Welcome to the real world
supernatural powers!

- Learn kungfu
- Infinite money
- Xray vision
- god mode
God mode illustrated (video)
Memory based attack
Memory based attack

Memory

Modification
Memory based attack

Memory

Modification
Benefits (fast and furious)

- Generic
- Fast
- Invisible
Drawbacks

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

Game memory Structures
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
Game type
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.
Units

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.
Minimap
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.
Supreme commander 2
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
How to do a map hack
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 do a map hack

Reduce
Find
Understand
Rewrite
Acquiring game memory

Game memory
Acquiring game memory
How to reduce the search space

Game memory

Play  Discover  Play more
How to reduce the search space

Game memory

Play

Discover

Play more
How to reduce the search space

Game memory

Play
Discover
Play more
How to reduce the search space

Game memory

Play
Discover
Play more
How to reduce the search space
Acquiring the game’s memory
Step 1
Removing unrelated memory
Step 2
Discovering the map and keeping relevant memory
Step 3
Removing more unrelated memory
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
Step 5
Isolating the potential map
In game

In memory
Step 6
Understanding the map’s structure
Step 8
Rewriting the memory for fun and profit
Unexpected effects
Unit hacking
Stay tuned for our next episode

Will be available in the online version of the slides
Kartograph Demo
Ongoing work

• Active attack (Network).
• Defense (Multi-parties crypto)
Questions

- Active attack (Network)
- Defense (Multi-parties crypto)