

Fuzzing online games

Elie Bursztein, Patrick Samy



Stay for a while and listen



Thank you !

- Drew
- Muaziz
- Intline9



Fuzzing online games is hard

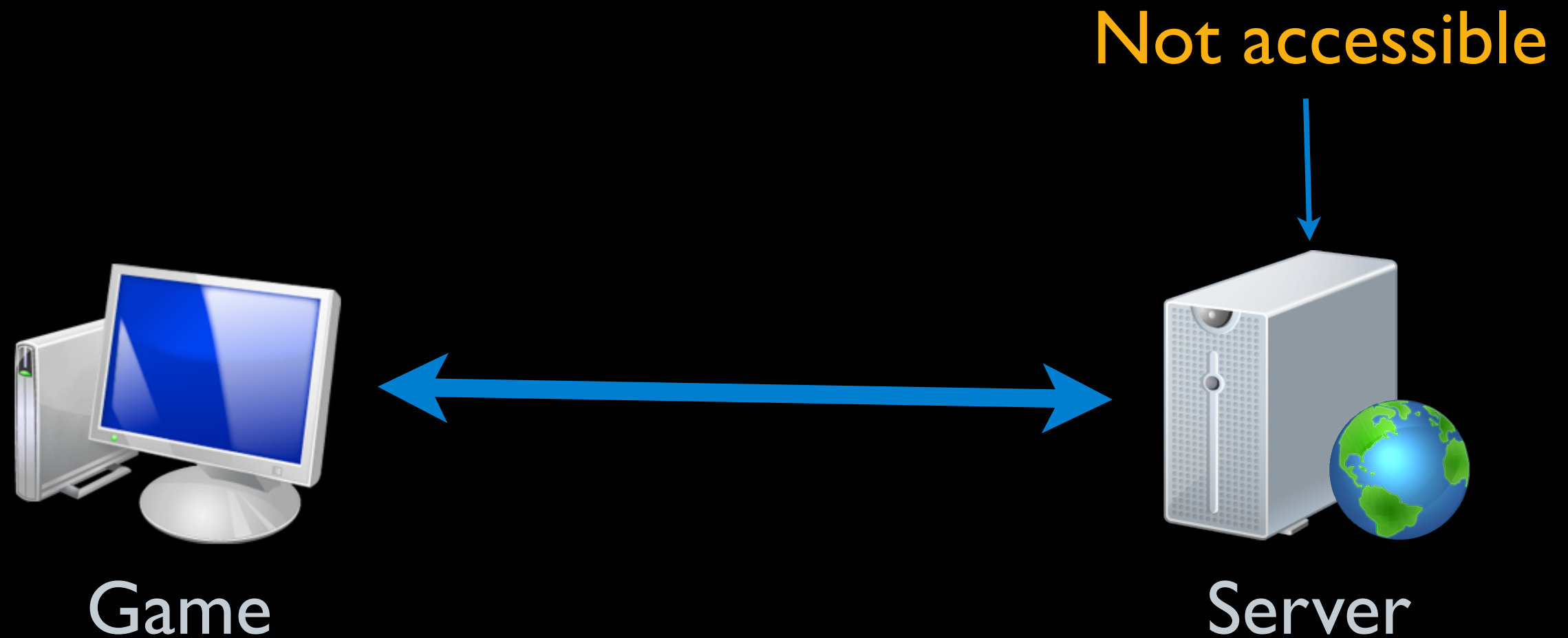


Game

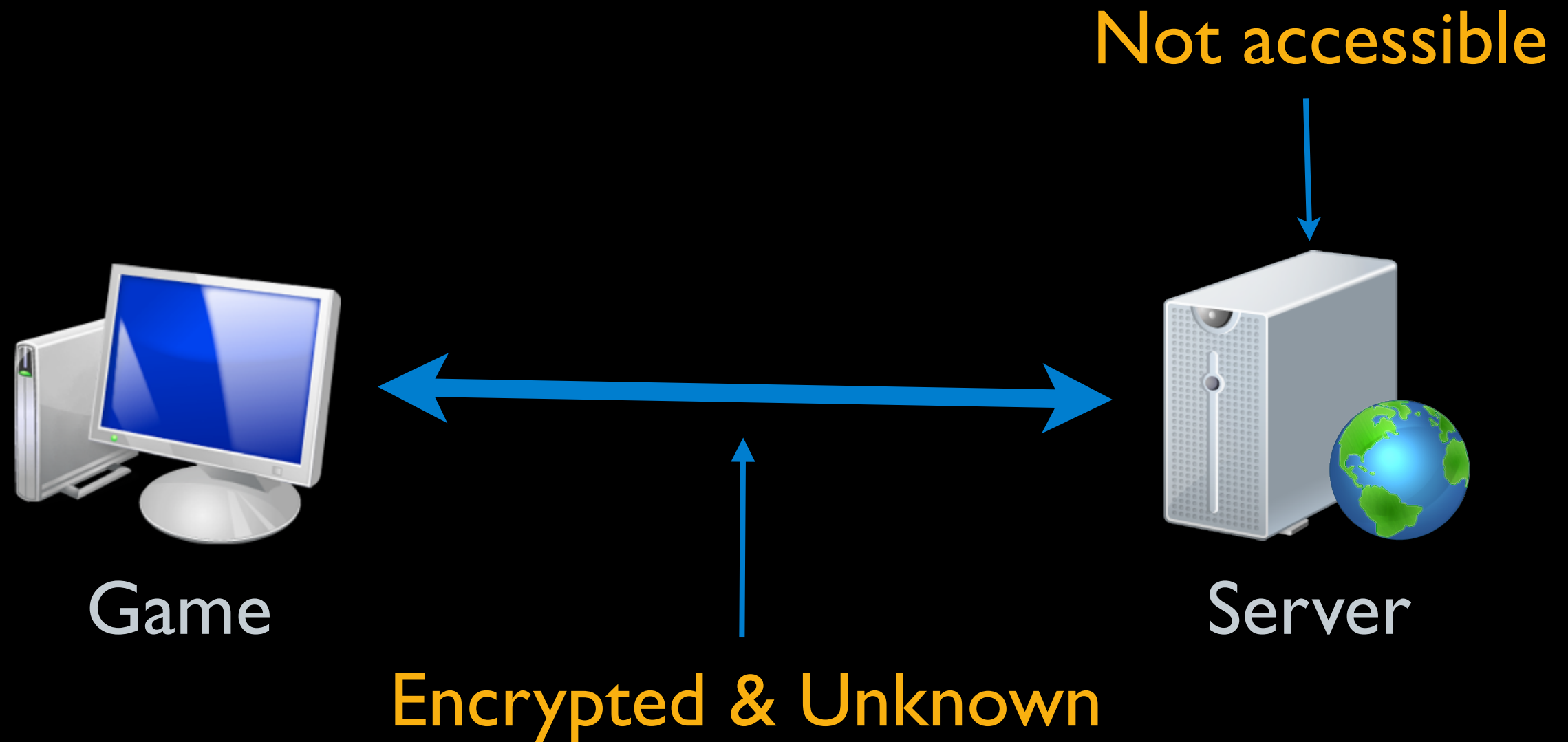


Server

Fuzzing online games is hard



Fuzzing online games is hard



Fuzzing online games is hard

Complex
Anti-debugging
Active security checks



Game

Not accessible



Server

Encrypted & Unknown





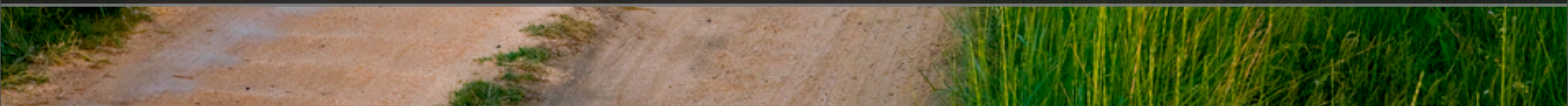
OMG ! Fuzzing games is really hard !



I don't know what to do



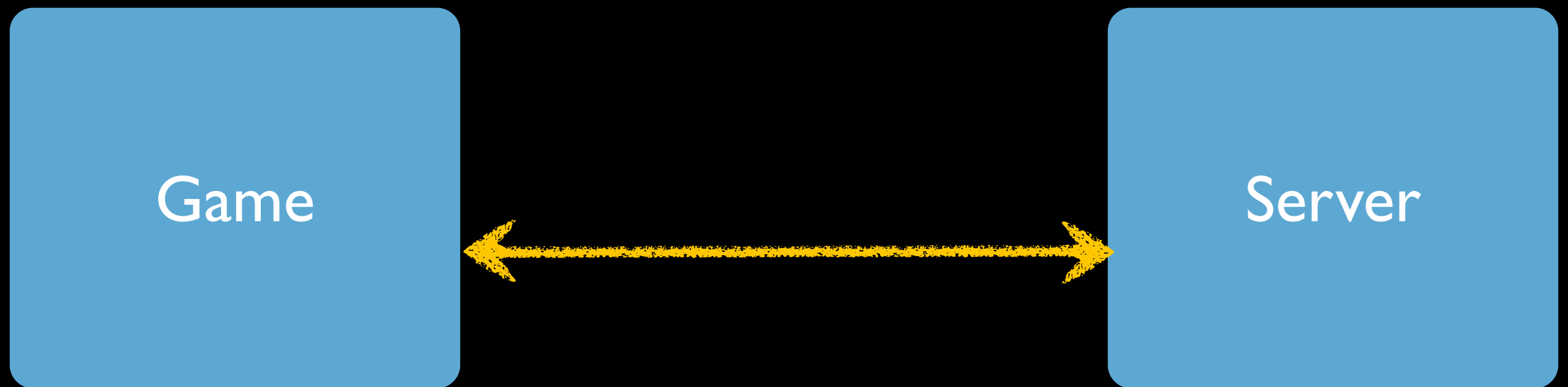
It is **possible** (albeit difficult) to fuzz games
by being **creative** and using **new techniques**





Teach you the new techniques we developed
while working on real games

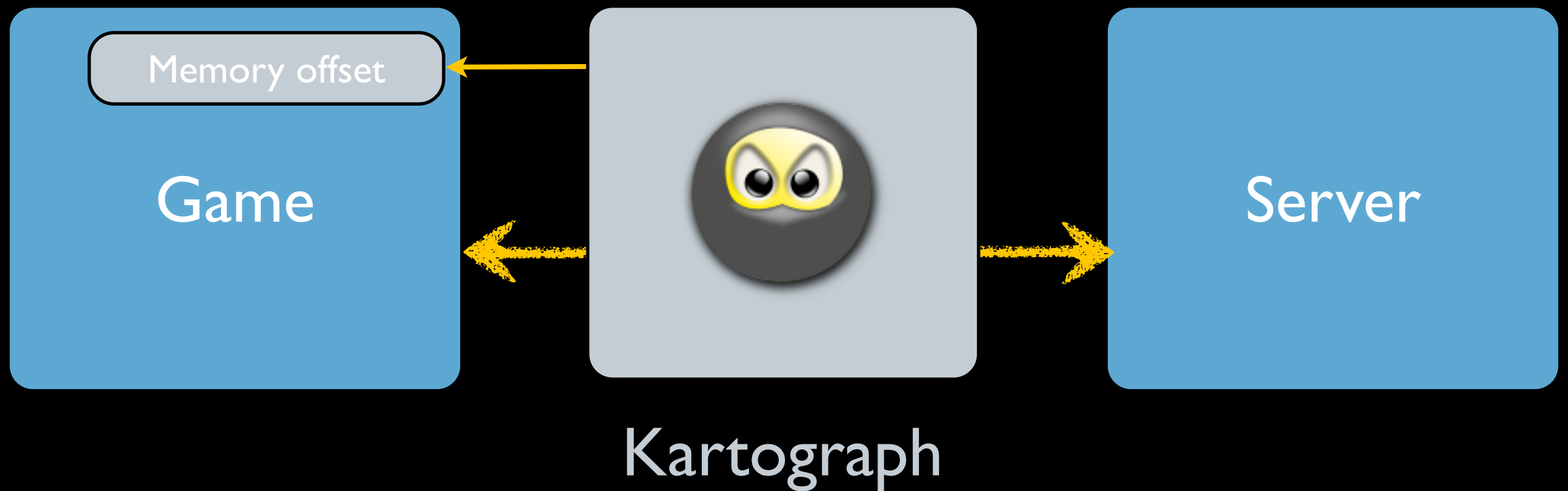
The master plan



The master plan



The master plan



Challenges

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

Intercepting traffic

Interception points

Game

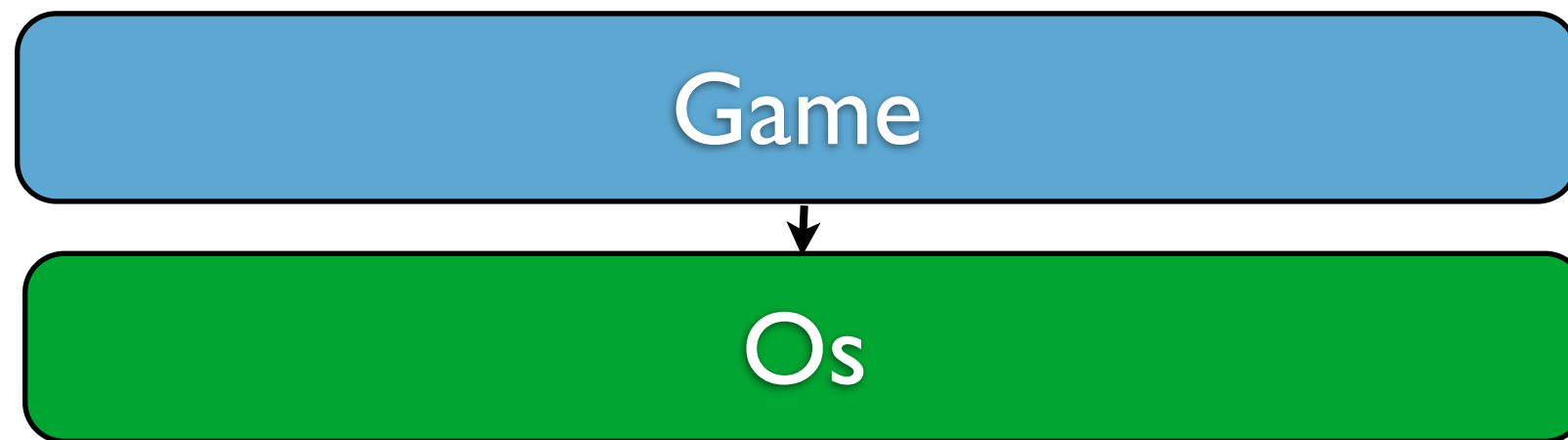
Interception points



Game

DLL injection

Interception points

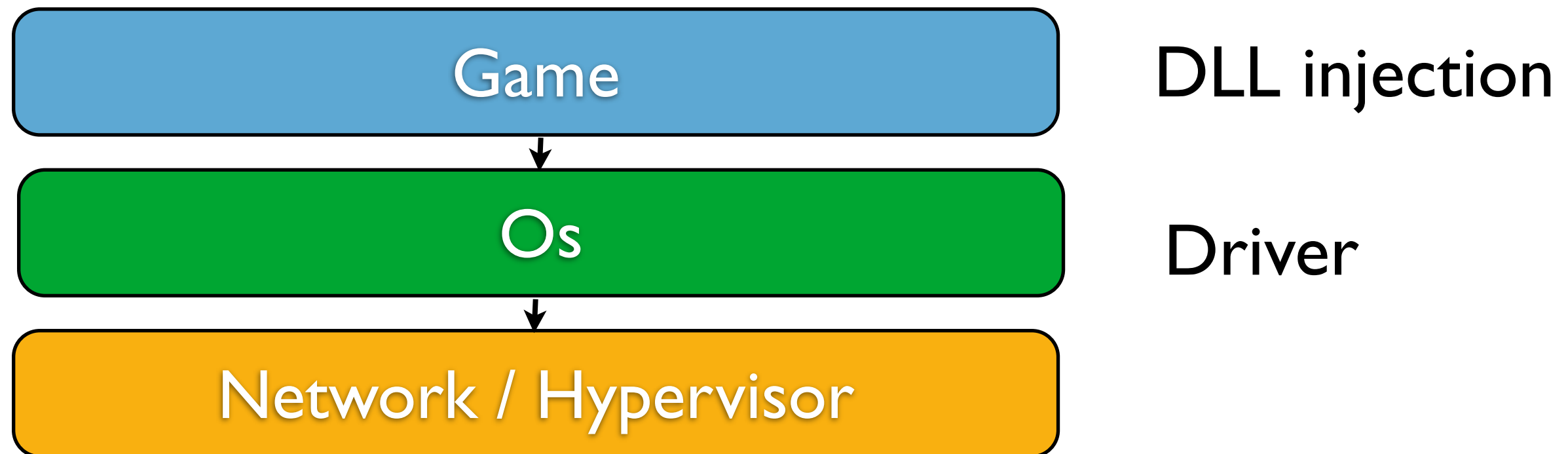


DLL injection

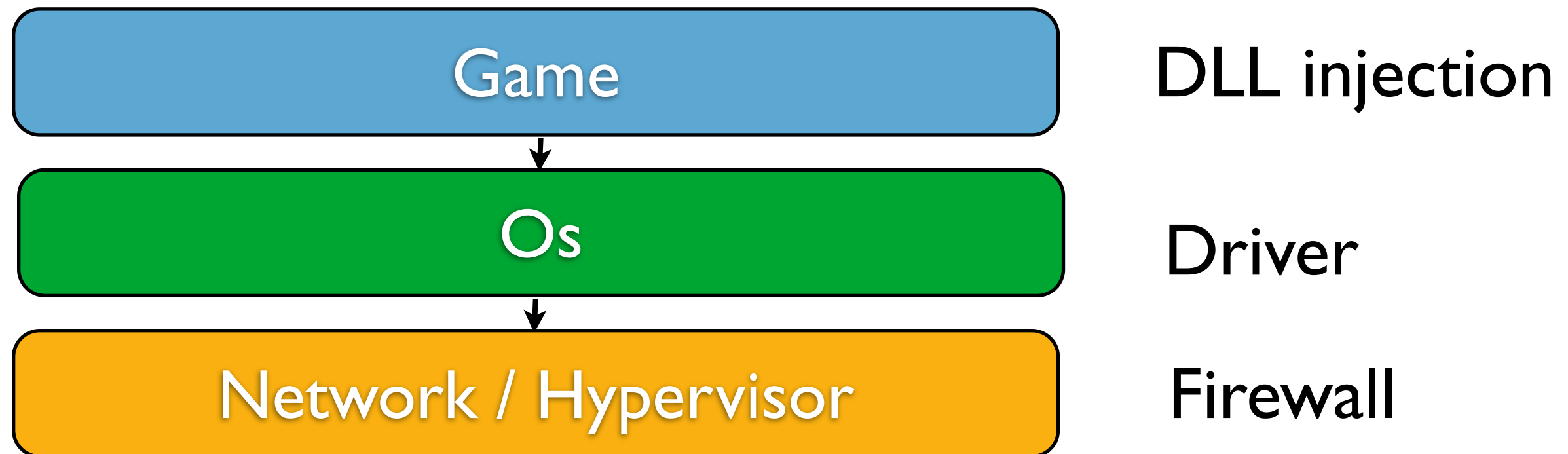
Interception points



Interception points



Interception points



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

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

Method	Pro	Con
DLL injection	Easy Direct access to game state	Detectable
Driver	Invisible Direct access to game state	Complexity
Network / Hypervisor	Invisible	Mild complexity No direct access to game state

Encryption

League of Legend Encryption

- Use Blowfish (???)
- The key is in the command line



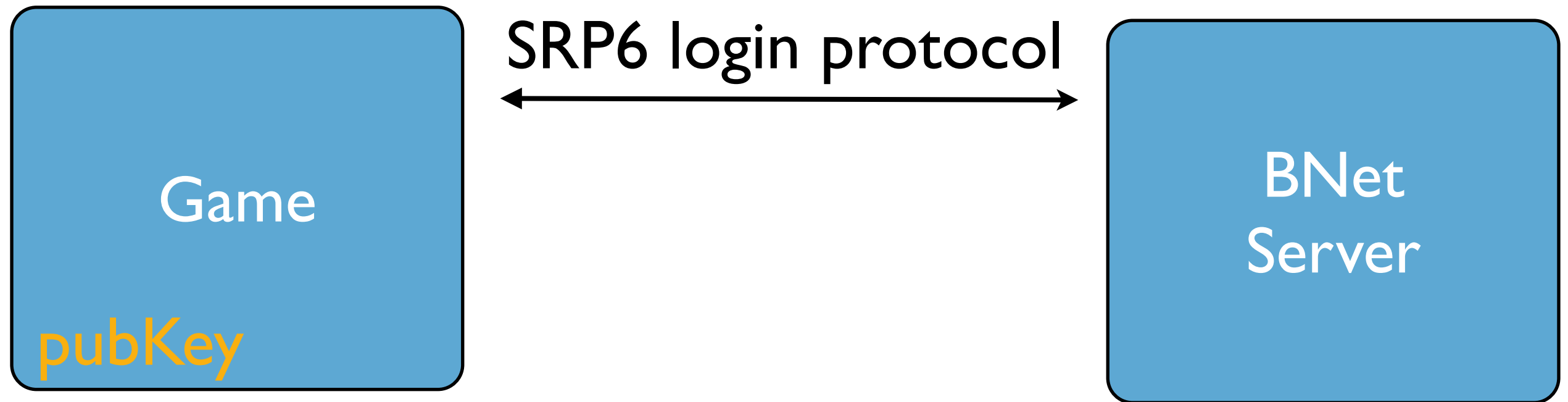
Diablo 3 encryption flow

Game

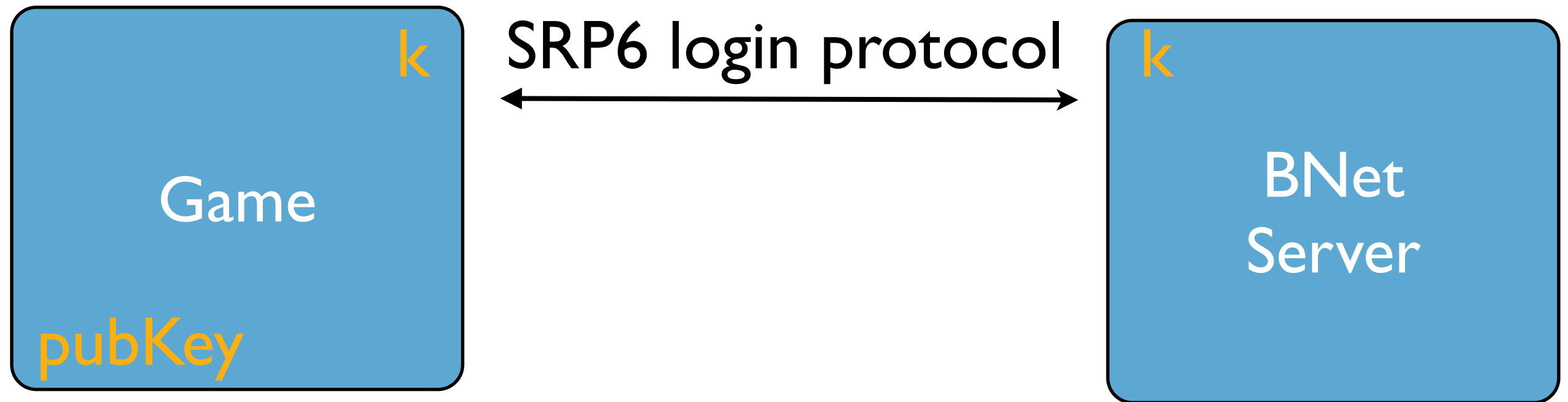
pubKey

BNet
Server

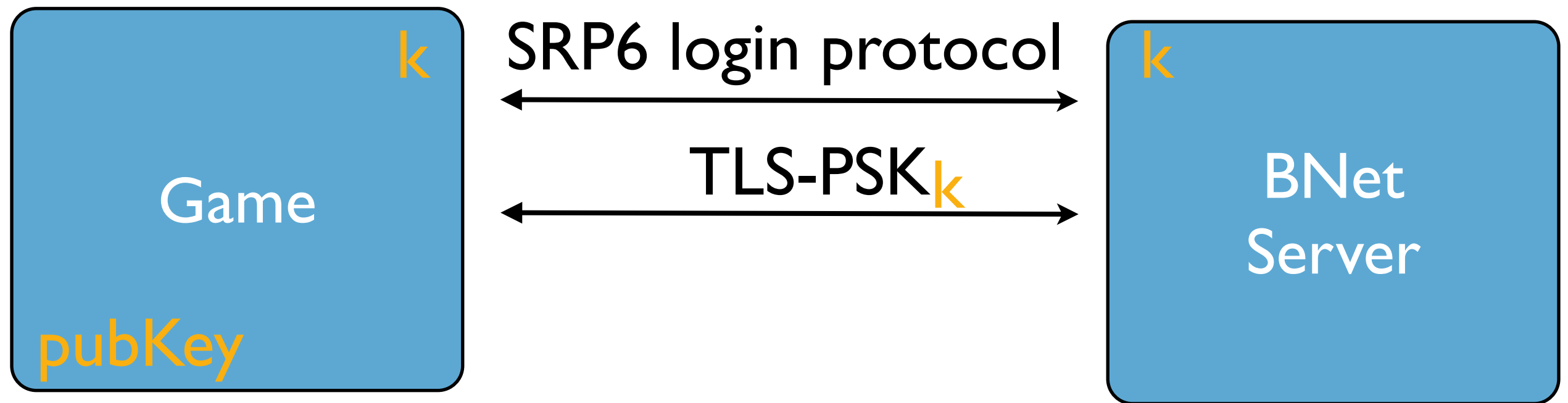
Diablo 3 encryption flow



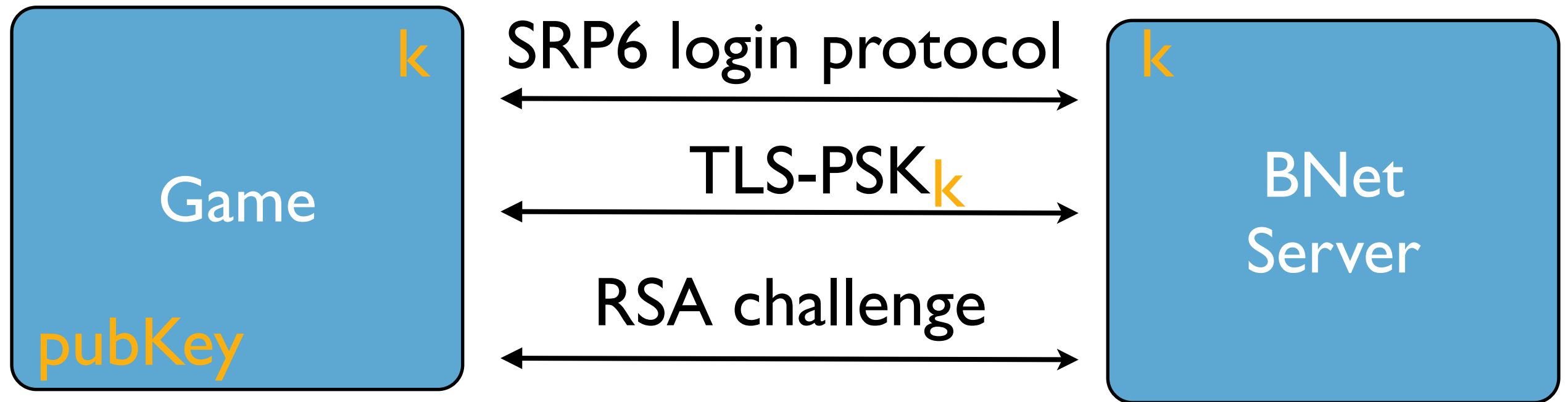
Diablo 3 encryption flow



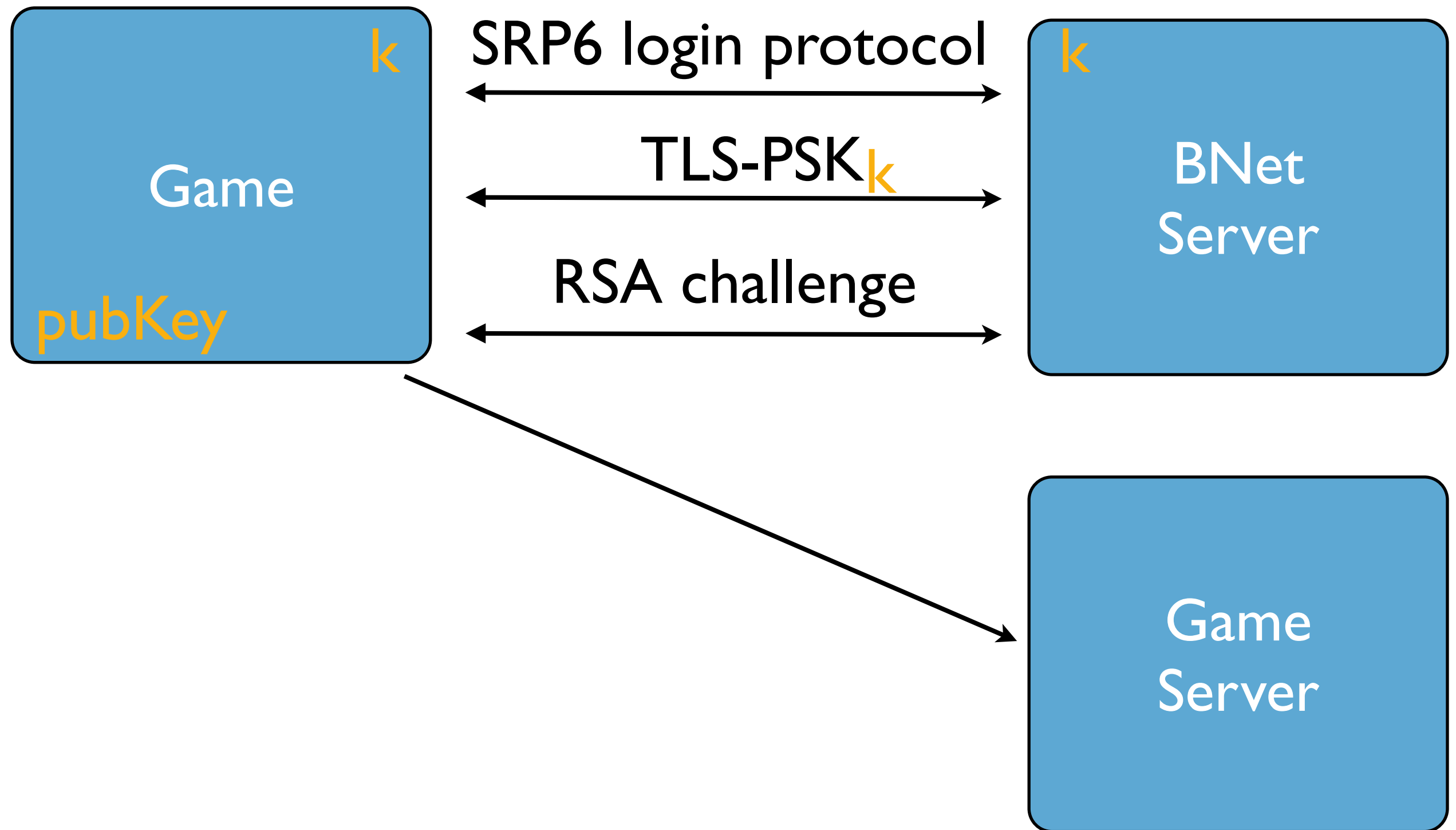
Diablo 3 encryption flow



Diablo 3 encryption flow



Diablo 3 encryption flow



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 game packets

Diablo 3 protocol (proto buf)

RPC

TCP

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

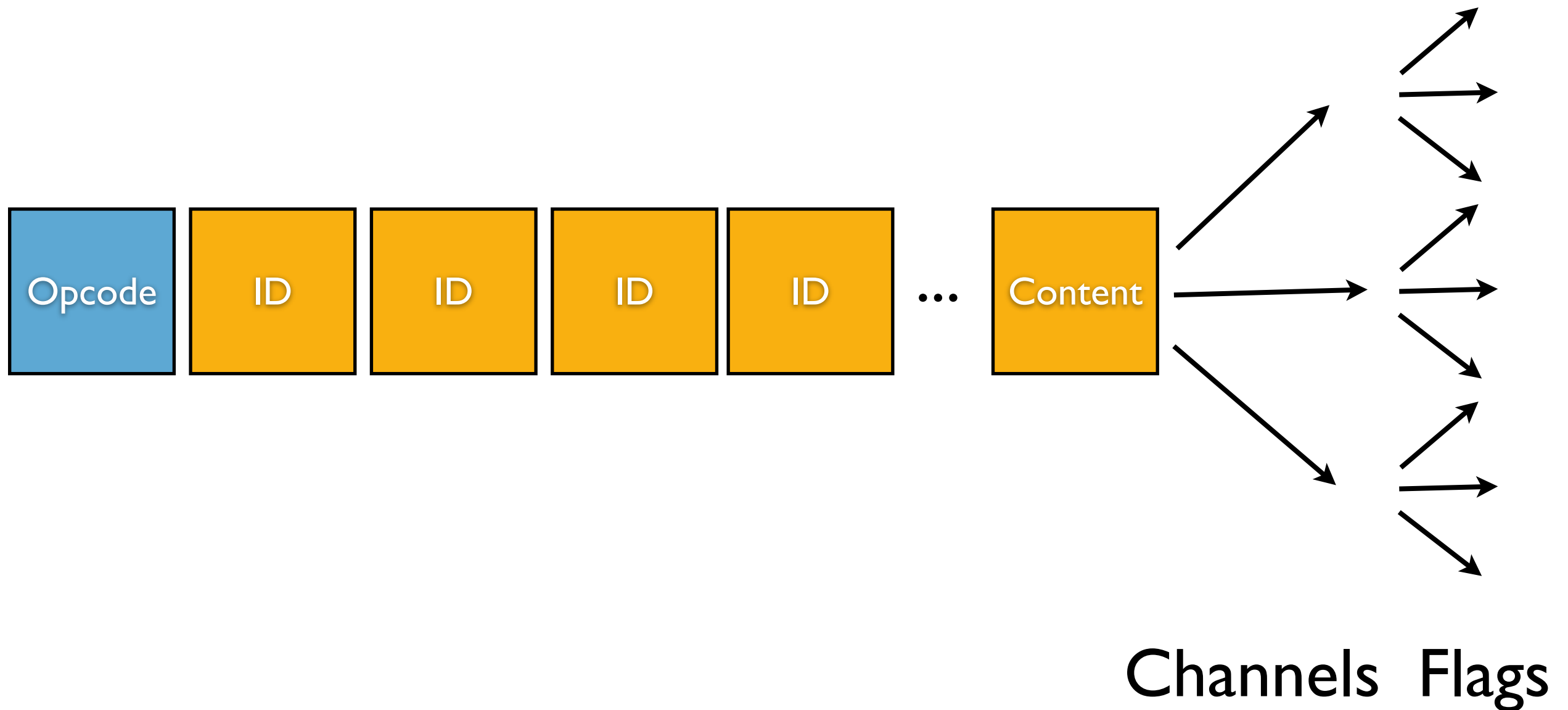
Blowfish

Enet protocol

UDP

Enet protocol : <http://enet.bespin.org/>

LOL packet format



Note: item are coded on int 32

Example of LOL traffic intensity

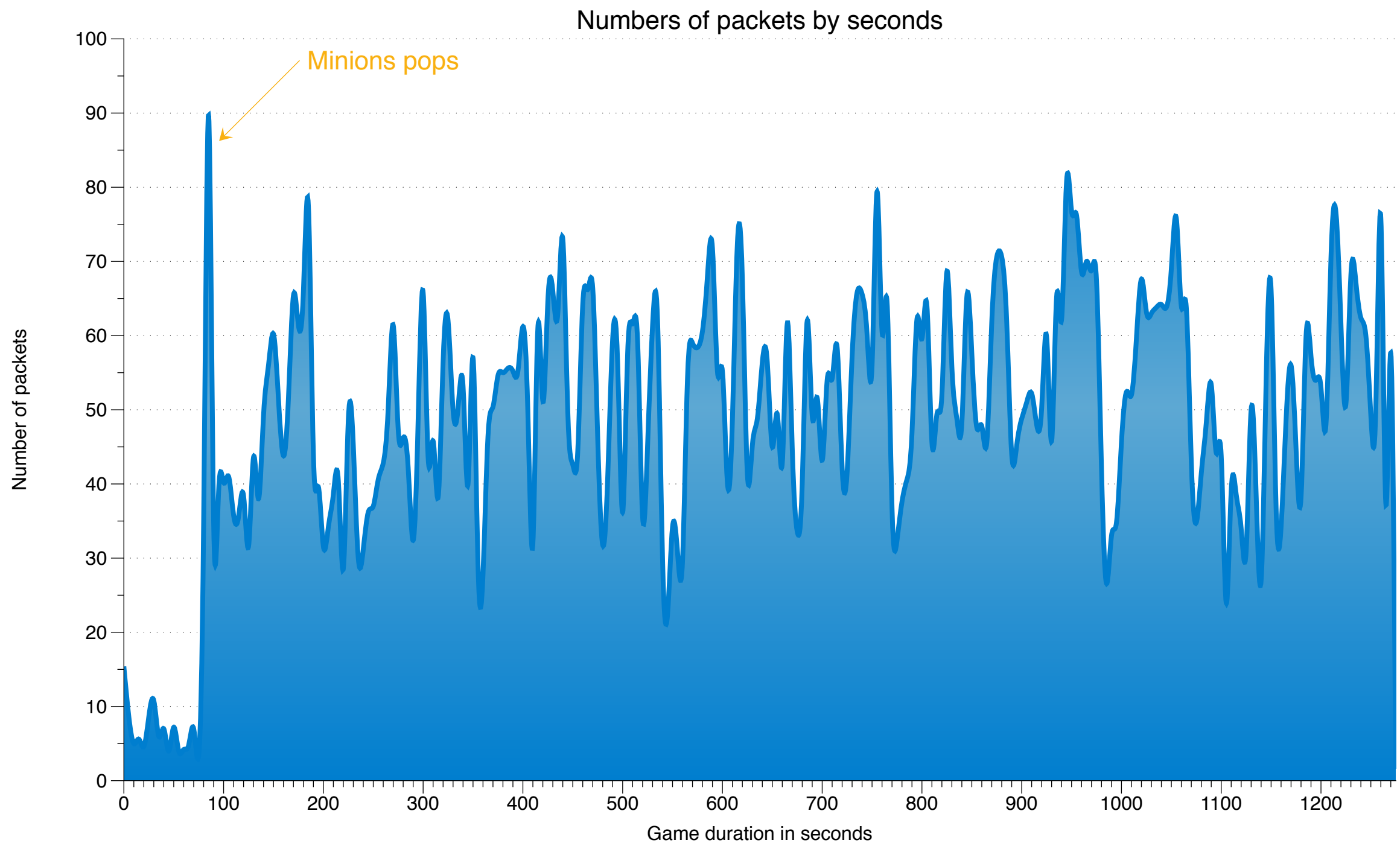
Duration: 21 mn

Nb pkts: 61854 (~48 pkt/s)

Nb Packet type: 78

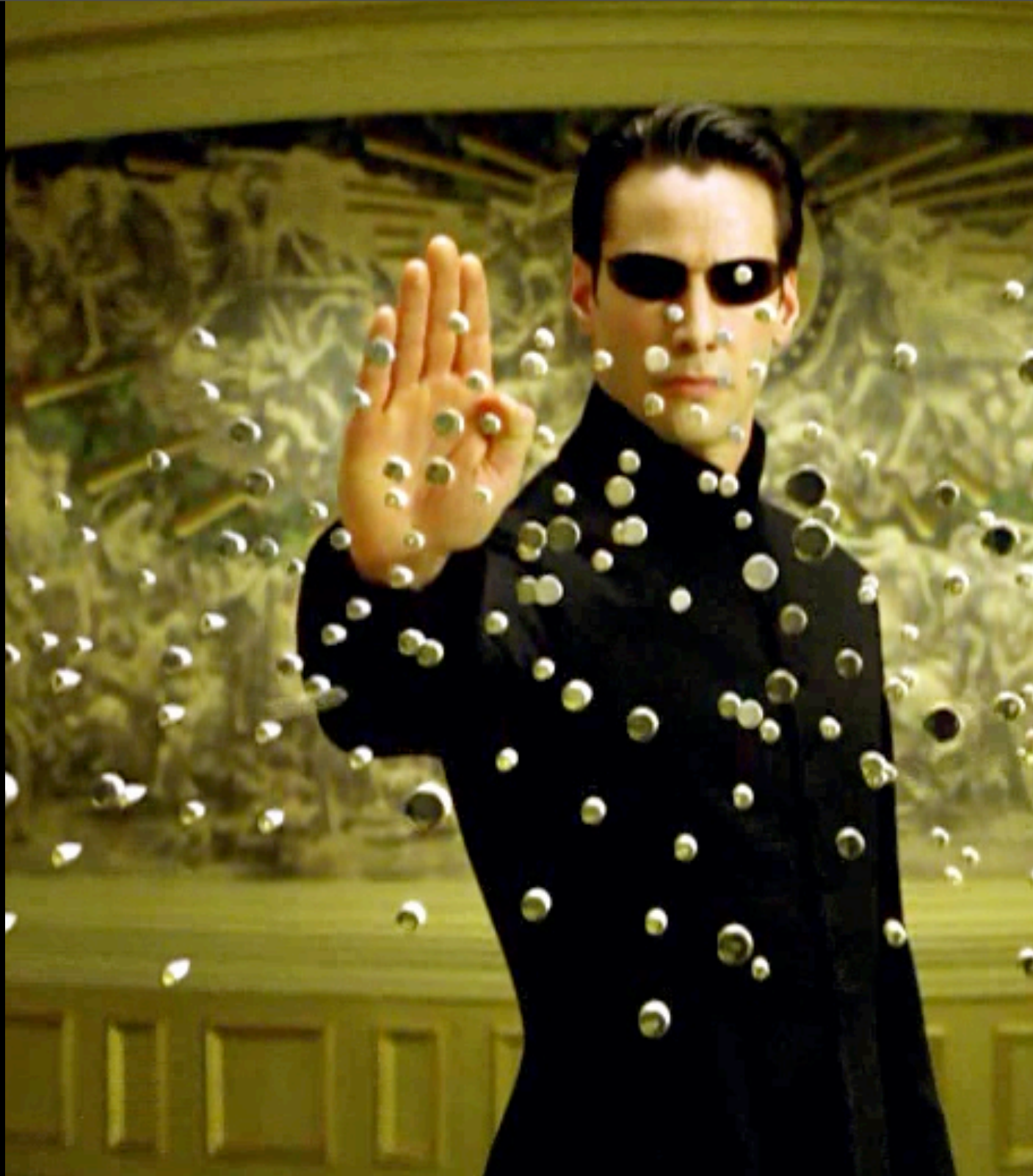


Packets per second





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

Buckting



AA

BB

Buckting



AA

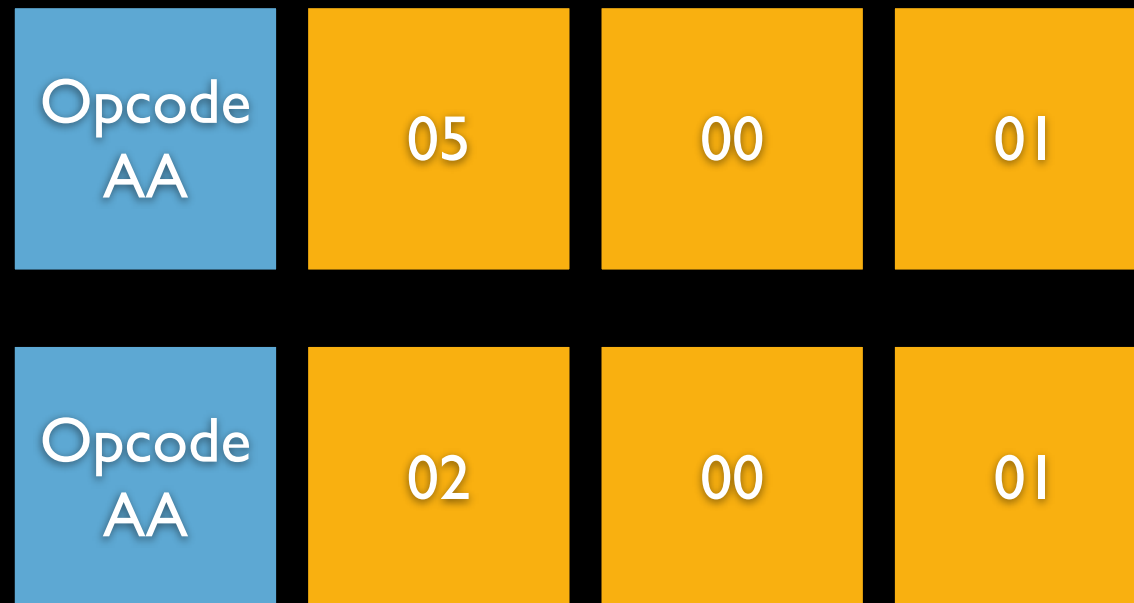


BB

Diff analysis within trace



Diff analysis within trace



Diff analysis within trace

Opcode AA	05	00	01
Opcode AA	02	00	01
Opcode AA	09	00	01

Diff analysis within trace



Diff analysis within trace



Diff analysis within trace

Opcode AA	05	00	01
Opcode AA	02	00	01
Opcode AA	09	00	01
	02-09	00	01

Diff analysis in between trace

Trace 1

Opcode
AA

02-09

00

01

Diff analysis in between trace

Trace 1

Opcode
AA

02-09

00

01

Trace 2

Opcode
AA

05-19

00

02

Diff analysis in between trace

Trace 1

Opcode
AA

02-09

00

01

Trace 2

Opcode
AA

05-19

00

02

Result

02-19

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

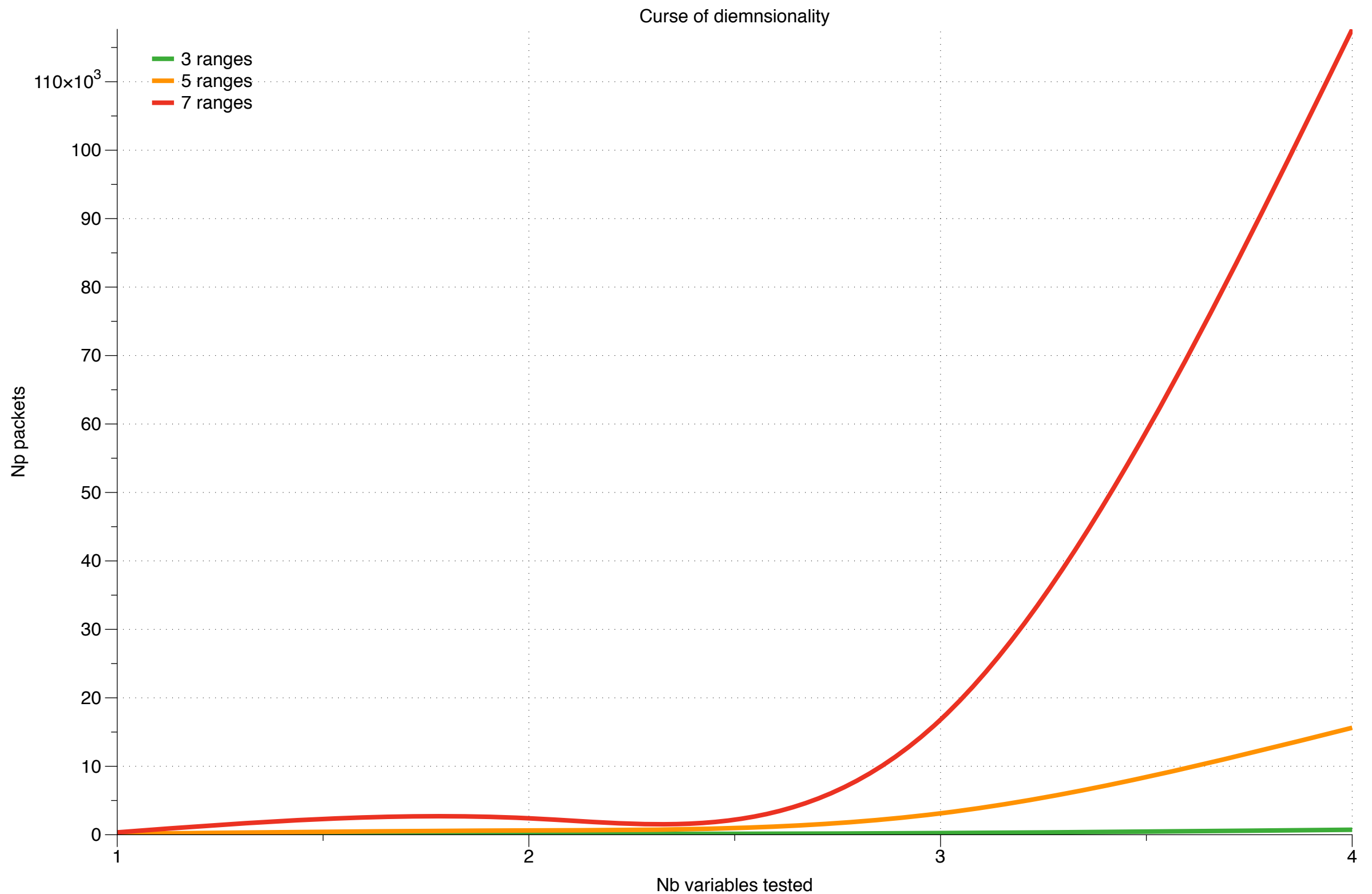
Result

02-19

00

01-02

Curse of dimensionality

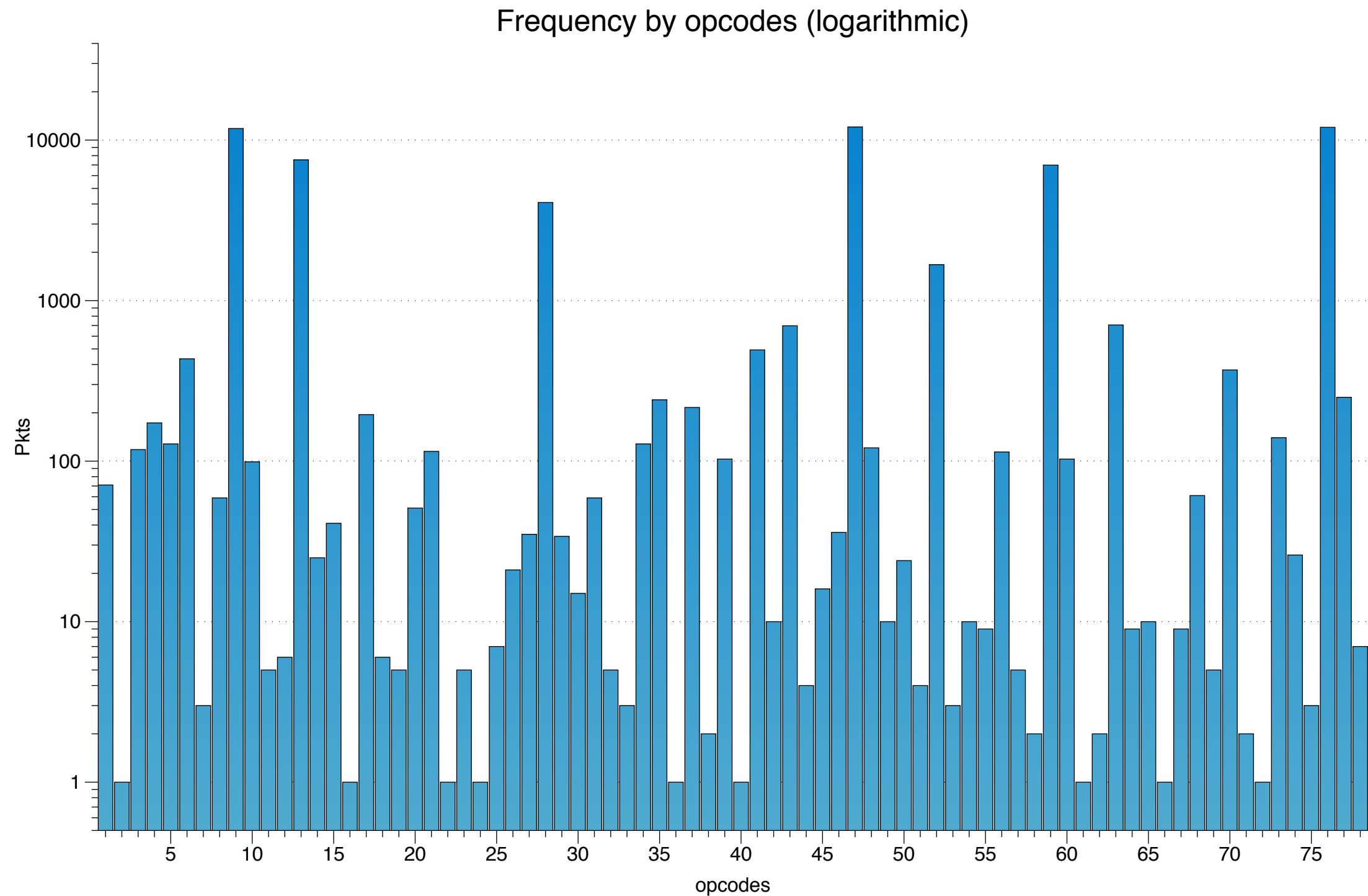


Fuzzing LOL client

- 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



Why frequency analysis is useful ?

- Help focus on the “good stuff”
- Example of low frequency packets:
 - Level UP
 - Buying items
 - Attack command

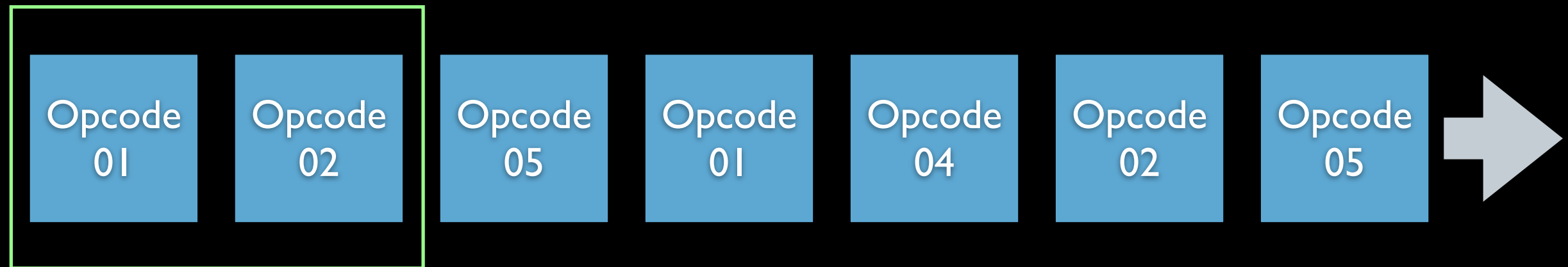
Why frequency is not enough

- We need to find packets that are correlated:
 - Attack trigger - Attack response / mob death
 - Skill assignation - Server response

N-gram analysis

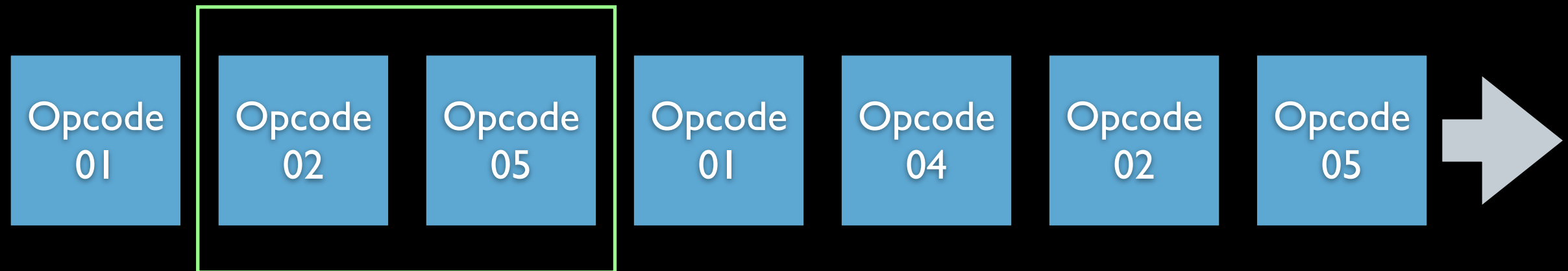


N-gram analysis



01 - 02 : |

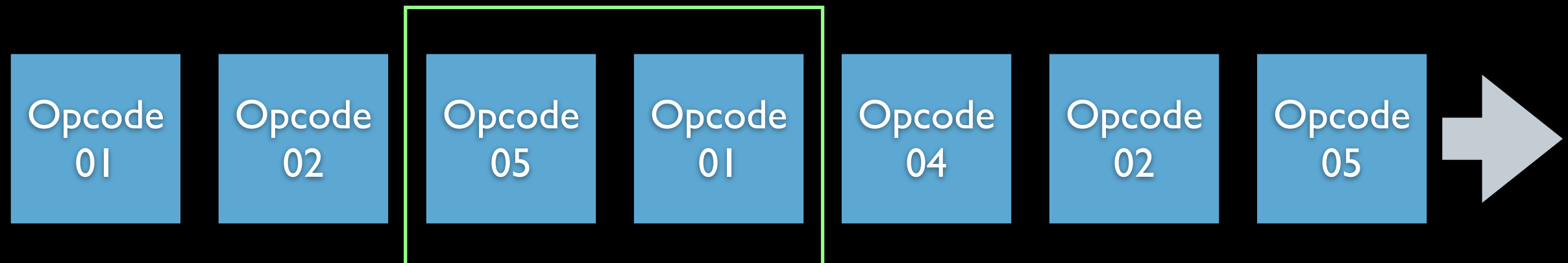
N-gram analysis



01 - 02 : |

02 - 05 : |

N-gram analysis

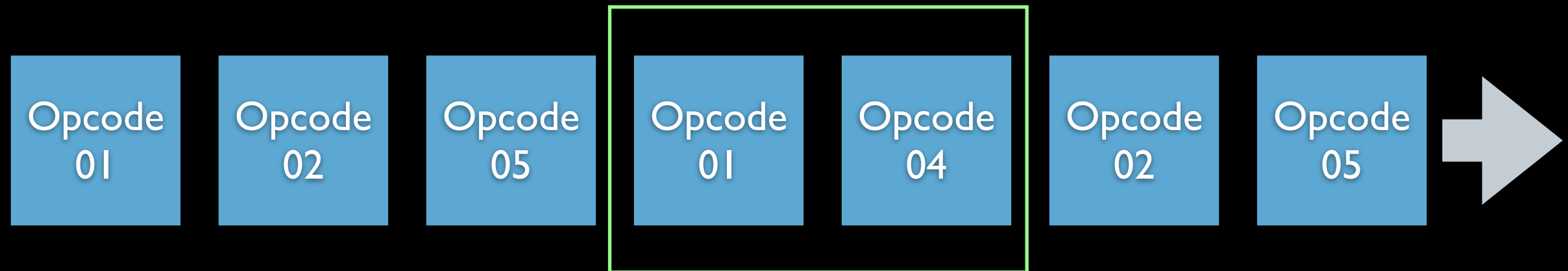


01 - 02 : |

02 - 05 : |

05 - 01 : |

N-gram analysis



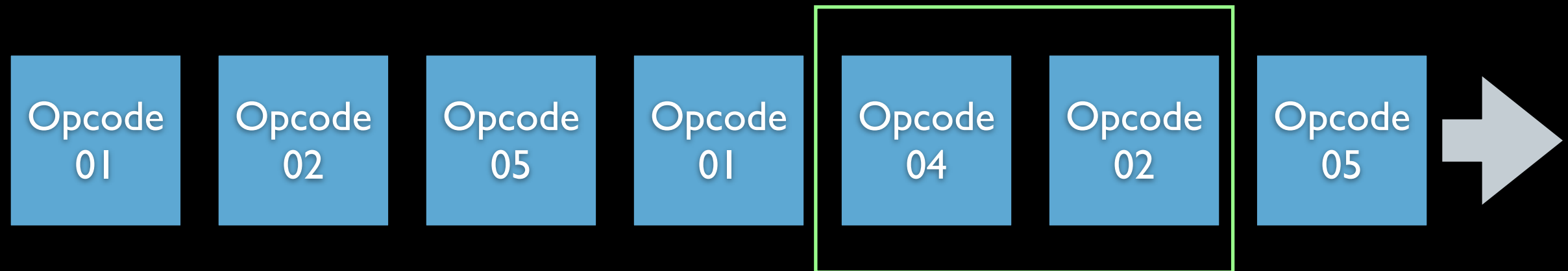
01 - 02 : |

02 - 05 : |

05 - 01 : |

01 - 04 : |

N-gram analysis



01 - 02 : |

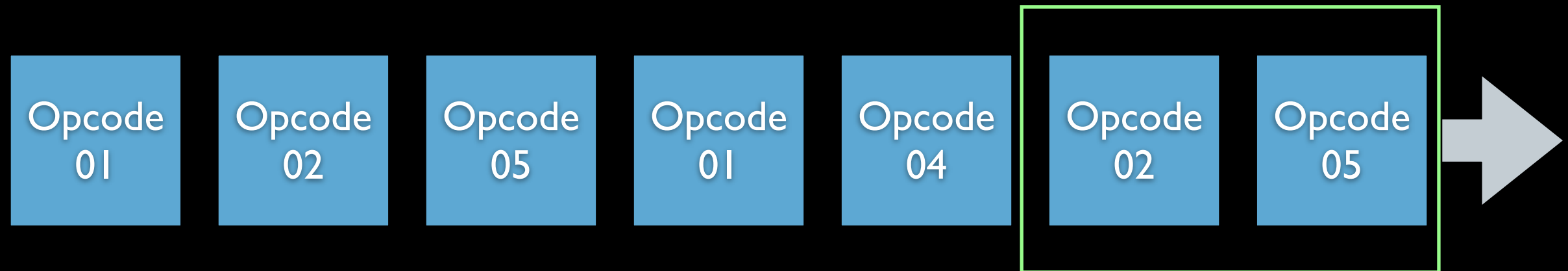
02 - 05 : |

05 - 01 : |

01 - 04 : |

04 - 02 : |

N-gram analysis



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

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



3E	18-1C	00	00	40	00-05
Op	Player				slot
code	Id				position

LOL packets example: 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

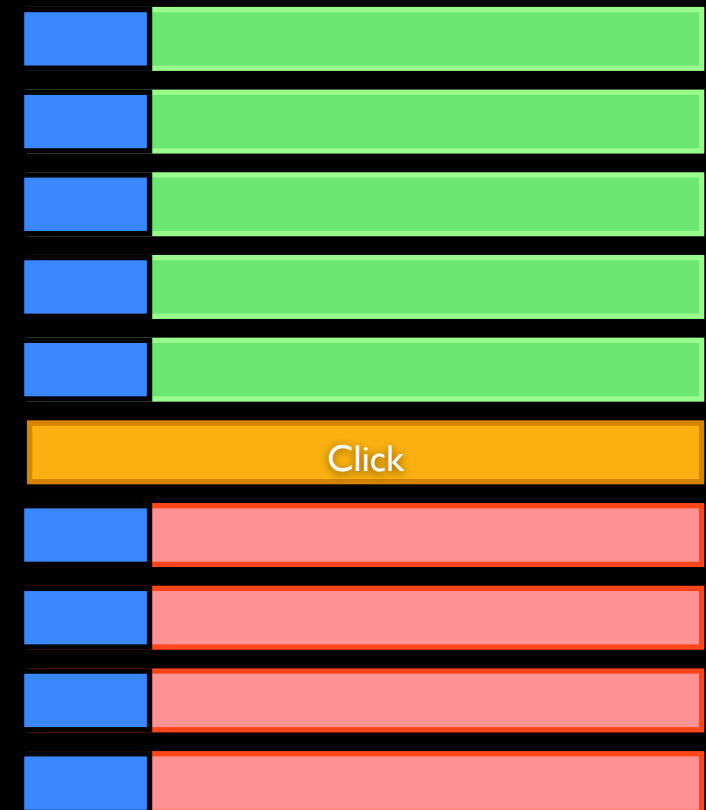
- Listen for a special keystrokes combo
- Inject the event into the trace log
- Use it to isolate interesting part
- Profit



Correlating click / packet

Receipt

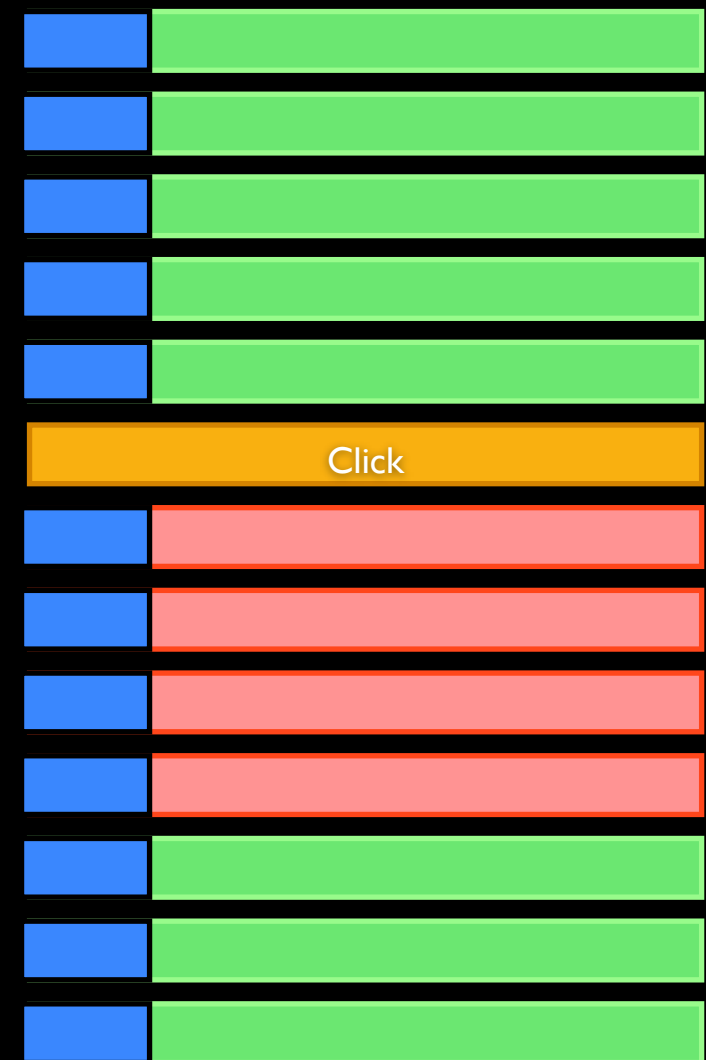
- Listen for a special keystrokes combo
- Inject the event into the trace log
- Use it to isolate interesting part
- Profit



Correlating click / packet

Receipt

- Listen for a special keystrokes combo
- Inject the event into the trace log
- Use it to isolate interesting part
- Profit

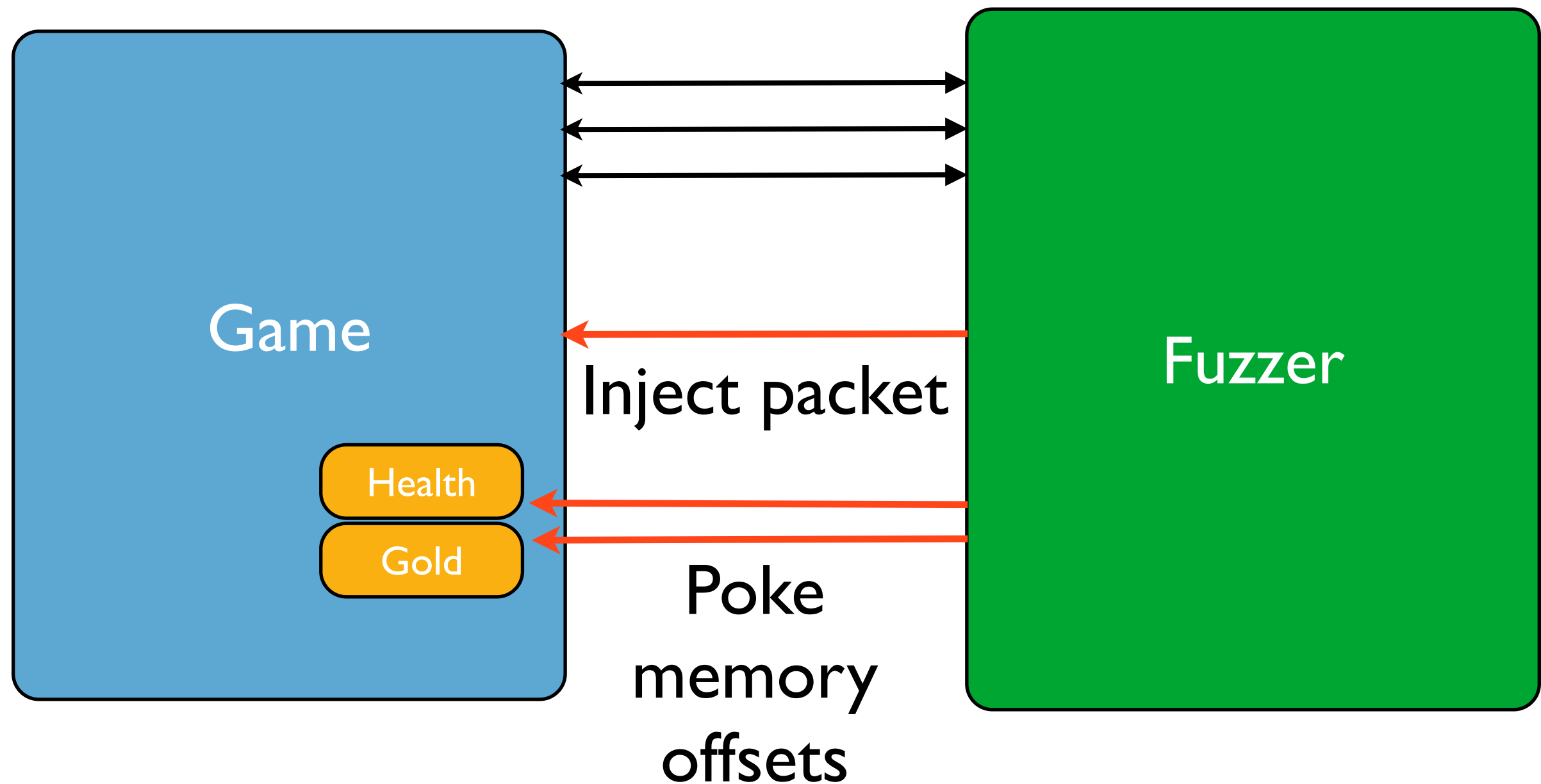


Monitoring results



Is my **packet affected** the
game state ?

Read the state of the game ?



Finding offset



Game
memory

Finding offset



Remove

Game
memory

Finding offset



Remove

Game
memory

Game
memory

Finding offset



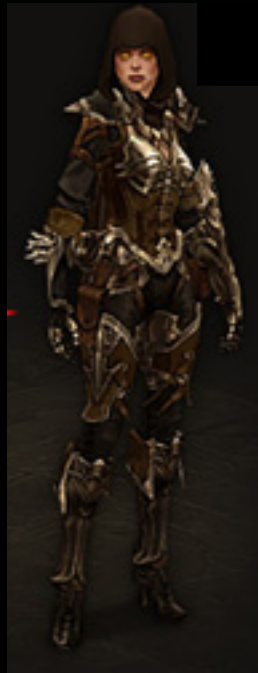
Remove

Add

Game
memory

Game
memory

Finding offset



Remove

Add

Game
memory

Game
memory

Game
memory

Finding offset



Remove

Add

Remove

Add

Game
memory

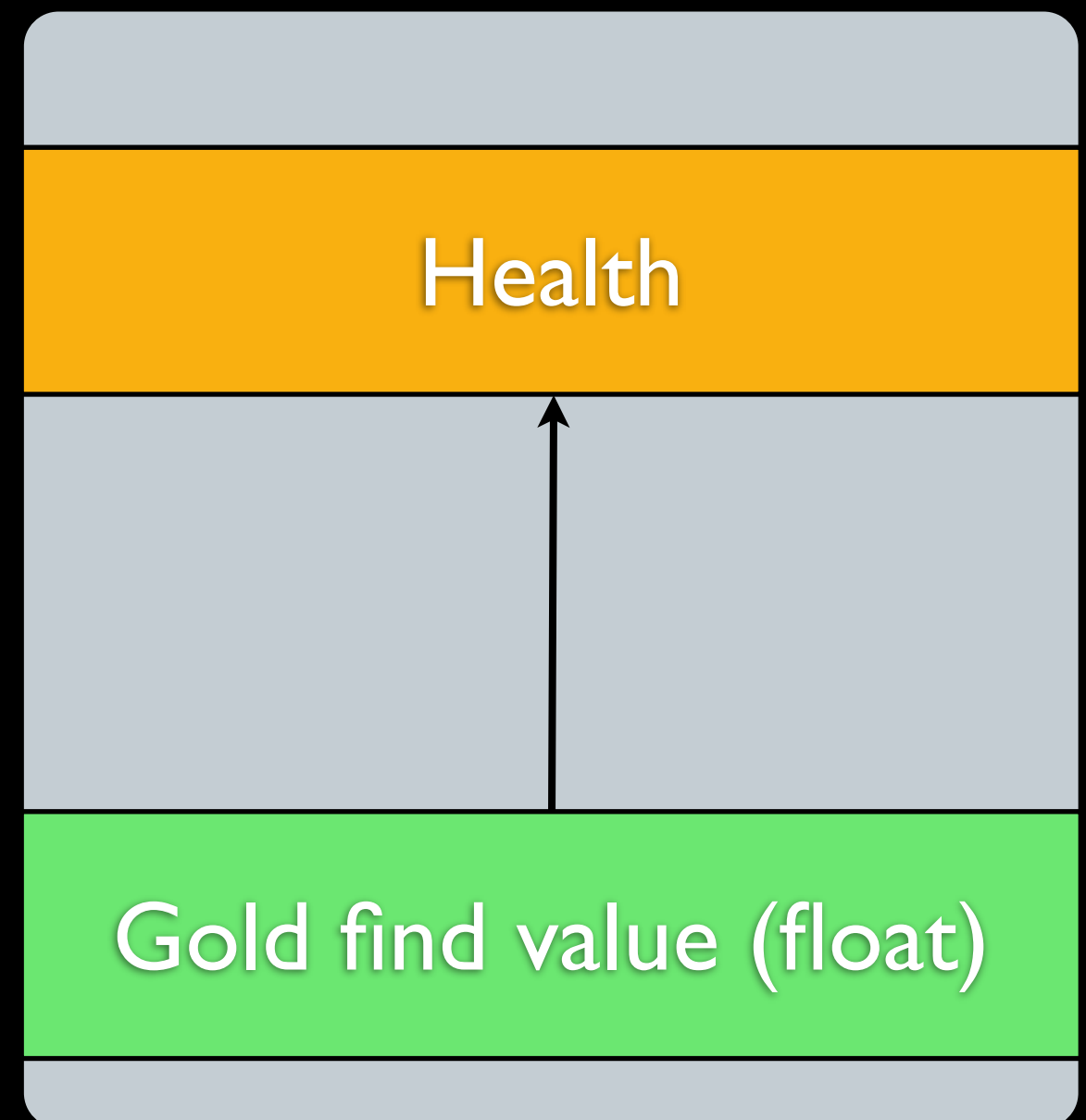
Game
memory

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

