

# Obtaining Firmware

---

The Path of Least Resistance

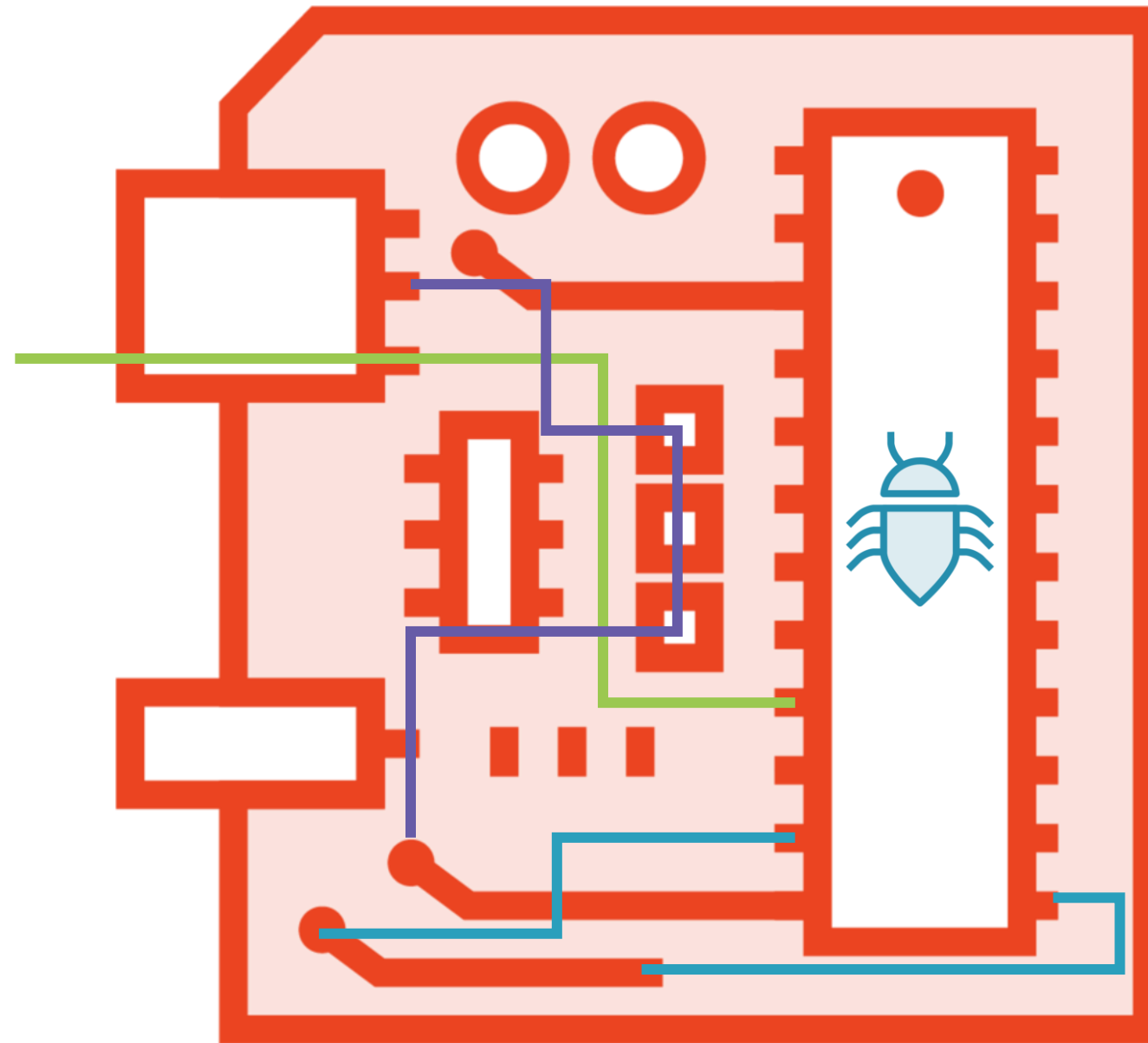


**Matt Lloyd Davies**

Capability Development Lead



# Firmware



# The Path of Least Resistance

**Do we need to?**

**The internet**

**Over serial via  
debug ports**





Flash memory size = 128Mb



Flash memory size = 128Mb

Dumped in hex



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space

64 bytes for error correction every 2 kbyte page



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space

64 bytes for error correction every 2 kbyte page

=> 3% overhead



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space

64 bytes for error correction every 2 kbyte page

=> 3% overhead

Dumped file =  $128 \times 3 \times 1.03 \sim 400\text{Mb}$



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space

64 bytes for error correction every 2 kbyte page

=> 3% overhead

Dumped file =  $128 \times 3 \times 1.03 \sim 400\text{Mb}$

Serial speed = 115,200kbps = 0.011 Mb/s



Flash memory size = 128Mb

Dumped in hex

=> 1 byte = 2 hex chars + 1 space

64 bytes for error correction every 2 kbyte page

=> 3% overhead

Dumped file =  $128 \times 3 \times 1.03 \sim 400\text{Mb}$

Serial speed = 115,200kbps = 0.011 Mb/s

Transfer time = 9.6 hours



# The Path of Least Resistance

**Do we need to?**

**The internet**

**Over serial via  
debug ports**

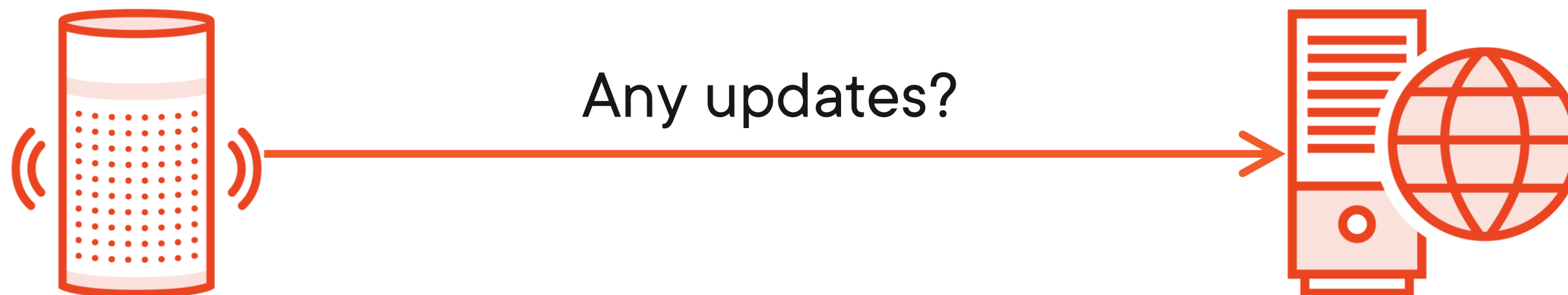
**Dump from flash  
memory**

**Dump via TFTP**



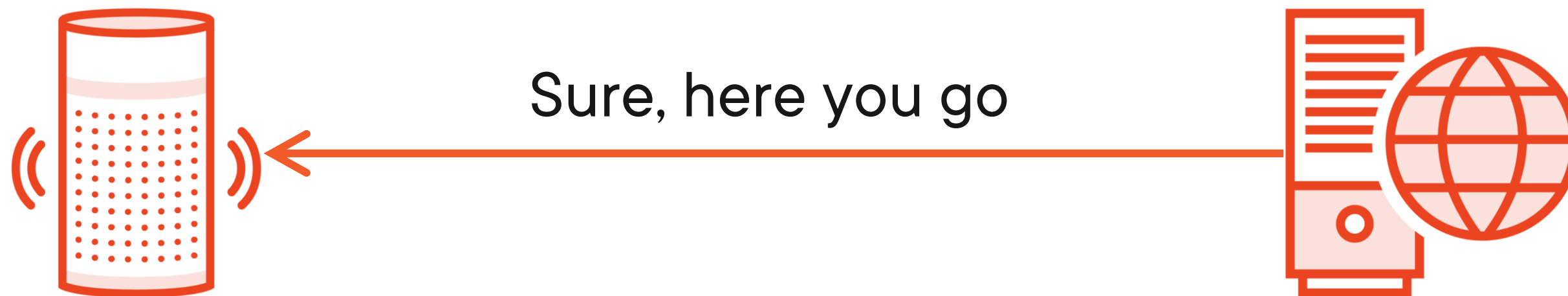


# Other Methods



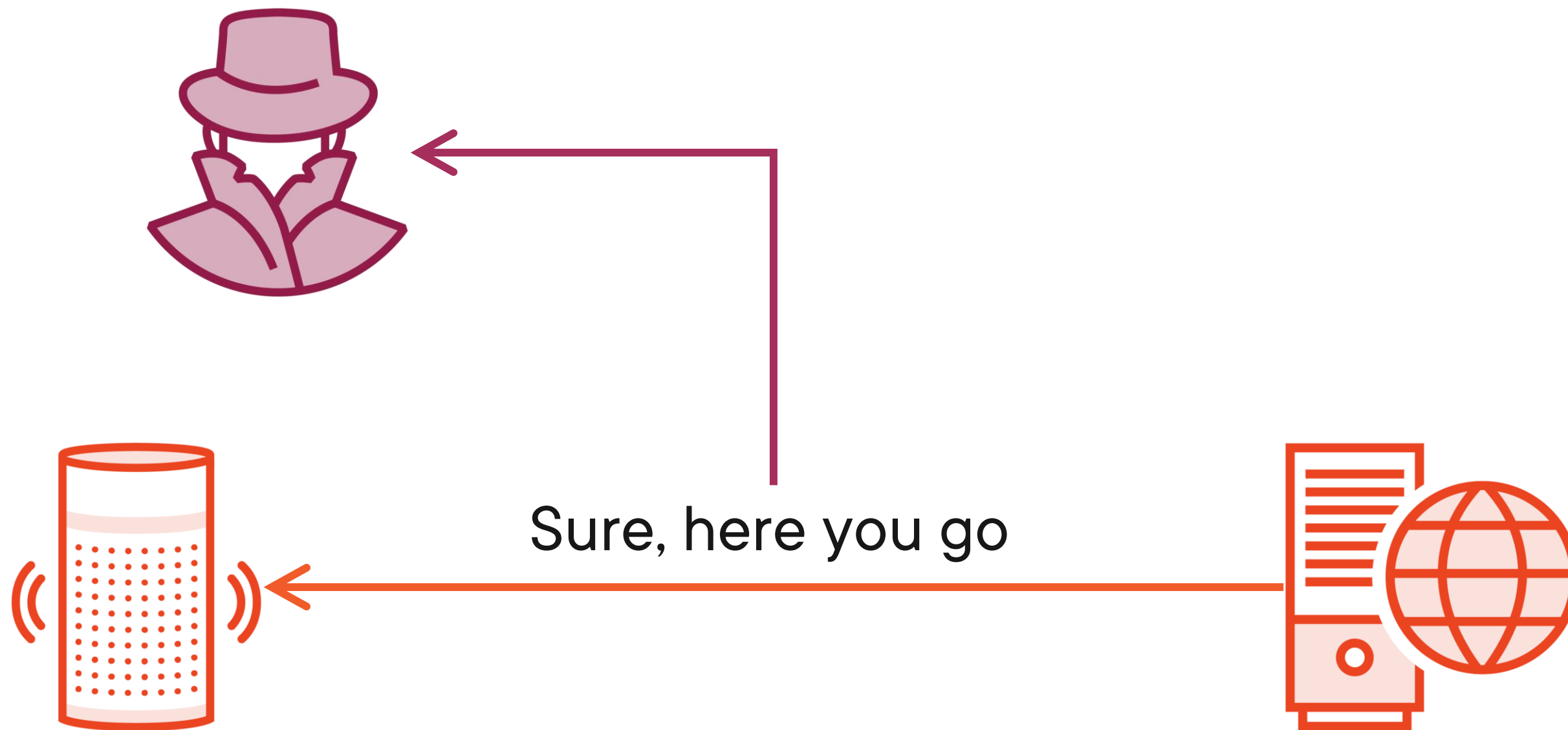


# Other Methods





# Other Methods





# Demo



**Do we need to?**







# Setup

The USB serial adapter is connected to the TL-WR841N serial pins.





# Demo



## Extract over serial







# Setup

The USB serial adapter is connected to the TL-WR841N serial pins





# Demo



## Dump from flash ROM

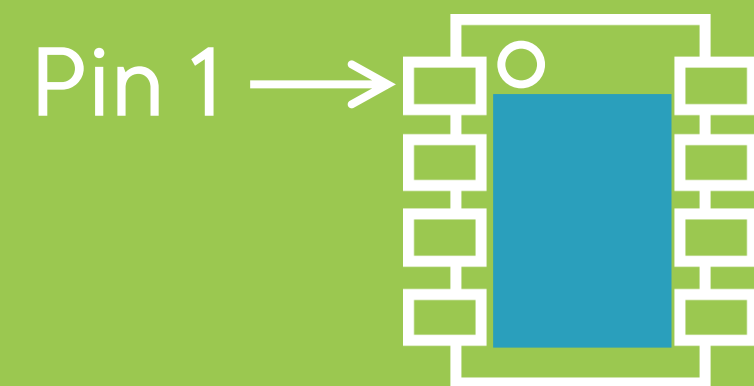






# Setup

The CH341A programmer is connected to the flash ROM chip using a SOIC clip. The red wire connects to pin 1.



# Demo



**Dump from RAM and TFTP out**







# Setup

The USB serial adapter is connected to the TL-WR841N serial pins, and an ethernet lead provides ethernet connectivity to the testing laptop.



# Up Next: Analyzing Firmware

---

