JULY 26, 2015

Cracking the Roku V2 WPA2-PSK

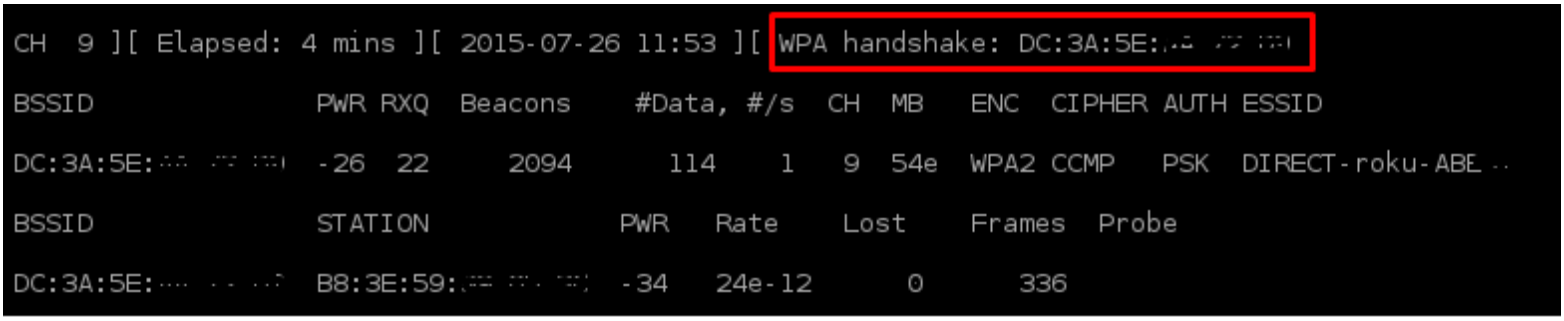
So my weekend ended up being a Roku vulnerability assessment project.

Starting with remotely sending API requests to navigate through Roku menu's from a bash shell to issue a reboot or factory-reset, adding channels, etc.. (http://x42.obscurechannel.com/2015/07/25/restart-a-roku-via-bash/) to ultimately leading to cracking the WPA2-PSK key between the Roku "Wifi-Direct" remote control and the Roku base-station. My thought process was that if I can crack the WPA2-PSK, and connect to the Roku SSID, that this could be potentially exploited in a wardrive type of scenario leading to abusing others' internet connections (through their Roku's), depending on how they're set up. The ability to connect to a users' Roku SSID could also lead to compromise of the internal network the Roku is sitting on.

The first thing I looked into was the "remote pairing" function. I wondered whether the PSK was passed along during the pairing process. That *didn't* happen. No EAPOL's were transmitted during the "Remote pairing" phase.

What i did find, was that the EAPOL handshake occurred after a reboot of the Roku. Once the Roku unit is rebooted, the remote control passes the WPA2-PSK to the "base-station" for authentication. This is what allows communication between the remote and the Roku. The remote is the "station", and the Roku unit is the WAP. The remote and station setup up their own Wi-Fi network for communication. It looks like the process Roku uses for this connectivity between the remote and the "base-station", is "Wifi-Direct (https://en.wikipedia.org/wiki/Wi-Fi_Direct)", similar to a standard ad-hoc WiFi mode.

So, firing up airodump-ng caught the handshake pretty quickly (within 4 minutes) upon reboot of the unit:



First, i ran aircrack-ng with a password list I've compiled over time against the captured EAPOL's with no luck.

I also created a custom dictionary (Company name, Serial Number variations, Roku MAC Addresses, etc..), added it to my existing wordlist, and ran a crack using John The Ripper with the "rules" option enabled on a GPU-based password cracking machine with 4 GPU's in it. No luck there either.

2 comments

JULY 26, 2015 - 18:09

Bart

Did you try with the remote units' MAC-adress cloned?

★ (http://x42.obscurechannel.com/2015/07/26/cracking-the-roku-v2-wpa2-psk/?like_comment=125&_wpnonce=733eae26a0)
Like

JULY 28, 2015 - 11:17

(http://www.obscurechannel.com)

i did. no luck there.

★ (http://x42.obscurechannel.com/2015/07/26/cracking-the-roku-v2-wpa2-psk/?like_comment=143&_wpnonce=130d8e05f4)
Like

Restart a Roku via bash (http://x42.obscurechannel.com/2015/07/25/restart-a-roku-via-bash/)

MS15-034 SSL (Detecting http.sys vulnerable hosts on SSL-based services) (http://x42.obscurechannel.com/2015/08/09/ms15-034_ssl/)