


Gaming Security

Aggelos Kiayias

Online Gaming

- A multibillion $ industry. Computer games represent a 10 bn $ market.
- Single games have sold as many as 20 million copies.

MMORPGs

massively multiplayer online role playing game

http://www.cracked.com/article_15657_world-warcraft-world-10-ways-online-gaming-will-change-future.html

Money

- virtual goods cost real money: $635,000 for a virtual resort purchase in the Entropia Universe (entropia Universe money “PED” have a fixed exchange rate to USD).
- real banking moves in.

Why Security is an issue?

- Game cheating
- is profitable for cheaters.
- threatens the game business model.

Criminal Behaviors (virtual)

Computer characters mugged in virtual crime spree

11:31 18 August 2005
NewScientist.com news service
Will Knight

A man has been arrested in Japan on suspicion of carrying out a virtual mugging spree by using software "bots" to beat up and rob characters in the online computer game Lineage II. The stolen virtual possessions were then exchanged for real cash.

The Chinese exchange student was arrested by police in Kagawa prefecture, southern Japan, the *Mainichi Daily News* reports.

Several players had their characters beaten and robbed of valuable virtual objects, which could have included the Earring of Wisdom or the Shield of Nightmare. The items were then fenced through a Japanese auction website, according to NCsoft, which makes Lineage II. The assailant was a character controlled by a software bot, rather than a human player, making it unbeatable.

Criminal Behaviors (real)

Online Gamer Sentenced to Death for Murder

Dispute over the ownership of a virtual sword led to a real-life killing in Shanghai.

Peter Sayer, IDG News Service
Thursday, June 09, 2005 8:00 AM PDT

The pair had argued over ownership of a virtual sword that Qiu and another player had won in the online game "Legend of Mir III." Qiu loaned the item to Zhu, but Zhu then sold it for approximately $870.

When Qiu tried to involve the police in recovering the item or the money, he was told that such virtual items are not protected by Chinese property laws. After Zhu refused to return the item or pay compensation, Qiu went to his home and stabbed him in the heart, according to the report.

Protective Mechanisms

- Example : Punkbuster (used in Call of Duty, Quake and others)
  - real-time scanning of memory for known cheats.
  - screenshot samples.
  - encrypted status reports.

WoW

- 12 million players
- >60% of the market
- game addiction issues
- virtual economy <=> real economy :
  - 2007 a game character sold for $10,000

farming characters

- sweat shops for collecting XP's

http://youtube.com/watch?v=ho5Yxe6UVv4

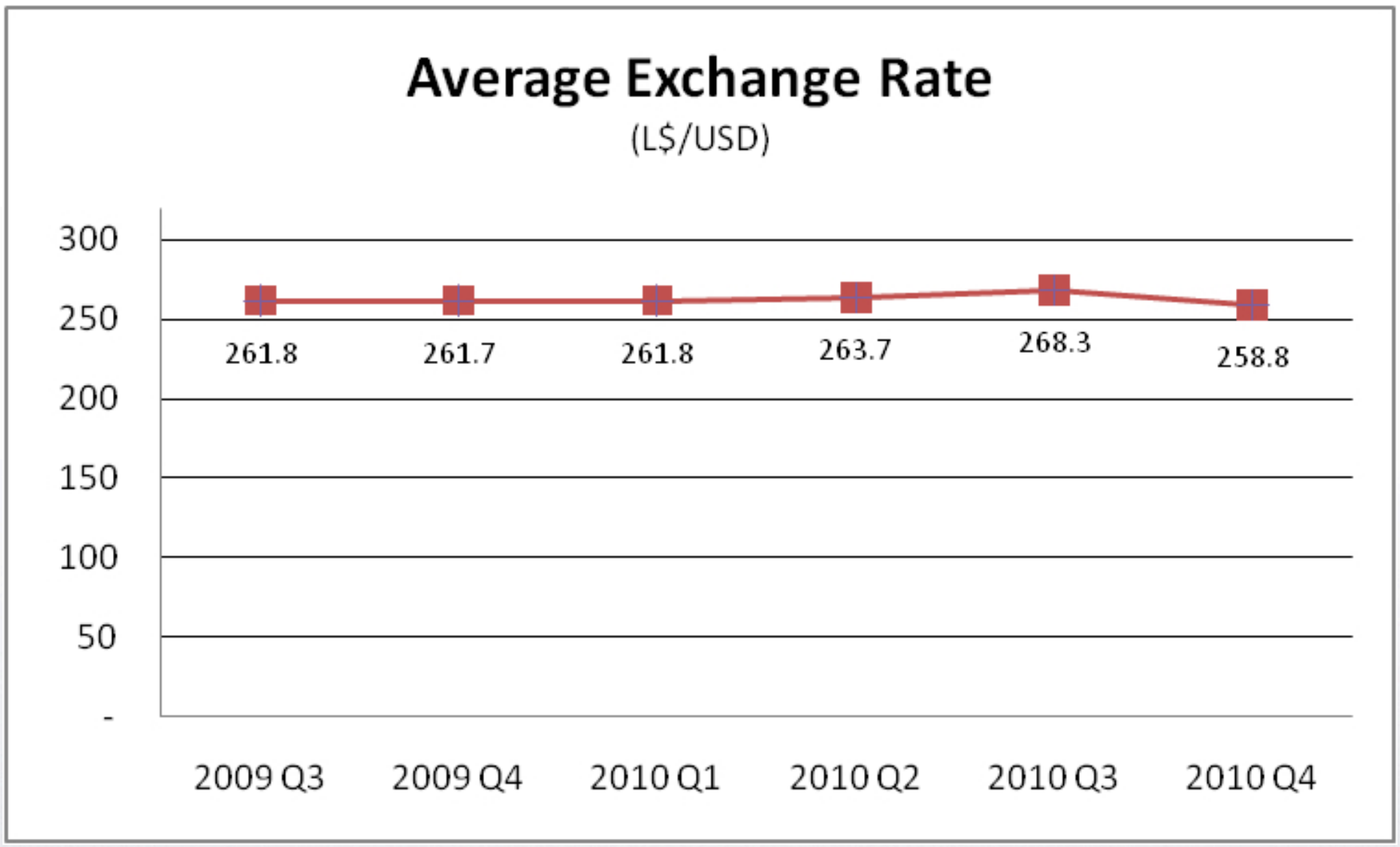
- grinding for XP's (maybe using bots)

```
// -------------------------
// hoglund's WoW_Agro Macro
// -------------------------
```

http://www.informit.com/articles/article.aspx?p=1074291&seqNum=6

highlights:
- monsters are sought & engaged.
- sampling color of pixels in screen to figure out health

Second Life



http://community.secondlife.com/t5/Featured-News/The-Second-Life-Economy-in-Q4-2010

Second Life Economy

- In 2008 there were 60000 users with positive cash flow. A small number of them were in-world-entrepreneurs making a (real) living in SL.

SL rise and fall in google trends


Second Life

- Trading of user created objects a major business (selling virtual land is another)
- Copybot : client-side hack that enables object replication.

Cheating in Poker

- In texas hold'em by ASF software the PRNG was seeded w/ msecs since midnight according to system clock!

- There are 86,400,000 msecs in a day and 52! = 8 × 10^67 possible shuffles.

- being relatively synchronous with the server can even reduce the time further. exact seed can be found by brute-force!

http://www.informit.com/articles/article.aspx?p=1074291&seqNum=3

Two-party random number generation

- Alice and Bob want to flip a coin over the phone.
- Can they do it so that nobody cheats?

Cryptographic tool : commitment scheme

Two phases : committing phase / opening phase


Blum's Coin Flipping Protocol

- Alice flips a coin b.
- Alice sends a commitment of b to Bob.
- Bob flips a coin b' and sends it to Alice.
- Alice opens her commitment of b to Bob.
- Both parties terminate with (b x-or b').

Legal Issues

- applying DMCA
- EULA
  - e.g. Frontpage 2002

"You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services, infringe any intellectual property or other rights of these parties, violate any state, federal or international law, or promote racism, hatred or pornography."

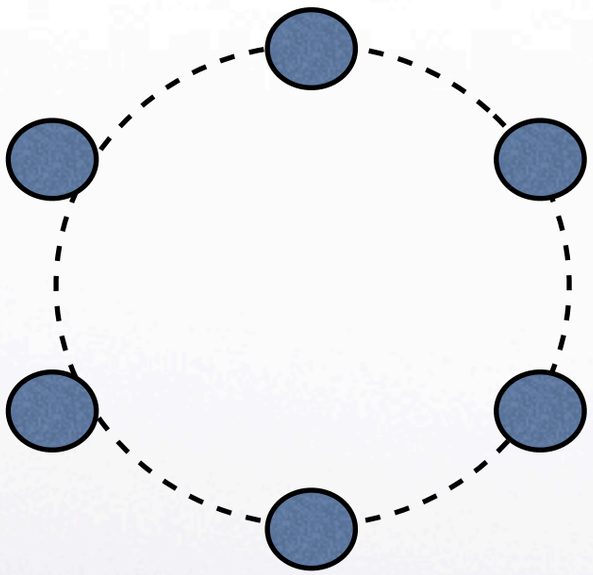
http://slashdot.org/articles/01/09/21/1438251.shtml

privacy issues

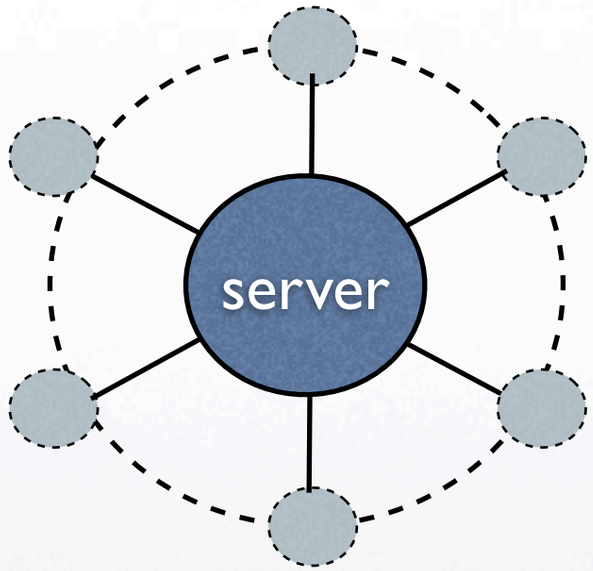
- monitoring your PC while you play.
  - e.g. *WoW warden* (among other things) monitors the window title of every active window
  - a program called 'governor' can report to you what the WoW warden is doing.

http://www.rootkit.com/vault/hoglund/Governor.zip

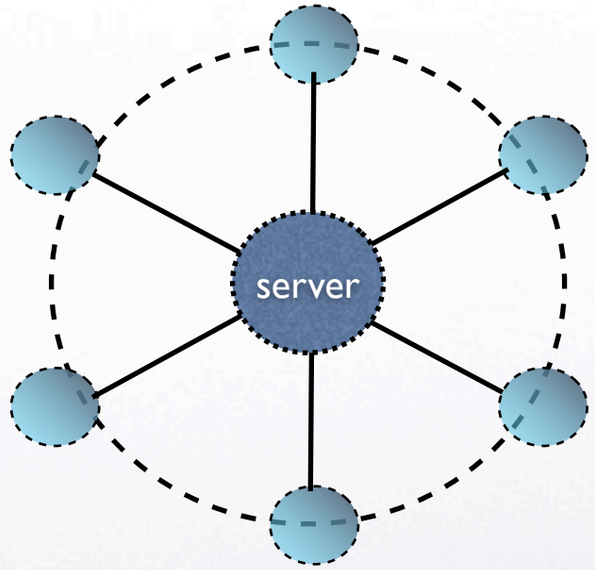
Distributing State



Real World



Ideal
Virtual World



Hybrid
Virtual World

Architecture

- Server is authoritative over clients :
  Server's state is the *true* game state.
- Player actions:
  - ask permission (server validates & updates game state)
  - do & inform later.
- Other player actions : receive regular state updates or receive when necessary.

Common Client Hacks

- Aimbotting.
- Wallhacking.
- Teleportation.
- inventory duplication.
- speed hacks.
- randomness control.

http://pimpmygame.org/

Game State Distribution

- Suppose that data {T(x,y)}_{x,y} define the game state.
- Each player at any moment is at a certain location (x,y) and its gameplay depends solely on the data T(x,y).
  - At each clock tick transmit state data to players.
    - Approach #1: Maintain each player's location locally and for each player recover (x,y) and transmit T(x,y).
    - Approach #2: Transmit {T(x,y)}_{x,y} to everyone, have the client pick up T(x,y).
      - Hybrid between two approaches possible.

Cryptographic Game State Distribution

- Is there a way to make approach #2 more secure?
  - Periodically make different keys for each cell (x,y).
  - Transmit table {T(x,y)} with each cell encrypted according to the cell key.
  - When client either moves to a new cell or its key expires it asks for the new key.

Real-Time Strategy Games

in the peer-to-peer setting

- Abusing the resource system (e.g., resources do not decrease)
- Hacking the unit list (adding new units)
- Tampering with map visibility (lifting the "fog of war")

Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, Dan Boneh: OpenConflict: Preventing Real Time Map Hacks in Online Games. IEEE Symposium on Security and Privacy 2011: 506-520

Game State in P2P

- Distinguish between the push and pull approaches. between clients.
- Push : client pushes changes to other clients.
- Pull: client pulls changes from other clients.

Cryptographic Set Intersection

- Alice and Bob have two sets A, B.
- Alice wishes to compute the intersection of the sets, so that
- Alice learns no element in B-A.
- Bob learns nothing.

P2P Game State Update

Players have units distributed in a region

- Using an SI protocol:
  - Receiving player's set is his visibility sub-region.
  - Sending player's set is the sub-region where he has units.
- Output of the protocol: sub-region where receiving player has visibility and sending player has units