MMO Reversing

Dave Kukfa
/who

- Dave Kukfa
- 3rd year
- MMO master
- Web
- Pentesting
- Reversing
- http://kukfa.co
Background

- Dungeon Runners
- Shut down in 2010
- Client still exists
- No servers to connect to
Server emulator

- Efforts to build a server emulator over the past year
  - AKA private server
- Goal: mimic the functionality of the original game’s server
- Server emulators exist for many online games
  - WoW
  - Everquest
  - Ultima Online
  - etc.
DR server components

- Authentication server
  - Logins
  - World selection
- Game server
  - Gameplay
  - Game environment (towns etc.)
  - Creating and saving characters
  - and more
Traffic flow

- Client initially connects to auth server
  - Sends back world list
- Player chooses a world to play on
- Passed to game server
- Select a character and start playing
Lots of things to implement
Easier said than done

- **Protocol analysis**
  - Analyzing traffic between the client and the server
  - Identifying what the data in each packet is controlling
  - Detecting patterns and structure
  - Encryption and custom data formatting make this difficult

- **Extremely difficult without an example**
  - Server was shut down years ago
  - No one has a network capture of actual gameplay
  - Resort to reverse engineering and guess-and-check
  - Long and tedious
Protocol analysis

---

Frame 9: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
Internet Protocol Version 4, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
Transmission Control Protocol, Src Port: 49181 (49181), Dst Port: 2110 (2110), Seq: 1, Ack: 12, Len: 50

Data (50 bytes)
- Data: 32005fe7cf9f0646c3409e98159578334d1992c6f069539b5...
  [Length: 50]
Spring break

- Took another look at the client
“L2”

- Dungeon Runners published by NCsoft
  - As are Lineage and Lineage II (other MMOs)
- Googling reveals..

![Google Search for l2crypt](https://i.imgur.com/31x336.png)
Timeline

● **Dungeon Runners**
  ○ Developed in 2005
  ○ Entered closed beta in May 2006

● **Lineage II**
  ○ Several different versions
  ○ First (Prelude) launched April 2004
  ○ Followed by C1 (June 2004) and C2 (December 2004)
Shot in the dark

- Set up a L2 server emulator
- Point the DR client at it
- See what happens
Again, easier said than done

- Trying to find Prelude/C1/C2 servers
- Not fun trying to download obscure programs made 12 years ago
  - Surfing old forums
  - Many dead links
  - Searching for mirrors
- web.archive.org is a life saver
L2J

● One of the popular L2 server emulators
  ○ Comes with auth server and game server

● Ended up using a legacy version
  ○ C1/C2 compatible
  ○ November 2004

● Thankfully archived on Sourceforge
Used to seeing this...
With L2J...
After some tweaks...
Aftermath

- Concluded that DR used L2 auth server protocols
- Clients could successfully connect to auth server
  - Passed to game server after selecting a world
- Ran into problems with the game server
  - Not responding to client packets
- Spring break ended
Current point
Positives

- Now have a working authentication server
- Huge lead for determining the rest of the game protocols
- Met a ton of devs in L2 emulator community
Tools

- IDA
- Wireshark
- Hex editor
- Lots of work by hand
  - Roll your sleeves up
Netpro

- L2 packet visualizer
  - Intercepts L2 traffic and analyzes it for you
Future work

- Revisit the game server
  - Hammer out bugs
- Determine how often game server uses L2 protocols
- Eventually recreate the game world
  - NPCs
  - Monsters
  - Quests
  - etc.
Questions?

- dxk2652@rit.edu