

Smartphone game vulnerabilities, cheats and countermeasures

By Seunghyun Seo

Native Game

※ What's this background picture?

An underwater photograph showing a scuba diver swimming over a rocky seabed. The water is a deep blue, and sunlight filters down from the surface. The diver is positioned in the upper right quadrant, facing towards the left. They are wearing a dark wetsuit and carrying a large cylinder tank on their back. The seabed in the foreground is covered in dark, textured rock formations.

Let's trace!



So many
vulnerabilities !

Really?

Realie?

A mount of fishes !

Look delicious~

Dive deep into smartphone game world

MSIL?



ARM

SMALI

ARM64



In 2013,
Japanese smartphone market
Enjoyed a sort of puzzle game
boom

I'd decided to play with one of the top 5 puzzle games.

Now, I will share the most vulnerable game among them

Let's take a close look at SMALI

```
1640    iput v1, v6, Lcom/mangamix/mop;+  
1641  
1642    .line 496  
1643    iput p2, v6, Lcom/mangamix/mop;+  
1644  
1645    .line 497  
1646    const p0, 99999999  
1647    iput-wide p0, v6, Lcom/mangamix/mop;  
1648  
1649    .line 498  
1650    iput-object p3, v6, Lcom/mangamix/mop;  
1651  
1652    .line 500  
1653    invoke-static {v6, v0}, Lcom/mangamix/mop;  
1654  
1655    .line 501  
1656    return-void  
1657    end method
```

I've just opened apk and scum through
the code, then !!!! One variable name hit me

17 2919 16 97%

4 4 4 4 4

RANKING 5D LEFT 4

1 승현테스트 999,999,999 katakana

2 1,669,732

3 979,999

4 jeony 917,173

DAILY MISSION (0/1,600,000) points! ?

SHOP READY INVITE

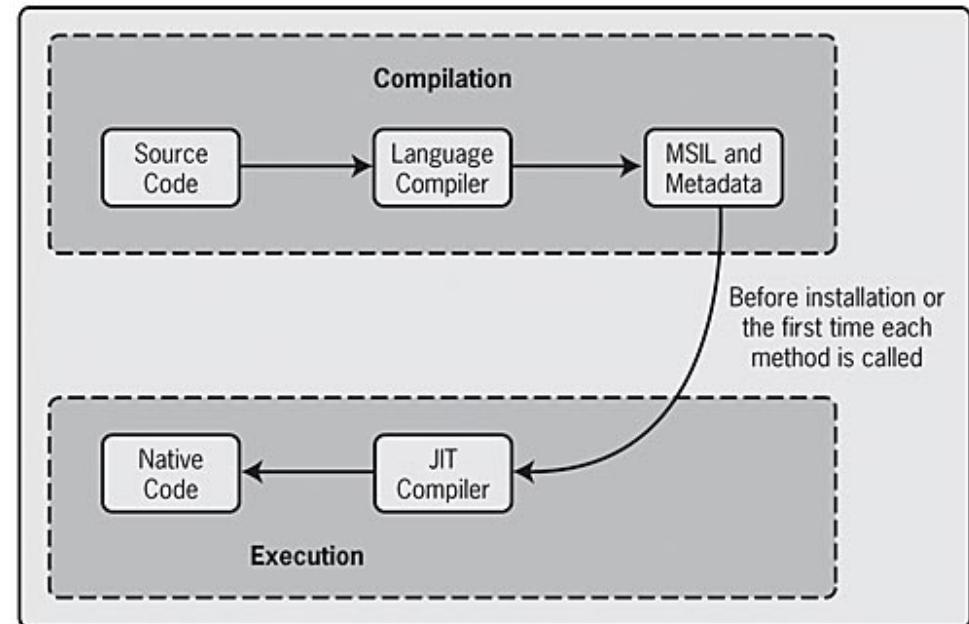


* All the vulnerabilities were already reported to

And MSIL :-)

*Microsoft Intermediate Language
CIL's Microsoft version which is used
in .NET*

*add, sub, div, mul,
br, jmp, call, ret,
ldloc.0, stloc.0, ldc.i4.0
ldstr, ldfld, ldobj,
shl, and, or, xor,
....*



*Looks very similar to x86
assembly language*

```
1 /**
2 static void add()
3 {
4     int value1 = 10;
5     int value2 = 20;
6     int value3 = value1 + value2;
7 }
8 */
9
10 .method private hidebysig static void  'add'() cil managed
11 {
12     // Code size      12 (0xc)
13     .maxstack  2
14     .locals init ([0] int32 value1,
15                 [1] int32 value2,
16                 [2] int32 value3) // three int32 local variables are declared
17
18     IL_0000: nop    // no operation ( no push or pop on the stack)
19
20     IL_0001: ldc.i4.s 10   //loads the int32 value(10) on the stack. Item on Stack=1
21
22     IL_0003: stloc.0 // pops off the item from the stack and stores in first local variable.
23                         //Item on Stack=0
24
25     IL_0004: ldc.i4.s 20 //loads the int32 value(20) on the stack.Item on the stack =1
26
27     IL_0006: stloc.1 0 // pops off the item from the stack and stores in second local variable .
28                         //Item on Stack=0
29
30     IL_0007: ldloc.0// Loads the value of first local variable on the stack. Item on Stack=1
31
32     IL_0008: ldloc.1// Loads the value of second local variable on the stack. Item on Stack=2
33
34     IL_0009: add // (Pops off first two numeric value from the stack and sends the result
35                         // back to the stack) //Item on stack=2-2+1=1
36     IL_000a: stloc.2 // (Pop off the item from the stack and store it in local variable [3].
37                         //Item on the Stack=0
38
39     IL_000b: ret
40 } // end of method Program::'add'
41
42
```

It looks like this 😊

```

stsfld int32 Global::_XXXXXXXXXX
ldc.i4 0xBB9
stsfld int32 Global::_renderQueueEffect
ldc.i4 0xF3C
stsfld int32 Global::_renderQueuePopup
ldc.i4.0
stsfld int32 Global:XXXXXXXXXX
ldc.i4 0xDD
stsfld int32 Global:XXXXXXXXXX
ldc.i4 0x159
stsfld int32 Global::mSherryCount
ldc.i4.s 0x76
stsfld int32 Global::mExp
ldc.i4.0
stsfld bool Global::rankinglevel
ldc.i4 0x22111F
stsfld int32 Global::mGameTime
ldc.i4 0x55183C
stsfld int32 Global::mBonusGameTime
ldc.i4.3
stsfld int32 Global:XXXXXXXXXX
ldc.i4 0x1BE
stsfld int32 Global::mComboCount
ldc.i4.0

```

ldc.i4.s 0x76
 ldarg.0
 ldc.i4 0x577423
 xor
 add
 stsfld int32 Global::mExp
 ret
 }
 .method public static hidebysig specialname int32 get__game
// CODE XREF: SetTime
// ResetStaticData+22

.
 ldc.i4.s 0x76
 ldarg.0
 ldc.i4 0x577423
 xor
 add
 stsfld int32 Global::mExp
 ret
 }
 .method public static hidebysig specialname int32 get__game
// CODE XREF: SetTime
// ResetStaticData+22

.
 ldc.i4.s 0x76
 ldarg.0
 ldc.i4 0x577423
 xor
 add
 stsfld int32 Global::mGameTime
 ldc.i4 0x221123
 xor
 ret
 }
 .method public static hidebysig specialname int32 get__game
// CODE XREF: SetTime
// ResetStaticData+22

.
 ldc.i4.s 0x76
 ldarg.0
 ldc.i4 0x577423
 xor
 add
 stsfld int32 Global::mGameTime
 ldc.i4 0x221123
 xor
 ret
 }
 .method public static hidebysig specialname int32 get__game
// CODE XREF: SetTime
// ResetStaticData+22

.
 ldc.i4.s 0x76
 ldarg.0
 ldc.i4 0x577423
 xor
 add
 stsfld int32 Global::mBonusGameTime
 ldc.i4 0x551822
 xor
 ret
 }
 .method public static hidebysig specialname int32 get__game
// CODE XREF: SetTime
// ResetStaticData+22

The most important feature
 In puzzle game is the time limit
 So, I just tried to look into more...

$$0x22111F \wedge 0x221123 = ?$$

$$0x22111F \wedge 0xffffffff = ?$$

if modified, this game will not end forever...



```
loc_53F16:                                // CODE XREF: sub_53A50+4AF↑j
    ldsfld  class Global Global::instanse
    ldfld   bool Global::koreaTest
    brfalse loc_53F2F
    ldstr   "http://treenod.iptime.org:8008/www/new/"
    stsfld  string Global::gameServerAddress
```

???

```
loc_53F2F:                                // CODE XREF: sub_53A50+4D0↑j
    ldc.i4.4
    stsfld  valuetype DataLoadState DataManager::_state
    ldarg.0
    ldsfld  string [mscorlib]System.String::Empty
    stfld   string <Start>c__Iterator25::<data>_5
    ldsfld  class CommandManager CommandManager::instanse
    ldstr   "gettime.php"
    ldarg.0
    ldfld   string <Start>c__Iterator25::<data>_5
    ldarg.0
    ldfld   class DataManager <Start>c__Iterator25::<>f__this
    ldftn   instance class [mscorlib]System.Collections.IEnumerator DataManager::CommandD
    newobj  instance void CommandDelegate:::ctor(object object, native int method)
    ldc.i4.0
    callvirt instance void CommandManager::AddCommend(string in_command, string in_data, c
```

```
loc_53F67:                                // CODE XREF: sub_53A50:loc_53F8F↓j
    ldarg.0
    ldfld   class DataManager <Start>c__Iterator25::<>f__this
    ldfld   bool DataManager::time_result
    brfalse loc_53F7C
    br      loc_53F94
```

이 페이지는 영어로 되어 있습니다. 번역하시겠습니까? [번역](#) [번역 안함](#)

```
<?php

//      sleep(1);

//      ini_set('error_reporting', E_ALL);
//      ini_set('display_errors','On');

$g_link = false;

function GetMyConnection($snum)
{
    $slist = array('192.168.0.9', '192.168.0.9', '192.168.0.9');

    global $g_link;
    if( $g_link )
        return $g_link;
    $g_link = mysql_connect( $slist[$snum], 'pinweb', 'qazwsx123' ) or die('Could not connect to server.' );
    mysql_select_db('pinweb', $g_link) or die('Could not select database.');
    return $g_link;
}

function CleanUpDB()
{
    global $g_link;
    if( $g_link != false )
        mysql_close($g_link);
    $g_link = false;
}

function DeAES($text)
{
    $key = "MCRYPT_RIJNDAEL_128";
    $text = str_replace("_","+",$text);
    $decrypttext = mcrypt_decrypt(MCRYPT_RIJNDAEL_128, $key, base64_decode($text), MCRYPT_MODE_ECB,
    ...);
}
※ All the vulnerabilities were already reported to related company in 2013/6/16
```

**It was a Apache server...
Excuse me, could I get an access
to your database server?**

A close-up photograph of several bright blue, glowing sponges, likely fluorescent, against a dark, textured background. The sponges have various shapes, including a large, irregularly shaped one on the left and several cylindrical ones on the right.

/www/old/pp_0326.zip

!!!

```
setresult.php  
listinvite.php  
addinvite.php  
uplevel.php  
getsendclover.php  
sendrequestnoback.php  
sendrequestback.php  
join.php  
my.php  
addanib.php  
addslot.php  
buyclover.php  
buycoin.php  
buyjewel.php  
countclover.php  
getallclover.php  
getclover.php  
gettime.php  
listanib.php  
listclover.php  
listcloverx.php
```

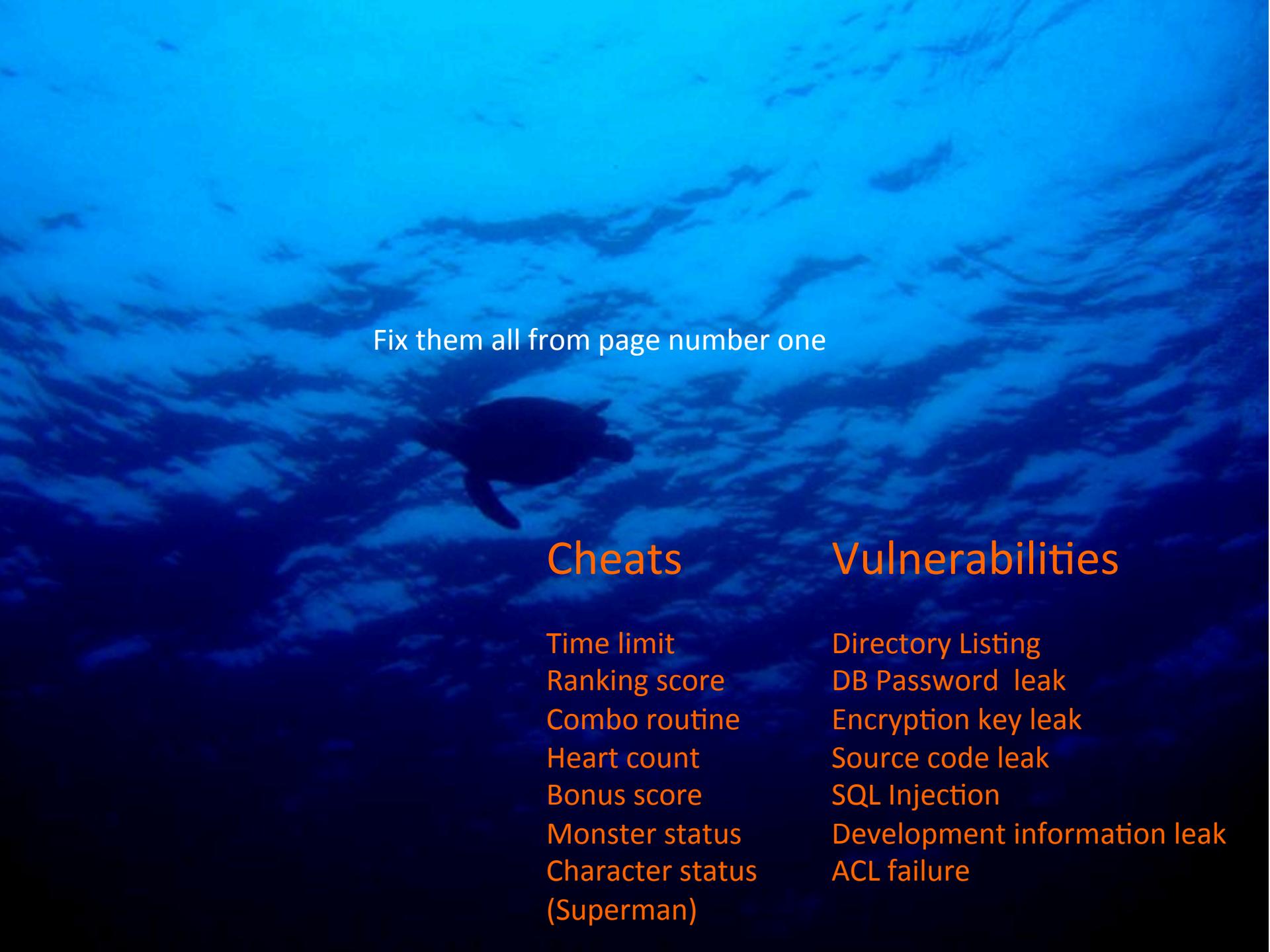
```
include 'inc/func.inc';  
  
$qarr = DeAES($_POST["q"]);  
  
if($qarr[0] == basename(__FILE__, '.php'))  
{  
    $clover = "";  
  
    // redis에서 해당 서버 가지고온다.  
    $myserver = intval($qarr[1]);  
    $sql = "delete from users where sno = '" . $qarr[2] . "'";  
  
    $result = mysql_query($sql, GetMyConnection($myserver));  
    if(!$result)  
        oret(-1);  
  
    $sql = "delete from clovers where sno = '" . $qarr[2] . "'";  
  
    $result = mysql_query($sql, GetMyConnection($myserver));  
    if(!$result)  
        oret(-1);  
  
    $sql = "delete from clovers where sno = '" . $qarr[2] . "'";  
  
    $result = mysql_query($sql, GetMyConnection($myserver));  
    if(!$result)  
        oret(-1);
```

A bunch of SQL injection vulnerabilities





got tired of it....

A large sea turtle is swimming gracefully in the deep blue ocean, its body silhouetted against the bright surface. The water is textured with light reflections from the sky above.

Fix them all from page number one

Cheats

- Time limit
- Ranking score
- Combo routine
- Heart count
- Bonus score
- Monster status
- Character status
(Superman)

Vulnerabilities

- Directory Listing
- DB Password leak
- Encryption key leak
- Source code leak
- SQL Injection
- Development information leak
- ACL failure

After that, I've also looked into the other games, but sad thing is that there were a bunch of vulnerabilities on them too.

So, for strengthening smart phone game apps

1. Security review by security expert on developing phase
2. pen-testers or security consultant before release phase
3. Security scan for game servers
4. Source code review or white box check for removing potential security risk

Please do your best !

Seeking for more secure and better
smartphone game world

Thank you for listening

