Security Issues and Crime Pertaining to Online Games / Virtual Worlds

HTCIA New England Chapter General Meeting
September 9, 2010

Ming Chow
Tufts University
mchow@cs.tufts.edu
http://www.cs.tufts.edu/~mchow

Introduction

- Online games and virtual worlds have pushed the limits of computing
- The stakes are extraordinarily high for online games and virtual worlds
- Tens of millions of players worldwide; over half-a-million users simultaneously on 6 continents
- Over 11,000,000 players for *World of Warcraft* alone. Do the math: $14 (subscription) * 11M = 154M * 12 (annually) = $1.848B / year. This does not include the client or add-ons!
- *"Many police officials, including seasoned and experienced cybercrime investigators, may not have yet investigated a case involving a virtual world or MMORPG; few investigators want additional work from virtual cases."* [1]
- There have been many of real cases of crime pertaining to virtual worlds and online games

What is an Online Game / Virtual World?

- *"A virtual world is a type of online community that often takes the form of a computer-based simulated environment, through which users can interact with one another and use and create objects, often in 3D virtual environments. In virtual worlds, users often take the form of avatars visible to others as graphical representation of the users."* [1]
- Massively Multiplayer Online Role Playing Game (MMORPG) - allows thousands of players to simultaneously enter a virtual world and interact with one another
- Basic architecture:
  - Create a new character (or avatar)
  - Save that character (server side)
  - Log in with the character
  - Be able to chat with others
  - Be able to navigate around (usually in 3D)
  - Perform actions (e.g., pick up goods, build, chat)

What is an Online Game / Virtual World? (continued)

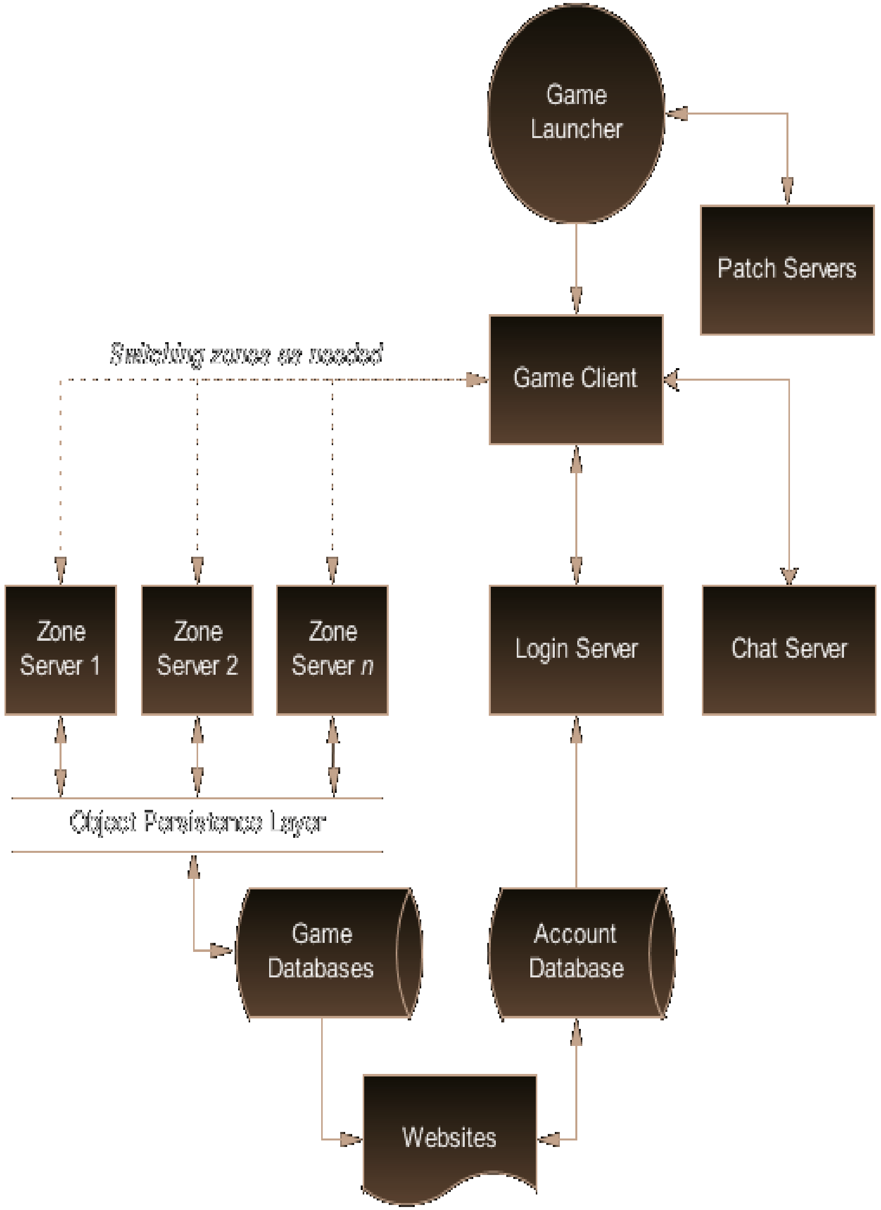
- The goals:
  - Level up your character
  - Grab as much gold / land / money / property that you can
  - Kill everything that moves
  - Build communities
- To achieve the goals:
  - Grind (boring)
  - Share information
  - Cheat
    - Just ask!
    - Download crack or mod
    - Buy the virtual goods with real money
    - Search for game hacks (e.g., in message boards)
    - Search for vulnerabilities in client
    - Bots
    - More later...

Examples of Online Games / Virtual Worlds

- World of Warcraft
- Second Life
- Meez
- Kaneva
- Onverse
- Final Fantasy XI
- Anarchy Online
- Guild Wars
- Star Wars Galaxies
- Pirates of the Carribeans
- EverQuest
- Age of Conan
- Club Penguin
- Mafia Wars / FarmVille / anything by Zynga

Anatomy of an Online Game / Virtual World

- *"An MMORPG is like a large piece of enterprise software: one consists of databases, specialized servers, client software and a huge amount of content."* [3]
- One fantasy world with many fantasy characters
- Deployed on a client-server architecture
- Need to use all computing resources to the fullest
- Computing power (including bandwidth) is *not* unlimited. You *cannot* have a dynamic world.
- Disclosed: over 1900 servers required for *World of Warcraft*



Why Target Online Games / Virtual Worlds?

- Lots of money to be made!
- Lots of kids play online games
- The "trinity of trouble:" connectivity, complexity, and extensibility
    - Networking
    - Game engines (building games on top of other people's work, can you trust other people's work)
    - Scripting engines
    - Dependency on software that are known to have security holes (e.g., Flash, QuickTime)

Why Target Online Games / Virtual Worlds? (continued)

- Legal issues are uncharted territory
- Mass-market appeal
- Homogenization
  - Typically, games are patched, not the game engines!
- One exploit can potentially give bad guy access to your entire PC
  - Personal information
  - Payment information
  - Virtual assets

Attacks and Crime

- In-game exploit via buffer overflow
- Malware
- Phishing
- Drive-by exploit
- Extortion
- Exploit game server vulnerabilities
- Money laundering
- Virtual rape

Real Scenario 1: Getting pwn3d in *Second Life* (thanks Charlie Miller)

- Compromise the host machine (via QuickTime vulnerability) of any player whose avatar approaches an in-game object embedded with malicious multimedia content
- How to do it:
  1. Attacker creates a virtual object (with malicious code) somewhere on his or her property and then associates a URL with the virtual object, indicating that a multimedia file is to be presented when this object is encountered.
  2. When a vulnerable player's avatar encounters this object in the virtual world, the malicious payload (from the multimedia content) is automatically downloaded, processed by the underlying QuickTime library, and the host machine is completely compromised.
- Video: http://www.youtube.com/watch?v=RaCo4USXd5Y

Real Scenario 2: Malware

- Example 1: Win32/Taterf
  - http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32/Taterf
- Example 2: Trojan-PSW.Win32.OnLineGames.a
  - http://www.f-secure.com/v-descs/trojan-psw_w32_onlinegames.shtml
- Example 3: Nude patch
  - Custom content
  - New character with script code. WTF?
  - The script is executed with game permissions, i.e., as administrator or root
  - What the script does: use your wildest imagination because the administrator can do anything to the system!
- Any unofficial patch or tool (e.g., no-CD cracks, trainers) can be suspect

Real Scenario 3: Phishing

- Becoming too common: stealing usernames and passwords for hard-earned virtual goods
- Players are hungry for bonuses, help, gold, points, etc.
- How to do it:
  1. Steal a player's username and password by luring player into a rigged website where he/she enters own game username and password, or install Trojan Horse via security hole in browser (e.g., Adobe Flash compromise)
  2. Use the stolen account in the game
  3. Transfer out virtual good (e.g., virtual sword)
  4. Profit! (yes, sell the virtual sword for good money, real money)

Real Scenario 4: Extortion

- **"China Sentences Virtual Currency Extorter to Prison"** (2009)
  - A man with three friends *"beat up the victim and forced him to turn over virtual currency worth 100,000 yuan (US$14,700), China's official Xinhua news agency reported late Sunday."* [6]
  - *"The attackers also extorted virtual equipment for online games from the victim"* [6]
  - *"Selling in-game weapons, armor and other items to players for real-world cash is a common way for China's online gaming companies to a turn a profit. Internet cafes in China are often packed with chain-smoking teenagers who play World of Warcraft or similar Chinese games for long hours."* [6]
  - The men were fined and were sentenced to three (3) years in prison.

Real Scenario 5: Child Pornography

- "Child predators who are apparently offering "game points" in exchange for nude images through Internet-connected video games have prompted a warning for parents from a cybercrime detective." [9]
- Case 1: **Man Held in Child Porn Case, Used Xbox to Make Contact (8/27/2010)**: *"A 22-year-old man is accused of paying a California boy points redeemable for online video game purchases in exchange for nude pictures of the child."* [10]
- Case 2: **Second Life Child Pornography Investigation (5/10/2007)**, *"The BBC reports that Second Life is being investigated by German police following allegations that some users are trading child pornography in the online world, as well as practicing 'virtual' child abuse..."* [11]

Looking Ahead

- *"Seven percent of global users accessing Facebook spend an average of 68 minutes per day playing the popular interactive game "FarmVille," according to the Cisco report. "Mafia Wars" is the second most popular game, with 5 percent of users each racking up 52 minutes of play daily."* [5]
- "No law in China currently grants protection to virtual property" [6]. Ditto in the US and in Europe.
- Criminals will always exploit new technologies
- If there is money to be made, you know criminals will be lurking
- Legal issues still largely uncharted
- "*While most computer users have been taught basic computer security skills, such as not opening attachments from untrusted sources and not following links in emails, these lessons become worthless when they immerse themselves in a virtual world."* [4]
- The problems are very real, but few people (still) take games seriously

References

1. http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=316:crime-and-policing-in-virtual-worlds&catid=50:issue-7&Itemid=161&goback=.gde_48392_member_26109577
2. http://radoff.com/blog/2008/08/22/anatomy-of-an-mmorpg/
3. http://ieeexplore.ieee.org/xpl/tocresult.jsp?reload=true&isnumber=5054895
4. http://threatpost.com/en_us/blogs/owning-online-games-fun-and-fake-profit-081810
5. http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=226200089
6. http://www.pcworld.com/article/165447/china_sentences_virtual_currency_extorter_to_prison.html
7. http://www.freehacking.net/2010/03/new-hacking-trend-cybercrime-goes.html
8. http://www.kaspersky.com/au/reading_room?chapter=207716493
9. http://www.clickorlando.com/family/16995600/detail.html
10. http://www.theledger.com/article/20100827/news/8275053
11. http://www.zdnet.com/blog/social/second-life-child-pornography-investigation/159