Cracking password protected Apple iWork files

Dhirendra Kholia (kholia@kth.se), Maxime Hulliger (hulliger@kth.se)

December 10, 2015

1 Abstract

Password auditing of password hashes, and password protected files is a process to find out weak passwords. It is a popular, and useful exercise because it helps in improving security, and simply because it is fun. Apple iWork [1] is a proprietary inexpensive office suite to create documents, presentations, and financial worksheets. However, an open-source or even a free software to crack password protected Apple iWork files did not exist previously, until now. The only alternate is the proprietary, commercial software called ElcomSoft Distributed Password Recovery (EDPR) [8], and it costs 600€ for a limited distributed version. Such proprietary, and closed-source services / software do not contribute to research, and general progress.

Besides solving the problem at hand, we believe that our work is a positive step in the process of rehabilitating reverse engineering [7] as a legitimate, and essential field of study. The best part of this project is that we will get to see the open-source community using, building upon, and improving our work in the near future.

2 Report

We started our work by trying to understand the underlying file format used by Apple the iWork suite. We used a combination of IDA Pro, LLDB (running under OS X 10.11.1), and WinHex for static, and dynamic analysis of Apple Keynote binaries [10]. After a while, we stumbled upon the "iWorkFileFormat" project[12], and it had already reverse engineered the file format used by Apple's iWork '13 suite. Later on, we were able to extend the project to work with Apple iWork '09 files [4], which are quite different, by reverse engineering EDPR itself (reversing of already reverse engineered projects is awesome fun).

Once we had figured out the underlying KDF (key derivation function) function, and the encryption cipher, we wrote a plug-in for John the Ripper (JtR) [2] software to crack password protected Apple iWork files. This plug-in has now been accepted, and merged into the John the Ripper repository itself [5].

Apple iWork '13 uses PBKDF2-HMAC-SHA1 [9] with 100000 iterations, and as such the cracking speed on CPUs is pretty low. To counter this problem, we decided to use GPUs to do the password cracking. Our OpenCL enabled plug-in has also been merged upstream [6]. The following sections show some benchmarking numbers for our JtR plug-ins.

2.1 Performance on Intel i5-6500 CPU @ 3.2 GHz)

```
[dhiru@ultra]$ ../run/john --format=iwork --test
Will run 4 OpenMP threads
Benchmarking: iwork, Apple iWork '09 / '13... [PBKDF2-SHA1... AVX2 8x]
Speed for cost 1 (iteration count) of 100000
Raw: 966 c/s real, 242 c/s virtual
```

2.2 Performance on nVIDIA GeForce TITAN X:

```
[dhiru@super]$ ../run/john --format=iwork-opencl --test --dev=6
Will run 32 OpenMP threads
Device 6: GeForce GTX TITAN X
Benchmarking: iwork-opencl, Apple iWork... '13 [PBKDF2-SHA1 OpenCL AES]
Speed for cost 1 (iteration count) of 100000
Raw: 21186 c/s real, 19980 c/s virtual
```

By using a single NVIDIA GPU, we are able to gain a 21x speed-up over the CPU version. This "super" host machine is a part of Solar Designer's HPC Village program, which provides Open Source software developers with access to a heterogeneous (hybrid) HPC platform [3] for free.

3 Summary

This was a fun project. Let's reverse engineer more proprietary software! [11]

References

[1] Apple iWork. https://en.wikipedia.org/wiki/IWork, 2015.

[2] DESIGNER, S. John the Ripper password cracker. http://www.openwall.com/john/, 1996.

[3] DESIGNER, S. Openwall's HPC Village. http://openwall.info/wiki/HPC/Village, 2015.

[4] DHIRU KHOLIA, M. H. JtR format for iWork '09 files. https://github.com/magnumripper/JohnTheRipper/pull/1899, 2015.

[5] DHIRU KHOLIA, M. H. JtR format for iWork '13 files. https://github.com/magnumripper/JohnTheRipper/pull/1896, 2015.

[6] DHIRU KHOLIA, M. H. JtR format for iWork files. https://github.com/magnumripper/JohnTheRipper/pull/1902, 2015.

[7] DOLAN-GAVITT, BRENDAN F AND HODOSH, JOSH AND HULIN, PATRICK AND LEEK, TIM AND WHELAN, RYAN. Repeatable Reverse Engineering for the Greater Good with PANDA.

[8] ELCOMSOFT. ElcomSoft Distributed Password Recovery (EDPR). http://www.elcomsoft.com/edpr.html, 2015.

[9] KALISKI, B. PKCS# 5: Password-based cryptography specification version 2.0.

[10] KHOLIA, D. Apple iWork reversing notes. https://github.com/kholia/iWork/blob/master/notes.txt, 2015.

[11] KHOLIA, D. JtR new formats wishlist. https://github.com/magnumripper/JohnTheRipper/issues/359, 2015.

[12] O'BRIEN, S. P. Unofficial documentation for the iWork '13 file format. https://github.com/obriensp/iWorkFileFormat, 2015.