wpa2slow Documentation

Release 0.4

Jarrett Rainier

November 18, 2016

Contents

wpa2slow is a full Python implementation of the WPA2 encryption algorithm, using no encryption libraries.

CHAPTER 1

Project goals

This project grew out of my FPGA implementation of WPA2, as a platform for regression testing and experimentation.

WPA2 requires three or four different algorithms to calculate a final password, depending on how you count them.

There is a fair amount of discussion on these functions in this category of my site.

The entire goal was to have intermediate steps of the algorithms to compare with the VHDL implementation. Perhaps this will be useful to someone else.

CHAPTER 2

Benchmarks

Hash speed of my general purpose computer; 2,000 keys / second

Hash speed of a Raspberry Pi 1: 45 keys / second

Hash speed of this project: 0.25 keys / second

CHAPTER 3

Sounds great! How can I get started?

See the Installation docs first for initial setup.

Usage docs give you a few examples, and references for more information.

For developers, or people looking to expand their brains, read about how WPA2 works in the Structure docs.

CHAPTER 4

Further reading

- Announcement post
- GitHub Page
- ReadTheDocs Page
- PyPi Page
- Usage in FPGA simulator regression testing (See `FPGA/tests` folder)
- hccap format specification format

CHAPTER 5

Contents:

5.1 Installation

For general usage, you should be able to use `pip install wpa2slow` and it will magically work.

Alternatively, clone this repo and install locally. This might be ideal if you intend to "get under the hood" and see how the data moves:

```
git clone https://github.com/JarrettR/WPA-Slowed-Down.git
cd WPA-Slowed-Down
pip install .
```

5.2 Using this library

Check out main.py for a few examples of the top level methods.

Additionally, this library is used in the regression tests for my VHDL implementation of WPA2 .

All of the intermediate methods(SHA1, HMAC, PBkDF2, and PRF) are available too, but undocumented at this time.

This module read and parse capture files in hccap format, outputting the required inputs. Standard capture formats may eventually be supported, but it's low priority, as the linked web converter is pretty good.

5.3 WPA2 Structure

Without getting too into the implementation details for the algorithms involves, here is a high level description of what happens when you are verifying a known password on captured WPA2 packet.