Hacking Logitech Unifying

whoami

- D0zer AKA Decrazyo
- Work for Veritas Technologies
- Former software engineer
- Penetration tester / Exploit developer
- Offensive Security OSCP, OSCE, OSWE
- Keyboard enthusiast

Why?!

Good Enough

- ☑ Short key travel
- ☒ Wired (USB)
- ☒ Non-standard layout
- ☒ Membrane switches

Okay

- ☑ Standard layout
- ☒ Wired (PS2)
- ☒ Keys jam
- ☒ Membrane switches

Hot Garbage

- ☒ Non-standard layout
- ☒ Short range
- ☒ Connection issues
- ☒ Chiclet keys
- ☒ Membrane switches
- ☒ Wears socks with sandals
- ☒ Takes candy from babies

Goal

- Wireless
- TKL / 87-key / 80%
- Trackpoint
- Mechanical switches
- Standard layout

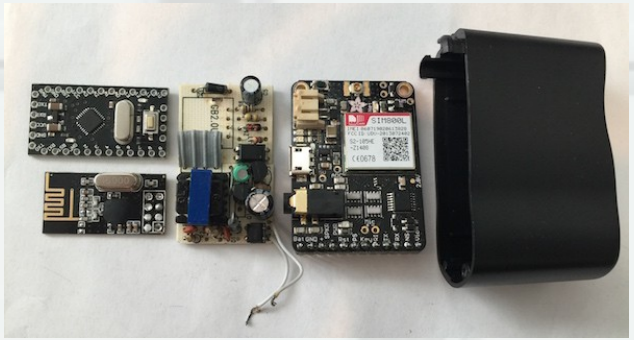
Logitech Unifying Features

- Purpose built
- AES Encrypted*
- 6 devices 1 receiver
- Host-independent pairing
- Long range
- Quick reconnect

*only keystrokes are encrypted

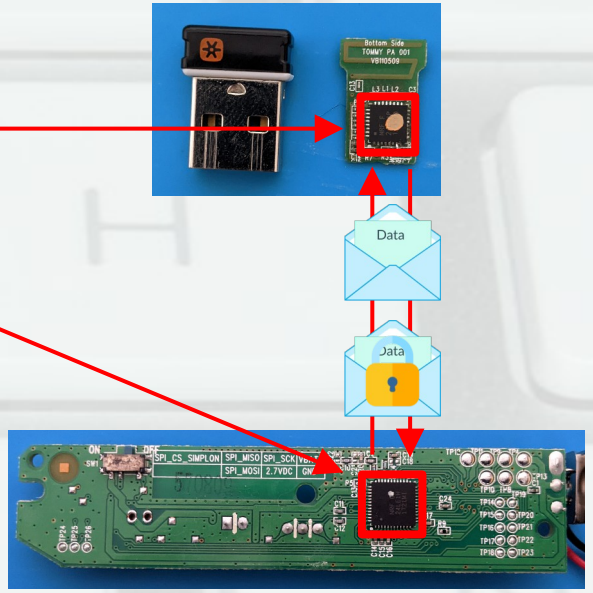
Prior Research

- Travis Goodspeed
  - nRF24 pseudo-promiscuous mode
- Samy Kamkar
  - KeySweeper
- Marc Newlin
  - MouseJack, KeyJack, KeySniffer
- Matthias Deeg and Gerhard Klostermeier
  - Of Mice and Keyboards



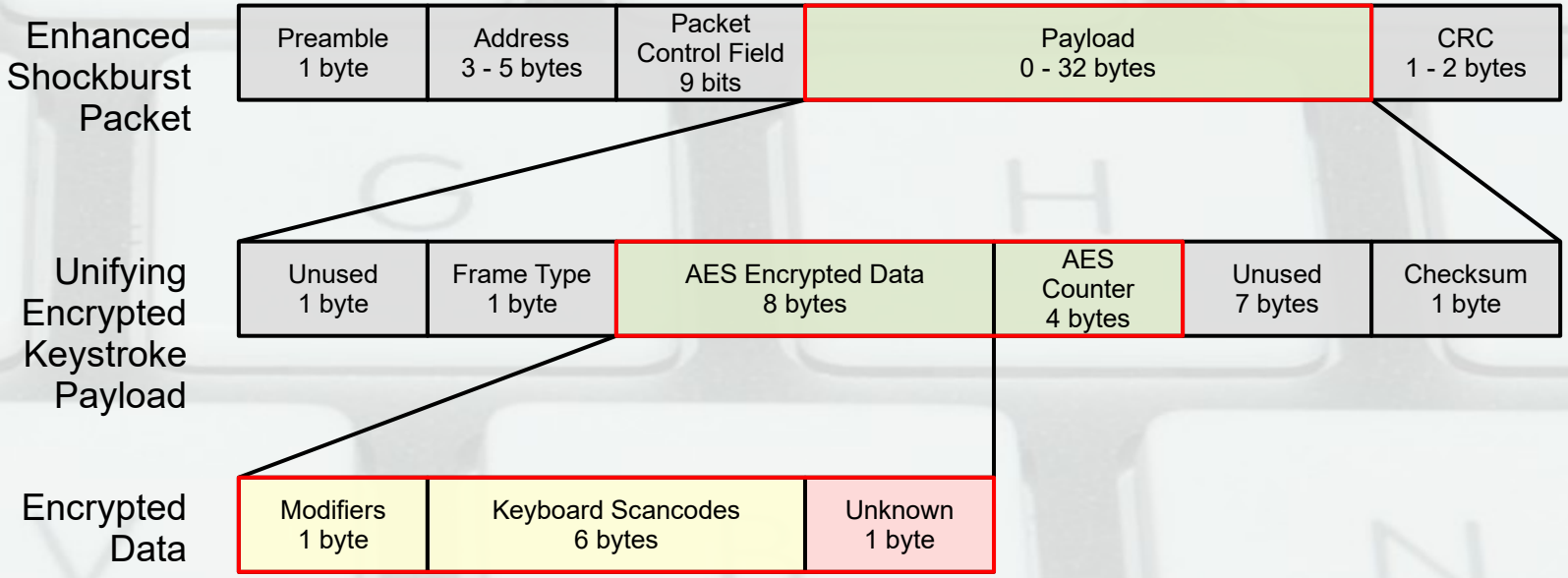
What We Know About Unifying

- Nordic Semiconductor hardware
  - Receivers: nRF24LU1
  - Devices: nRF24LE1
- Enhanced Shockburst protocol
  - Packet based data link layer
- Most Unifying payload data
- AES-128-CTR encryption



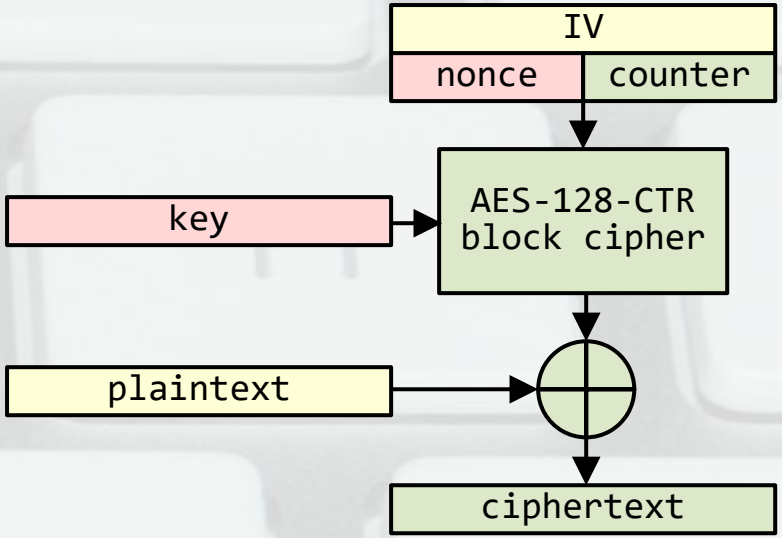
K400r Keyboard PCB

Payload Structure



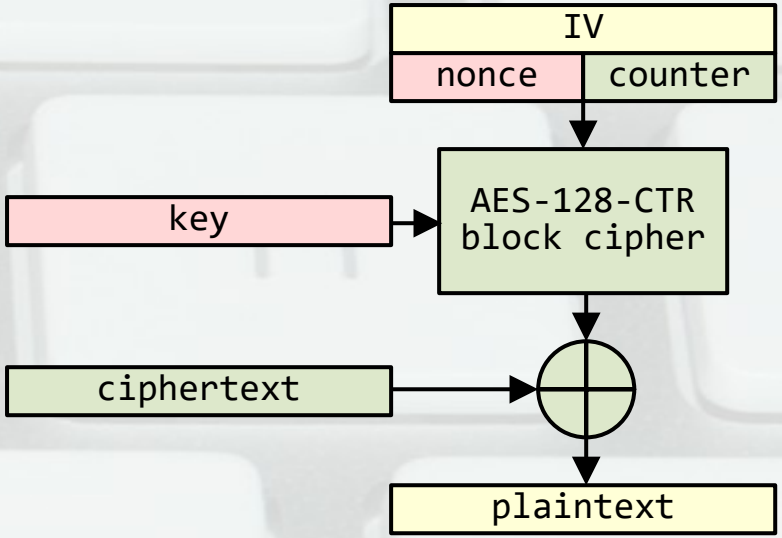
AES Encryption Overview

- Initialization vector (IV)
  - Nonce
  - Counter
- Encryption key
- Encrypt IV with key
- XOR with plaintext



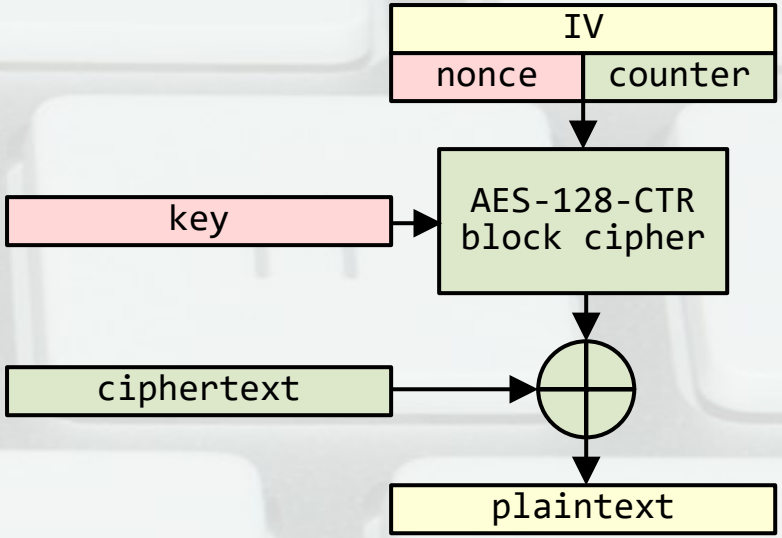
AES Decryption Overview

- Similar to encryption
- Encrypt IV with key
- XOR with ciphertext



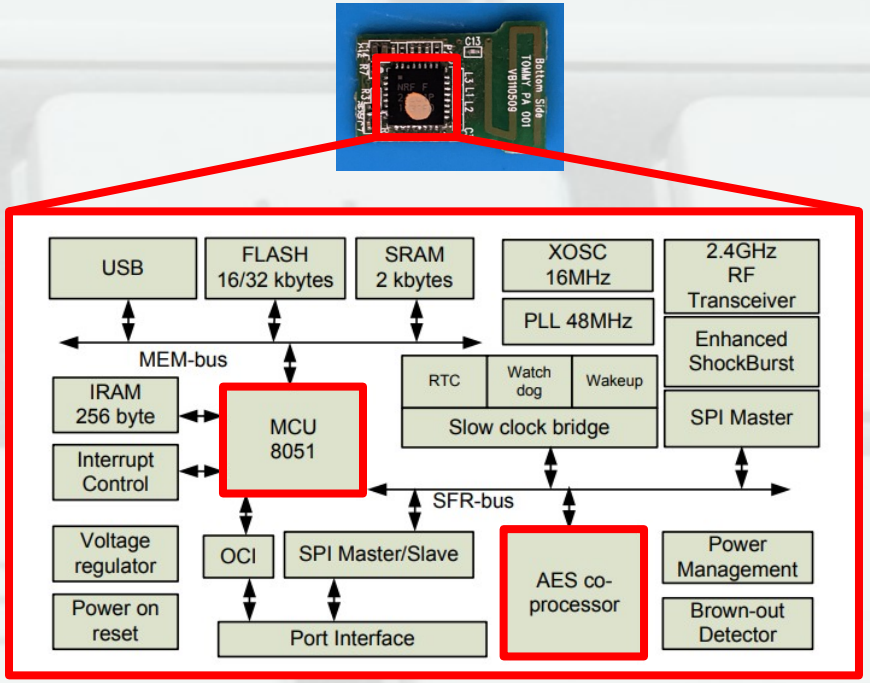
What We Don’t Know About Unifying

- Nonce value
- How the IV is generated
- How the key is negotiated
- Plaintext value



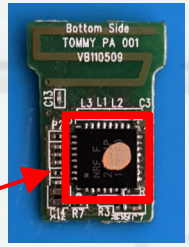
Plan of Attack

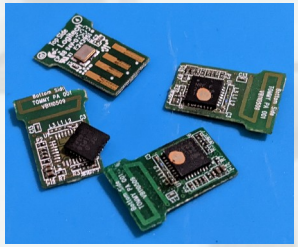
- Modify receiver firmware
- Hijack AES interrupt
  - AESIRQ
- Wait for encrypted payload
- Read AES registers
  - AESKIN
  - AESIV
- Write AES key / IV to flash



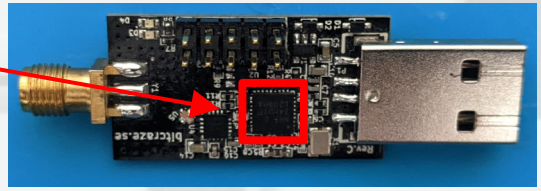
Testing Hardware

- Unifying receiver
  - Easy to brick
- Crazyradio PA
  - Same chip
  - SPI Interface





RIP

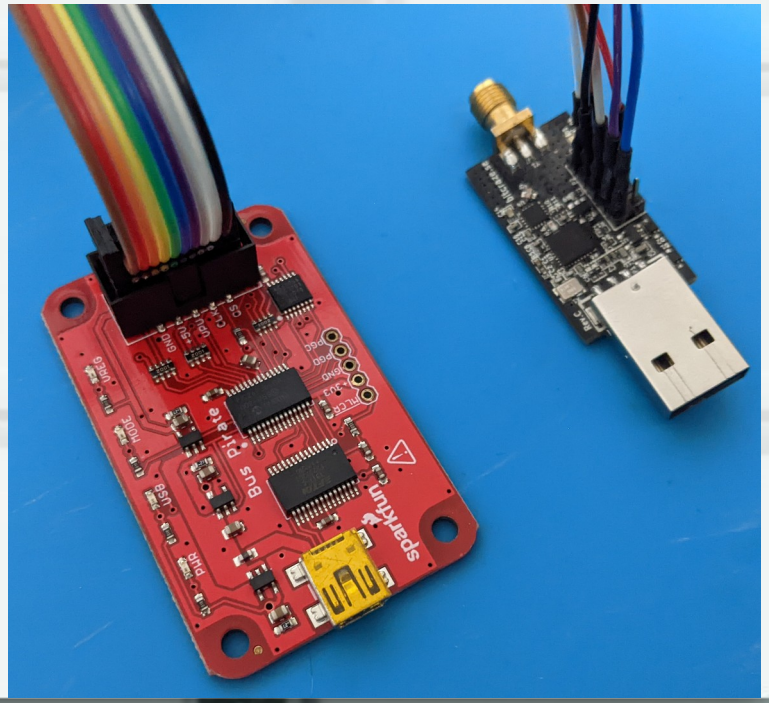


Testing Hardware

- Unifying receiver
  - Easy to brick
- Crazyradio PA
  - Same chip
  - SPI Interface

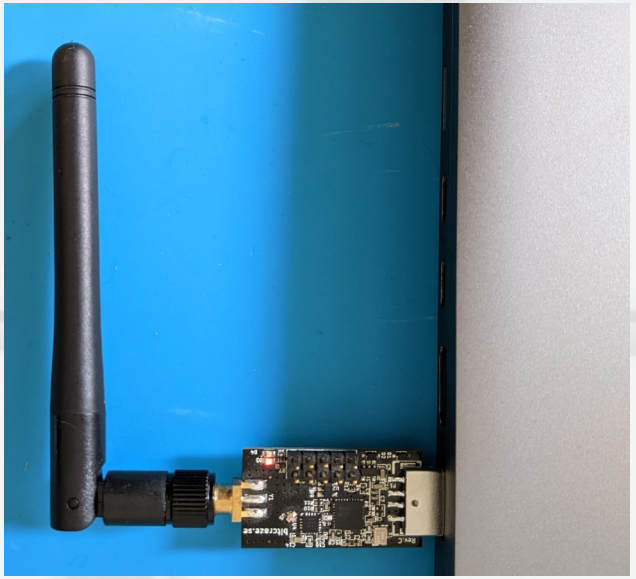
Testing Hardware

- Unifying receiver
  - Easy to brick
- Crazyradio PA
  - Same chip
  - SPI Interface
- Bus Pirate
  - Read / write flash



Performing the Attack

- Flash modified firmware
- Pair a device
- Type something
- Dump flash



Success?

- Encryption key (AESKIN)
  `25 8A 18 6E 6F 78 81 E5 C8 29 E5 B6 40 4A 23 D8`
- Initialization vector (AESIV)
  `B8 F7 6A 0E 2A A3 73 04 67 0D DD 49 F8 4C C1 61`
- Values changes after every boot
- IV does not include the counter
- Firmware doesn’t write to AESKIN and AESIV

Lets Ask Support

… “Is communication between a Unifying device an its associated receiver secure?”

- D0zer

“Its suppport it by 128-BIT AES ENCRYPTION”

- Logitech Support

Lets Ask Support

… “How do a device and a receiver negotiate a shared AES encryption key?”

- D0zer

...“this is a LOGITECH pivate information, the only thing that i can tell you is that if you wanna use any of our products you need to use a software or hardware provide it from us.”

- Logitech Support

… “How a shared AES er

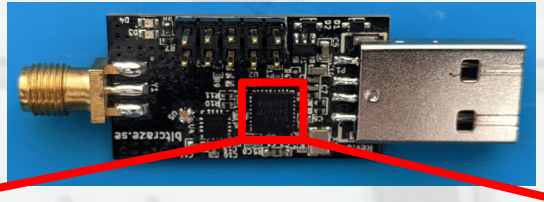
- D0z

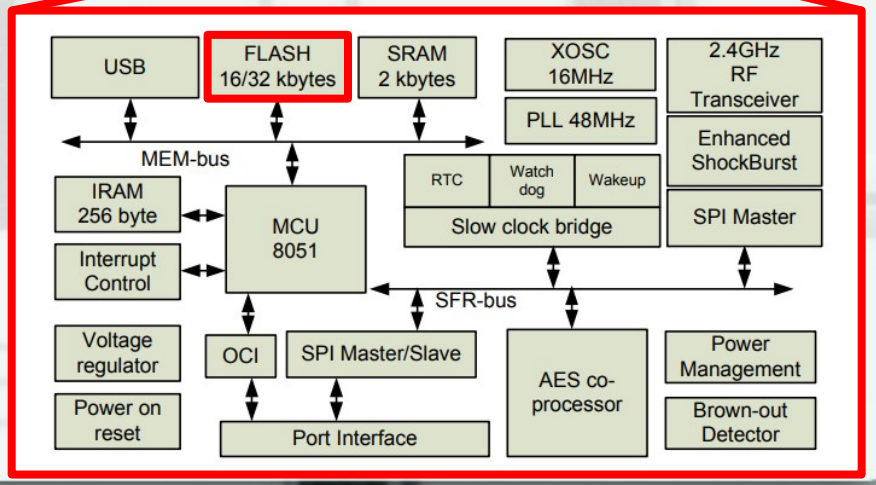
…“this is only thing that i ca ny of our products you need to use a software or hardware provide it from us.”

- Logitech Support

Plan of Attack

- Flash Crazyradio PA
  - Unifying receiver firmware
- Dump flash over SPI
  - Bus Pirate + Crazyradio PA
- Pair a device
- Dump flash again
- Compare flash dumps





Flash Dump

- Before pairing

```
6c00: 3f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
6c10: 02 12 05 00 28 88 02 04 01 00 00 00 00 00 00 00
6c20: 03 fd 26 92 04 01 06 06 00 00 00 00 00 00 00 00
6c30: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
*
```

- After pairing

```
6c00: 3f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
6c10: 02 12 05 00 28 88 02 04 01 00 00 00 00 00 00 00
6c20: 03 fd 26 92 04 01 06 06 00 00 00 00 00 00 00 00
6c30: 03 fd 26 92 04 02 06 07 00 00 00 00 00 00 00 00
6c40: 20 07 14 40 16 04 02 01 0d 00 00 00 00 00 00 00
6c50: 30 9f 22 a5 75 1a 00 00 00 01 00 00 00 00 00 00
6c60: 40 04 4b 33 33 30 00 00 00 00 00 00 00 00 00 00
6c70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
*
7000: 00 fd 26 92 04 40 16 88 02 bc 66 6a a3 61 e6 33
7010: 38 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7020: 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7030: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7040: 02 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7050: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7060: 03 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7070: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7080: 04 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7090: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
70a0: 05 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
70b0: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

Flash Dump

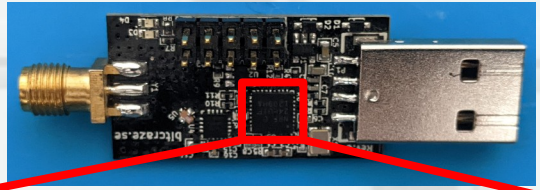
- 16 consecutive bytes
- AES key?
- Still need the nonce

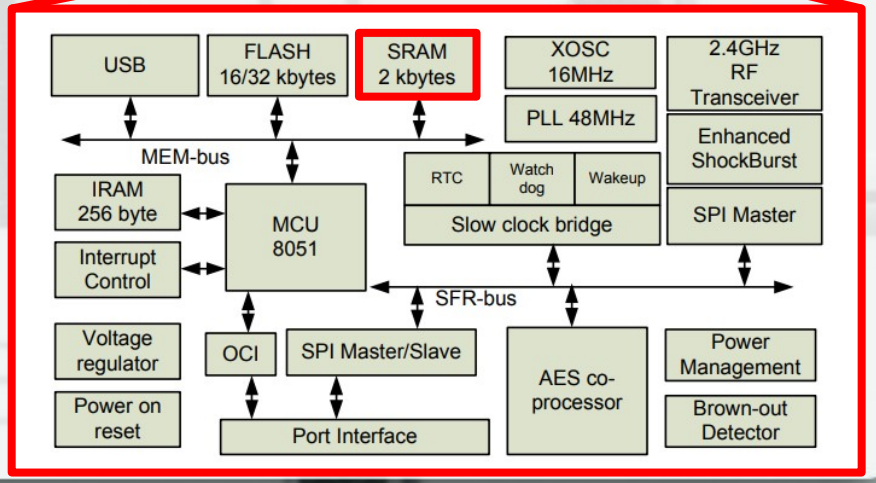
- After pairing

```
6c00: 3f ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
6c10: 02 12 05 00 28 88 02 04 01 00 00 00 00 00 00 00
6c20: 03 fd 26 92 04 01 06 06 00 00 00 00 00 00 00 00
6c30: 03 fd 26 92 04 02 06 07 00 00 00 00 00 00 00 00
6c40: 20 07 14 40 16 04 02 01 0d 00 00 00 00 00 00 00
6c50: 30 9f 22 a5 75 1a 00 00 00 01 00 00 00 00 00 00
6c60: 40 04 4b 33 33 30 00 00 00 00 00 00 00 00 00 00
6c70: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
*
7000: 00 fd 26 92 04 40 16 88 02 bc 66 6a a3 61 e6 33
7010: 38 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7020: 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7030: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7040: 02 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7050: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7060: 03 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7070: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7080: 04 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
7090: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
70a0: 05 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
70b0: ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff
```

Plan of Attack Part 2

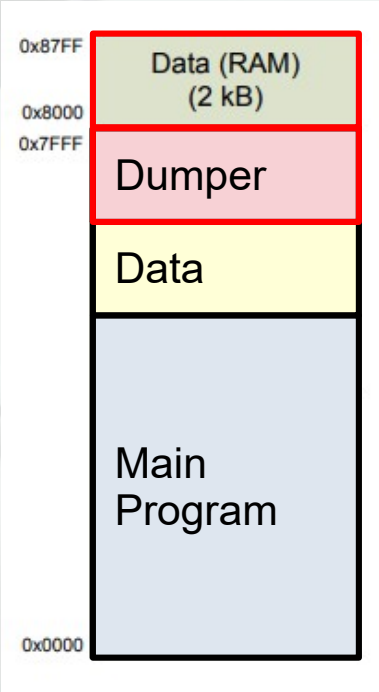
- AES in software?
- Everything is in RAM!
- Dump RAM
- Pair a device
- Type something
- Dump RAM again
- Compare RAM dumps





How to Dump RAM

- Bootloader?
- We don’t need no stinkin’ bootloader
- SPI flashing bypasses the bootloader
- Hijack execution at the bootloader
- Dump RAM to flash
- Dump flash over SPI like before



RAM Dump

- Before pairing

```
0260: 00 00 00 01 02 03 FF 00 FF FF FF 00 AA FF FF FF
0270: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 01 81 FA 00 FA 00
0330: FF 18 00 1D FF FF FF FF FF 06 83 29 6C 21 01 83
0340: 5D 10 FF C6 C0 00 00 00 61 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 03 FD 26 92
0360: 04 01 06 06 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 00 00 00 00 0A 0D 13 26 0E 00 00 00
```

- After pairing and typing

```
0260: 00 00 00 01 02 03 02 D9 FD 04 6A 6D 33 33 BC 88
0270: 9E 16 E6 6D 40 A3 FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 00 81 FA 00 FA 00
0330: 07 00 00 1D 05 FF FF 30 FF 06 83 29 00 00 00 00
0340: 00 10 FF C6 C0 00 00 00 11 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E 00 00 00
```

RAM Dump

- Before pairing

```
0260: 00 00 00 01 02 03 FF 00 FF FF FF 00 AA FF FF FF
0270: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 01 81 FA 00 FA 00
0330: FF 18 00 1D FF FF FF FF FF 06 83 29 6C 21 01 83
0340: 5D 10 FF C6 C0 00 00 00 61 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 03 FD 26 92
0360: 04 01 06 06 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 00 00 00 00 0A 0D 13 26 0E 00 00 00
```

- After pairing and typing

```
0260: 00 00 00 01 02 03 02 D9 FD 04 6A 6D 33 33 BC 88
0270: 9E 16 E6 6D 40 A3 FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 00 81 FA 00 FA 00
0330: 07 00 00 1D 05 FF FF 30 FF 06 83 29 00 00 00 00
0340: 00 10 FF C6 C0 00 00 00 11 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E 00 00 00
```

Encrypted keystroke packet

00:D3:82:92:B3:D3:D6:D2:93:E0:05:67:4F:29:00:00:00:00:00:00:00:94

RAM Dump

- Before pairing

```
0260: 00 00 00 01 02 03 FF 00 FF FF FF 00 AA FF FF FF
0270: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 01 81 FA 00 FA 00
0330: FF 18 00 1D FF FF FF FF FF 06 83 29 6C 21 01 83
0340: 5D 10 FF C6 C0 00 00 00 61 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 03 FD 26 92
0360: 04 01 06 06 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 00 00 00 00 0A 0D 13 26 0E 00 00 00
```

- After pairing and typing

```
0260: 00 00 00 01 02 03 02 D9 FD 04 6A 6D 33 33 BC 88
0270: 9E 16 E6 6D 40 A3 FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 00 81 FA 00 FA 00
0330: 07 00 00 1D 05 FF FF 30 FF 06 83 29 00 00 00 00
0340: 00 10 FF C6 C0 00 00 00 11 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E 00 00 00
```

Encrypted keystroke packet

```
00:D3:82:92:B3:D3:D6:D2:93:E0:05:67:4F:29:00:00:00:00:00:00:00:94
```

RAM Dump

- Before pairing

```
0260: 00 00 00 01 02 03 FF 00 FF FF FF 00 AA FF FF FF
0270: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 01 81 FA 00 FA 00
0330: FF 18 00 1D FF FF FF FF FF 06 83 29 6C 21 01 83
0340: 5D 10 FF C6 C0 00 00 00 61 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 03 FD 26 92
0360: 04 01 06 06 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 00 00 00 00 0A 0D 13 26 0E 00 00 00
```

- After pairing and typing

```
0260: 00 00 00 01 02 03 02 D9 FD 04 6A 6D 33 33 BC 88
0270: 9E 16 E6 6D 40 A3 FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 00 81 FA 00 FA 00
0330: 07 00 00 1D 05 FF FF 30 FF 06 83 29 00 00 00 00
0340: 00 10 FF C6 C0 00 00 00 11 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E 00 00 00
```

Encrypted keystroke packet

```
00:D3:82:92:B3:D3:D6:D2:93:E0:05:67:4F:29:00:00:00:00:00:00:00:94
```

RAM Dump

- Before pairing

```
0260: 00 00 00 01 02 03 FF 00 FF FF FF 00 AA FF FF FF
0270: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 01 81 FA 00 FA 00
0330: FF 18 00 1D FF FF FF FF FF 06 83 29 6C 21 01 83
0340: 5D 10 FF C6 C0 00 00 00 61 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 03 FD 26 92
0360: 04 01 06 06 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 00 00 00 00 0A 0D 13 26 0E 00 00 00
```

- After pairing and typing

```
0260: 00 00 00 01 02 03 02 D9 FD 04 6A 6D 33 33 BC 88
0270: 9E 16 E6 6D 40 A3 FF 00 FF FF FF 00 AA FF FF FF
0280: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
0290: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02A0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02B0: 00 FF FF AA FF FF FF 00 FF FF FF 00 AA FF FF FF
02C0: 00 FF FF AA FF FF 01 00 00 00 00 00 00 00 00 00
02D0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
*
0300: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 FF
0310: 80 F0 49 43 50 00 00 00 00 00 00 00 00 00 00 00
0320: 00 00 00 00 00 00 00 00 03 01 00 81 FA 00 FA 00
0330: 07 00 00 1D 05 FF FF 30 FF 06 83 29 00 00 00 00
0340: 00 10 FF C6 C0 00 00 00 11 00 00 00 00 00 00 00
0350: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 14 1D
0370: 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E 00 00 00
```

Encrypted keystroke packet

00:D3:82:92:B3:D3:D6:D2:93:E0:05:67:4F:29:00:00:00:00:00:00:00:94

Success!

- Initialization vector

  `04 14 1D 1F 27 28 0D 05 67 4F 29 0A 0D 13 26 0E`

- Encryption key

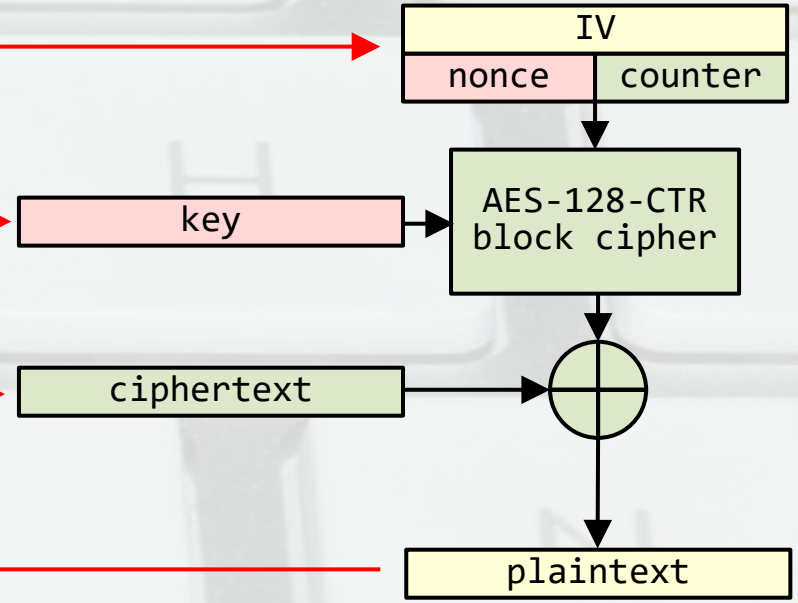
  `02 D9 FD 04 6A 6D 33 33 BC 88 9E 16 E6 6D 40 A3`

- Encrypted payload

  `82 92 B3 D3 D6 D2 93 E0`

- Decrypted payload

  `00 00 00 00 00 00 00 C9`



Encryption Key Generation

- RAM after pairing (encryption key)
  `02 D9 FD 04 6A 6D 33 33 BC 88 9E 16 E6 6D 40 A3`

- Flash after pairing
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

- RAM after pairing (encryption key)
  `02 D9 FD 04 6A 6D 33 33 BC 88 9E 16 E6 6D 40 A3`

- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

- RAM after pairing (encryption key)
  `02 D9 FD 04 6A 6D 33 33 BC 88 9E 16 E6 6D 40 A3`
- RAM before pairing (bitmask)
  `FF 00 FF FF FF 00 AA FF FF FF 00 FF FF AA FF FF`
- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

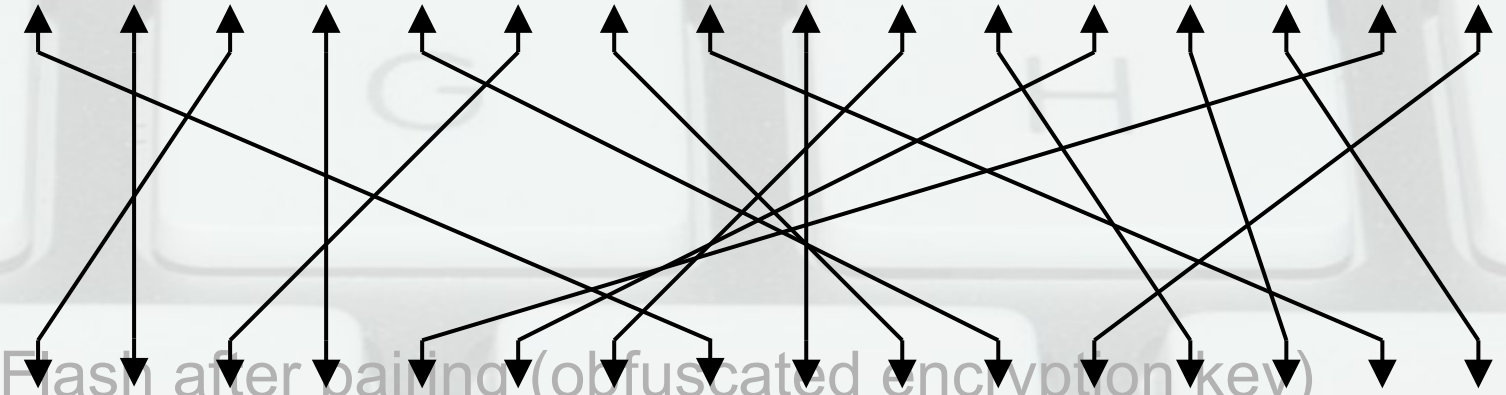
Encryption Key Generation

- RAM after pairing (encryption key)
  `02 D9 FD 04 6A 6D 33 33 BC 88 9E 16 E6 6D 40 A3`
- RAM before pairing (bitmask)
  `FF 00 FF FF FF 00 AA FF FF FF 00 FF FF AA FF FF`
- Bitwise XNOR
  `02 26 FD 04 6A 92 66 33 BC 88 61 16 E6 38 40 A3`
- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

- Bitwise XNOR

```
02 26 FD 04 6A 92 66 33 BC 88 61 16 E6 38 40 A3
```



- Flash after pairing (obfuscated encryption key)

```
FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38
```

Encryption Key Generation

- Bitwise XNOR

```
02 26 FD 04 6A 92 66 33 BC 88 61 16 E6 38 40 A3
```

- Flash after [illegible] key)

```
FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38
```

Encryption Key Generation

- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

BB:0A:DC:A5:75

- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

15:5F:01:81:15:CF:B4:F3:08:40:16:04:00:01:47:00:00:00:00:00:01:D4

BB:0A:DC:A5:75

- Flash after pairing (obfuscated encryption key)
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

Encryption Key Generation

15:5F:01:81:15:CF:B4:F3:08:40:16:04:00:01:47:00:00:00:00:00:01:D4

15:1F:01:FD:26:92:04:02:08:88:02:04:01:01:07:00:00:00:00:00:00:71

~~BB:0A:DC:A5:75~~

FD:26:92:04:02

- Flash after pairing (obfuscated encryption key)

  FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38

Encryption Key Generation

15:5F:01:81:15:CF:B4:F3:08:40:16:04:00:01:47:00:00:00:00:00:01:D4

15:1F:01:FD:26:92:04:02:08:88:02:04:01:01:07:00:00:00:00:00:00:71

00:5F:02:BC:66:6A:A3:58:8A:51:EA:1E:40:00:00:01:00:00:00:00:00:F4

~~BB:0A:DC:A5:75~~

FD:26:92:04:02

- Flash after pairing (obfuscated encryption key)

  FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38

Encryption Key Generation

15:5F:01:81:15:CF:B4:F3:08:40:16:04:00:01:47:00:00:00:00:00:01:D4

15:1F:01:FD:26:92:04:02:08:88:02:04:01:01:07:00:00:00:00:00:00:71

00:5F:02:BC:66:6A:A3:58:8A:51:EA:1E:40:00:00:01:00:00:00:00:00:F4

00:1F:02:61:E6:33:38:58:8A:51:EA:1E:40:00:00:01:00:00:00:00:00:B1

~~BB:0A:DC:A5:75~~

FD:26:92:04:02

- Flash after pairing (obfuscated encryption key)

  FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38

Encryption Key Generation

15:5F:01:81:15:CF:B4:F3:08:40:16:04:00:01

15:1F:01:FD:26:92:04:02:08:88:02:04:01:01

00:5F:02:BC:66:6A:A3:58:8A:51:EA:1E:40:00

00:1F:02:61:E6:33:38:58:8A:51:EA:1E:40:00

~~BB:0A:DC:A5:75~~

FD:26:92:04:02

- Flash after pairing (obfuscated encryption key)

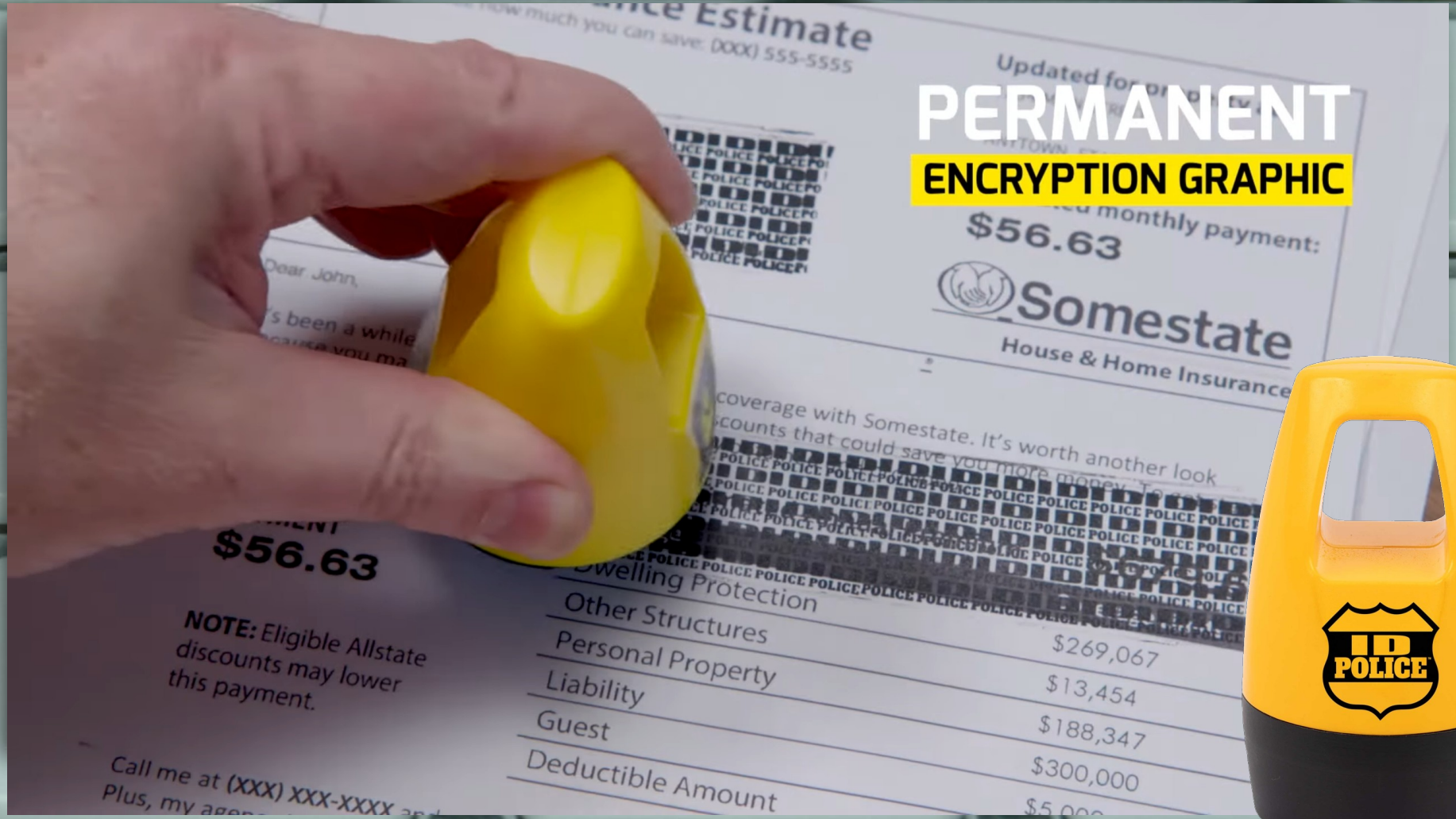
  `FD 26 92 04 40 16 88 02 BC 66 6A A3 61 E6 33 38`

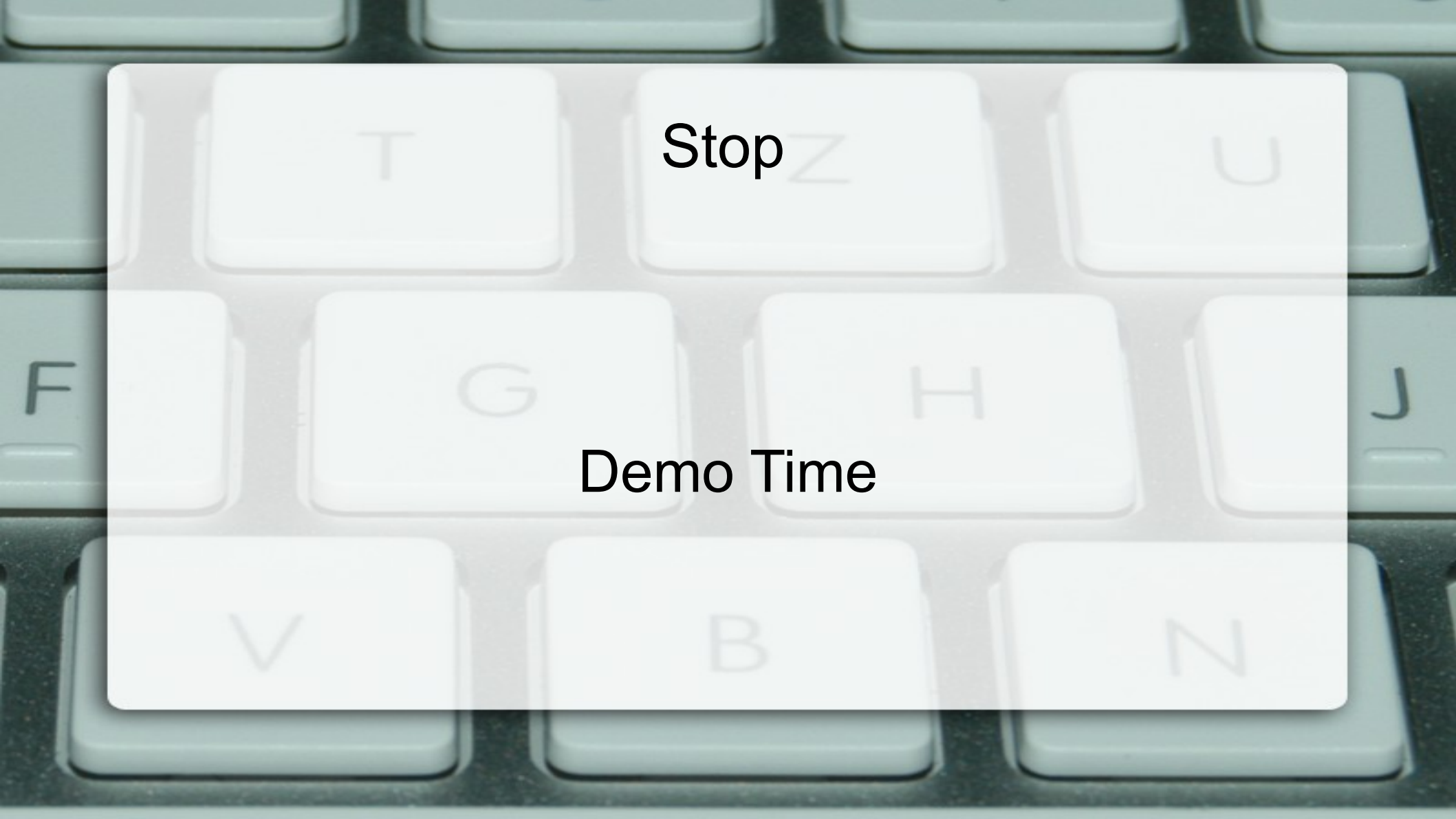
It Gets Worse

- Typical AES-128 key space
  2^{128} = 340282366920938463463374607431768211456 keys
- Key space minus 4 bytes from known RF address
  2^{96} = 79228162514264337593543950336 keys
- Minus 2 more bytes from predictable receiver product ID
  2^{80} = 1208925819614629174706176 keys
- Minus 2 more bytes from predictable device product ID
  2^{64} = 18446744073709551616 keys

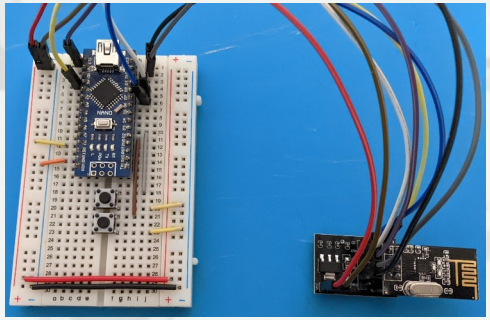
How Bad is This?

	Typical AES-128	Weakened AES-128
Key space	340282366920938463463374607431768211456 keys	18446744073709551616 keys
Cracking speed w/ 3.8GHz i7-10700K	300000000 keys/sec	300000000 keys/sec
Cracking time	35967610236020047296568 years	1949 years
Age of the universe	13800000000 years	13800000000 years


PERMANENT
ENCRYPTION GRAPHIC
Somestate
House & Home Insurance
$56.63
Dear John,
NOTE: Eligible Allstate discounts may lower this payment.
Dwelling Protection
Other Structures $269,067
Personal Property $13,454
Liability $188,347
Guest $300,000
Deductible Amount
ID POLICE


Stop
Demo Time

Next Steps



- Receiver firmware
- Enhanced security

- Build keyboard
- Unifying library
- TMK, QMK, ZMK, BlueMicro

Thank You

Questions?

Email – decrazyo@gmail.com

Discord – @decrazyo

https://github.com/decrazyo/logihack

https://github.com/decrazyo/unifying