CS6431: Security and Privacy Technologies

Lecture: Online-Game Security

Instructor: Ari Juels
22 Nov. 2016
Here’s real estate mogul Anshe Chung.

Notice anything peculiar about her?
Anshe Chung is a “real estate” broker in virtual worlds, i.e., she’s an avatar!

Real name: Ailin Graef

In 2006,

Chung / Graef declared herself “first online personality to achieve a net worth exceeding \textit{one million [real]} US dollars\textit{ from profits entirely earned inside a virtual world}”

Again, selling “real estate”!

Incorporated "Anshe Chung Studios, Ltd." in Hubei, China

Employed 80 people developing real estate in virtual worlds / MMOs: \url{http://acs.anshechung.com}
What’s a Virtual World / Massive Multiplayer Online (MMO) game?

• SecondLife is an MMO

• MMO involves many users co-existing in a single, server-maintained “world”

• Canonical example: World of Warcraft
  • Peak of 12+ million users; 5+ million today
    • Population of NYC: 8.4 million
  • Partitioned into shards or realms, each a distinct duplicate of the “world” (parallel universe)
    • Each character is confined to a realm, to prevent overloading of servers
    • 200+ realms in each of U.S. and E.U.
Massive Multiplayer Online (MMO) game market

More generally:

- 46% of online gamers are women
- 59% of Americans play video games
- 1.2 billion gamers worldwide

Source: ad2games (2014)
Where there’s money and competition…

“Games are a harbinger of software security issues to come.”

—Hogland and McGraw
Gold farming

“Gold farming” is the practice of mining gold in virtual worlds for sale in real world.

Who does it?

Gold farmer plays to harvest virtual gold for resale

In 2005, *The New York Times* stated that there were over 100,000 full-time gold farmers in China alone.

Roughly five times the total student population of Cornell Univ.!

In 2007, *NYT* reported salaries of $0.30 / hour and 84 hours / week for some gold farmers
Gold farming

• Trading of virtual currency for real cash employs hundreds of thousands of people worldwide and generates between $200 million-$1 billion annually
  • R. Heeks, Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games (2008)
  • "Third party gaming services industry"
    • Gold farming
    • "Power leveling": making game characters more powerful

• V. Lehdonvirta and M. Ernkvist. Knowledge Map of the Virtual Economy, 2011. (World Bank paper)
  • Third party gaming services industry produced an estimated $3 billion in 2011, mostly in developing economies
  • By contrast, of $70 billion coffee industry, only $5.5 billion in developing economies
North Korean army of hackers generating money for Kim Jong-il

Kim Jong-il has found an unusual way to give the North Korean economy a boost. According to South Korean authorities, the leader of the Democratic People’s Republic of Korea has turned to *gold farming* - yes, that kind of gold farming. As The New York Times reported, North Korea has been using its top science universities to train hackers, who are then unleashed on popular South Korean MMOs, such as Lineage and *Dungeon Fighter Online*, to generate money for North Korea.

A group of five organizers were arrested Thursday in Northern China for drawing on the North Korean army of hackers to create a group of 30 “video gaming experts” to generate money by abusing MMOs. The experts were able to write software that infiltrated several games and allowed unmanned computers to operate in the game 24 hours a day.

Just call me Goldfinger.
World of Warcraft woes

- WoW and other massive multiplayer online games are one frontier for security issues and cybercrime!
- Gold farmers are in fact a security issue
  - Considered "unfair" element in game
  - Can lead to various forms of abuse
- Blizzard bans 50,000+ gold farmers in 2006
  - Cost of gold coin rose from $0.06 to $0.35 in January 2007 (NYT)
World of Warcraft woes

- Another problem: Hacked accounts became epidemic—keylogging Trojans looking specifically for WoW players
- Blizzard starts offering two-factor authentication in 2009 ($6 / token)
- Major Blizzard breach in 2012 revealing
  - Answers to life questions
  - Passwords (SRP-protected, but crackable)
World of Warcraft woes

- **Two-factor authentication** defeated in WoW by attackers in 2014

- How?
  - Man-in-the-middle attack!
    - Trojan captures passcode for immediate re-use
    - Note that phishing attack can in principle accomplish the same…without malware
World of Warcraft woes

• Warlords of Draenor launch in Nov. 2014 crippled by massive distributed denial-of-service attack
  • Such attacks are becoming common (e.g., EVE in 2013)

• Why?
• One hypothesis is that they are serving as cover for breaches.
  • But we don’t really know…
MMO-specific security concern

- Money laundering in virtual worlds has been a concern since before Bitcoin (2008)!
  - In this sense, MMOs were a forerunner of Bitcoin
- Old method of money laundering: Leave $10,000 in unmarked notes in briefcase under bridge
- New method: Bad Guy A gives Bad Guy B a pile of Teebu’s Blazing Longswords
- Is the FBI going to monitor ownership of magic longswords?
Online-game security issues

In-game cheats of two types:

1. **Bots / overlays** (client-side software agents) that
   - Assist in / perform repetitive activities like farming
   - Confer enhanced capabilities
     - E.g., Macros can inject keystrokes and mouse movements at superhuman speed
Online-game security issues

In-game cheats of two types:

1. **Bots / overlays** (client-side software agents) that
   - Assist in / perform repetitive activities like farming
   - Confer enhanced capabilities
     - E.g., Macros can inject keystrokes and mouse movements at superhuman speed

2. **Code modification** in games exploited to achieve
   - Teleportation
   - Item duplication
   - Semi-god mode
   - X-ray vision (active)
   - Arise because performance requires code execution on client side
     - E.g., opaque walls may be *rendered on client*
   - Code modification yields x-ray vision
Online-game security issues

- MMOs are massively distributed systems.
- “Time and state” (synchronization) errors are rampant.
- Errors in which views of clients and servers differ.
- “Time and state errors are the XSS attacks of tomorrow.”
Code-Modification
Attacks
Sad story:
The saga of Iggy the Dwarf

Rule: Hit by dragon always causes 100-1000 points of damage

200 hit points

500 hit points

client

server

offload
Choose your own adventure:
Iggy the Dwarf becomes a “semi-god”

Iggy the Dwarf

1 hit point

Cheat Engine

offload

server

client
Cheat Engine is an open source tool designed to help you with modifying single player games running under window so you can make them harder or easier depending on your preference.

The tool for games mods (and a little more)

Cheat Engine is a utility to modify and apply "touch-ups" to video games, along with some extra tool for debugging software and games.

Cheat your way to the top

Cheat Engine is an open source tool for editing the code of a game. The program opens the process of the game and allows you to change the data. It includes a scanner so that you can easily find the values you're looking for.

we are able to change a lot of functions in a game to our advantage. Seeing and walking through walls, flying around, jumping very high, checking out inventories of other players, disabling cooldowns, reducing damage taken, invisibility and partial invisibility, teleporting, auto aim functions – there are a lot of cheats that can be achieved using hacks.

(semi-god mode)
Challenge for server: How to ensure client ran valid game code?
Challenge: Was valid game code $F$ executed?

I.e., $F(A,X) = B$ for some $X$
As opposed to illegal “mod” (state-modifying code) $G$?

where for all $X$, $F(A, X) \neq B$
Idea 1: All authoritative state on server

• Idea: Pure server-side execution
• Server runs code $F$
• Client provides input $X$
• Server renders graphics for client
• Problem: Bandwidth intensive!
• “In the US and European markets, a good goal to shoot for is 4–6 kilobits per second / player or less”


• Developers try to put as much authoritative state on the server side as possible…
• But performance considerations make this hard
Idea 2: Audit client management of state

- Server uses model of code $F$
- Server sends state A, receives state B
- Server checks whether there exists an input $X$ that creates a path $A \rightarrow B$ through $F$
  - Interesting use of symbolic execution
- Non-existence of code path in valid software $\rightarrow$ use of hacked software
- Client doesn’t have to transmit $X$, which keeps bandwidth low…
- Keeps pace with some games, but not all… and doesn’t address all cheats.
Idea 3: Use trusted hardware on client

- $F$ can run on a client with the support of trusted hardware
- Server can verify that client is running $F$
- Emerging technologies, such as Intel Software Guards Extension (SGX) will make this increasingly easy by
  - Isolating $F$ even from a rogue OS or user
  - Allowing a client to *attest* to execution of $F$
    - I.e., generates digitally signed statement proving that it’s running $F$
  - Server can check attestation
- Unfortunately, SGX is only in its infancy today…
Code-Overlay Attacks
Unfortunately, Ideas 1-3 don’t necessarily help against bots!

• E.g., aimbot
  • Automatically targets user’s weapons
  • Superhuman aim and speed in shooter
• Doesn’t even need to look at game data!
• Can intercept data sent to video subsystem.
  • (Includes information about hidden objects)
• So no core code modification required
Interesting challenge

- How does a server distinguish a very skillful player from a bot-assisted one?
- How do you tell a farmer from a real player? How do you enforce “fair play”? 
Another challenge: Hacking maps to lift fog of war

Kartograph
Elie Bursztein and Jocelyn Lagarenne
Stanford University

IEEE S&P 2011
Strategy account for 35% of the games sold in 2009
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Units

Tankbuster

$ 300  0.05

Anti-Armor

Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Building

Tankbuster
$300 0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Resources

Tankbuster

$300  0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Tankbuster
$300  0.05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Visible

Tankbuster
$300  0.05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Fog of war

Tankbuster

$300  0.05

Anti-Armor

Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
What is a map hack
What is a map hack
Why are map hacks possible?

- Real-time strategy games are fast-moving
  - Game lasts at most 30 minutes
  - Important to keep bandwidth low
- Data sent peer-to-peer
  - State promiscuously *pushed*, i.e., one client's state resident on another client
    - *Pulling* would introduce more traffic
- Note: Not MMOs
  - World not persistent
- Defense: *Obfuscate* map data
How to do a map hack
How to do a map hack

Reduce
How to do a map hack

Reduce

Find
How to do a map hack

Reduce  Find  Understand
How to reduce the search space

Game memory

Play
Discover
Play more
Step 1

Removing unrelated memory
How to reduce the search space

- Game memory

- Play
- Discover
- Play more
Step 2
Discovering the map and keeping relevant memory
Now, STOP everything. Use a unit to discover the map. Try to do a square representing 1/4 of the total map.
How to reduce the search space

Game memory

Play

Discover

Play more
Step 3
Removing more unrelated memory
(UNCHANGED) Now, like in step 2 try to do everything except discovering the map.
How to reduce the search space

Game memory

Play    Discover    Play more
Step 4
Finding the map in the remaining memory
Working assumption
Maps are stored in 2-D arrays
Working assumption
Maps are stored in 2-D arrays
Figure 7. *Kartograph* heat map visualization of the reduced memory space. Possible map structures are circled in red.

Figure 8. Example of a misaligned visibility map for Age of Empire III
Supreme Commander 2 encodes the visibility as a short integer, representing how many units are able to see a given cell of the map.
Step 5
Understanding the map’s structure
Key idea: Adversarial game instrumentation

- Move units
- Diff will represent
  - Part of map unit discovers or
  - Unit's previous and new position
- Study memory regions where diffs occur to understand data structures

Figure 9. Diff-map visualization of adversarial game instrumentation
Final steps

• Also need to locate and reverse-engineer data structures for *units*
  • Create units and study changes in memory
• Map can be locally *rewritten* to remove fog of war
• If code performs state-consistency checks among clients, use separate (out-of-band) visualization

• N.b.: Passive attack: No way for server / other clients to detect it!
Countermeasure: cryptography!

Ideal protocol: Private Set Intersection

- Alice inputs $V_A$, her visible grid elements
- Bob inputs $U_B$, his units' grid locations
- Protocol outputs $V_A \cap U_B$ to Alice
Private Set Intersection (PSI)

Key ideas for Jarecki-Liu, honest-but-curious version:

- PRF $o_k(u)$
  - Secret key $k$ held by Bob
- Bob:
  - Computes $k_u = o_k(u)$ on all $u$ in $U_B$
  - Constructs ciphertext $c_u = \text{Enc}(k_u, \text{unit } u \text{ data})$
  - Sends set $C$ of all ciphertexts to Alice
- Alice
  - Obtains *obliviously* from Bob $k_v = o_k(v)$ for all $v$ in $V_A$
  - Tries to decrypt ciphertexts $C$ using keys
Practical oblivious PRF

- Group $G$ of order $q$
  - Non-standard elliptic curve
- $M$ is set of map cell values
- Hash $H_t: M \to G \setminus \{1\}$
- $k \leftarrow \$ Z_q$

$$o_k(v) := H_1(v)^k \in \mathbb{G}$$

Oblivious evaluation of $o_k()$

- Alice chooses a random integer $r \in [1, q - 1]$ and sends $x := H_1(v)^r$ to Bob;
- Bob responds with $y := x^k = H_1(v)^{rk}$;
- Alice computes $o_k(v) = y^{r^{-1}}$. 
The future of gaming
Many interesting ongoing challenges

• How do you protect against *insider attacks* in MMOs?

• In 2006, three Chinese employees from Shanda Interactive in 2006 sold virtual weapons from the MMO Legend of Mir II for a huge profit.

• They were charged with embezzlement and sentenced to five years in prison.

• Big problem on all kinds of systems…
Games are colliding with physical world

Ingress

- Augmented reality MMO published by Google
- Overlays gameplay on real physical landscape (like Manhattan)
- Game goal: Gain control of “portals” corresponding to real-world landmarks and link them to establish fields of control
  - I.e., game board is real world

Where Virtual Meets Real

Ingress, a Mobile Game From Google

By CHRIS SUELLENTROP  JULY 14, 2014

Many of the best video games create distinctive places for their players to visit: Rapture, the cratered libertarian society on the bottom of the ocean, from BioShock; Liberty City and Los Santos, the fun-house mirrors of New York and Los Angeles, from
Games are colliding with physical world

• How might you cheat?
• E.g., “touch” a portal?
• Possible new vectors for cheats:
  • GPS spoofing
  • Game-playing drones
A game controller: Brain-Computer Interface (BCI)

- Another type of interface, allows computer control via thoughts
- BCI generally uses electroencephalography (EEG)
  - Measures electrical fields produced by neuronal synaptic activity
- Process is non-invasive
- Headsets for a few hundred dollars now available as gaming controllers
  - E.g., NeuroSky Mindset and Emotiv EPOC
Security / privacy?

- In 2008, The Nielsen Company (a leading market research company) acquired NeuroFocus, a neuroscience research firm
- Nielsen has developed an EEG-based BCI device called Mynd
  - “…market researchers will be able to capture the highest quality data on consumers’ deep subconscious responses in real time wirelessly, revolutionizing mobile in-market research and media consumption at home.”
Can secrets be extracted?

- Examined Event-Related Potential (ERP)
  - P300 ERP is response to target (recognized) stimulus
    - detected as amplitude peak in EEG signal 300 ms after the stimulus
  - E.g., unknown face vs. that of President Obama
- Month-of-birth extraction experiment:
  1. Message displayed on screen for two seconds: "When were you born?"
  2. Months presented sequentially in randomly permuted order
  3. P300 ERPs examined
- Researchers guessed month of birth correctly with 60% probability!
- Could also extract some information about PINs, face familiarity, etc.
- Not devastating attack, but just the beginning of really deep privacy issues…