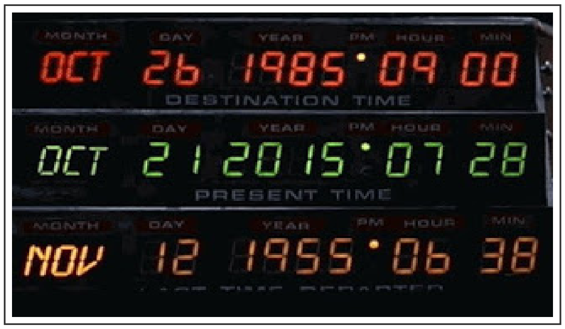
PENTESTER.ES (EN)

INFORMATION SYSTEMS SECURITY

WEDNESDAY, 21 OCTOBER 2015

NTP MitM Attack using a Delorean

Around one and a half year ago, I started a research about how computers synchronize their internal clocks, and how this could be used in order to attack well-known protocols and services running in Operating Systems. As a result, I have presented my findings in several security conferences such as BlackHat Europe 2014, RootedCON 2015 (Spanish), DEF CON 23 and Navaja Negra / ConectaCON 2015 (Spanish).



Today, October 21th 2015, it's the date when Marty McFly went to the future in the second part of the amazing Back to the Future saga, so I can't think in a better date to start releasing all the details about this research.

[1] NTP MitM Attack using a Delorean
[2] Mac OS X Time Synchronization
[3] Fedora / Ubuntu Time Synchronization
[4] Microsoft Time Synchronization
[5] Attacking HTTP Strict Transport Security
[6] Attacking the Public Key Infrastructure
[7] Other Attacks
[8] Helper tools

As we will see in the upcoming posts, all the OS vendors that I have tested use the Network Time Protocol (NTP) in order to keep their internal clock accurate, which is very important for some authentication protocols and other stuff. Most of them don't deploy this service in a secure way, making it vulnerable to Man-in-the-Middle attacks.

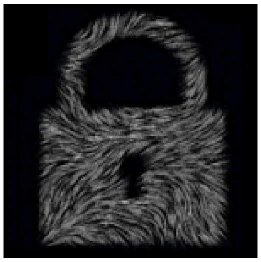
In order to exploit this issue, I developed a tool called **DELOREAN**. Delorean is an NTP server written in python, open source and available from GitHub (contributions are welcomed). I borrowed a few lines of code from kimifly's ntpserver and, of course, all the credits to him have been included.

What makes Delorean different and useful for us is that we can configure its flags in order to make it work in a different way than a regular NTP server. Basically, we can configure it in order to send fake responses, similar to the Metasploit's fakedns module.

```
$ ./delorean.py -h
Usage: delorean.py [options]

Options:
-h, --help show this help message and exit
-i INTERFACE, --interface=INTERFACE Listening interface
```

TRANSLATE IT!



ARCHIVE
▶ 2016 (3)
▼ 2015 (9)
▶ November (2)
▼ October (4)
Microsoft Time Synchronization
Fedora / Ubuntu Time Synchronization
Mac OS X Time Synchronization
NTP MitM Attack using a Delorean
▶ September (1)
▶ February (2)
▶ 2014 (1)

TWITTER JOSESELVI

-p PORT, --port=PORT Listening port
-n, --nobanner Not show Delorean banner
-s STEP, --force-step=STEP Force the time step: 3m (minutes), 4d (days), 1M (month)
-d DATE, --force-date=DATE Force the date: YYYY-MM-DD hh:mm[:ss]
-x, --random-date Use random date each time

We have the typical interface (-i) and port (-p) flags, that help us to bind the service exactly where we want. The -n flag only hides the super-cool Delorean banner :)

```
                                     _'_
                                _.-="_-         _
                           _.-="   _-          | ||"""""""---._______    __..
              ___.===""""-._______-,,,,,,,,,,,`_''____" """""       """""  __'
       __.--""    __          ,'                   o \            __        [__|
  __-""=======.--""  ""--.=================================.--""  ""--.=======:
 ]       [w] : /        \ : |========================|    : /        \ :  [w] :
 V___________:|          |: |========================|    :|          |:   _-"
  V__________: \        / :_|=======================/_____: \        / :__-"
  -----------'  ""____""  `-------------------------------'  ""____""
```

We can use Delorean in several modes, but we are going to focus in the most useful ones. There are some other attacks that weren't really interesting after developing them, but they are still in the code. Perhaps I will remove them in the future, sine they require scapy and some dependencies.

Since it's too soon yet to talk about how OS synchronize, we will test how Delorean works using the command line tool "ntpdate":

```
$ ntpdate -q 192.168.1.2
server 192.168.1.2, stratum 2, offset 97372804.086845, delay 0.02699
20 Oct 06:05:45 ntpdate[881]: step time server 192.168.1.2 offset 97372804.086845 sec
```

By default (no flags), Delorean responses a date that matches the same week and month day than the current date, but at least 1000 days in the future. This was useful for the HSTS bypass as we will see in upcoming posts.

```
# ./delorean.py -n
[19:44:42] Sent to 192.168.10.113:123 - Going to the future! 2018-08-31 19:44
[19:45:18] Sent to 192.168.10.113:123 - Going to the future! 2018-08-31 19:45
```

We can set a relative jump from the current date using the step flag (-s). Relative jumps can be defined as 10d (ten days in the future), -2y (two years in the past), etc:

```
# ./delorean.py -s 10d -n
[19:46:09] Sent to 192.168.10.113:123 - Going to the future! 2015-08-10 19:46
[19:47:19] Sent to 192.168.10.113:123 - Going to the future! 2015-08-10 19:47
```

We can also set a specific date, and Delorean would answer always the same date:

```
# ./delorean.py -d ‘2020-08-01 21:15’ -n
[19:49:50] Sent to 127.0.0.1:48473 - Going to the future! 2020-08-01 21:15
[19:50:10] Sent to 127.0.0.1:52406 - Going to the future! 2020-08-01 21:15
```

There are an additional attack called "Skimming Attack" that is useful only on certain configurations, but we will go in depth with it when we will talk about Microsoft synchronization, despite it could be useful in other platforms.

POSTED BY JOSE SELVI AT 08:00
TAGS: DELOREAN , MITM , NTP , TOOLS

NO COMMENTS :

Tweets by @JoseSelvi

Jose Selvi
@JoseSelvi

@vierito5 Mucho ánimo amigo...

16 Mar

Jose Selvi Retweeted

XSS Payloads
@XssPayloads

XSS Polyglot, a single vector that fits most of the injection contexts. That's a nice one! bit.ly/227D80v @0xSobky

0xsobky/HackVault
HackVault - A container...
github.com

11 Mar

Jose Selvi Retweeted

Alvaro Muñoz
@pwntester

[Paper] The perils of Java deserialization
community.hpe.com/t5/Security-Re...

10 Mar

Embed View on Twitter

SEARCH PENTESTER.ES

Search

FOLLOW BY EMAIL

Email address... Submit

SUSCRIBIRSE A

Posts

Post a Comment

Newer Post Home Older Post