Hacking Online Games

Matt Ward & Paul Jennas II

April 22, 2012
Agenda

- Importance
- Attack Tree for Cheating On-line Poker
- Bots
- Denial of Service
- Collusion
- Software Exploits
- Conclusion
Importance

- Out-of-band market for virtual equipment
  - *EverQuest* example
    - In 2004, "the Gross National Product of EverQuest, measured by how much wealth all the players together created in a single year inside the game ... turned out to be $2,266 U.S. per capita."
    - 77th wealthiest country: equivalent to Russia - ahead of India, Bulgaria, and China
  - Most gaming companies frown upon these markets
Importance (cont’d)

- **Question**
  - If the markets are outside of the game itself, should they add any more motivation for gaming companies to prevent cheating?
  - Real motivation for gaming companies is to keep the customer happy
    - 2005 survey showed “no game hacking and cheating” as the #2 reason users chose a particular game and the #1 reason they stopped playing a game
    - “Any behavior that hurts business is bad behavior.” - Raph Koster, Creative Director for *Star Wars Galaxies*

- **Focus on on-line gambling**
  - The “market” in on-line gambling is in-band
  - Obvious added motivation to prevent cheating
Attack Tree for Cheating Online Poker

Cheating Poker Games

- Automation/Bots
  - Resource Collection
- Use DoS
- Collusion
- Software Exploits
  - Client Code
  - Network Packets
  - Server Code
  - Memory
    - Exploit Vulnerability
    - Insider Attack
      - Access Hidden Data
    - Exploit Random # Generator
Poker Tutorial

- Card game where card ranks and forming “hands” are used to determine winner.
  - High card, Pair, Two Pair, Three of a Kind, Straight, Flush, Full House, Four of a Kind, Straight Flush
- Skilled players understand game statistics and human psychology
- Many variations of the game (hand definitions fairly standard)
  - Texas Hold’em, Omaha, Stud, etc.
- Actions include Bet, Check, Fold, Call, Raise

![Playing cards image]
Bots

Resource collection

- Simple poker bots that win most of the time are sufficient for making money
- Cheater can deploy large number of bots
- Each bot may only make a small dollar amount per hour but having several that run simultaneously and around the clock can add up to significant amounts of money
- More complex bots with advanced AI can improve win percentages
- Polaris Pokerbot won 2008 Man vs. Machine Poker Championship
Macros

- Scripts used to create bots that can play a game
- Farming - having a bot perform a repetitive process to gain game resources
  - e.g. In WOW find a location where an enemy spawns, have bot locate and kill enemy, then wait for respawn, rinse and repeat
- AC Tool is a powerful Macro builder (http://www.actool.net/)
- Macros have many legitimate purposes, such as GUI automation testing
AC Tool

- Macro builder - build sequence of commands
- Press any number of keys for any amount of time
- Move mouse to specific mouse location and click left or right mouse button
- Hold left mouse button down and move mouse to drag windows
- Sample pixels
  - Allows you to locate items on the screen (e.g. enemies)
- Simple programming logic (if/else, loops, variables, procedures, etc.)
- Can even ftp
Bots

Countermeasures

- Players can chat to try to discover a bot
  - Some players play several games at once and can’t respond
  - In a game of revolving around misdirection, players may refuse to respond to try to disguise themselves as a bot
- CAPTCHAs - prompt players periodically during long periods of play
- Scan player’s computers
Bot Detection

- World of Warcraft (WOW) has client program called "Warden"
  - Runs every 15 seconds (new versions of Warden come from the server whenever Blizzard’s wants)
  - Checks every dll injected into WOW.exe
  - Reads the titlebar text of every open window
  - Also reads memory of every open process
Greg Hoglund wrote program called "The Governor" to monitor Warden and see exactly what it looks at. Greg noticed email addresses, open URLs, IM contacts and program names being sent back to server. Considers Warden spyware and a major privacy issue. Do you agree?
In on-line poker, users are required to act within a set amount of time.
In on-line poker, users are required to act within a set amount of time.

If the site policy is to auto-fold a disconnected player.
Denial of Service

- In on-line poker, users are required to act within a set amount of time
- If the site policy is to auto-fold a disconnected player
  - Opportunity for a cheater to perform a DDoS attack
Denial of Service

- In on-line poker, users are required to act within a set amount of time
- If the site policy is to auto-fold a disconnected player
  - Opportunity for a cheater to perform a DDoS attack
  - Alice and Bob are in a heads-up situation with a large pot at stake
Denial of Service

- In on-line poker, users are required to act within a set amount of time
- If the site policy is to auto-fold a disconnected player
  - Opportunity for a cheater to perform a DDoS attack
  - Alice and Bob are in a heads-up situation with a large pot at stake
  - When the action gets to Alice, Bob performs a DDoS attack to prevent her from acting
In on-line poker, users are required to act within a set amount of time.

If the site policy is to auto-fold a disconnected player:

- Opportunity for a cheater to perform a DDoS attack
- Alice and Bob are in a heads-up situation with a large pot at stake
- When the action gets to Alice, Bob performs a DDoS attack to prevent her from acting
- Alice is auto-folded, Bob wins the pot
In on-line poker, users are required to act within a set amount of time.

If the site policy is to auto-fold a disconnected player:
- Opportunity for a cheater to perform a DDoS attack
- Alice and Bob are in a heads-up situation with a large pot at stake.
- When the action gets to Alice, Bob performs a DDoS attack to prevent her from acting.
- Alice is auto-folded, Bob wins the pot.

If the site policy is to place the player “all-in”
Denial of Service

- In online poker, users are required to act within a set amount of time.
- If the site policy is to auto-fold a disconnected player:
  - Opportunity for a cheater to perform a DDoS attack.
  - Alice and Bob are in a heads-up situation with a large pot at stake.
  - When the action gets to Alice, Bob performs a DDoS attack to prevent her from acting.
  - Alice is auto-folded, Bob wins the pot.
- If the site policy is to place the player "all-in":
  - Players can intentionally disconnect themselves.
DoS (cont’d)

- DoS attacks for ransom
  - Attack on Grafix Softech
  - Hackers bypassed firewalls and security systems to insert virus that encrypted data on all five production servers
  - Grafix paid ransom to get the encryption key
  - Lost $75,000 per day for approx 1 week
DoS (cont’d)

DoS Countermeasures
- Don’t provide IP addresses of other users
- Use multiple ISPs
- Disaster-recovery plan and replication
- Track user disconnect history
Collusion

- One of the major issues in on-line poker
- Requirement: out-of-band communication
- Two or more players acting together have a significant advantage
  - Whipsawing - coordinated raises to isolate opponents
  - Can share information on hole cards – improves odds calculations
Collusion (cont’d)

The Board

Eve’s hole cards

- 5 cards left that could improve Eve’s hand
  - three 6’s, two 7’s
- Eve needs at least 4:1 pot odds
Collusion (cont’d)

The Board

- 3 cards left that could improve Eve’s hand
  – one 6, two 7’s
- Eve now needs over **7:1** pot odds
- Bob also gains information
- This information saves both Eve and Bob money
Combining chip stacks in a tournament

- In tournament play, size matters
- Colluding players can purposefully lose to one member to create a large chip stack

A single player with multiple accounts can also employ these cheats
Collusion (cont’d)

Collusion Countermeasures
  - IP checking - prevent nearby players from sitting at the same table
Collusion Countermeasures

- IP checking - prevent nearby players from sitting at the same table
  - does not prevent communication via phone, text message, IM
Collusion (cont’d)

- Collusion Countermeasures
  - IP checking - prevent nearby players from sitting at the same table
    - does not prevent communication via phone, text message, IM
    - even less effective given wifi and cell phone tethering
Collusion Countermeasures

- IP checking - prevent nearby players from sitting at the same table
  - does not prevent communication via phone, text message, IM
  - even less effective given wifi and cell phone tethering
- Collusion-detection algorithms
Collusion Countermeasures

- IP checking - prevent nearby players from sitting at the same table
  - does not prevent communication via phone, text message, IM
  - even less effective given wifi and cell phone tethering

- Collusion-detection algorithms
  - effective against whipsawing
Collusion Countermeasures

- IP checking - prevent nearby players from sitting at the same table
  - does not prevent communication via phone, text message, IM
  - even less effective given wifi and cell phone tethering
- Collusion-detection algorithms
  - effective against whipsawing
  - unlikely to detect players sharing hole card information
Collusion Countermeasures

IP checking - prevent nearby players from sitting at the same table
- does not prevent communication via phone, text message, IM
- even less effective given wifi and cell phone tethering

Collusion-detection algorithms
- effective against whipsawing
- unlikely to detect players sharing hole card information

Track player stats, investigate anomalies
Software Exploits

- Software Exploits
  - Client code
  - Network Packets
  - Server Code
    - Exploit Vulnerability
    - Insider Attack
  - Memory or data modifications
Software Exploits

- Exploit the game’s card shuffling algorithm
  - ASF Software displayed shuffling algorithm online to show how fair it was
  - Cigital Software was able to break it in real time
  - A seed is used for random number generator
  - Seed just 32 bits, which allows 4 billion shuffles, much less than a real deck’s 52!
Seed set with number of milliseconds since midnight, but just 86 million milliseconds in a day, so now just 86 million possible shuffles.

Guessing system clock and seed allowed Cigital to reduce number of shuffles to 200,000 possibilities.

Once 5 cards were known they were easily able to tell how the deck was shuffled.
Insider attack at AbsolutePoker

Players noticed a few accounts on AbsolutePoker’s high stakes tables with an abnormally high win-percentage
Insider attack at AbsolutePoker

- Players noticed a few accounts on AbsolutePoker’s high stakes tables with an abnormally high win-percentage
- One player estimated losing as much as $700,000
Insider attack at AbsolutePoker

- Players noticed a few accounts on AbsolutePoker’s high stakes tables with an abnormally high win-percentage
- One player estimated losing as much as $700,000
- Group of players obtained hand histories involving the suspect accounts
Insider attack at AbsolutePoker

- Players noticed a few accounts on AbsolutePoker’s high stakes tables with an abnormally high win-percentage
- One player estimated losing as much as $700,000
- Group of players obtained hand histories involving the suspect accounts
- Win rate was 15 standard deviations above the mean
Insider attack at AbsolutePoker

- Players noticed a few accounts on AbsolutePoker’s high stakes tables with an abnormally high win-percentage
- One player estimated losing as much as $700,000
- Group of players obtained hand histories involving the suspect accounts
- Win rate was 15 standard deviations above the mean
- Video of reconstructed game: [http://www.youtube.com/watch?v=FczbS7FiWSM](http://www.youtube.com/watch?v=FczbS7FiWSM)
Win rates of 5,200 online players

- X-axis represents the number of blinds won per 100 hands
- Y-axis represents the percent of hands the user enters
- Cheater’s win rate is the equivalent of winning a lottery with one-in-a-million odds 6 times in a row
Hacking

Insider attacks which allow a player to see opponents’ hole cards

- 5 cards left that could improve Eve’s hand
  - three 6’s, two 7’s
- Eve needs at least 4:1 pot odds
Software Exploits (cont’d)

- **Software Exploits**
- Insider attacks which allow a player to see opponents’ hole cards

The Board

- if Eve is heads up against Bob then pot odds no longer matter
- Eve has Bob beat
- she can even attempt to induce a bluff out of Bob
Software Exploits (cont’d)

- Hacking Client Side
  - Hacking client code itself (need source access or decompile from exe)
  - Modifying network packets
  - Modifying client memory (memory modifying tools or DLL Injection)
Software Exploits - DLL Injection

- DLL Injection - get application to run your DLL
- DLL vs EXE
  - exe is executable program, has main()
  - exe runs in own memory
  - dll is dynamic linked library, no main()
  - dll is like a library, can be loaded dynamically in memory by many processes
  - Can link dll at load time or run time
Software Exploits - DLL Injection

- DLL Injection - get application to run your DLL cont
- Three examples:
  - CreateRemoteThread
    - Use Windows API to start a thread (running your dll) in another process
  - SetWindowsHookEx
    - ”Hook” onto a Windows message for a remote thread
    - Your dll will run in remote thread when message is received
  - Code Cave Method
    - Suspend target thread (use SuspendThread)
    - Save address of next instruction to be executed (look in register for stack pointer)
    - Allocate and load dll in memory (use VirtualAllocEx). Set target thread’s next execution instruction to the beginning of our dll’s location in memory
    - Resume suspended target thread. When we finish our work, call back what would have been the next instruction
    - Can imagine running some code each pass in game loop
Software Exploits - Create Remote Thread Demo

- CreateRemoteThread example with Minesweeper
  - Used Ollydbg and IDA to learn Minesweeper timer memory location and function signatures
  - Allows me to change time and open about dialog
Interactive Disassembler (IDA)
- Generates assembly code from exe
- Show imported functions from other dlls
- By analyzing stack and register usage and cross referencing with known libraries can generate function names and parameters
- Has debugger capabilities

IDA - Software Exploits cont.
; int __stdcall DrawBombCount(HDC hdc)
_DrawBombCount@4 proc near

l= dword ptr 4

push ebx
push ebp
push esi
mov esi, [esp+0Ch+1]
push edi
push esi
; hdc
call ds:__imp__GetLayout@4 ; GetLayout(x)
mov ebp, ds:__imp__SetLayout@8 ; SetLayout(x,x)
mov ebx, eax
mov [esp+10h+1], ebx
and ebx, 1
jz short loc_10027AA

_DrawBombCount@4 endp
Debugger

- OllyDbg
  - Also shows assembly, but can set breakpoints in code
  - View stack and registers

- http://www.ollydbg.de/
Olly - Software Exploits cont.
Hacking Countermeasures

- Employ insider attack safeguards (background checks, code reviews, access to critical info requires multiple people, etc.)
- Simple client
  - Minimize data available to client
  - All critical decisions should be made by server
- Tools that check for injected DLLs or checksums on client code
Conclusion

As a user
- On-line gamblers need to do their homework
- Review the security features employed by the gambling site

As a gaming company
- Security precautions need to be regularly reviewed and updated
  – security is an ongoing and evolving battle

Even out-of-band markets provide motivation
- “of course, there is one kind of help you usually don’t want: the government.” – Stephen Davis
End of Document
Online gambling - american gaming association, 2012.
http://www.americangaming.org/government-affairs/key-issues/online-gambling.

Noa Bar-Yosef.
Hacking the house: How cybercriminals attack online casinos.
Security Week, August 2011.

Simon Carlass.
Gaming Hacks.

Darawk.
Dll injection.
Blizz Hackers, March 2006.

Stephen Davis.
Course Technology PTR, 2009.

Jack M. Germain.
Global extortion: Online gambling and organized hacking.

Greg Hoglund and Gary McGraw.
Exploiting Online Games: Cheating Massively Distributed Systems.

Adam Lake.
Game Programming Gems 8.
Course Technology PTR, 2010.
Gary McGraw and Greg Hoglund.  
*Cheating Online Games.*  
Addison-Wesley Professional, 2006.

Matthew Pritchard.  
How to hurt the hackers: The scoop on internet cheating and how you can combat it.  
Gamasutra, July 2000.  

Andrew Rollins and Ernest Adams.  
*Andrew Rollings and Ernest Adams on Game Design.*  

Shahen Ramezany.  
Hacking / exploiting / cheating in online games.  
Abysssec, March 2011.  
Ira Rosen.  
How online gamblers unmasksd cheaters.  

Nikola Strahija.  
Russian hackers raid largest online gaming operation and destroy data in blackma.  

Daniel Terdiman.  
Hacking online games a widespread problem.  
CNET, April 2009.  

Cheating in online games.  
Wikipedia, February 2012.