IoT and the Future of Pentesting

Jeremy Goldstein

Agenda

TRUSTED SECURITY SERVICES

- whoami
- Technology/Pentesting Evolution
- Where are we heading?
- **IoT/Hardware Hacking** <-- the fun part
- Why does this matter?
- Conclusion

$ whoami

$ whoami -> jeremy@tss

TRUSTED SECURITY SERVICES

Head of Security Testing @ TSS

Previously

- Team Lead, REDteam @ KPN (Amsterdam, The Netherlands)
- Director of Security Testing @ ATO

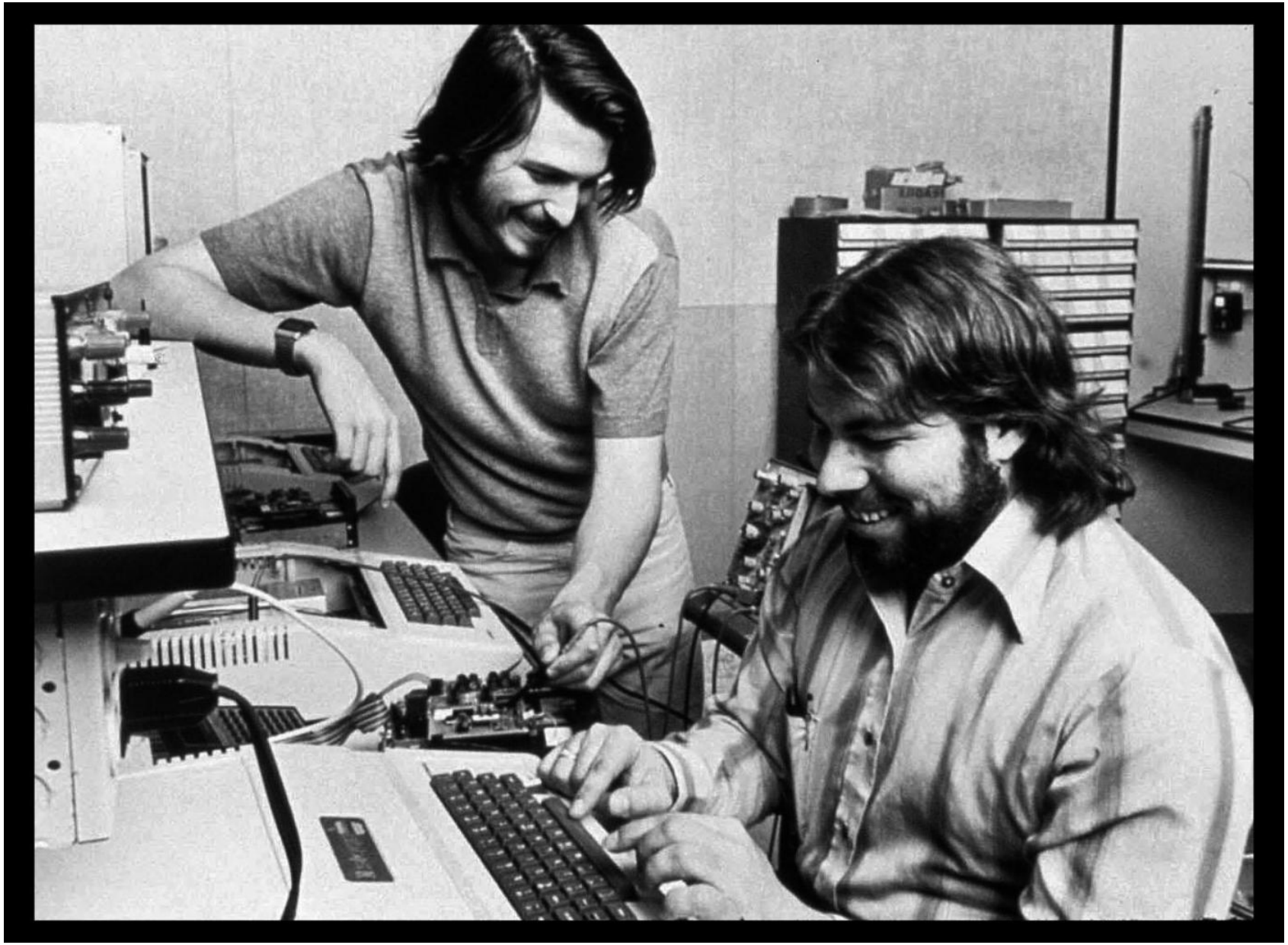
Infosec for 15 years

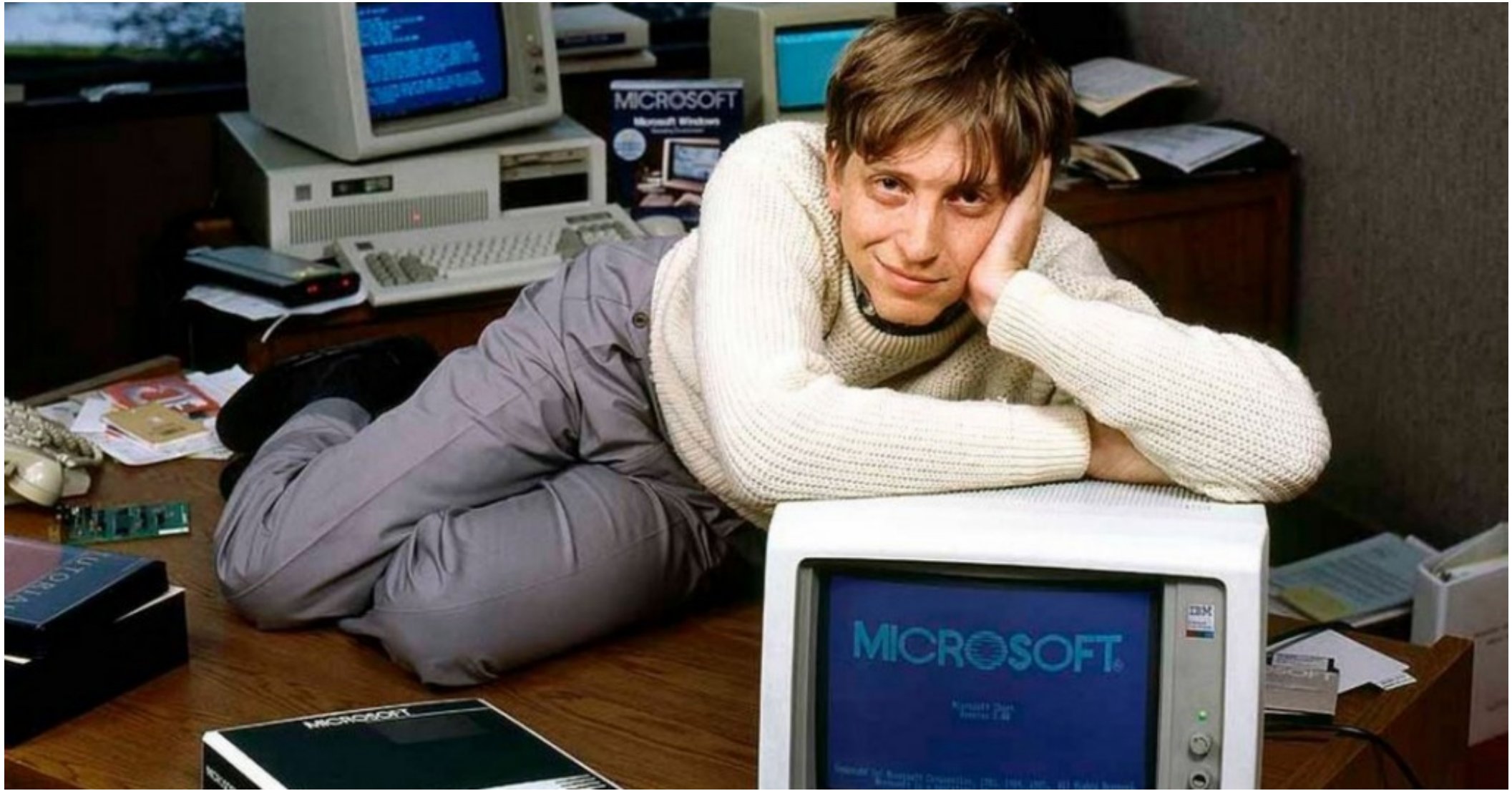
Running technical security teams for 10 years

Lots of technical security - pentesting, IR & threat intel

A Brief History of Modern Computing

and its impact on pentesting




MICROSOFT
MICROSOFT

Desktop Applications

Thick client pentesting

TRUSTED SECURITY SERVICES

->

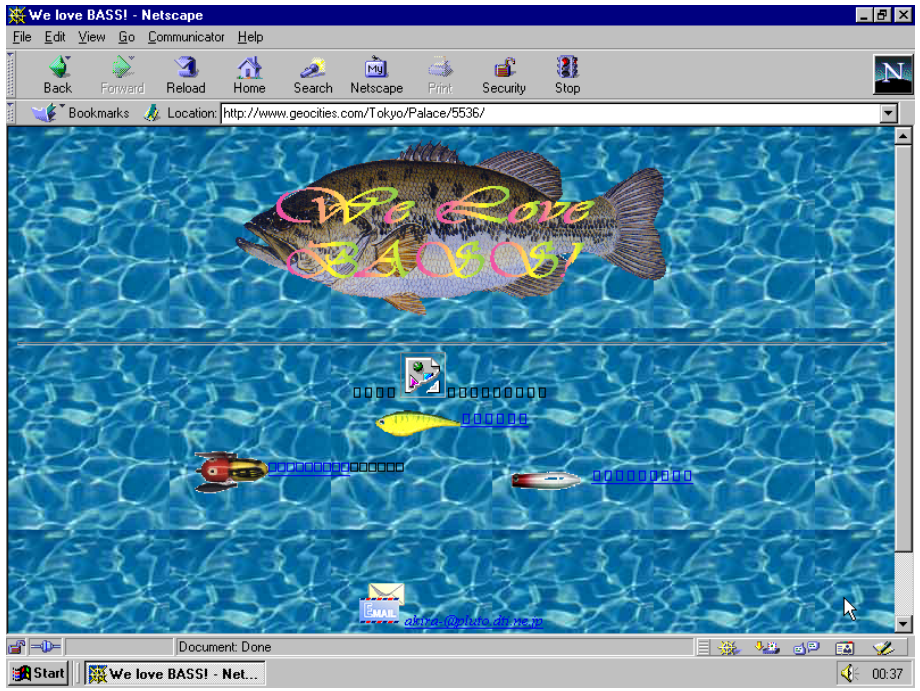
LordPE

Networks and the Internet

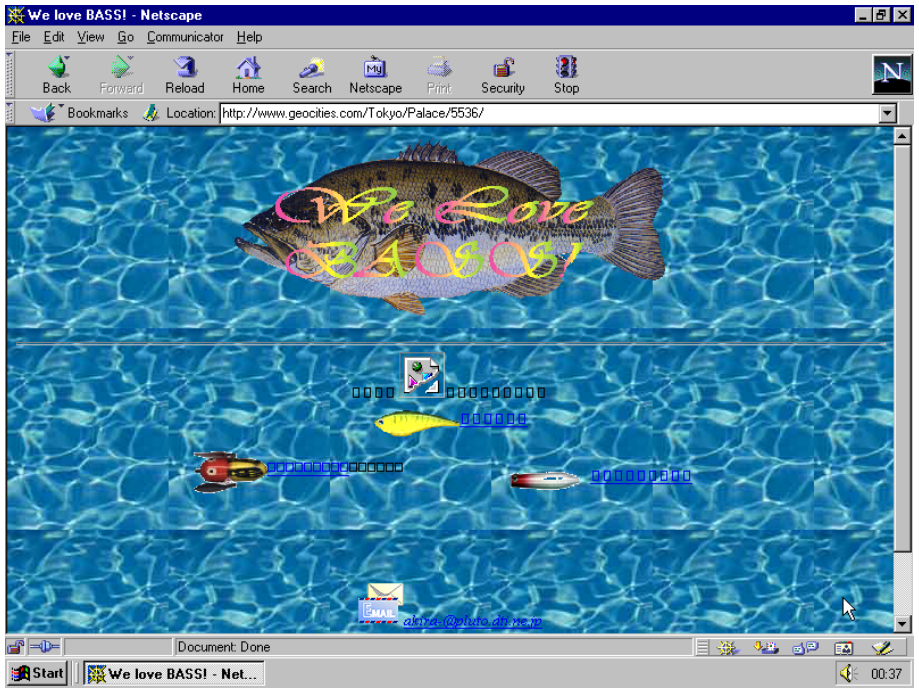
Infra pentesting

->

Web sites/applications



Web app pentesting



->

OWASP
The Open Web Application Security Project

Smart Phones and Apps

Mobile app pentesting

->

OWASP Mobile Security Project

FRIDA

The Cloud™

Cloud pentesting

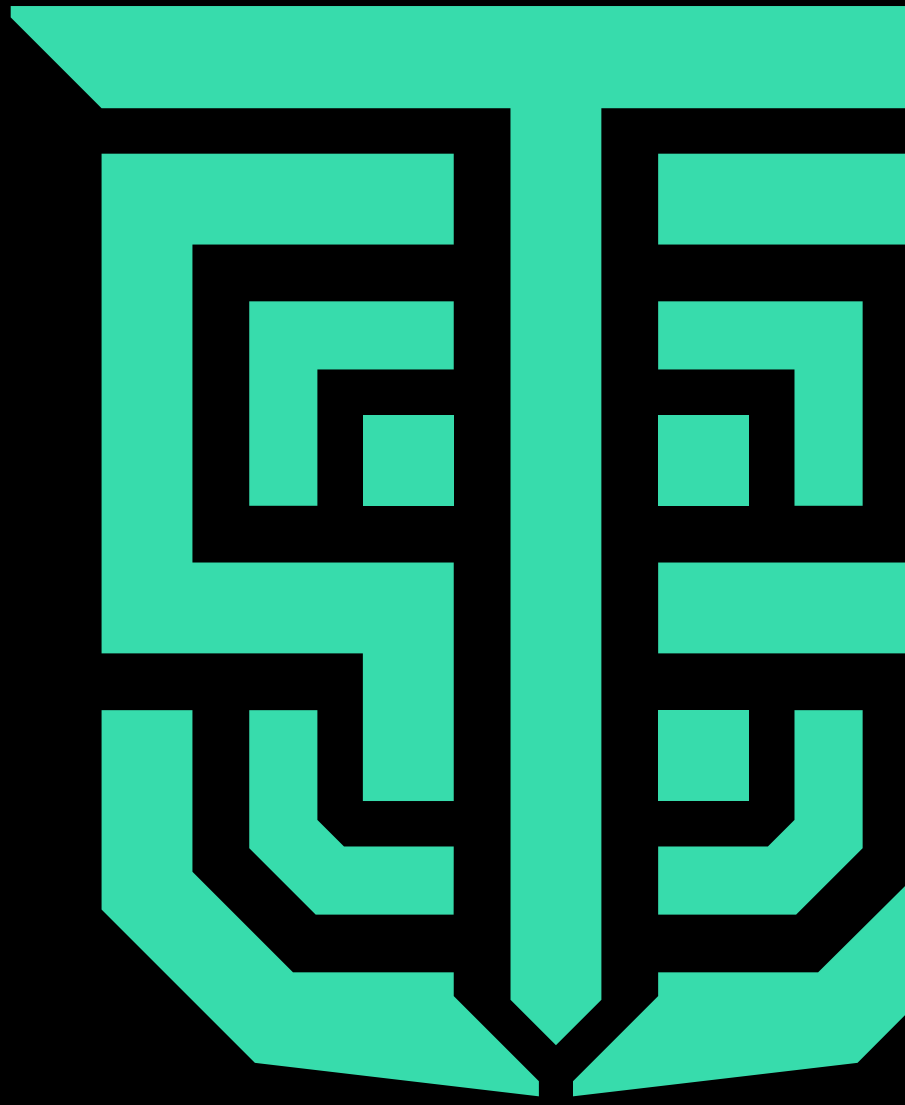
->

Azure

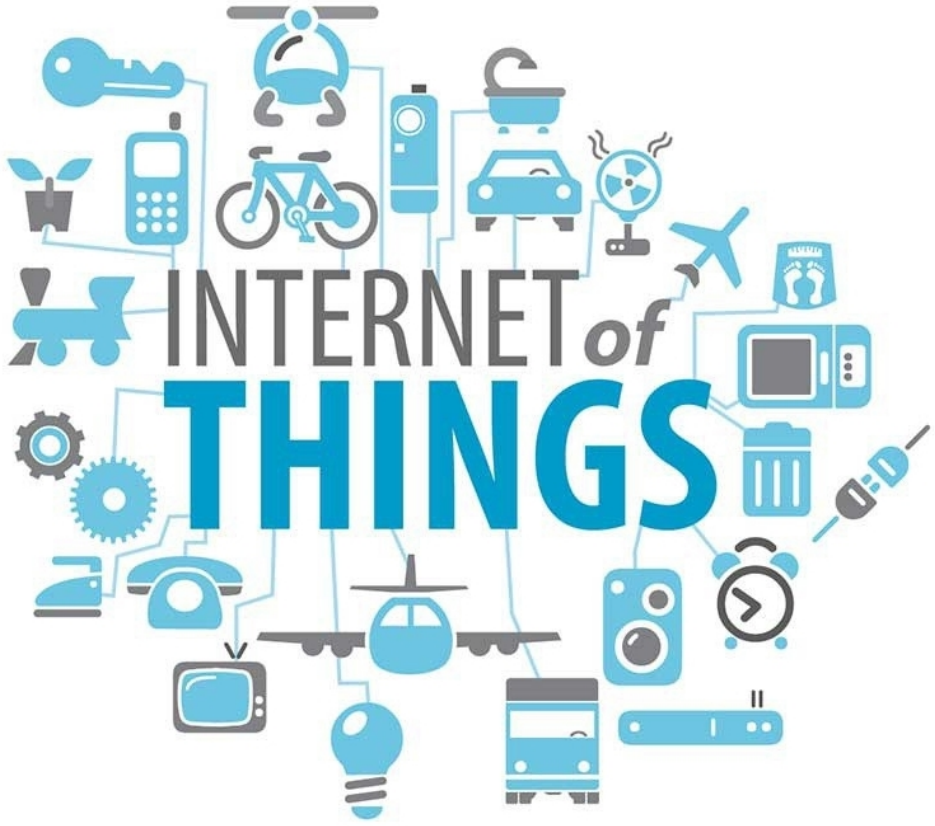
aws

flAWS 2

Where are we heading?




Cloud Computing


INTERNET of
THINGS

IoT though…

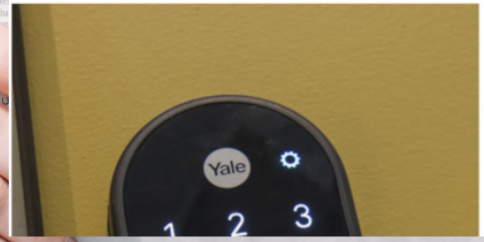
TRUSTED SECURITY SERVICES

Is different

IoT at the moment

Families are LOCKED OUT of or INSIDE their homes as Yale 'smart' security app crashes leaving dozens stranded

By Lara Keay For Mailonline
07:58 12 Oct 2018, updated 12:37 15 Oct 2018



skoops 🦷😷

@skoops

Follow

The @netatmo servers are down and twitter is already full of freezing people not able to control their heating :D (via [protected]) / cc @internetofshit


Forbes
3,775 views | Nov 23, 2018, 02:13pm
86% Of Enterprises Increasing IoT Spending In 2019
Louis Columbus Contributor
Enterprise & Cloud
TWEET THIS
Enterprises increased their investments in IoT by 4% in 2018 over 2017, spending an average of $4.6M this year.

Telstra Exchange

Telstra Exchange > Tech and Innovation > IoT >
Our exclusive partnership with Arduino set to fuel the growth of IoT in Australia

Our exclusive partnership with Arduino set to fuel the growth of IoT in Australia

IoT

Posted on November 30, 2018

3 min read

by **Håkan Eriksson**
Chief Technology Officer - CTO

Telstra Exchange

Telstra Exchange > Business and Enterprise > **Launching our global IoT capability with Ericsson**

Launching our global IoT capability with Ericsson

Business and Enterprise

Posted on February 25, 2019

2 min read

by **Håkan Eriksson**
Chief Technology Officer - CTO

"Given IoT's current trajectory, I believe it's only a matter of time until it makes its way into businesses and enterprises in a meaningful way"

- me, just now

IoT Security/Pentesting

What's the big deal?

Hardware

The fun part

IoT and hardware hax0ring

Housekeeping

TRUSTED SECURITY SERVICES

- IoT/Hardware **solution** Pentesting

Housekeeping

TRUSTED SECURITY SERVICES

- IoT/Hardware **solution** Pentesting
- Not hardware hacking research

Housekeeping

TRUSTED SECURITY SERVICES

- IoT/Hardware **solution** Pentesting
- Not hardware hacking research
- Achievable within budget and time contraints

What a hardware pentest isn't

TRUSTED SECURITY SERVICES

What a hardware pentest is

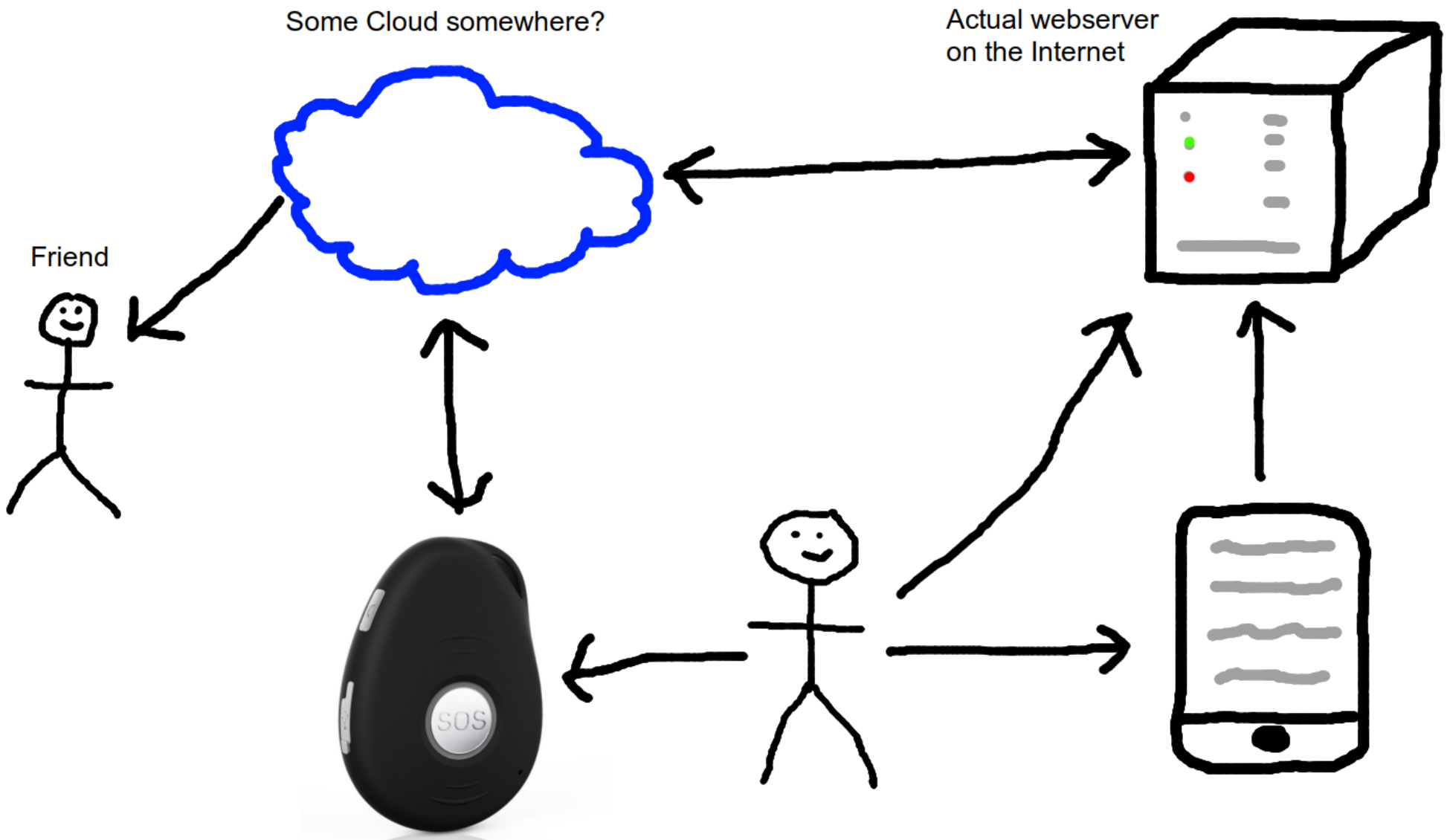
TRUSTED SECURITY SERVICES

- Two real world examples:
  - A personal safety device
  - An ECG test solution

The personal safety device

The device

TRUSTED SECURITY SERVICES


Some Cloud somewhere?
Actual webserver
on the Internet
Friend
SOS

Analysing the attack surface

TRUSTED SECURITY SERVICES

- Understand the device's functionality

Analysing the attack surface

TRUSTED SECURITY SERVICES

- Understand the device's functionality

Analysing the attack surface

TRUSTED SECURITY SERVICES

- Try the easy stuff first

Analysing the attack surface

TRUSTED SECURITY SERVICES

- Try the easy stuff first

Analysing the attack surface

TRUSTED SECURITY SERVICES

- Next step, open the device up

Analysing the attack surface

- Next step, open the device up

Analysing the internals

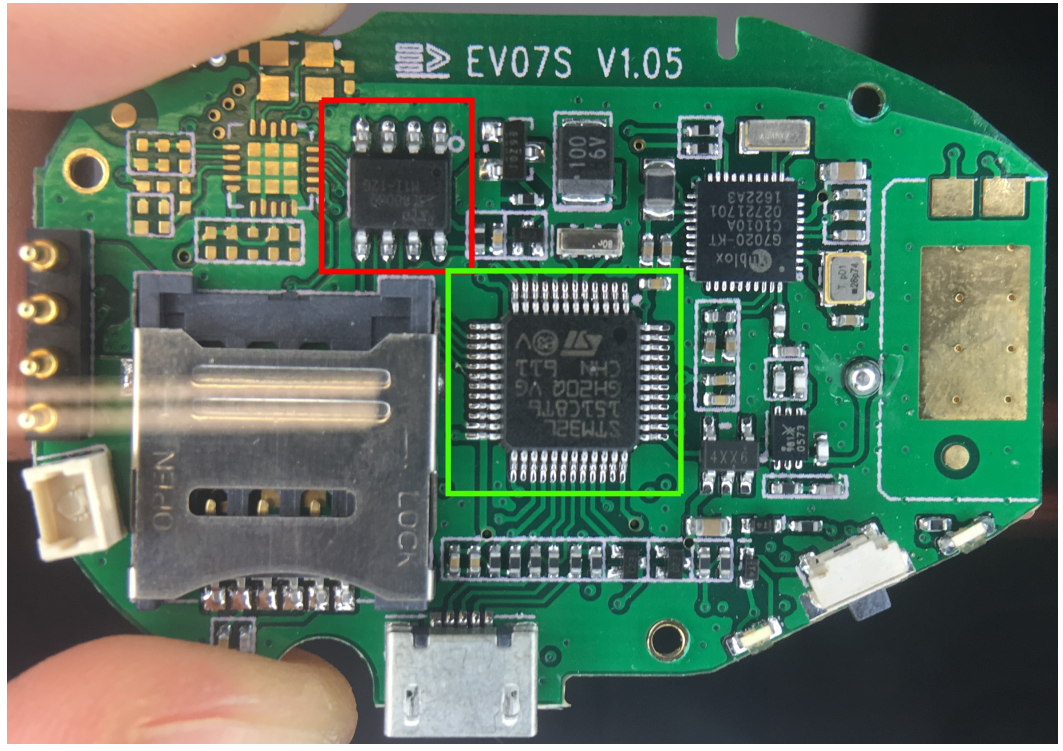
TRUSTED SECURITY SERVICES

- Identify chips, debug ports and read the data sheets!

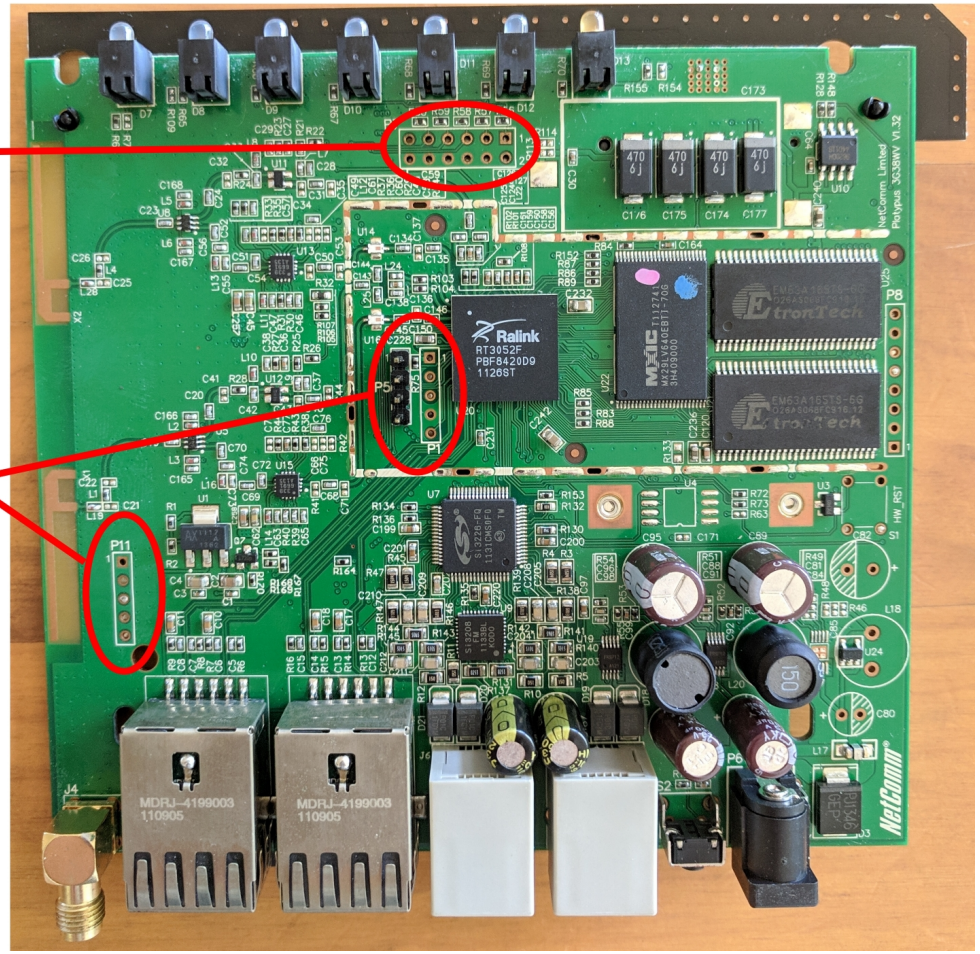
Analysing the internals

TRUSTED SECURITY SERVICES

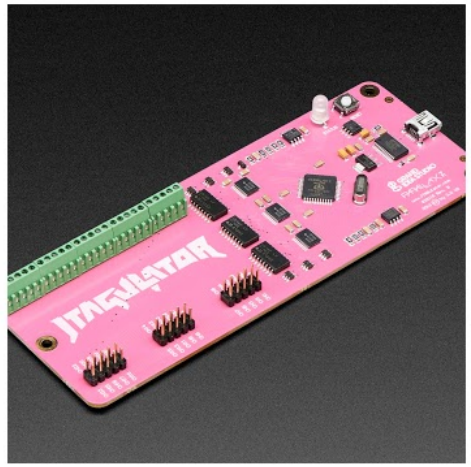
- Identify chips, debug ports and read the data sheets!

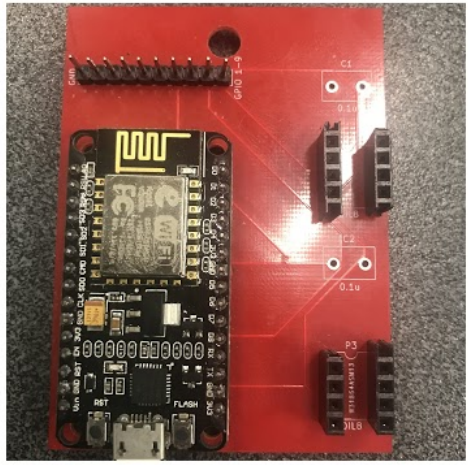


Debug ports


JTAG?
UART?
P11
P5
P1
P8
P6
Ralink
RT3052F
PBF8420D9
1126ST
MDRJ-4199003
1,10905
MDRJ-4199003
110905
NetComm


MEASURE UP
000

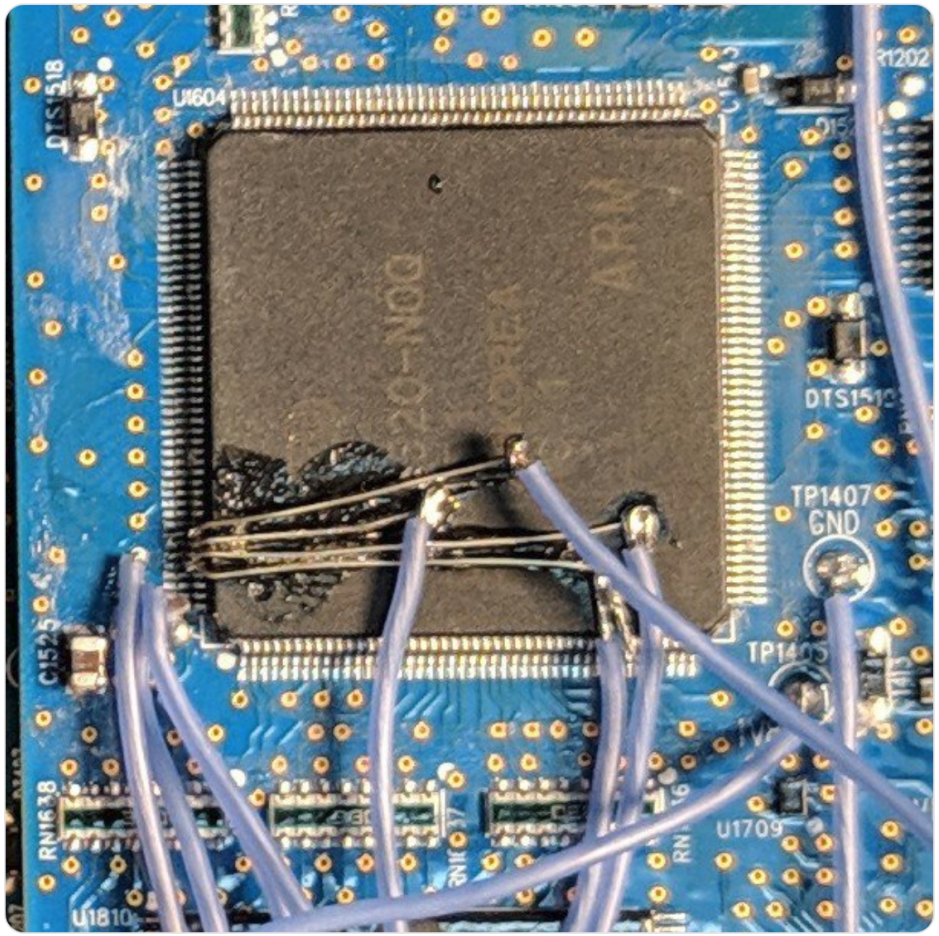

JTAGulator



Dave A
@dave_32768

Follow

It's ugly, but it works! So inconsiderate to not have a jtag connector on the board. 🤣😂

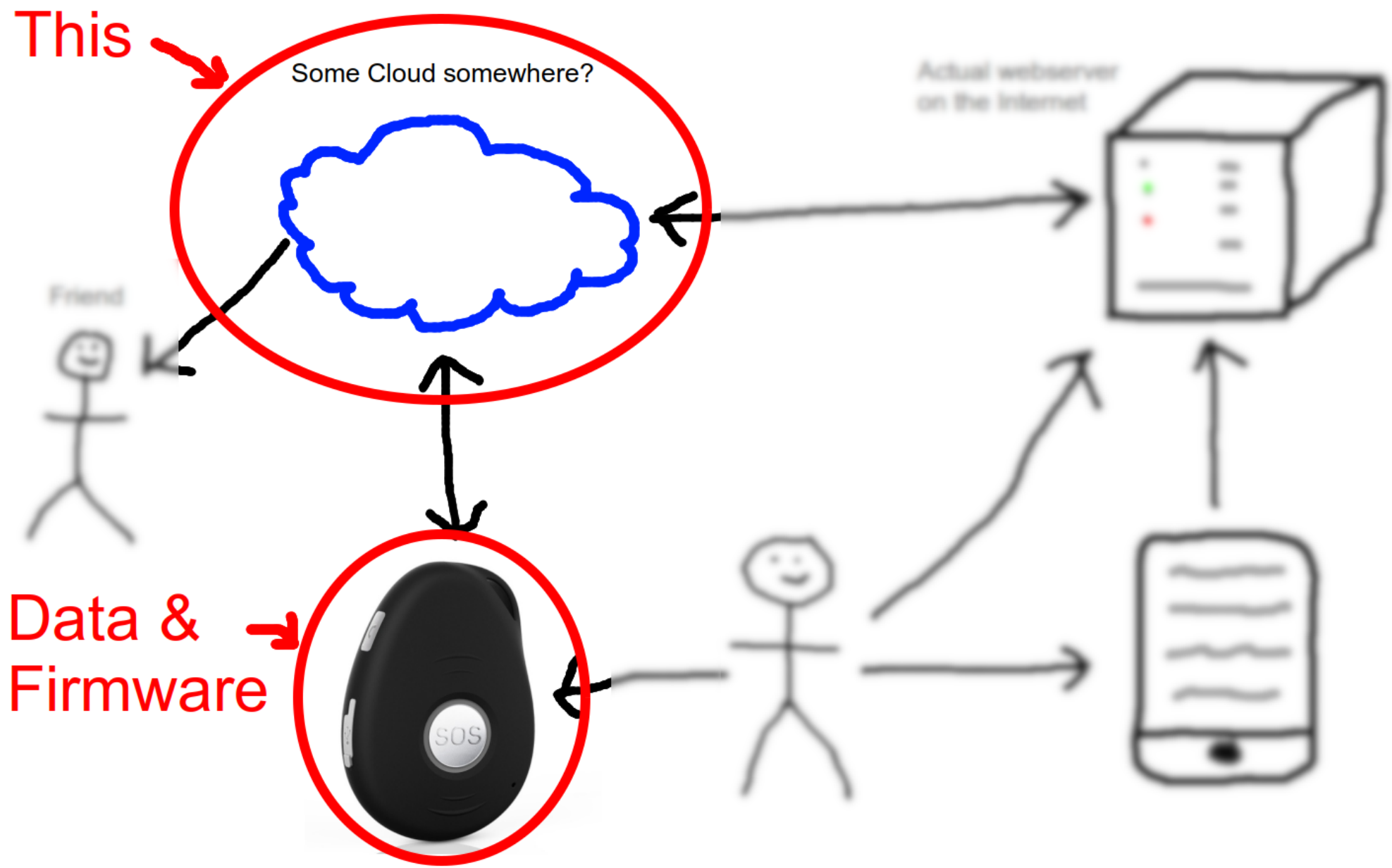


3:38 AM - 8 Nov 2018

Quick review

TRUSTED SECURITY SERVICES

- Understand functionality and components
- Inputs and outputs
- Analysed and identified internals


This
Some Cloud somewhere?
Actual webserver
on the Internet
Friend
Data &
Firmware
SOS

Attack!

TRUSTED SECURITY SERVICES

1. Extract firmware and data off device

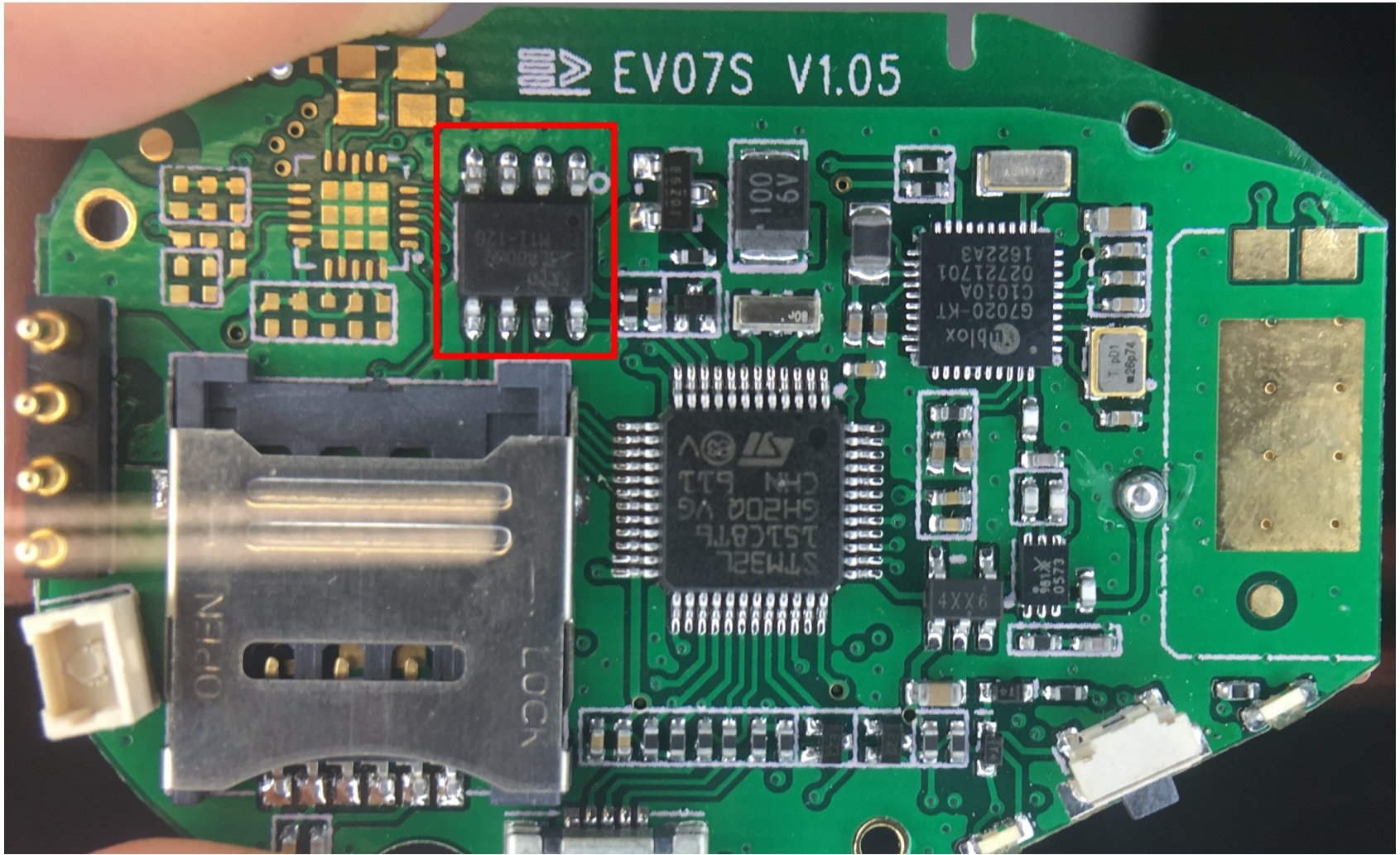
2. Intercept comms between device and cloud

Extracting firmware and data

TRUSTED SECURITY SERVICES

- Download off the Internet
- Remove SD card
- Debug ports
- Desoldering the chip
- In-circuit chip manipulation
- Bus snooping

Desoldering the chip



Desoldering the chip

Firmware Analysis

Attack!

TRUSTED SECURITY SERVICES

1. ~~Extract firmware and data off device~~

2. Intercept comms between device and cloud

Intercept device comms

TRUSTED SECURITY SERVICES

- 3G interception
  - IMSI catching
  - Create our own test 3G network
- Bus snooping on the device

3G Intercept: Equipment

TRUSTED SECURITY SERVICES

3G Intercept: IMSI Catching

TRUSTED SECURITY SERVICES

- Create a fake base station with the SDR
- Jam the 4G/3G frequencies to downgrade to GSM
- Provide a stronger signal than the real base station
- Intercept and/or manipulate the traffic

3G Intercept: IMSI Catching

TRUSTED SECURITY SERVICES

It's illegal

3G Intercept: Create a 3G Network

TRUSTED SECURITY SERVICES

1. Setup test 3G network using the SDR and BTS software, e.g. USRP with OpenBTS
2. Use a SIM card programmed for the test network
3. ???
4. Profit!

Intercept device comms

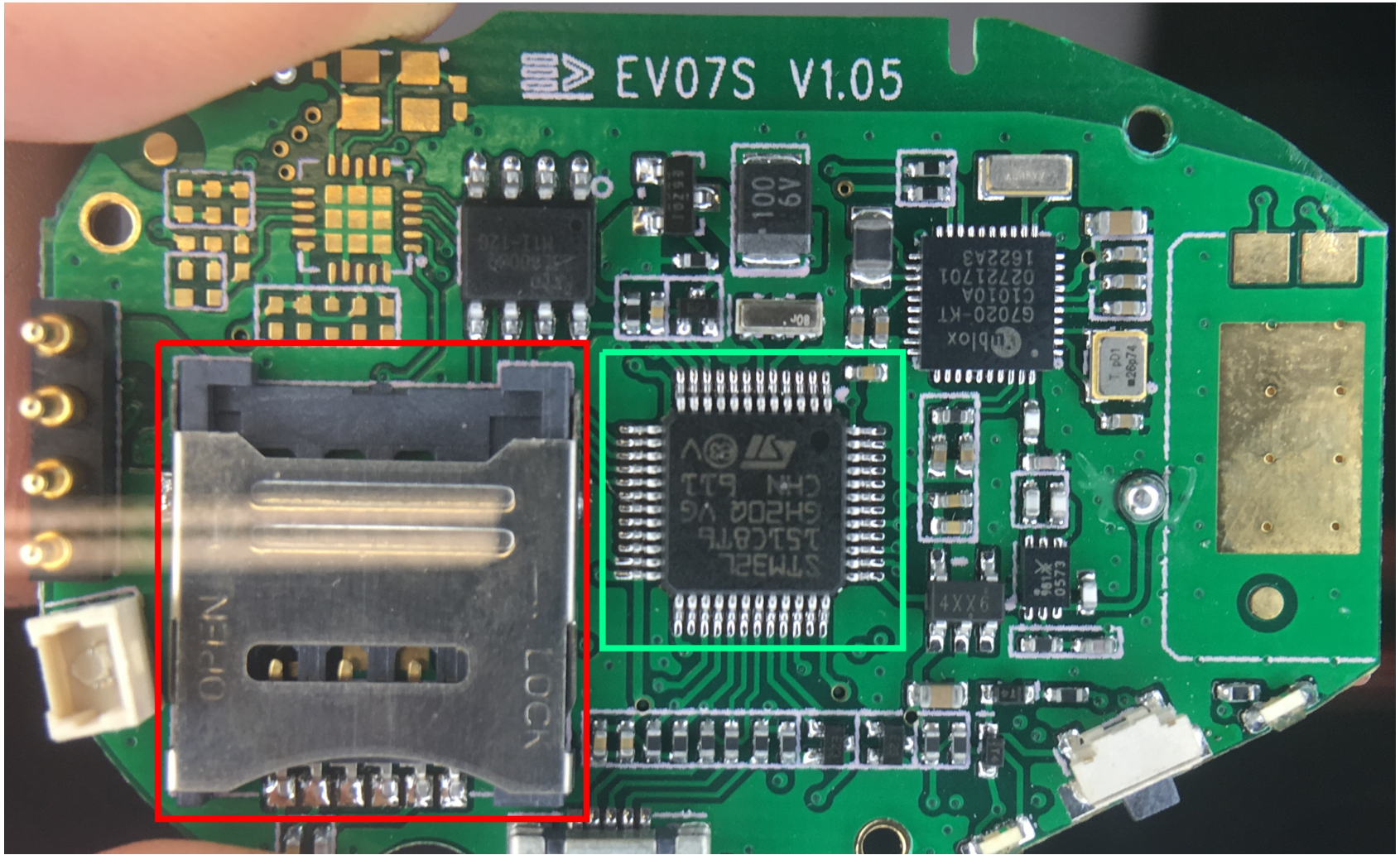
TRUSTED SECURITY SERVICES

- ~~3G interception~~
  - ~~IMSI catching~~
  - ~~Create our own test 3G network~~
- Bus snooping on the device

Bus Snooping

TRUSTED SECURITY SERVICES

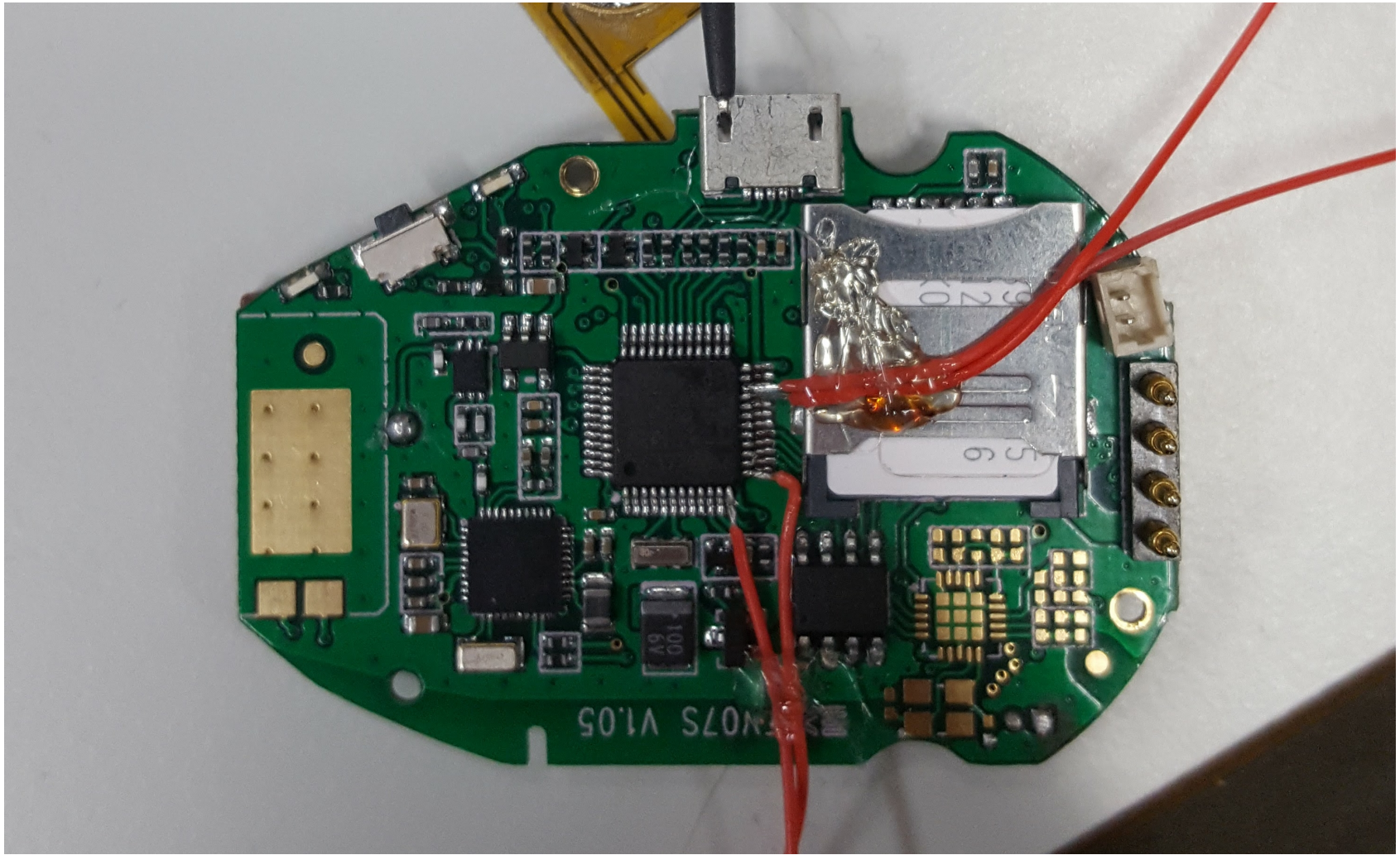
Bus Snooping



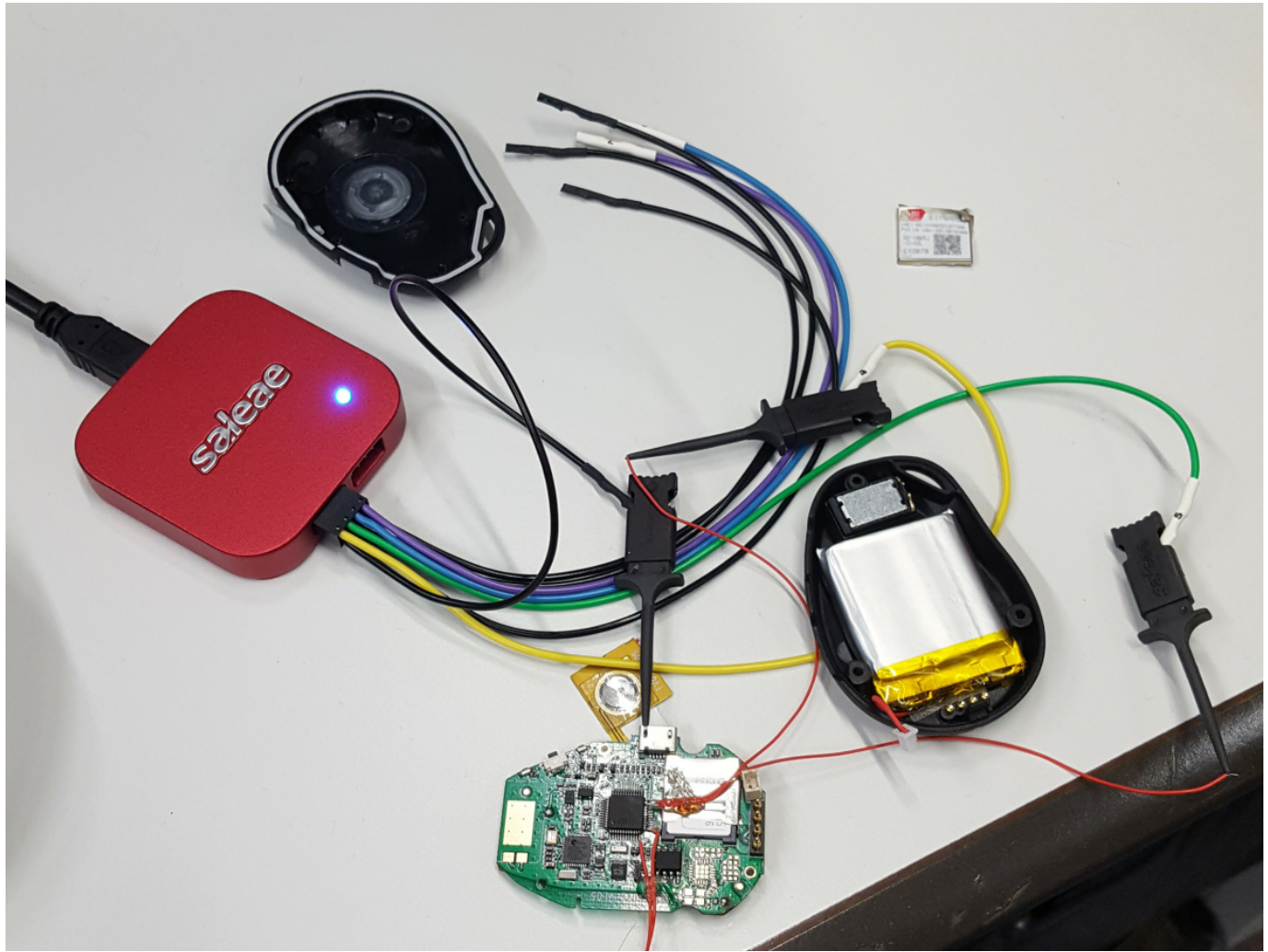
Logic Analyser

Putting theory into practice

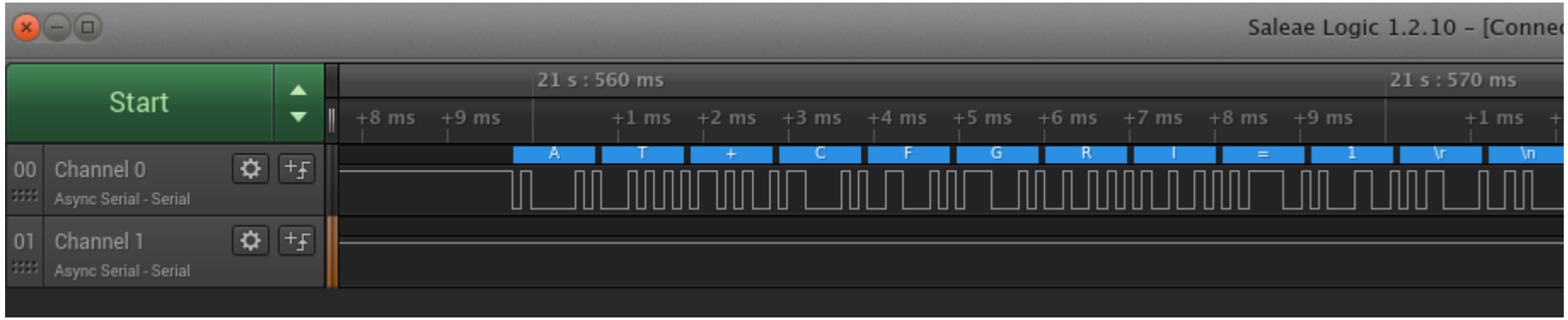
TRUSTED SECURITY SERVICES



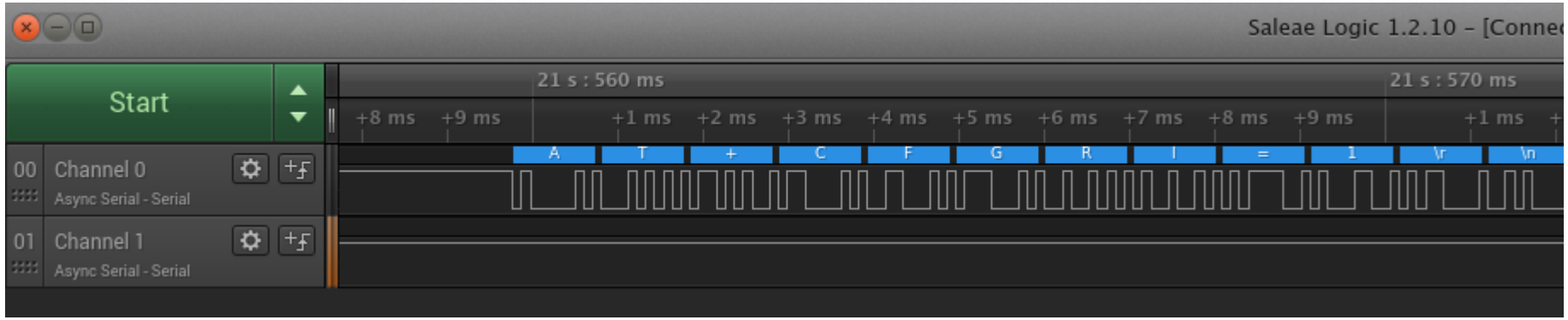
Putting theory into practice



Decoded Results



Decoded Results



AT+CFGRI=1\r\n

Saleae Results

TRUSTED SECURITY SERVICES

```
AT+CIPSTATUS

 OK
 STATE: IP INITIAL
```

Saleae Results

TRUSTED SECURITY SERVICES

```
AT+CIPSTATUS

 OK
 STATE: IP INITIAL
```

```
AT+CIPCSGP=1,"CUSTOM.APN","",""

 OK
```

Saleae Results

TRUSTED SECURITY SERVICES

```
AT+CIPSTATUS

 OK
 STATE: IP INITIAL
```

```
AT+CIPCSGP=1,"CUSTOM.APN","",""

 OK
```

```
AT+CIPSTART="TCP","hidden.server.com",50138

 OK
 CONNECT OK
```

Saleae Results

TRUSTED SECURITY SERVICES

```
AT+CIPSTATUS

 OK
 STATE: IP INITIAL
```

```
AT+CIPCSGP=1,"CUSTOM.APN","",""

 OK
```

```
AT+CIPSTART="TCP","hidden.server.com",50138

 OK
 CONNECT OK
```

```
AT+CIPSEND

> !1,231445023129590;'\x1a'

 SEND OK
```

Actual footage of celebration

Understanding the comms

```
AT+CIPSEND
> !1,231445023129590;'\x1a'
 SEND OK
```

!1,231445023129590;'\x1a'

Understanding the comms

```
AT+CIPSEND
> !1,231445023129590;'\x1a'
 SEND OK
```

!1,231445023129590;'\x1a'

Understanding the comms

```
AT+CIPSEND
> !1,231445023129590;'\x1a'
 SEND OK
```

!1,231445023129590;'\x1a'

!1, + IMEI + ;\x1a

Understanding the comms

```
AT+CIPSEND
> !1,231445023129590;'\x1a'
 SEND OK
```

!1,231445023129590;'\x1a'

!1, + IMEI + ;\x1a

It's a login request :-)

What do we have here?

TRUSTED SECURITY SERVICES

- No authentication

What do we have here?

TRUSTED SECURITY SERVICES

- No authentication
- IMEI/Username enumeration

What do we have here?

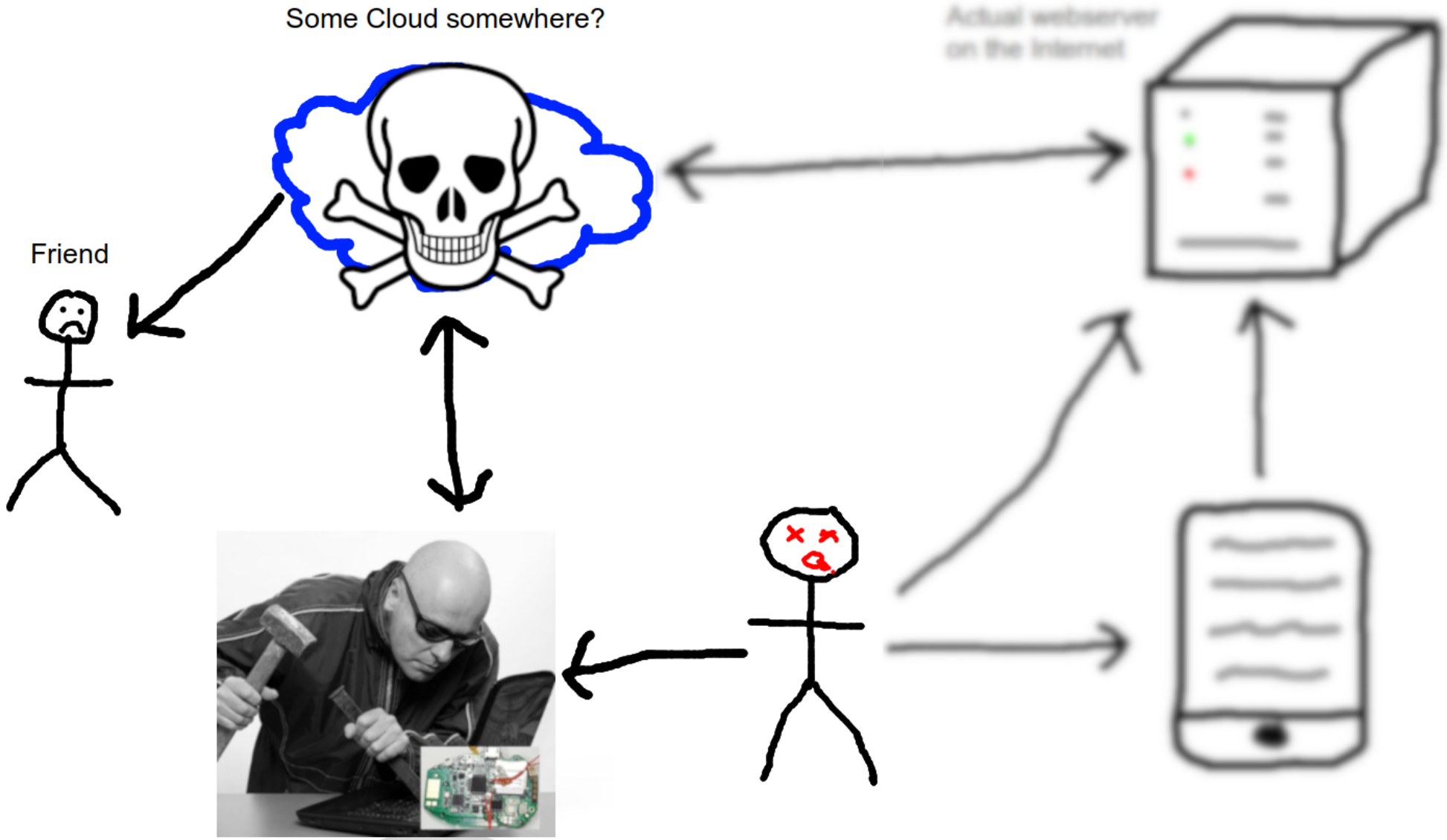
TRUSTED SECURITY SERVICES

- No authentication
- IMEI/Username enumeration
- Spoof location data and SoS messages

What do we have here?

TRUSTED SECURITY SERVICES

- No authentication
- IMEI/Username enumeration
- Spoof location data and SoS messages
- How bad could it be?

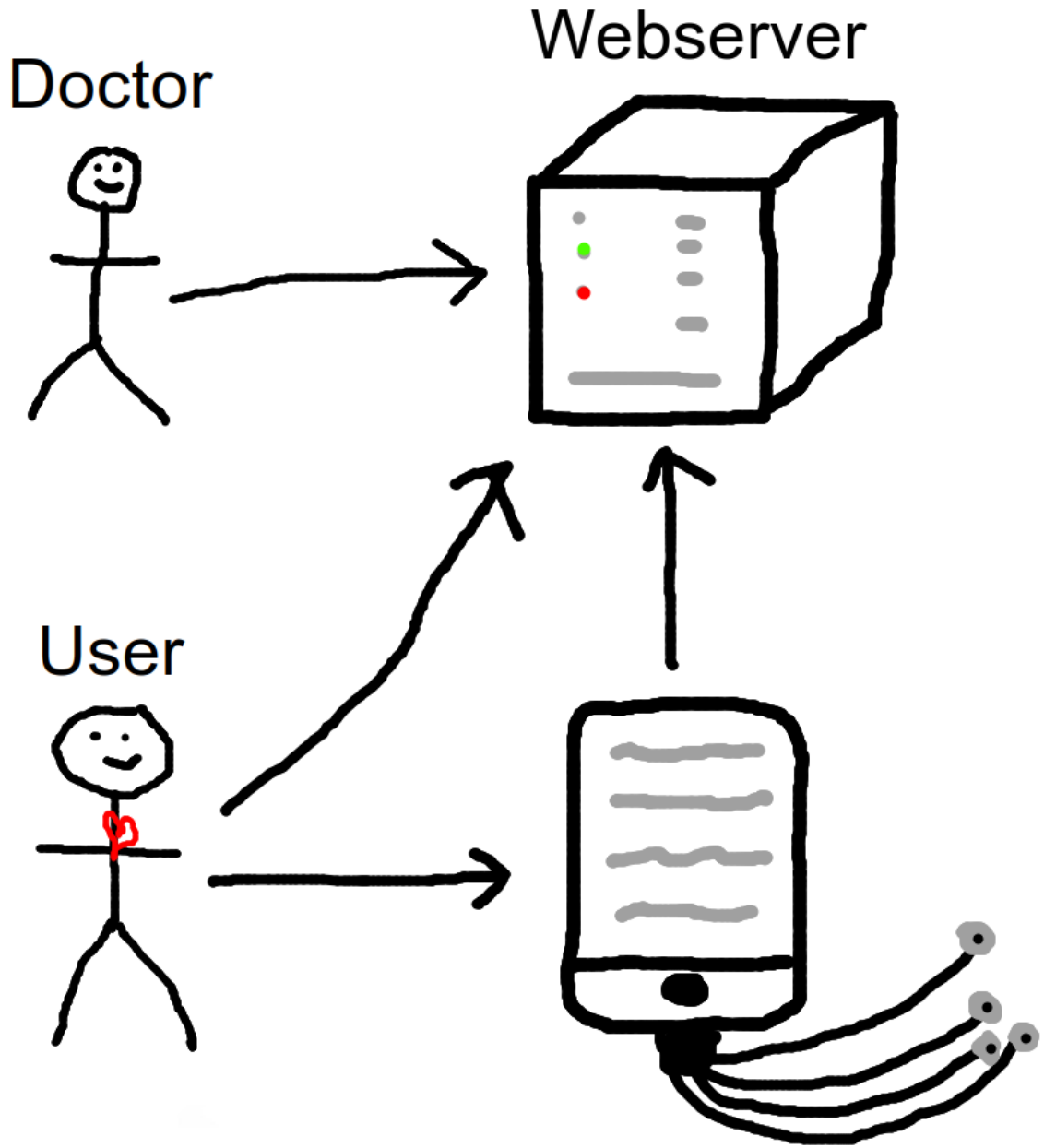

Some Cloud somewhere?
Actual webserver on the Internet
Friend

The ECG Test Solution

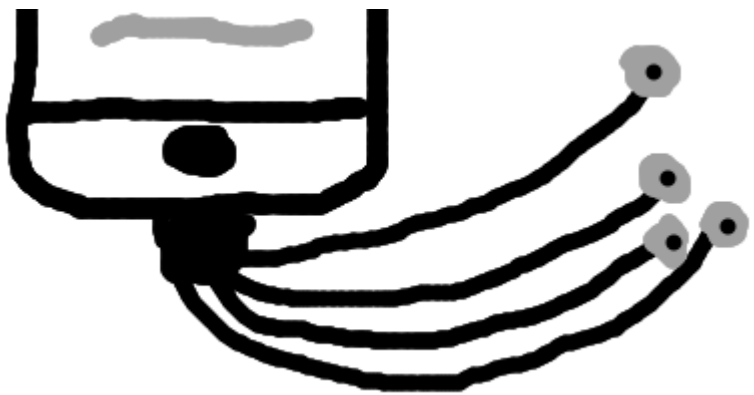
What is it?

TRUSTED SECURITY SERVICES

- Dongle attaches to chest
- Takes cardio measurements
- Instant reporting
- Shareable with doctor

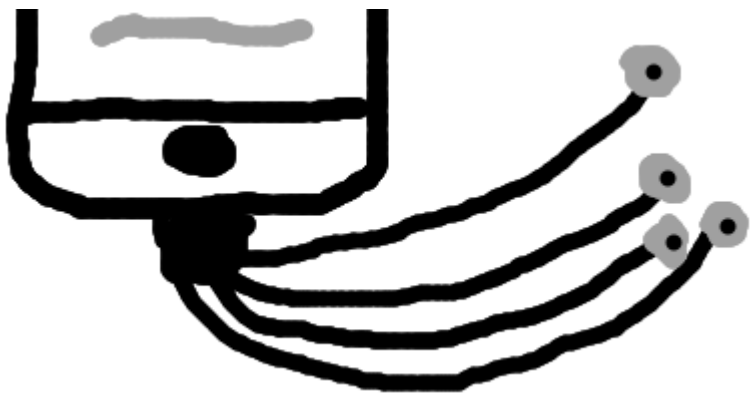

Webserver
Doctor
User

The Hardware



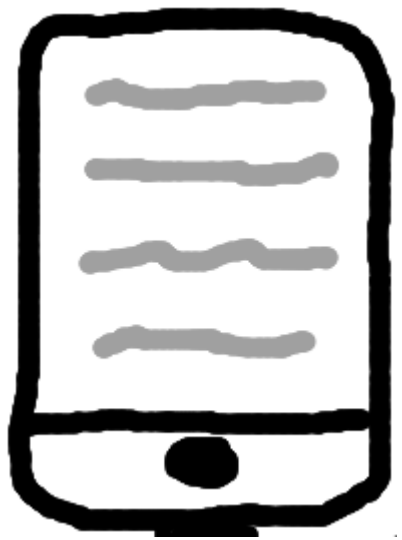
The Hardware

TRUSTED SECURITY SERVICES

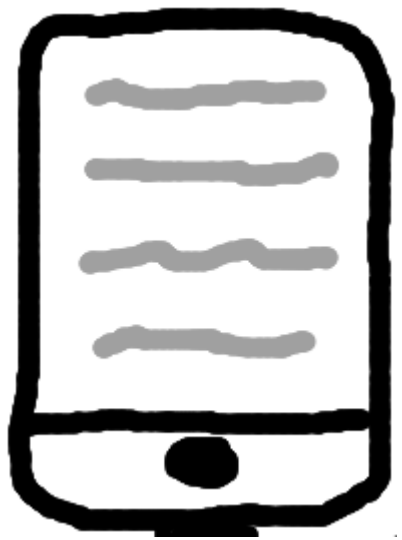


Not very interesting at all :-(

The App

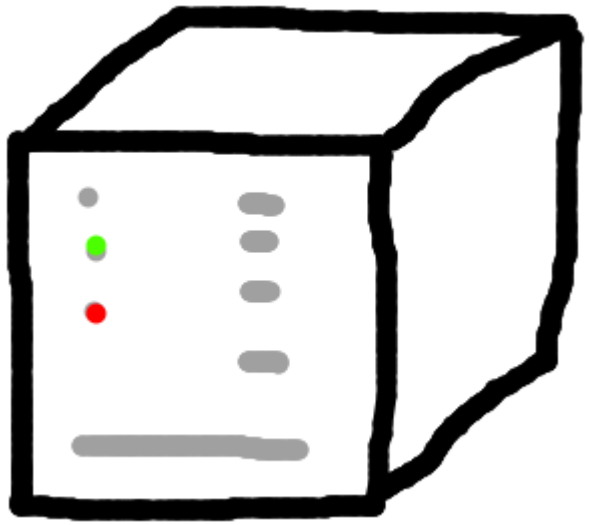


The App



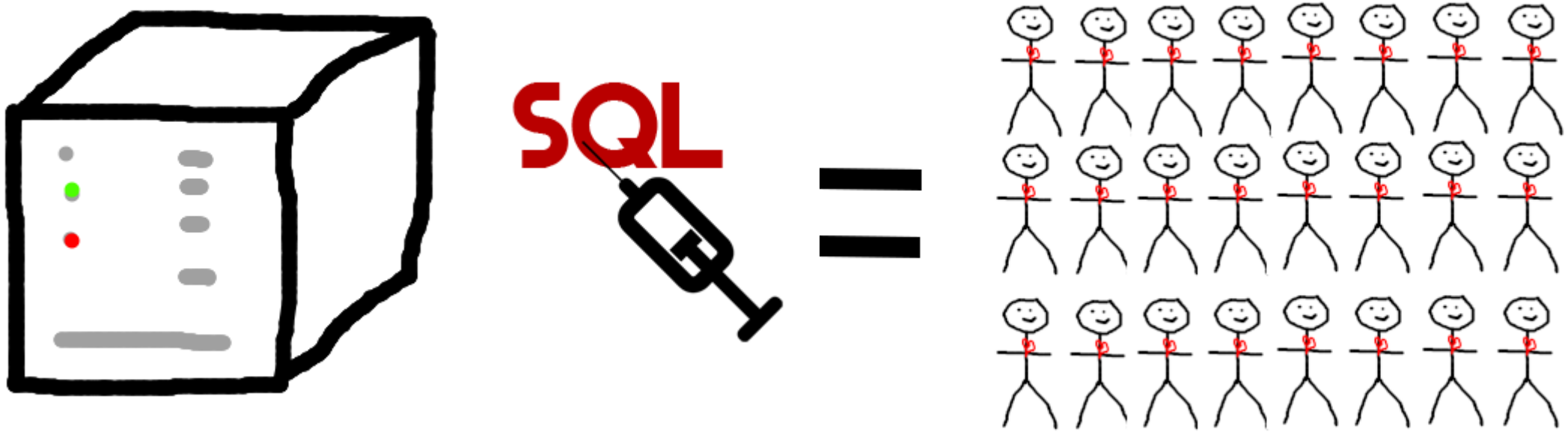
Also nothing of interest :-(

The Website



The Website

The Website



Why does this matter?


Forbes
8,899 views | Jul 15, 2018, 11:00 pm
Alexa, Are You A Spy? Israeli Startup Raises $12.5 Million So Governments Can Hack IoT
Thomas Brewster Forbes Staff
Security


BAIN & COMPANY
Cybersecurity Is the Key to Unlocking Demand in the Internet of Things
Enterprise customers would buy more IoT devices if vendors could ensure better security.
By Syed Ali, Ann Bosche and Frank Ford
June 13, 2018 • 11 min read

Where we come in

TRUSTED SECURITY SERVICES

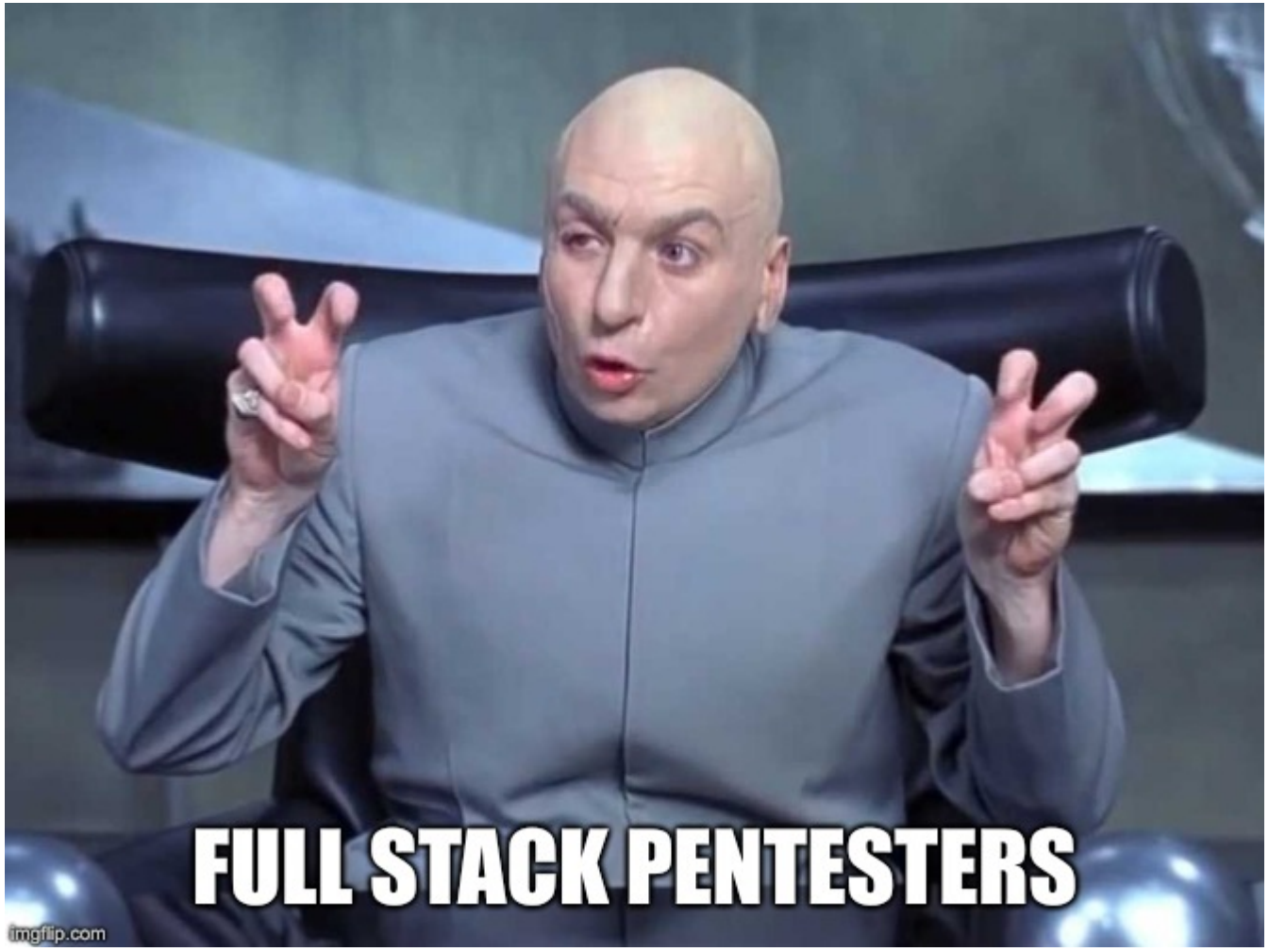
- Security architecture advice and guidance
- Educating product/solution decision makers
- Pentesting IoT solutions

Where we come in

TRUSTED SECURITY SERVICES

- Security architecture advice and guidance
- Educating product/solution decision makers
- Pentesting IoT solutions

- Wait for it…


FULL STACK PENTESTERS
imgflip.com

Conclusion

Parting thoughts

Parting thoughts

Thank you :-)

@jg_10

Now back to the CTF...