Pwning games – Cheaters, hookers and endbosses

Summer of Pwnage

What does this have to do with WordPress ??

What does this have to do with WordPress ??

Nothing! ☺

Target : iOS games with GameCenter

Handling highscores and achievements

Handling highscores and achievements

Player

Play
Game

Send score

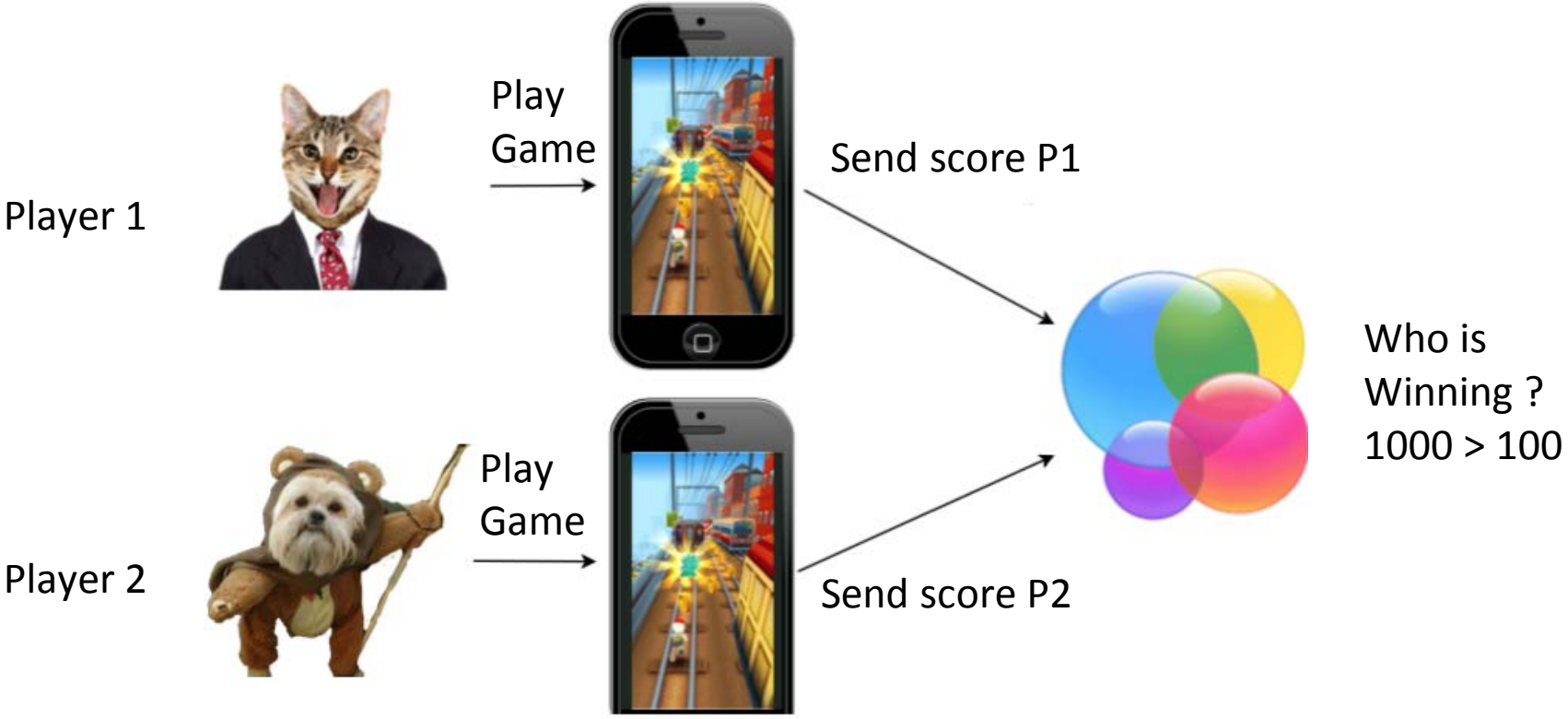
Handling highscores and achievements

Player

Play
Game

If 100000 pts
update
achievement

Handling highscores and achievements



Cheating

Cheating

Player

Play
Game

Send score

Cheating

Player

Play
Game

Modify score
With Burp

Cheating

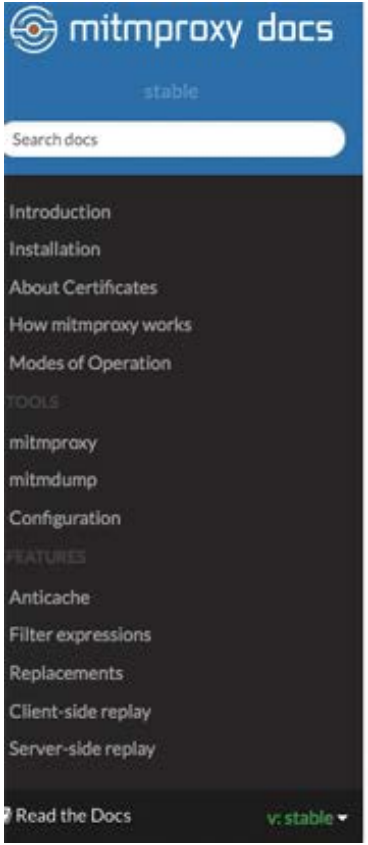
Player

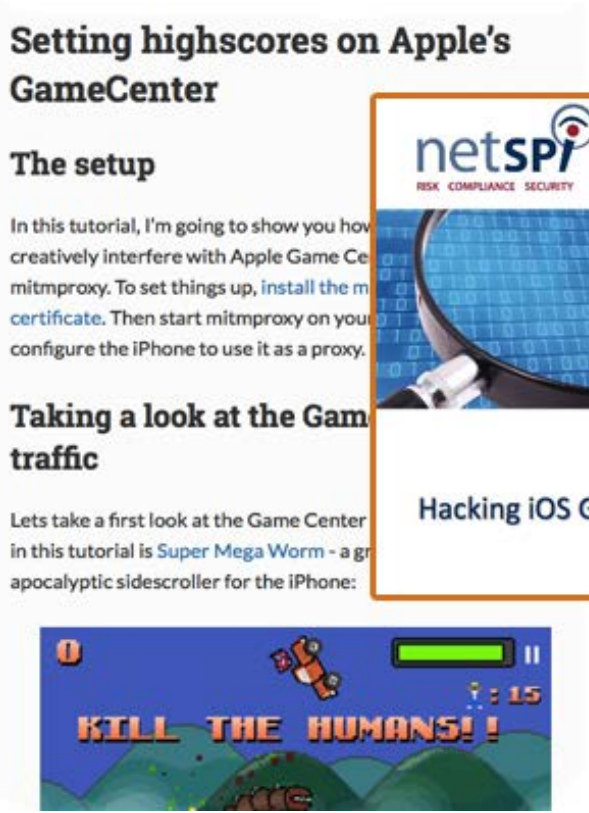
Play
Game

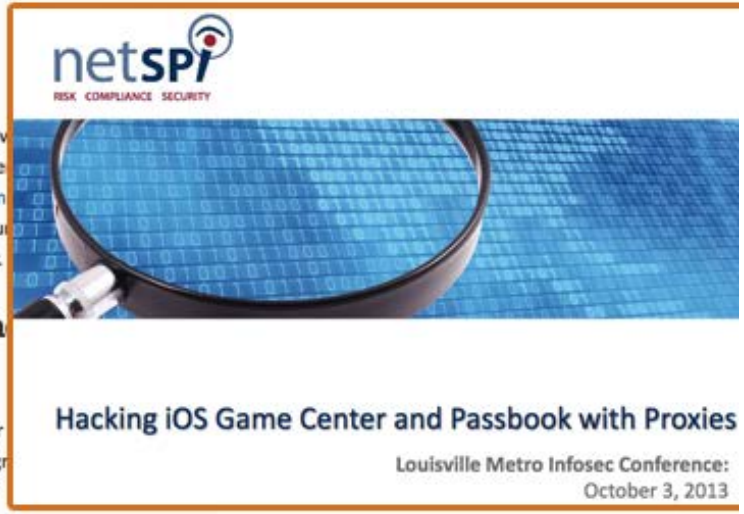
Modify score
With Burp

WINNING!!!

Online tools and guides







Questions ??

But wait ….

But wait ….

What if Burp fails?

What if Burp fails?

- App signs messages

What if Burp fails?

- App signs messages
- App encrypts messages

But wait ….

What if Burp fails?

- App signs messages
- App encrypts messages
- App uses other protocol

But wait ….

What if Burp fails?

- App signs messages
- App encrypts messages
- App uses other protocol
- App uses SSL certificate pinning

Possible solutions

Possible solutions

- Reverse the ”security” mechanism and write a Burp plugin if possible

Possible solutions

- Reverse the ”security” mechanism and write a Burp plugin if possible
- Binary patch the app to send other score

Possible solutions

- Reverse the ”security” mechanism and write a Burp plugin if possible
- Binary patch the app to send other score
- Dynamically modify functions and values in runtime

Possible solutions

- Reverse the ”security” mechanism and write a Burp plugin if possible
- Binary patch the app to send other score
- Dynamically modify functions and values in runtime
- Other…

Choices, choices .....

Modification during runtime

Modification during runtime using …

Hook(er)s

Modification during runtime using …

Hook(er)s

(And Black Jack)

Modification during runtime using …

Hook(er)s

(And Black Jack)

“Burp” for methods

Pros and Cons

Pros and Cons

Pros:

- No reversing required when hooking the framework and library methods!

Pros and Cons

Pros:

- No reversing required when hooking the framework and library methods!
- No binary (re)signing

Pros and Cons

Pros:

- No reversing required when hooking the framework and library methods!
- No binary (re)signing
- No binary decryption (required for reverse engineering)

Pros and Cons

Pros:

- No reversing required when hooking the framework and library methods!
- No binary (re)signing
- No binary decryption (required for reverse engineering)
- No nasty binary patching (e.g. mach-o universal binary patching)

Pros and Cons

Pros:

- No reversing required when hooking the framework and library methods!
- No binary (re)signing
- No binary decryption (required for reverse engineering)
- No nasty binary patching (e.g. mach-o universal binary patching)

Cons:

- Reverse engineering if non-framework and library methods need to be hooked

Pros and Cons

Pros:

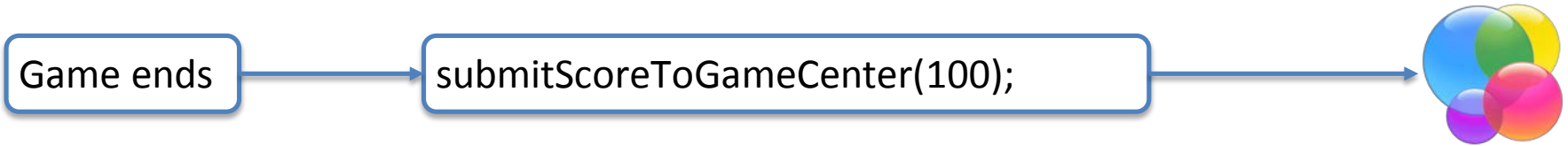
- No reversing required when hooking the framework and library methods!
- No binary (re)signing
- No binary decryption (required for reverse engineering)
- No nasty binary patching (e.g. mach-o universal binary patching)

Cons:

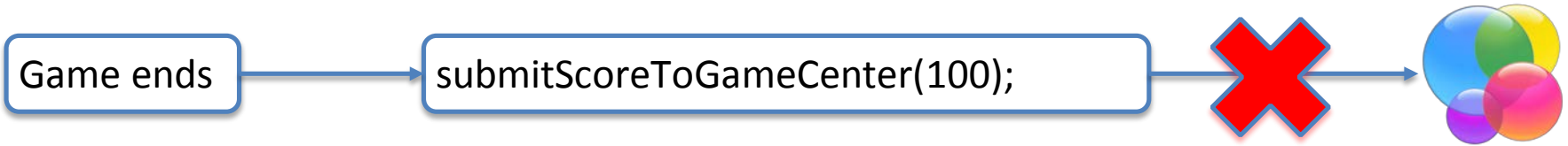
- Reverse engineering if non-framework and library methods need to be hooked
- Requires iOS Jailbreak !

How does it work ?

How does it work ?

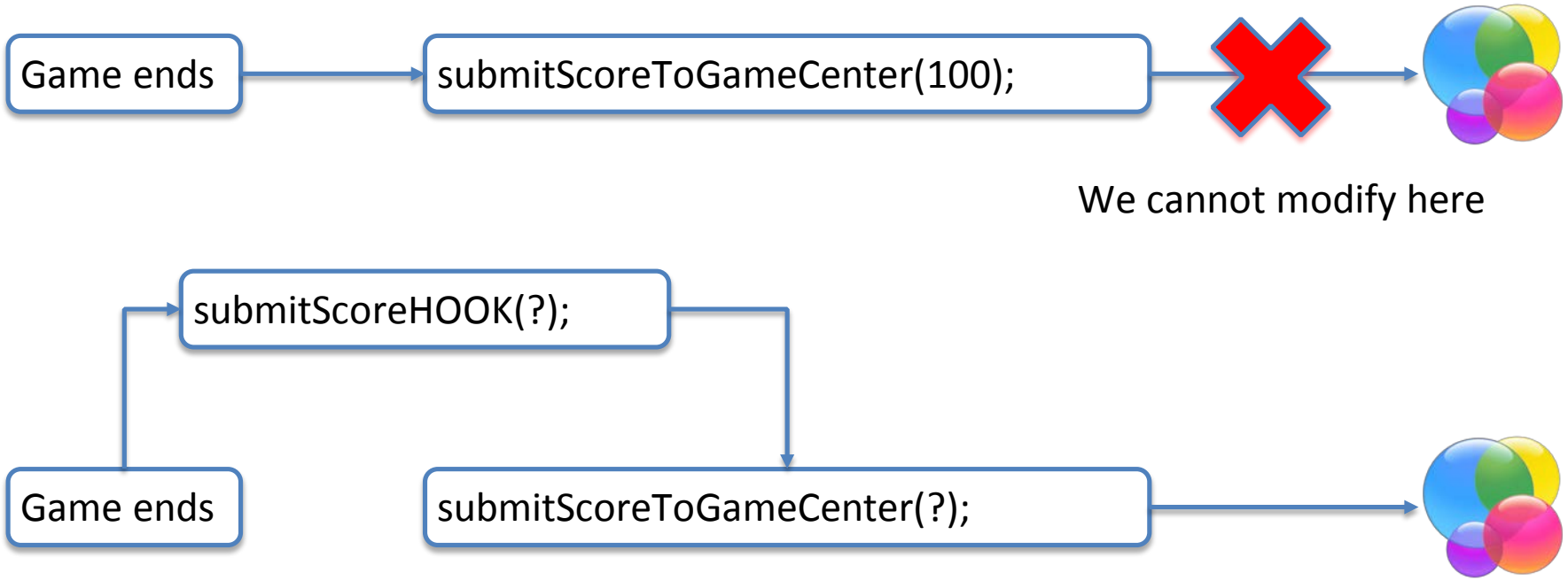


How does it work ?

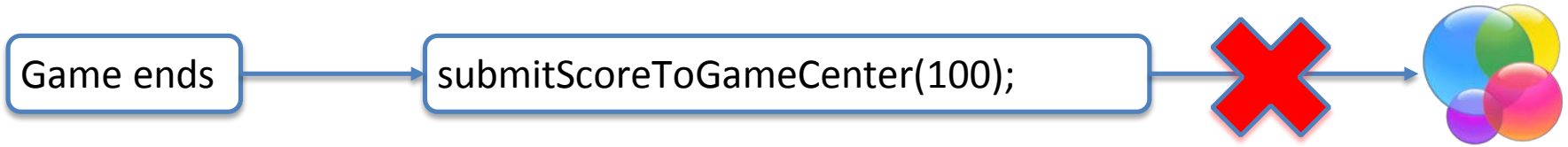


We cannot modify here

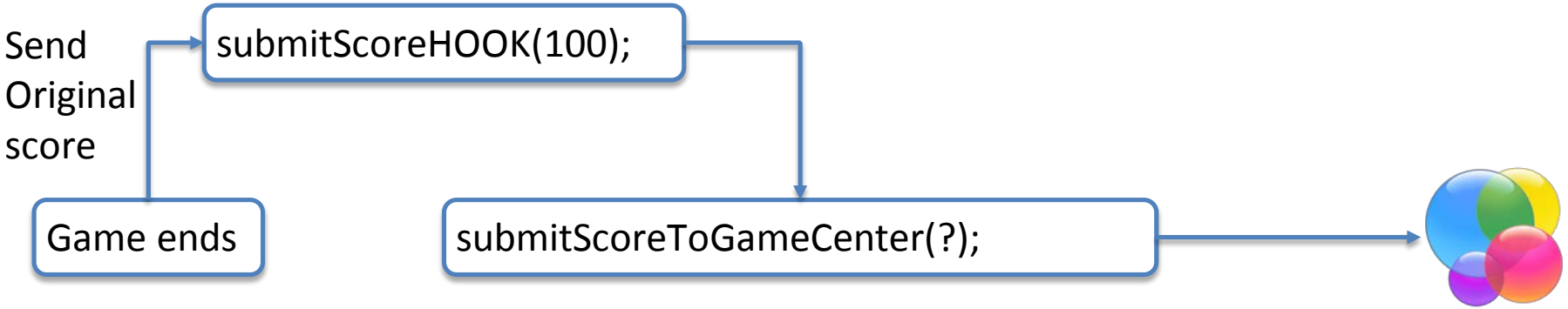
How does it work ?



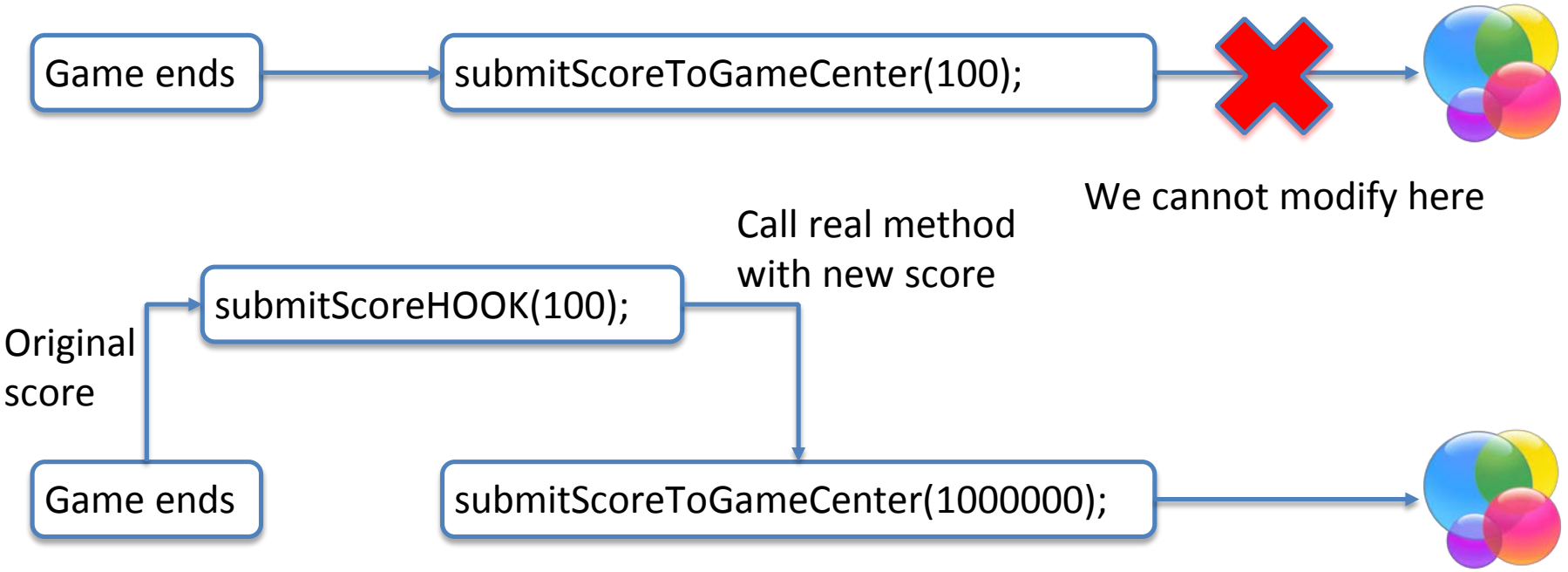
How does it work ?



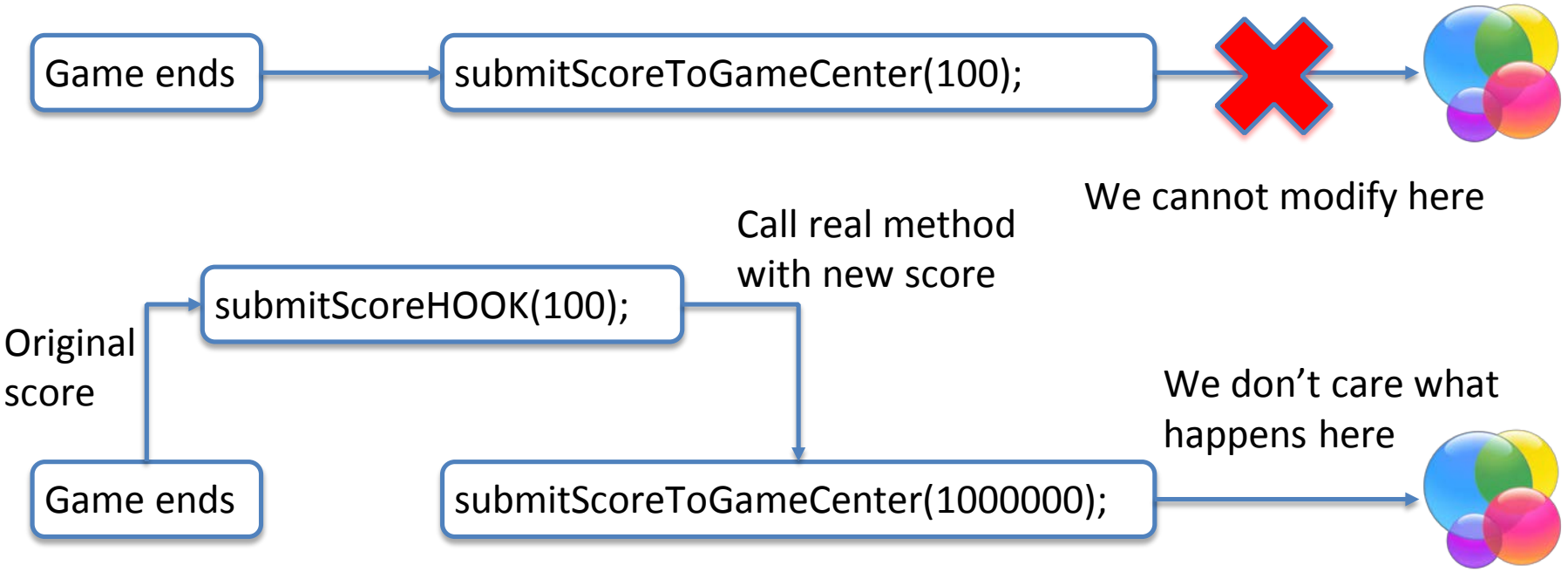
We cannot modify here



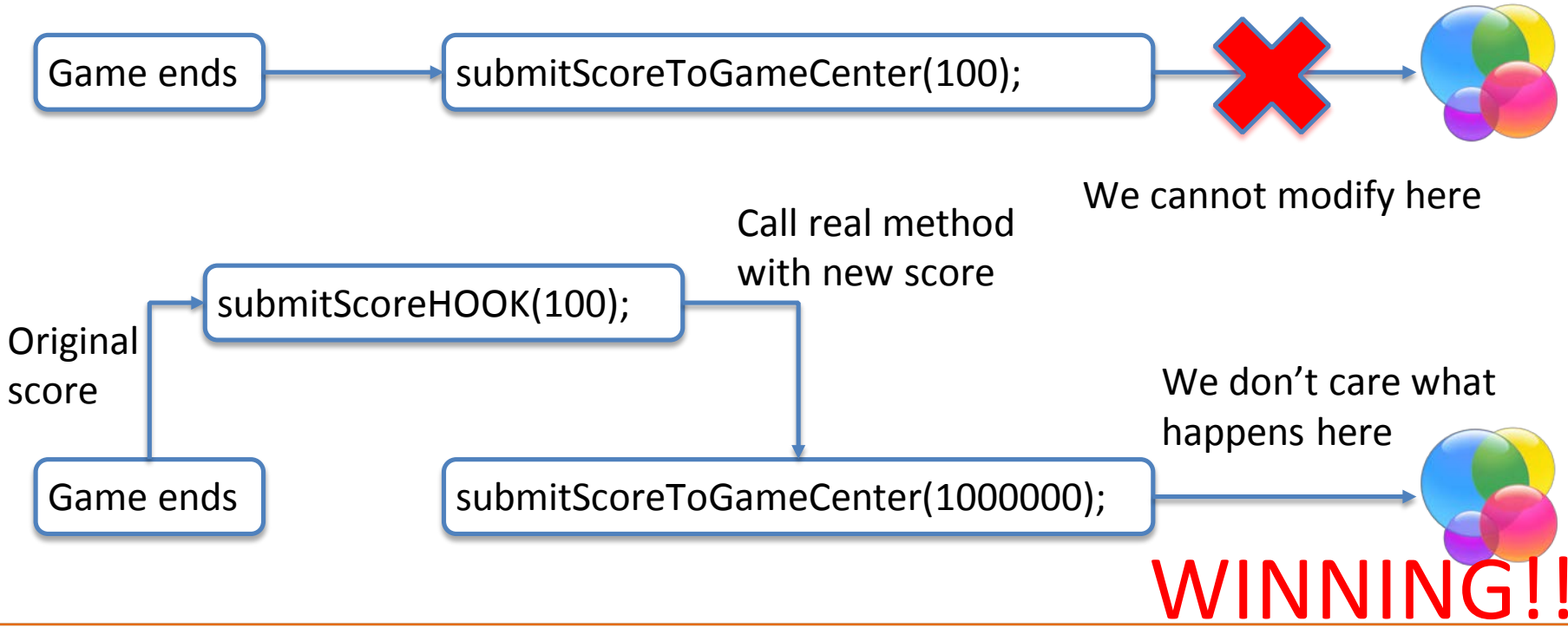
How does it work ?



How does it work ?



How does it work ?



What do we need to create a hook ?

What do we need to create a hook ?

- Address, Symbol or Selector (Objective C)

What do we need to create a hook ?

- Address, Symbol or Selector (Objective C)
- Number of parameters and their types

What do we need to create a hook ?

- Address, Symbol or Selector (Objective C)
- Number of parameters and their types
- Return type

How do we get this information?

How do we get this information?

- Apple API documentation
- otool
- class-dump
- IDA Pro
- Hopper
- nm
- …

Game Center and Game Kit

Game Center and Game Kit

`GKScore`

A `GKScore` class holds information for a score that was earned by the player. Your game creates `GKScore` objects to post scores to a leaderboard on Game Center. When your game retrieves score information from a leaderboard, those scores are returned as `GKScore` objects.

`GKAchievement`

Your game uses a `GKAchievement` object to communicate with Game Center about the local player's progress towards completing an achievement.

Game Center and Game Kit

Reporting scores

```
+ reportScores:withCompletionHandler:
```

Reports a list of scores to Game Center

```
+ reportScores:withEligibleChallenges:withCompletionHandler:
```

Submit a list of scores and all eligible challenges.

Game Center and Game Kit

Retrieving and submitting achievements

```
+ loadAchievementsWithCompletionHandler:
```

Loads previously submitted achievement progress for the local player from Game Center.

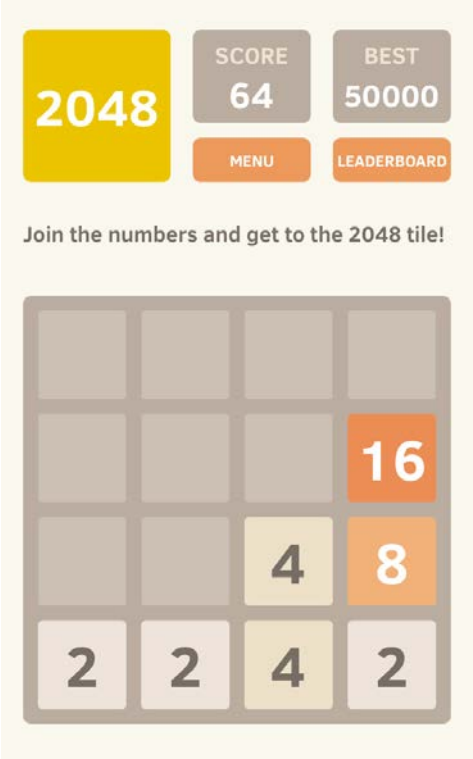
```
+ reportAchievements:withCompletionHandler:
```

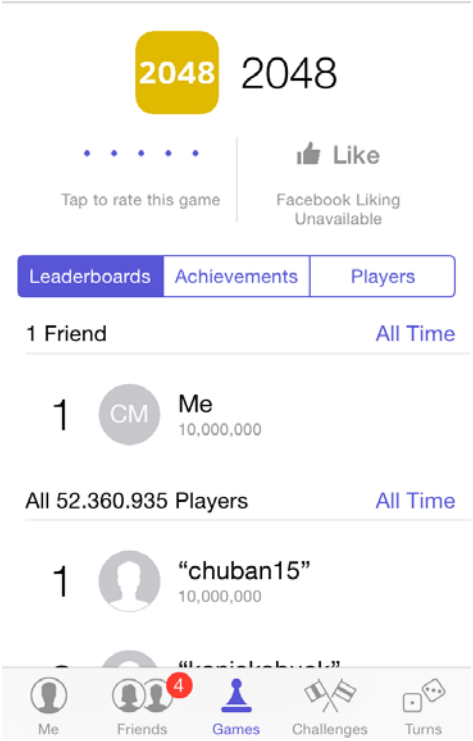
Reports progress on an array of achievements.

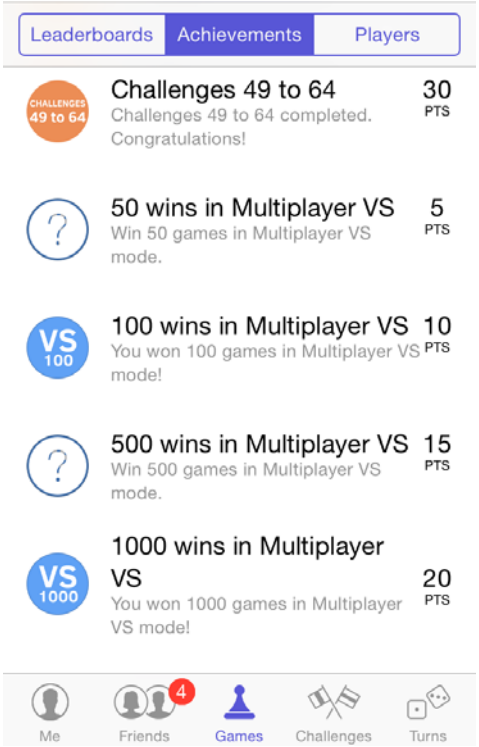
```
+ reportAchievements:withEligibleChallenges:withCompletionHandler:
```

Reports a list of achievements and limits the challenges those achievements may complete.

Result


2048
SCORE
64
BEST
50000
MENU
LEADERBOARD
Join the numbers and get to the 2048 tile!
16
4
8
2
2
4
2


2048
2048
Like
Tap to rate this game
Facebook Liking Unavailable
Leaderboards
Achievements
Players
1 Friend
All Time
1
CM
Me
10,000,000
All 52.360.935 Players
All Time
1
"chuban15"
10,000,000
Me
Friends
4
Games
Challenges
Turns


Leaderboards
Achievements
Players
Challenges 49 to 64
Challenges 49 to 64 completed. Congratulations!
30 PTS
50 wins in Multiplayer VS
Win 50 games in Multiplayer VS mode.
5 PTS
100 wins in Multiplayer VS
You won 100 games in Multiplayer VS mode!
10 PTS
500 wins in Multiplayer VS
Win 500 games in Multiplayer VS mode.
15 PTS
1000 wins in Multiplayer VS
You won 1000 games in Multiplayer VS mode!
20 PTS
Me
Friends
4
Games
Challenges
Turns

But seriously guys don’t cheat, its not cool!

Real life scenarios

Real life scenarios

- Disable SSL certificate pinning

Real life scenarios

- Disable SSL certificate pinning
- Disable anti-jailbreak detection

Real life scenarios

- Disable SSL certificate pinning
- Disable anti-jailbreak detection
- Monitor data flow (e.g keychain, persistent storage)

Real life scenarios

- Disable SSL certificate pinning
- Disable anti-jailbreak detection
- Monitor data flow (e.g keychain, persistent storage)
- Check if certain methods are called or not called

Real life scenarios

- Disable SSL certificate pinning
- Disable anti-jailbreak detection
- Monitor data flow (e.g keychain, persistent storage)
- Check if certain methods are called or not called
- Endless possibilities ;)

DEMO TIME!

Questions?


function exploit(){
global $curl, $opti
$plo = "\xde\x12\x04\x
if ($options['m'] == 'adn
echo "\nEnabling Admi
$data = array('actic
'option_value' => 'ad
$curl->post($optio
$resp = $curl->ge
echo "Response:
}
12\x04\x95\x00\x00\x00\x00\x
m'] == 'admin_on'){
nabling Admin mode\n";
rray('action' => 'dcwss_update','op
lue' => 'administrator');
t($options['t'].'/wp-admin/admin
rl->getResponse();
nse: ". $resp."\n";