The bardesc CTF I've Ever Ооце

My Experiences Reverse Engineering an MMORPG

Dave Kukfa

/who

- Dave Kukfa
- Senior Computing Security student @ RIT
- Application Security
- Reverse Engineering
- https://kukfa.co
- @kukfa_

Cheeseburgers without cheese are just hamburgers

λζευdα

Project intro

- Game background
- Concept of a server emulator
- Overview of MMO reversing process
- Tools of the trade

Technical analysis

- Technical details of the reversing process
- My experiences with my specific game
- Project demo
- Legal implications
- Questions

Audience Survey

Are there any...

- MMO players?
- CTF players?
- Game hackers?

Project Incro

Game Background

- Dungeon Runners (NCSoft, 2007)
- MMORPG
 - Online game where thousands of players interact in a virtual world
- Custom game engine
 - Scrapped several times until it became Dungeon Runners
- Decommissioned in 2010
 - Lack of profit
 - Servers shut down -
- Game client has no server to connect to



Server Emulacor

- An attempt to recreate an online game's server
- Lots of proprietary components
 - Communication protocol
 - Server architecture
 - Database schemas
 - Etc.
- Involves a great deal of reverse engineering
 - Taking something apart to see how it works
 - Very long, arduous process
- Implementation is generally hacky
 - Built in a 'guess & check' fashion

Typical Reversing Process

Protocol analysis

- Determine how the client and server communicate
- Packet identification
 - Identify the different types of packets and their purpose
- Packet structure
 - "What do these bytes represent or control?"
- Encryption & checksum algorithms
- Connection handoffs
 - "At what point does the authentication server direct the client to the game server?"
- Serialization
 - "How are things like character data sent over the wire?"

0000	00	0c	29	eb	d2	55	00	0c	29	19	5a	43	08	00	45	00)U).ZCE.
0010	00	5a	02	ae	40	00	80	06	e3	ed	0a	00	00	02	0a	00	.z@	
0020	00	01	c0	1d	08	3e	74	86	30	53	23	a3	9b	f3	50	18	>t.	<s#p.< th=""></s#p.<>
0030	01	00	44	86	00	00	32	00	5f	e7	cf	9f	C6	4c	34	09	D2.	L4.
0040	e9	81	69	57	83	34	d1	99	2c	6f	06	95	39	b5	61	09	iw.4	,o9.a.
0050	f3	28	72	52	c 6	d9	b3	33	d 5	a2	22	e2	bf	a8	bd	3e	.(rR3	
0060	e5	37	57	5e	02	79	b7	f9									.7W^.y	

Typical Reversing Process conc.

Server design

- Designing massive game servers is a very complex problem
- Architecture
 - Many moving parts
 - Authentication server, game logic server, zone servers, database server...
 - Load balancing/caching
- Database design
 - SQL vs NoSQL? Schema?
- Code structure
- Scalability
- Backups/failover

Typical Reversing Process conc.

• Populate with data

- Depends on how much data is stored client-side
 - Usually the bulk of it is (good!)
- Vendor/merchant inventory
- Quest info
- Enemies in combat zones
- Loot/drops·
- If you have it particularly bad:
 - Zone layouts *
 - NPC locations
 - Dialogue

Tools of the Trade

• Disassembler

- Transforms machine language into assembly language
- Makes a compiled program (sort of) human-readable
- Static analysis
- IDA, Binary Ninja, Hopper, Radare2...
- Debugger
 - View the state of a running program
 - Current instruction, register values, memory
 - Dynamic analysis
 - IDA, OllyDbg, gdb, x64dbg...



Tools of the Trade cout.

Packet sniffer

- Capture and inspect network traffic
- Wireshark, tcpdump, Fiddler...
- Hex editor
 - Manipulate binary data (in hex form)
 - HxD, Vim, Hex Fiend...

	Edit View Go Canture Analyse	Statistics Telanha	Windles	Tools Help		
rite	Edit view oo capture Analyza	statistics relepine				
4		♥ ≌ 1 ⊻ 📃	🔳 લ લ	Q. 11		
	Apply a display filter <ctrl-></ctrl->				Expression	
No.	Time Source	Destination	Protocol	Length Info		
	343 65.142415 192.168.0.21	174.129.249.228	TCP	66 40555 → 80 [ACK]	Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827	
	344 65.142715 192.168.0.21	174.129.249.228	HTTP	253 GET /clients/net	tflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&	٨n
	345 65.230738 174.129.249.228	192.168.0.21	TCP	66 80 → 40555 [ACK]] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347	
	346 65.240742 174.129.249.228	192.168.0.21	HTTP	828 HTTP/1.1 302 Mov	ved Temporarily	
	347 65.241592 192.168.0.21	174.129.249.228	TCP	66 40555 → 80 [ACK]	Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=55181185	52
	348 65.242532 192.168.0.21	192.168.0.1	DNS	77 Standard query 0	0x2188 A cdn-0.nflximg.com	
-	349 65.276870 192.168.0.1	192.168.0.21	DNS	489 Standard query r	response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.ed	dg
	350 65.277992 192.168.0.21	63.80.242.48	TCP	74 37063 → 80 [SYN]	Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSe	ec
	351 65.297757 63.80.242.48	192.168.0.21	TCP	74 80 → 37063 [SYN,	ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=32	29
	352 65.298396 192.168.0.21	63.80.242.48	TCP	66 37063 → 80 [ACK]	Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130	
	353 65.298687 192.168.0.21	63.80.242.48	HTTP	153 GET /us/nrd/clie	ents/flash/814540.bun HTTP/1.1	
	354 65.318730 63.80.242.48	192.168.0.21	TCP	66 80 → 37063 [ACK]	Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503	
	355 65.321733 63.80.242.48	192.168.0.21	TCP	1514 [TCP segment of	a reassembled PDU]	
< > > >	Frame 349: 489 bytes on wire (39 Ethernet II, Src: Globalsc_00:30 Internet Protocol Version 4, Src	12 bits), 489 byt 1:0a (f0:ad:4e:00: 1: 192.168.0.1, Ds	es capture 3b:0a), Ds t: 192.168	d (3912 bits) t: Vizio_14:8a:e1 (00:1 .0.21	9:9d:14:8a:e1)	;
	Frame 349: 489 bytes on wire (35 Ethernet II, Src: Globalsc_00:3b Enternet Protocol Version 4, Src Jser Datagram Protocol, Src Port Jomain Name System (response) [Request In: 348]	12 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po	es capture 3b:0a), Ds t: 192.168 ort: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:e1)	>
	Frame 349: 489 bytes on wire (36 Ethernet II, Src: Globalsc_00:3t Internet Protocol Version 4, Src Jser Datagram Protocol, Src Port Domain Name System (response) [Request In: 348] [Time: 0.34333000 seconds]	12 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po	tes capture 3b:0a), Ds t: 192.168 ort: 34036	d (3912 bits) t: Vizio_14:8a:e1 (00:1 .0.21 (34036)	9:9d:14:8a:e1)	2
	Frame 349: 489 bytes on wire (35 Fithernet II, Src: Globalsc_00:3k Internet Protocol Version 4, Src Jorain Name System (response) <u>[Request In: 348]</u> [Time: 0.034338000 seconds] Transaction ID: 0x188	12 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po	es capture 3b:0a), Ds t: 192.168 ert: 34036	d (3912 bits) t: Vizio_14:8a:e1 (00:1 .0.21 (34036)	9:9d:14:8a:e1)	>
	Frame 349: 489 bytes on wire (35 Fthernet II, Src: Globals_00:34 Internet Protocol Version 4, Src Ster Datagame Protocol, Src Port Domain Name System (response) <u>[Request In: 348]</u> [Time: 0.03333000 seconds] Transaction ID: 0x2188 > Flags: 0x81880 Standard query	12 bits), 489 byt 0:0a (f0:ad:4e:00: 0: 192.168.0.1, Ds 0: 53 (53), Dst Po response, No erro	r capture 3b:0a), Ds t: 192.168 rt: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:el)	`
	rame 349: 489 bytes on wire (3 Ethernet II, Src: Globalsc_00:3 Internet Protocol Version 4, Src Sarr Datagram Protocol, Src Port Domain Name System (response) [<u>Request In: 348]</u> [Time: 0.03330000 seconds] Transaction 10: 08/2188 > Flags: 0x8180 Standard query Questions: 1	12 bits), 489 byt :08 (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po response, No erro	r r r r r r r r r r r	d (3912 bits) t: Virio_14:8a:e1 (00:1 .0.21 (34036)	9:9d:14:8a:el)	>
	Frame 349: 489 bytes on wire (36 thternet II, Src: Globals_00:34 Internet Protocol Version 4, Src Josen Datagam Protocol, Src Port Jonain Name System (response) [<u>Request In: 343]</u> [Transaction ID: 002180 Y-lags: 005180 Standard query Questions: 1 Answer RS: 4	112 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po response, No erro	r	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:e1)	>
	rame 349: 489 bytes on wire (3 thermet II, Src: Globalc_00:34 Limbernet Protocol, Src Port Domain Name System (response) <u>ERequest In: 3481</u> [Time: 0.03330000 seconds] Transaction 10: 0x2180 > Flags: 0x6180 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9	12 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po response, No erro	res capture 3b:0a), Ds t: 192.168 rt: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:el)	
	rame 349: 489 bytes on wire (3 Ethernet II, Src: Globals_00:34 Internet Protocol Version 4, Src Jaser Datagram Protocol, Src Port Domain Name System (response) [Request In: 348] [Time: 0.034338000 seconds] Transaction 10: 0x2188 > Flags: 0x8188 Standard query Questions: 1 Answer RS: 4 Authority RB: 9 Additional RS: 9	12 bits), 489 byt :0a (f0:ad:4e:00: :: 192.168.0.1, Ds :: 53 (53), Dst Po response, No erro	res capture 3b:0a), Ds t: 192.168 ort: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:e1)	
	rame 349: 489 bytes on wire (3 thermet II, Src: Globalc.00:31 Jser Datagram Protocol, Src Port Domain Hame System (response) [Request in 1482] [Time: 0.034308000 seconds] Tranasciton 10: 08/280 > Flags: 08/880 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9 Additional RRs: 9 V Queries	12 bits), 489 byt 12 bits), 489 byt 1:0a (f0:ad:4e:00: 1: 132.168.0.1, Ds 1: 53 (53), Dst Po response, No erro	res capture 3b:0a), Ds t: 192.168 ort: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 0.21 (34036)	9:9d:14:8a:e1)	
	rame 349: 489 bytes on wire (35 Ethernet II, Src: Globalsc_00:34 Internet Protocol Version 4, Src: Jaser Datagram Protocol, Src: Port Domain Name System (response) [Request In: 348] [Time: 0.034330000 seconds] Transaction 10: 042188 > Flags: 040180 Standard query Questions: 4 Authority RRs: 9 Additional RRs: 9 > Con-onfixing.com: type Å,	12 bits), 480 byt :0a (f0:ad:4e:00: : 192.168.0.1, Ds : 53 (53), Dst Po response, No erro class IN	res capture 3b:0a), Ds it: 192.168 irt: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:el)	>
	rame 349: 489 bytes on wire (3 thermet II, Src: Globalc.00:31 Internet Protocol Version 4, Sr Jser Datagram Protocol, Src Port Jonain Name System (response) [<u>Requert In: 343</u>] [Time: 0.034330000 seconds] Tranasciton 10: 042180 > flags: 04080 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9 Additional RRs: 9 V Queries > con-0.nflximg.com: type A, Answers	12 bits), 489 byt :00 (f0:ad:4e:00: : 192.168.0.1, Ds : 53 (53), Dst Po response, No erro	res capture 3b:0a), Ds t: 192.168 rt: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 0.21 (34036)	9:9d:14:8a:el)	
	<pre>rame 349: 489 bytes on wire (35 Ethernet II, Src: Globalsc_00:3b Internet Protocol Version 4, Src: Sher Datagram Protocol, Src: Port Domain Name System (response) [<u>Bequest In: 3481</u> [Time: 0.034330000 seconds] Transaction 10: 0x2188 > Flags: 0x8180 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9 Additional RRs: 9 Queries > con-0.nflxing.com: type A, > Answers</pre>	12 bits), 489 byt :0a (forad.4c:00: : 192.106.0; : 53 (53), Dst Po response, No erro class IN	es capture 3b:0a), Ds t: 192.168 rt: 34036	d (3912 bits) t: Virio_14:8a:el (00:1 .0.21 (34036)	9:9d:14:8a:el)	2
<	<pre>rame 349: 489 bytes on wire (3) thermet TI, Snc: Globalce.00:31 internet Protocol Version 4, Src Jser Datagram Protocol, Src Port Damain Name System (response) (Enqueri In: 143] Transaction ID: 002188 > Flags: 003188 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 Additional RRs: 9 Vgerlas > con-0.nflxing.com: type A, Answers > Authoritative nameservers > Que 15 00 25 46 46 01 c7 03</pre>	12 bits), 489 byt :0a (f0:ad.4e:00: : 192.108.03; : 53 (53), Dst Po response, No erro class IN	es capture 30:0a), Ds t: 192.160 rt: 34036 r	d (3912 bits) t: Vicio_14:8a:el (00:1 (34036)	9:9d:14:8a:el)	
<	Frame 349: 489 bytes on wire (3 Ethernet II, Src: Globalc_00:81 Einternet Protocol Version 4, Src Ber Datagram Protocol, Src Port Domain Hame System (response) [<u>Request In: 3481</u> [Time: 0.03330000 seconds] Transaction 10: 0x2188 > Flags: 0x6180 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9 Additional RRs: 9 > Queries > Answers > Authoritative nameservers > Authoritative nameservers 10: 00: 15: 00: 55: 46: 46: 10: 76: 33 0: 00: 40: 40: 00: 60: 40: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 40: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76: 37 10: 00: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 40: 17: 76 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 56: 36: 46: 56: 36 10: 00: 00: 00: 00: 56: 36: 46: 56: 36	12 bits), 489 byt :0a (fo:ad.4e:00: : 192.168.0; : 53 (53), Dst Po response, No erro class IN 37 <u>21 06</u> 81 80 00 6 2d 30 07 6e 66	es capture 30:00), Ds t: 192.160 rt: 34036 r r	d (3912 bits) t: Virio_14:8a:el (00:1 0.21 (34036)	9:9d:14:8a:el)	2
<	rame 349: 489 bytes on wire (3 Ethernet II, Src: Globalsc_00:34 Ethernet Protocol Version 4, Src: Jaser Datagram Protocol, Src: Port Domain Name System (response) [Request In: 348] [Tmanaction 10: 0x2188 > Flags: 0x8180 Standard query Questions: 1 Answer RRs: 4 Authority RRs: 9 > Cdn:0.nfflxing.com: type A, > Answers > Authoritative nameservers 0 00 15 00 35 04 f4 01 c7 83 0 00 04 00 09 00 09 06 53 64 0 78 09 64 07 80 53 65 f6 d0	12 bits), 489 byt :0a (f0:ad:4e:00: : 192.108.0; 153), Dst Po response, No erro class IN 57 21 06 81 80 00 6e 2d 30 07 6e 66 00 01 00 01 ce 66	es capture 3b:0a), Ds t: 192.168 rt: 34036 r r 015 6c 06	d (3912 bits) t: Vico 14:8a:el (00:1 (34036)	9:9d:14:8a:el)	>
2002 0002 0003 0004 0003 0004 0003 0004 0003 0004 0003 0004 0003 0004 0003 0004 0003 0004 0003 000000	<pre>Frame 349: 489 bytes on wire (3) thermet II, Src: 610balc_00:31 internet Protocol, Src Port Domain Hame System (response) [Enquart In: 348] [Time: 0.03330000 seconds] [Tenanaction 10: 0x2180 > Flags: 0x6180 Standard query Questions: 1 Answer RRs: 4 Authority RR: 9 Additional RRs: 9 > Queries > Authoritative nameservers 0 00 15 00 35 84 f4 01 c7 83 > 40 64 00 90 09 05 63 64 0 76 95 66 07 93 63 64 64 07 76 95 66 07 93 63 64 64 0 76 95 66 07 98 62 76 0 02 90 2</pre>	12 bits), 489 byt :0a (f0:ad.4e:00: : 192.108.0 (53), Dst Po : 53 (53), Dst Po class IN 3f 21 00 81 80 00 class IN 3f 21 00 81 80 00 6 69 6d 61 67 55	es capture 3b:0a), Ds t: 192.168 rr: 34036 r r 015 6c 00 xing 72	d (3912 bits) t: Viro_14:8a:el (00:1 0.21 (34936)	9:9d:14:8a:e1)	>

Technical Analysis

What I bad to Work With

- Dormant game client
- No game server protocol documentation
 - We'll talk about this in a bit
- No packet captures
- But!
 - Debug symbols
 - Verbose log output

	config
	DFData
-	logs
\$	dbghelp.dll
Ć	DungeonNCLauncher.exe
Ð	DungeonRunners.exe
3	DungeonRunners.pdb
3	fmodex.dll
	game.pkg
7	game.pki

Function name	Segmen
Participation Provide the state of the s	.text
🛃 DRAuthClient::SelectGameServer(int)	text
🛃 DRAuthClient::OnConnected(netAddress &)	.text
🛃 DRAuthClient::OnDisconnected(void)	.text
🛃 DRAuthClient::OnConnectionFailed(uchar)	.text
街 DRAuthClient::RecvLoginFail(uchar)	.text
DRAuthClient::RecvBlockedAccount(uint)	.text
DRAuthClient::RecvLoginOk(dm_loginInfo const &)	.text
DRAuthClient::RecvServerListEx(uchar,std::vector <dm_serverinfo< td=""><td>.text</td></dm_serverinfo<>	.text
🛃 DRAuthClient::RecvServerFail(uchar)	text
🛃 DRAuthClient::RecvPlayFail(uchar)	.text
🛃 DRAuthClient::RecvPlayOk(uint,uint,uchar)	.text
🛃 DRAuthClient::RecvAccountKicked(uchar)	.text
DRAuthClient::RecvBlockedAccountMsg(std::vector <dm_blockinf< td=""><td>.text</td></dm_blockinf<>	.text
ADDAUCT ID COOL ID COL ID	

	12/09	09:50:39.875	832:	DRAuthClient::Login Connecting to Auth: '206.127.154.204:2110'
	12/09	09:50:39.875	832:	DRAuthClient::Login changed state from 0 to 1.
	12/09	09:50:40.171	2332:	DRAuthClient::OnConnected changed state from 1 to 2.
	12/09	09:50:40.328	2332:	DRAuthClient::RecvLoginOk LoggedIn as simic024
	12/09	09:50:40.328	2332:	DRAuthClient::RecvLoginOk changed state from 2 to 3.
F.	12/09	09:50:40.500	2332:	DRAuthClient::RecvServerListEx changed state from 3 to 4.
	a second s			

Scarcinς Ouc

- Game only ran if launched from the publisher's game portal
- Looked at command-line options
 - ran_from_launcher
- Looking through config folder
 - DungeonRunners.cfg
 - Specifies authentication server addr/port
 - Direct the client to connect to local server

Dun	geonRunners.cfg 🖸
1	[AuthServer]
2	Address = auth.dungeonru



nners.com

IDA View	-A 🔛 Hex V	/iew-A	🛍 Exports 🛍 Imports N Names 🎢 Functions "" Strings 🕺 Structures 🖪 En Enums
Address	Length	Туре	String
"" .rdata:0	00000050	С	fmodSampleManager::Init Unknown Sound InputFileType '%s' in the config
"" .rdata:0	00000028	С	http://www.dungeonrunners.com/join.html
"" .rdata:0	00000018	С	.\\DungeonNCLauncher.exe
"" .rdata:0	00000056	C	%s /LauncherArgs=\" /LaunchGame=%s /StartLocation=\\\"{_stub_dir}\\\" \" ran_from_launcher
"" .rdata:0	0000002D	С	Failed to launch %s in %s with last error %u
"" .rdata:0	00000011	С	

Auch Server Drococol

- So the client can connect to our custom auth server...
 - Now we need to understand the protocol
- Looking through functions list

🖹 IDA View-A 🔛 Hex View-A 🏂 Exports 🎼 Imports	Names 谢	Functions ""	Strings 🐧
Function name	Segment	Start	Length
IinAQLogoutPacket::~IinAQLogoutPacket(void)	.text	00797EC0	0000001D
IinAQLogoutPacket::Serialize(stoChunkFileWriter &)	.text	00797EE0	00000029
👔 linAQLogoutPacket::Unserialize(stoChunkFileReader &)	.text	00797F10	0000004A
BL2BlowfishEncrypt::Blowfish_decipher(ulong *,ulong *)	text	00797F60	00000488
2 L2BlowfishEncrypt::Blowfish_encipher(ulong *,ulong *)	.text	007983F0	00000486
12BlowfishEncrypt::InitializeBlowfish(uchar * const,short)	.text	00798880	00000121
2 L2BlowfishEncrypt::BlowfishEncrypt(uchar *,int)	.text	007989B0	00000023
2 L2BlowfishEncrypt::BlowfishDecrypt(uchar *,int)	.text	007989E0	00000023

- 'lin' and 'L2' prefixes
- Right next to authentication functions

Lin and L3

- Some quick Googling reveals these refer to Lineage II
 - Another NCSoft MMO (2003 present)
 - Several releases over the years
 - Game has been reverse engineered and publicly documented
- Could DR have borrowed L2's auth server?
 - Each major L2 release had a different protocol
 - Find an early version of the server and see if it works
- Hunted for an L2 server from around the same time period
 - Easier said than done
 - Old forums/dead links
 - archive.org is a life saver
- Found legacy auth server from 2004

Used to seeiny ...



AFCER L2



Re-Implementation

- DR did use L2's authentication protocols
 - This turns out to be a common practice for NCsoft MMOs
- While DR and the L2 server shared the same protocols, the L2 server was (obviously) built for L2
 - Not 100% compatible out of the box
 - Some things didn't work
- Instead of changing L2 code, let's build our own auth server!
- Good news: L2's protocols have been reversed and publicly documented
- Bad news...

Ic's never easy

Протокол Lineage II

Автор: TechnoWiz@rd Последнее редактирование: 23 ноября 2007

Содержание

};

<u>1. Общие сведения</u> <u>2. Пакеты Client -> Login Server</u> <u>3. Пакеты Login Server -> Client</u> <u>4. Пакеты Game Server -> Client</u> <u>5. Пакеты Client -> Game Server</u>

1. Общие сведения

Каждый пакет состоит из размера пакета(2 байта), типа пакета(1 байт) и блока параметров(переменная длина). авторизации, в конце добавляется контрольная сумма и дополняется нулями так, чтобы размер пакета был кратен 8быть рассчитана следующей функцией:

unsigned long checksum(unsigned char *packet, int count)

```
long chksum = 0L;
for( int i = 0; i < count; i += 4 ) chksum ^= *((unsigned long *)&raw[i]);
return chksum;
```

Rosecca Scone

• After much help from Google Translate, I had a basic working prototype

- Client logs in
- Server sends a list of game servers (worlds)
- Client selects a world and connects to it
- Issue: Client authentication packet did not follow protocol spec
 - Having trouble extracting player credentials
 - Username & password were unintelligible blobs of data
 - Needed to figure out how credentials were being encrypted

Finding Encryption Routine

; public: int __thiscall ncAuthClientImpl::SendLogin(char const *, char const *, unsigned int, unsigned short)
?SendLogin@ncAuthClientImpl@@QAEHPBD0IG@Z proc near



?DesWriteBlock@L2DESEncrypt@@YAXPAXH@Z ; L2DESEncrypt::DesWriteBlock(void *,int)

; void __cdecl L2DESEncrypt::DesKeyInit(char const *)
?DesKeyInit@L2DESEncrypt@@YAXPBD@Z proc near

ad the second		
	loc_7	9765B:
>	mov	dl, ds: <mark>byte_8534B4</mark> [eax]
Sall	xor	<pre>byte ptr [esp+ecx+0Ch+var_C], dl</pre>
	lea	<pre>ecx, [esp+ecx+0Ch+var_C]</pre>
	inc	eax
+	cmp	ds: <mark>byte_8534B4</mark> [eax], 0
	jnz	short loc_797647

And the key is...

Aud che key is...

.rdata:	008534B4	aTest	db	'TEST',0
.rdata:	008534B4			
.rdata:	008534B9		db	0
.rdata:	008534BA		db	0
.rdata:	008534BB		db	0

...TEST with 4 null bytes

Credencial Encryption

- Algorithm: DES
- Symmetric Key: TEST + 4 null bytes
- Mode of Operation: Take a guess, given our track record
 - Yeah, ECB
- Block size: 64 bits (8 bytes)
 - This presents an interesting problem `



L2 Losin specifications

- Max username length: 14 characters
- Max password length: 16 characters
- Total size: 30 characters \rightarrow 30 bytes
 - ASCII encoded
- DES block size: 8 bytes
 - Can encrypt data with sizes 8 bytes, 16 bytes, 24 bytes, 32 bytes...
- What happens when the credential size isn't perfectly divisible by 8?
 - You might think it's padded to round up?

Nope!

- Username: 14characterusr
- Password: 16characterpassw
- Network traffic:



Ouwards

- At this point, the authentication server was pretty much figured out
- When the player selects a game server:
 - Game client will disconnect from the auth server
 - Attempts to connect to the game server
- Game server uses a custom (undocumented) protocol
 - Where do I start?

Scarcinς Ouc

Tried to mimic the protocol of the auth server

- Didn't get too far (two different protocols)
- Good: Verbose game logs pointed out what was wrong
 - Can use this to fix problems and work out correct packet structure

04/19 10:30:59.138 3236: DRAuthClient::SelectGameServer changed state from 4 to 5. 04/19 10:30:59.164 3236: DRAuthClient::RecvPlayOk changed state from 5 to 8. 04/19 10:30:59.175 3236: DFCSocketChannel::updateReceiveQueue Closing socket 10.0.0.1:7777 because packet size 3277056 exceeds max 1048576 04/19 10:30:59.192 3236: GatewayClient::UpdateAuthorize Lost connection during Authorization.

• 3277056 = 0x320100

- Find where in the packet I'm sending these bytes
- Modify it and see what happens afterwards

Ic's noc always easy

- The game doesn't log every issue it has when things don't work
- Often need to dive in with a debugger and fix things
 - Identify functions related to the issue you're having
 - Get an idea of what each function is doing
 - "Are there any checks that are failing?"
 - "What is the expected value of this (register | return value | ...)?"
 - Set a bunch of breakpoints

•

- Compare actual values to expected values
- Can be very time-consuming and frustrating
 - That's why these projects take so long to complete
 - If the high-level code was spaghetti, you'll become real familiar with these steps

Dacket Structures

- Eventually identified 4 different packet structures
 - Small tweaks between each variant
- Example:
 - 1. [1 byte] Packet type
 - 2. [3 bytes] Unknown data
 - 3. [4 bytes] Compressed size of packet data + 4 (little-endian)
 - 4. [4 bytes] Uncompressed size of packet data (little-endian)
 - 5. [Variable] Zlib-compressed packet data
- Different 'packet types' hold the same data, but are assigned to a specific packet structure
 - e.g. Packet type 0x02 can only be used with packet structure #4

Chaunel Types

- Packet data starts out with a 1-byte 'channel type'
 - Essentially identifies what component of the game server we're talking to
- Started filling in different values for the channel type and seeing what happens
- Identified a bunch of different channels:
 - CharacterManagerClient
 - Character selection
 - ClientEntityManager-
 - Game entities
 - ZoneClient
 - Entering and leaving different zones (essentially maps)

Channel δαca

- After the channel type, we can start feeding data to be sent to that channel
- Usually starts with an identifier for the packet we'll be sending
- e.g. for CharacterManagerClient:
 - 0x00: Connected
 - 0x01: Disconnected
 - 0x02: CharacterCreated
 - 0x03: GotCharacter -
 - 0x04: Enter Character Creation Screen
- This is followed by additional data for that packet
 - e.g. a list of the player's characters, a serialized character...

Current State

- After piecing enough of these together, I was able to get some basic game functionality
 - Character serialization
 - Creating a character
 - Sending character list
- There's still a lot to be done
 - Loading into a zone
 - Creating game entities
 - Other players
 - Monsters
 - Synchronizing multiple clients
 - Properly architect the server

Project demo

Lesal Implications

Game Company Scances

• They (usually) don't like it

- Large game companies will fight tooth and nail over intellectual property
- Indie studios might be more relaxed, but it's a toss-up

• Some famous examples:

- (2016) Nostalrius shut down
 - WoW private server with 150k+ active users
- (2012) UMaple lawsuit
 - Ordered to pay \$3.6M to Nexon
- (2009) Scapegaming lawsuit
 - Ordered to pay \$88M to Blizzard
- (2008) Glider Bot lawsuit
 - Ordered to pay \$6M to Blizzard

NCSoft Distory

- (2006) Lineage II FBI investigation & home raid
- (2007) City of Heroes Cease & Desist
- (2010) Aion C&D
- (2011) Tabula Rasa C&D
- (2012) Exteel C&D
- (2014) Lineage I C&D

EFF Exemptions

- EFF landed recent DMCA exemption for video game archiving
- Proposed to reduce legal uncertainty of reversing games for preservation purposes
- Catch: Not intended to apply to games with persistent worlds
 Literally the definition of MMORPGs
- Interpretation has been debated
- General consensus is the exemption does not apply to MMO server emulators

Case For Ounseon Runners

- Attempts to purchase IP have gone nowhere
- Continue reversing the game
- Avoid piracy
 - Don't distribute the game client
 - Don't use NCSoft-owned server code
- Not meant to be commercial
 - Only intend to restore gameplay
- Hope for the best

Quescious?

Thank you!

dkukfa@mail.rit.edu https://kukfa.co @kukfa_