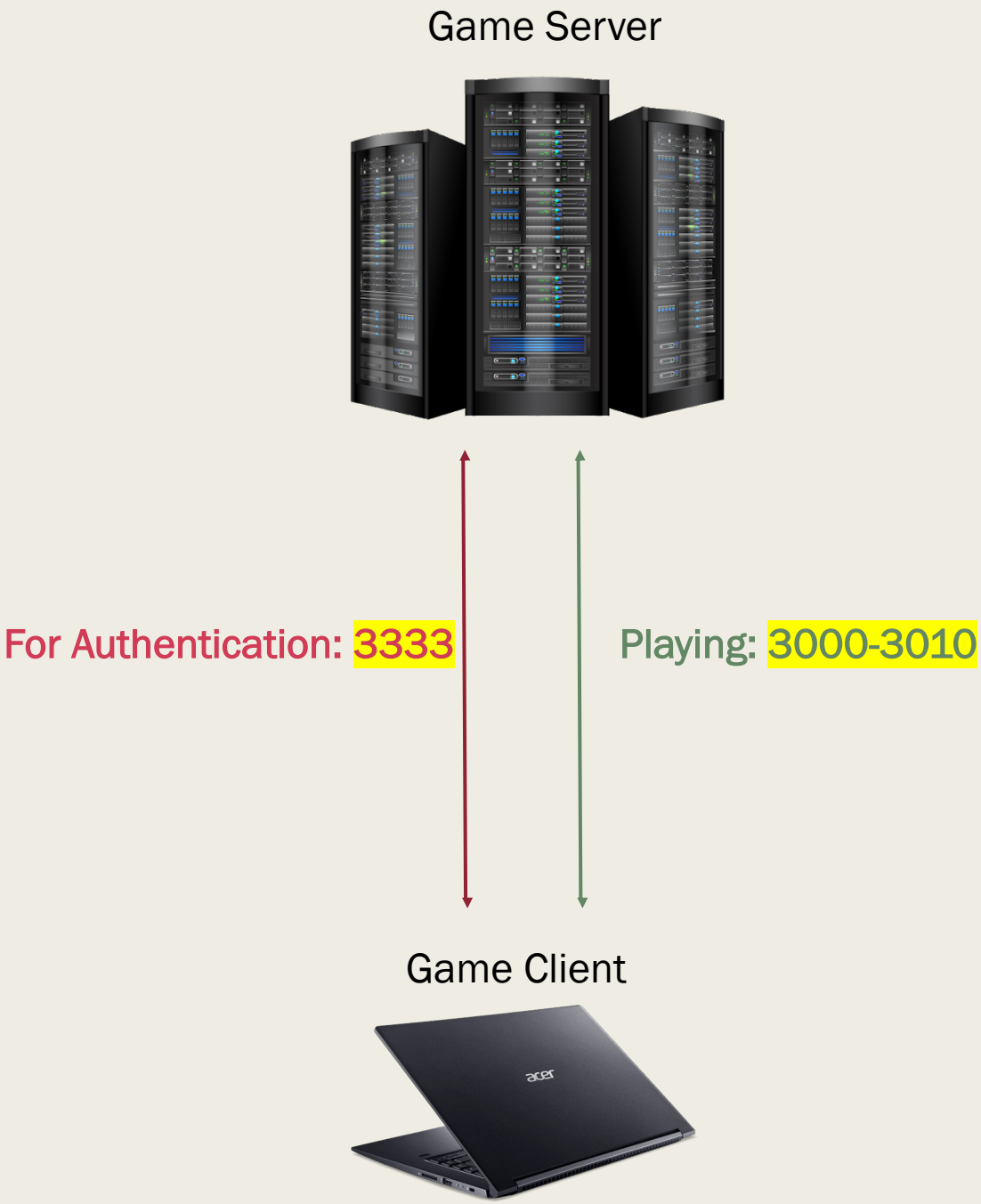
PWN ADVENTURE 3 *
BUILDING PROXY SERVER

* PWN Adventure 3 : https://www.pwnadventure.com/

Before


Game Server
For Authentication: 3333
Playing: 3000-3010
Game Client

After

Game Server

Proxy Server

For Authentication:
listen on port :3333

Playing:
listen on ports: 3000-3010

Game Client

Java Program

Java Version: 1.8.0_221

Java APIs: ServerSocket , Socket

Usage : java Proxy <portNumber>

```java
// Client Variables
private Socket clientSocket; // Client socket
private String clientAddress; // to store the client address
private InputStream fromClient; // Data sent by Client to the Proxy
private OutputStream toClient; // Data sent by the Proxy to the client (the data that we are forwarding from the Game Server)

// Game Server Variables
private Socket gameServerSocket; // Game Server socket
private String gameServerHostName = "";
private int gameServerPort; // the port that the Game Server is listening on
private InputStream fromGameServer; // Data sent by Game Server to the Proxy
private OutputStream toGameServer; // Data sent by Proxy to the Game Server (the data that we are forwarding from the Client)

// Creating buffers for client-to-server and server-to-client communication.
final byte[] request = new byte[500];
final byte[] reply = new byte[2000];

// Location Packet Variables ==> Should be Moved to PacketParsing Class
private boolean locationPacket = false;
private boolean JMPPacket = false;
private boolean MsgPacket = false; // NOT COMPLETED
private boolean MANAPacket = false; // NOT COMPLETED
```

CLASS VARIABLES

```java
new Thread() {

    public void run() {
        int bytes_read;
        try {
            // while the Client is sending streams , forward them to the Game Server
            // read() : it returns the total number of bytes read into the buffer,
                        // or -1 if there is no more data because the end of the stream has been reached.
            while ((bytes_read = fromClient.read(request)) != -1) {
                toGameServer.write(request, 0, bytes_read);
                System.out.println("[+] Client is sending " + bytes_read + " Bytes to the Game Server:\n" + printHex(request));
                toGameServer.flush();
            }
        } catch (IOException e) {
        }
        // if the Client close the connection with the Proxy, close the connection with the Game Server
        try {
            toGameServer.close();
        } catch (IOException e) {
        }
    }
```

GAME CLIENT TO PROXY

```java
// 9 - Reading the Game Server's response , then forward it to the Client
int bytes_read;
try {
    // while the Game Server is sending streams, forward them to the Client
    while ((bytes_read = fromGameServer.read(reply)) != -1) {
        try {
            Thread.sleep(1);
            System.out.println("[+] Game Server is sending " + bytes_read + " Bytes to the Client:\n" + printHex(request));
        } // end try
        catch (InterruptedException e) {
            e.printStackTrace();
        } // end catch
        toClient.write(reply, 0, bytes_read);
        toClient.flush();
    } // end while
} // end try
catch (IOException e) {
} // end catch
// if the Game Server close the connection with the Proxy, close the connection with the Client
toClient.close();
```

PROXY TO GAME SERVER

Identifying Game Packets by ID

LOCATION PACKET 0X6D76

No.	Time	Source	Destination	Protocol	Length	Info
1048	4.906408	[redacted]	[redacted]	TCP	88	58271 → 3001 [PSH, ACK] Seq=491 Ack=15227 Win=2048 Len=22 TSval=789794412 TSec

```
    TCP payload (22 bytes)
▼ Pwn Adventure 3 - Game server protocol
  ▼ Update location
      Action: Update location (0x6d76)
    ▼ Location
        X coordinate: -12984.5
        Y coordinate: 36690.4
        Z coordinate: 1496.29

0000  00 09 0f 09 62 0b 8c 85  90 73 d5 4a 08 00 45 00   ····b··· ·s·J··E·
0010  00 4a 00 00 40 00 40 06  dc 08 ac 16 9f c7 93 bc   ·J··@·@· ····· ···
0020  7f 0b e3 9f 0b b9 b0 0b  3b 8f fc 3b d4 48 80 18   ····· ··;··;·H··
0030  08 00 33 ff 00 00 01 01  08 0a 2f 13 4e 6c ab df   ··3····· ··/·Nl··
0040  8a 2a 6d 76 d7 e1 4a c6  5d 52 0f 47 4b 09 bb 44   ·*mv··J· ]R·GK··D
0050  00 00 00 00 00 00 7f 00                            ····· ···
```

Wireshark View with Lua plugin *

* Lua plugin: https://github.com/beaujeant/PwnAdventure3/blob/master/Network/pwn3-gs.lua

Identifying Game Packets by ID

LOCATION PACKET 0X6D76

```
Location Packet has been captured!
[+] Client is sending 22 Bytes to the Game Server:
6d76d7e14ac65d520f474b09bb4400000000000007f0000000000
```

Proxy View

Identifying Game Packets by ID

LOCATION PACKET 0X6D76

```
private static boolean isItLocationPacket (byte [] request)
{
    boolean condition = false;
    if ( (request[0] == 109) && (request[1] == 118) )
    {
    condition = true;
    } // end if
    return condition;
} //  isItLocationPacket()
```

Code View

Identifying Game Packets by ID

JUMP PACKET 0X6A70

No.	Time	Source	Destination	Protocol	Length	Info
1032	4.521292	[redacted]	[redacted]	TCP	91	58271 → 3001 [PSH, ACK] Seq=441 Ack=13903 Win=2048 Len=25 TSval=789794033 TSec

```
    TCP payload (25 bytes)
▼ Pwn Adventure 3 - Game server protocol
  ▼ Jump
      Action: Jump (0x6a70)

0000  00 09 0f 09 62 0b 8c 85  90 73 d5 4a 08 00 45 00   ····b··· ·s·J··E·
0010  00 4d 00 00 40 00 40 06  dc 05 ac 16 9f c7 93 bc   ·M··@·@· ····· ····
0020  7f 0b e3 9f 0b b9 b0 0b  3b 5d fc 3b cf 1c 80 18   ····· ··· ;]·;····
0030  08 00 63 2d 00 00 01 01  08 0a 2f 13 4c f1 a6 df   ··c-···· ··/·L···
0040  89 fe 6a 70 01 6d 76 a5  a8 4e c6 5d 52 0f 47 d3   ··jp·mv· ·N·]R·G·
0050  2a ba 44 00 00 00 00 00  00 00 00                  *·D····· ···
```

Wireshark View with Lua plugin *

* Lua plugin: https://github.com/beaujeant/PwnAdventure3/blob/master/Network/pwn3-gs.lua

Identifying Game Packets by ID

JUMP PACKET 0X6A70

```
Jump Packet has been captured!
[+] Client is sending 25 Bytes to the Game Server:
6a70016d76a5a84ec65d520f47d32aba4400000000000000000
```

Proxy View

Identifying Game Packets by ID

JUMP PACKET 0X6A70

```
  private static boolean isItJMPPacket (byte [] request)
{
    boolean condition = false;
    if ( (request[0] == 106) && (request[1] == 112) )
    {
    condition = true;
    } // end if
    return condition;
} //  isItLocationPacket()
```

Code View

Demo

How about **Packets Injection** ?

Find out what I don’t know!

- Methodology for building the proxy has been inspired by:
  - http://www.jcgonzalez.com/java-simple-proxy-socket-server-examples
  - https://youtu.be/iApNzWZG-10
- Java Program code can be found here (contribution is **HIGHLY** welcomed :]!) :
  - https://github.com/0xb1tByte/PWN/tree/master/PwnAdventure/Proxy/src/proxy

Sources

THANK YOU FOR YOUR ATTENTION, QUESTIONS?

- Alaa