Embedded Linux Conference
Europe

OpenIoTSummit
Europe

Linaro

# IoT TLS: Why It Is Hard

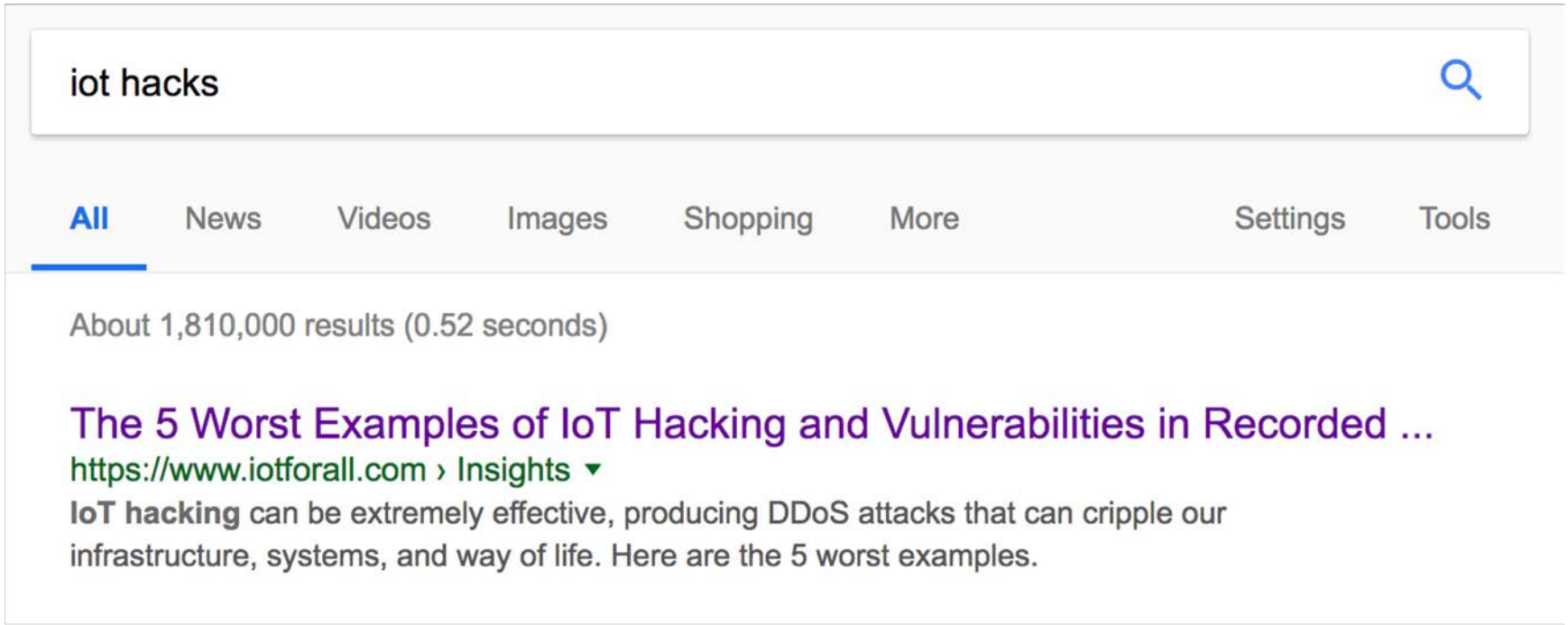
**David Brown**

THE LINUX FOUNDATION

# What is IoT

"The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."

— TechTarget


iot hacks
All
News
Videos
Images
Shopping
More
Settings
Tools
About 1,810,000 results (0.52 seconds)
The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded ...
https://www.iotforall.com › Insights
IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems, and way of life. Here are the 5 worst examples.


iot hacks
About 1,810,000 results (0.52 seconds)
The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded ...
https://www.iotforall.com › Insights
IoT hacking can be extremely effective, producing DDoS attacks that can cripple our infrastructure, systems, and way of life. Here are the 5 worst examples.

# 5 Worst Examples

- The Mirai Botnet
- The Hackable Cardiac Devices from St. Jude
- The Owlet WiFi Baby Heart Monitor Vulnerabilities
- The TRENDnet Webcam Hack
- The Jeep Hack

“IoT Security is not Interesting”

— James Mickens
Harvard University,
Associate Professor,
Authority on All Things

“TLS is the only good thing we have”

— James Mickens
Harvard University,
Associate Professor,
Authority on All Things

Raspberry Pi

- Memory: GBs
- Flash: GBs
- CPU: GHz

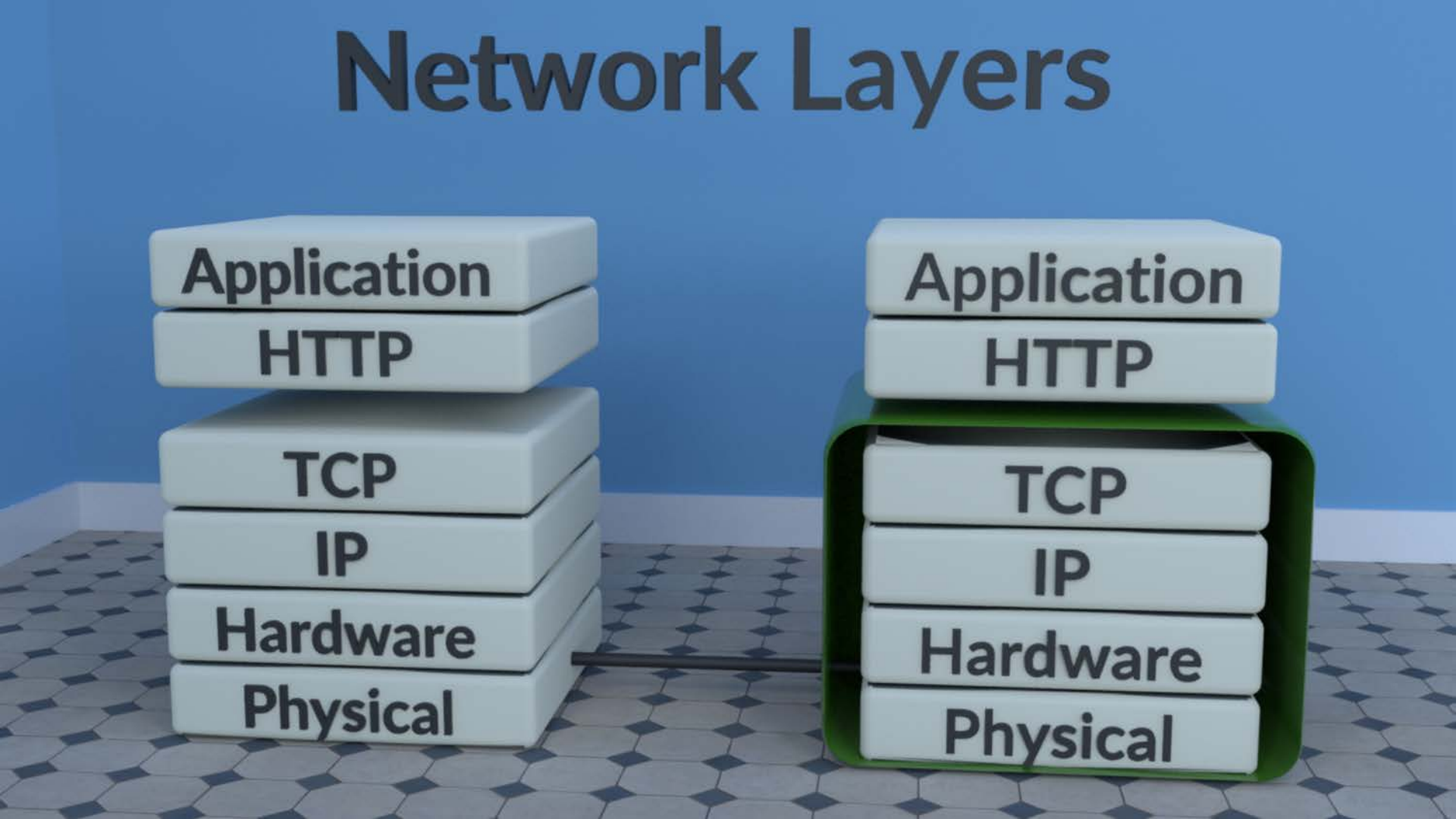
Tiny devices

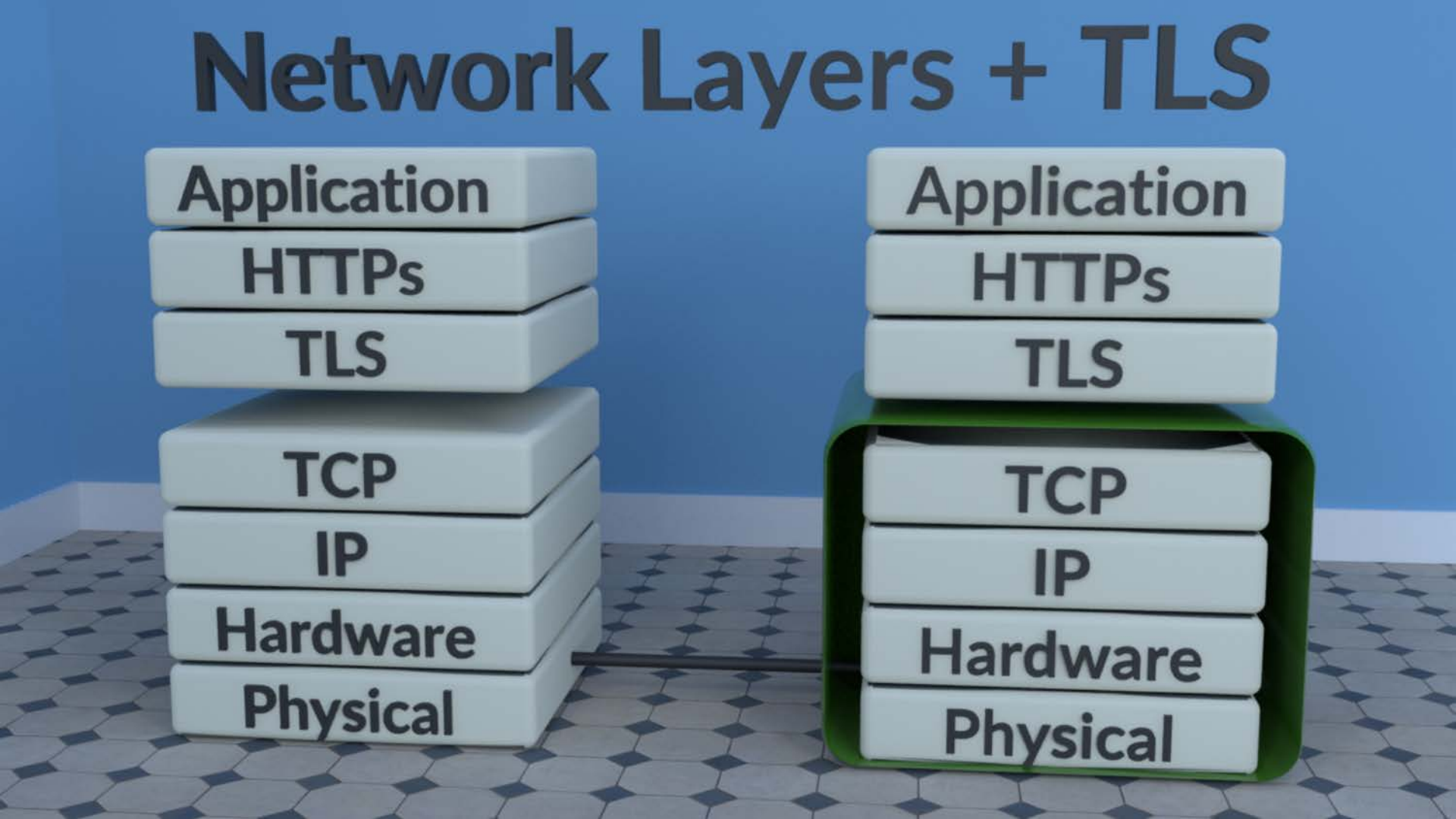
- Memory: 10s KB
- Flash: 100s KB
- CPU: 10s MHz

Middle Devices

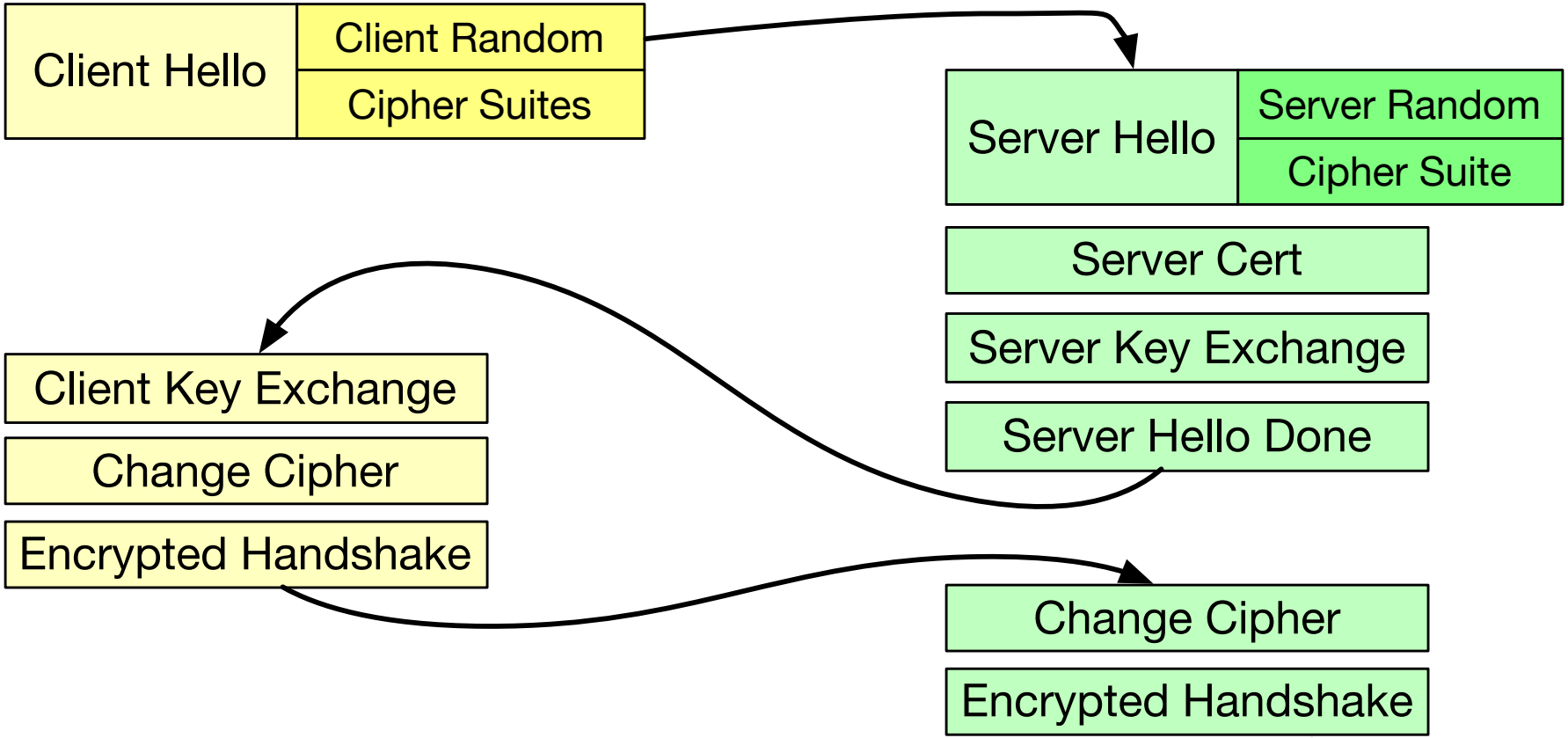
- Memory: 100s Kb
- Flash: 1Mb
- CPU: 10-100 MHz

# How Does TLS?


Network Layers
Application
HTTP
TCP
IP
Hardware
Physical
Application
HTTP
TCP
IP
Hardware
Physical


Network Layers + TLS
Application
HTTPs
TLS
TCP
IP
Hardware
Physical
Application
HTTPs
TLS
TCP
IP
Hardware
Physical

# TLS Handshake



# Handshake Requirements

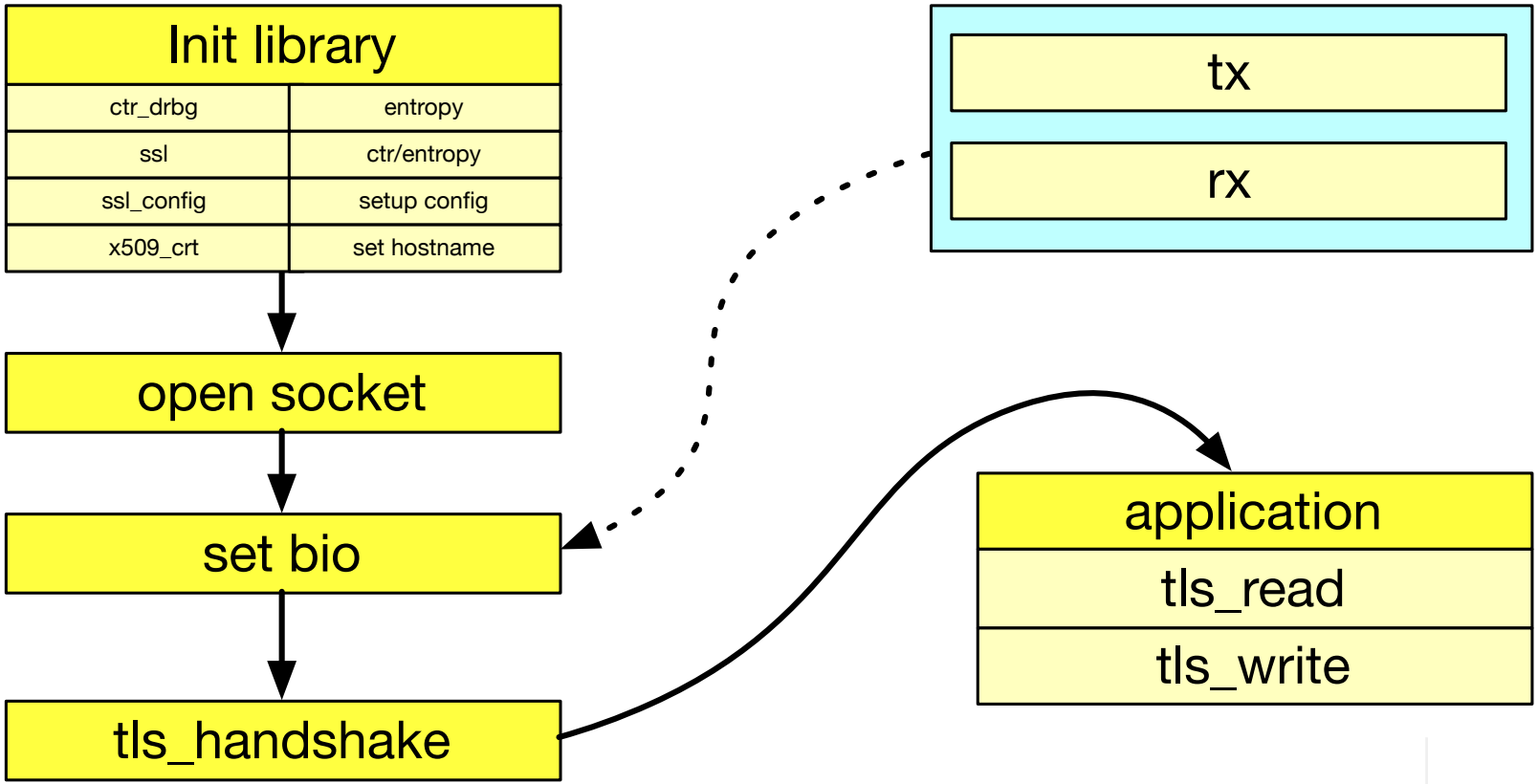
- Ciphersuite agreement
- Verification of certificate, **not optional**

  “TLS done incorrectly is worse than not using it at all. At least with no TLS you know that the communication is insecure.” — hallway talk at ICMC18

# Implementation Requirements

- Memory
- Time
- Randomness

# Traditional TLS API



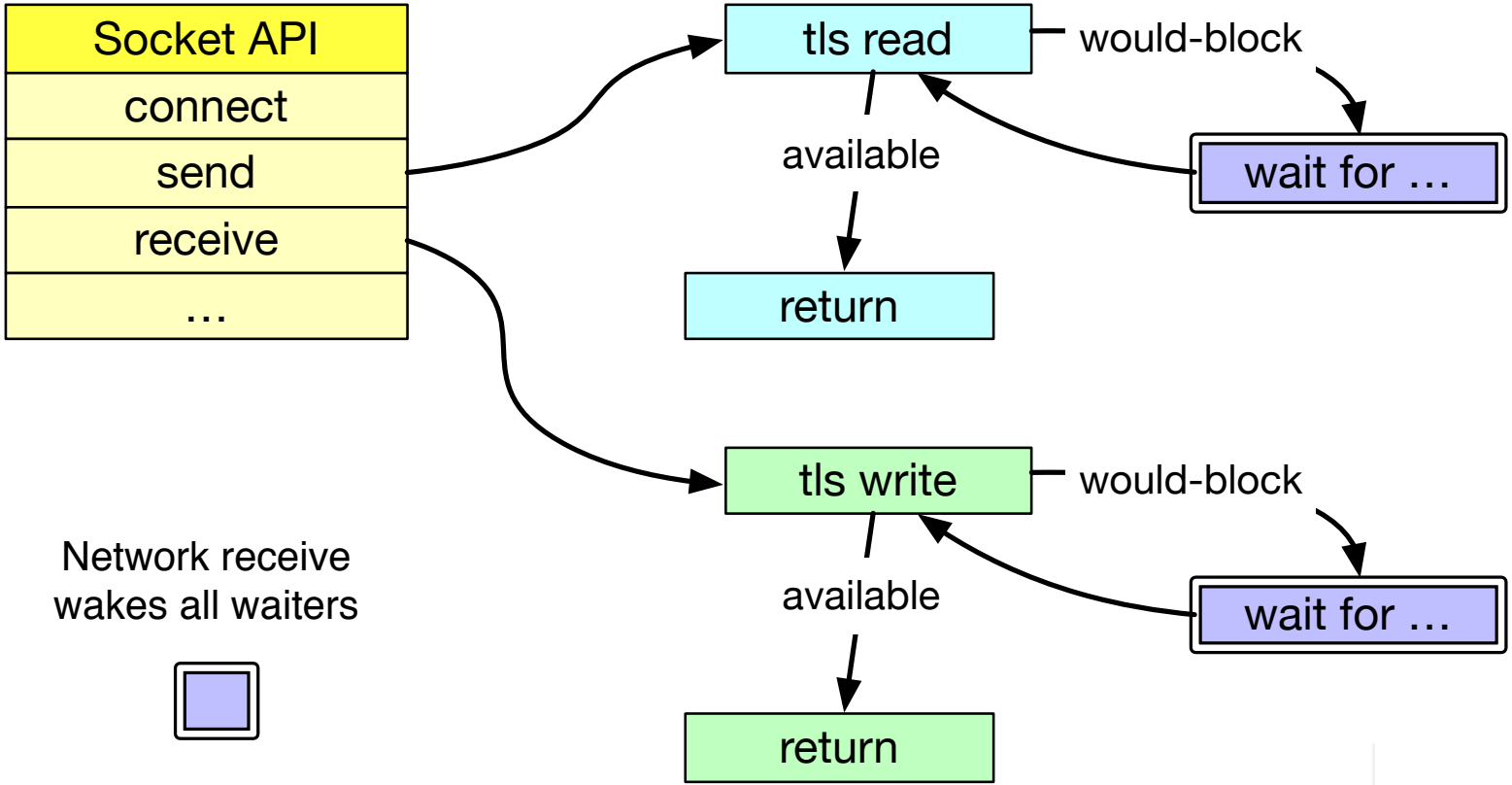
# Improving Layering

- Stream abstraction
  - Common in higher level languages
  - Same API for TLS and non-TLS
- Put under Socket API
  - Not really done in Linux (really, not done in Linux)
  - Keeps same API
  - The layering is wrong, though

# Zephyr’s Approach

- Second approach
- Already offloading support, including one that has TLS
- Abstractions are “scary”

# API Mismatch



# Where are we now?

- Video of a demo?
- Zephyr network API changes
- JWT, time, MQTT