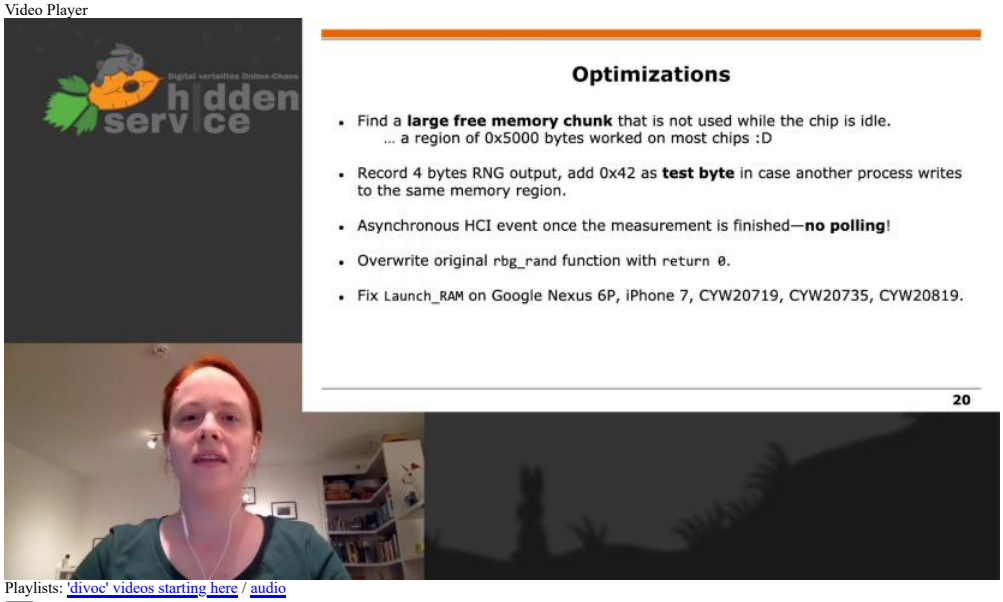
Finding Eastereggs in Broadcom's Bluetooth Random Number Generator

jiska

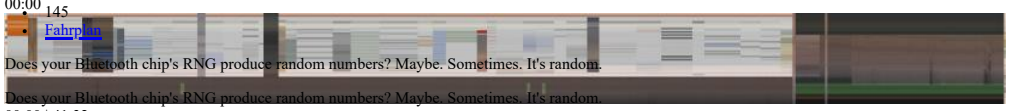
Video Player



Playlists: 'divoc' videos starting here / audio

15
30

- 41 min
- 2020-04-11
- 2021-03-14
- 145
- Fahrplan



Does your Bluetooth chip's RNG produce random numbers? Maybe. Sometimes. It's random.

Does your Bluetooth chip's RNG produce random numbers? Maybe. Sometimes. It's random.

00:00 | 41:32

The 90 day deadline for CVE-2020-6616 exactly passed during this Easterhegg \o/

1.00x

- 2.00x
- 1.50x
- 1.25x
- 1.00x

According to the Bluetooth specification, the chip is required to contain a proper RNG. This RNG is used for key generation within the chip, but also exposed to the operating system. This is a great feature for embedded devices, which otherwise might not have access to a good RNG.

When analyzing the source code of Broadcom's RNG, we found that it accesses a Hardware Random Number Generator (HRNG) but has a Pseudo Random Number Generator (PRNG) fallback.

The HRNG76 looked good at least at first sight, and since it is a black box coming out of some memory mapped hardware registers, it is hard to analyze. It is missing some properties like a warm-up, which means reading out a couple of values during initialization before using it. However, the hardware might also do this internally.

Way more interesting is the PRNG, analyzed by @matedealer. The PRNG takes a couple of values which are not random at all. The most random value is the chip's clock. In most contexts within the code that require randomness, the PRNG is called multiple times in a row, thus, the clock is basically constant except from the initial value. Similar issues apply to the other registers and values the PRNG takes as input. The PRNG code was changed multiple times over the years of firmware dumps that we have, such as an additional caching behavior, different input values, etc.—and dropped in the most recent version.

On one development board, we found that the RNG function might run into the PRNG when calling it multiple times in a row. However, this seems to be an issue within the RNG cache of that specific development board.

When reporting this issue to Broadcom with CVE-2020-6616 already assigned by MITRE, they claimed all their chips had a HRNG and there was no reason ever to use the PRNG. That code was just there but would never be used. However, this is not true, and at least one comparably recent chip of a popular smartphone released in 2017 is missing a HRNG. Ooops :)

So we might have something like the KNOB attack here with slightly less entropy reduction but present in the hardware…

Download

Video

- MP4
- WebM

Download 1080p
eng-deu-fra 227 MB
Download 576p
eng-deu-fra 141 MB
Download 1080p
eng-deu-fra 266 MB
Download 576p
eng-deu-fra 134 MB

These files contain multiple languages.

This Talk was translated into multiple languages. The files available for download contain all languages as separate audio-tracks. Most desktop video players allow you to choose between them.

Please look for "audio tracks" in your desktop video player.

Subtitles

Help us to subtitle this talk!

Audio

Download mp3
eng 38 MB
Download opus
eng 23 MB

Embed

```
<iframe width="1024"
height="576"
```

Share:

Tags

divoc20 6 2020
by Chaos Computer Club e.V — About — Apps — Imprint — Privacy — c3voc