Welcome to the real world
#kartograph
supernatural powers!

- Learn kungfu
- Infinite money
- Xray vision
- god mode
Supreme commander 2
Memory based attack
Memory based attack

Memory

Modification
Memory based attack
Benefits (fast and furious)

- Generic
- Fast
- Invisible
Drawbacks: Needle in a Haystack

- Structure are hard to find
- No control over the flow

Game memory

Structures
Outline

• Background
Outline

• Background
• Building a maphack
• Background
• Building a maphack
• Invulnerable unit
Outline

• Background
• Building a maphack
• Invulnerable unit
• Network
Outline

• Background
• Building a maphack
• Invulnerable unit
• Network
• Demo
Background
273 Millions games sold in 2009
Game type

Action
Game type

Action

First person
Game type

- Action
- First person
- Sport
Game type

- Action
- First person
- Sport
- Role playing
Game type

- **Action**
- **First person**
- **Sport**
- **Role playing**
- **Adventure**
Game type

- Action
- First person
- Sport
- Role playing
- Adventure
- Strategy
Strategy account for 35% of the games sold in 2009
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.
Resources

Tankbuster
$300 0:05
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.
Minimap

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.
How to cheat at a RTS?
How to cheat at a RTS?

Resources
How to cheat at a RTS?

Resources

units
How to cheat at a RTS?

Resources  units  map
What is a map hack
What is a map hack
There is no spoon
Maphack
Map hack step
Map hack step
Map hack step

Reduce haystack
Map hack step

Reduce haystack

Find
Map hack step

Reduce haystack  Find  Understand
Map hack step

Reduce haystack  Find  Understand  Rewrite
Acquiring game memory
Acquiring game memory
Reducing memory

Game memory
Reducing memory

Game memory

Step 1 play
Reducing memory

Game memory

Step 1 play
Reducing memory

- Game memory
- Step 1: play
- Step 2: discover
Reducing memory

Game memory

Step 1 play

Step 2 discover
Reducing memory

Game memory

Step 1 play

Step 2 discover

Step 3 play
Reducing memory

Game memory

Step 1 play
Step 2 discover
Step 3 play
Reducing memory
Acquiring the game’s memory
Step 1
Removing unrelated memory
Step 2
Discovering the map and keeping relevant memory
Step 3

CHANGE! Now, STOP everything. Use a unit to discover the map. Try to do a square, representing 1/4 of the total map.
Step 3
Removing more unrelated memory
Step 4
Finding the map in the remaining memory
Working assumption
Working assumption

Maps are stored in 2-D arrays.
Step 5
Isolating the potential map
Step 6
Understanding the map’s structure
Step 8
Rewriting game memory for fun and profit
Starcraft 2 mini map
Starcraft 2 mini map
Unexpected effects
unit hacks
When things become harder

- Unit lists are very small
- Visualization won’t work this time to find it :(  
- Solely based on memory shape analysis algorithms
Stack detection heuristics

• **Only one new integer by unit**
• **Each integer is a valid pointer**
Unit hack Step

Game memory
Unit hack Step

Game memory
Unit hack Step

Game memory
Unit hack Step
Unit hack Step
Game memory
Unit Hack shape
Understanding unit structure
Understanding unit structure
Understanding unit structure

make it move
Understanding unit structure

make it move
Understanding unit structure

make it move
Understanding unit structure

make it move

make it bleed
Understanding unit structure

make it move
make it bleed
Network
Here is what happen when you are actively cheating
Here is what happen when you are actively cheating
Rewriting network traffic

- Resync the game or get caught
- Use LSP (Layer service provider) to rewrite network traffic
Understanding the network traffic
Understanding the network traffic

Bucket
Understanding the network traffic

Bucket

Visualize
Understanding the network traffic

Bucket  Visualize  Understand
Understanding the network traffic

- Bucket
- Visualize
- Understand
- Resync
Civilization 4 visualization
Civilization 4 visualization

LSP listener

Jocelyn Lagarenne & Elie Bursztein
Kartograph
http://ly.tl/t10
Civilization 4 visualization

LSP listener

Buckets
Civilization 4 visualization

Bucket visualization

LSP listener

Buckets
Civilization 4 visualization

Bucket visualization

LSP listener

Buckets
Civilization 4 visualization

Bucket visualization

LSP listener

Buckets

Length

time
Civilization 4 visualization

Bucket visualization

Trace diff map

LSP listener

Buckets

Length

time
Civilization 4 visualization

- Trace diff map
- Fixed value
- Buckets visualization
- LSP listener
- Time
- Length
- Fixed value

Buckets

LSP listener

Bucket visualization

Trace diff map

Fixed value

Length
Civilization 4 visualization

Bucket visualization

Trace diff map

Fixed value

Counter value

LSP listener

Buckets

Length

time

Fixed value

Counter value
Civilization 4 visualization

Bucket visualization

- Fixed value
- Counter value
- Random/crypted value

Trace diff map

LSP listener

Buckets

Length

time
Ongoing work

• A cryptographic lib to improve games
  • Multi-party cryptography against map hack
  • Private Equality Test against synch manipulation
  • Homomorphic encryption for the rest
• A classifier to defend against bots
Get your video and the slides!

We made a video tutorial of Kartograph for you!

http://ly.tl/t10