µProxy

A Hardware Relay for Anonymous and Secure Internet Access

David Cox & David Oswald
School of Computer Science
The University of Birmingham

Connections, Proxies, and IPs

User connects to server via a WiFi hotspot (e.g. in café)

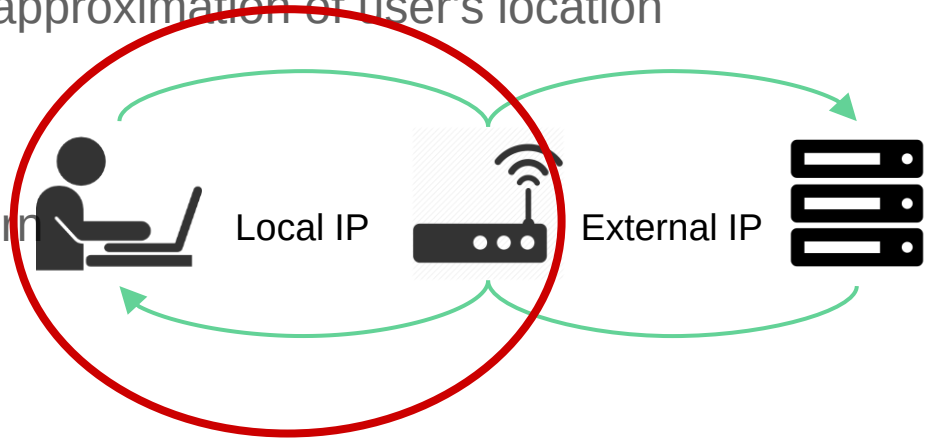
Hotspot uses an external IP to communicate with the server

External IP gives a real-time approximation of user's location

Leak of information

Privacy and anonymity concern

VPNs don’t help



What is µProxy?

A secure internet relay

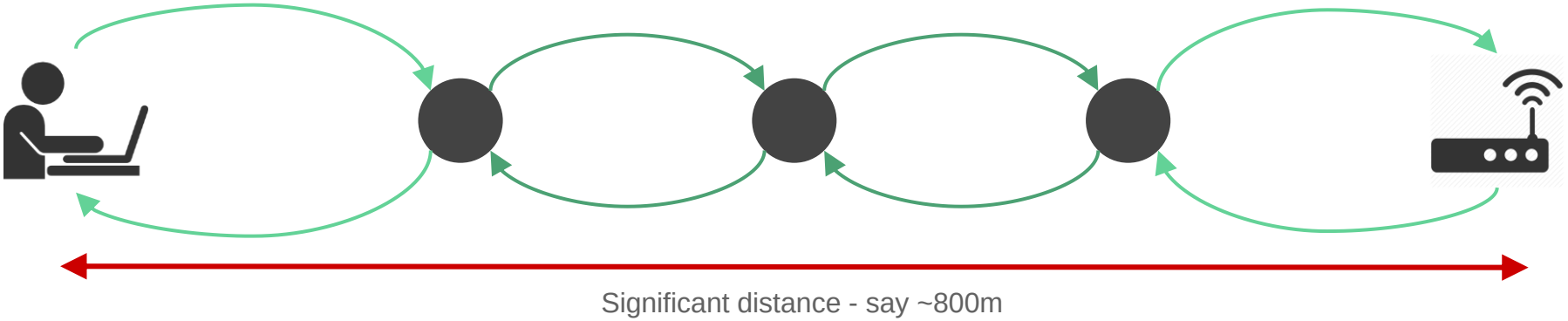
Using low-cost WiFi microcontrollers (32-bit, 80 MHz, *not* ARM)

Allows to connect to a WiFi from a distance in order to ...

… access a network without revealing physical location

Covert, secure, anonymous and affordable

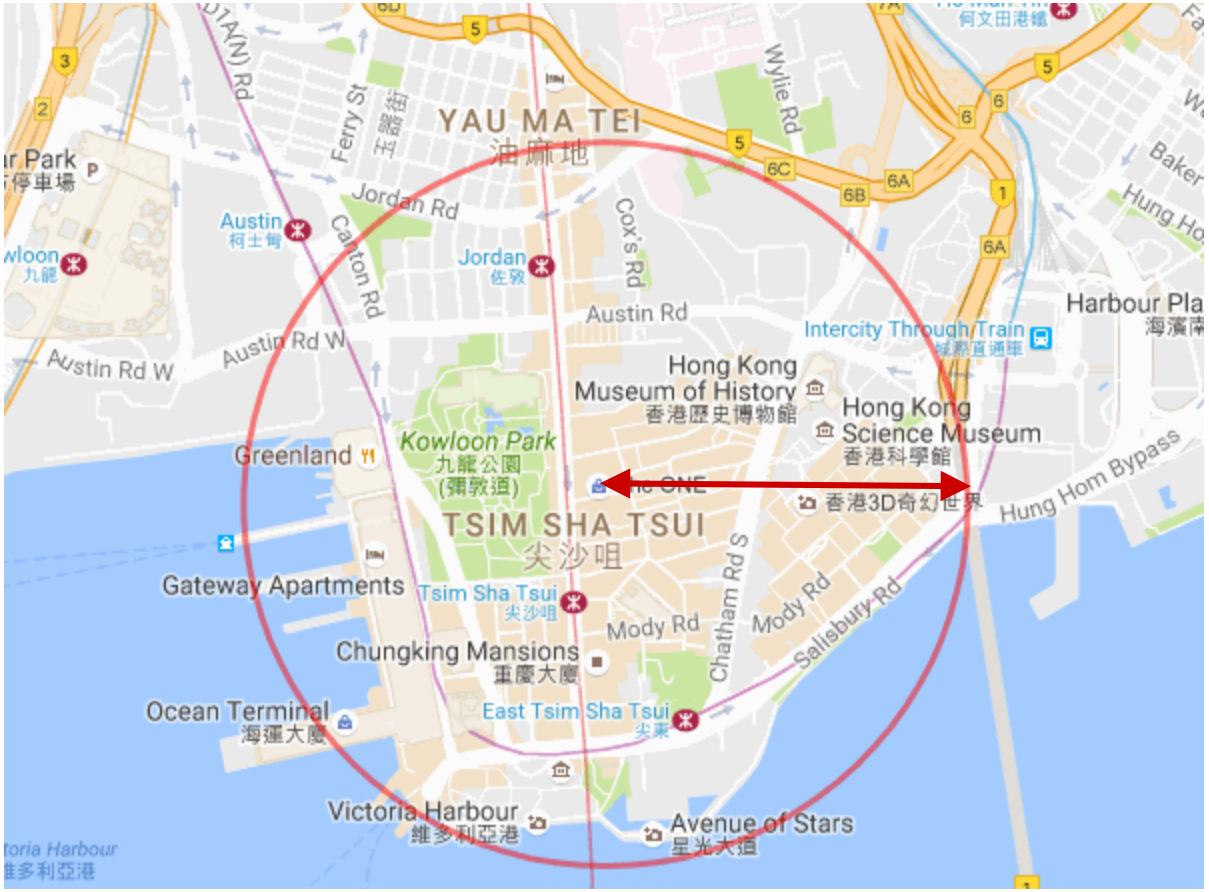
What is µProxy?



Relay formed of hidden wifi networks

Fully encrypted

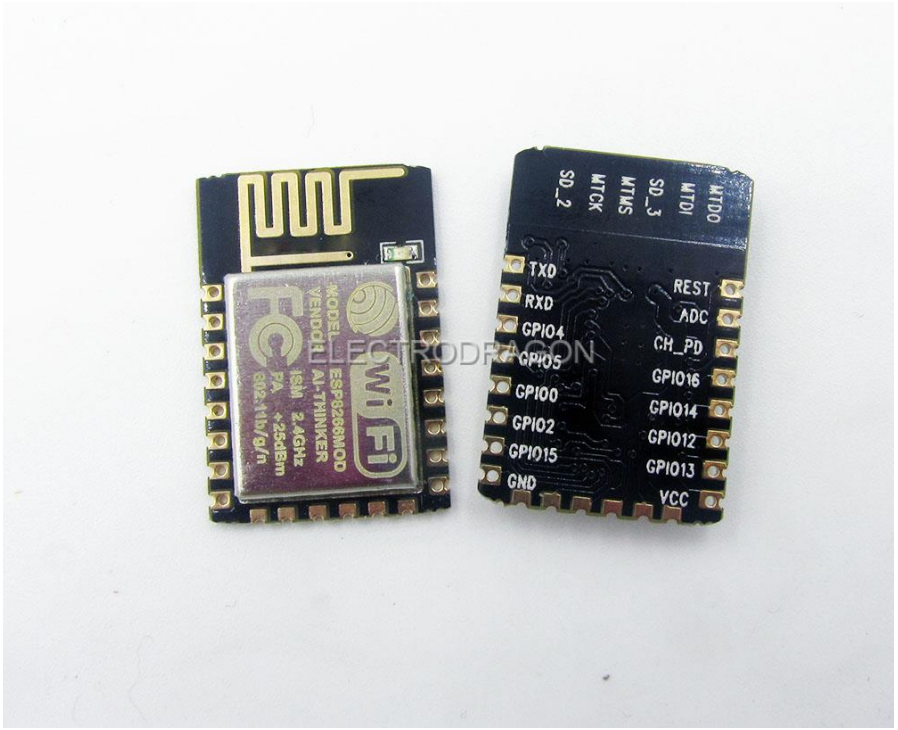
Each hop up to ~150m (under ideal conditions)



Not one building, but hundreds

Meet the ESP8266

- WiFi microcontroller
- Billed as the ‘go to’ IoT board
- Station, Access Point or both
  - Software defined
- $3.50 price point
  - Previous relay cost < $50
- Dimensions 24mm - 16mm
  - Can be hidden



Cryptography on IoT Devices

Huge security issues in the IoT
(cf. recent DDoS attacks)

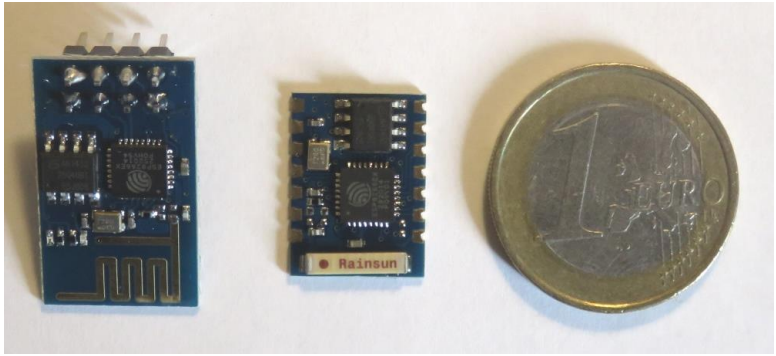
ESP8266 standard mechanisms have
Questionable security (ESPnow)

But encryption is key to µProxy, so
we added some of our own

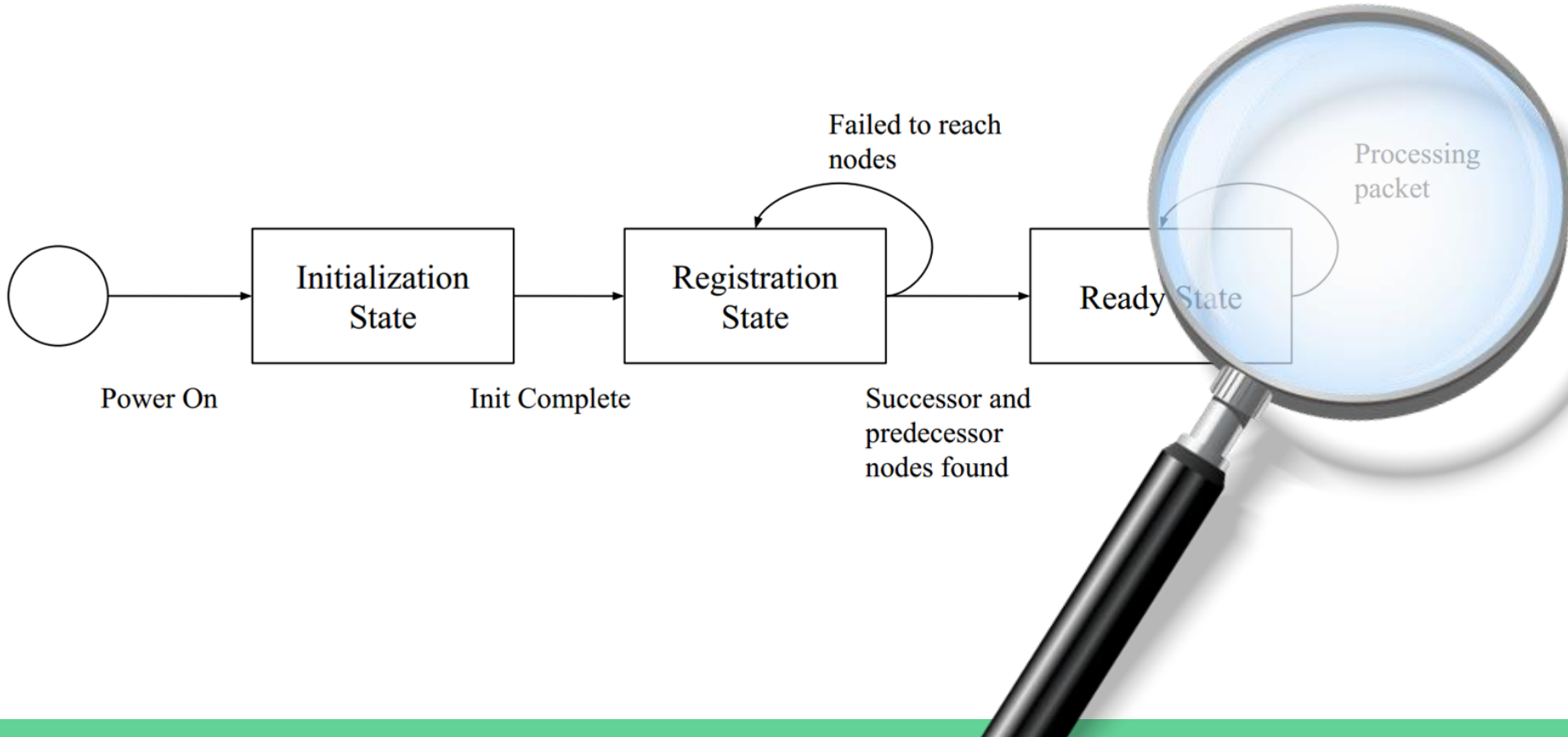
NaCL (C crypto lib) ported to ESP8266

µProxy uses:

Curve25519 for the initial key exchange



Robustness: Protocol State Machine

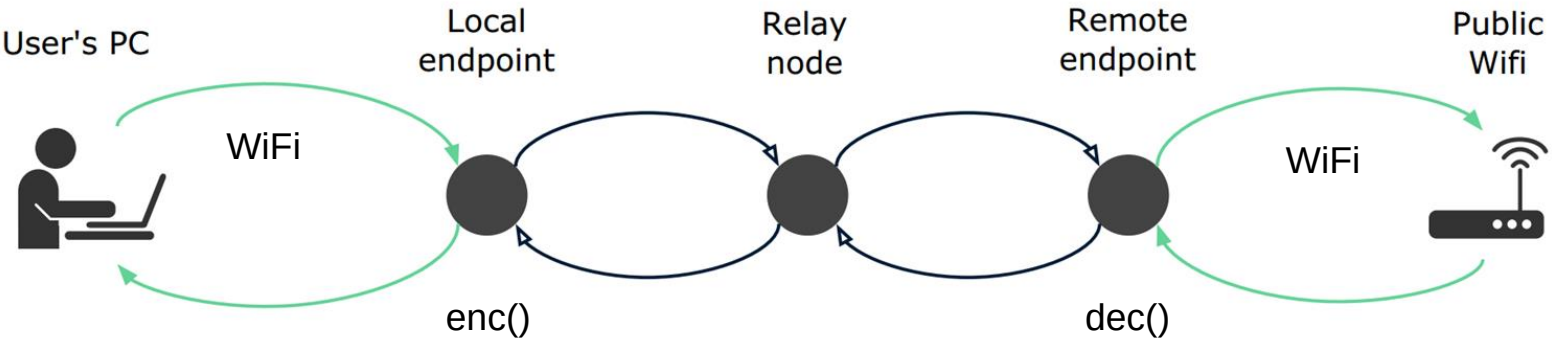


Protocol Design

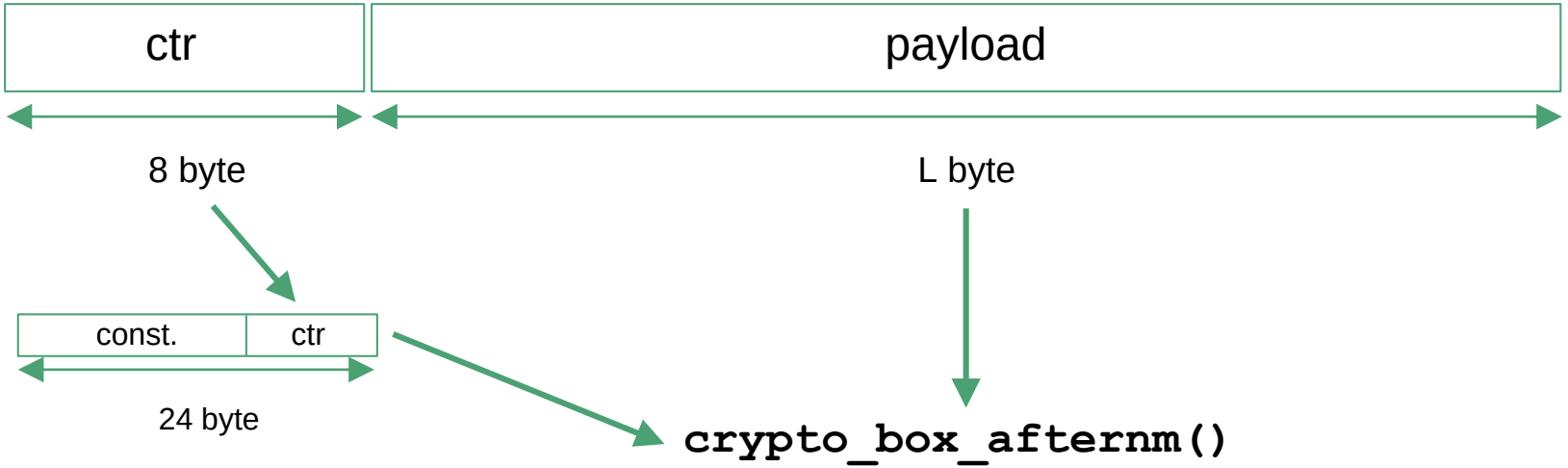
Initial key exchange between endpoint nodes using Curve25519

Hardcoded public keys

Afterwards: authenticated encryption channel between local and remote endpoint (symmetric crypto only, using `crypto_box_afternm()`)



µProxy Packet



Performance Evaluation

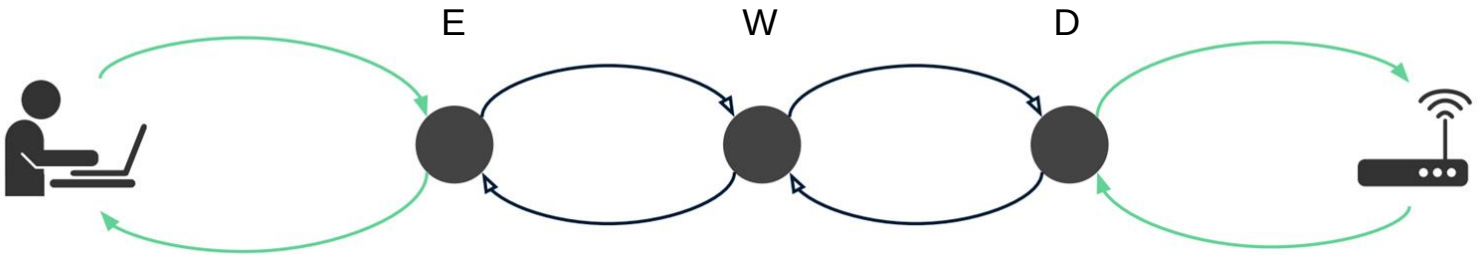
Measured: time for encryption E = 1.9 ms, for decryption D = 2.3 ms
(done only at endpoints)

N nodes in the relay

Estimated latency per node W = 20.4 ms

Ro[illegible]

e.g



Security Evaluation

Aim to achieve security equal to typical connections with added location privacy

Assumptions:

- Local endpoint is secure
- All nodes are initially secure

Only endpoints need keys

- leaves us with one vulnerable node

If an adversary reaches the remote endpoint you're already in trouble

Conclusions

Low-cost WiFi relay

Can have other uses apart from location privacy

Open-source project soon available at: https://github.com/david-oswald/microproxy

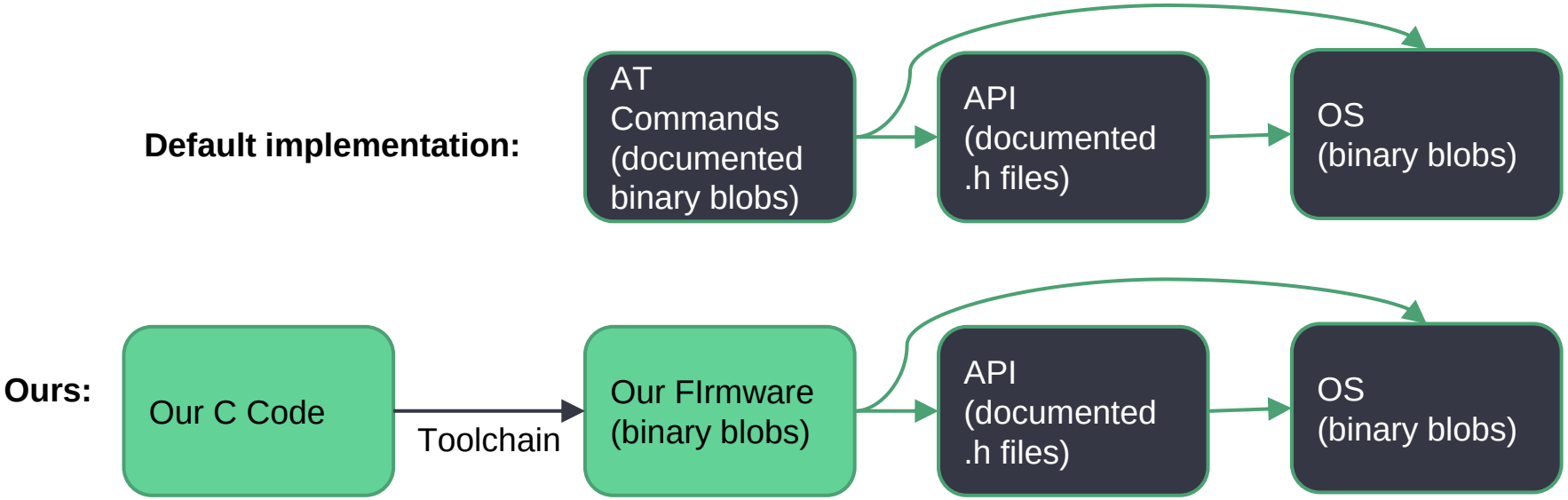
Possible extensions:

- More automation
- Period re-keying
- Full forwarding of e.g. VPN traffic

Thank you, any questions?

github.com/david-oswald/microproxy

Firmware architecture



DEMO???