CS 592: Security Practicum

Lecture 2

On-line PC games and their cheats

Popular on-line PC games

- FPS (First-person shooters)
  - You control a gun/crosshair
  - You shoot and kill other players doing the same
- MMORPG (Massively multi-player on-line role-playing games)
  - You control an avatar
  - You kill other avatars to gain loot and power
- RTS (Real-time strategy)
  - You control an army
  - You go head-to-head against another player’s army

Popular FPS games

- Half-Life/Counter-Strike (1/2), Battlefield (2 & 2142)
- Wolfenstein: Enemy Territory, Call of Duty (1/2)

Popular MMORPG games

- World of Warcraft, Lineage (1 & 2)
- Runescape, Final Fantasy XI, EverQuest (1 & 2)

You dance with Keeg Gilin.
You dance with Keeg Gilin.
You dance with Keeg Gilin.
[1. General] Seryl: get down tonight?
Dunmore says: join in folks
[1. General] FourInchTool: Considering we're dwarves, little is right.
Damador bursts into dance.
Dunmore bursts into dance.

Popular RTS games

- Warcraft 3/Starcraft, Age of Empires
- Warhammer 40000, Command & Conquer 3

Cheats

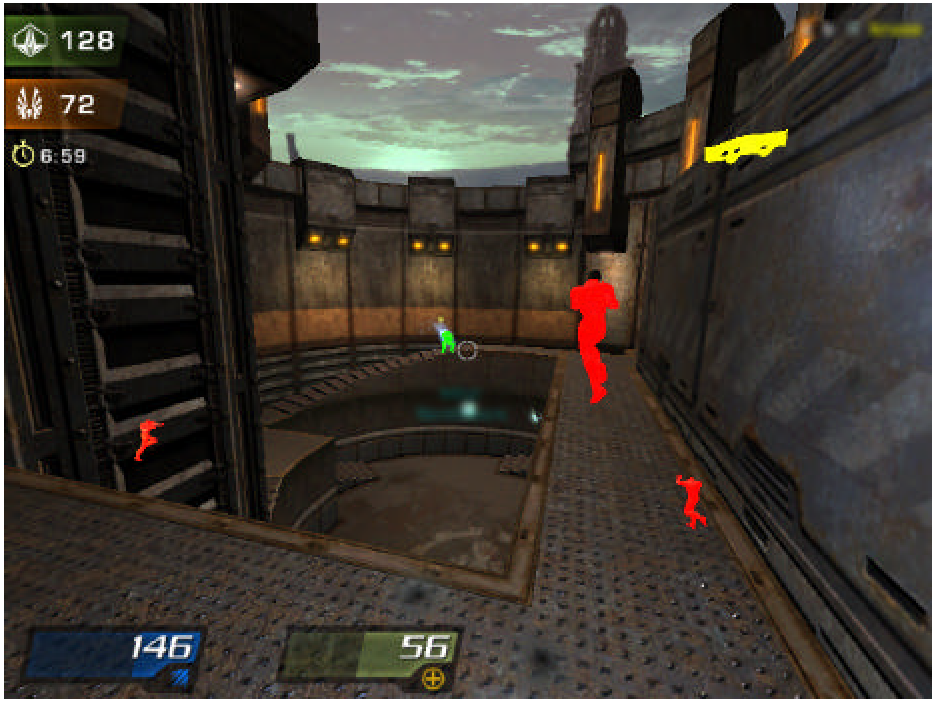
- Achilles heel of the PC gaming platform (besides crappy integrated graphics cards)
  - Must be fixed to compete with consoles
  - Causes legitimate, paying players to quit
  - Creates bad word-of-mouth to discourage new players
  - Wrecks virtual economies in MMORPGs

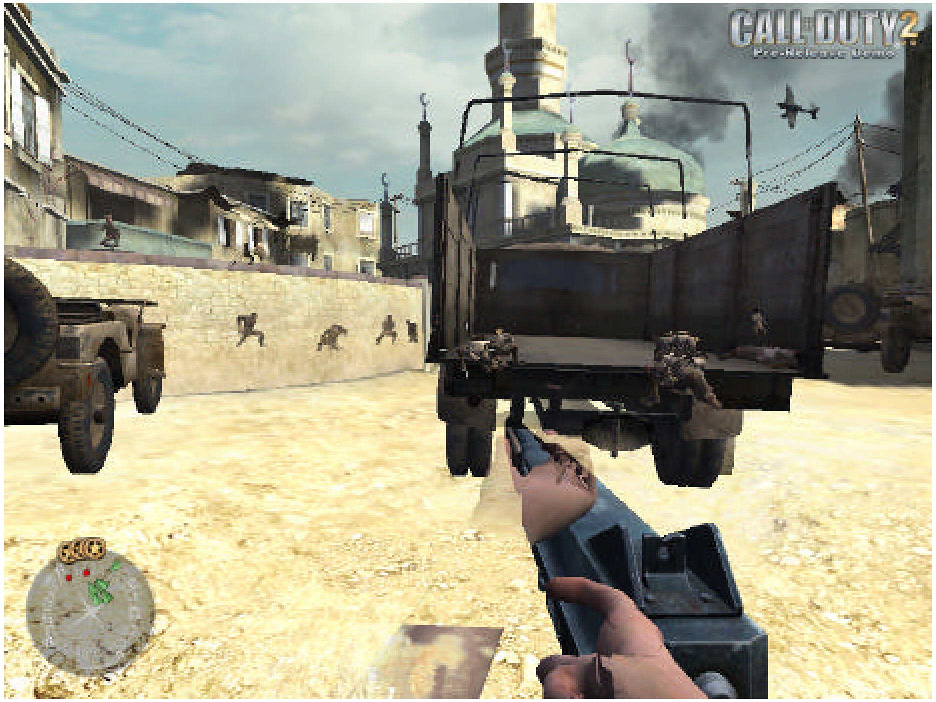
Types of cheats

- Information exposure
  - Wallhacks (OGC), Maphacks (Warcraft 3), Chest hacks (showEQ)
- Automation
  - Aimbot (OGC), Troop command macros (Warcraft 3), Auto-looting (WoW QuickLoot), AFK bots
- Protocol
  - Reset cheat (Half-Life), Unit fabrication (Warcraft 3), Item duping (MMO), Speed hack (Half-Life), Hit point hack (Diablo), Disconnect cheat
- Game bugs
  - Game-specific coding errors that lead to unintended behavior

Information exposure cheats

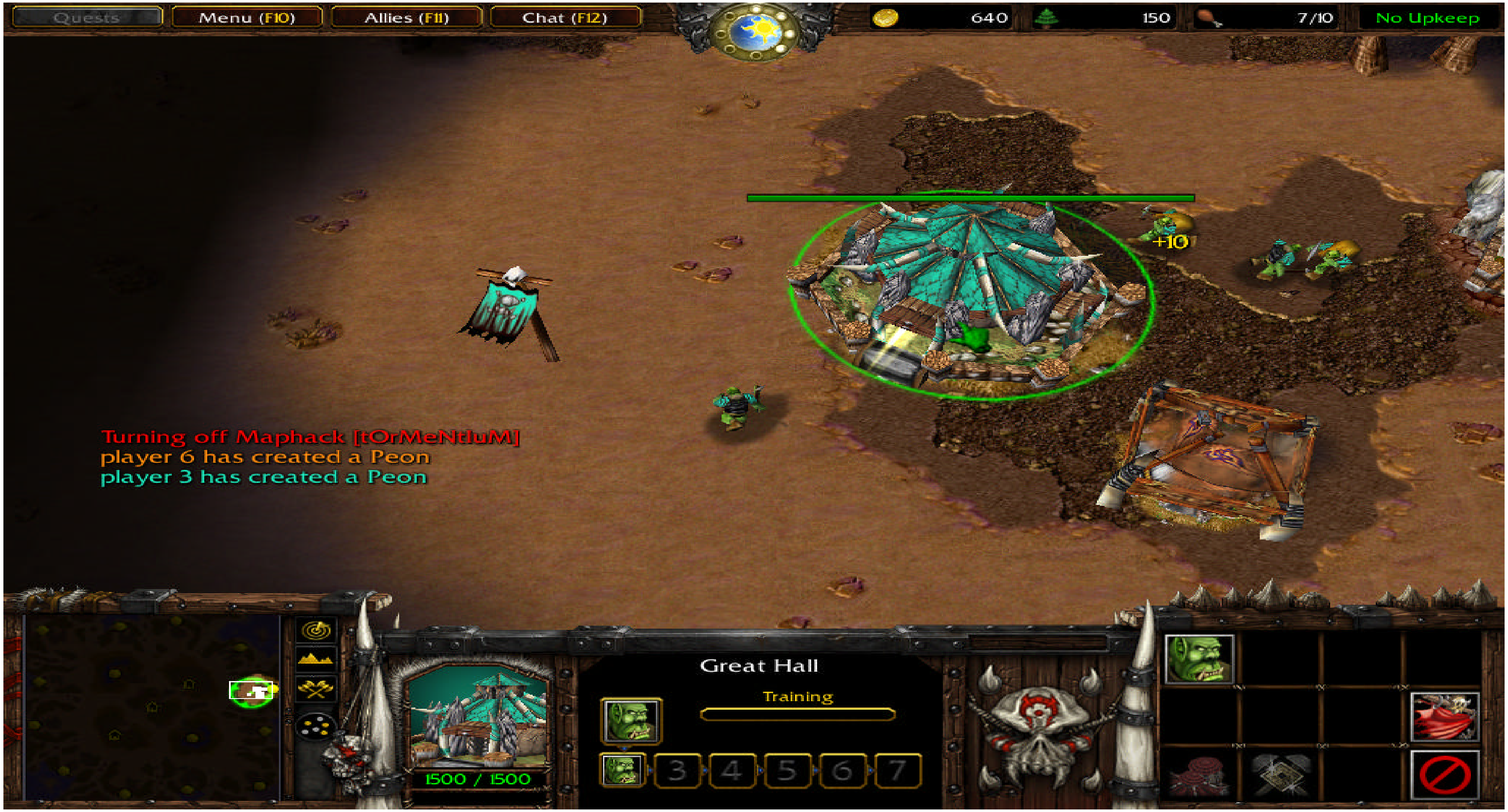
- Server or peer sends complete information to other client
  - Cheat reveals information that should be hidden
- Wallhack
  - Quake 4 – released 10/18/2005
  - Call of Duty 2 – released 10/25/2005 (Server boycott due to cheats)





Information exposure cheats

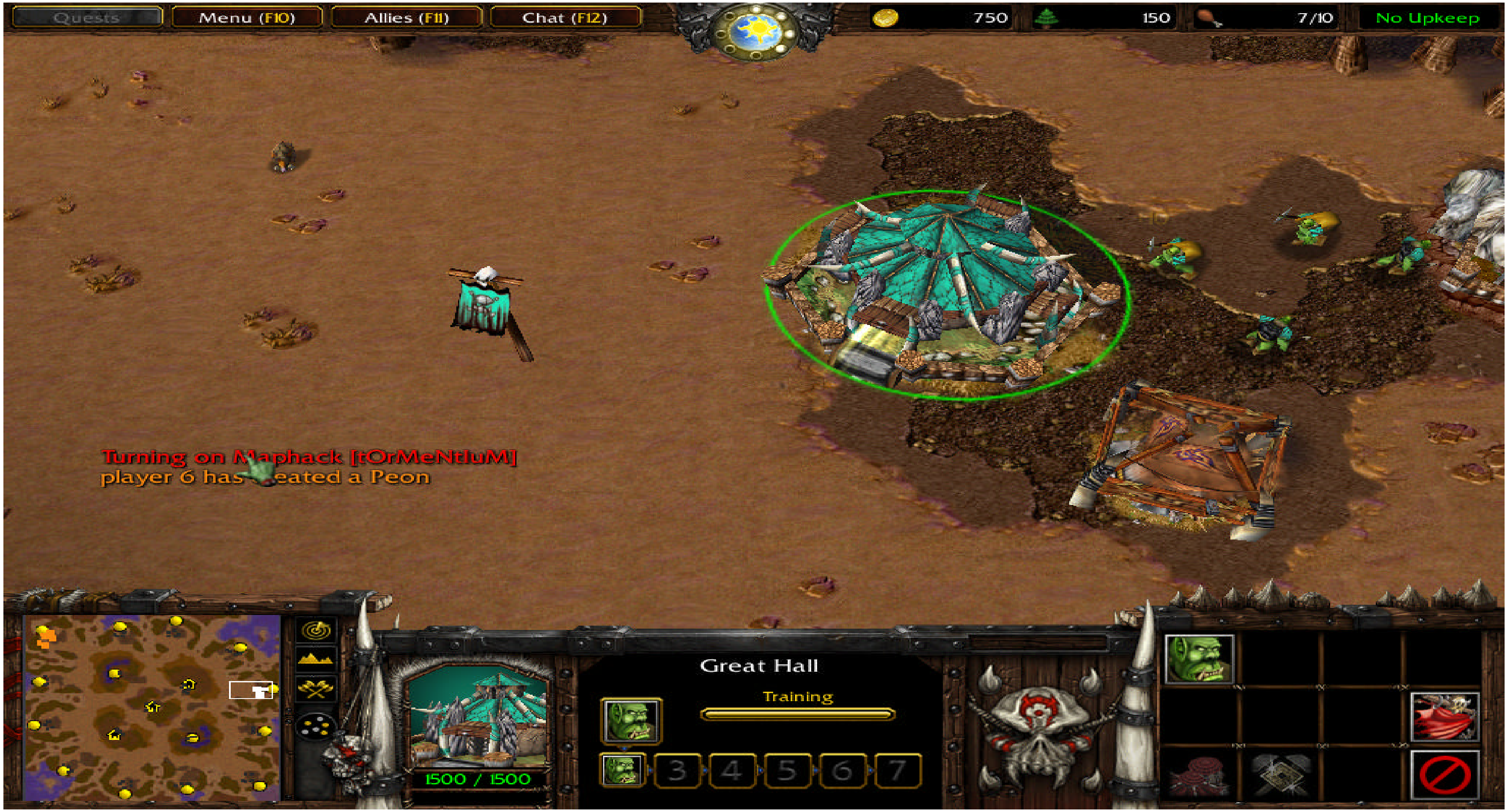
- Maphack (reveal map and enemy units)
  - Warcraft3 without Maphack



Turning off Maphack [tOrMeNtluM]
player 6 has created a Peon
player 3 has created a Peon

Information exposure cheats

- Maphack (reveal map and enemy units)
  - Warcraft3 with Maphack



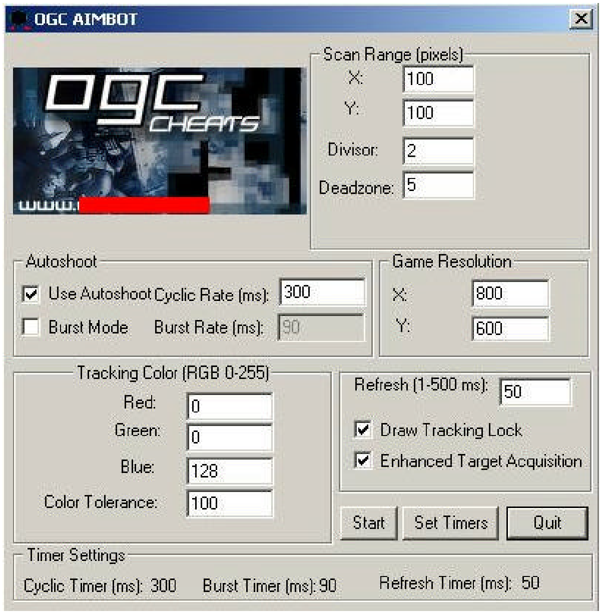
Turning on Maphack [tOrMeNtIuM]
player 6 has created a Peon

Information exposure cheats

- Chest hacks
  - Information about what loot is available in map exposed
  - Player goes straight to the locations with the best loot

Automation cheats

- Automate game activities via Bots
- Aimbots
  - OGC
  - Automate aiming in FPS
- Macros and game bot farming
  - MacroQuest for EQ2
  - Automate wealth acquisition via programs



OGC AIMBOT

Scan Range (pixels)
X: 100
Y: 100
Divisor: 2
Deadzone: 5

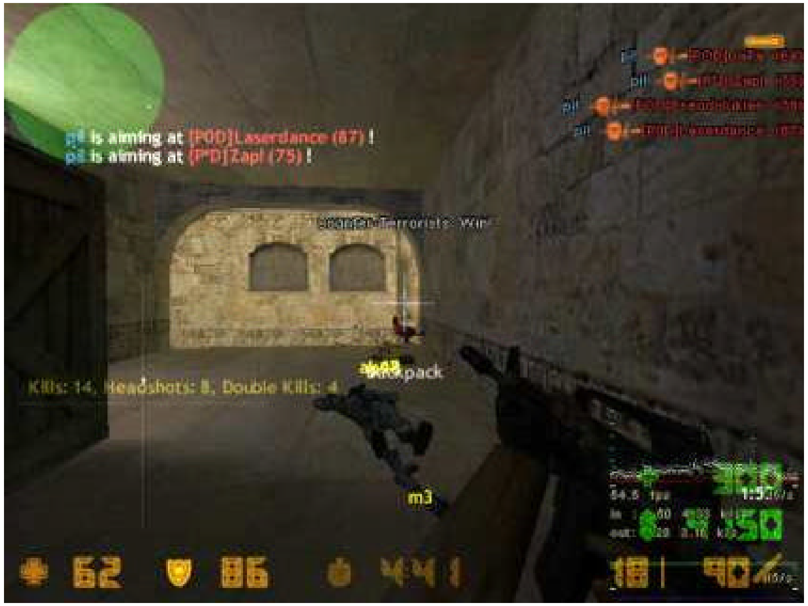
Autoshoot
☑ Use Autoshoot Cyclic Rate (ms): 300
□ Burst Mode Burst Rate (ms): 90

Game Resolution
X: 800
Y: 600

Tracking Color (RGB 0-255)
Red: 0
Green: 0
Blue: 128
Color Tolerance: 100

Refresh (1-500 ms): 50
☑ Draw Tracking Lock
☑ Enhanced Target Acquisition

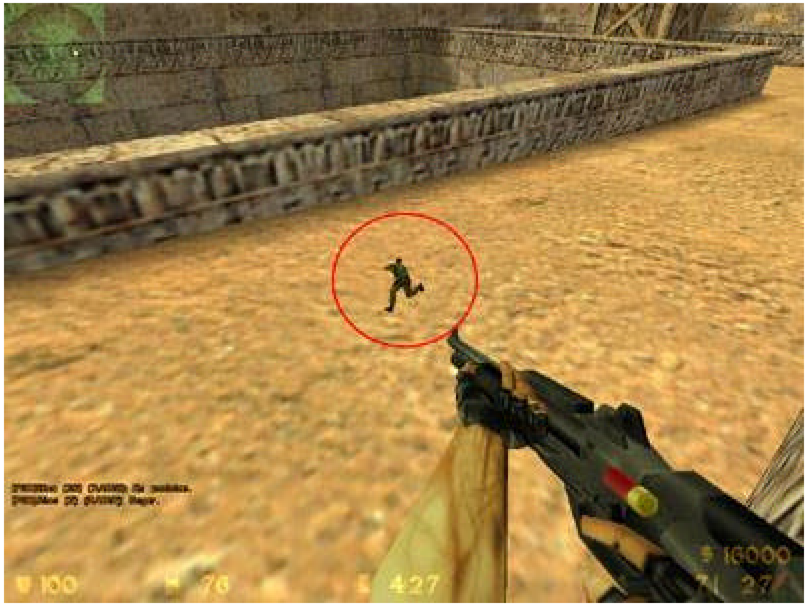
Timer Settings
Cyclic Timer (ms): 300 Burst Timer (ms): 90 Refresh Timer (ms): 50



pil is aiming at [POD]Laserdance (87) !
pil is aiming at [P*D]Zapl (75) !

Counter-Terrorists Win

Kills: 14, Headshots: 8, Double Kills: 4



Protocol cheats

- Hit point cheating
  - Diablo protocol messages indicating damage done to enemy
  - Inject messages with inflated damage to instantly kill opponent
- Item duping
  - Disconnect while dropping item
  - Ambiguity in whether event happened globally
- Speed hack
  - Inject movement messages to make your character move or fire “faster” than normal

Game cheats

- Exploit inconsistencies and errors in game code
  - Magic “pizza” machine in The Sims On-line
  - Vending machine and pawn shop hack in Lucasfilm’s Habitat
  - Skin cheats in Counter-Strike
  - Not highly relevant to this course

Software methodology of cheats

- What they do
  - Read memory to expose information
  - Modify display path to add visual aids
  - Inject protocol messages
  - Modify game textures and models on disk or in memory
  - Programmatically play game on behalf of player

Software methodology of cheats

- How they do it
  - Proxy
    - Use separate machine to modify network packets (aimproxies)
  - Program external to game
    - Separate process running at higher privilege level
    - In-kernel modules
    - Graphics/IO drivers (see-through drivers)
    - Additional layer between game and Windows/DirectX
  - Library that hijacks game calls
    - Runs in address space of game

Software methodology of cheats

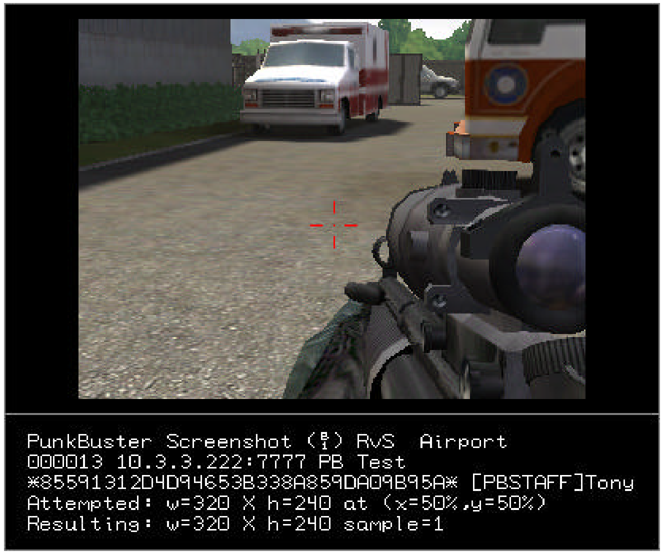
- How they hide from anti-cheats
  - Ability to disassemble signatures being checked
    - Polymorphism to thwart file and memory signatures
  - Run in privileged mode or in-kernel to prevent anti-cheat from accessing it
  - Automatic disable when anti-cheat code is about to run
  - Automatic disable when new anti-cheat distributed
  - More sophisticated mechanisms described in next lecture

Anti-cheats

- HLGuard (United admins)
- Cheating Death (United admins)
- PunkBuster
- Warden
- Our approach: Intel AMT

Anti-cheats

- Scanners
  - Continuously scan memory and filesystem for foreign libraries and cheats
    - Randomize to keep cheats honest, delay ban to confuse
    - Steam and VAC, PunkBuster
    - Heuristics not perfect: Steam and modified OpenGL drivers
- Remote screenshot
  - Provide a facility for dumping a player’s screen remotely
    - PunkBuster



```
PunkBuster Screenshot (Bi) RvS  Airport
000013 10.3.3.222:7777 PB Test
*85591312D4D94653B338A859DA09B95A* [PBSTAFF]Tony
Attempted: w=320 X h=240 at (x=50%,y=50%)
Resulting: w=320 X h=240 sample=1
```

Anti-cheats

- Authentic peripherals
  - Trusted keyboard/mouse clicks
    - Hardware signing its movement and clicks
  - Trusted network output
    - Cryptographic timestamping/ordering
    - Prevent look-ahead cheats
- Continuous player performance monitoring
  - HLGuard
    - Machine learning of reasonable human reaction time
    - Ban those who react too fast
    - Prone to false positives
      - Cal-I (Cyberathlete league) players

Cheating links

- General
  - http://rpgexploits.com
  - http://msxsecurity.com
  - http://zerogamers.com
- WoW
  - WoW Glider
    - http://wowglider.com
  - WoW radar, WoW Sharp, ByteBot, GALB
  - WardenNet, ISXWarden (anti-anti-cheats)
    - http://ismods.com/warden
    - http://edgeofnowhere.cc/viewtopic.php?t=311208
    - http://www.rootkit.com/newsread.php?newsid==360
  - ISXWoW
    - http://ismods.com/downloads.php

Cheating links

- Half-Life
  - OGC
    - http://mpcdownloads.com
    - http://www.mpcforum.com/showthread.php?t=31409
- EverQuest 2
  - MacroQuest
    - http://sourceforge.net/projects/macroquest

Anti-cheat links

- WoW Warden
  - http://www.ismods.com/warden
- PunkBuster
  - http://punkbuster.com
- Valve Anti-Cheat (VAC)
  - http://server.counter-strike.net/server.php?cmd=VAC
- HLGuard, Cheating-Death
  - http://unitedadmins.com
- Intel’s AMT
  - http://www.intel.com/go/iamt/