

EMERGING TECHNOLOGIES FOR THE ENTERPRISE CONFERENCE



WIFI

ETE2019



HASHTAG

#PhillyETE



SESSION Q&A

Visit [sli.do](#)

#PHILLYETE

Presented By



PINNACLE²¹



VISTAR MEDIA



WTF IoT or IoΤ FTW?

Don Coleman - Chariot Solutions





The Verge

@verge

Follow



Samsung's new fridge will ping your phone if you leave the door open
theverge.com/2019/1/7/18169...





Internet of Shit

@internetofshit

Following



why the heck doesn't it just close the door itself if it's so smart



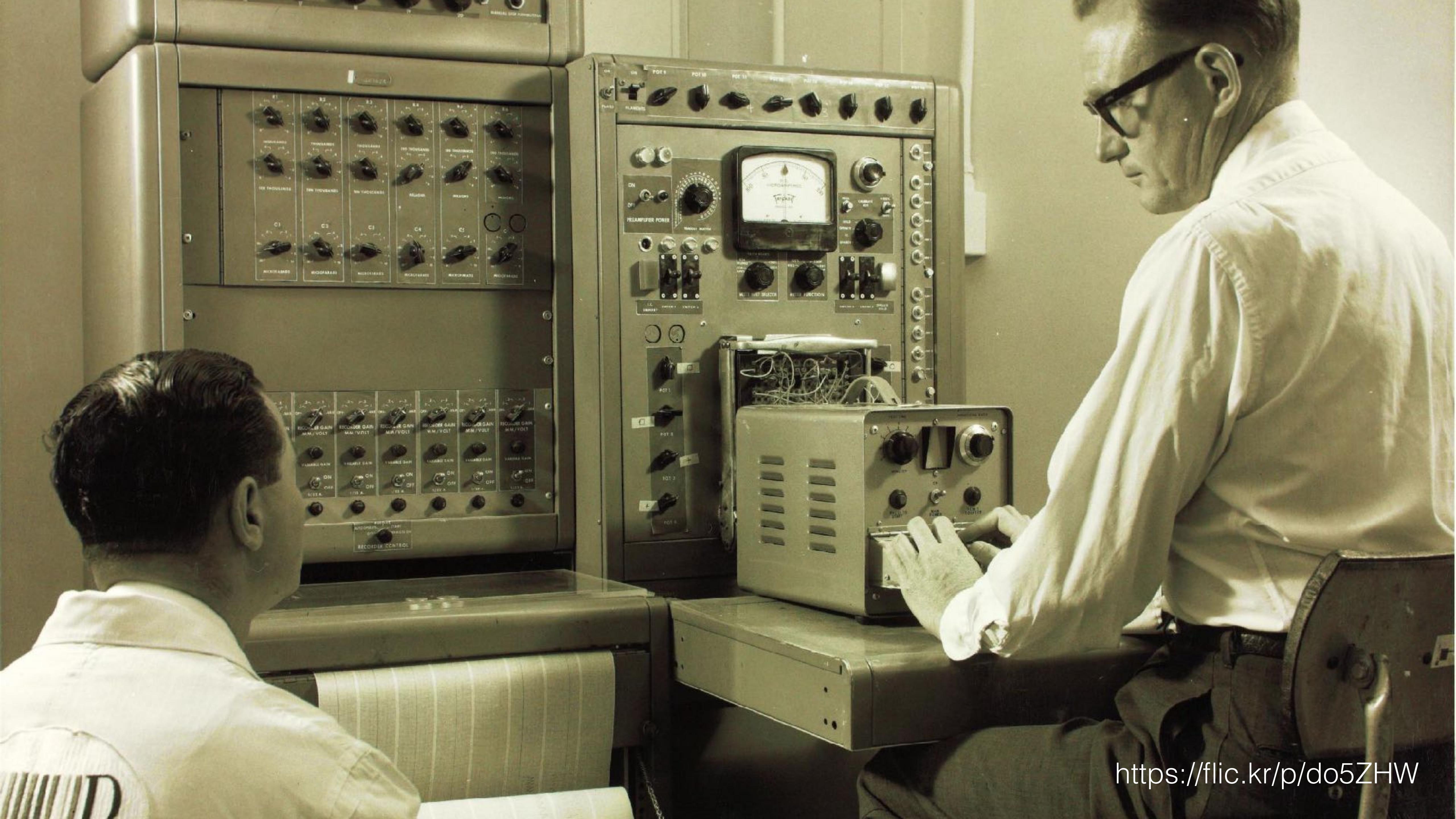
The Verge ✅ @verge

Samsung's new fridge will ping your phone if you leave the door open theverge.com/2019/1/7/18169...

4:42 PM - 13 Jan 2019

Hype Cycle for Emerging Technologies, 2011





<https://flic.kr/p/do5ZHW>

The Computer for the 21st Century

Specialized elements of hardware and software, connected by wires, radio waves and infrared, will be so ubiquitous that no one will notice their presence

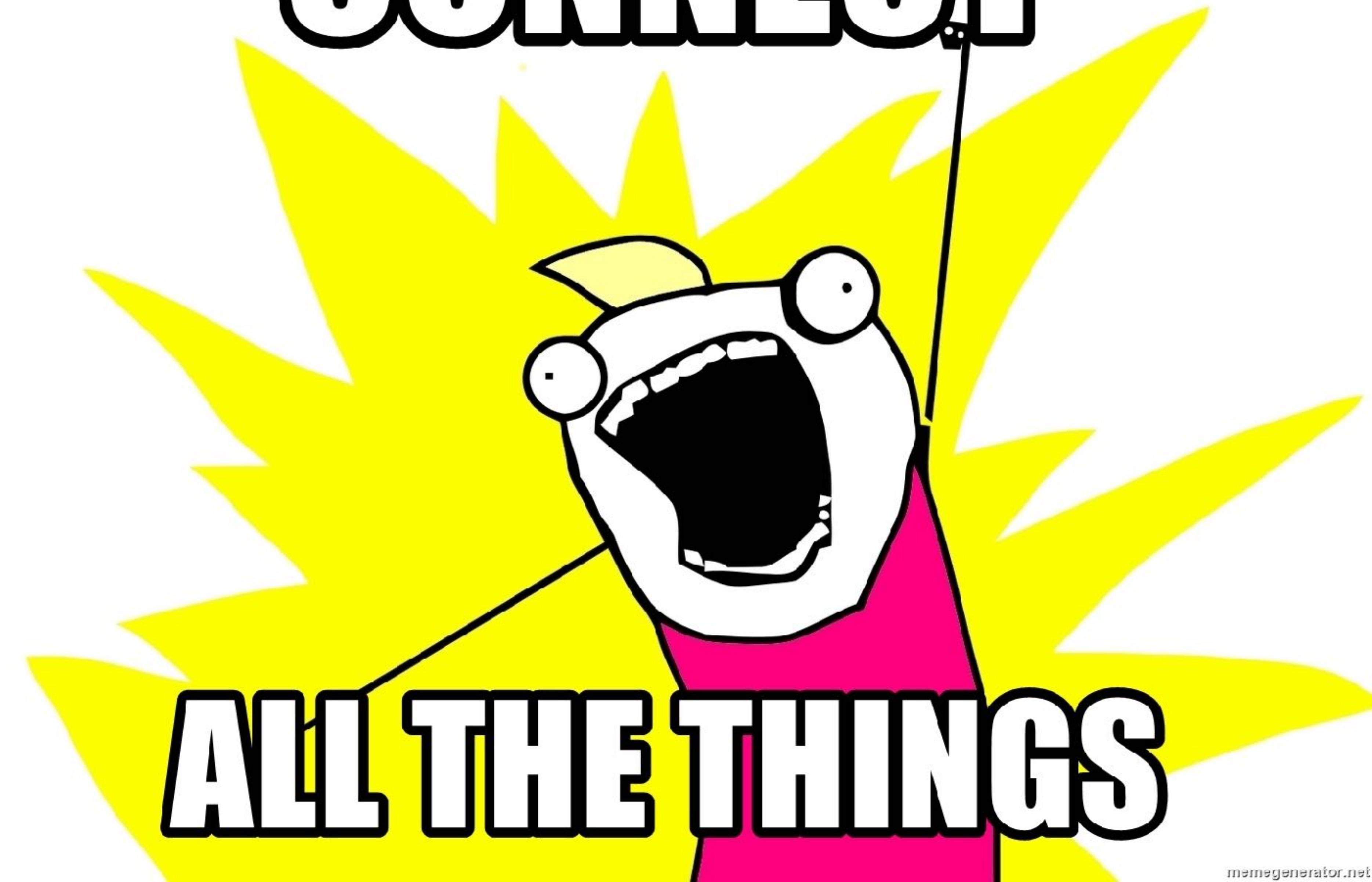
by Mark Weiser

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.

is approachable only through complex jargon that has nothing to do with the tasks for which people use computers. The state of the art is perhaps analogous to the period when scribes had to

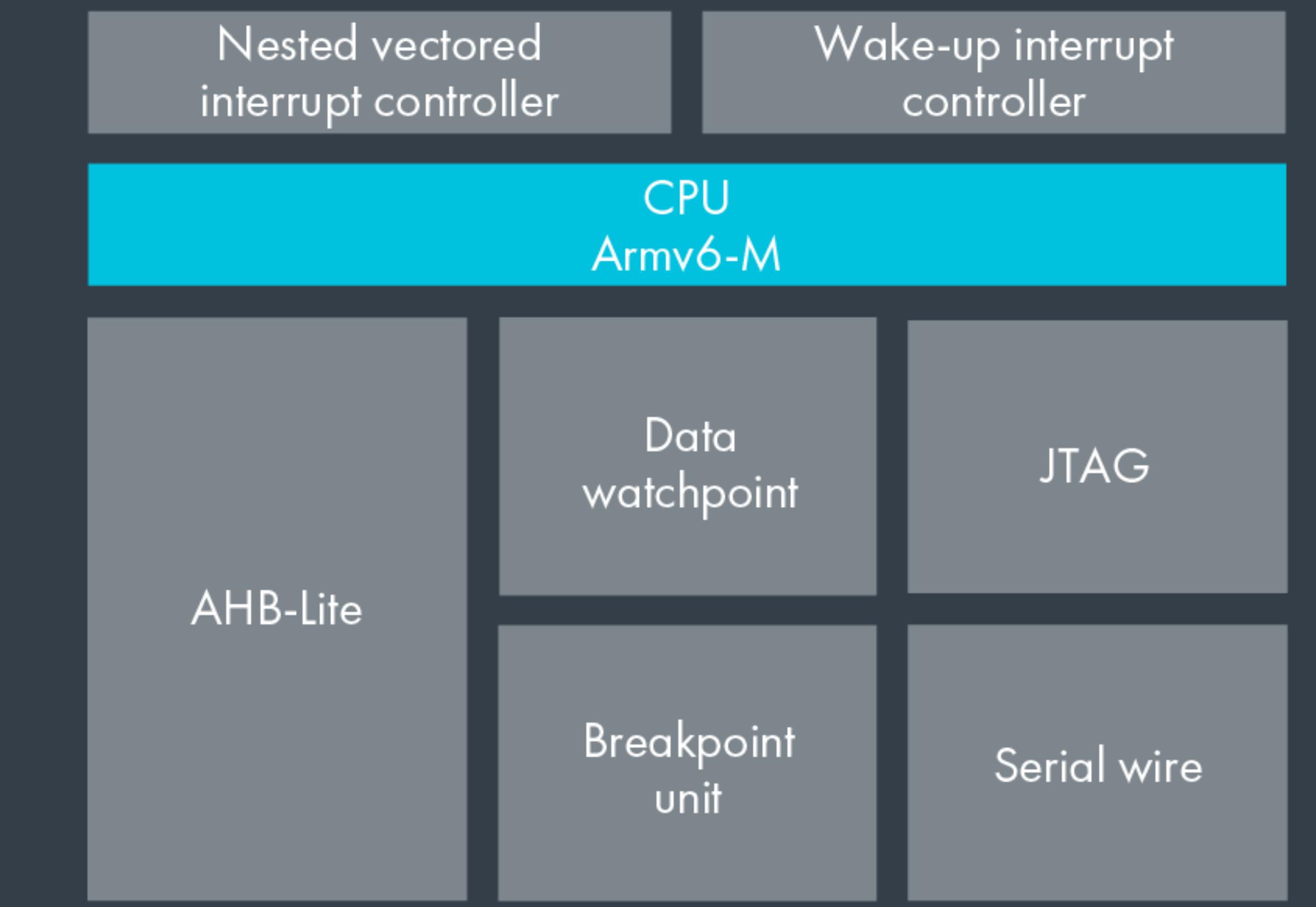
The idea of integrating computers seamlessly into the world at large is counter to a number of present trends. "Ubiquitous computing" in context does not mean just comp-

CONNECT

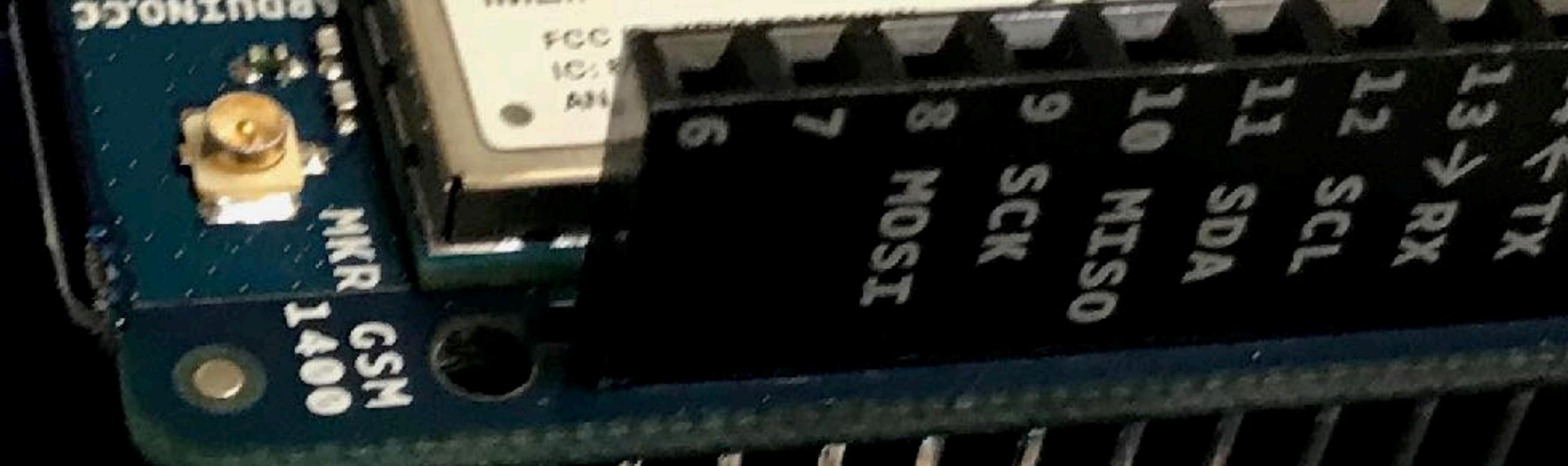


ALL THE THINGS

arm CORTEX®-M0



Hologram





No one asks for an IoT project



<https://flic.kr/p/awo1tu>

PLUS!

VEEDER-ROOT



MAY 4, 2017 4:12:24 PM
T 2:PROBE OUT

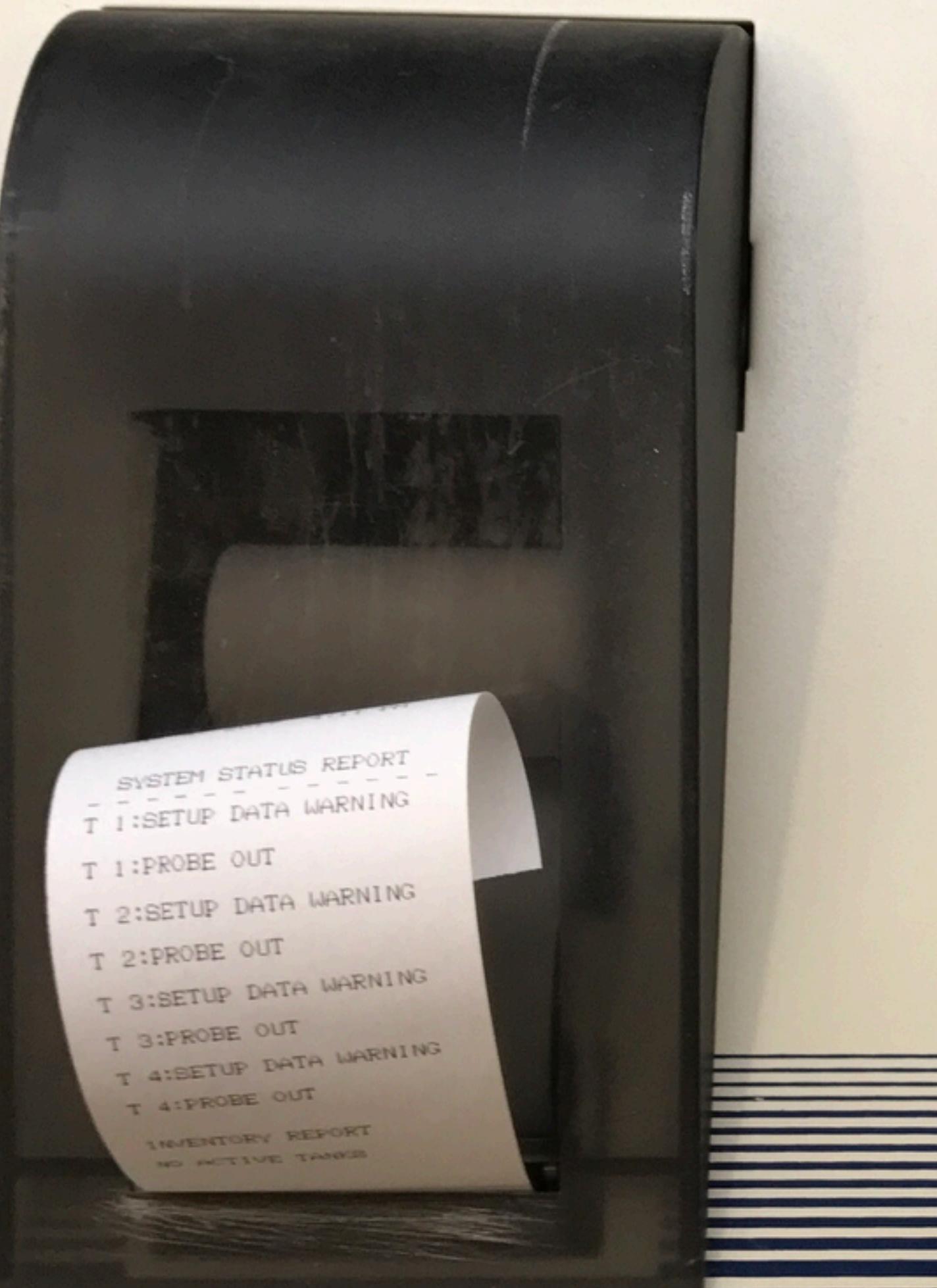
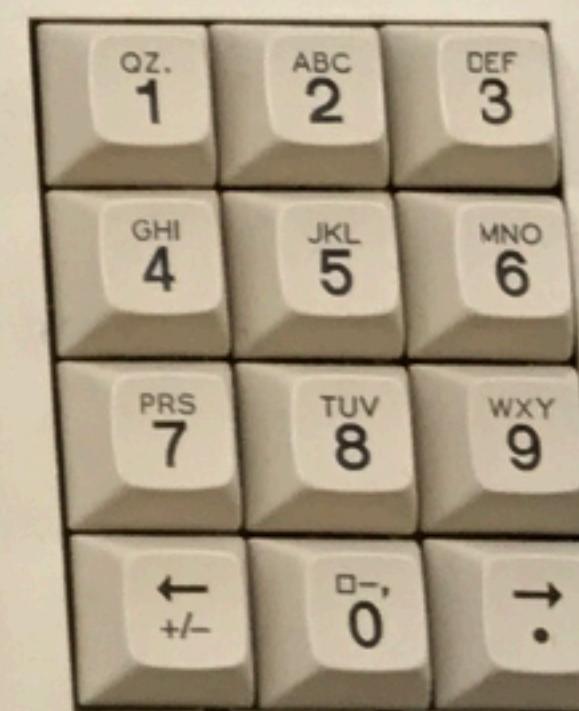
ALARM



WARNING

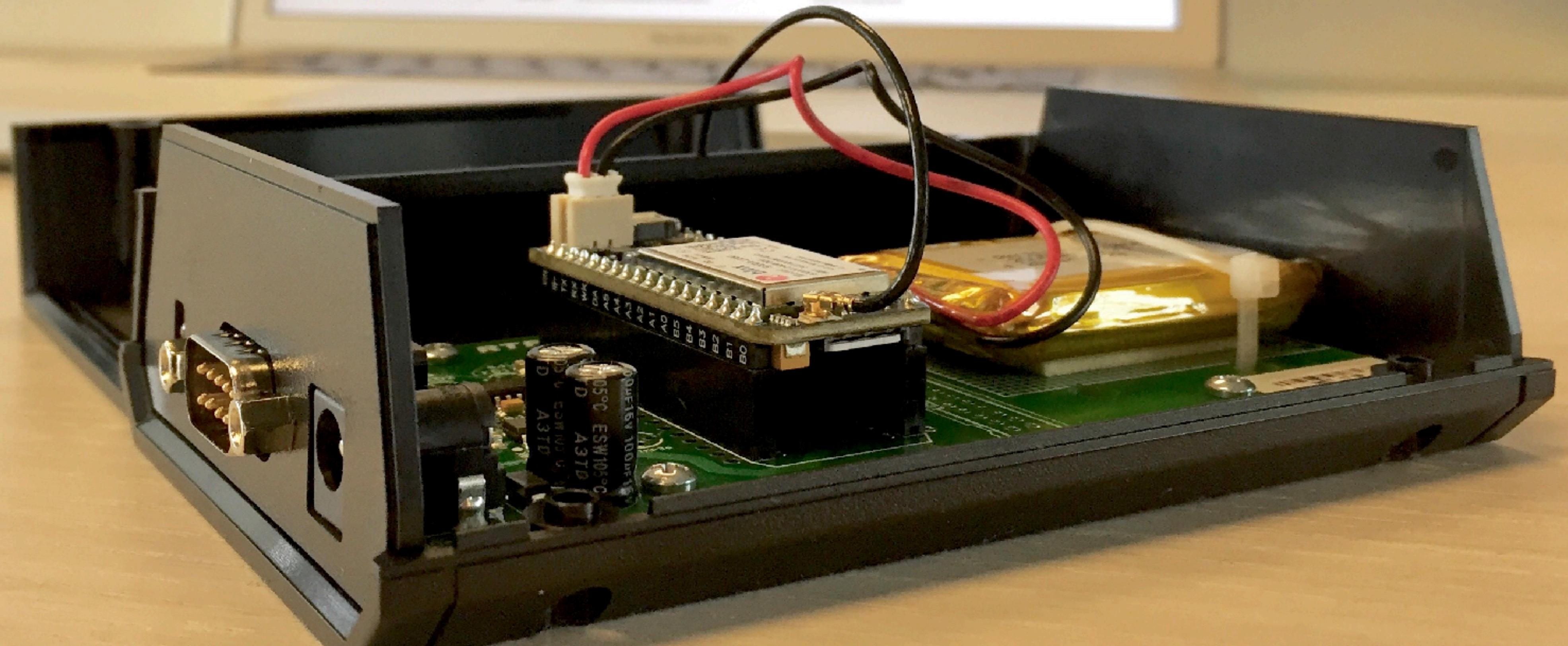


POWER

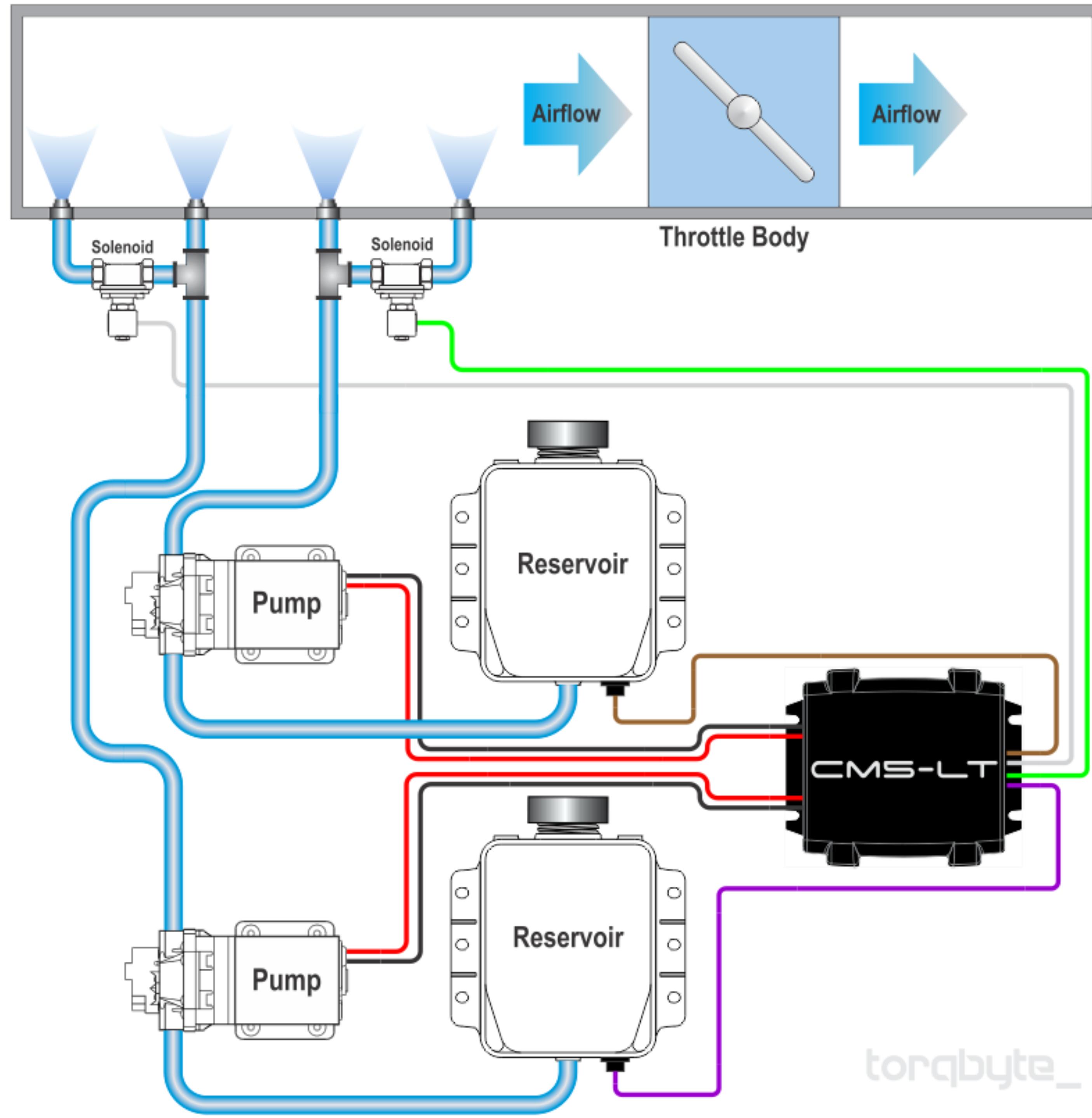


VEEDER-ROOT

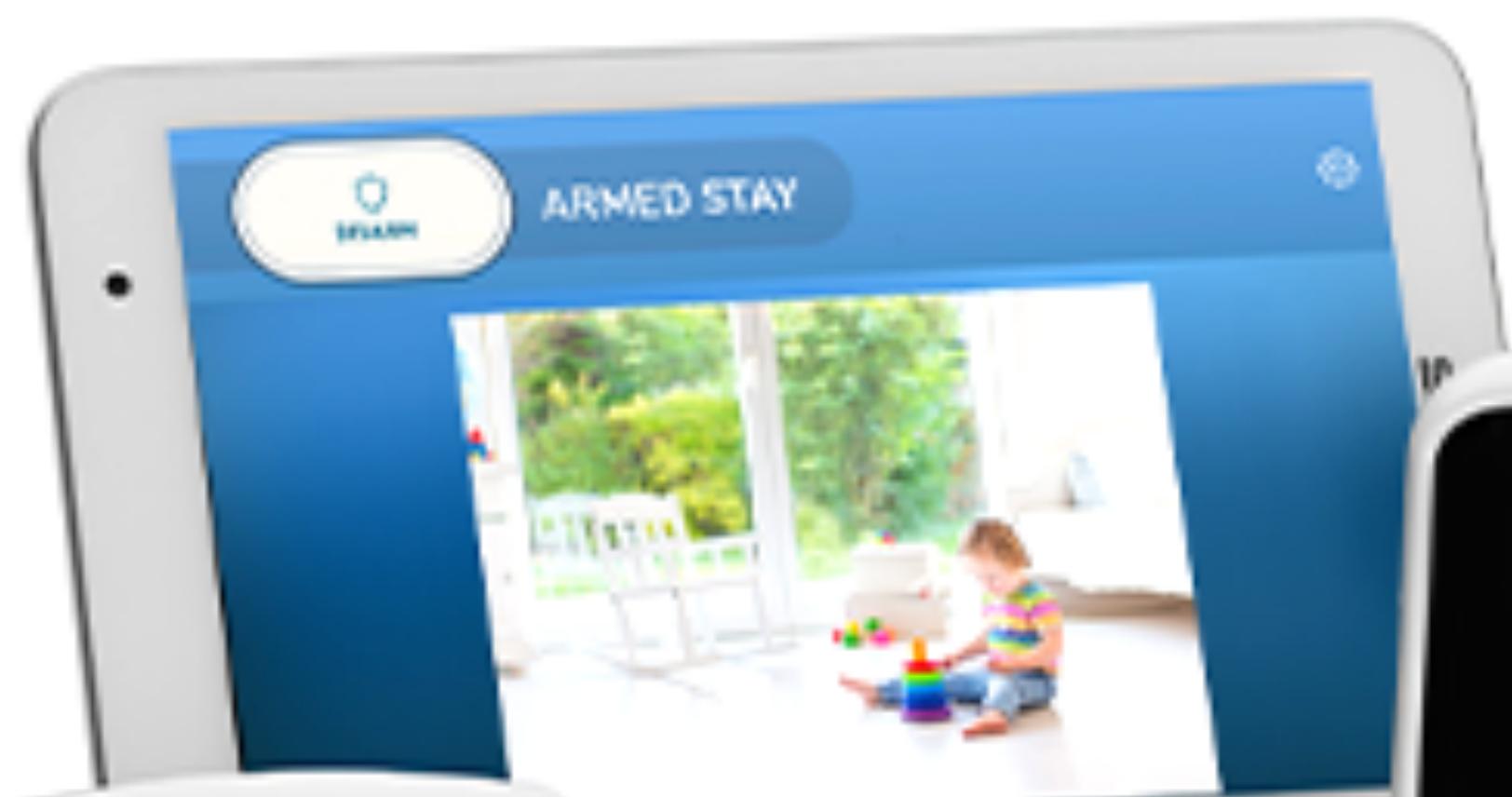
UST Monitoring System







torqbyte_









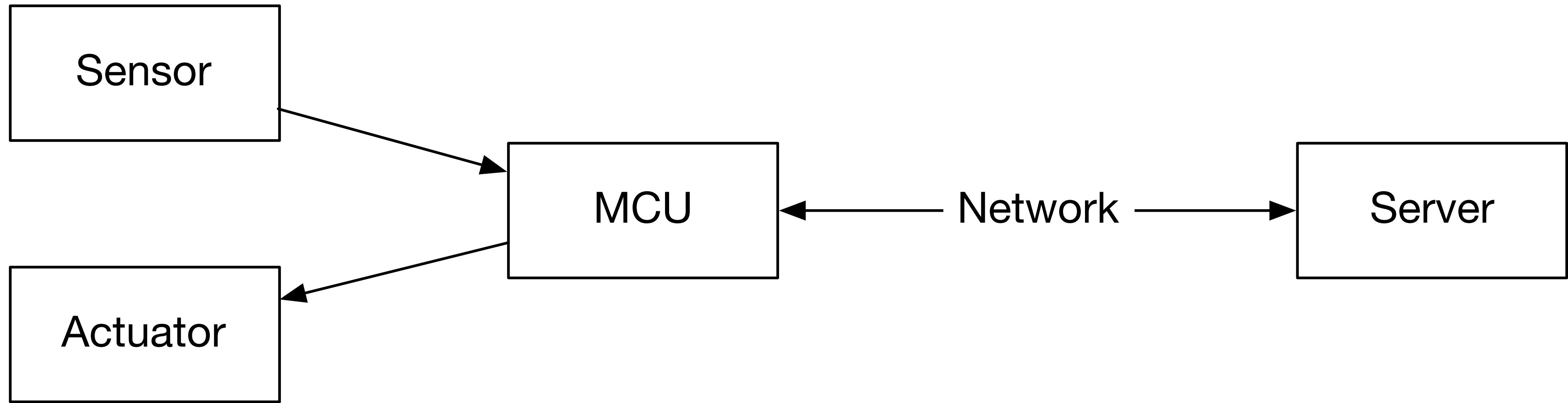
THE WORLD'S FIRST WIRELESS NPK SENSOR

Get the most detailed soil quality data available, via a single probe with 26 sensors reporting soil moisture, salinity, and NPK at three different depths, as well as aeration, respiration, air temperature, light, and humidity.

No wires. Nothing to catch or snag. Easy to install and built to stand up to the wear and tear of your farm.

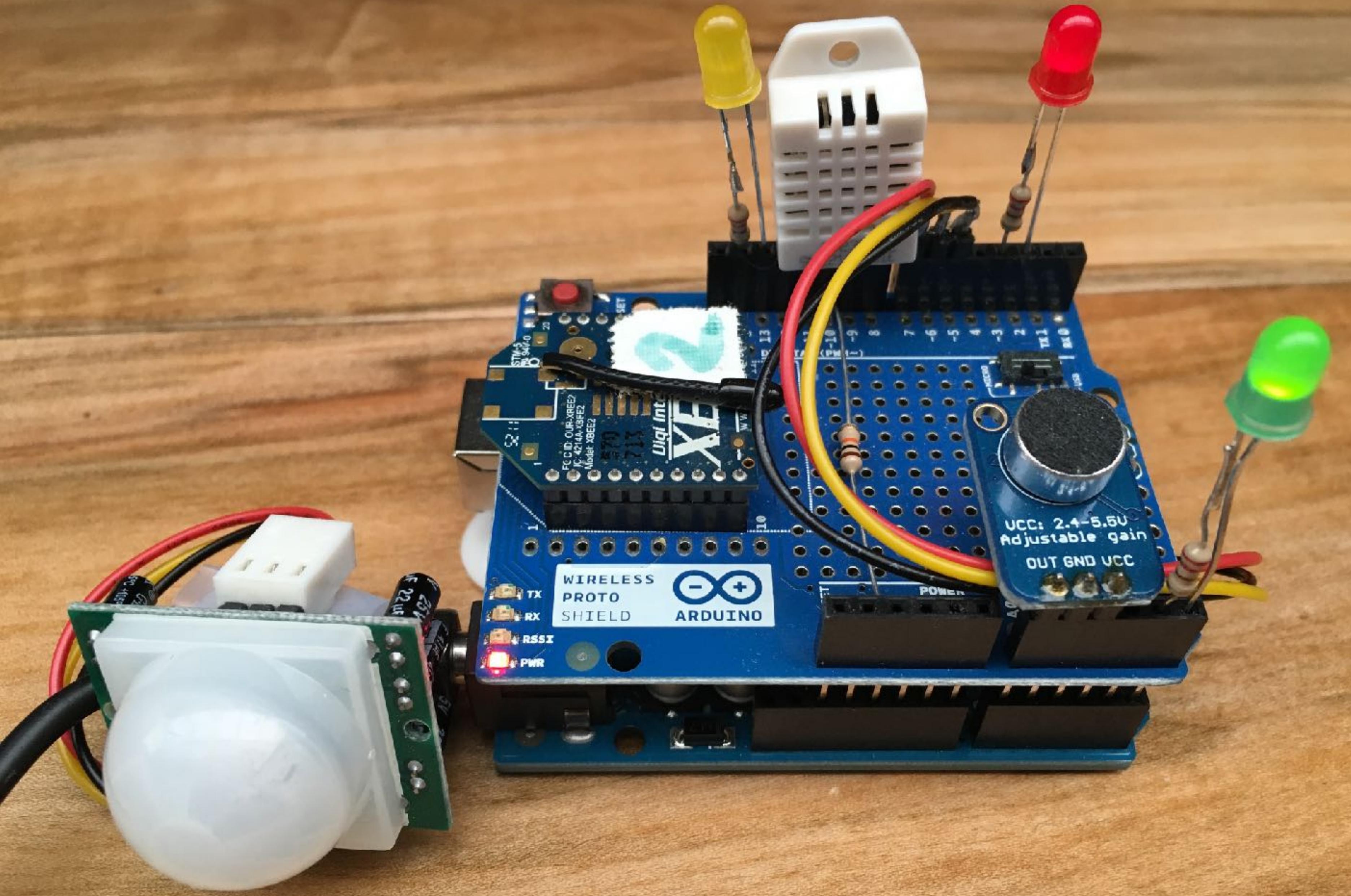
[Learn More →](#)

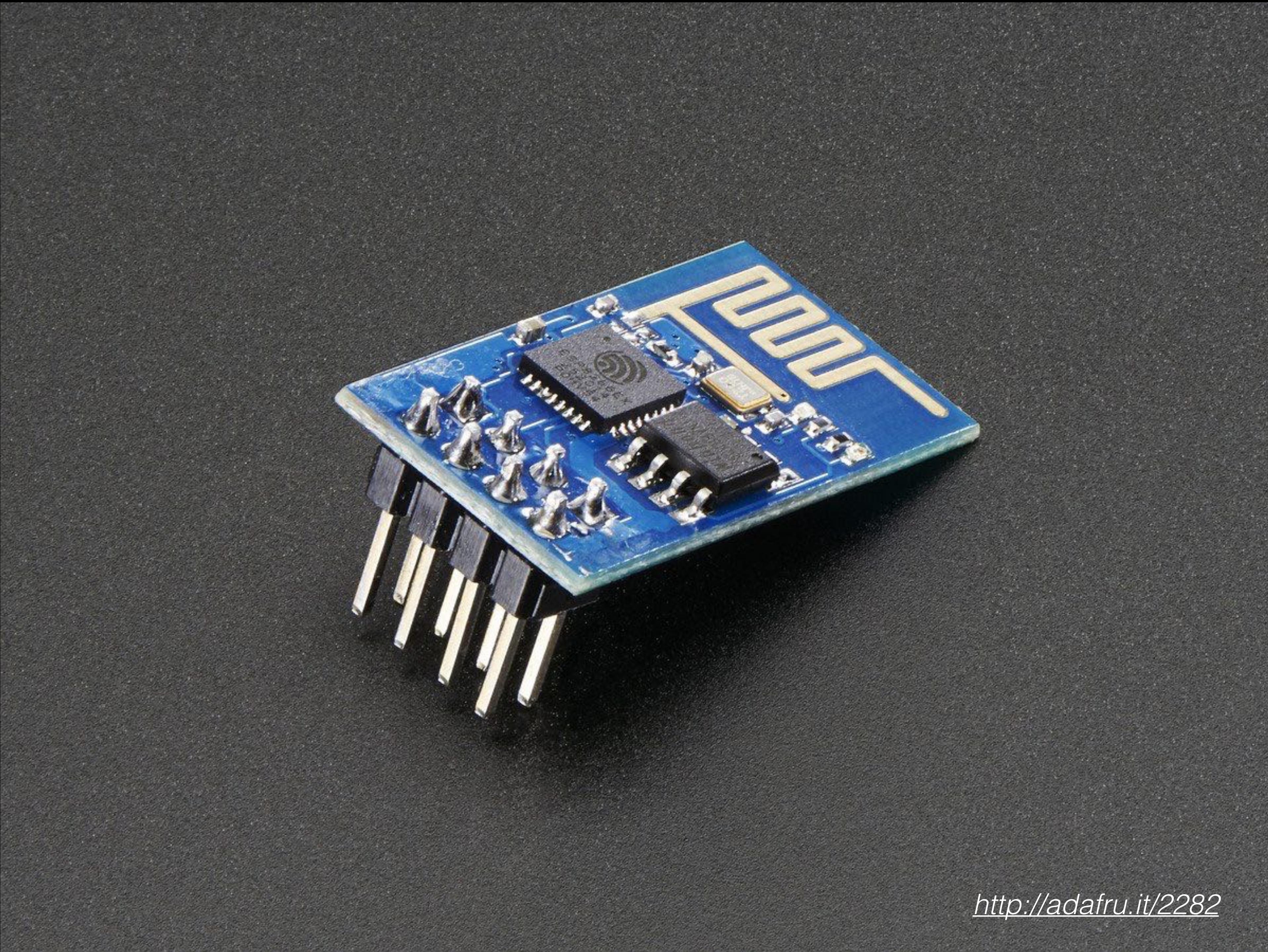
[Pre-Order Your Probes Now](#)



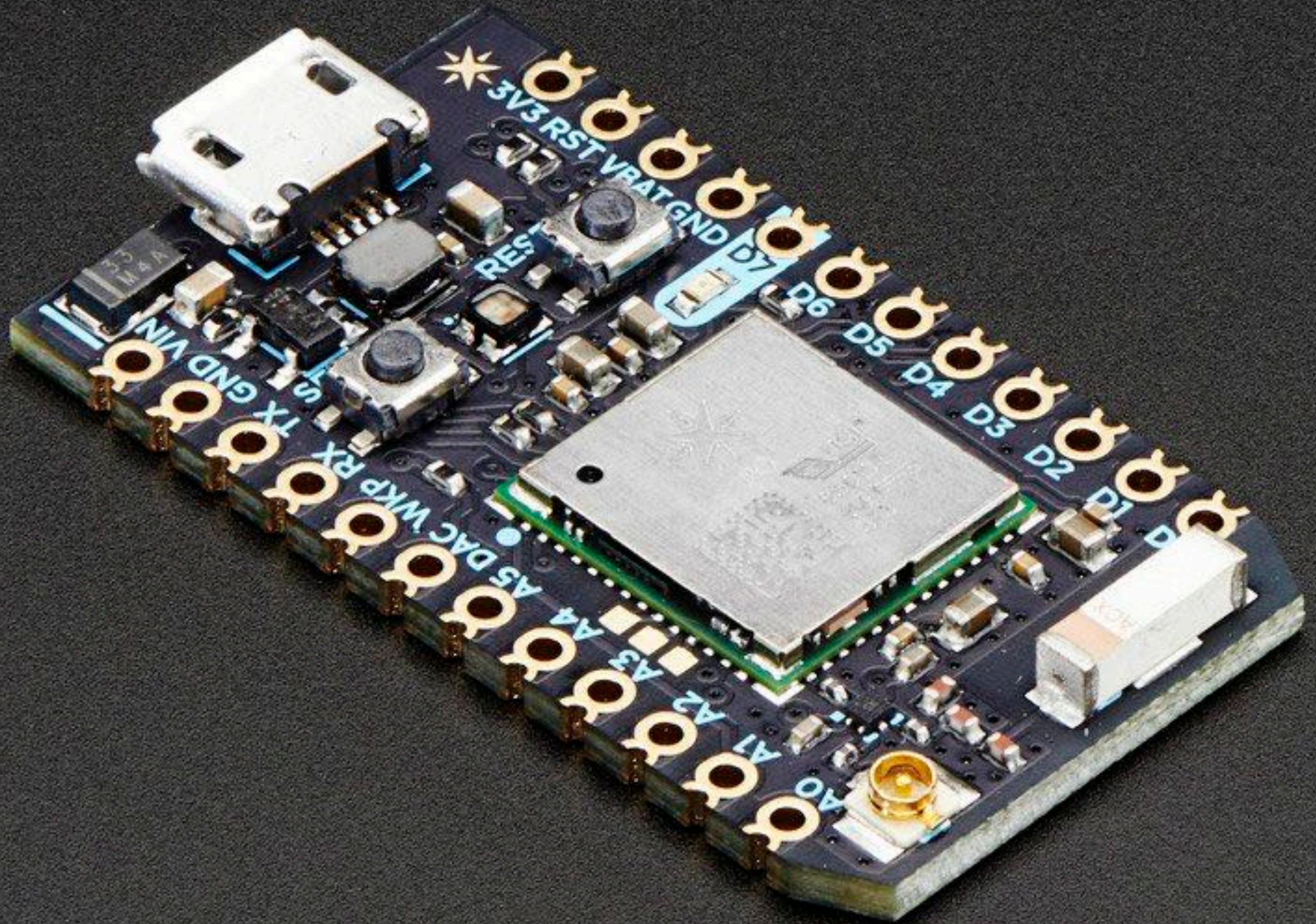
Transports

Protocols





<http://adafru.it/2282>



<http://adafru.it/2722>





AWS IoT



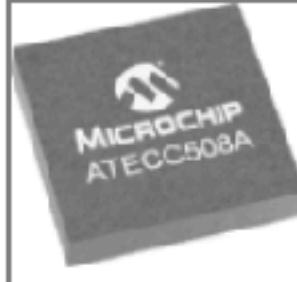
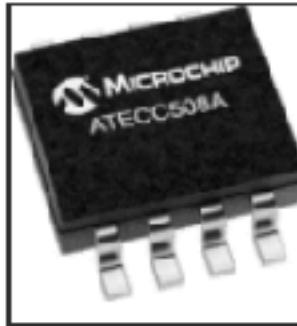
Products

Applications

Design

Sample and
Buy

About



ATECC508A

Status: In Production

[View Datasheet](#)

Features:

- Easy way to run ECDSA and ECDH Key Agreement
- ECDH key agreement makes encryption/decryption easy
- Ideal for IoT node security
- Authentication without the need for secure storage in the host
- No requirement for high-speed computing in client devices
- Cryptographic accelerator with Secure Hardware-based Key Storage



Nathan Ruser
@Nrg8000

Follow

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option).
medium.com/@strava/strava-engineering/strava-global-heatmap-13-trillion-gps-points-1000x1000 ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable



The best gift is more of you. Starting at \$99.* Order by 5/8 10am PST to get by Mother's Day.

portal

Home Products Privacy Support Log In to 

portal

from **facebook**

Starting at \$199 \$99

through Mother's Day.*

A smarter way to video call. Alexa Built-in.
And so much more.

[Buy Now](#)

 Watch to Learn More



port portal.portal.facebook.com

IMPORTANT -- READ CAREFULLY: THIS LICENSE AGREEMENT IS A LEGAL CONTRACT BETWEEN YOU AND JOHN DEERE SHARED SERVICES, INC., A CORPORATION HAVING A PRINCIPAL ADDRESS OF ONE JOHN DEERE PLACE, MOLINE, IL 61265 (THE "LICENSOR"). THIS LICENSE AGREEMENT GOVERNS YOUR USE OF ANY SOFTWARE AND OTHER MATERIALS (SOFTWARE AND OTHER MATERIALS INDIVIDUALLY OR COLLECTIVELY REFERRED TO AS "LICENSED MATERIALS" OR "LM") THAT IS (1) PROVIDED BY LICENSOR OR ITS AFFILIATES; (2) EMBEDDED OR INSTALLED IN, OR ASSOCIATED WITH, ANY DISPLAY, ENGINE CONTROL UNIT, INVERTER, CONTROLLER, ELECTRONICS MODULE, SENSOR, ACTUATOR, OR COMPUTING UNIT (INDIVIDUALLY OR COLLECTIVELY "LICENSED PRODUCTS" OR "LP") OF JOHN DEERE EQUIPMENT OR OF OTHER EQUIPMENT THAT IS MADE A PART OF A SALE OR LEASE TO YOU (EITHER OR BOTH JOHN DEERE EQUIPMENT AND SUCH OTHER EQUIPMENT REFERRED TO AS "AUTHORIZED EQUIPMENT"); AND (3) NOT OTHERWISE LICENSED BY A SEPARATE WRITTEN AGREEMENT BETWEEN YOU AND LICENSOR OR ITS AFFILIATES, OR (4) NOT OTHERWISE LICENSED BY A THIRD PARTY (OR SUPPLIER).

BY ACTIVATING OR OTHERWISE USING THE LP, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT WITH RESPECT TO THE LM THAT HAVE BEEN PRE-INSTALLED ON YOUR LP. YOU AGREE THAT THIS LICENSE AGREEMENT, INCLUDING THE WARRANTY DISCLAIMERS, LIMITATIONS OF LIABILITY, TERMINATION, AND ARBITRATION PROVISIONS BELOW, IS BINDING UPON YOU, AND UPON ANY COMPANY ON WHOSE BEHALF YOU USE THE LM AND LP AS WELL AS THE EMPLOYEES OF ANY SUCH COMPANY (COLLECTIVELY REFERRED TO AS "YOU" IN THIS LICENSE AGREEMENT). IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE AGREEMENT, OR IF YOU ARE NOT AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF YOUR COMPANY OR ITS EMPLOYEES, DECLINE THESE TERMS AND CONDITIONS AND DO NOT USE THE LP OR THE AUTHORIZED EQUIPMENT. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE LM BETWEEN YOU AND THE LICENSOR AND IT REPLACES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN YOU AND THE LICENSOR.

1. Definitions. Licensed Materials ("LM") shall mean any Software, data files, documentation, engine calibration tables, proprietary data messages, and controller area network (CAN) data messages that are in or communicated to or from any LP (e.g., to monitor, diagnose, or operate the Authorized Equipment). Data files shall include but not be limited to any data structure that adjusts engine control parameters, such as fuel metering, fuel injection rate, fuel injection timing, fuel pressure, engine speed versus torque relationship, intake boost pressure, fuel-to-air ratio or engine timing.

2. License. Licensor hereby grants to you, and you accept, a nonexclusive license to use the LM in machine-readable, object code form, only as authorized in this License Agreement and the applicable provisions of the Operators' Manuals, which you agree to review carefully prior to using the LM. The LM may be used only on the LP in which it was initially installed and solely in conjunction with the Authorized Equipment in which it was initially installed; or, in the event of the inoperability of that LP, on a replacement LP provided to you by an authorized dealer pursuant to the Limited Warranty of Section

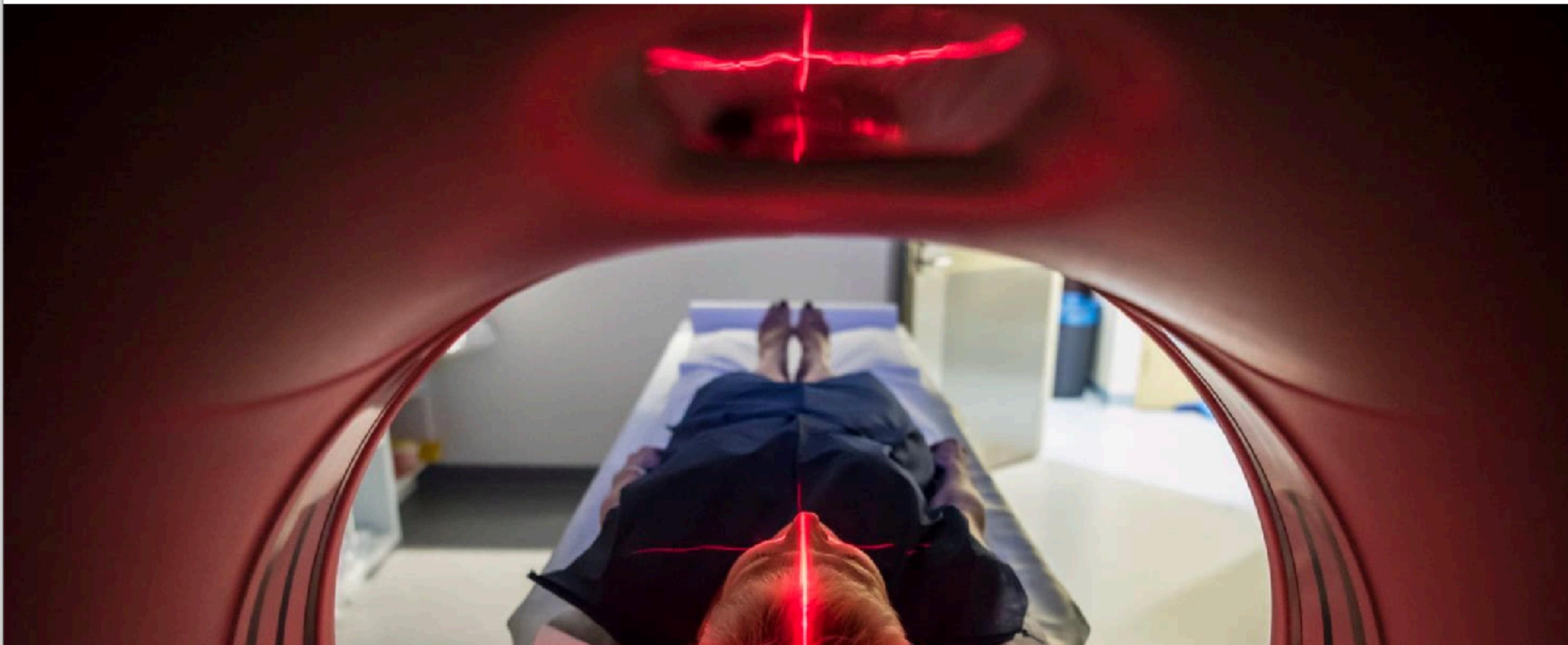
the LM, including associated intellectual property rights, are and shall remain with Licensor, its affiliates, and their licensors. This License Agreement does not convey to you any title or interest in or to the LM, but only a limited right of use revocable in accordance with the terms of this License Agreement. Licensor and its Affiliates reserve all worldwide rights not expressly granted under this Agreement.

4. License Restrictions, Reverse Engineering. You may not reproduce, prepare derivative works based on, disclose, publish, distribute, rent, lease, modify, loan, display, or perform the LM or any part thereof. You may not reverse engineer, decompile, translate, adapt, or disassemble the LM, nor shall you attempt to create the source code from the object code for the Software. You may not transmit the LM over any network or via a hacking device, although you may use the LM to make transmissions of diagnostic data messages that are authorized by Licensor and you may receive Software updates authorized by Licensor. You also agree not to permit any third party acting under your control to do any of the foregoing activities related to reverse engineering of the Licensed Materials. You agree not to remove or obliterate any copyright, trademark or other proprietary rights notices from the LM, except as expressly permitted in writing by Licensor or its licensors or expressly

Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists

Researchers in Israel created malware to draw attention to serious security weaknesses in medical imaging equipment and networks.

Kim Zetter • April 3



Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane

Security researchers from Tencent have demonstrated a way to use physical attacks to spoof Tesla's autopilot

Evan Ackerman

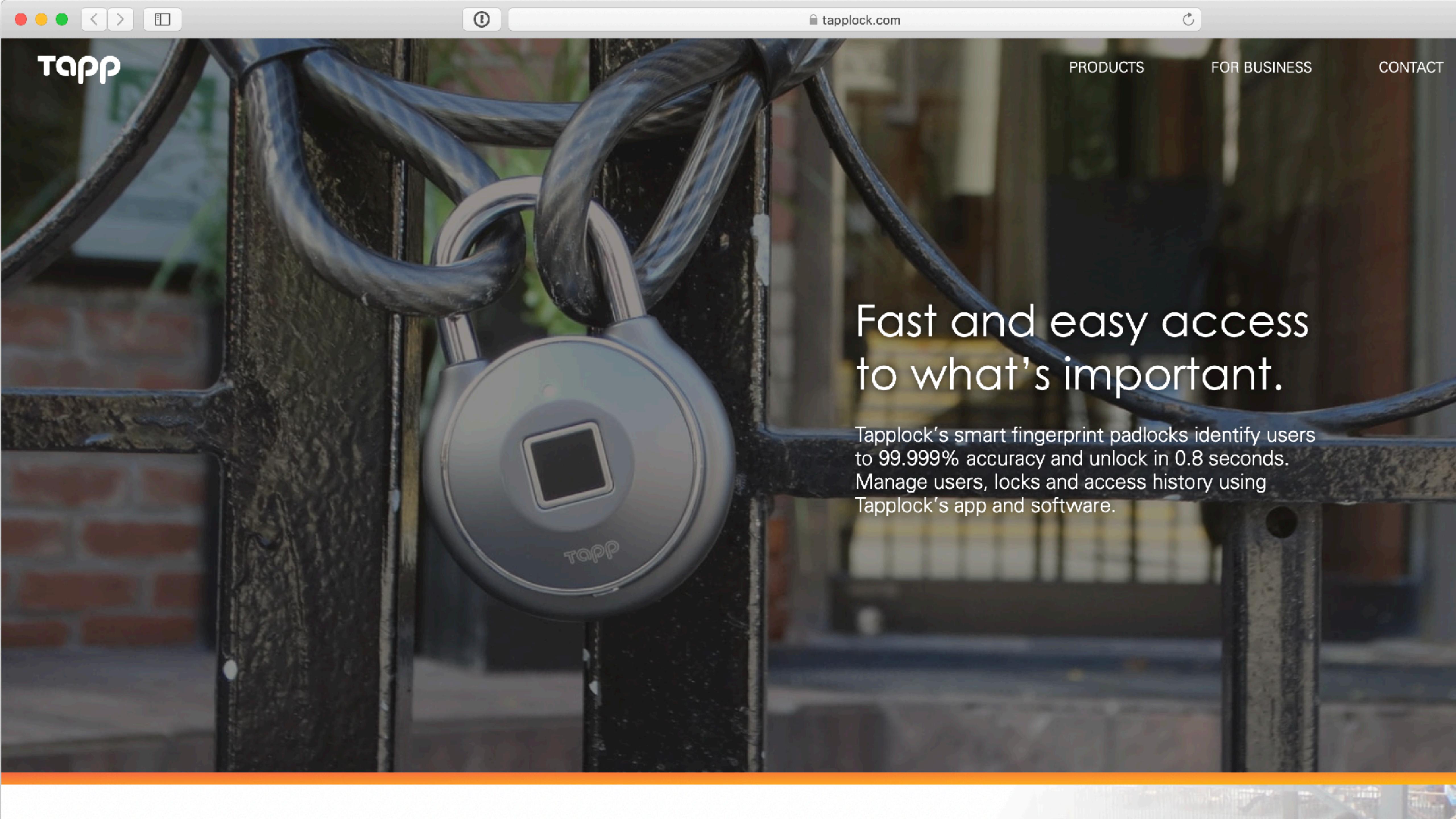






How A Researcher Hacked iKettles to Steal WiFi Passwords All Across London

Adarsh Verma • October 21, 2015



Fast and easy access to what's important.

Tapplock's smart fingerprint padlocks identify users to 99.999% accuracy and unlock in 0.8 seconds. Manage users, locks and access history using Tapplock's app and software.

BLOG: INTERNET OF THINGS

Totally Pwnning the Tapplock Smart Lock



Share



TL;DR – How to open a Tapplock over BLE in under two seconds:



Categories

Show all

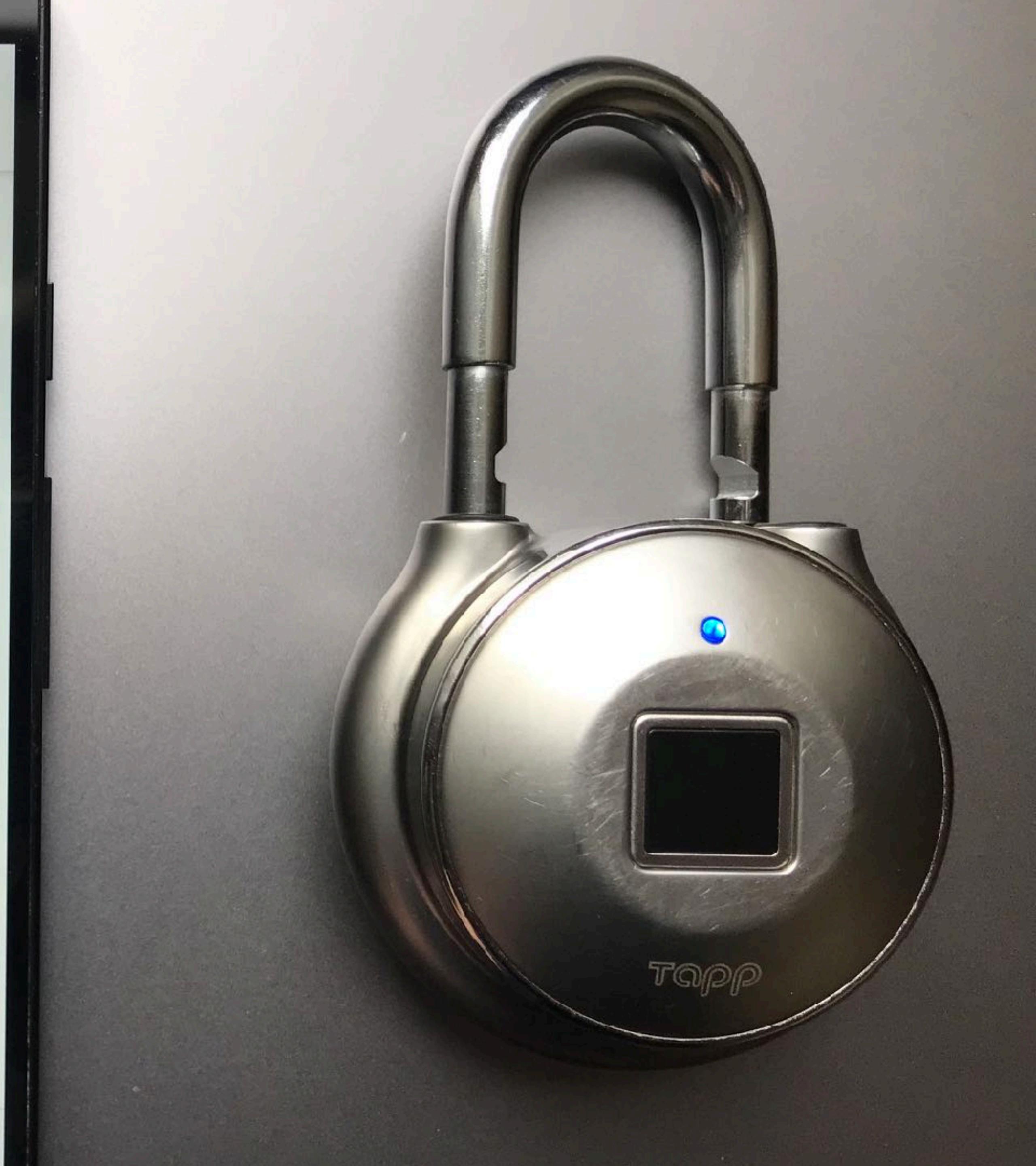
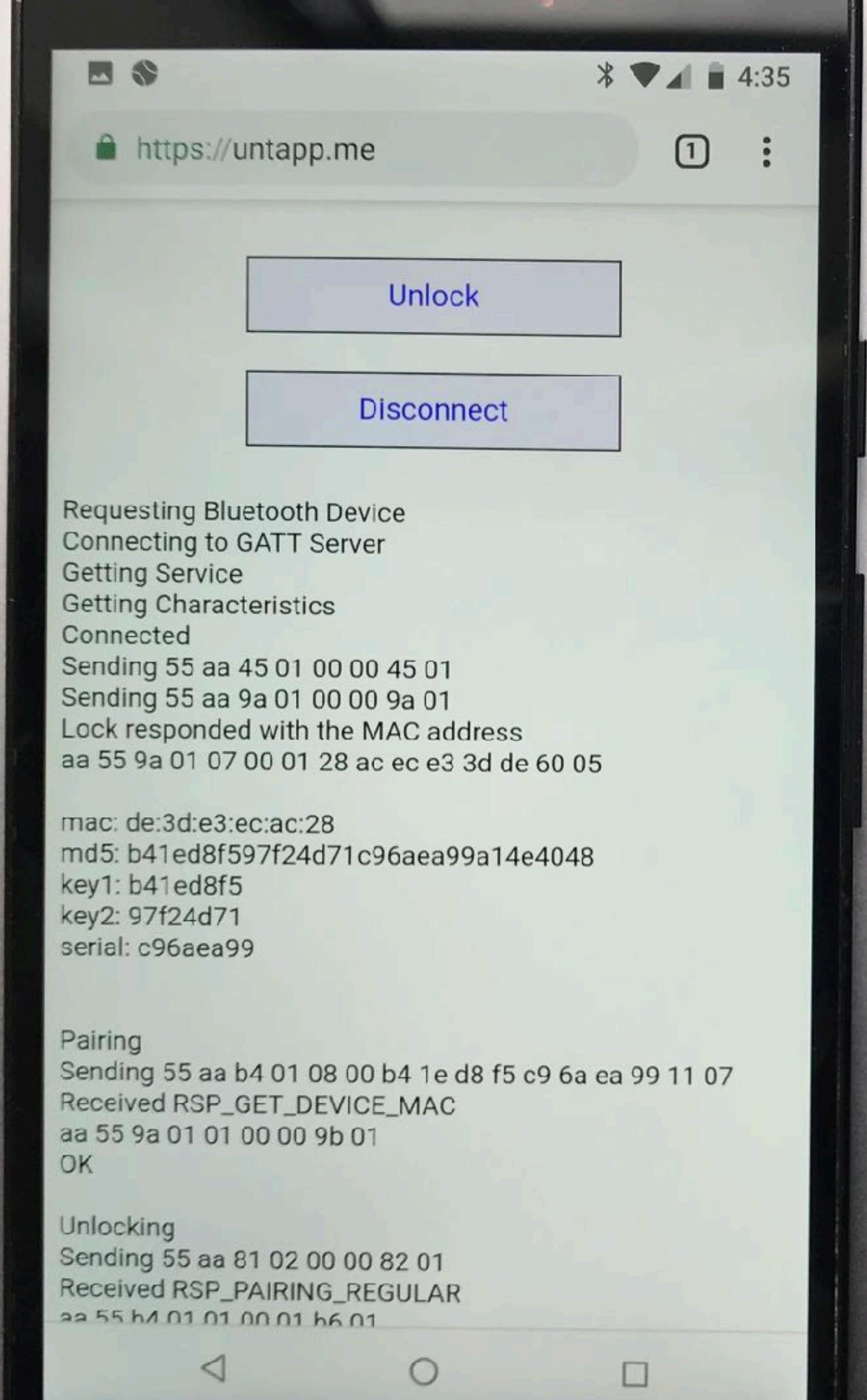
See the other cool stuff we've been doing...

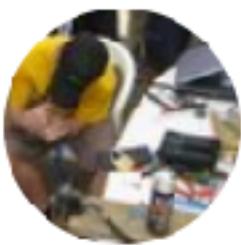


RED TEAMING

Cobalt Strike

MARITIME CYBER SECURITY





Luca Bongiorni
@LucaBongiorni

Following

So, apparently my Tapplock has even earlier FW with hardcoded 01020304 key.

Good catch from [@slawekja](#)

CC:[@cybergibbons](#)

The image contains two screenshots. The left screenshot shows a portion of Java code from a file named `Tapplock.java`. The code includes imports for `intelligent.tapp.bluetooth`, `intelligent.tapp.model.SubscribeModel`, `intelligent.tapp.tools.AndroidTool`, `util.Locale`, and `util.Random`. It defines a class `BluetoothTool` with static final strings: `KEY_ONE`, `KEY_TWO`, `NULL_ONE` (containing the value `01020304`), and `SERIAL_NO`. It also includes a static method `byteToStr` that converts a byte array to a hex string. The right screenshot shows a terminal window on a Kali Linux VM. The terminal output shows the results of a lock cracking attempt, including the lock ID (`f7:22:eb:f3:03:3a`), reverse MAC address (`3A:03:F3:EB:22:F7`), calculated hash (`bedef425bbc88cf5020feb2783cd75df`), and the key and serial number (`bedef425, 020feb27`). It also shows the packet sent (`55AAB4010B00bedef425020feb279405`), a static key packet (`55aab40108000102030400000000c601`), and messages indicating a sending pair and unlock. The terminal prompt is `root@kali:~/tapp#`.

```
intelligent.tapp.bluetooth;
intelligent.tapp.model.SubscribeModel;
intelligent.tapp.tools.AndroidTool;
util.Locale;
util.Random;

    s BluetoothTool {
        static final String KEY_ONE = "KEY_ONE";
        static final String KEY_TWO = "KEY_TWO";
        static String NULL_ONE = "01020304";
        static final String SERIAL_NO = "SERIAL_NO";

        c static String byteToStr(byte[] bArr) {
            stringBuilder stringBuilder = new StringBuilder();
            int length = bArr.length;
            for (int i = 0; i < length; i++) {
                stringBuilder.append(String.format("%02X", new
            } return stringBuilder.toString();
        }
    }
}
```

Totally Pwning the Tapplock Smart Lock (the API way)



Vangelis Stykas

Follow

Jun 15, 2018 · 3 min read

tl;dr: Tapplocks api endpoints had no security checks other than a valid token to access any data. This results in anyone with a valid login (easily obtained by creating an account) being able to manipulate every tapplock available!

BRUCE SCHNEIER

BEST-SELLING AUTHOR OF *DATA AND GOLIATH*



Ruined By Design

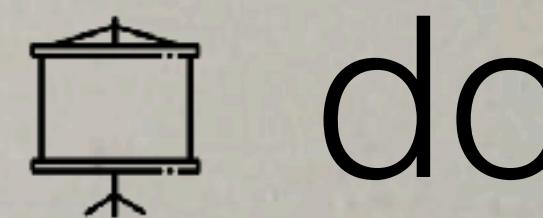
How Designers Destroyed the World,
and What We Can Do To Fix It

Mike Monteiro

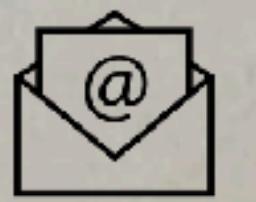
Foreword by Vivianne Castillo



Don Coleman



don.github.io/slides



don@chariotsolutions.com



github.com/don



[@doncoleman](https://twitter.com/doncoleman)



