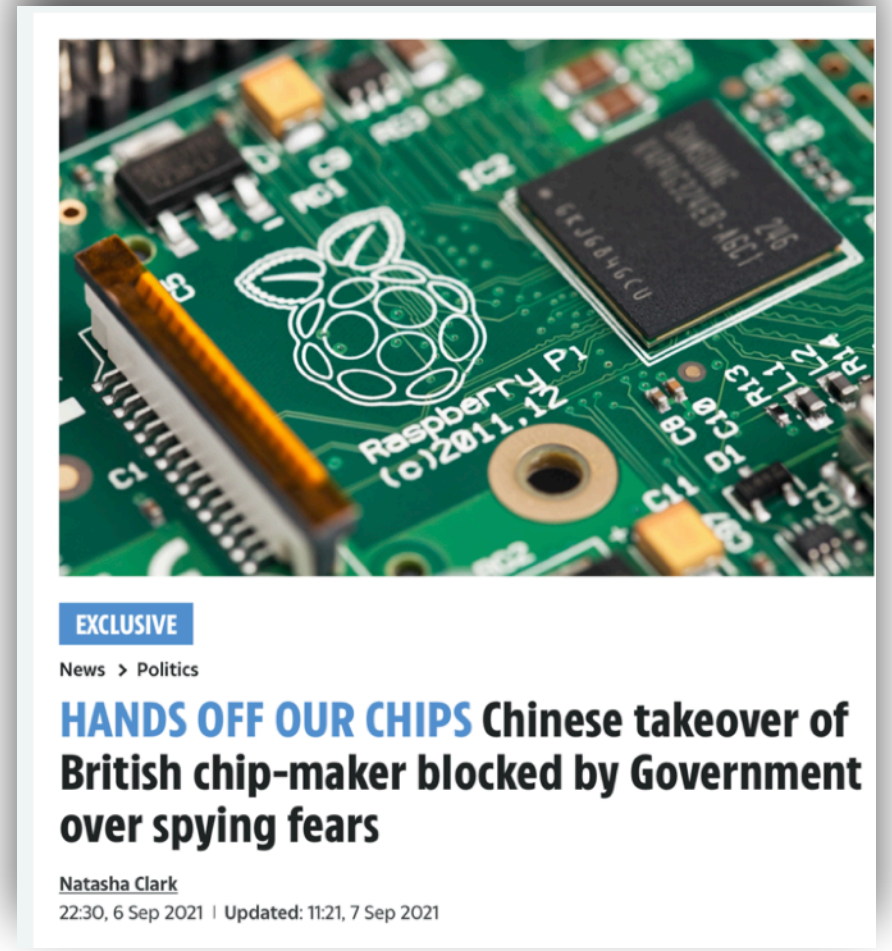
Selected Topics on Hardware for Security (NWI-IMC065)

Ileana Buhan, November 2021

EOS N 01.760, Tuesdays 10.30-12.15

Radboud University

In the news



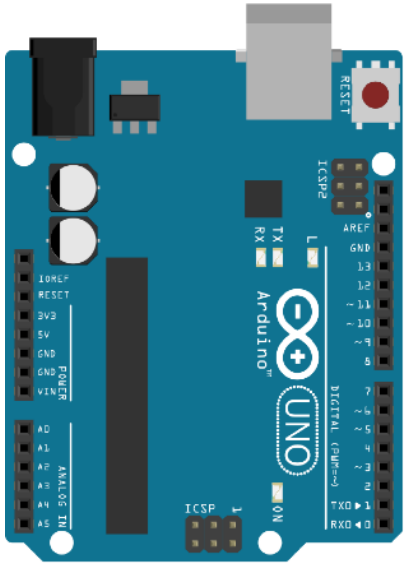
China's Taurus International Ltd and others are seeking to take over Swansea-based Perpetuus Group, which **makes semiconductors used in a wide variety of tech**.

Business Secretary Kwasi Kwarteng has ordered the competition watchdog to report back by February before a final call is made on whether the controversial merger can go ahead.

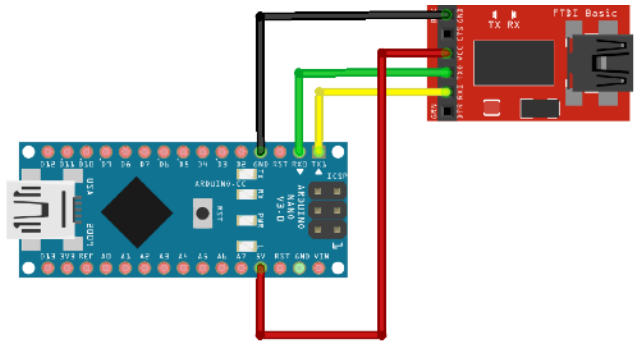
Taurus already owns a huge chunk of the business and th**ere are concerns that approving the deal will give China the upper hand in mobile and tech communications…**

This lecture

Meet TOM



Who are you?
PCB RE



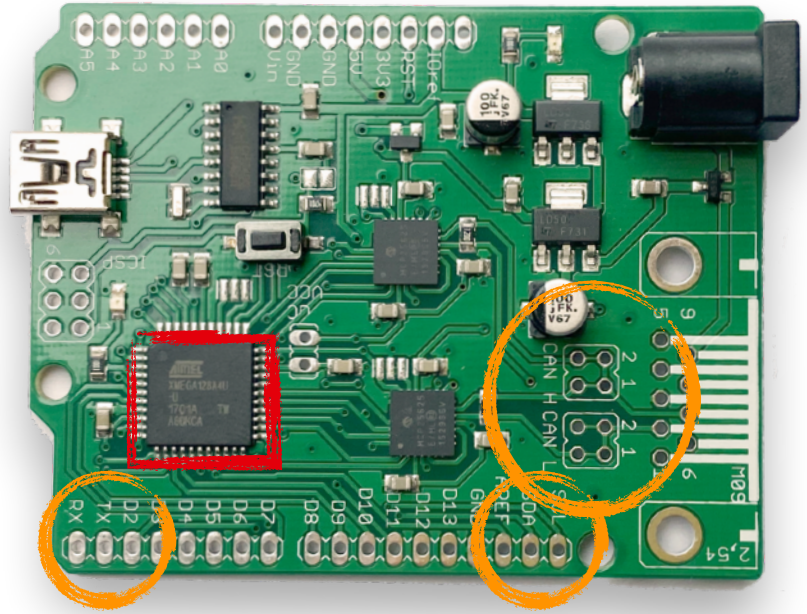
Can we talk?
Serial communication

PART I
MEET TOM

Embedded Systems everywhere

What is an Embedded System?

Image source: author collection



Memory

Computer processor

Interfaces

- A computer with a dedicated function within a larger mechanical and electronic system.
- Hardware: components attached to a PCB
- Software/Firmware controlls the functioning
- Interfaces: few interface to complex GUI
- Complexity and design choices vary considerably
- 98%
- Architecture of a ES is classified information

IS THE DEVICE A THREAT TO YOU?

How much do you trust your hardware?

Security Analysis of Wearable Fitness Devices (Fitbit)

Britt Cyr, Webb Horn, Daniela Miao, Michael Specter
Massachusetts Institute of Technology
Cambridge, Massachusetts, U.S.A.
cyrbritt@mit.edu, webbhorn@mit.edu, dmiao@mit.edu, specter@mit.edu

Abstract

This report describes an analysis of the Fitbit Flex ecosystem. Our objectives are to describe (1) the data Fitbit collects from its users, (2) the data Fitbit provides to its users, and (3) methods of recovering data not made available to device owners. Our analysis covers four distinct attack vectors. First, we analyze the security and privacy properties of the Fitbit device itself. Next, we observe the Bluetooth traffic sent between the Fitbit device and a smartphone or personal computer during synchronization. Third, we analyze the security of the Fitbit Android app. Finally, we study the security properties of the network traffic between the Fitbit smartphone or computer application and the Fitbit web service.

We provide evidence that Fitbit unnecessarily obtains information about nearby Flex devices under certain circumstances. We further show that Fitbit does not provide device owners with all of the data collected. In fact, we find evidence of per-minute activity data that is sent to the Fitbit web service but not provided to the owner. We also discovered that MAC addresses on Fitbit devices are never changed, enabling user-correlation attacks. BTLE credentials are also exposed on the network during device pairing over TLS, which might be intercepted by MITM attacks. Finally, we demonstrate that actual user activity data is authenticated and not provided in plaintext on an end-to-end basis from the device to the Fitbit web service.

2015

A Look at the Security and Privacy of Fitbit as a Health Activity Tracker

Jason Orlosky
Osaka University and Augusta University
orlosky[at]lab.ime.cmc.osaka-u.ac.jp

Onyeka Ezenwoye
Augusta University
oezenwoye[at]augusta.edu

Heather Yates
Augusta University
hyates[at]augusta.edu

Gina Besenyi
Kansas State University and Augusta University
gbesenyi[at]ksu.edu

ABSTRACT

Given the popularity of consumer grade wearable health trackers, there is an increasing need to evaluate their accuracy and security. In this paper, we present the results of a study with 24 participants who used and evaluated a small form factor personal health device, the Fitbit Blaze. Our study includes both the analysis of data taken from an exercise-based experiment and a review of the security risks associated with current protocols used to access Fitbit device data and participant information. In addition to discussion of the FitBit's accelerometer and pulse data as compared to clinical grade devices, we gathered and analyzed subjective participant data on usability and perception of privacy and security using both quantitative and subjective methods. Results showed that FitBit accuracy was not equivalent to medical grade devices, that a majority of risk comes from potentially fraudulent third party applications, and that users are typically justified in their concerns.

CCS CONCEPTS

• **Computer-Communication Networks → General.**

typically stays with a user throughout the day. These devices can be beneficial for improving physical activity for different user groups.

However, like many other tracking technologies, wearable devices carry a significant amount of user data, some of which potentially carries information about the person's genetic factors and disease state. For example, Farzanehfar et al. showed that motion trackers can be used to infer and monitor disease state, such as Parkinson's disease [7], and can even be used to diagnose tremor [18]. This is significant from a security and privacy perspective, especially concerning the Health Insurance Portability and Accountability Act (HIPAA) rules and regulations. Unlike data that is typically recorded and confined to a lab or hospital setting or transferred over physical media [12], Fitbit devices leave secured areas with personal data and travel with the user into many domains.

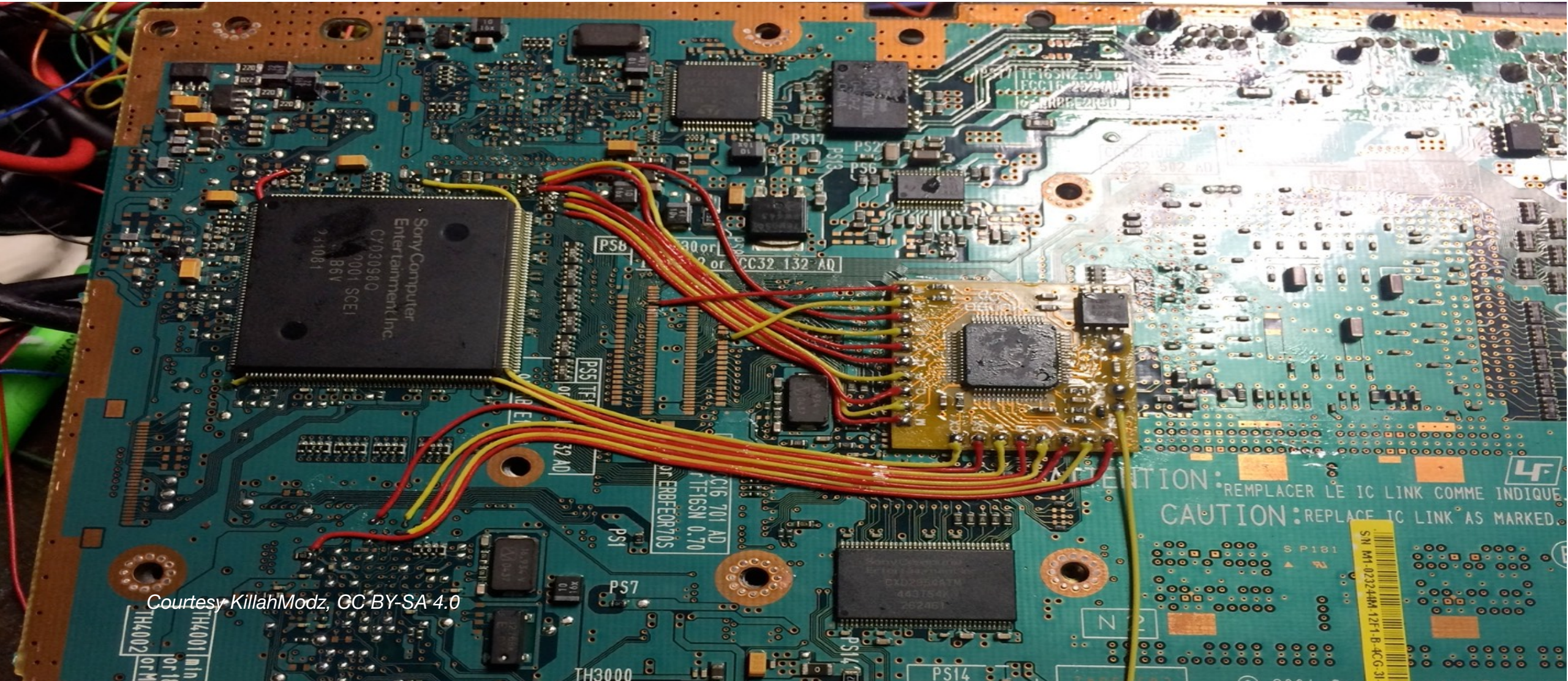
To help explore the issue of security and determine user perceptions of personal data and privacy, this paper 1) analyzes the authentication technologies associated with wearable tracking devices, 2) describes the results of a series of experiments testing accuracy of information of wearable trackers against two different devices, as shown in Figure 1, with a group of participants in differ-

2019

IS THE DEVICE A THREAT TO YOU?

ARE YOU A THREAT TO THE DEVICE?

Are you a threat to the device?

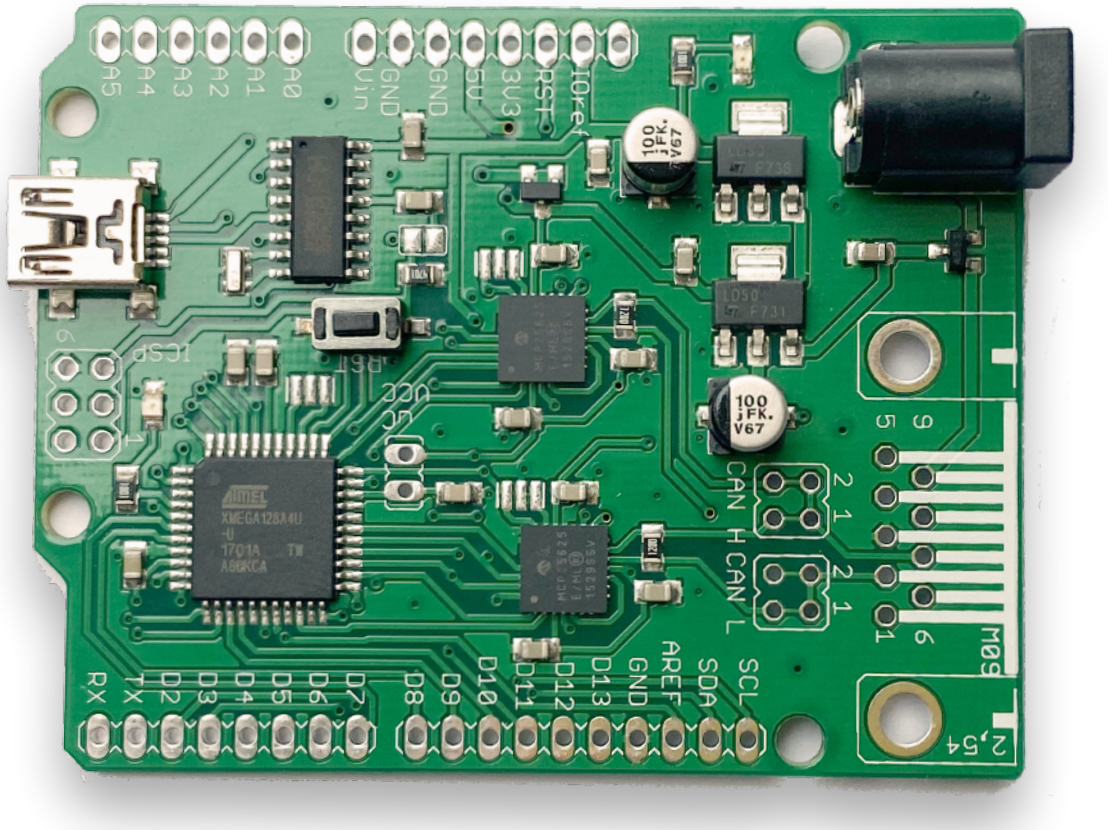


Courtesy KillahModz, CC BY-SA 4.0

Hardware Trojans

- Malicious modification of an integrated circuit
- Introduced during manufacturing
- Bypass or disable security
- High security IT departments buy hardware from trusted sources

Image source: author collection



Does this PCB have “unadvertised features”?

The adversary - TOM

Tamper:

- obtain access to the hardware (evidence, resistant, proof)

Observe:

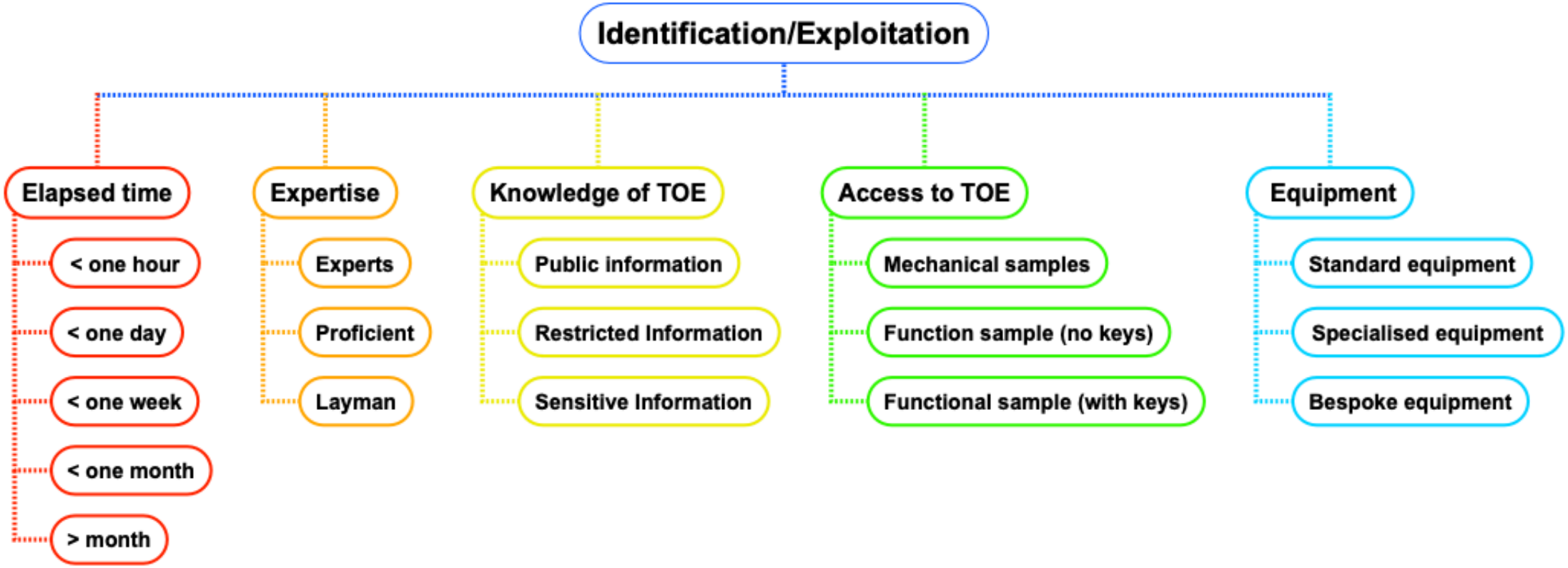
- identify components, *side channels**;

Modify:

- read restricted data, bypass security checks, *inject faults*;*

** covered in the course Physical Attacks on Secure Systems*

Many TOMs


Identification/Exploitation
Elapsed time
< one hour
< one day
< one week
< one month
> month
Expertise
Experts
Proficient
Layman
Knowledge of TOE
Public information
Restricted Information
Sensitive Information
Access to TOE
Mechanical samples
Function sample (no keys)
Functional sample (with keys)
Equipment
Standard equipment
Specialised equipment
Bespoke equipment

How much do you trust your hardware?

Security Analysis of Wearable Fitness Devices (Fitbit)

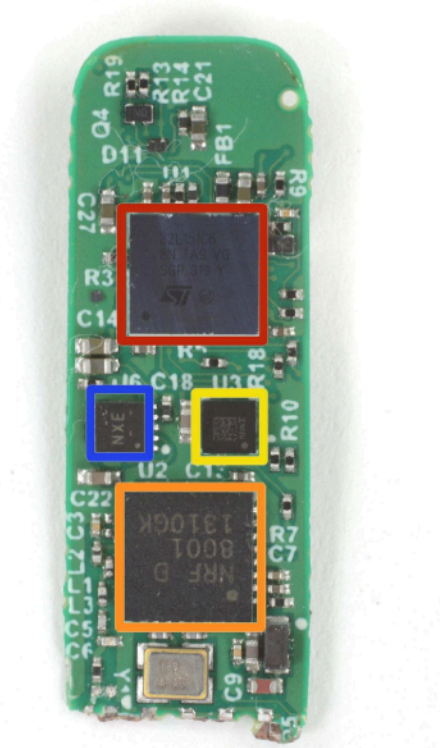
Britt Cyr, Webb Horn, Daniela Miao, Michael Specter
Massachusetts Institute of Technology
Cambridge, Massachusetts, U.S.A.
cyrbritt@mit.edu, webbhorn@mit.edu, dmiao@mit.edu, specter@mit.edu

Abstract

This report describes an analysis of the Fitbit Flex ecosystem. Our objectives are to describe (1) the data Fitbit collects from its users, (2) the data Fitbit provides to its users, and (3) methods of recovering data not made available to device owners. Our analysis covers four distinct attack vectors. First, we analyze the security and privacy properties of the Fitbit device itself. Next, we observe the Bluetooth traffic sent between the Fitbit device and a smartphone or personal computer during synchronization. Third, we analyze the security of the Fitbit Android app. Finally, we study the security properties of the network traffic between the Fitbit smartphone or computer application and the Fitbit web service.

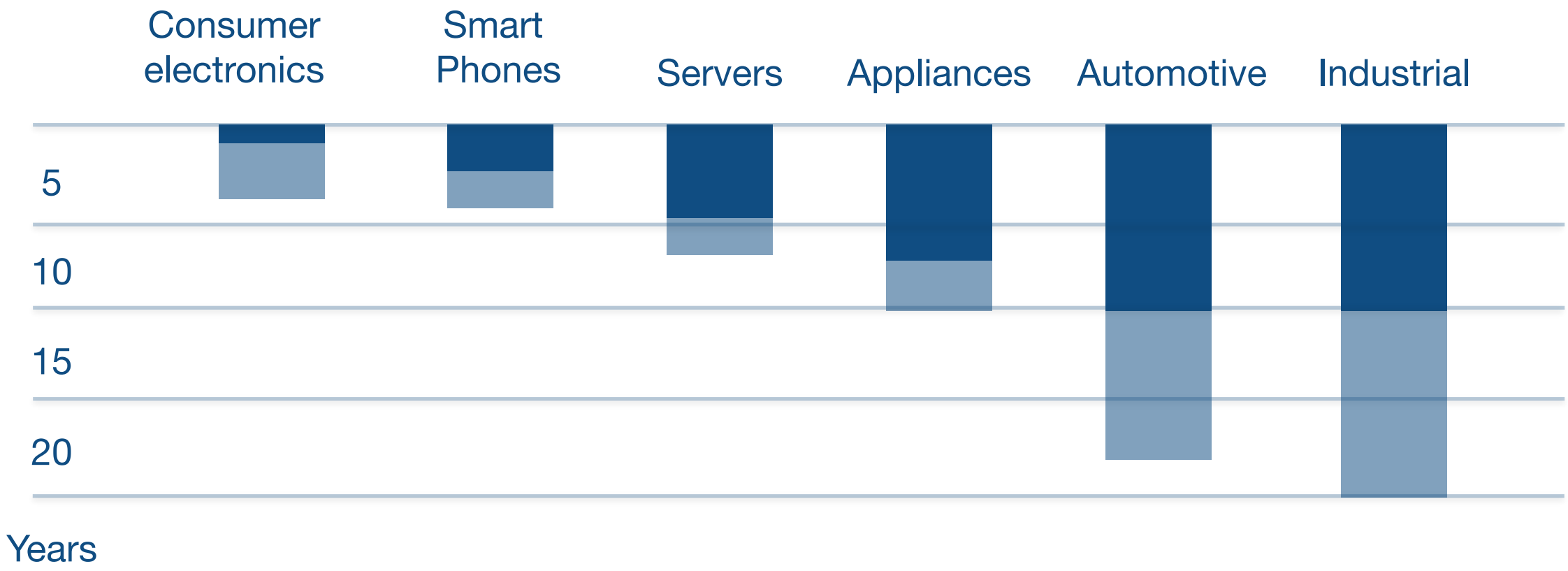
We provide evidence that Fitbit unnecessarily obtains information about nearby Flex devices under certain circumstances. We further show that Fitbit does not provide device owners with all of the data collected. In fact, we find evidence of per-minute activity data that is sent to the Fitbit web service but not provided to the owner. We also discovered that MAC addresses on Fitbit devices are never changed, enabling user-correlation attacks. BTLE credentials are also exposed on the network during device pairing over TLS, which might be intercepted by MITM attacks. Finally, we demonstrate that actual user activity data is authenticated and not provided in plaintext on an end-to-end basis from the device to the Fitbit web service.

2015



Average life expectancy for chips

Source: https://semiengineering.com/making-chips-to-last-their-lifetime/



Attacks only get better; they never get worse (NSA)

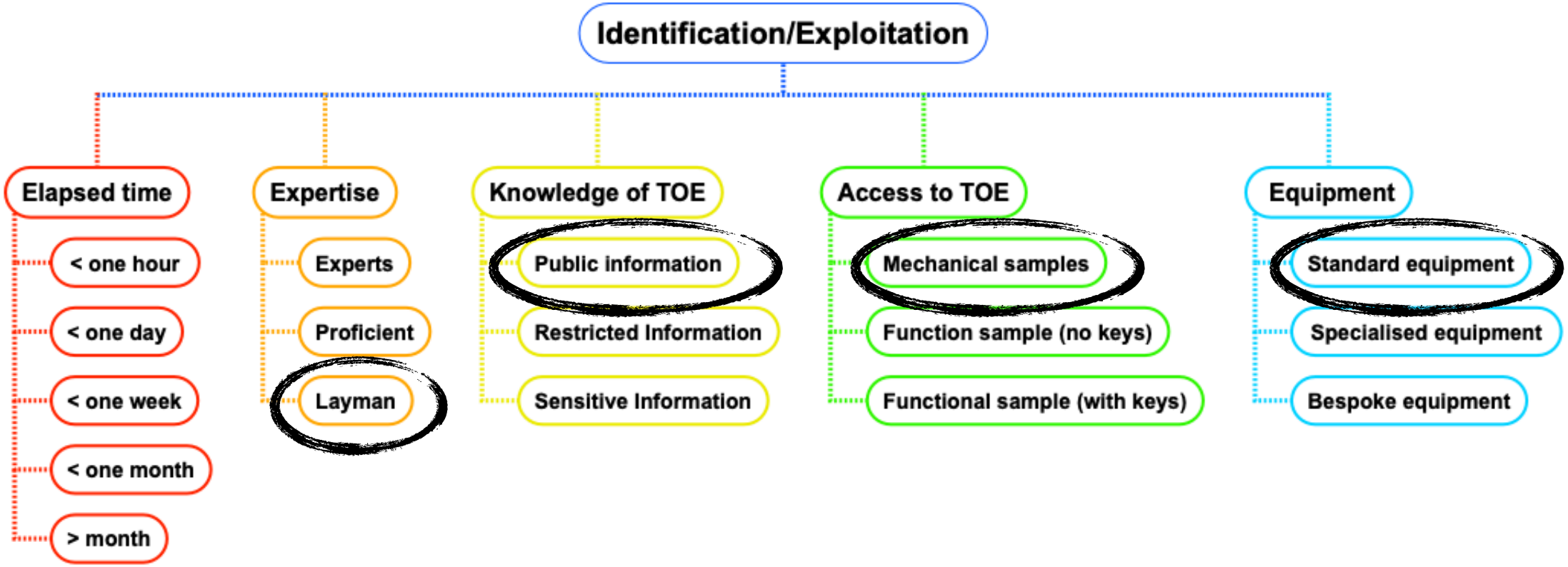
What makes securing embedded devices challenging ?

Challenges for securing embedded systems:

- Cost
- Complexity
- Long life expectancy
- Hardware is static
- Lack of regulations
- …

Hardware Security aims to protect a device and its end-user against TOM

TOM : this lecture



TOM @ work

Who are you?

Can we talk ?

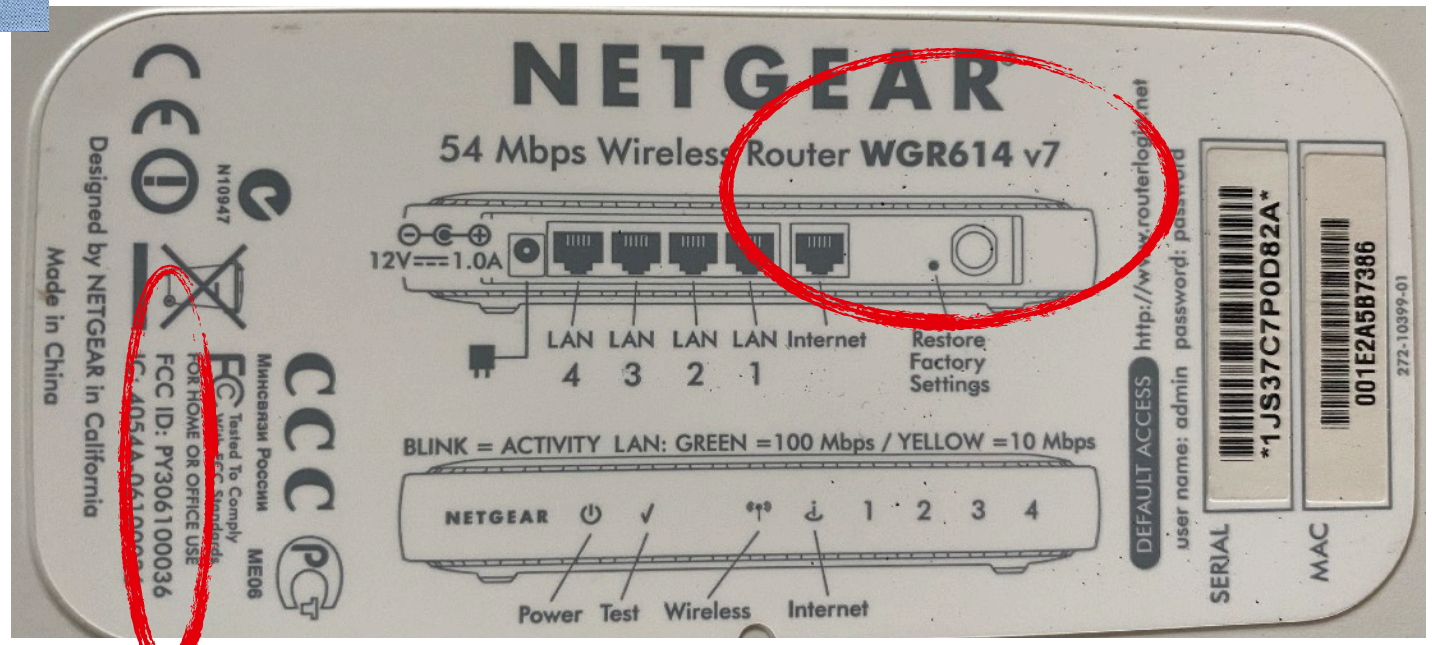
I want to get to know you

You are mine!

WHO ARE YOU?
PCB RE

Read the labels

Image source: author collection

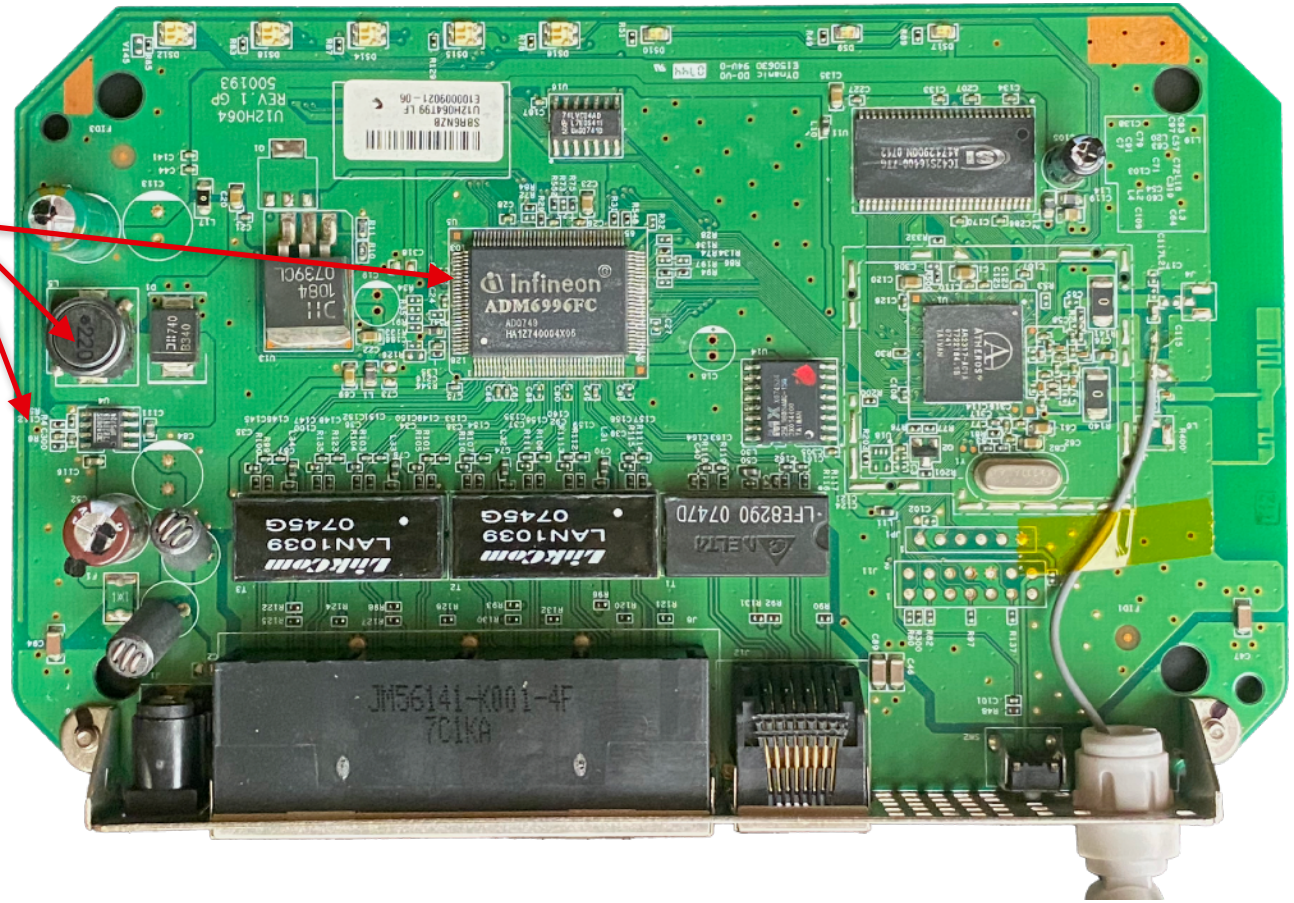


Exploring the PCB

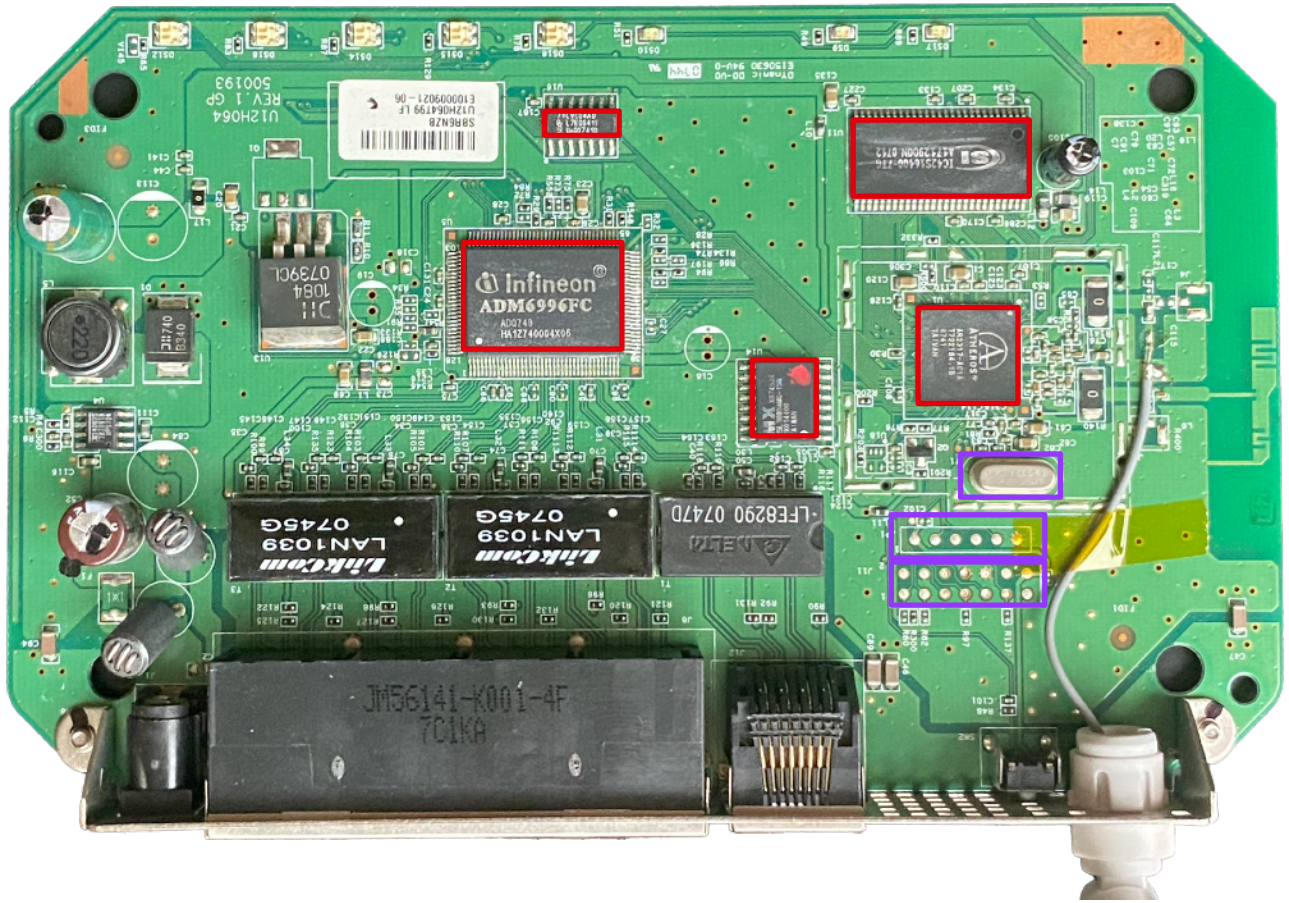
Image source: author collection

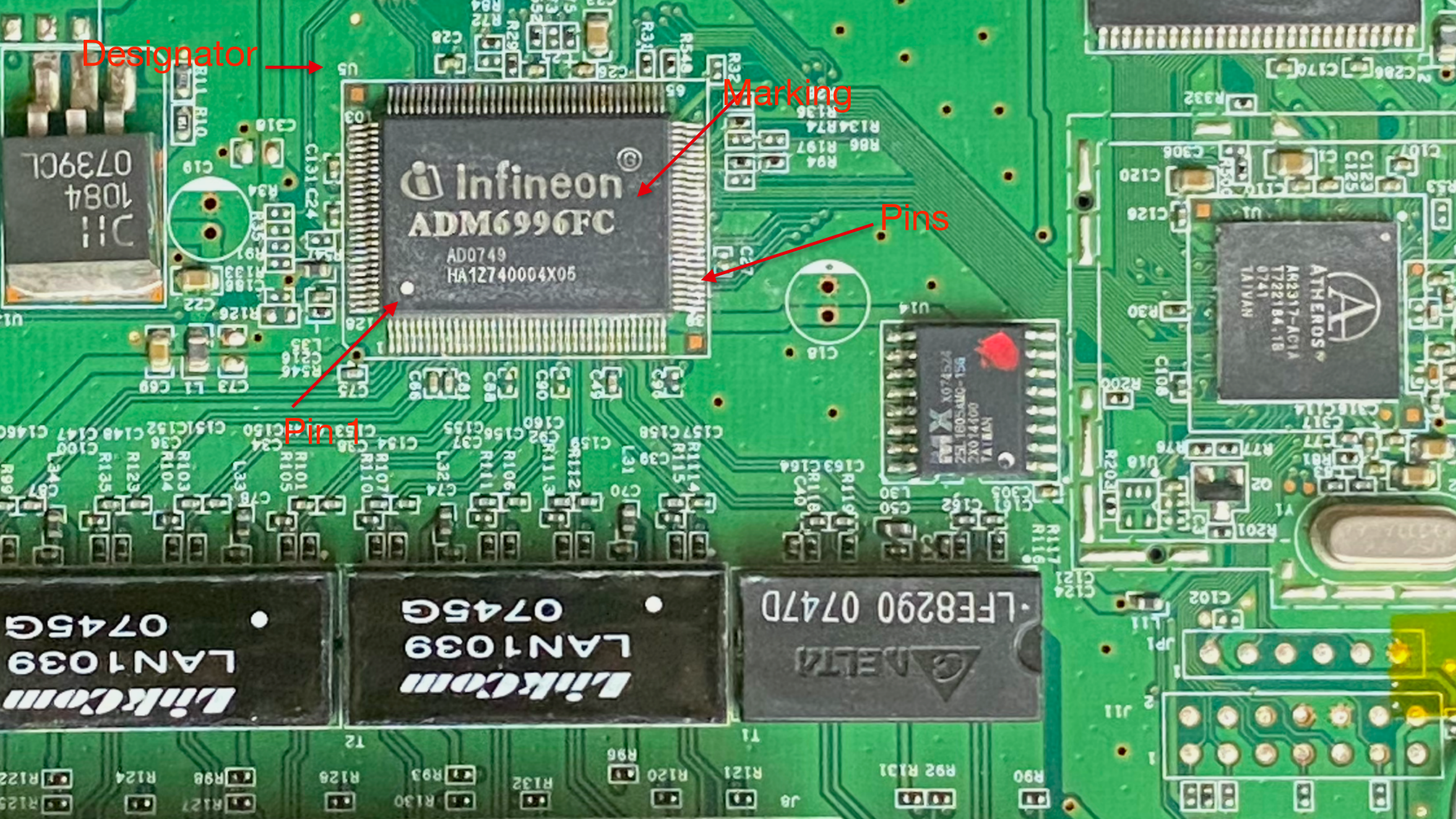
Components

- Designator
- Package type
- Markings

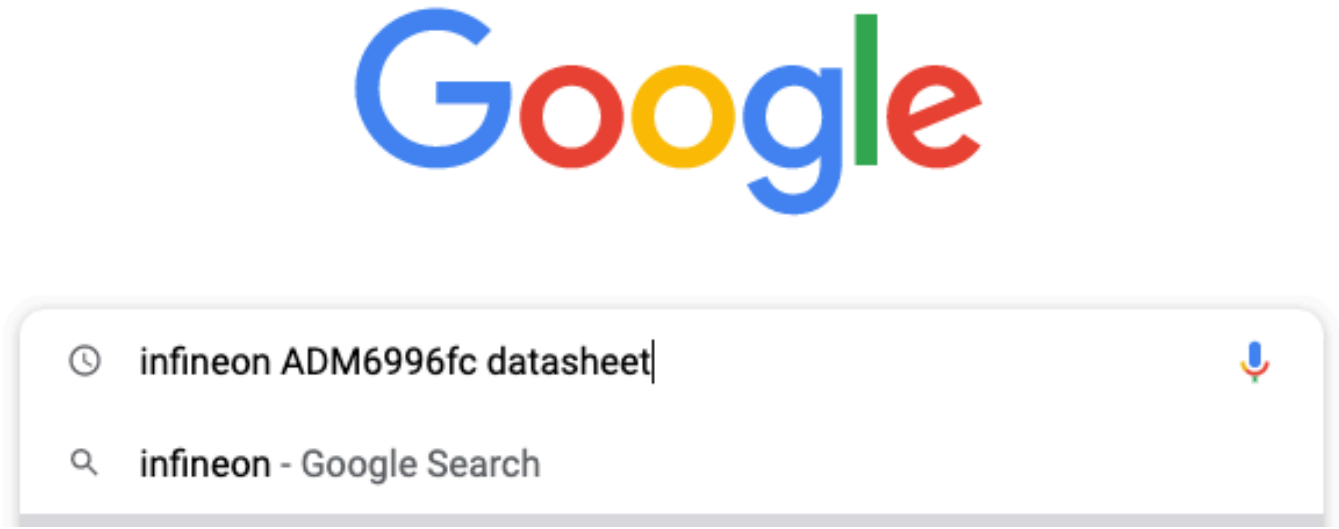


What are we looking for?

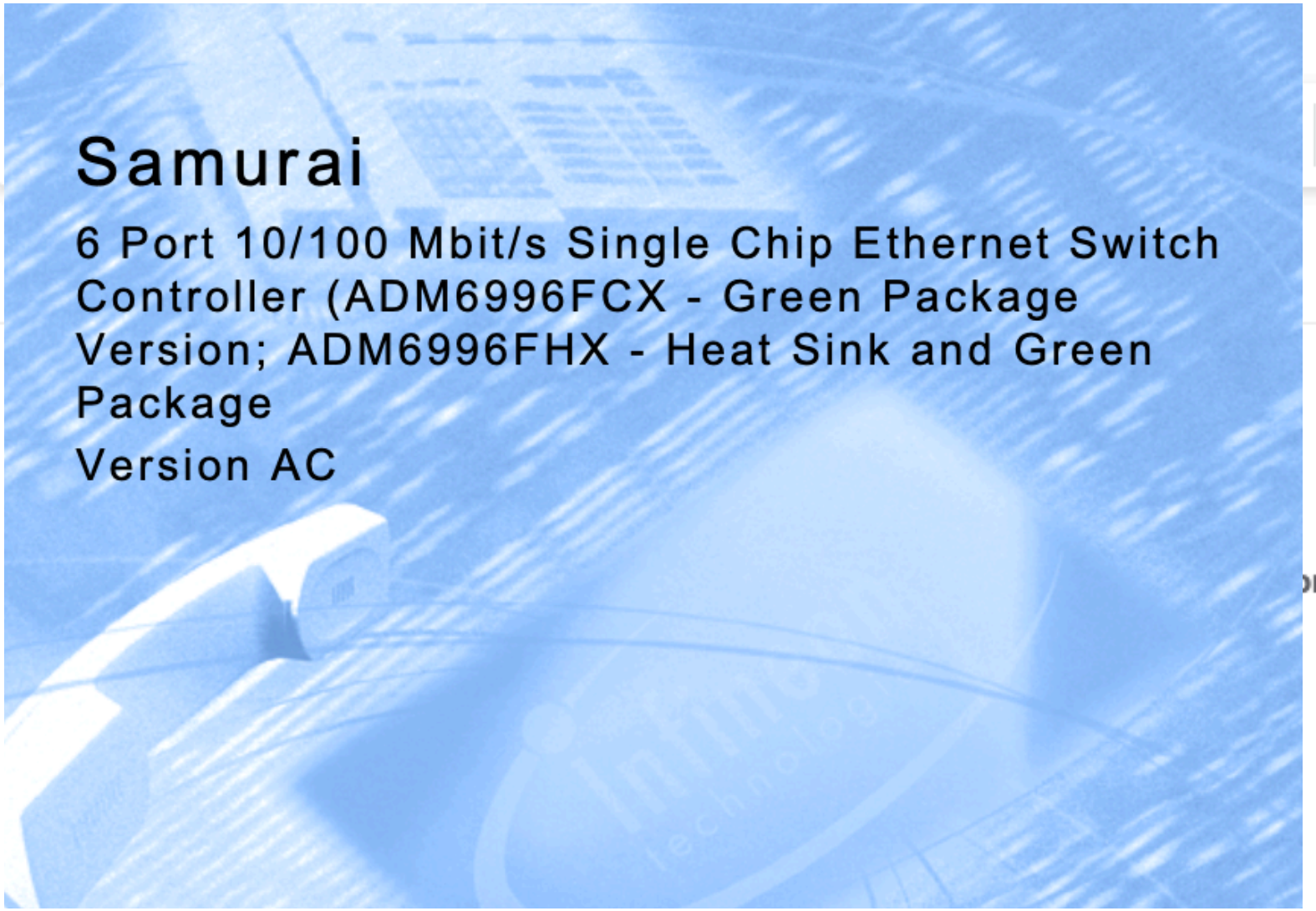



Designator
Marking
Pins
Pin 1
Infineon
ADM6996FC
AD0749
HA1Z740004X05
ATHEROS
LAN1039
0745G
LAN1039
0745G
LFE8290 0747D

Searching for components



Searching for components



Pinout map

1 Product Overview

1.1 Samurai - ADM6996FC/FCX/FHX Overv

The Samurai - ADM6996FC/FCX/FHX is a high performance
Memory) 6-port MII MAC ports with five supporting 10/100 Mbi
The ADM6996FCX is the environmentally friendly package or
sink which can be used in special circumstances bu
ADM6996FC/FCX/FHX is intended for applications such as st
such as 5-port switches and router applications.

The ADM6996FC/FCX/FHX provides functions such as: 802.1
address locking, management, port status, TP auto-MDIX, 25M
requests on switch demand.

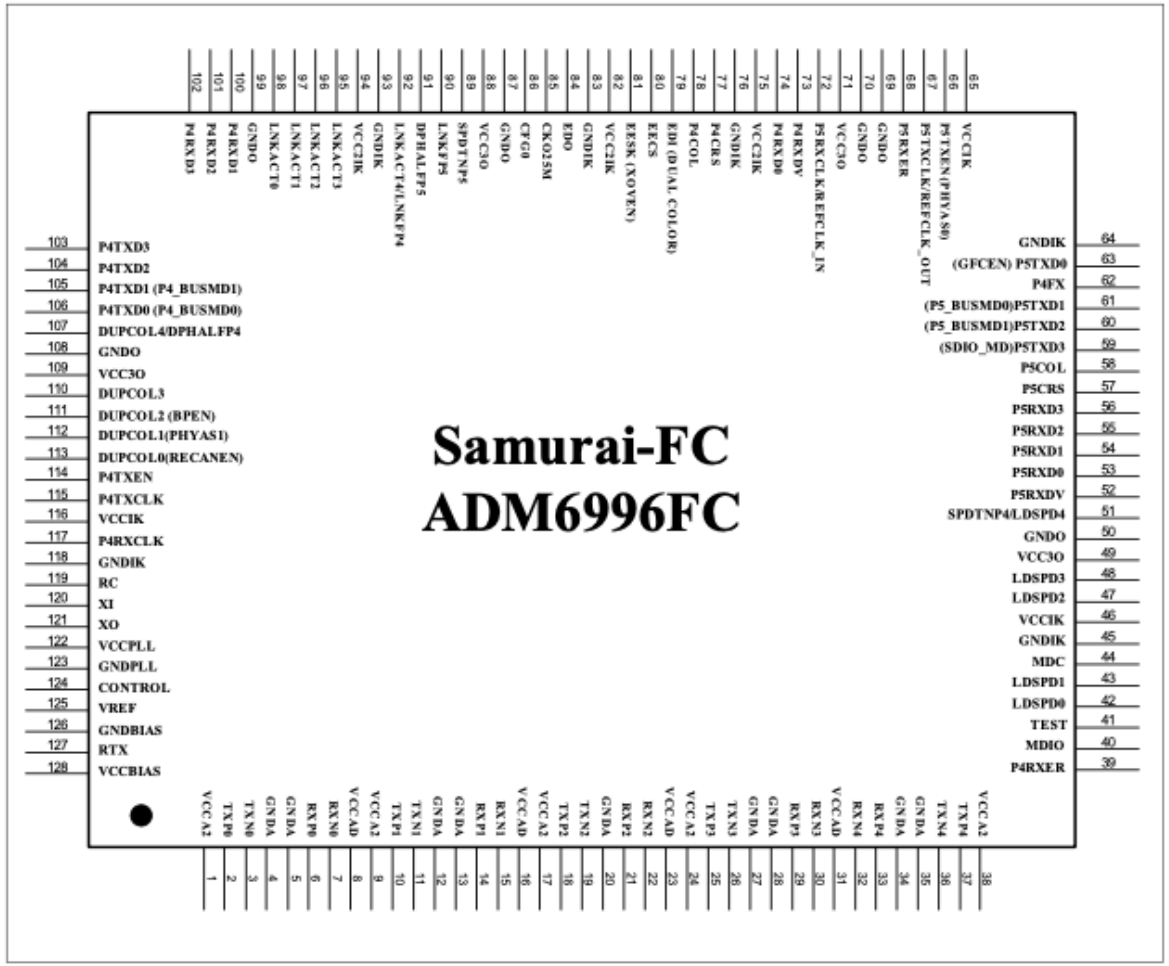
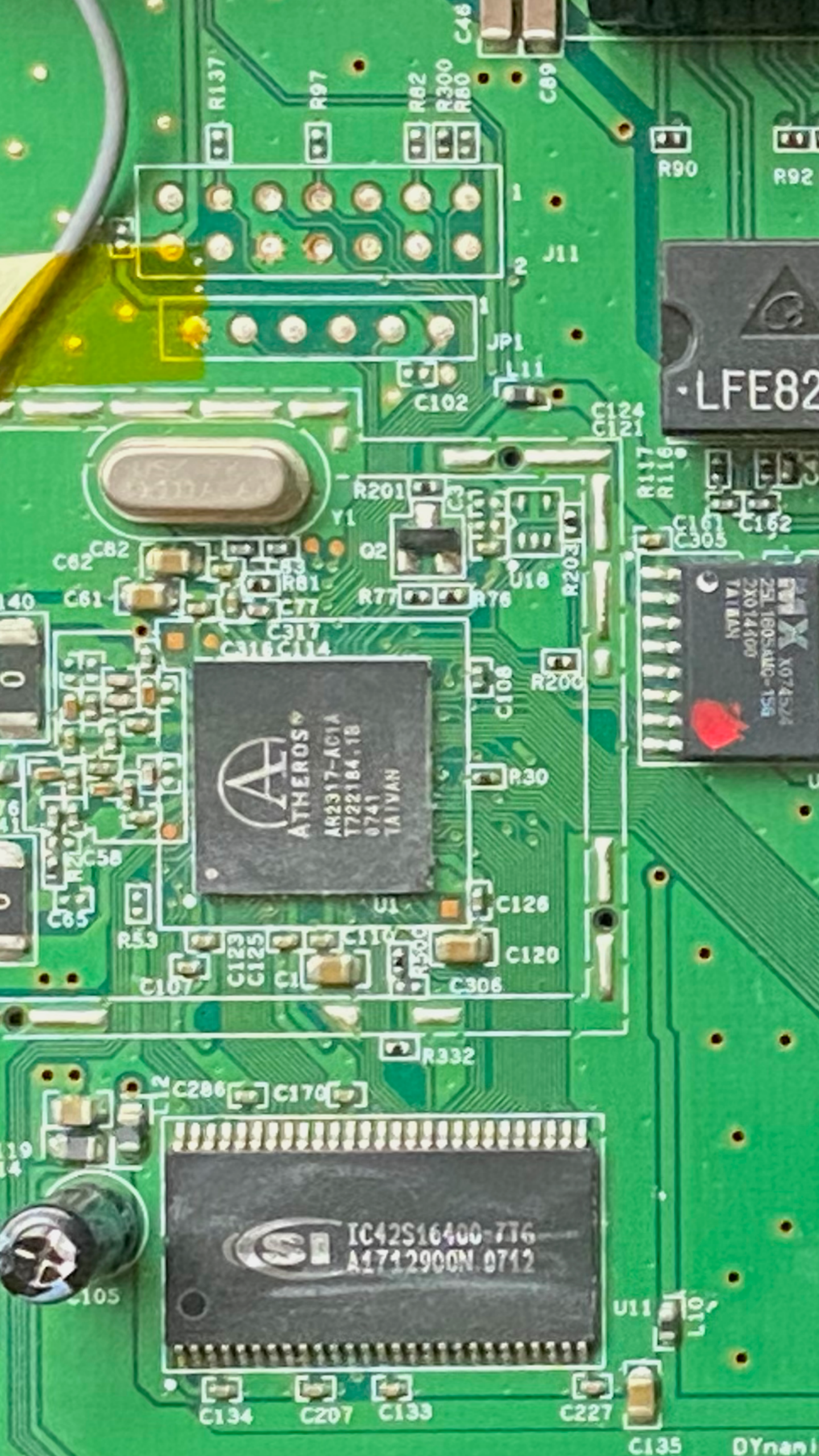


Figure 2 4 TP/FX PORT + 2 MII PORT 128 Pin Diagram


R137
R97
R82
R300
R80
C46
C89
R90
R92
J11
JP1
L11
C102
C124
C121
LFE82
R201
Y1
Q2
C82
C62
C61
R81
C77
R77
R76
U16
R231
C161
C305
C162
R117
R116
C317
C316
C114
C108
R200
ATHEROS
AR2317-AC1A
T722184.1B
0741
TAIWAN
R30
C58
C65
R53
U1
C126
C120
C123
C125
C107
C306
R332
C286
C170
IC42S16400-7TG
A1712900N 0712
C105
U11
C134
C207
C133
C227
C135

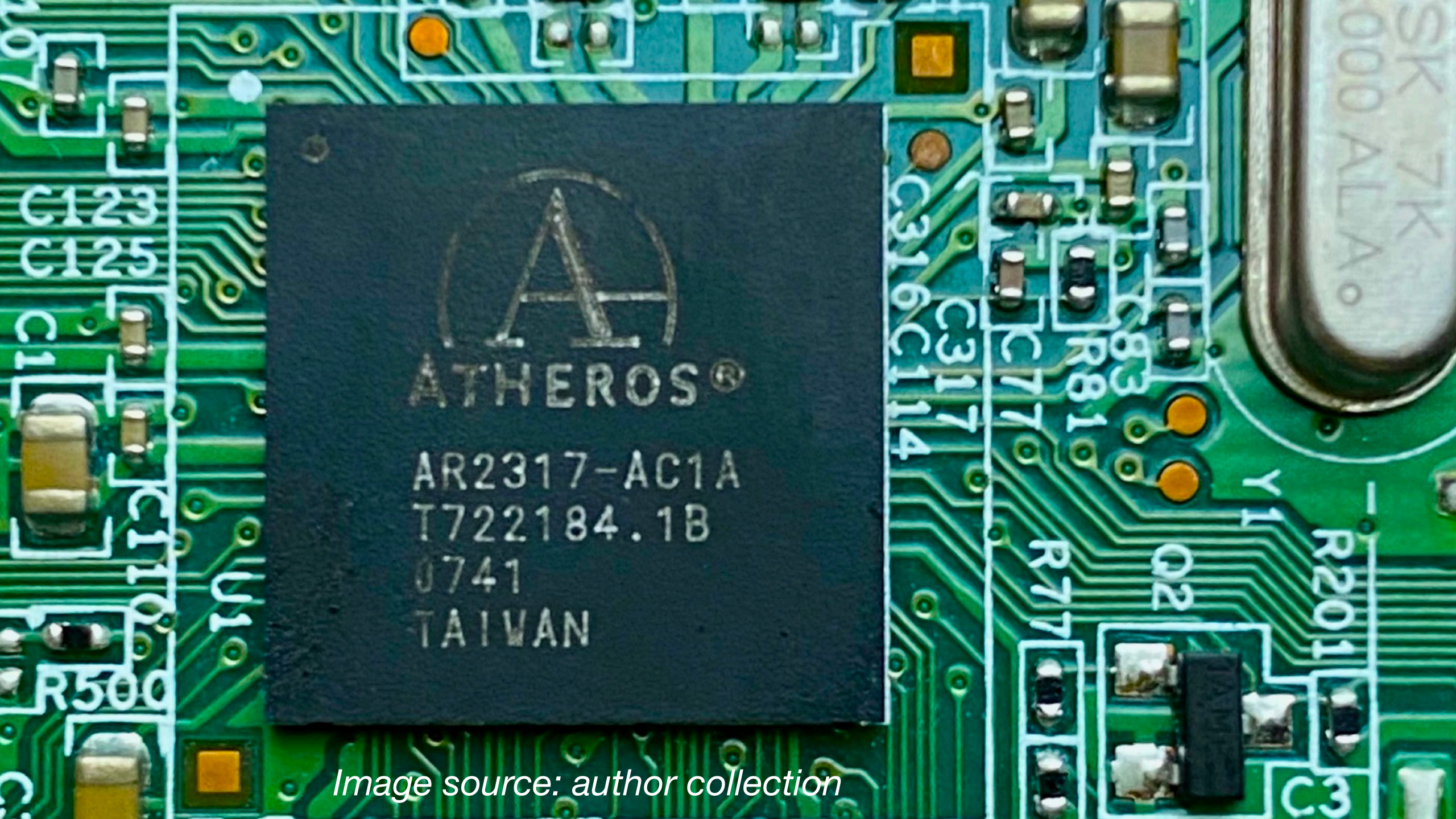


Image source: author collection

AR2317 Single Chip MAC/Baseband/Radio and Processor for 2.4 GHz Wireless LANs

General Description

The Atheros AR2317 is an all-CMOS, fully-integrated, single-chip 802.11b/g WLAN solution. It integrates the PA, LNA, 2.4GHz radio, baseband PHY, MAC, and a MIPS 4000 CPU into a single chip for wireless access point and router applications. Other major modules include 802.3 Ethernet MAC and MII interface, SDRAM controller, external memory interface for Flash, ROM, or RAM, a UART, GPIOs as well as LED controls.

The AR2317 implements an 802.11 MAC/BB processor supporting all IEEE 802.11g data rates (1 to 54 Mbps) and all IEEE 802.11b complementary key coding (CCK) data rates (1 to 11 Mbps). Additional features include forward error correction coding at rates for 1/2, 2/3, and 3/4, signal detection, automatic gain control, frequency offset estimation, symbol timing, channel estimation, error recovery, enhanced security, and quality of service (QoS). The AR2317 performs receive and transmit filtering for IEEE 802.3 and 802.11 networks.

Features

- Integrated high-output PA
- Integrated LNA/optional external LNA support
- Integrated 1.8 V voltage regulator; NO need for a 1.8 V supply
- Switched Rx antenna diversity
- Integrated Rx/Tx antenna switch
- Integrated power detector
- 25 MHz output for Ethernet switch
- Integrated MIPS 4000 processor
- 180 MHz processor frequency
- IEEE 802.11b/g Access Point, Ad Hoc, and station functions supported
- OFDM and CCK modulation schemes supported
- Data rates of 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
- IEEE 802.3 Ethernet MAC supporting 10/100 Mbps, full and half duplex, and MII interface to external Ethernet PHY
- UART for console support
- IEEE 1149.1 standard test access port and boundary scan architecture supported
- EJTAG based debugging of the processor core supported
- Standard 0.18 µm CMOS technology
- 12 mm x 12 mm 260 BGA package

Summary - PCB RE

- Where is the SoC (model, instruction set,memory,…)
- External memories (e.g flash - package, type, etc)
- UART port pinout
- JTAG port pinout

Visual inspection not always possible

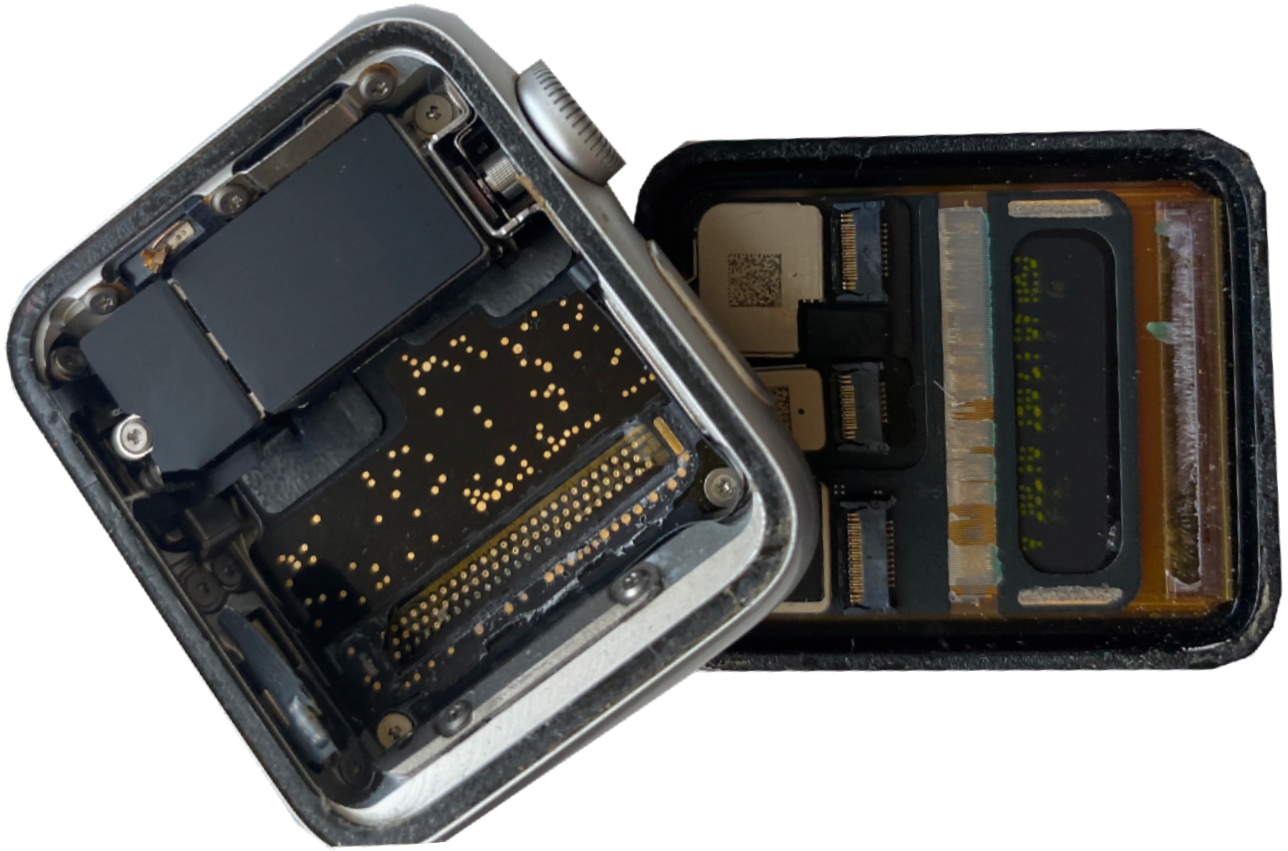
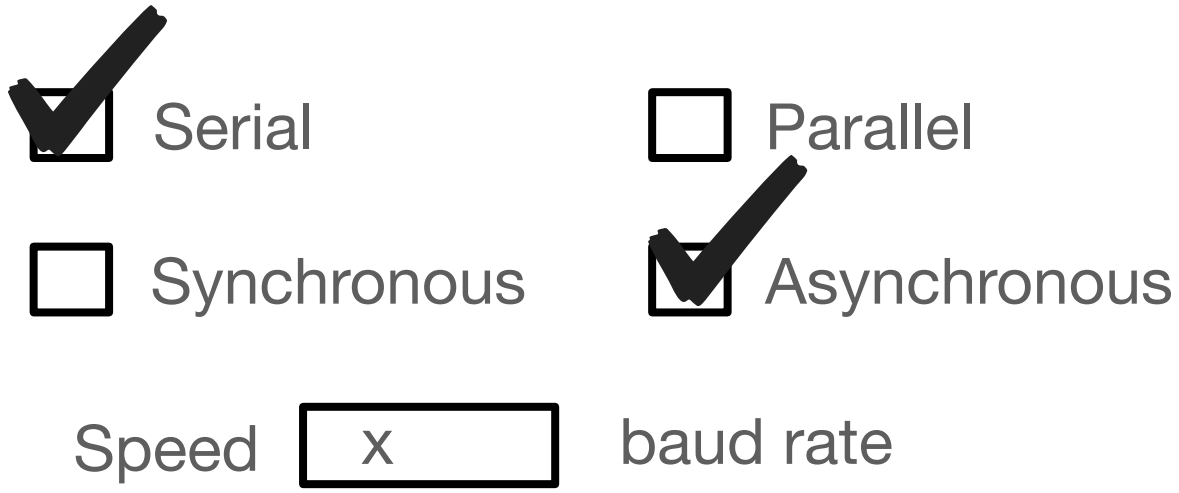
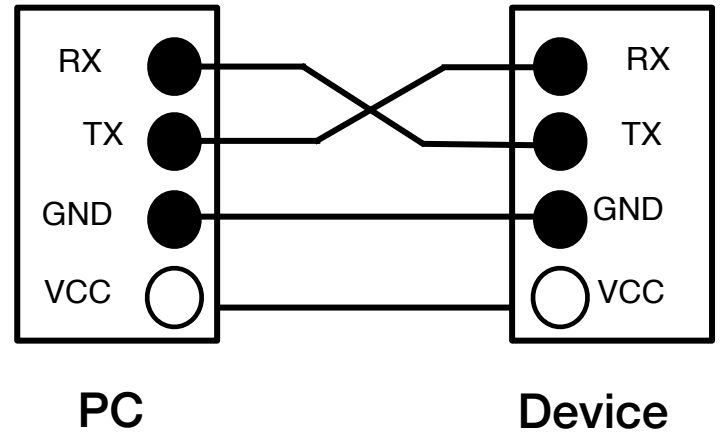


Image source: author collection

CAN WE TALK?
UART

Universal Asynchronous Receiver-Transmitter (UART)





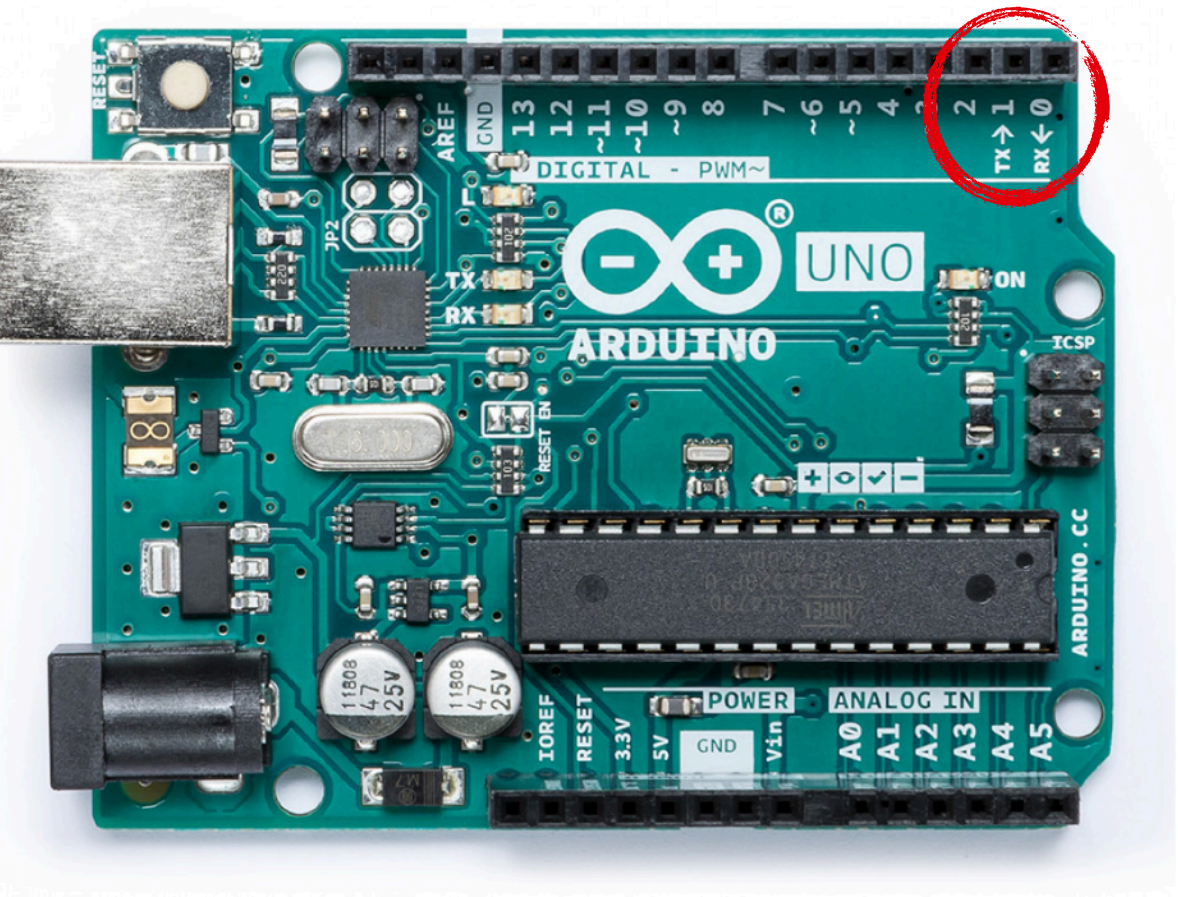
Pro's

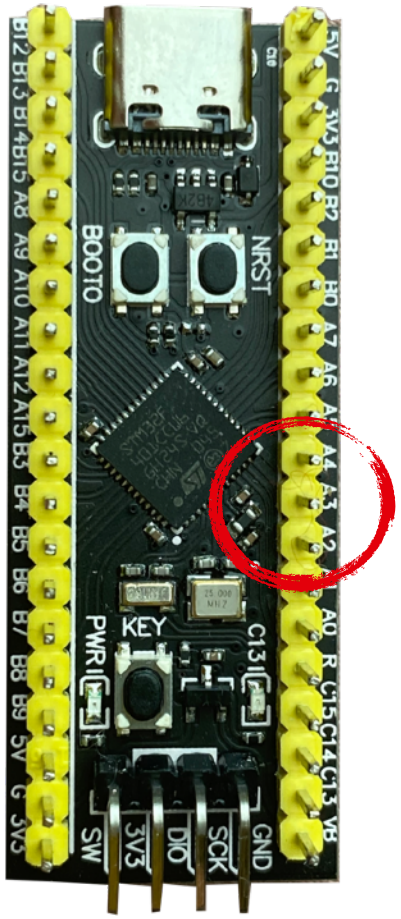
- Two-way communication;
- Two wires;
- Very common

Con's

- Dedicated hardware, required
- Sometimes locked
- Sometimes not easy to recognize

UART in the wild





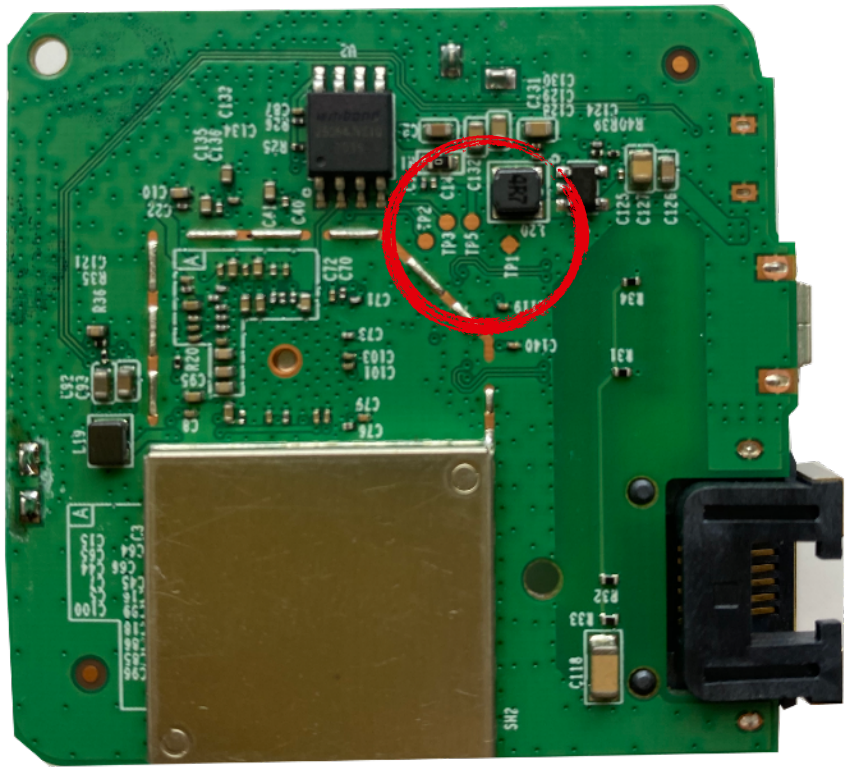
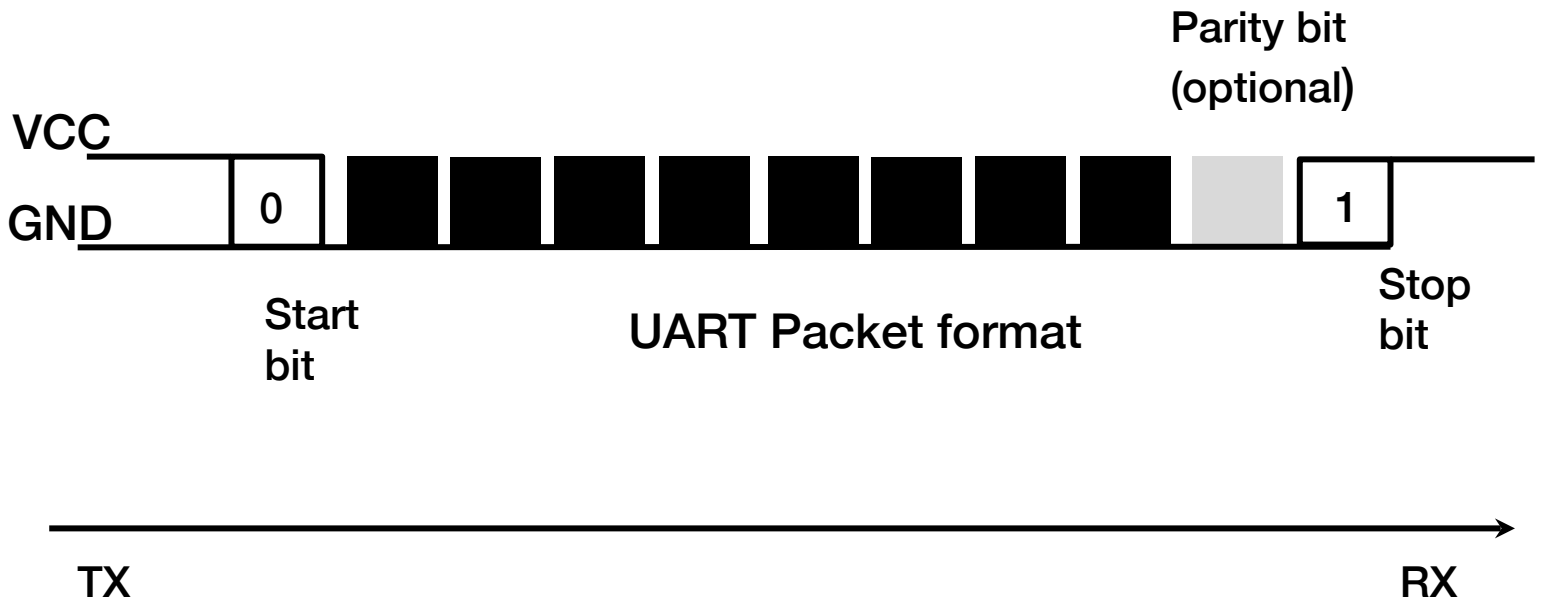
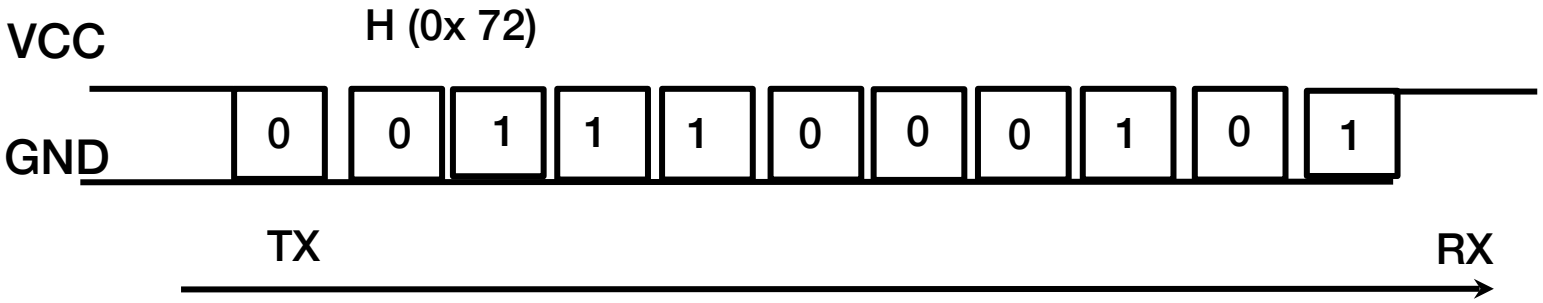


Image source: author collection

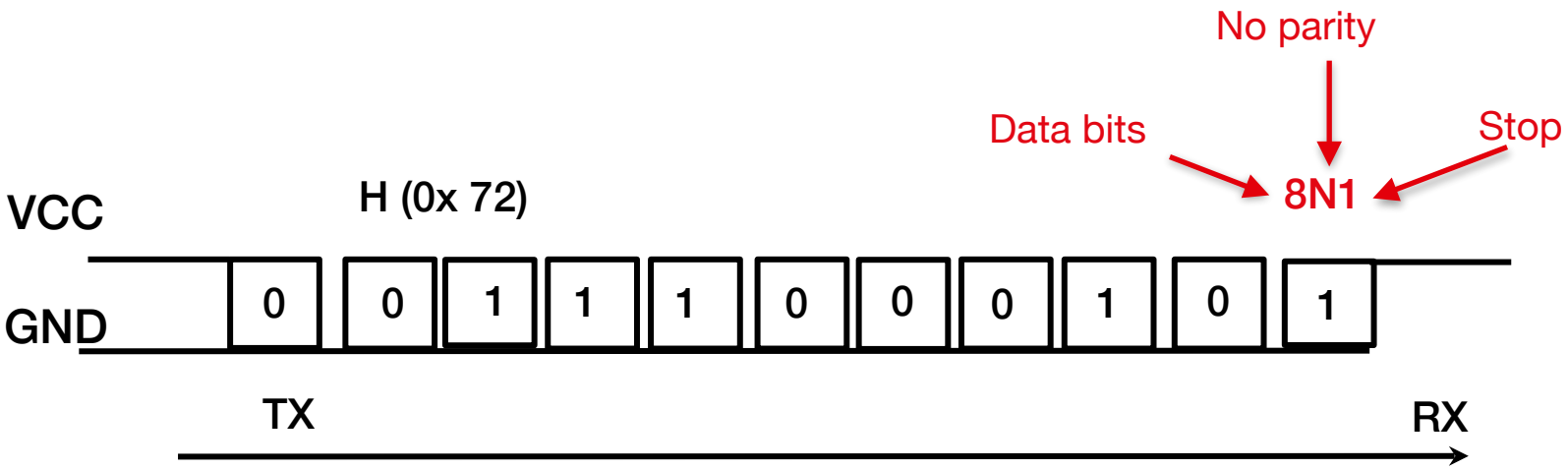
Universal Asynchronous Receiver-Transmitter (UART)



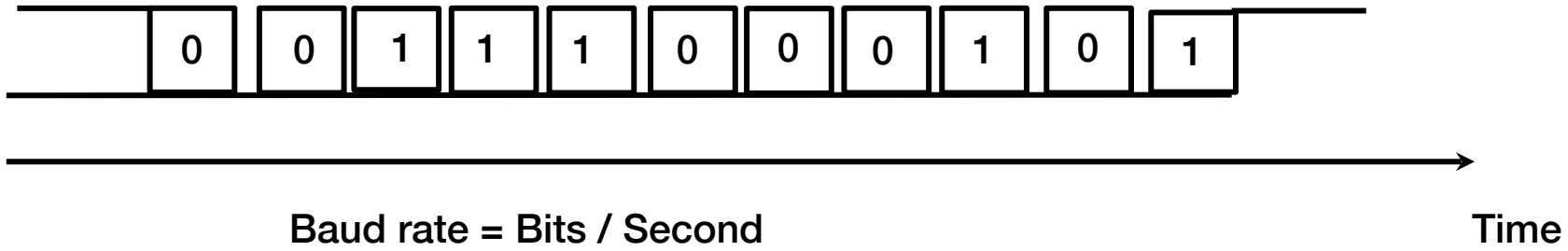
Universal Asynchronous Receiver-Transmitter (UART)



Universal Asynchronous Receiver-Transmitter (UART)



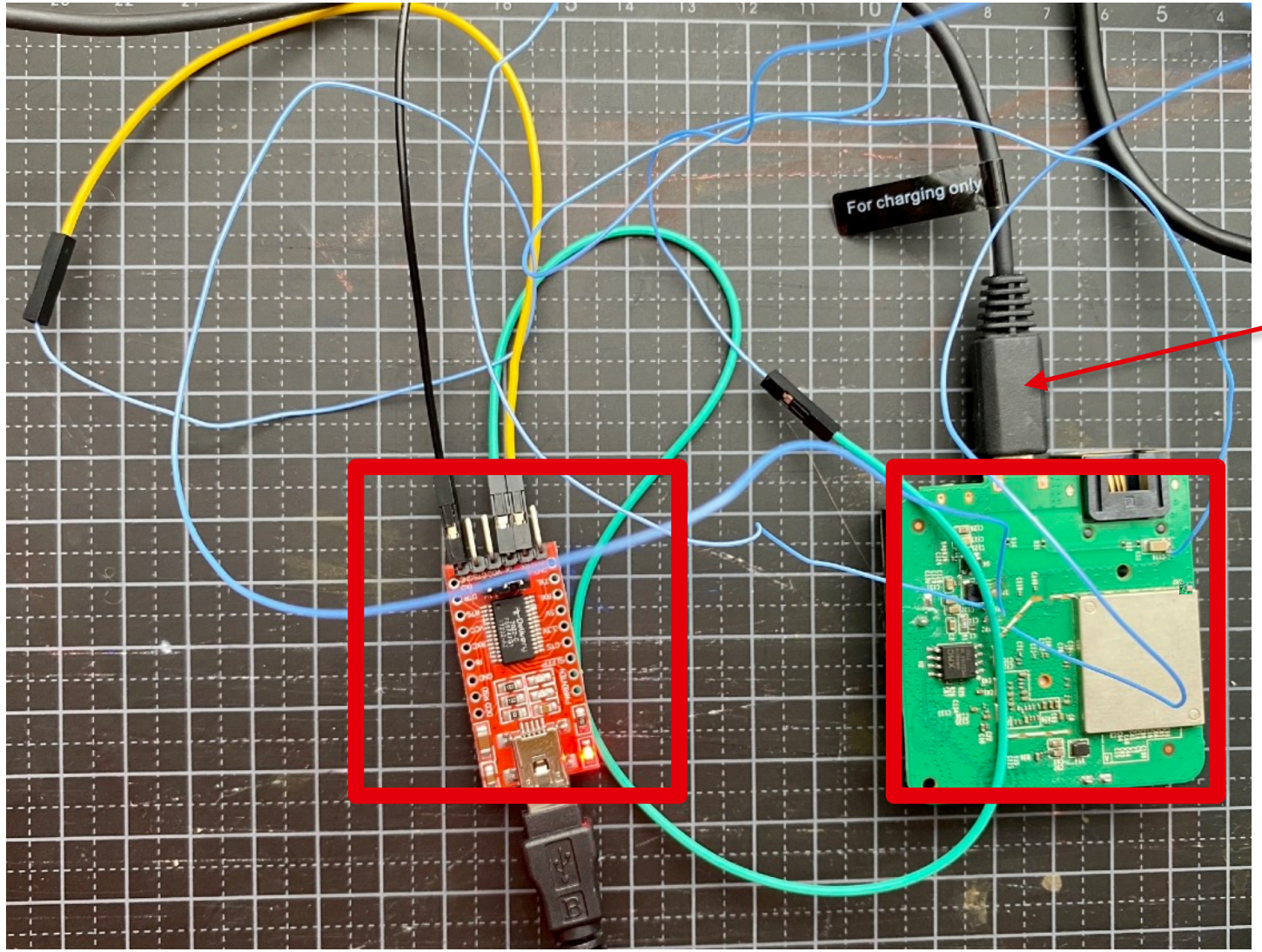
Baud rate



Common baud rates: **9600**, 14400,**19200**,.. **115200**

DEMO: UART sniffing

Image source: author collection



FDTI adapter
FT232RL

TOE Booting

TP-Link Nano

DEMO

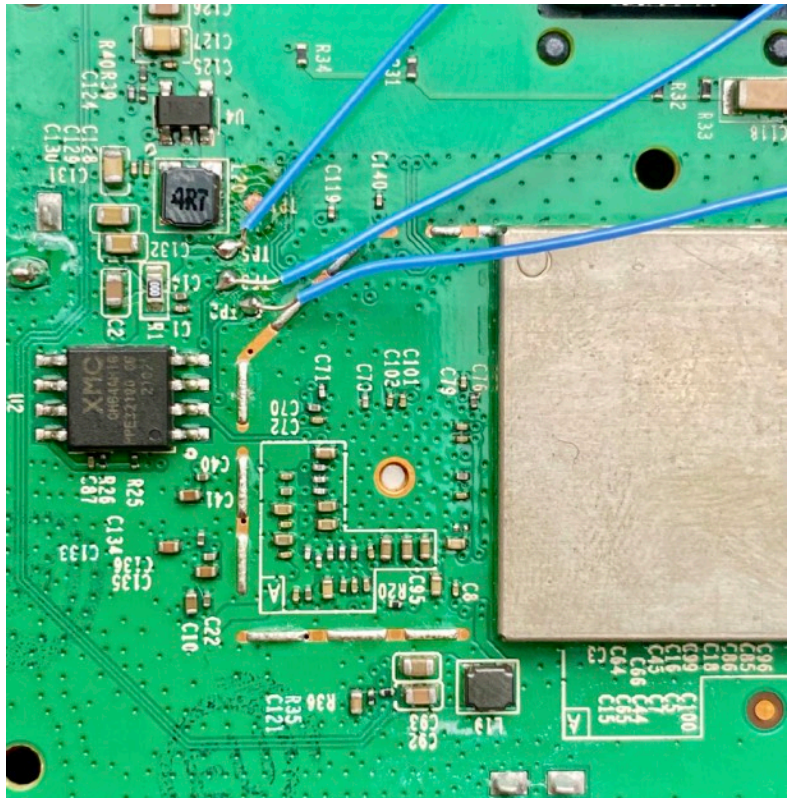


Image source: author collection

Summary

- Identify RX, TX, GND pins
- Connect to the pins (soldering may be involved)
- Connect ToE to PC via a FDTI adapter
- Power up ToE
- Indentify baud rate

ToE = target of evaluation

NEXT UP..

Next lecture:

Part 1. Serial interfaces

- SPI
- I2C

Part 2.Typical tools

- Bus Pirate
- Logic analyzer
- ….

Part III Adding security to COTS devices