Obligatory who is this guy?

- Adrian Bednarek
- Security Analyst/Researcher at ISE (Independent Security Evaluators)
- Started in the security field as a mostly ethical blackhat*
  - Creating side channel ‘in app purchase’ functionality
    - E.g. Selling gold and virtual goods on ebay, then playerauctions/wholesale
    - First sale – castle in Ultima Online
    - Over 100+ 0day virtual economy exploits in 24+ online games
- Here to talk about common exploits in MMORPG’s
  - Tools
  - Methods
  - Challenges!
What is an MMORPG?

- Massively Multiplayer Online Role Playing Game
  - Single virtual world with multiple thousands of players interacting
- Typically used to be windows based
  - MMORPG’s are highly popular on iOS/Android
Overly simplified game architecture

Interacts With

Game Client

ProcessUIEvent(anEvent)
- >SendDataRoutine(Buffer)
- >Encrypt(Buffer)
- >Send(Buffer)

Send Updates

Single UI Thread

Game Server

RecvData()
- >RecvDataRoutine(Buffer)
- >Decrypt(Buffer)
- >Process(Buffer)

Receive Updates
Player Demographics

Gender and Age Distribution

N male = 2439, N female = 404

https://www.gamasutra.com/view/feature/130552/unmasking_the_avatar_the_.php
Player Demographics

https://www.gamasutra.com/view/feature/130552/unmasking_the_avatar_the_.php
MMORPG Popularity

- Lots of players across many demographics!

MMORPG Business Model

- **Early Days (1990s to early 2010 years)**
  - Subscription model
  - Buy a box
  - Includes 30 days of playtime
    - To continue playing you typically pay $15 per month
      - Unlimited unrestricted play (all you can eat!)
  - Seldomly used these days
MMORPG Business Model

- Current
  - Free/One time fee for game
  - In app purchase model
    - Buy items that enhance gameplay
      - 'Pay 2 Win' complaints
        - Cosmetic items
    - Play time limit
      - To continue playing pay more
        - Or wait! (maybe*)
MMORPG Business Model

*South Park Studios – Freemium Isn’t Free
MMORPG Business Model

*South Park Studios – Freemium Isn’t Free
MMORPG Business Model

*South Park Studios – Freemium Isn’t Free
Pay for virtual game goods?

- Paying for virtual game goods
  - That’s crazy talk!
  - Why not just hack it?
- But first... Integer overflows!
Integer Overflows!
Integer Overflows!
Integer Overflows!
Pay for virtual game goods?

- An integer overflow in the wild:
  - Demo: WSO.flv
Pay for virtual game goods?

- Submit a buy order for max signed int64
  - 7FFFFFFF FFFFFFFF
- Server adds a small fee
- 7FFFFFFF FFFFFFFF + fee = integer roll into negative
- >8000000 00000000
- This then gets subtracted from the player account balance
Pay for virtual game goods?

- Subtracting a negative number puts you in the positive
  - e.g. 5 - -8 = 13
- 9.038904600371e+018
- 9 Quintillion gold! (credits)
- (Implications later)

Log + Debug command to show player money
MALICIOUS ACTORS

Hacking MMORPGs
But first...Motivation?

1) For the lulz:

lulz

/ˈləlz/  n

noun informal

fun, laughter, or amusement, especially that derived at another's expense. "the splinter group embarked on a spree of daring cyberattacks for the lulz"
But first...Motivation?

- 2) For profit:
Type 1) Adversaries/Researchers

- Researchers
  - Can I bypass client side checks
  - What kind of encryption is being used
  - What libraries are being used?
  - Can I view art/sound files?
  - How does the protocol work
  - How do they validate inputs
Type 2) Adversaries/Hackers

- Cheaters/Hackers (for the advantage)
  - Client RE
  - Modify game client
    - Runtime
    - Static
  - Typically to gain advantage over players
  - Disruptive
    - Upset players (ever been 360 noscoped?)
Type 3) Adversaries/Professional Hackers

- For profit
  - In game commodities
- Tools/Bots
  - Custom
  - Off shelf
- 0-Days
  - Server compromise
  - Client compromise
- Countermeasure evasion
  - High level statistics
  - Client modification

*https://github.com/ncatlin/rgat*
Type 4) Adversaries/Nation states

- Nation states? *(In my game?... its more likely than you think.)*

- North Korea
  - employing MMO hackers to fund government

- South Korea
  - 30 North Korean operatives
    - Bot and farm 6 million USD$ worth of digital goods (L2)
Adversaries/Nation states

- Chinese prisoners
  - Forced to farm World of Warcraft gold
  - 300 prisoners play WoW 12 hours a day
    - Generate ~800 USD$ per day
Type 5) Adversaries/Chinese Farmers

- Over 100k active farmers
- Typically
  - Bot assisted
  - Manual
- Sweatshop like conditions
- Detrimental to gameplay
  - Spawn camping
  - Resource sniping
Hacking for profit?

- What a million looks like in USD$
- Weighs about 22 lbs.
Hacking for profit

- What a million USD looks like in Elder Scrolls Online Currency
- < billionth of a billionth of a gram, or 0.000000000000000001g*
Hacking for profit

- 1 million ESO gold sells for about 77$
Hacking for profit?

- 77$ per million ESO gold
- $1,000,000/77 = 12,987 million units of ESO gold
- 12,987,000,000 gold

That seems like a lot of gold!

How easy would it be to get that much?

- Manually – forever
- Hacking...
Remember WildStar?

- 5$ per million units of WildStar gold
Hacking for profit?

- 5$ per million WSO gold
- ~ 9 Quintillion gold
- \( \frac{9038904600371000000}{1,000,000} \times 5 = 45,194,523,001,855 \) USD$
- 45 Trillion Dollars
Challenges

- Countermeasures
  - Then – Nearly none
  - Now – Many! (Advanced!)
    - Proprietary encryption
    - Anti Debugging
    - Packet integrity checks
    - Packet sequencing
    - Server side statistics (e.g. Sudden jumps in player wealth)
    - Client/Host machine fingerprinting
    - Code flow obfuscation!

- Advanced countermeasures help threats
Type A Game Client (Easy)
Type A Insertion Point

Typical Game Client: Type A flow

UI Processing Layer

0x005138B0: Login(...)
0x0049CE00: Move(...)
0x005F8B0B: Trade(...)
0x0044AC00: Attack(...)
0x004A890A: ChatMsg(...)

0x004FCAAE: DispatchMessage(...)

0x00500010: EncryptMessage(...)

0x005C904C: WSASend(...)

Series of tubes (Internet)
Type A Insertion Point

Typical Game Client: Type A flow

UI Processing Layer

0x005138B0: LogIn(…)
0x0049CE00: Move(…)
0x005F8B0B: Trade(…)
0x0044AC00: Attack(…)
0x004A890A: ChatMsg(…)

0x004FCAAE: DispatchMessage(…)

0x00500010: EncryptMessage(…)

0x005C904C: WSARecv(…)

Series of tubes (Internet)
Pros

- Complete takeover of the incoming and outgoing client to server messages
- Data can be routed to off computer tools to analyze and modify packets.
- Cheat/Hack detection irrelevant

Cons

- Time consuming
- Must RE encryption/Negotiation
- Must RE any hashing/checksums
- Must RE and takeover any sequencing of packets
- Must have prior knowledge of message encoding structure i.e. how do you know where data for one packet begins and ends?
- Encryption/Packet structure probably will change every patch
Pros

- Modify global values that dictate gameplay behavior
- Movement Speed
- Character Location
- Wall hacking (disable collision)

Cons

- Time consuming
  - RE each behavior and find where code handling it is
- Can miss a lot of hidden code features or messages being sent to server that may do more interesting things!
Pros

- Complete takeover of the incoming and outgoing client to server messages
- Can be done pre encryption/checksum for outgoing
- Can be done post decryption/checksum for incoming messages
- Easily inject forged packets to outgoing or incoming data stream
- Automatic detection of packet boundaries

Cons

- Need custom tools
- Lots of RE
- Client anti-cheat/modification detection is possible*
Methodology Demo

- Runtime binary data flow analysis
  - thread-hello.mp4
Summary

- Extreme obfuscation works in favor of the highly skilled adversaries
- Low hanging fruits are protected
- Typically 6-7 integer over-under exploits
- Expect to be probe and hacked
- Honeypots in code, extreme logging, offloading
- Take a wholistic approach to security (Don’t focus on one area)
Summary Continued.

- Security through obscurity makes it harder to discover successful attacks
- Monitor high level characteristics
  - Look for outliers in statistical data
- Don’t ignore compiler warnings!
  - They can be annoying but they do help
    - (Usually...)
QUESTIONS?

About tools?/Other common exploits?/Anything?
Ew! Code at 9 AM!?
It Lives!

- It compiles!
- But wait...

It compiles! Let's ship it!
I don’t like warnings...compiler spam.
signed int playerGold = 1;

void bidOnItem(unsigned int playerBid){
    if (playerGold < (signed int)playerBid)
    {
        printf("Failed Bid!");
    }
    else{
        printf("Successful Bid!");
        playerGold -= playerBid;
    }
}
Easy fix!

```c
signed int playerGold = 1;

void bidOnItem(unsigned int playerBid){
    if (playerGold < (signed int)playerBid){
        printf("Failed Bid!");
    } else{
        printf("Successful Bid!");
        playerGold -= playerBid;
    }
}
```
COMPILED/NO WARNINGS/ALL SET/DEPLOY!

Few days/weeks later: There's some weird stuff going on. Is my server haunted?