[Re]Vuln

OWNING MULTIPLAYER ONLINE GAMES

(POC 2012 - SEOUL)

Luigi Auriemma & Donato Ferrante

Who are we?

Luigi Auriemma (luigi@revuln.com /@luigi_auriemma)
Co-Founder and Security Researcher at ReVuln Ltd.

Donato Ferrante (donato@revuln.com /@dntbug)
Co-Founder and Security Researcher at ReVuln Ltd.

DAILY-JOB

- breaking software and hardware
- **hunting for Odays..**
- managing **revuln.com**

Agenda

- **Introduction**
- **Why attacking games?**
- **Attack Scenarios**
- **The Market**
- **Warm-up**
  - How to find vulnerabilities in video games
- **Hands On Bug Hunting (demo)**
- **Welcome to the Real World**
  - Call Of Duty: Black Ops
  - Something Unreal
  - Team chat? Teamspeak
  - Game protection? Punkbuster
  - Exploiting the Source (Engine)
- **0day time (demo)**
  - Call Of Duty: Modern Warfare 3 (**0day**)
  - There is some Crysis (**0day**)
- **What about the future?**
- **Conclusion**

DEMO++!

Introduction

- Multiplayer games **are an underestimated field**

- Some numbers:
  - #Multiplayer games: **1 + .. + 99 + 1 + .. + 1**
  - #Multiplayer game players:

    0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, 196418, 317811…
  - **Is this an interesting attack vector?**

Why attacking Games?

Why attacking Games? (1/2)

[Re]Vuln

WHO WANTS TO ATTACK YOUR GAME ?

Script Kiddies

They like running tools made by others, without even knowing how to use them..

Others..

Your room-mate

he doesn't like you wasting bandwidth

Why attacking Games? (2/2)

[Re]Vuln

WHO WANTS TO ATTACK YOUR COMPANY SERVER ?

Script Kiddies
They are everywhere..

Others..
Their target can be one of your players playing on your company server, do you know how many people play online games nowadays ??

Your competitors
the more you are bad, the more they are good

Scenarios

Never feel safe while playing online…

Scenarios (1/2)

[Re]Vuln

CLIENT-SIDE

(1-N)

Victim

Server

Player

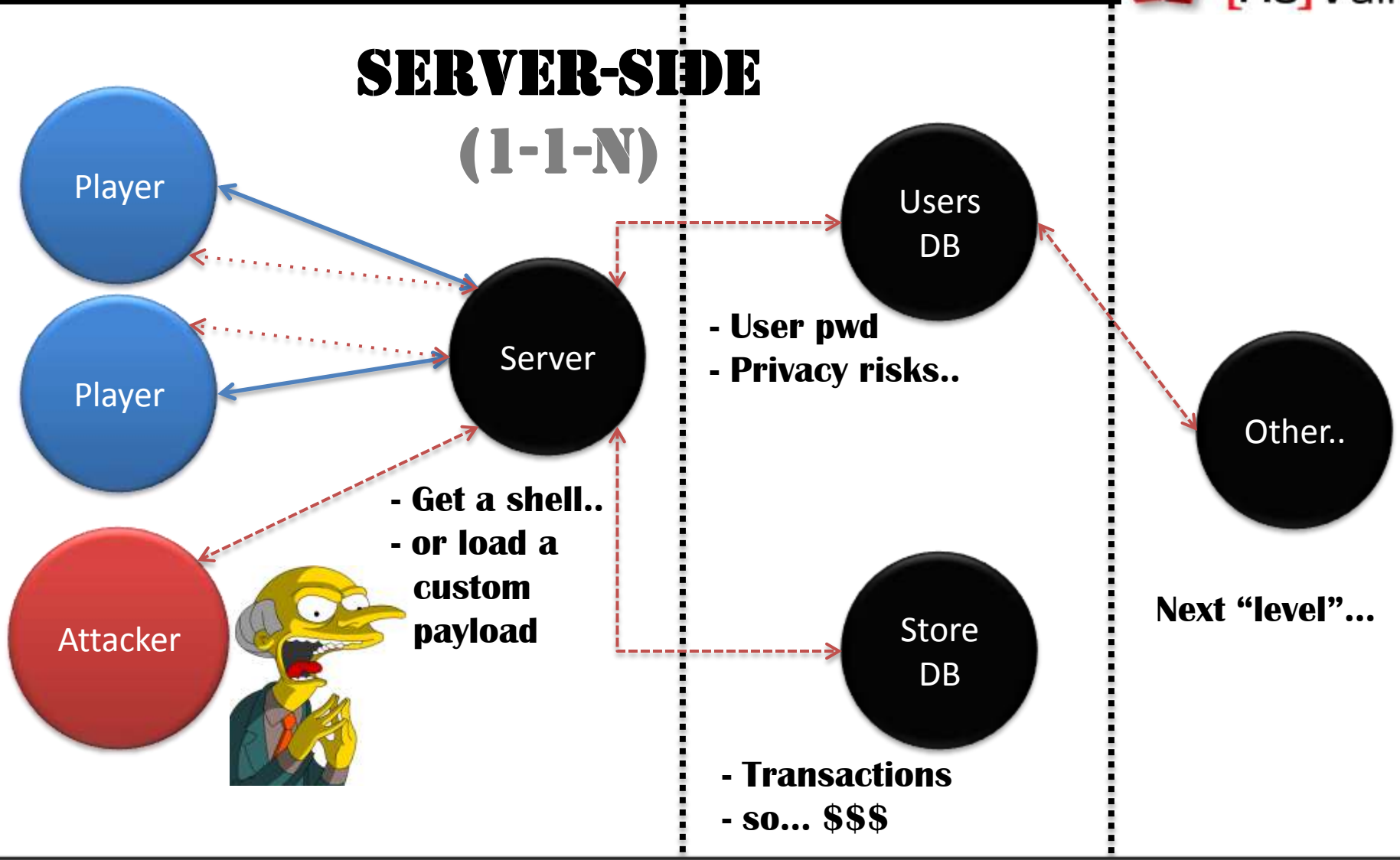
Player

Attacker

1. Get user IP..

2. Profit..

Scenarios (2/2)



The Market

I heard you need expl0its..

The Market (1)

- Yes, there is a **MARKET FOR GAMES VULNERABILITIES**
- **THEY BUY EXPLOITS** for a fair amount of money
- They ask for **NEW ODAY**..

What about trying to spot some vulnerabilities for **FUN/PROFIT ?**

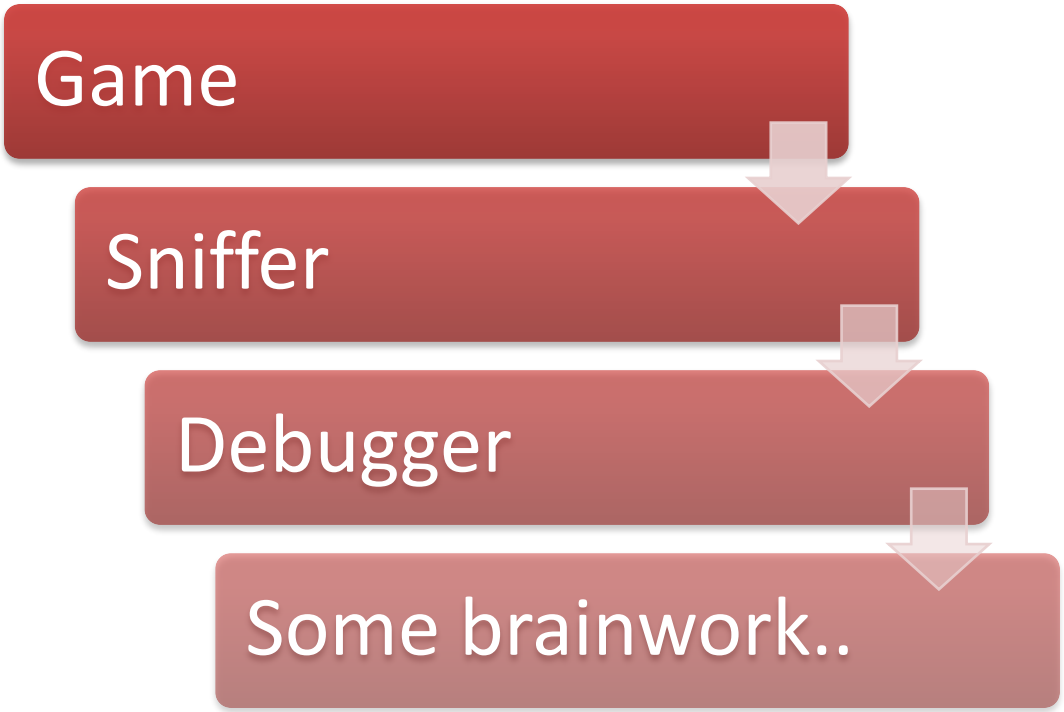
Warm-up

Things to know to start hunting for vulnerabilities in video games

Warm-up (1/7)

[Re]Vuln

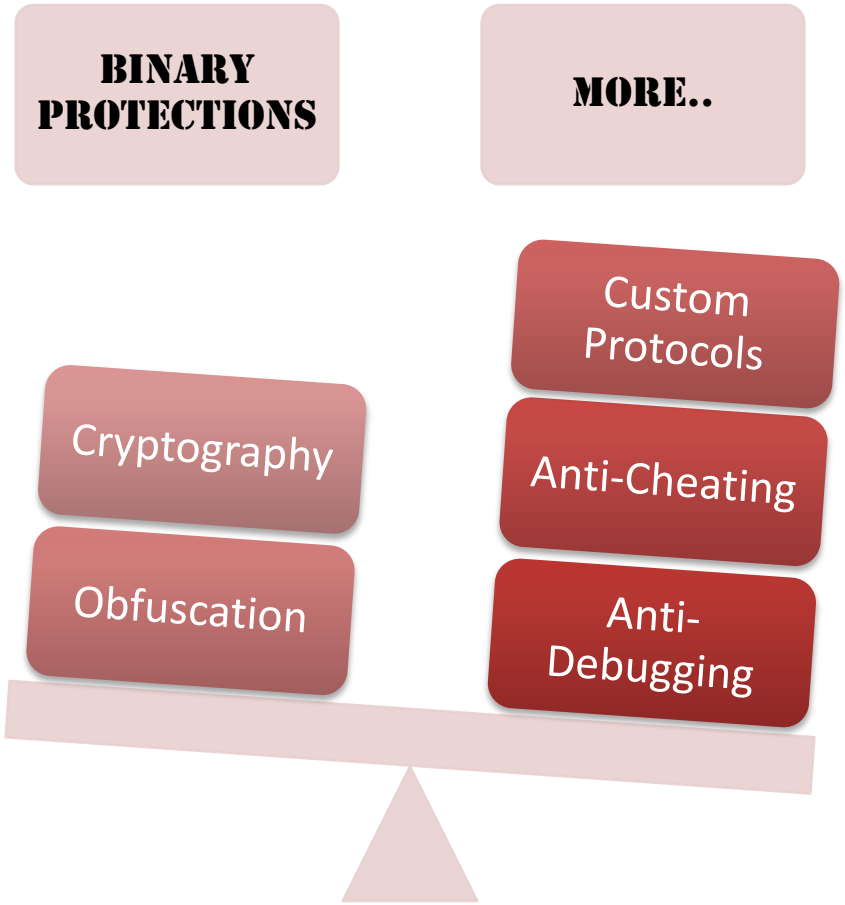
A GENERIC WALKTHROUGH…



Warm-up (2/7)

[Re]Vuln

Games are not an easy target, as it may seem..



Warm-up (3/7)

[Re]Vuln

Some points of interest…

- **Communication**:
  - *recv*
  - *send*
  - *recvfrom*
  - *sendto*
  - *Connect*
  - WSARecv
  - WSASend
  - WSARecvFrom
  - WSASendTo
  - *more..*

- **Cryptography**:
  - *known numbers*
  - *signatures*
  - *more..*

Warm-up (4/7)

[Re]Vuln

CUSTOM-PROTOCOLS…

- **90% of "big" multiplayer games goes over UDP**
  - not a simple UDP, but a reimplementation of TCP over UDP
    - plus some anti-lag mechanisms (players don't like lag..)
    - plus additional stuff..

We must be able to understand which part is useful, and which part is not

Being able to analyze packets on the fly helps…

Warm-up (5/7)

[Re]Vuln

SNIFFERS..

Logging network traffic, without Wireshark, but with a **proxy DLL**:

- ❑ lighter
- ❑ and scriptable (via LUA, Python or Ruby..)

```
HMODULE hm = NULL;

#define CALLING_CONVENTION WINAPI        // default for Windows DLLs
#define PROXY_FUNCTION(FUNCTION_NAME)    /* for the proxified functions not modified */ \
        void CALLING_CONVENTION (FUNCTION_NAME)(void)
#define PROXY_FUNCTIONX(FUNCTION_NAME) \
        static PROXY_FUNCTION(*_##FUNCTION_NAME) = NULL; \
        PROXY_FUNCTION(FUNCTION_NAME) { \
            POP_EBP __asm__("jmp *__"#FUNCTION_NAME); \
        }

#include "proxocket.h"
PROXY_FUNCTIONX(getpeername)
PROXY_FUNCTIONX(getsockname)
PROXY_FUNCTIONX(getsockopt)
PROXY_FUNCTIONX(htonl)
PROXY_FUNCTIONX(htons)
PROXY_FUNCTIONX(inet_addr)
PROXY_FUNCTIONX(inet_ntoa)
PROXY_FUNCTIONX(ioctlsocket)
PROXY_FUNCTIONX(listen)
PROXY_FUNCTIONX(ntohl)
PROXY_FUNCTIONX(ntohs)
PROXY_FUNCTIONX(select)
PROXY_FUNCTIONX(setsockopt)
```

Warm-up (6/7)

[Re]Vuln

DEBUGGING THE RECV'D BUFFER..

```
0059F1DF    CC              INT3
0059F1E0  /$ 83EC 10        SUB ESP,10
0059F1E3  |. 8B4424 14       MOV EAX,DWORD PTR SS:[ESP+14]
0059F1E7  |. 8B08            MOV ECX,DWORD PTR DS:[EAX]
0059F1E9  |. 8B40 04         MOV EAX,DWORD PTR DS:[EAX+4]
0059F1EC  |. 53              PUSH EBX
0059F1ED  |. 55              PUSH EBP
0059F1EE  |. 56              PUSH ESI
0059F1EF  |. 8B7424 24       MOV ESI,DWORD PTR SS:[ESP+24]
0059F1F3  |. 57              PUSH EDI
0059F1F4  |. 8B7E 08         MOV EDI,DWORD PTR DS:[ESI+8]
0059F1F7  |. 897C24 14       MOV DWORD PTR SS:[ESP+14],EDI
0059F1FB  |. 8B7E 0C         MOV EDI,DWORD PTR DS:[ESI+C]
0059F1FE  |. 897C24 10       MOV DWORD PTR SS:[ESP+10],EDI
0059F202  |. 8B7E 04         MOV EDI,DWORD PTR DS:[ESI+4]
0059F205  |. 8B36            MOV ESI,DWORD PTR DS:[ESI]
0059F207  |. 897C24 1C       MOV DWORD PTR SS:[ESP+1C],EDI
0059F20B  |. BA 2037EFC6     MOV EDX,C6EF3720
0059F210  |. 897424 18       MOV DWORD PTR SS:[ESP+18],ESI
0059F214  |. BF 20000000     MOV EDI,20
0059F219  |. 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
0059F220  |> 8B5C24 10       MOV EBX,DWORD PTR SS:[ESP+10]
0059F224  |. 8B6C24 14       MOV EBP,DWORD PTR SS:[ESP+14]
0059F228  |. 8BF1            MOV ESI,ECX
0059F22A  |. C1EE 05         SHR ESI,5
0059F22D  |. 03F3            ADD ESI,EBX
0059F22F  |. 8BD9            MOV EBX,ECX
0059F231  |. C1E3 04         SHL EBX,4
0059F234  |. 03DD            ADD EBX,EBP
0059F236  |. 8B6C24 1C       MOV EBP,DWORD PTR SS:[ESP+1C]
0059F23A  |. 33F3            XOR ESI,EBX
0059F23C  |. 8D1C0A          LEA EBX,DWORD PTR DS:[EDX+ECX]
0059F23F  |. 33F3            XOR ESI,EBX
0059F241  |. 8B5C24 18       MOV EBX,DWORD PTR SS:[ESP+18]
0059F245  |. 2BC6            SUB EAX,ESI
0059F247  |. 8BF0            MOV ESI,EAX
0059F249  |. C1E6 04         SHL ESI,4
0059F24C  |. 03F3            ADD ESI,EBX
0059F24E  |. 8BD8            MOV EBX,EAX
0059F250  |. C1EB 05         SHR EBX,5
0059F253  |. 03DD            ADD EBX,EBP
0059F255  |. 33F3            XOR ESI,EBX
0059F257  |. 8D1C02          LEA EBX,DWORD PTR DS:[EDX+EAX]
0059F25A  |. 33F3            XOR ESI,EBX
0059F25C  |. 2BCE            SUB ECX,ESI
0059F25E  |. 81C2 4786C861   ADD EDX,61C88647
0059F264  |. 4F              DEC EDI
0059F265  |.^75 B9           JNZ SHORT          _ 0059F220
0059F267  |. 8B5424 24       MOV EDX,DWORD PTR SS:[ESP+24]
0059F26B  |. 5F              POP EDI
0059F26C  |. 5E              POP ESI
```

It's common for commercial games to use **encryption/compression algorithms**, we usually need to reverse them to reach the core..

```
268 void tea_decrypt(uint32_t *p, uint32_t *keyl) {
269     uint32_t    y,
270                 z,
271                 sum,
272                 a = keyl[0],
273                 b = keyl[1],
274                 c = keyl[2],
275                 d = keyl[3];
276     int         i;
277
278     y = p[0];
279     z = p[1];
280     sum = 0xc6ef3720;
281     for(i = 0; i < 32; i++) {
282         z -= ((y << 4) + c) ^ (y + sum) ^ ((y >> 5) + d);
283         y -= ((z << 4) + a) ^ (z + sum) ^ ((z >> 5) + b);
284         sum -= 0x9e3779b9;
285     }
286     p[0] = y;
287     p[1] = z;
288 }
```

Warm-up (7/7)

.. AND THE OPCODES PROCESSING

```
395F2905  . C2 0C00          RETN 0C
395F2908  > 0FB6C0           MOVZX EAX,AL
395F290B  . 48               DEC EAX                          Switch (cases 1..91)
395F290C  . 3D 90000000      CMP EAX,90
395F2911  .v0F87 2B010000    JA          .395F2A42
395F2917  . 0FB680 782A5F39  MOVZX EAX,BYTE PTR DS:[EAX+395F2A78]
395F291E  . FF2485 4C2A5F39  JMP DWORD PTR DS:[EAX*4+395F2A4C]
395F2925  > 8B4C24 1C        MOV ECX,DWORD PTR SS:[ESP+1C]    Cases 8E,8F,90 of switch 395F290B
395F2929  . 51               PUSH ECX
395F292A  . 55               PUSH EBP
395F292B  . 57               PUSH EDI
395F292C  . 8D4B F0          LEA ECX,DWORD PTR DS:[EBX-10]
395F292F  . E8 CCBBFFFF      CALL C.     .395EE500
395F2934  . 5F               POP EDI
395F2935  . 5E               POP ESI
395F2936  . 5D               POP EBP
395F2937  . 5B               POP EBX
395F2938  . C2 0C00          RETN 0C
395F293B  > 8B4B 08          MOV ECX,DWORD PTR DS:[EBX+8]     Case 1 of switch 395F290B
395F293E  . 8B4424 1C        MOV EAX,DWORD PTR SS:[ESP+1C]
395F2942  . 8B51 04          MOV EDX,DWORD PTR DS:[ECX+4]
395F2945  . 8B52 04          MOV EDX,DWORD PTR DS:[EDX+4]
395F2948  . 50               PUSH EAX
395F2949  . 83C1 04          ADD ECX,4
395F294C  . 55               PUSH EBP
395F294D  . 57               PUSH EDI
395F294E  . FFD2             CALL EDX
395F2950  . 5F               POP EDI
395F2951  . 5E               POP ESI
395F2952  . 5D               POP EBP
395F2953  . 5B               POP EBX
395F2954  . C2 0C00          RETN 0C
395F2957  > 8B4424 1C        MOV EAX,DWORD PTR SS:[ESP+1C]    Case 5 of switch 395F290B
395F295B  . 50               PUSH EAX                         Arg3
395F295C  . 55               PUSH EBP                         Arg2
395F295D  . 57               PUSH EDI                         Arg1
395F295E  . 8D4B F0          LEA ECX,DWORD PTR DS:[EBX-10]
395F2961  . E8 2A93FFFF      CALL C.     .395EBC90
395F2966  . 5F               POP EDI
395F2967  . 5E               POP ESI
395F2968  . 5D               POP EBP
395F2969  . 5B               POP EBX
395F296A  . C2 0C00          RETN 0C
395F296D  > 57               PUSH EDI                         Arg1; Case 6 of switch 395F290B
395F296E  . 8D4B F0          LEA ECX,DWORD PTR DS:[EBX-10]
395F2971  . E8 7A94FFFF      CALL C.     .395EBDF0
395F2976  . 5F               POP EDI
395F2977  . 5E               POP ESI
395F2978  . 5D               POP EBP
395F2979  . 5B               POP EBX
395F297A  . C2 0C00          RETN 0C
```

THE MOST INTERESTING PART..

Hands On Bug Hunting (D)

[Re]Vuln

Welcome to the Real World

Welcome to the Real World (1/15)

[Re]Vuln

- **Call Of Duty: Black Ops**
  (remote memory disclosure)
- **Unreal**
  (remote code execution)
- **Teamspeak**
  (admin commands without admin permissions)
- **Punkbuster**
  (exploiting a protection to get an attack vector)
- **Source Engine**
  (fragments memory corruption, file upload and format string)

Welcome to the Real World (2/15)

Call Of Duty: Black Ops (remote memory disclosure) 1/3

Call of Duty Black Ops is a game from the CoD series.

BUG: When the server receives an **RCON PACKET** (**opcode 0x00**) it replies with a packet having a fixed size of **1168** bytes, and it doesn't matter if its content is smaller.

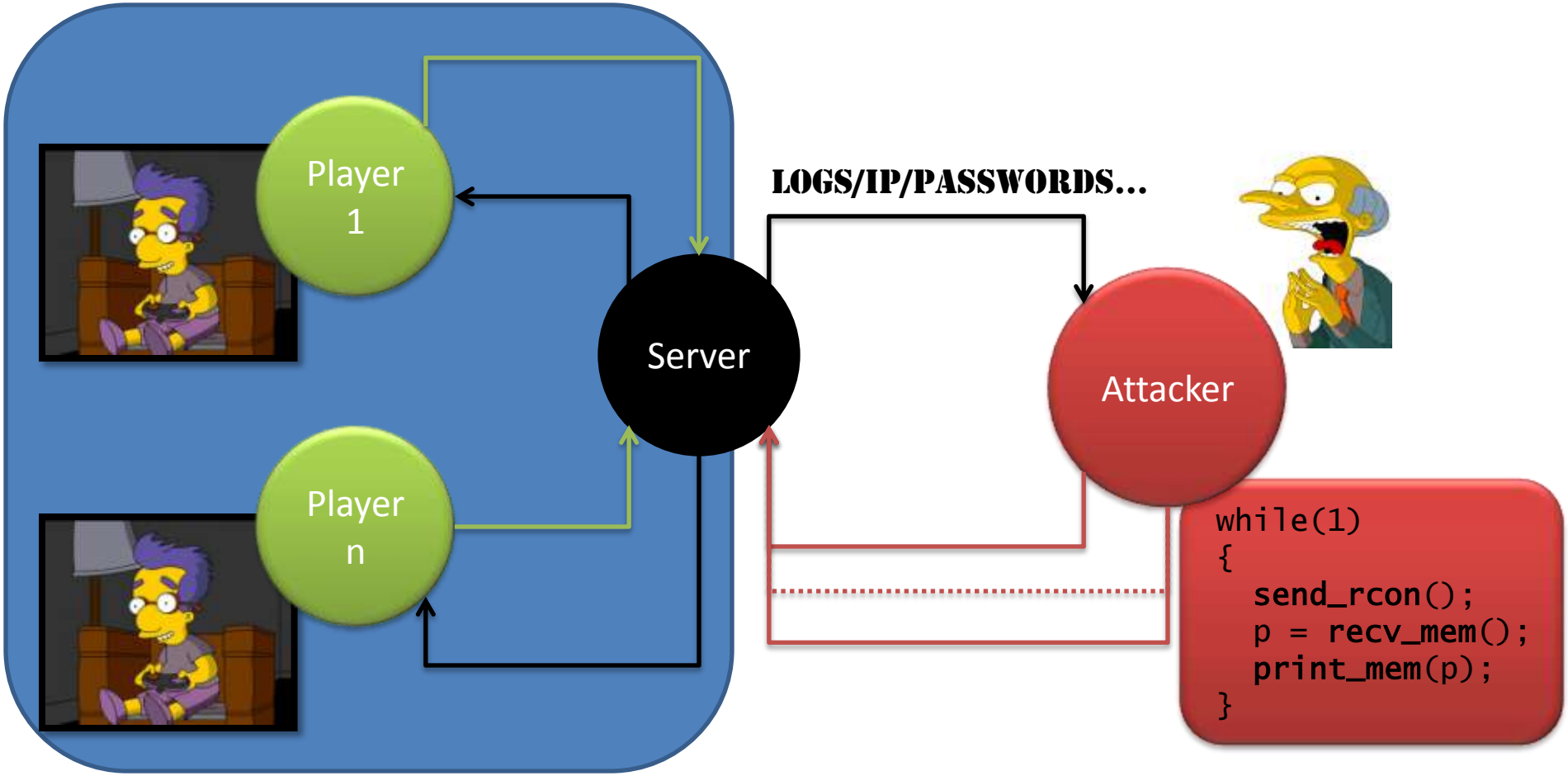
The result is that various parts of the **server's memory are disclosed remotely** to anyone sending various invalid **RCON PACKETS**. So an attacker can retrieve:

- ❑ **rcon passwords** (via cvars)
- ❑ **logs** (rcon info)
- ❑ **client IPs**
- ❑ **…**

Welcome to the Real World (3/15)

[Re]Vuln

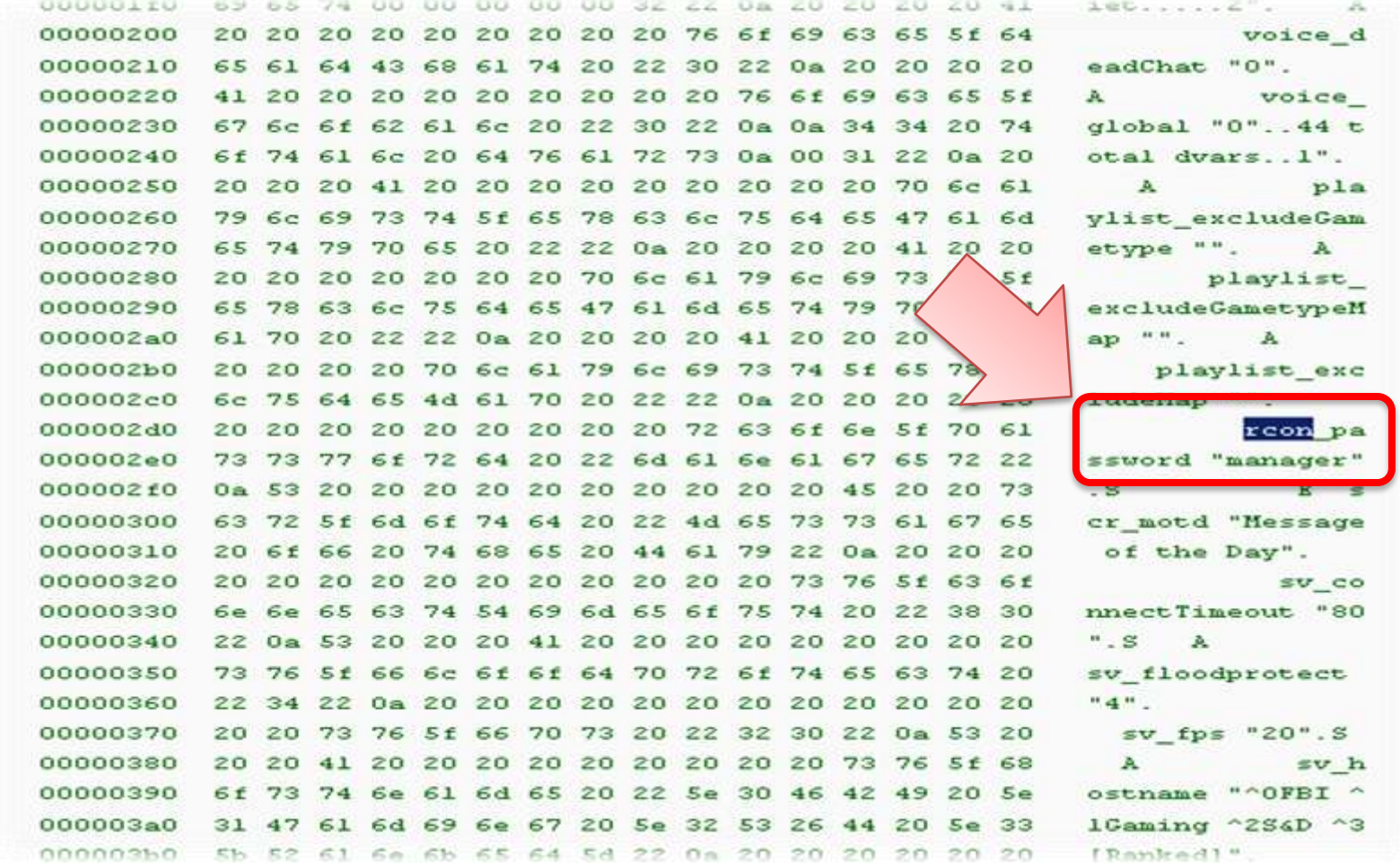
Call Of Duty: Black Ops (remote memory disclosure) 2/3



Welcome to the Real World (4/15)

[Re]Vuln

Call Of Duty: Black Ops (remote memory disclosure) 3/3



```
00000200  20 20 20 20 20 20 20 20 20 76 6f 69 63 65 5f 64   voice_d
00000210  65 61 64 43 68 61 74 20 22 30 22 0a 20 20 20 20  eadChat "0".
00000220  41 20 20 20 20 20 20 20 20 20 76 6f 69 63 65 5f  A  voice_
00000230  67 6c 6f 62 61 6c 20 22 30 22 0a 0a 34 34 20 74  global "0"..44 t
00000240  6f 74 61 6c 20 64 76 61 72 73 0a 00 31 22 0a 20  otal dvars..1".
00000250  20 20 20 41 20 20 20 20 20 20 20 20 20 20 70 6c     A          pl
00000260  79 6c 69 73 74 5f 65 78 63 6c 75 64 65 47 61 6d  aylist_excludeGam
00000270  65 74 79 70 65 20 22 22 0a 20 20 20 20 41 20 20  etype "".    A
00000280  20 20 20 20 20 20 70 6c 61 79 6c 69 73 74 5f 65        playlist_e
00000290  78 63 6c 75 64 65 47 61 6d 65 74 79 70 65 4d 61  xcludeGametypeMa
000002a0  70 20 22 22 0a 20 20 20 20 41 20 20 20 20 20 20  p "".    A
000002b0  20 20 20 20 70 6c 61 79 6c 69 73 74 5f 65 78 63      playlist_exc
000002c0  6c 75 64 65 4d 61 70 20 22 22 0a 20 20 20 20 20  ludeMap "".
000002d0  20 20 20 20 20 20 20 20 20 72 63 6f 6e 5f 70 61           rcon_pa
000002e0  73 73 77 6f 72 64 20 22 6d 61 6e 61 67 65 72 22  ssword "manager"
000002f0  0a 53 20 20 20 20 20 20 20 20 20 20 20 45 20 20  .S           E
00000300  63 72 5f 6d 6f 74 64 20 22 4d 65 73 73 61 67 65  cr_motd "Message
00000310  20 6f 66 20 74 68 65 20 44 61 79 22 0a 20 20 20   of the Day".
00000320  20 20 20 20 20 20 20 20 20 20 73 76 5f 63 6f           sv_co
00000330  6e 6e 65 63 74 54 69 6d 65 6f 75 74 20 22 38 30  nnectTimeout "80
00000340  22 0a 53 20 20 20 41 20 20 20 20 20 20 20 20 20  ".S   A
00000350  73 76 5f 66 6c 6f 6f 64 70 72 6f 74 65 63 74 20  sv_floodprotect
00000360  22 34 22 0a 20 20 20 20 20 20 20 20 20 20 20 20  "4".
00000370  20 20 73 76 5f 66 70 73 20 22 32 30 22 0a 53 20    sv_fps "20".S
00000380  20 20 41 20 20 20 20 20 20 20 20 20 73 76 5f 68    A        sv_h
00000390  6f 73 74 6e 61 6d 65 20 22 5e 30 46 42 49 20 5e  ostname "^0FBI ^
000003a0  31 47 61 6d 69 6e 67 20 5e 32 53 26 44 20 5e 33  1Gaming ^2S&D ^3
000003b0  5b 52 61 6e 6b 65 64 5d 22 0a 20 20 20 20 20 20  [Ranked]".
```

Welcome to the Real World (5/15)

[Re]Vuln

Something Unreal (RCE) 1/2

These vulnerabilities target a **game engine** (http://unreal.epicgames.com)

Vulnerable games:

- ❑ **DeusEx**
- ❑ **Devastation**
- ❑ **Mobile Forces**
- ❑ **Nerf Arena Blast**
- ❑ **Postal 2**
- ❑ **Rune**
- ❑ **Tactical Ops**
- ❑ **TNN Pro Hunter**
- ❑ **Unreal 1**
- ❑ **Unreal II XMP**
- ❑ **Unreal Tournament**
- ❑ **Unreal Tournament 2003**
- ❑ **Unreal Tournament 2004**
- ❑ **and other…**

BUG: Almost all the games based on the Unreal engine support the **"secure" query**. This type of query is part of the so called **Gamespy query protocol**.

The query is a simple UDP packet like **\secure\ABCDEF**

If an attacker uses a long value in his secure query, the server engine will overwrite some memory locations.

Both remote code execution and spoofing are possible.

Welcome to the Real World (6/15)

[Re]Vuln

Something Unreal (RCE) 2/2

The proof-of-concept:

1 UDP packet to the query port of the game server:

\secure\aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...aaaa

A nice **OLD SCHOOL OVERFLOW...**

Welcome to the Real World (7/15)

[Re]Vuln

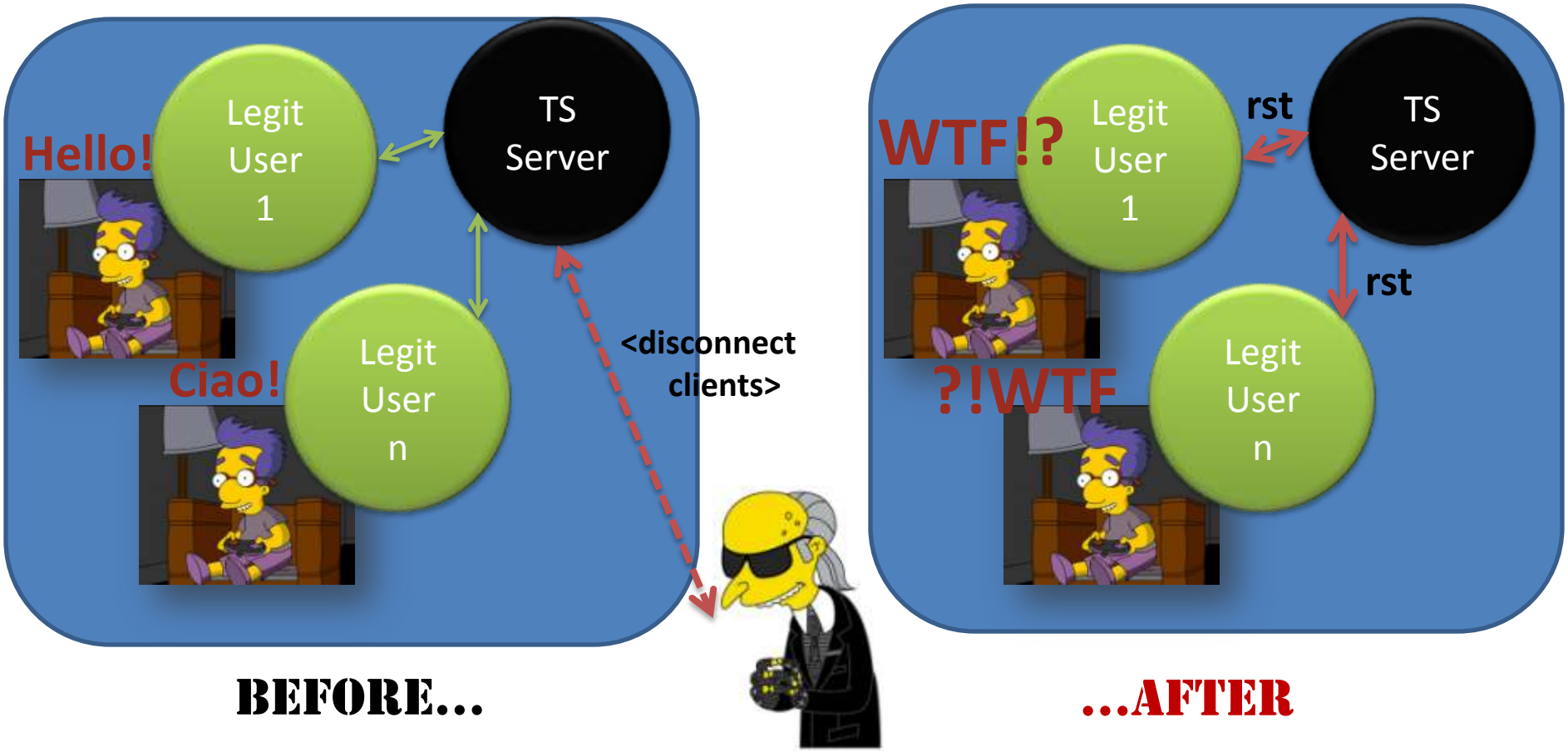
Team chat? Teamspeak! (admin privs) 1/2

TeamSpeak 3 is a version of one of the most popular VOIP software intended mainly for gamers.

BUG: execution of various admin commands. The commands available are exactly those described in the TeamSpeak 3 ServerQuery Manual.

Welcome to the Real World (8/15)

Team chat? Teamspeak! (admin privs) 2/2



Welcome to the Real World (9/15)

[Re]Vuln

Game protection? Punkbuster! (as attack vector) 1/2

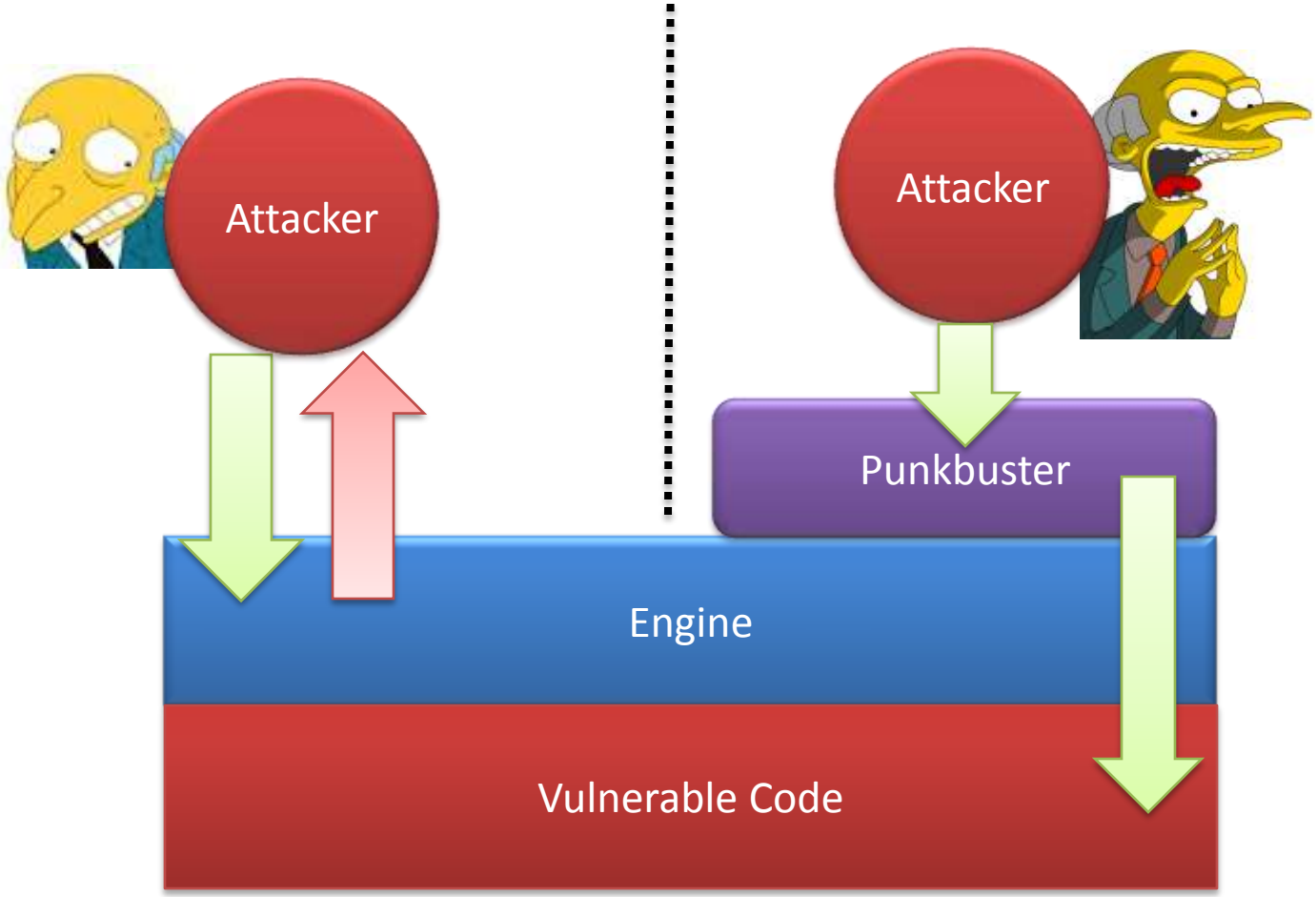
PunkBuster is a loved/hated **anti-cheat system** developed by Even Balance (www.evenbalance.com) and officially used in many diffused games like **America's Army, Battlefield 1942/Vietnam/II, Call of Duty, Doom 3** and almost all the games based on the **Quake 3 engine**.

- **Format string** versus games using PunkBuster:
  - SOLDIER OF FORTUNE 2
  - QUAKE 4
  - DOOM 3
  - PREY
  - others

Welcome to the Real World (10/15)

[Re]Vuln

Game protection? Punkbuster! (as attack vector) 2/2



[Re]Vuln

Exploiting the Source [Engine] (intro) 1/4

The Source engine is a rewrite of the original **Half-Life** engine developed by **Valve** (www.valvesoftware.com). It's the engine used for games like **Half-Life 2**, **Counter Strike Source**, **Team Fortress 2**, **Left 4 Dead** and various others which are also the most played internet multiplayer games with over **10000 online servers**.

- ❑ FRAGMENTS MEMORY CORRUPTION
- ❑ FILE UPLOADING

Exploiting the Source [Engine] (fragment mem. corr.) 2/4

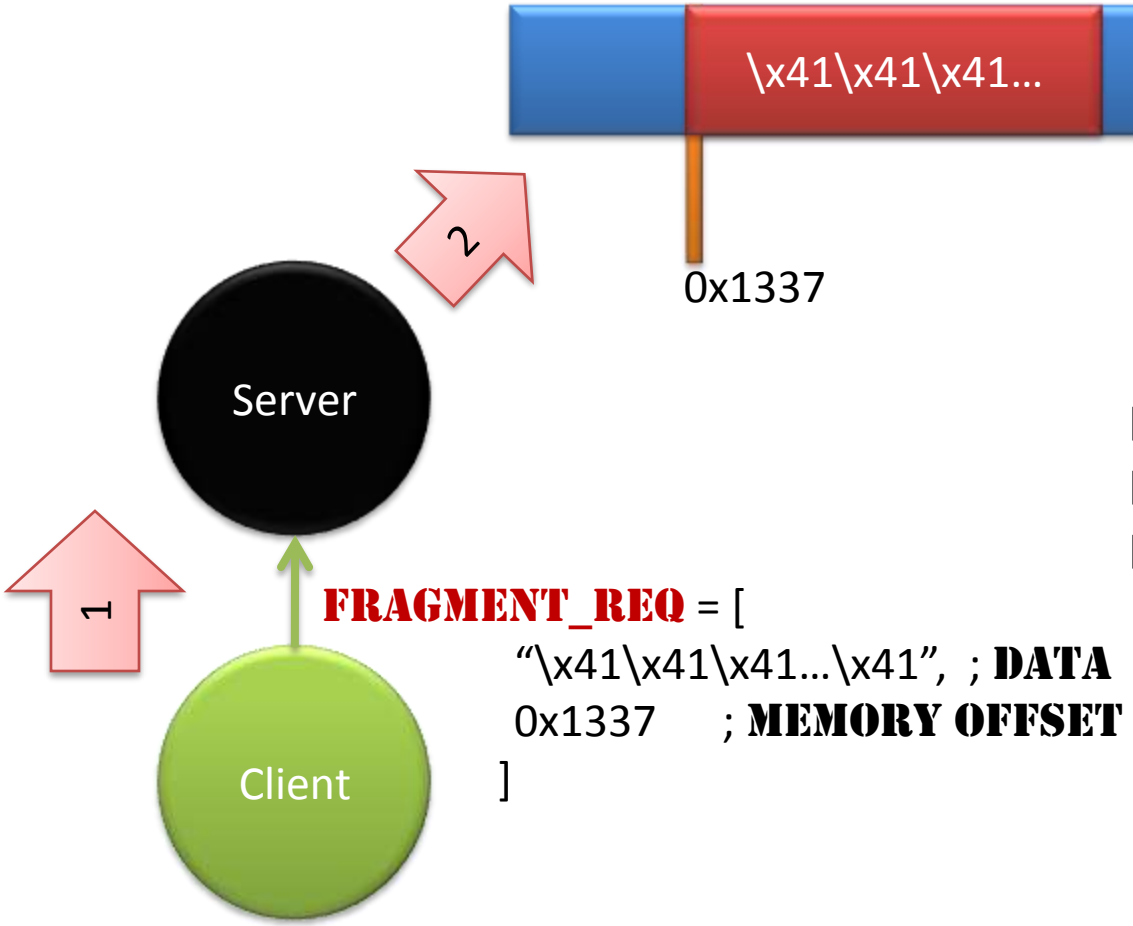
Source engine implements a **complex method** for handling fragmented packets.

A small heap buffer is assigned to contain the entire packet, and the client can decide arbitrarily the offset for placing the new fragment in a certain range bigger than the available memory.

The memory assigned to handle the packet can be in the range [**0, 0X3FFF00**] and the maximum amount of data that can be contained in a packet (fragment) is: **0X700**.

Welcome to the Real World (13/15)

Exploiting the Source [Engine] (fragment mem. corr.) 3/4



FRAGMENT_REQ = [
"\x41\x41\x41…\x41", ; **DATA**
0x1337 ; **MEMORY OFFSET**
]

A WAY TO EXPLOIT:

- ❑ Locate a function pointer
- ❑ Override the pointer address
- ❑ Pr0fit..

[Re]Vuln

Exploiting the Source [Engine] (file uploading) 4/4

By default the Source engine allows downloading and uploading files.

While the download operation is denied if there is a slash or a *".."* or an unsupported extension in the requested file, for the **upload operation there are just no checks**.

Interesting related bug:
If the name of the file to upload contains a slash or backslash at its end, like *"c:\file.txt/"* or *"c:\file.txt\"*, a folder with such name will be created, and **in case the file with the provided name exists it will be deleted**.

WHAT HAPPENS IF YOU REMOVE SOME WINDOWS FILE ?

Welcome to the Real World (15/15)

[Re]Vuln

Some Game-Specific Vulnerabilities..

- **Map Loading Attack:**
  - Interesting because they have a lot of **complex functions**..
- **Fake-Players Attack:**
  - Consists of sending several "**zombies**" in a game, avoiding legit players to join the match, because the server will be full..

- **DoS Forward via Server:**
  - Usually **anonymous** (1 UDP packet) and the server will forward the "**attacker**" request to any connected clients..

0day time


you killed [ASS]josh
you killed alber_34
you killed eXterminator64
you killed [xXx] offembach
you killed [=vVv=] mui
you killed Lt. super sniper
you killed lone_wolf_88
you killed too_rambo_for_u
you killed mushroom
you killed smoke_joints
you killed [SS] panzerfaust90
you killed SS] atman

0day time (1/2) (D)

[Re]Vuln

DEMO

0day time (2/2) (D)

[Re]Vuln

DEMO

Post-0day thoughts

[Re]Vuln

What about the future?

Simple: MMOG / MMORPG / and all the variations of MMO…

Server-side risks:

- ❑ You don't have (99%) a local server for testing, legal problems if you crash an online server

Client-side risks:

- ❑ If they spot (via anti-cheating) your testing, your account will be banned..

Conclusion

- Games are no longer for kids..
- Multiplayer games are getting more complex
  - remember: **more complex = more security concerns**
- Games are an exceptional **stealth attack** vector due to their low visibility
  - Playing Online **!=** Safe

MULTIPLAYER GAMES
ARE THE NEXT STEP FOR
OFFENSIVE SECURITY.

More?


If you like this topic, and you want more information or consulting:
info@revuln.com

Thanks!

[Re]Vuln

QUESTIONS ?

Web: revuln.com / **Info:** info@revuln.com / **Twitter:** @revuln