-time counter-measures

Collusion types

- active collusion
  - cheaters play more aggressively than they normally would
  - can be detected with styling
- passive collusion
  - cheaters play more cautiously than they normally would
  - practically undetectable