Hacking High Scores in iOS GameCenter

written by Karl Fosaaen | March 18, 2013

I recently wrote a blog post about cracking email hashes from the iOS GameCenter application. During my research on the issue, I noticed that there were a number of games where users had insanely high scores. Lots of the users also had the exact same score (9,223,372,036,844,775,807) for each of the games that they played. Coincidentally this number is the largest possible signed integer value that you can have. It turns out that getting these high scores isn't that hard to do.

Setup

In order to modify our scores, we will need to proxy our iOS traffic through Burp. In order to properly intercept the encrypted iOS traffic, you will also need to install the Portswigger certificate on your iOS device At this point, you will want your Burp listener to be on the same wireless network as your iOS device. You also need to have your Burp listener set to listen on all interfaces to allow your iOS device to proxy through it. The iOS proxy settings are fairly easy to set up. Just enter your Wi-Fi settings, tap on the blue and white arrow-in-a-circle (to the right of your SSID), and scroll down to your HTTP Proxy settings. Set the server IP to your Burp listener and set your port to the Burp listener port. Visit an https website on your iOS device to see if the Portswigger certificate is properly installed. If you don't have any issues (or SSL warnings), you should be ready to go.

Modifying Scores

Once your iOS device is properly proxying traffic through your Burp listener, you will want to generate a score to post to GameCenter. For most games, this is not very hard to do. We

will be using “Cut the Rope”as our example. Open up the first level, set Burp to intercept traffic, and complete the level (you cut one rope, it’s really easy). At this point you will see the “Level Complete” screen on your iOS device and the following request will come through Burp.

```
POST    /WebObjects/GKGameStatsService.woa/wa/submitScores
HTTP/1.1
Host: service.gc.apple.com
User-Agent:  gamed/4.10.17.1.6.13.5.2.1  (iPhone4,1;  6.1.2;
10B146; GameKit-781.18)
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Accept: */*
Some-Cookies: have been removed to make this shorter
Content-Type: application/x-apple-plist
Connection: keep-alive
Proxy-Connection: keep-alive
x-gk-bundle-version: 2.1
Content-Length: 473
x-gk-bundle-id: com.chillingo.cuttherope

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE  plist  PUBLIC  "-//Apple//DTD  PLIST  1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>scores</key>
    <array>
        <dict>
            <key>category</key>
            <string>1432673794</string>
            <key>context</key>
            <integer>0</integer>
            <key>score-value</key>
            <integer>12345</integer>
            <key>timestamp</key>
            <integer>1361998342937</integer>
        </dict>
    </array>
</dict>
```

</plist>

If you are seeing other requests come through, just forward them and keep your eye out for the request for the “submitScores” page. Before forwarding the score on to Apple, you will want to modify the score. The highest possible value that you can submit is 9,223,372,036,844,775,807. Replace the “score-value” stored in the tags (bolded in the example) with 9223372036844775807 and forward the request. You should receive a “status 0” response from Apple and your score will be updated in GameCenter.

Conclusion

I don’t intend on modifying my high scores for each of my GameCenter games. I really don’t care that much about the scores, but some people do. Given Apple’s current model for GameCenter leaderboards, this may not be an easy fix. At a minimum, Apple may want to do some checking on these high

scores to weed out any of the users that are maxing out their top scores. For now, I’m going to put the iPhone down and get some work done.