Thread: [Vulnerability] WPA2 cracking dictionary for TP-Link Routers

03-19-2013, 11:22 AM #1

AlexAltea

Just burned their ISO

Join Date: Mar 2013
Posts: 1

[Vulnerability] WPA2 cracking dictionary for TP-Link Routers

I am not sure if this is the best section to post this thread, but I think this issue can be interesting for some people.
If the topic doesn't fit this section, feel free to move it elsewhere. : P

Details:
This issue affects most of TP-Link routers (their ESSID is usually TP-LINK_XXXXXX), and has nothing to do with the firmware. The problem is the key generation in the EasySetupAssistant. Using WPA2, the assistant generates random passwords of length 10, with 32 possible characters (2-9; A-Z without 'I' or 'O'). If someone tried to break this password with a speed 20.000 keys/sec. (this speed can be easily achieved with a desktop computer and GPU acceleration), he would need 32^{10} / 20000 = **1785.1 years** to break it. So the system is apparently secure. The problem is that the assistant is using a linear congruential generator with seeds of 32 bits to generate the characters of the key. That is, there are 2^{32} possible keys in the key set. Here is the code (Python) of the generator:

Code:

```
chars = "2345678923456789ABCDEFGH
JKLMNPQRSTUVWXYZ"
def gen(seed, length): #length=10
 for WPA/WPA2, length=13 for WEP
    key = ""
    for i in range(length):
      seed = (seed)*0x343FD + 0x2
69EC3
```

Hmmm, not exactly... **The seeds are NOT random**.
The seed is obtained by transforming the 64-bit output of KERNEL32.GetSystemTimeAsFileTime into a 32-bit unsigned integer, which is in practice just a number that increases on 1 each second based on the UTC time at the moment of generating the key. Here is the code in Python of that function:

Code:

```
import datetime

def genSeed(t1):
    dt = t1 - datetime.datetime(1
601, 1, 1, 0, 0, 0)
    t = dt.days*86400 + dt.second
s*100 + dt.microseconds*10

    tA = (t/2**32 + 0xFE624E21)
    tB = (t%2**32 + 0x2AC18000) %
 (1<<32)

    if tA >= (1<<32):
      tA += 1
      tA %= 1<<32

    r = (tA % 0x989680) * (2**32)
```

```
    r = ((r + tB) / 0x989680) % (
2**31)
```

Since we can predict the values of the seeds between two dates, we can reduce the cases from 2^31 to the seconds elapsed between two dates. Let me explain, suppose we know one AP was installed during 2012, regardless of the month, day, etc... Thanks to this method we know we have to check only the keys corresponding to seeds that lie between 0x4EFFA3AD and 0x50E22700. That is:

Code:

```
print genSeed(datetime.datetime(2
012, 1, 1, 0, 0, 0)) #0x4EFFA3AD
print genSeed(datetime.datetime(2
```

There are around 365*24*60*60 = 31536000 seconds in a year (which is more or less 0x50E22700 - 0x4EFFA3AD). Therefore, we have only to check 31536000 keys. That is really easy: **we can do it in 26 minutes with GPU acceleration or in 5 hours using only the CPU**. Notice that regarding the computing time, this would be the worst case possible. If some attacker knew that a router was recently installed, he could break the password in **a few minutes or even seconds**!

Vulnerable TP-Link Routers: (Any wireless router made by TP-Link since 2010, I guess)

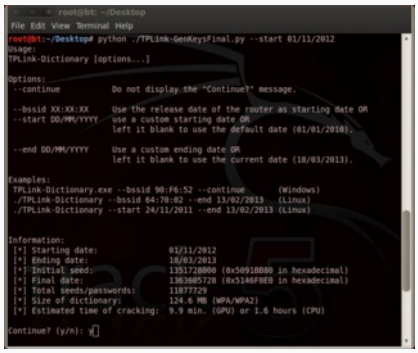
TL-W8151N (V1, V3)
TL-WA730RE (V1, V2)*
TL-WA830RE (V1, V2)*
TL-WDR3500
TL-WDR3600
TL-WDR4300
TL-WR720N
TL-WR740N (V1, V2, V3, V4)
TL-WR741ND (V1, V2, V3,V4)*
TL-WR841N (V1,V5, V7, V8)*
TL-WR841ND (V3, V5, V7, V8)*
TL-WR842ND
TL-WR940N (V1, V2)
TL-WR941ND (V2, V3, V4, V5)
TL-WR1043N
TL-WR1043ND
TD-VG3511 (V1)*
TD-VG3631
TD-W8901N
TD-W8950ND
TD-W8951NB (V3,V4, V5)*
TD-W8951ND (V1, V3, V4, V5)
TD-W8960N (V1, V3, V4)
TD-W8961NB (V1, V2, V3)*
TD-W8961ND
TD-W8968
TD-W8970
TD-W340G
TD-W300KIT
TD-W8101G
TD-W8960N
TL-WR2543ND

**Possibly vulnerable. I could not download the assistant to verify it.*

Download tool:
http://www.mediafire.com/?gor6b9b63nu6020
Here is the program to generate dictionaries for cracking these routers. It has been tested by other people, and we managed to crack the WPA2 password of 3 TP-Link APs. Of course these tests were made with our **own routers**. Tell me what you think about this program, feel free to post your "success stories", and report any bugs you found, please.

I have included versions for Windows and Linux as well as the source code of the program. Run the program **TPLink-GenKeysFinal** and follow the instructions. At the moment it is useless to specify the BSSID since I haven't focused on the list of release dates yet. My suggestion is to use the default arguments until we got the complete list of release dates for each router. If you know certainly the model of the AP, then pass the release date of the router to the program in the format *--start DD/MM/YYYY*.

I have also included some utilities I made to test this vulnerability. If you are interested about the details of this issue, you should take a look at them and read all I wrote on my blog about this [ES]. I don't really want to rewrite everything in English since I guess many of you are not really interested in reading all this information, but I hope Google Translator can make this a bit more understandable.



« Previous Thread | Next Thread »

Similar Threads

Cracking WPA/WPA2 without dictionary By strakar in forum BackTrack 5 Beginners Section	Replies: 7 Last Post: 03-26-2013, 11:20 AM
wpa2 dictionary By xshit in forum OLD New bie Area	Replies: 1 Last Post: 04-06-2010, 03:51 PM
The only thing that confuses me about WPA/WPA2 cracking is the dictionary By emran2626 in forum OLD New bie Area	Replies: 7 Last Post: 01-08-2010, 02:13 AM
D-link routers with captcha... authentication partially broken By Jac01 in forum OLD General IT Discussion	Replies: 0 Last Post: 05-20-2009, 05:12 AM
D-Link DIR-45x routers By law sanx in forum OLD Wireless	Replies: 0 Last Post: 12-28-2008, 02:26 PM

Posting Permissions

You may not post new threads	**BB code** is On
You may not post replies	**Smilies** are On
You may not post attachments	**[IMG]** code is On
You may not edit your posts	**[VIDEO]** code is On
	HTML code is Off
	Forum Rules