Securing MMOs

A Security Professional's View From the Inside

Who Is This Guy?

- Security industry professional
  - Years writing subversive software
  - Static analysis tools for C and Java
- Former Senior Software Engineer at Bioware Mythic
- Pwned other games
- Ran Defcon CTF & Quals for 4 years as part of Kenshoto

What This Talk Includes

- Thoughts on what it's like to go from security to gaming
- Stories on how bad it currently is
- Some examples of hacks & tools in the wild
- Some thoughts on how the games industry can get better at security
- Why it won’t get better any time soon

What This Talk Doesn't Include

- 0-day
- Release date for Star Wars: The Old Republic
- Crappy clip-art
- Shout-outs

Making the Jump

- Alternate slide title: How I Learned to Stopped Worrying and Love the Shorts
- Expectations
  - Coming from a world where crashes and vulns mean a big deal
  - Going to a world where crashes are matter-of-course and extended downtime might elicit an apology on a forum
  - From a world of KB to a world of GB
    - No matter how much code you write, your binary will still be smaller than the intro video
    - 30-60 minutes for compilation, 3-5 minutes for linking

Making the Jump

- High Performance
  - 4000 simultaneous clients per "shard"
  - Under 100ms of latency
  - Dozens of commands per user per second
  - 4Hz target server frame speed
- Low Speed
  - Much slower paced
  - Greater tendency for formal education

Challenges of Security in an MMO

- The Rest of the World
  - Most servers have well-defined, community-reviewed specs
  - Many are restricted to trusted users
  - Some are open-source and benefit from peer review

Challenges of Security in an MMO

- Games
  - We define a spec as we go
    - Features are added, cut, change scope
  - We give a connection to anyone that asks
    - Often for free
  - We closely guard our code
  - All of this makes our lives harder

Challenges of Security in an MMO

- More sophisticated games breed more sophisticated hacks
- Client-side security is always a losing battle
  - But you can have fun trying
- It's an arms race

Motivations of Cheats, Crashes & Exploits

- Financial gain
  - RMT
  - In-game currency
- Griefing a captive audience
- Getting an edge in the game
- Extend the lifetime of a game by offering a new type of challenge
  - This applies largely to recreational hackers
  - That's us

Security in the Gaming Industry

- Security is still a new concept to those outside the industry
  - Everyone's heard the term "buffer overflow”
  - Few know how to prevent it in practice

Security in the Gaming Industry

- But we don't write vulnerabilities, we're professionals!
  - Knowledge of vulns isn’t the same as being able to spot them in your own code
- People don't like to hear that they write less secure code than IE
- At least they don't use the word "Cyber" without referring to chat sex

Hack Types and Techniques

- Blind scripting (a.k.a. macro'ing)
  - Easy to detect when things go awry and the bot fails miserably
- Screen scraping & scripting (AutoIt)
  - Harder to detect, but also unreliable
  - Complex screens make scraping difficult
- Memory analysis & modification
  - Sophisticated, but easier to detect

Hack Types and Techniques

- Logic flaws
  - Item duplication
  - Race/state conditions
- Classic exploitation
  - Buffer overflows
  - Numeric overflows

Hack Types and Techniques

- Packet injection / sniffing
  - Useful for spotting events
  - Easily mitigated by introducing encryption on the line
- Account theft
  - Phishing
  - Keyloggers

Bioware's MMO Portfolio

- Ultima Online
  - 12 years old
- Dark Age of Camelot
  - 9 years old
- Warhammer Online
  - 3 years old
- Star Wars: The Old Republic
  - Shipping right after Duke Nukem Forever

How Bad Is It?

- Herald web site hacked
  - Used to host viruses
  - Defense-in-depth saves the day
  - Boxes used to host forums had no access to back network

How Bad Is It?

- Legitimate command from the client
  - Bad parameter validation
  - Array index condition
  - Negative numbers would bring the server down
  - Fortunately, it was a GM-only command

How Bad Is It?

- Remote, pre-auth vulnerabilities
  - `memcpy(dest, message->data, message->len);`
  - `dest` was a fixed size buffer

How Bad Is It?

- Trial accounts
  - The majority of trial accounts belonged to spammers and gold sellers
  - 10% of trial accounts created in a 3-month period were attributed to a single IP
  - Originating from: China
  - These accounts were then used for advertising gold-selling services

How Bad Is It?

- Rash of players' accounts being emptied
  - Accounts had been logged into once, months before they were victims from a Chinese IPs
  - This was most likely an inventory step
  - Assets were later liquidated and then gold transferred 1,000,000 at a time to customers
  - No brute force attempts, so conclusion was keylogging

How Bad Is It?

- EVE Online Senior Producer “Oveur” says:
  - We don’t trust the client
  - Blizzard trusted their client, and look at the mess they’re in
- I guess that’s why I was able to puppet-master their client via Python injection

In the Wild

- In the Wild: “AutoEVE”
- Direct Python injection
  - Uses CCP’s own APIs
  - Has the distinct advantage of allowing application to be minimized
- CCP is hiring security professionals
  - AutoEVE is a point of discussion
  - How to catch it and its ilk

In the Wild

- In the Wild: “UO Made Easy”
- Simple UO scripting tool
  - Used GetProcAddress to mask imports of Read/WriteProcessMemory
  - XOR’d the string name of imports
  - But then stored results in globals, making hooking & observation simple
- Direct manipulation and reading of memory

In the Wild

- In the Wild: "Undetectable”
  - Developer claimed it was impossible for Mythic to detect
  - Actually registered as a debugger
  - Engineers were able to monitor development of the tool in real-time
  - They then proceeded to ban users of the tool, while the developer continued unscathed

Mitigation

- Detection
  - Memory checksums
  - Timing
  - Anti-debugging measures
  - Cheat detection shouldn’t stop the cheat
  - Instead, notify developers
- Agility and rapid response
  - Effective PR management
  - Quick patch turn-around

Mitigation

- Write your own rootkit
  - Warden
  - Highly effective at catching known tools
- Gameplay work-arounds for impossible problems
  - Give the players radar
- Psych warfare
  - Leaving developers of cheats/exploits alone
  - Nail their users instead

Ways to Improve

- Automated analysis
  - PREfast
  - Other power-assist tools
- Basic fuzzing and internal “red-teaming”
- Education & Methods
  - Writing secure code
  - Can I at least get a decent threat model?
- Balancing code quality and release time
  - Realize that large-scale hacks hurt the game
  - Alienate community

Why It Won't Get Better

- In quantifiable dollars, it is cheaper to react to exploits in use
  - Customer Service Reps restoring lost items/gold are cheaper than engineers sifting through code
  - There may not even be anything to find
  - Measuring true cost in reputation and lost players is much harder
- It's good press to ban cheaters
  - If you claim there are no cheaters, even if it's true, no one will believe it