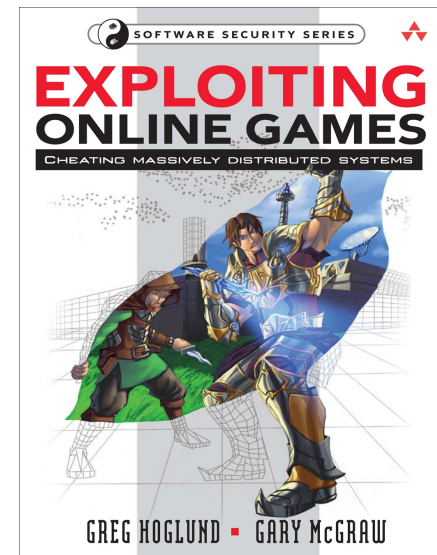




cigital

Exploiting Online Games: Cheating massively distributed systems

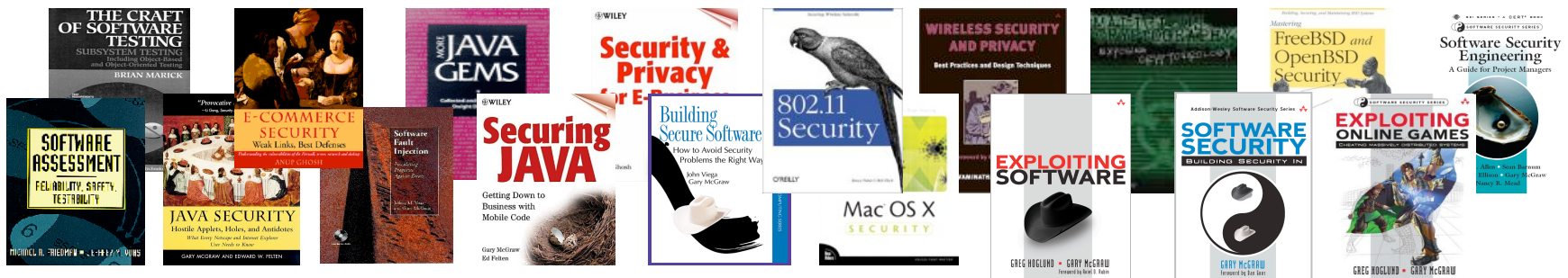
Gary McGraw, Ph.D.
CTO, Cigital
<http://www.cigital.com>





Cigital

- Founded in 1992 to provide software security and software quality professional services
- Recognized experts in software security and software quality
 - Widely published in books, white papers, and articles
 - Industry thought leaders



Disclaimer

- In our research for this book and this presentation we have broken no laws.
- We expect our readers likewise not to break the law using the techniques we describe.



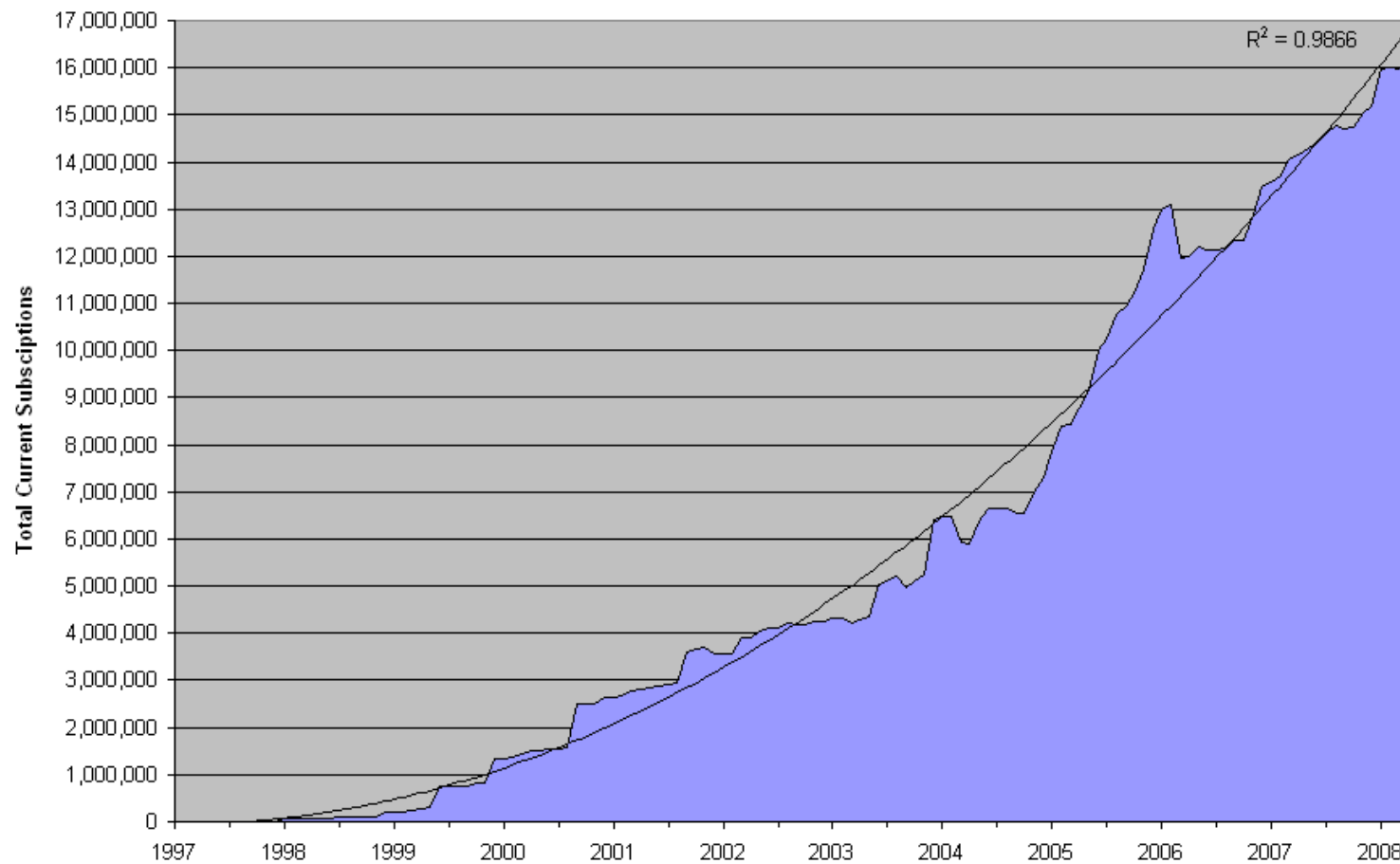
Why online games?



Online games are a bellwether

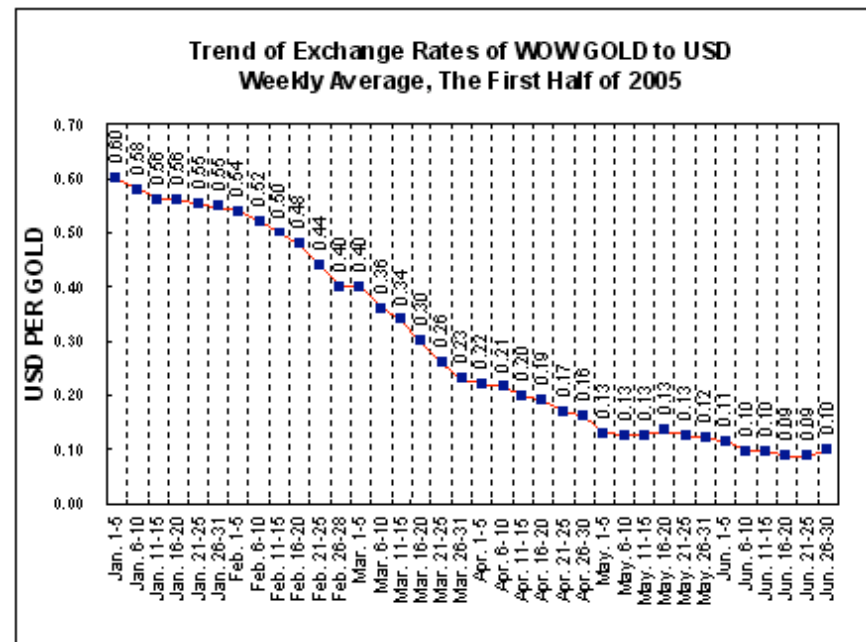
- Online games (like World of Warcraft) have up to 900,000 simultaneous users on six continents
 - 10,000,000 people subscribe to WoW
 - 16,000,000+ play MMORPGs
 - Clients and servers are massively distributed
 - Time and state errors are rampant
- MMORPGs push the limits of software technology
- Modern distributed systems in other domains are evolving toward similar models
 - SOA, Web 2.0
- Time and state errors are the XSS of tomorrow

Total MMOG Active Subscriptions

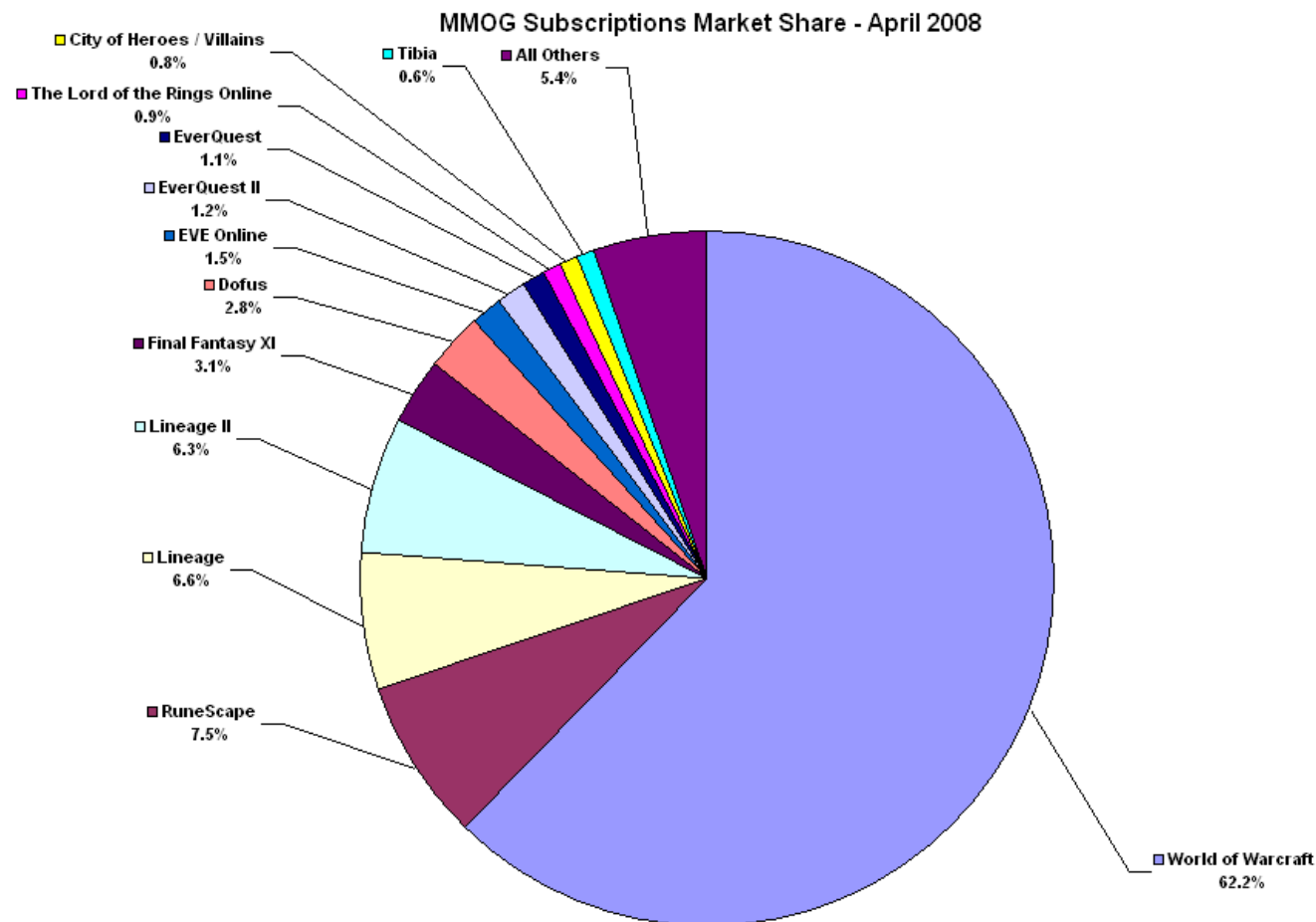


Online games are big business

- One game (WoW) has over 10,000,000 subscribers
- $\$14 * 10M = 140M * 12 = \$1.68B$ (not to mention buying the client)
- A healthy middle market exists for pretend stuff
- Cheating pays off



Why pick on World of Warcraft?



Isn't this exploit discussion bad?

1995

- Dan Farmer fired from Silicon Graphics for releasing SATAN with Wietse Venema
- FUD: possible attack tool!

2009

- Any system administrator not using a port scanner to check security posture runs the risk of being fired

Fall 2004

- John Aycock at University of Calgary publicly criticized for malware course
- FUD: possible bad guy factory

Should we talk about attacking systems?



The good news and the bad news

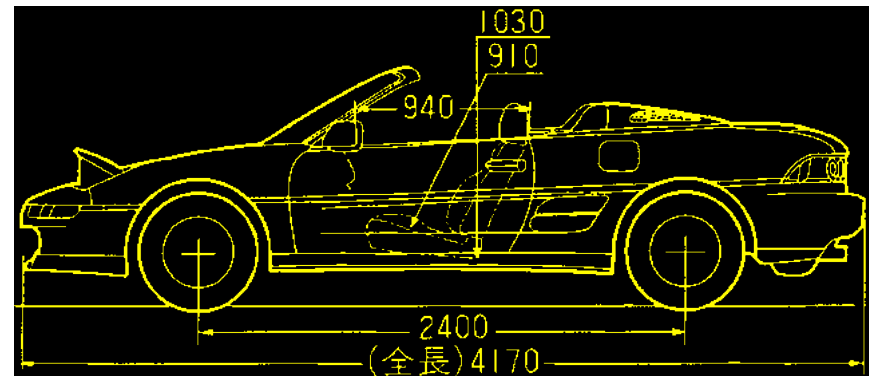
Good news

- The world loves to talk about how stuff breaks
- This kind of work sparks lots of interest in computer security



Bad news

- The world would rather not focus on how to build stuff that does not break
- It's harder to build good stuff than to break junky stuff



Lawyers, guns, and money



Lawyers

- Game law is set up to counter piracy (not cheating)
 - “Cracking” a game costs game companies big money
 - Security mechanisms protect against cracking
 - Online components answered this problem wholly
- The DMCA is now being used to counter cheating as well
- End User License Agreements (EULAs) and Terms of Use (TOU) lay out license obligations
 - WoW Glider case
 - Ginko Financial disappears
- Click to agree



Egregious EULAs

- Sony's EULA allows installation of a rootkit on your machine
- Blizzard's EULA allows monitoring
 - The Warden
 - The Governor
 - Spyware or security mechanism?
- Gator's EULA disallows removal of the software
- Microsoft's Frontpage disallows negative comments about Microsoft
- EULAs for viruses allow (legal) propagation!
- Apple's EULA never dies





cigital

“Guns”





Money

- Exchange rates exist between in-game currency and real money
 - Per capita GDP in some MMO worlds is greater than the per capita GDP of some real countries
 - Economists study game economies
- Microsoft reports that the market in 2005 was over \$6B
- DFC says the market will double to \$12B by 2010
- Secondary markets are also thriving
 - In 10/2005 a player paid \$100,000 for virtual stuff (an Asteroid Space Resort in Project Entropia)
 - IGE has over 420 employees and project a \$7B market by 2009
 - Connections to thottbot (for better sweat shop work)
 - Chinese sweat shops make economic sense
 - Second Life is set up as a market in virtual stuff (and players own their creations)

“It’s easier than making shoes!”

- In China, over a half-million people “farm” MMO games
 - Some sleep on cots near the computers and work in shifts
- People choose this job. It can be better than working on your dad’s state-owned farm
- Almost anyone can get this job, even “unskilled” labor



<http://youtube.com/watch?v=ho5Yxe6UVv4>

Bugs, bots, and kung fu



Two kinds of cheating

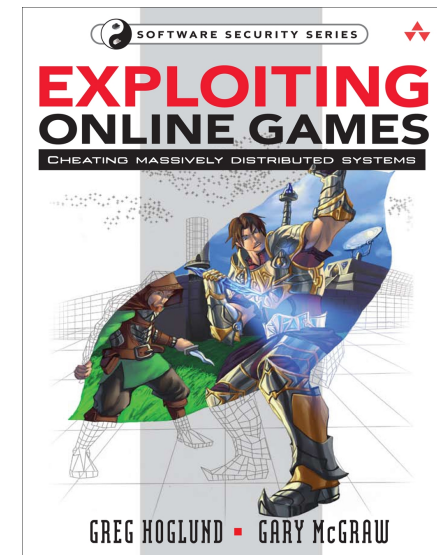
- “Exploits” - actual game bugs, which are exploited to
 - Teleport
 - Duplicate items or gold
 - See stuff you’re not supposed to see
- Bots
 - Both AFK and non-AFK
 - Only performing legal inputs, but in an automated fashion

Botting

- Botting happens because
 - “Grinding” is really boring
 - Players are “farming”
 - Running the game to farm a resource, possibly running multiple accounts at once
- Farming bots are common
- Aimbots are a different story
 - FPS hacks
- PvP combat bots help too
 - For use in RPG combat

How botting happens

- MACRO's & Scripts (most common)
- Memory read & write
- DLL Injection
- Debugging



MACROs

- Inject keystrokes and mouse movement
- Sample pixels and read memory locations
 - Take over the GUI
 - Must dedicate the computer to this
 - Error prone
 - Screen and controls must be preconfigured exactly as required
- ACTool, AutoHotKey, Autolt3.0, LTool-0.3, xautomation
- Example: WoW_Agro Macro (in chapter 2)

 **Xanier**
7

Northshire Valley



There is nothing to attack.

[Xanier] whispers: im curently in atack mode
To [Xanier]: im curently in atack mode
[Xanier] whispers: lazydraw
To [Xanier]: lazydraw
[Xanier] whispers: im atempting to start atack mode
To [Xanier]: im atempting to start atack mode
[Xanier] whispers: lazydraw
To [Xanier]: lazydraw



1 2 3



Process manipulation

- Read & Write memory data
 - Coordinates
 - Speed
 - Direction
- Use with a MACRO
 - Read data directly (instead of sampling pixels)
- Build fresh spoils
 - Map hacks
 - Teleporting
 - Speed hacks

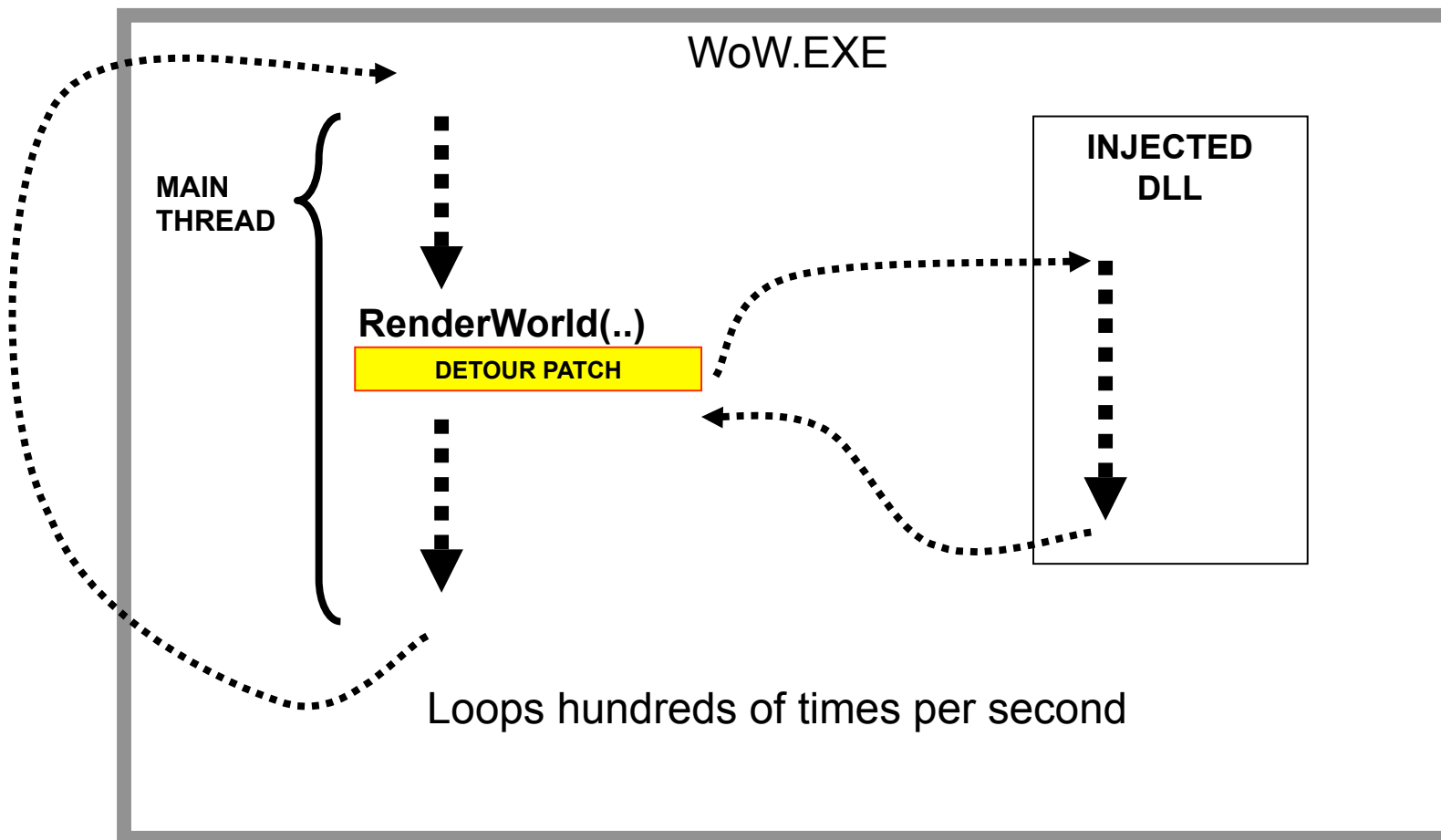


Thread hijacking

- Hijack main system thread
 - Eliminates thread safety issues
- Call internal functions within game client directly
 - Minimize the game program
 - Runs itself
 - Doesn't have errors in sampling
- Eliminates need for MACRO altogether

Thread hijacking

- Used in a few WoW botting programs



Techniques for cheating

- Over the game (control the GUI)
 - keystrokes
 - mouse dropping
 - pixel sampling
- In the game (manipulating objects)
 - memory manipulation
 - finding objects (automatically)
- Under the game
 - 3D teleporting
 - DLL injection
 - be the graphics card
- Outside the game
 - sniffing
 - crypto cracking
 - kernel fu

Total conversion and mod'ing

- Replace graphics with new graphics
- Replace client logic



Advanced game hacking fu

- See *Hacking World of Warcraft: An exercise in advanced rootkit development*
 - Greg Hoglund's presentation from Black Hat 2006
 - <http://www.rootkit.com/vault/hoglund/GregSlidesWoWHack.rar>



State of the art

- Combine injected payload with cloaking and thread hijacking to FORCE in-game events
 - Spell casting
 - Movement
 - Chat
 - Acquire and clear targets
 - Loot inventory





MAIN
THREAD

RenderWorld(..)

HARDWARE BP

super

uncloak

branch

CastSpellByID(..)

ScriptExecute(..)

ClearTarget(..)

MAIN
THREAD

RenderWorld(..)

restore

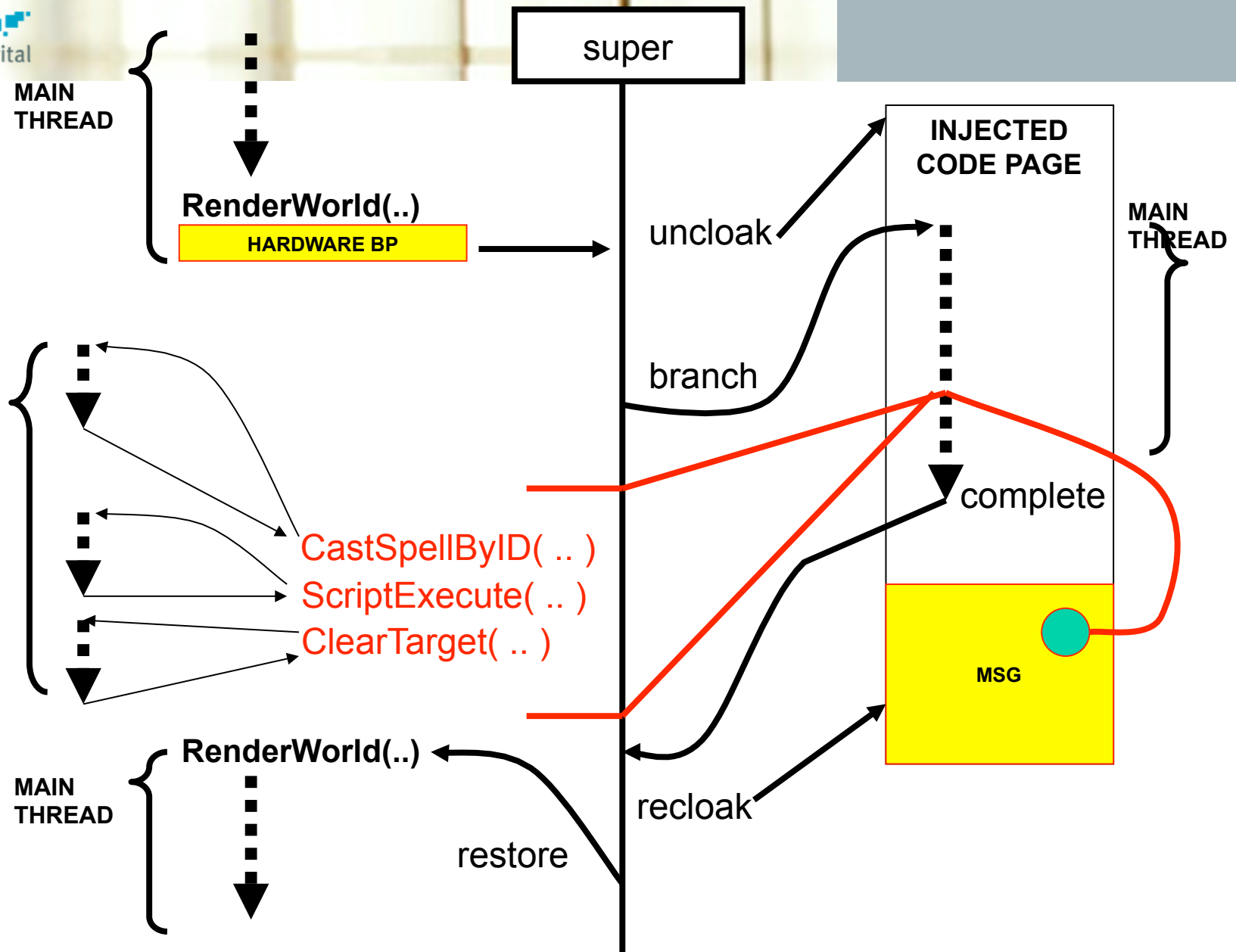
recloak

INJECTED
CODE PAGE

MAIN
THREAD

complete

MSG





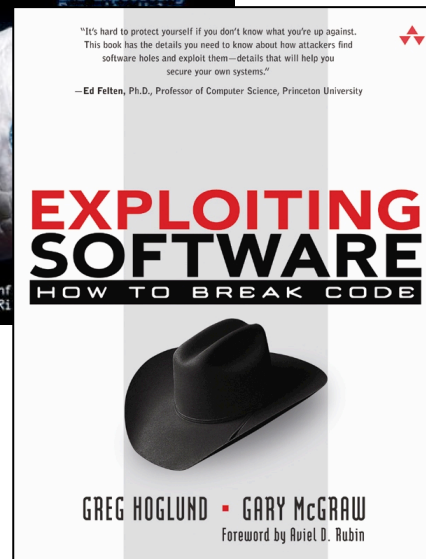
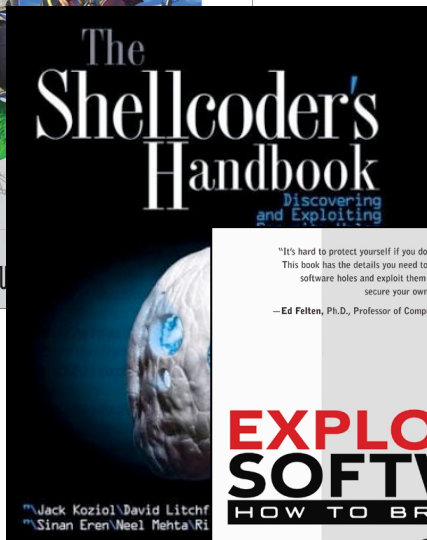
cigital

Classic arms race



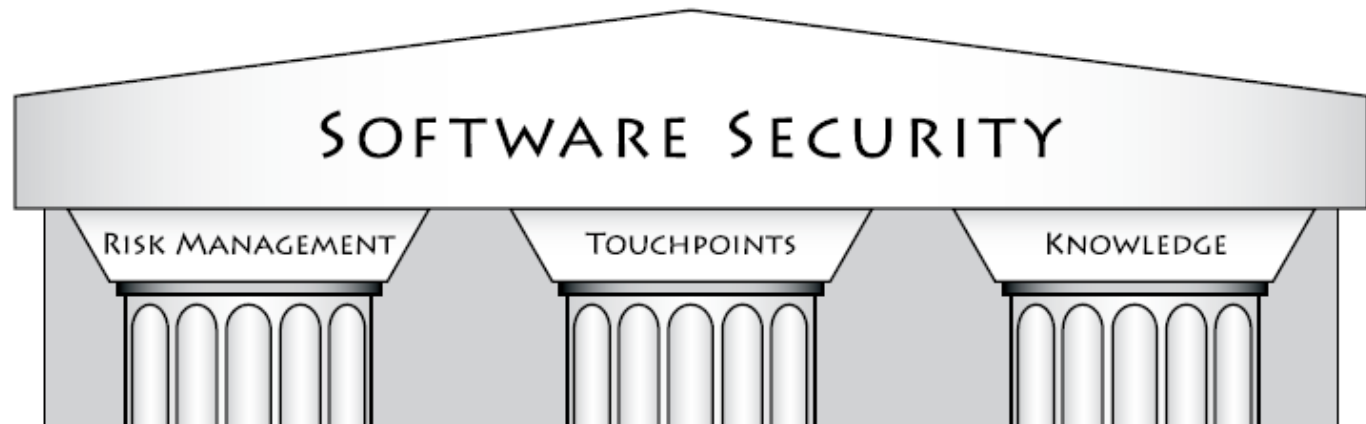
Breaking stuff is important

- Learning how to think like an attacker is essential
- Do not shy away from discussing attacks
 - Engineers learn from stories of failure
- Attacking class projects is also useful!



Solving the problem: Software Security





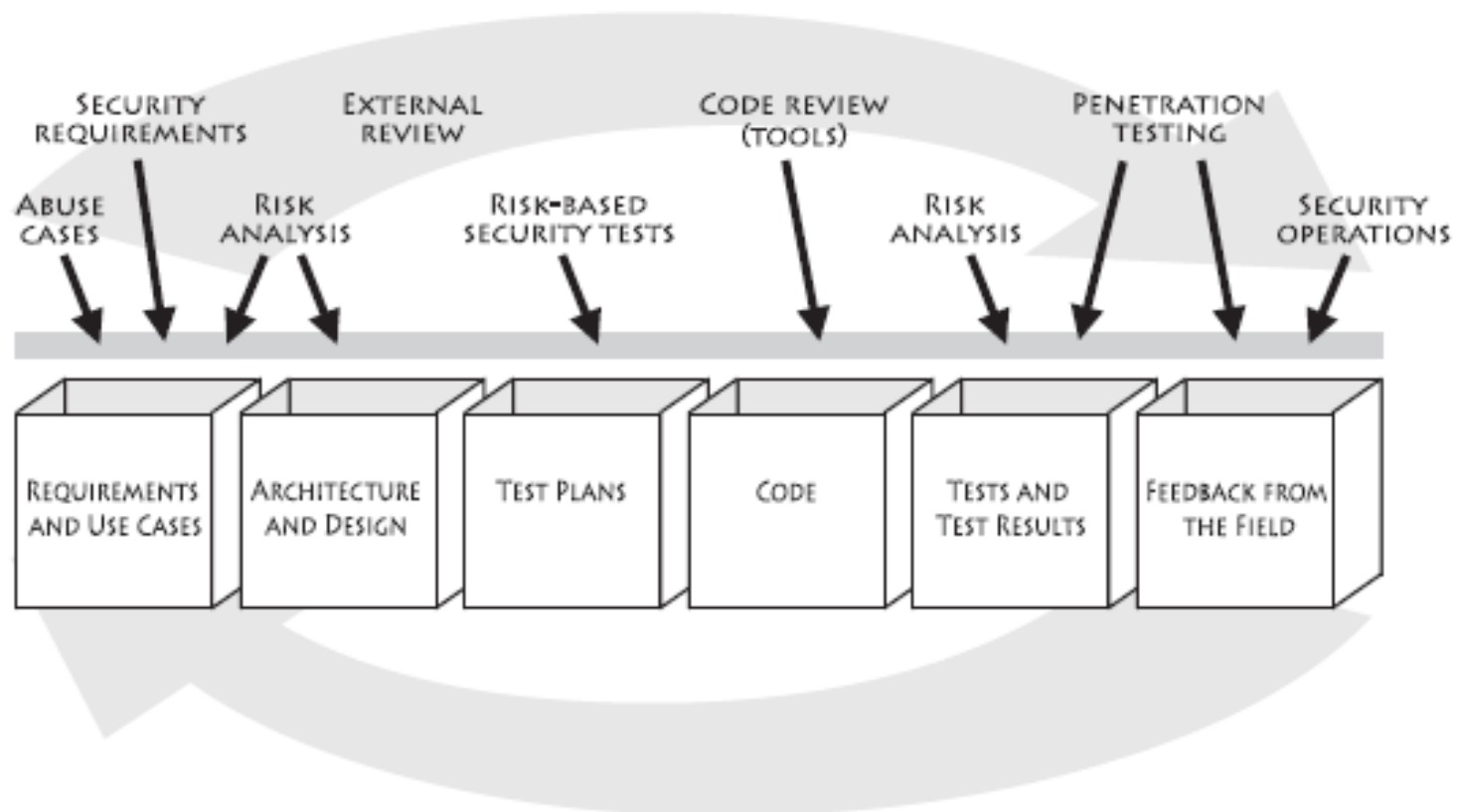
Three pillars of software security

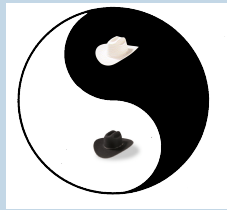
- Risk management framework
- Touchpoints
- Knowledge



cigital

Software security touchpoints





Where to Learn More



informIT & Justice League



- www.informIT.com
- No-nonsense monthly security column by Gary McGraw

- www.cigital.com/justiceleague
- In-depth thought leadership blog from the Cigital Principals
 - Scott Matsumoto
 - Gary McGraw
 - Sammy Miguez
 - Craig Miller
 - John Steven





IEEE Security & Privacy Magazine + 2 Podcasts



The Silver Bullet Security Podcast

with Gary McGraw

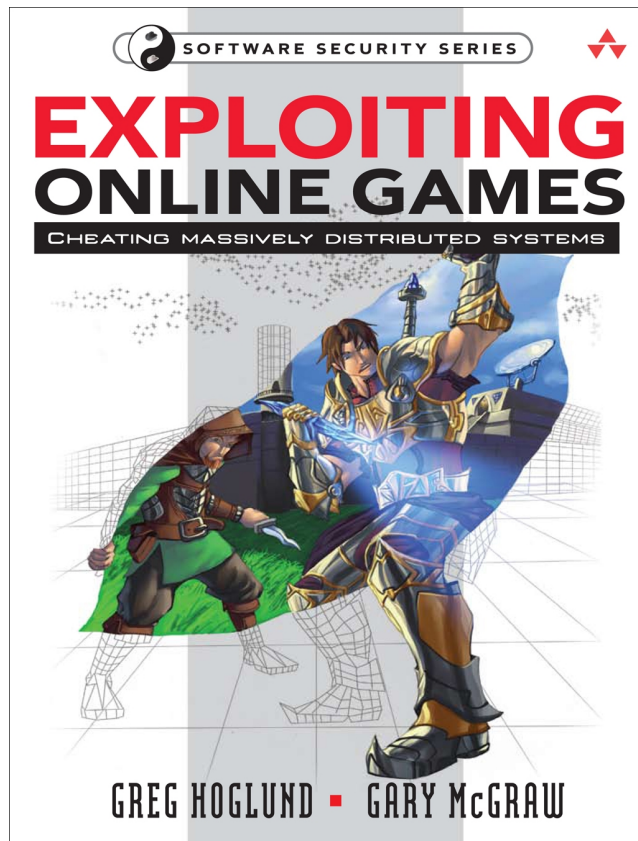


- www.cigital.com/silverbullet
- www.cigital.com/realitycheck

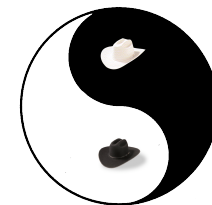
- Building Security In
- Software Security Best Practices column edited by John Steven
- www.computer.org/security/bsisub/



Exploiting Online Games: the book



- Cheating massively distributed systems
 - Sploits, hacks, mods
 - Key lessons for other software
- Part of the Addison-Wesley Software Security Series
- **AVAILABLE NOW**



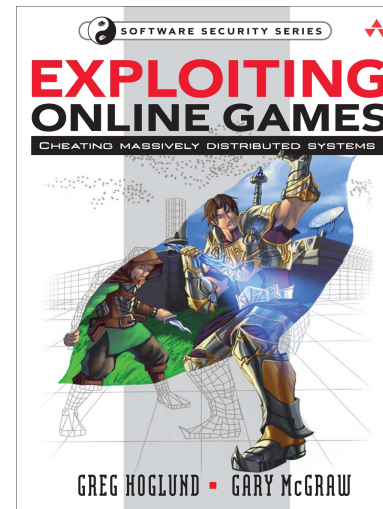

Addison
Wesley



- Cigital's Software Security Group invents and delivers software security
- **WE NEED GREAT PEOPLE**
- See the Addison-Wesley Software Security series
- Send e-mail: gem@cigital.com

"If we're going to improve our security practices, frank discussions like the ones in this book are the only way forward."

-Ed Felten
Princeton



For more

cigital

