pCTF2011 Challenge 34 write-up

April 2011 © Daniel Kachakil @ int3pids

Summary

This document describes a solution to the challenge 34 ("**We play cards – 300 pts**") of the first edition of the Plaid CTF, organized by the team Plaid Parliament of Pwning (PPP) held on April 22-24th, 2011.

Official description of the challenge

Category: *crypto*

Groups of 2 are the best.

Decrypt: **VFXFMFHJGHQXLIABIFNOHQEMYZKNXVCEBIDSJTFNRCLVSVUFNLWR**.

There was also a MP4 video file attached in which we can see somebody playing cards alone:

Analysis of the data

It's a crypto challenge, we have a deck, an encrypted message and someone playing Solitaire. Do we really need something else to solve it? Ok, a paper and a pen can help us ;-)

The only thing to assume at this point is that we're trying to solve a Solitaire Cipher challenge (a well-known cipher designed by Bruce Schneier) and we have all the data we need!

After reading carefully the original description of this algorithm, we see that the numbering suggested by the author is the bridge order of suites: from ace to king (1 to 13) and sorted by clubs, diamonds, hearts and spades (in this particular order). There are also two different jokers that must be tagged the same way: we will call "A" (or 53) the joker with a small painting and "B" (or 54) the bigger one (that's it, the one on the left in the video).

Now we can assume that the deck used to cipher the message was the initial deck, or maybe the final one (because the order is different), so we have to take a chance. If we assume the first option, the order of the cards will be:

> *King of diamonds, joker B, joker A, 5d, Jc, Jd, 6s, 10c, 5h, 4s, Qc, …*

And the numbering matching these cards will be:

> *26,54,53,18,11,24,45,10,31,43,12,25,44,48,7,30,33,2,23,22,38,42,20,5,1,50,49,27,9,32, 17,37,29,40,6,4,21,14,8,35,46,16,41,34,15,3,28,51,19,47,36,13,39,52*

Getting the solution

Once we have the data in a manageable way, we have to use it as an input to the algorithm. After spending some time trying to do it with Cryptool, I finally gave up and then looked for an implementation of the Solitaire Cipher algorithm, so I could manipulate it the way I wanted.

I chose this class in C#, but you can find it in different languages on the same web page of the author. The only remaining thing to do is to initialize the algorithm directly with our cards' sequence, so let's take the source code and modify the class constructor as follows:

```
public Solitaire() {
    _deck = new Int32[54] {26,53,54,18,11,24,45,10,31,43,12,25,44,
                           48,7,30,33,2,23,22,38,42,20,5,1,50,49,27,9,
                           32,17,37,29,40,6,4,21,14,8,35,46,16,41,34,
                           15,3,28,51,19,47,36,13,39,52};

    String solution =
    Decrypt("VFXFMFHJGHQXLIABIFNOHQEMYZKNXVCEBIDSJTFNRCLVSVUFNLWR");
}
```

The variable *solution* will hold the flag after run it. Not so difficult after all, right? ;-)

Flag of the challenge

WHYDODINOSAURSSORTCARDSANDLOSEATSORTINGWHEREISTHEFUN

Acknowledgments

Thanks to the **PPP** team for this awesome CTF! Almost every single challenge was very original and funny the whole CTF was one of the best I've ever played. We're waiting for the next one!

And of course, thanks to all my **int3pids** teammates, because they're also really awesome!

Regards,

Daniel Kachakil
dani@kachakil.com