Stay for a while and listen
Thank you!

- Drew
- Muaziz
- Intline9
Fuzzing online games is hard
Fuzzing online games is hard

Game

Not accessible

Server

http://ly.tl/
Fuzzing online games is hard
Fuzzing online games is hard

Complex
Anti-debugging
Active security checks

Not accessible

Game

Encrypted & Unknown

Server
OMG! Fuzzing games is really hard!
I don't know what to do
It is possible (albeit difficult) to fuzz games by being creative and using new techniques.
Teach you the new techniques we developed while working on real games
The master plan

Game → Server

Server → Game

Monday, September 10, 12
The master plan

Game

Kartograph

Server
The master plan

Game

Memory offset

Kartograph

Server
Challenges

- Intercepting traffic
- Bypassing encryption
- Reversing the protocol
- Monitoring fuzzing results
Intercepting traffic
Interception points

Game
Interception points

Game

DLL injection
Interception points

Game

DLL injection

Os
Interception points

Game

DLL injection

Os

Driver

Monday, September 10, 12
Interception points

Game

Os

Network / Hypervisor

DLL injection

Driver

Monday, September 10, 12
Interception points

Game

Os

Network / Hypervisor

DLL injection

Driver

Firewall
Hooking winsock

- Most games use Windows Winsock API
- Inject a DLL that “overwrite/detour” interesting functions:
  - connect
  - recv
  - send
How to do Winsock hooking

- Multiples "standard" ways
  - Microsoft detour library
  - IAT hooking
Fuzzing online games

Elie Bursztein, Patrick Samy

http://ly.tl/

Side note: the Warden

- Blizzard Anti-cheating engine
- Read specific game memory offset
- Scan process name
- Execute code blob

- Will find your hooks ...
- Scan for AutoAlloc(), VirtualAlloc(),
Using a driver

- Windows offers two API:
  - LSP (old)
  - Windows Filter Platform (new)
- Careful when intercepting and emitting on the same port. Your own packets will be passed to the filter.
Side note Diablo III IP checking

• Diablo 3 check for server ip
• Located in thumbprint.dll
• Force to use a driver interception or reroute server IP
### Injection method comparison

<table>
<thead>
<tr>
<th>Method</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLL injection</td>
<td>Easy</td>
<td>Detectable</td>
</tr>
<tr>
<td></td>
<td>Direct access to game state</td>
<td></td>
</tr>
<tr>
<td>Driver</td>
<td>Invisible</td>
<td>Complexity</td>
</tr>
<tr>
<td></td>
<td>Direct access to game state</td>
<td></td>
</tr>
<tr>
<td>Network / Hypervisor</td>
<td>Invisible</td>
<td>Mild complexity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No direct access to game state</td>
</tr>
</tbody>
</table>
Encryption
League of Legend Encryption

- Use Blowfish (???)
- The key is in the command line ....
Diablo 3 encryption flow

Game

pubKey

BNet Server
Diablo 3 encryption flow

Game

pubKey

SRP6 login protocol

BNet Server
Diablo 3 encryption flow

SRP6 login protocol

Game

BNet Server

pubKey

k

k
Diablo 3 encryption flow

Game

k

pubKey

SRP6 login protocol

k

TLS-PSK

k

BNet Server
Diablo 3 encryption flow

Game   k

SRP6 login protocol

TLS-PSK_k

RSA challenge

BNet Server

pubKey

Monday, September 10, 12
Diablo 3 encryption flow

Game k

SRP6 login protocol

TLS-PSK k

RSA challenge

pubKey

k

BNet Server

Game Server
Why a RSA challenge?

- TLS-PSK: confidentiality
- RSA challenge: authentication
- Prevents Man in the middle
- Bypassing the challenge
  - Factoring the key (impossible)
  - Patching the game (warden !)
Traffic to game server is not encrypted
Reversing protocol
Diablo 3 packet example

GameMessage(0x0091):
{
  AimTargetMessage:
  {
    Field0: 0x2C58CA56 (744016470)
    Field1: 0x00000000 (0)
    Field2: 0x00B99444 (12162116)
  }
  WorldPlace:
  {
    Vector3D:
    {
      X: 2.746353E-23
      Y: -3.169127E+29
      Z: 1.504633E-36
    }
    WorldID: 0x468A6D7F (1183477119)
  }
}
LOL network stack

- LOL protocol
- Blowfish
- Enet protocol
- UDP

Enet protocol: http://enet.bespin.org/
LOL packet format

Opcode  ID  ID  ID  ID  ...  Content

Channels  Flags

Note: item are coded on int 32
Example of LOL traffic intensity

Duration: 21 mn
Nb pkts: 61854 (~48 pkt/s)
Nb Packet type: 78
There is too much packets to deal with
Having **lot of data** is good
we can apply **data analysis techniques** :}
Divide and conquer approach
Divide and conquer approach

Bucket
Divide and conquer approach

Bucket

Analyze
Divide and conquer approach

Bucket  Analyze  Mutate
Divide and conquer approach

Bucket  Analyze  Mutate  Inject
Diff analysis within trace

Opcodes:
- AA
- 05
- 00
- 01
Diff analysis within trace

<table>
<thead>
<tr>
<th>Opcode</th>
<th>05</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>02</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Diff analysis within trace

<table>
<thead>
<tr>
<th>Opcode</th>
<th>05</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>02</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>09</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Diff analysis within trace

<table>
<thead>
<tr>
<th>Opcode</th>
<th>02</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>05</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>09</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

02-09
<table>
<thead>
<tr>
<th>Opcode</th>
<th>05</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>00</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>09</td>
<td>00</td>
<td>01</td>
<td></td>
</tr>
</tbody>
</table>

02-09  00
## Diff analysis within trace

<table>
<thead>
<tr>
<th>Opcode</th>
<th>02</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>02</td>
<td>00</td>
<td>01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>09</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>09</td>
<td>00</td>
<td>01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opcode</th>
<th>05</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>05</td>
<td>00</td>
<td>01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>02-09</th>
<th>00</th>
<th>01</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trace 1</td>
<td>Opcode</td>
<td>02-09</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>Trace 2</td>
<td>Opcode</td>
<td>05-19</td>
</tr>
<tr>
<td>Trace 1</td>
<td>Opcode</td>
<td>02-09</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>Trace 2</td>
<td>Opcode</td>
<td>05-19</td>
</tr>
<tr>
<td>Result</td>
<td></td>
<td>02-19</td>
</tr>
</tbody>
</table>

Diff analysis in between trace

Elie Bursztein, Patrick Samy

Fuzzing online games

http://ly.tl/
Diff analysis in between trace

Trace 1
Opcode AA
02-09 00 01

Trace 2
Opcode AA
05-19 00 02

Result
02-19 00
Diff analysis in between trace

Trace 1

| Opcode | AA | 02-09 | 00 | 01 |

Trace 2

| Opcode | AA | 05-19 | 00 | 02 |

Result

| 02-19 | 00 | 01-02 |
Curse of dimensionality

- 3 ranges
- 5 ranges
- 7 ranges

Np packets vs Nb variables tested

Monday, September 10, 12
Fuzzing LOL client

- Used **3 values** for each range (min / max / median)
- ~**1.5 Million** packets to inject
- Tons of crashed generated
  - Need to restart - relog the whole client :(
  - Accounts banned (leaving points through the roof)
• Take it to the next level
Frequency Analysis

Frequency by opcodes (logarithmic)

Monday, September 10, 12
Why frequency analysis is useful?

- Help focus on the “good stuff”
- Example of low frequency packets:
  - Level UP
  - Buying items
  - Attack command
We need to find packets that are correlated:

- Attack trigger - Attack response / mob death
- Skill assignment - Server response
N-gram analysis

Opcode 01  Opcode 02  Opcode 05  Opcode 01  Opcode 04  Opcode 02  Opcode 05

01 - 02 : 1
N-gram analysis

 Opcode 01
 Opcode 02
 Opcode 05
 Opcode 01
 Opcode 04
 Opcode 02
 Opcode 05

 01 - 02 : 1
 02 - 05 : 1
N-gram analysis

 Opcode 01  Opcode 02  Opcode 05  Opcode 01
 Opcode 04  Opcode 02  Opcode 05

01 - 02 : 1
02 - 05 : 1
05 - 01 : 1
N-gram analysis

01 - 02 : 1
02 - 05 : 1
05 - 01 : 1
01 - 04 : 1
N-gram analysis

 Opcode 01  Opcode 02  Opcode 05  Opcode 01  Opcode 04  Opcode 02  Opcode 05

01 - 02 : 1
02 - 05 : 1
05 - 01 : 1
01 - 04 : 1
04 - 02 : 1
N-gram analysis

 Opcode 01  Opcode 02  Opcode 05  Opcode 01  Opcode 04  Opcode 02  Opcode 05

01 - 02 : 1
02 - 05 : 2
05 - 01 : 1
01 - 04 : 1
04 - 02 : 1
N-gram gottcha

- **High-frequency** packets will **mess-up** the analysis when working on low frequency one
- **Filter** those before doing N-gram analysis
### LOL example: Set Skill packet

<table>
<thead>
<tr>
<th>Op code</th>
<th>Player Id</th>
<th>slot position</th>
</tr>
</thead>
<tbody>
<tr>
<td>3E 1B</td>
<td>00 00 40 00</td>
<td></td>
</tr>
<tr>
<td>3E 1C</td>
<td>00 00 40 02</td>
<td></td>
</tr>
<tr>
<td>3E 1A</td>
<td>00 00 40 03</td>
<td></td>
</tr>
<tr>
<td>3E 1B</td>
<td>00 00 40 02</td>
<td></td>
</tr>
</tbody>
</table>

```
3E 1B 00 00 40 00
3E 1C 00 00 40 02
3E 1A 00 00 40 03
3E 1B 00 00 40 02
```

Monday, September 10, 12
### LOL packets example: Set sill answer

<table>
<thead>
<tr>
<th>Op code</th>
<th>Player Id</th>
<th>slot position</th>
<th>Nb points</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-1D</td>
<td>00 00</td>
<td>40</td>
<td>00-05</td>
</tr>
<tr>
<td>18</td>
<td>00 00</td>
<td>40</td>
<td>01-06</td>
</tr>
<tr>
<td>18</td>
<td>00 00</td>
<td>40</td>
<td>03 02</td>
</tr>
<tr>
<td>18</td>
<td>00 00</td>
<td>40</td>
<td>03 00</td>
</tr>
<tr>
<td>18</td>
<td>00 00</td>
<td>40</td>
<td>05 00</td>
</tr>
</tbody>
</table>

**Example packets:**

- **Set sill answer**
  - `18 1C 00 00 40 02 04 00`
  - `18 19 00 00 40 01 03 00`
  - `18 1D 00 00 40 00 05 00`
  - `...`
  - `18 1B 00 00 40 00 03 00`
  - `18 1B 00 00 40 03 02 00`
Correlating click / packet

Receipt

• Listen for a special keystrokes combo
• Inject the event into the trace log
• Use it to isolate interesting part
• Profit
Correlating click / packet

Receipt

• Listen for a special keystrokes combo

• Inject the event into the trace log

• Use it to isolate interesting part

• Profit
Correlating click / packet

Receipt

• Listen for a special keystrokes combo
• Inject the event into the trace log
• Use it to isolate interesting part
• Profit
Correlating click / packet

Receipt

• Listen for a special keystrokes combo
• Inject the event into the trace log
• Use it to isolate interesting part
• Profit
Correlating click / packet

Receipt

- Listen for a special keystrokes combo
- Inject the event into the trace log
- Use it to isolate interesting part
- Profit
Monitoring results
Is my packet affected the game state?
Read the state of the game?

Game

Fuzzer

Inject packet

Poke memory offsets

Health

Gold
Finding offset

Remove

Game memory
Finding offset

Remove

Game memory

Game memory
Finding offset

Remove

Add

Game memory

Game memory
Finding offset

Remove

Add

Game memory

Game memory

Game memory
Finding offset

Game memory

Remove

Add

Remove

Add

Game memory

Game memory

Game memory
The offset is encrypted / obfuscated :( 

- Usually not all the structure is encrypted, only "interesting values" are.
- Find field in the structure that are not encrypted.
- Do field Climbing through the structure
Alternative option

• Do more set/unset until one value remain (might can take a lot of iteration)

• If obfuscated look for value that change / do not change
Game analysis TAO
Thank you

Follow-us on Twitter / G+

@elie