THE PERILS OF PRIORITIZING TIME TO MARKET OVER SECURE DEVELOPMENT LIFECYCLE

Adam Callis – adam@simpleorsecure.net

5/6/2018

DISCLAIMERS

- This presentation is an extension of previous research and disclosures by Dr. Andrew Zonenberg of IOActive and Mr. Michael Ossmann of Great Scott Gadgets
- This presentation and associated advisory have been shared with and confirmed by SimpliSafe's internal and external security teams.

ASSUMPTIONS

- Participants should have-
  - Basic understanding of Software Defined Radio – SDR
  - Basic understanding data transmission over radio frequency (RF) techniques
    - On-Off-Keying OOK
    - Amplitude Shift Keying ASK
    - Frequency Shift Keying FSK
  - Basic understanding of data modulation and encoding schemes
    - Pulse Interval Modulation
    - Pulse Width Modulation
    - Pulse Interval and Width Modulation

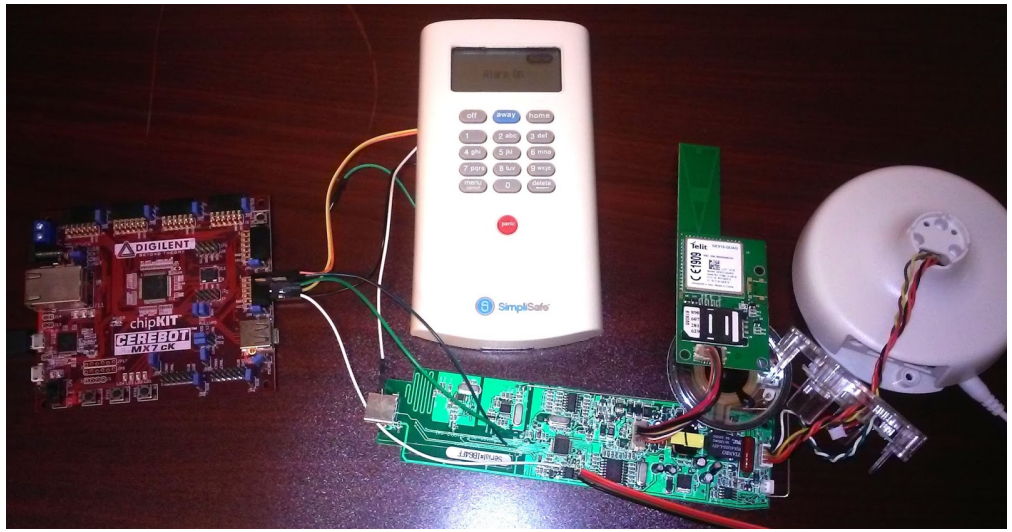
SESSION OBJECTIVES

- At the end of this session participants should be able to understand:
  - The basics of reverse engineering RF Signals
  - The hidden costs of failing to design in security from the start
  - The vulnerability findings of the SimpliSafe 2 DIY security system
  - How a bad actor could exploit the vulnerabilities discovered.

AGENDA

- Review of the original findings published by Dr. Andrew Zonenberg and Mr Michael Ossmann
- Summary of my findings published to SimpliSafe in March 2018
- Building a successful exploit
  - Learning SDR through manual reverse engineering
  - Building upon existing OpenSource projects to automate reverse engineering
- Retrospective Analysis
- A working demonstration

PREVIOUS WORK – DR. ANDREW ZONENBERG



(Zonenberg, 2016)

Component Checklist (Prices as of 5/6/18)

- SimpliSafe 2 Keypad: $69.99
- SimpliSafe 2 Basestation: $114.99
- MicroController: ~$50

Total Cost: $234.50

Complexity: Hard

Comments: Requires writing hundreds of lines of C code for microcontroller for decoding

- Dismantled and repurposed a SimpliSafe 2 Base Station and Keypad
- Leveraged existing test points and a micro controller to record and replay pin
- Attempted to report to SimpliSafe September 2015, October 2015
- Published advisory on 17-Feb-2016 located here - https://ioactive.com/wp-content/uploads/2018/05/IOActive_Advisory_SimpliSafe-Replay-1.pdf
- Interesting Blog explaining his journey located here - https://ioactive.com/remotely-disabling-a-wireless-burglar-alarm/

PREVIOUS WORK – MR. MICHAEL OSSMANN

(Ossmann, 2016)

Component Checklist (Prices as of 5/6/18)

- Yard Stick One: $124.95

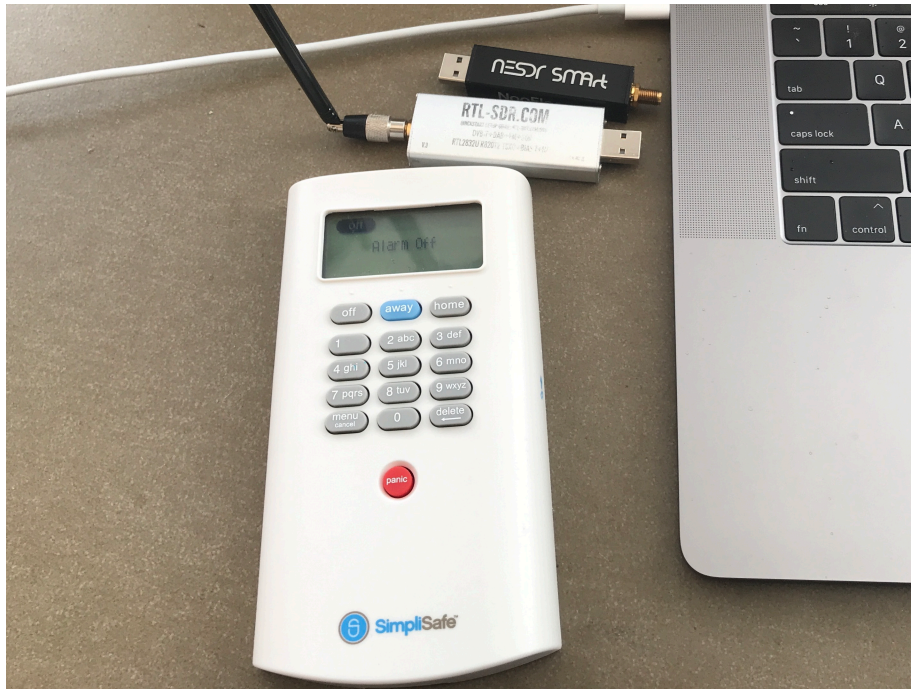
Total Cost: $124.95

Complexity: Medium

Comments: Requires working knowledge of rfcat and writing Python code to decode and replay data

- Leveraged Yard Stick One (https://greatscottgadgets.com/yardstickone/) with RFCat for capture and replay
- Reverse Engineered Signal and identified it as ASK encoded using Pulse Interval and Width Modulation (PiWM)
- Published his findings via the Great Scott Gadgets website on 20-Feb-2016 located here-
  - https://greatscottgadgets.com/2016/02-19-low-cost-simplisafe-attacks/

EVOLUTION OF RESEARCH



Component Checklist (Prices as of 5/6/18)

- RTL-SDR Dongle: $20.95 (Via Amazon)

Total Cost: $20.95

Complexity: Easy

Comments: Primarily a receive only attack, however a 433mhz transmitter could be added to a raspberry pi to handle replays. Requires you to install a patched copy of rtl_433 available on GitHub

- Previous research and a "Rapid Radio Reversing Guide" as a starting point
  - https://greatscottgadgets.com/2015/12-29-rapid-radio-reversing-toorcon-2015/)
- Manual reverse engineering using osmocom_fft / inspectrum to understand protocol
- Partnership with rtl_433 contributor Christian Zuckschwerdt to add PiWM detection in rtl_433 test branch accelerated protocol reverse engineering
- Built a decoder plugin for rtl_433 which decodes SimpliSafe sensor and keypad transmissions

SUMMARY OF ADVISORY REPORT SENT TO SIMPLISAFE 21-MARCH-2018

Finding Number	Finding Heading	Status
SS01	Unencrypted Keypad Transmissions	Confirmed by SS 4/24/18
SS02	Unencrypted Sensor Transmissions	Confirmed by SS 4/24/18
SS03	RF Interference Disables Alarm	Confirmed by SS 5/6/18
SS04	Base station fails to detect tamper attempt	Confirmed by SS 5/6/18

A full write up advisory report was provided to SimpliSafe on 21-March-2018. They have been exceptionally quick to respond and work through the findings with their internal security, external security support firm, and me as the researcher.

SS01 – UNENCRYPTED KEYPAD TRANSMISSIONS

SS01 – Unencrypted Keypad Transmissions – Confirmed by SimpliSafe 4/24/2018

The SimpliSafe keypad (U9K-KP1000) transmits data including PIN, Arm, Disarm, and test mode commands to the SimpliSafe base station (U9K-BS1000) leveraging the frequency of 433.92Mhz. These transmissions are completely unencrypted and can be captured leveraging a Software Defined Radio (SDR) from up to 200 feet away.

Leveraging a Software Defined Radio (SDR) USB Dongle and the popular RTL-SDR Software known as "rtl_433" with a custom module we were able to capture and decode in real time all messages sent to the base station including the most sensitive key data fields of

- KeyPad Serial Number
- Command (Arm, Disarm, Test Mode)
- Pin Code

With the standard omni-directional antenna that comes with the SDR Dongle the the keypad transmissions can be received from approximately 100 feet in free space (i.e. no walls, trees, or obstructions between keypad and antenna) and approximately 50-60 feet when transmissions must penetrate walls.

Leveraging a High Gain YAGI Directional Antenna reception distances became 200+ feet in free space and approximately 115 feet when transmissions must penetrate walls. Given the 433.92mhz falls within the HAM bands, antennas tuned to this frequency are relatively inexpensive and commercially available.

SS02 – UNENCRYPTED SENSOR TRANSMISSIONS

SS02 – Unencrypted Sensor Transmissions – Confirmed by SimpliSafe 4/24/2018

The SimpliSafe Entry Sensor (U9K-ES1000), KeyChain Remote (U9K-KR1), Motion Sensor (U9K-MS1000) and Water Detector (U9K-WT1000) have all been confirmed to leverage the the same 433.92Mhz frequency and encoding methods as the SimpliSafe Keypad (U9K-KP1000) described in SS01.

Leveraging a Software Defined Radio USB Dongle and the popular RTL-SDR Software known as "rtl_433" with a custom module we were able to capture and decode in real time all messages sent to the base station including the key data fields of

- Sensor Serial Number
- Command (Arm, Disarm, Panic) - KeyChain Remote
- Status (Active/Open, Inactive/Closed) – Sensors

Unlike the Keypad which appears to transmit quite a strong signal, the sensors appear to have a much weaker signal which limits reception to approximately 50-75% of the distance which a keypad could be received. It should be noted, sensors with new batteries appeared to have the furthest signal propagation while sensors with older batteries had the most limited distance.

SS03 – RF INTERFERENCE DISABLES ALARM

SS03 – RF Interference Disables Alarm – Unconfirmed by SimpliSafe as of 5/6/2018

The SimpliSafe system operates on the Unlicensed ISM Frequencies of 433.92Mhz (for transmissions to the Base Station), and 315Mhz (for base station to keypad status transmissions). The 433.92Mhz portion of the ISM band also falls within the Amateur (HAM) radio frequency allocation of the 70cm band. As a result HAM radio operators can and do legally transmit on these frequencies using much higher power (25-50 Watts) which while transmitting overruns the receiver of the base station making it impossible for it to hear the weaker signals of the sensors. In effect, rendering the alarm "Disabled".

While the RF Noise is not by itself a vulnerability, the fact that the base station does not report this noise to the monitoring center creates a scenario where an attacker could intentionally transmit noise on the receivers frequency making it impossible for it to hear the sensors, thereby able to bypassing the security without the monitoring center becoming aware of a possible attack.

SS04 – BASE STATION FAILS TO DETECT TAMPER ATTEMPT

SS04 – Base station fails to detect tamper attempt – Unconfirmed by SimpliSafe as of 5/6/2018

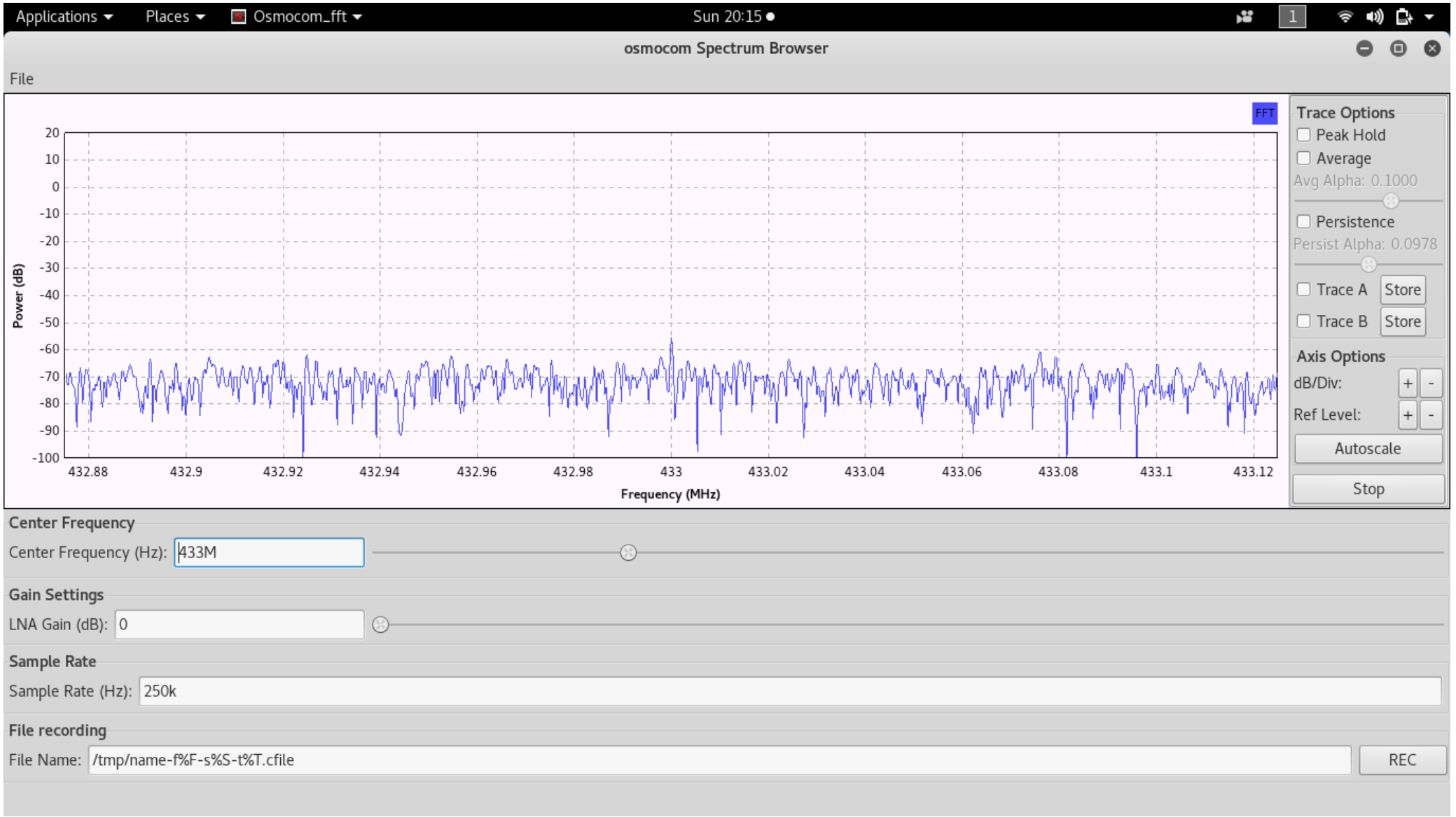
The SimpliSafe Base station (U9K-BS1000) provides the key gateway from the RF sensors to the monitoring center via a cellular connection. Breaking this units ability to relay messages from the sensors or keypad to the monitoring center effectively defeats the entire security system.

As has been demonstrated on YouTube by Jay Security the base station can be easily disabled within the typical 30 second timeout from sensor trip to transmission to monitoring center by removing the battery and external power from the system.

Furthermore there are no tilt sensors to detect the unit being turned over to remove the batteries.
This attack vector could be leveraged by itself or in combination with the RF Noise to allow an attacker to disable the simplisafe security monitoring.

MANUAL REVERSE ENGINEERING

Step 1: Record the transmission – Tool osmocom_fft

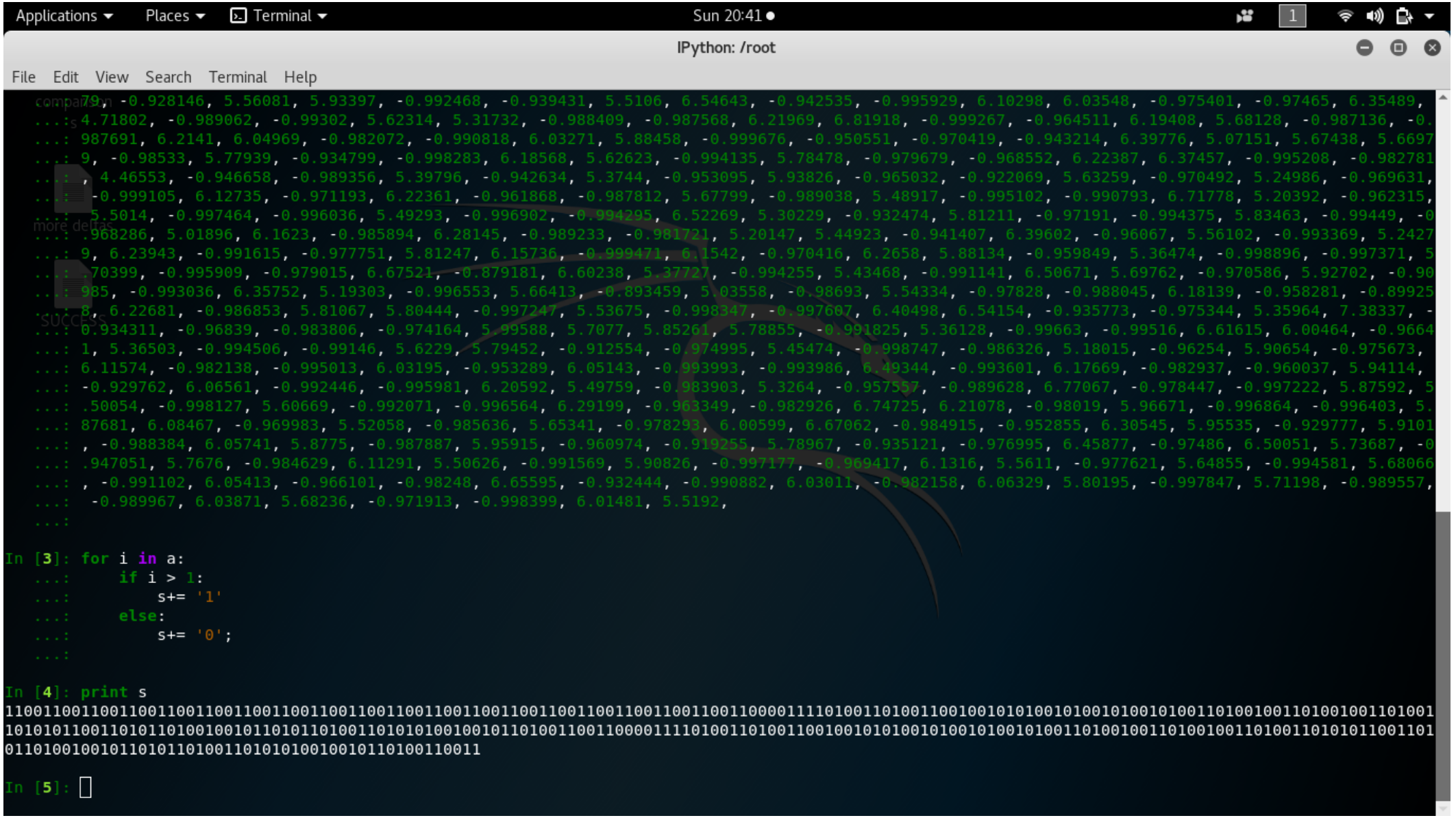


MANUAL REVERSE ENGINEERING

Step 2: Extract Symbols from recording – Tool Inspectrum

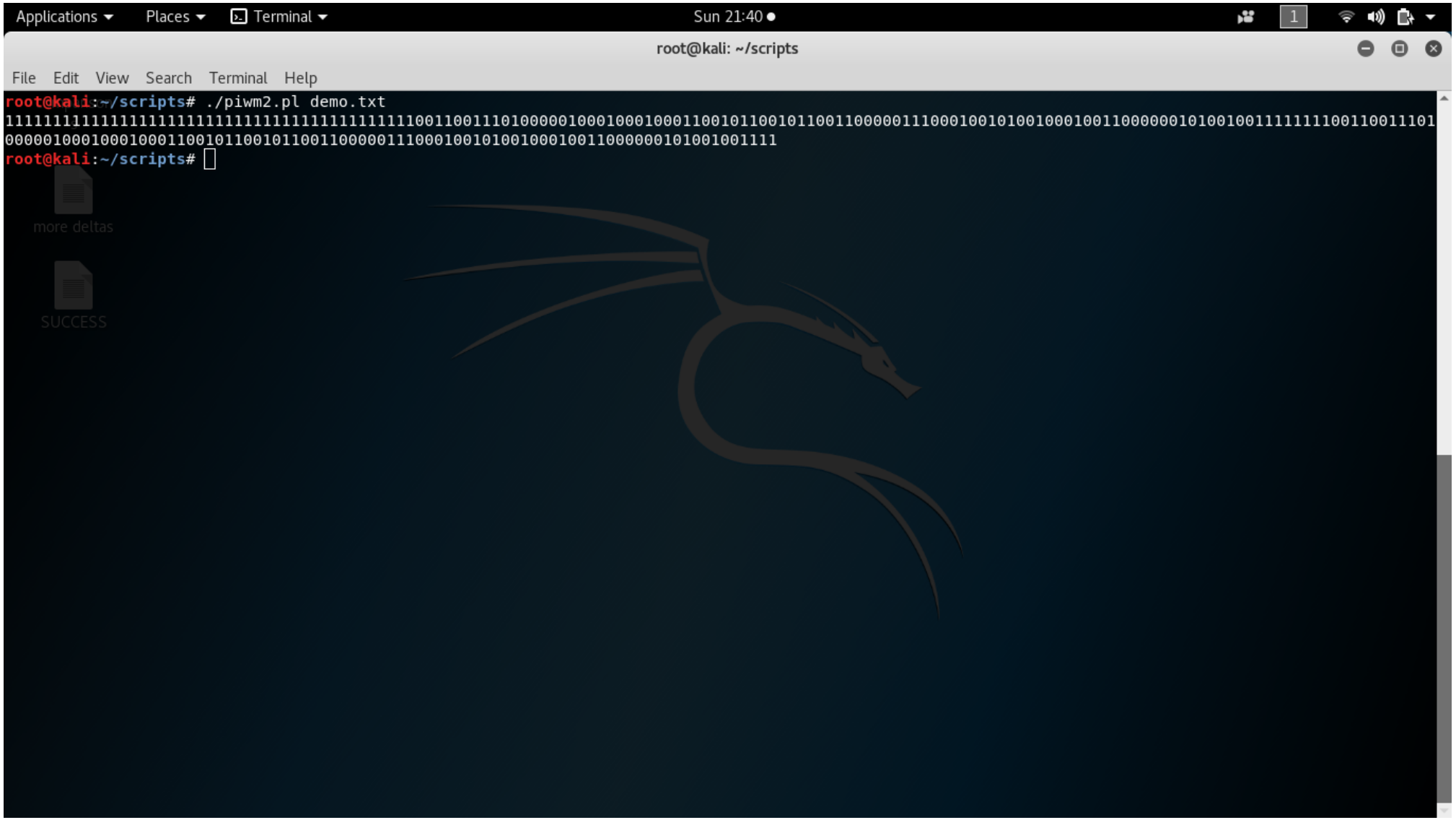
MANUAL REVERSE ENGINEERING

Step 3: Convert Symbols to 1's and 0's– Tool iPython



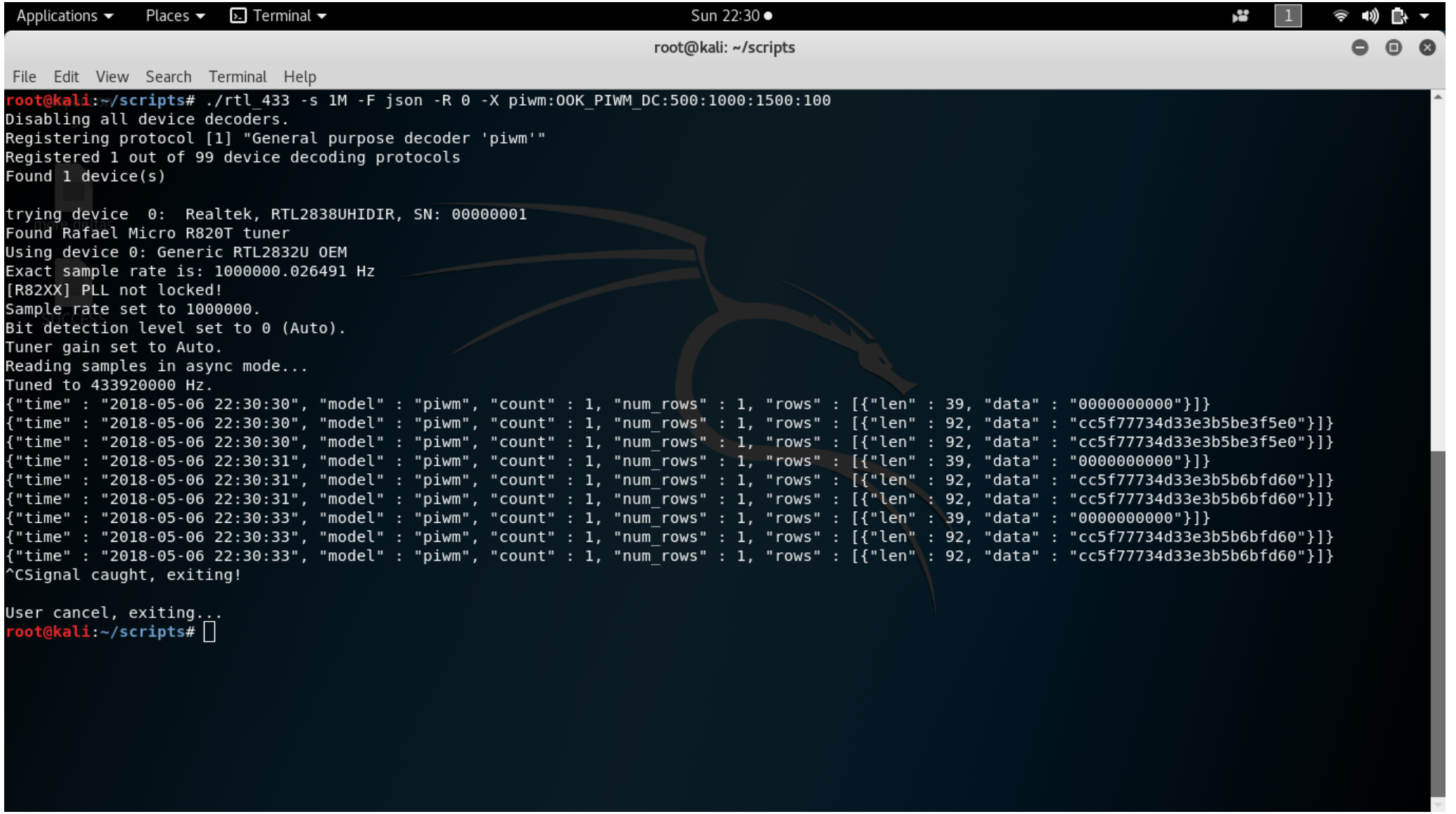
MANUAL REVERSE ENGINEERING

Step 4: Convert PiWM 1's and 0's to Data 1's and 0's – Tool Perl Script



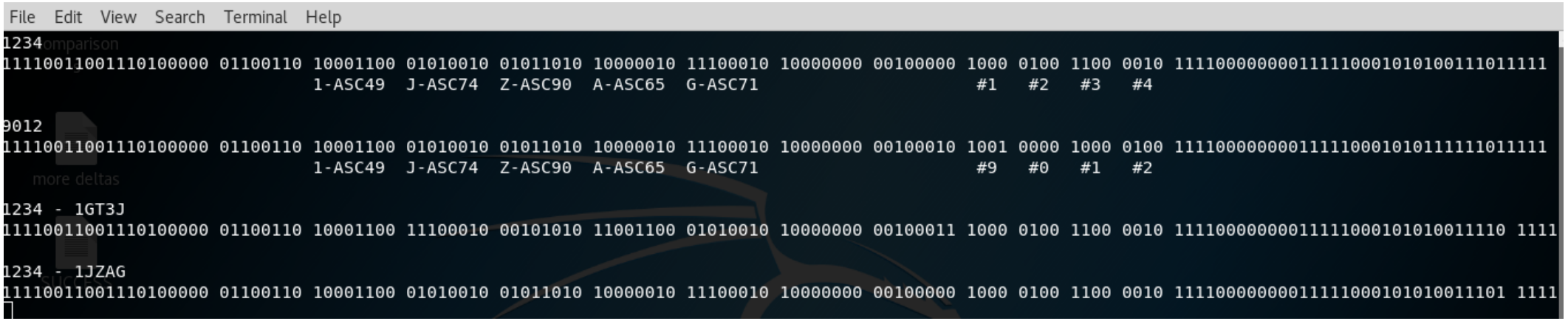
REVERSE ENGINEERING THE MORE AUTOMATED WAY

Leverage rtl_433 in test mode for captures



ANALYZING THE PROTOCOL

By comparing known entries (Different Pins/Same Keypad or Same Keypad/Different Pins)



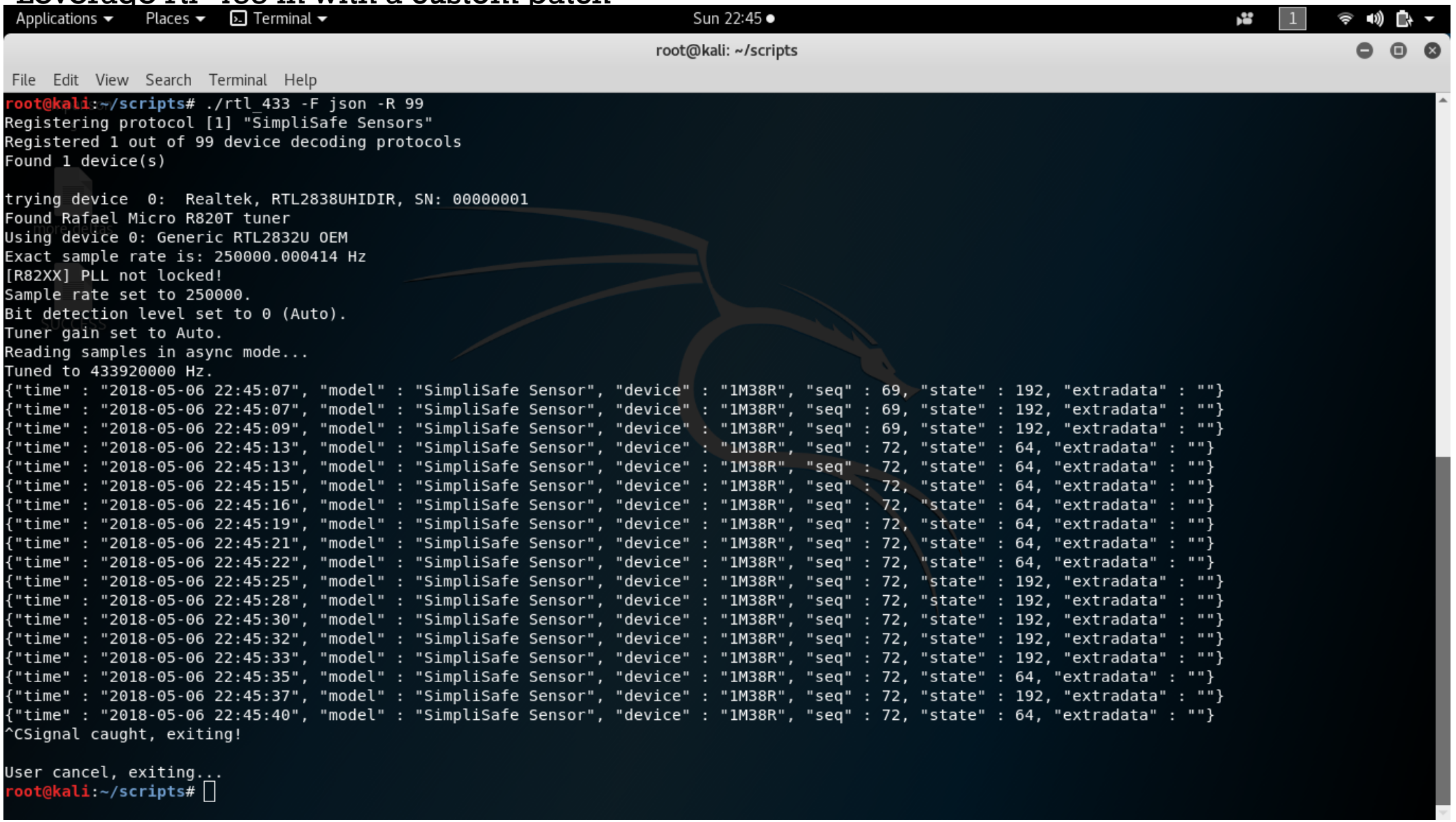
By comparing known entries I was able to determine what was changing between captures and further was able to determine where the serial number and the pin were in the messages.

The serial number is sent as the ASCII number for each character (regardless of letter or number) leverages a full 8 bits per character. The PIN Numbers were sent as a binary number leveraging 4 bits.

The most interesting component discovered was that the byte order was backwards of how I was expecting. For example, the number 49 I would expect to be 00110001, however in reality it was sent as 10001100.

WALA, NOW WE HAVE A SUCCESSFUL EXPLOIT!

Leverage rtl_433 in with a custom patch

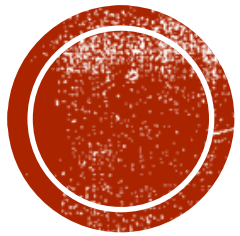


IMPACT ANALYSIS

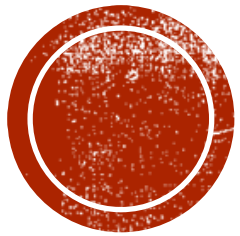
- Attackers can leverage a very cheap and easy to use solution to surveil your home security system status 24x7 without your awareness or knowledge.
- With minimal effort one can build a profile about the consumer which can help me infer
  - One or more of your favorite pin codes (Human nature suggests that you reuse pin codes)
  - Sleeping habits (I can assume you arm your alarm before bed, and disarm in the morning)
  - When the home is unoccupied (Software can determine if Alarm was armed in Home or Away Mode)
  - When there is motion within your home (assuming you have a motion sensor)
  - When a door or window has been left open
- System doesn't support over the air upgrades. Meaning it has to be replaced to resolve this issue.

RETROSPECTIVE

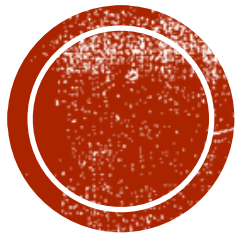
- They say hindsight is always 20/20, assuming that is true, we should leverage clear sight to learn from those mistakes.
- Design failures
  - RF Transmissions using obscure, but not secure encrypted communications left the system vulnerable to this attack.
  - Inability to upgrade software "over the air" requires consumers to replace hardware at a significant cost to resolve issue. (As of 5/6/18 there was no free or discounted upgrade for existing customers, however the vendor has committed to announcing an upgrade program in the coming months)
  - Minimal tamper controls built into system allowing an attacker to disable the system without the monitoring center or consumer ever knowing



LIVE DEMONSTRATION



QUESTIONS?



THANK YOU