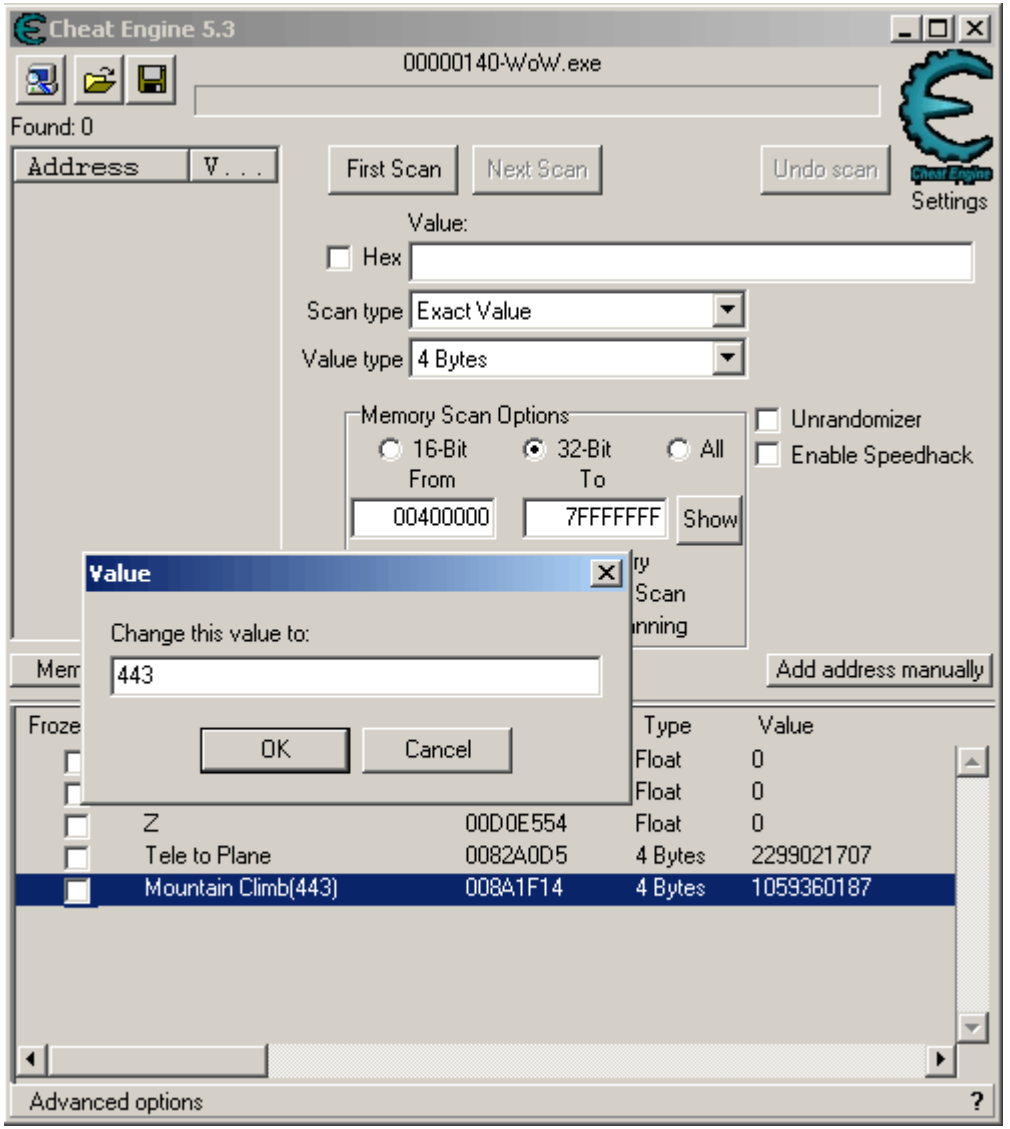
World of Warcraft cheats

Presented by
Alex Ten and Dan Lake
for CS592 Computer
Security Practicum

Cheat Engine

- An open-source program maintained by a single person. http://cheatengine.org
- Allows to do VM editing, DLL injections and API hooking.
- Can act like a root kit by hiding itself (both user and kernel mods are available).
- Written in Delphi (Object Oriented Pascal), 20Mb of data/machine code and 2Mb source code.

Cheat Engine



Cheat Engine

- Wall climbing hack
  - Mechanics: replacing certain values of certain virtual memory addresses. For WoW it's VM address 008A1F14, and its value should be changed to 443.
  - Benefits: a hacker can climb any walls and therefore access certain locations much faster than normal players.

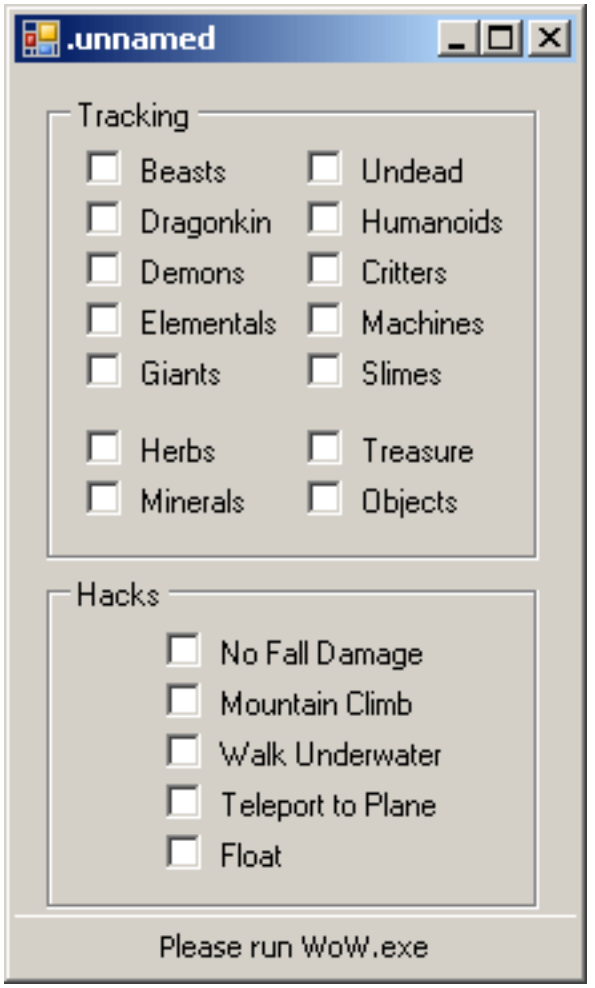
Cheat Engine

- Teleporting
  - Mechanics: works almost the same as wall climbing, just slightly more complicated in the sense of calculating player's current position.
  - Benefits: a hacker can teleport around.

Cheat Engine

- Speed hack
  - Mechanics: "The speed hack works by controlling the time in the game by pausing the clock, and then continuing the clock after a few milliseconds with a specific amount of time."
  - Benefits: a hacker can move faster than normal players.

Extracting hidden information from the game client



Kick-Ass Map

- Written by Michael Donnelly (aka Mercury, WoW Glider's author as well).
- Allows to see all game objects on the much wider area that it was intended by the game devs.
- Can be used across the network (to hide from Warden).
- No longer maintained, source code is now the subject of sale.

Kick-Ass Map


Young Wolf
Cow
L1
Deer
L5
Young Wolf
L1
Young Wolf
L1
Young Wolf
L1
Rabbit
L1
Young Wolf
L1

Kick-Ass Map


Young Wolf
Cow
L1
L5
Deer
L5
Kira Songshine
Young Wolf
L5
Young Wolf
L1
L5
L1
Mangy Wolf
Forest Spider
L6
Young Wolf
L1
Rabbit
L1
Young Wolf
Young Wolf
L1

Simple bots: FishBuddy

- A fishing robot
  - Mechanics: making 'screenshots' of the game and looking for a specified color, once it found and then changed, bot attempts to get the fish.
  - Benefits: a hacker can seat back and let the bot do all the work.

Simple bots: FishBuddy

Simple bots

- Anti-afk bots: moves your character slightly once in a while. Almost legal, but rarely used.
- Auto-BG accepting bots: accepts invitations to the battle grounds while player is AFK. Somehow useful.

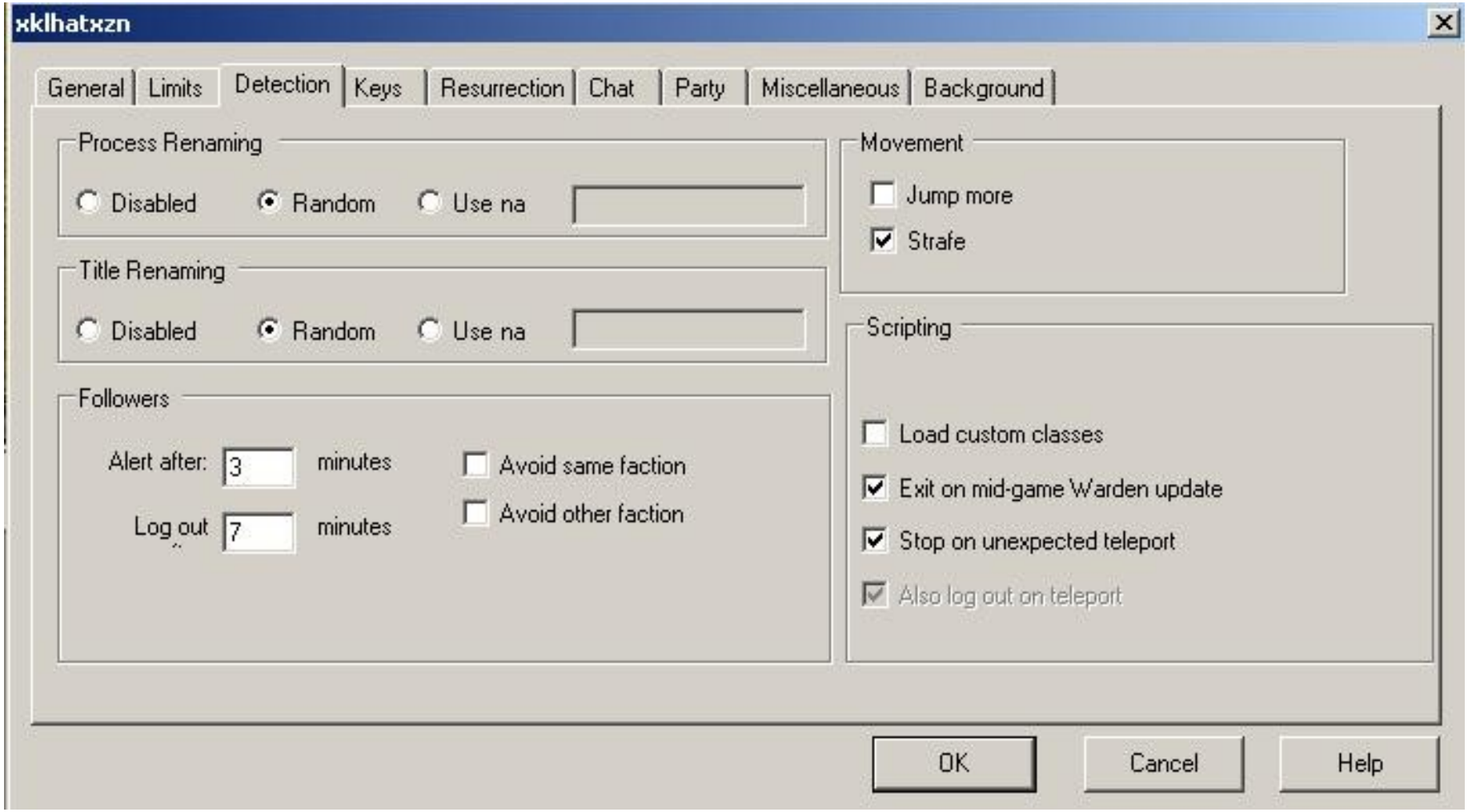
WoW Glider/MMO Glider

"Glider is a tool that plays your World of Warcraft character for you, the way you want it. It grinds, it loots, it skins, it heals, it even farms soul shards... **without you**."

Glider and Launchpad are written entirely in C#, with the Microsoft .NET Framework 2.0. Glider's helper driver is written in regular C and i386 assembly.

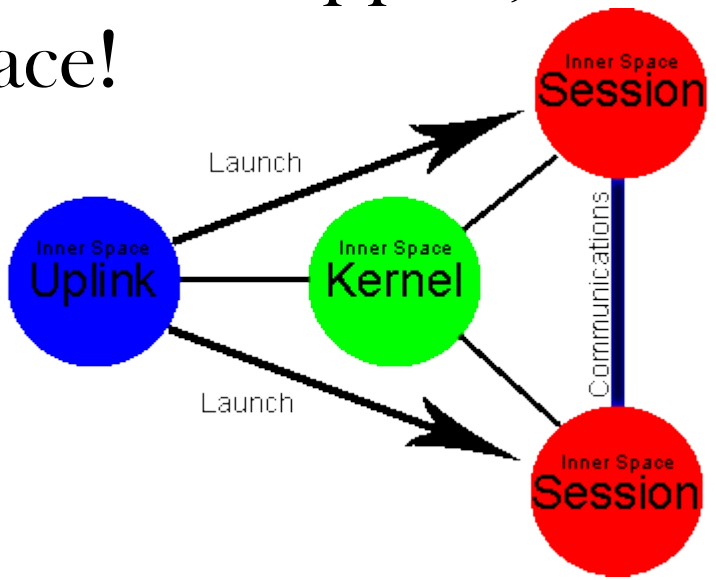
Uses "shadow driver" rootkit to hide from Warden

WoW Glider/MMO Glider



Innerspace & ISX

Inner Space is a layer between Windows and games. Within this layer, programs written for Inner Space can safely perform nearly any task inside the game ... Inner Space provides systems for automation (scripting), input emulation, customizable user interfaces, bindable input (hotkeys), dual monitor support, and that's just scratching the surface!



Innerspace Extensions

ISXDK (Innerspace eXtension Development Kit)

Extensions published for:

- EverQuest
- World of Warcraft
- Star Wars: Knights of the Old Republic
- Sims 2
- Others....

http://www.lavishsoft.com/innerspace/
http://www.isxwow.net
http://www.ismods.com

Innerspace Extensions (WoW)

TrackMaster - Kick-Ass Map implemented in ISX

ISXWoW – WoW-specific framework for IS. Plug-ins include AFKAlarm, Autofish, RunningMan, WoWBot, and others

ISXWarden - ISXWarden modifies Warden so that programs under its protection (Inner Space, loaded IS extensions, etc) are simply invisible to Warden.

WardenNet - WardenNet tracks signatures of Warden so that it can be determined how many are in circulation, and when signatures move into or out of circulation.