RIPE NCC
RIPE NETWORK COORDINATION CENTRE

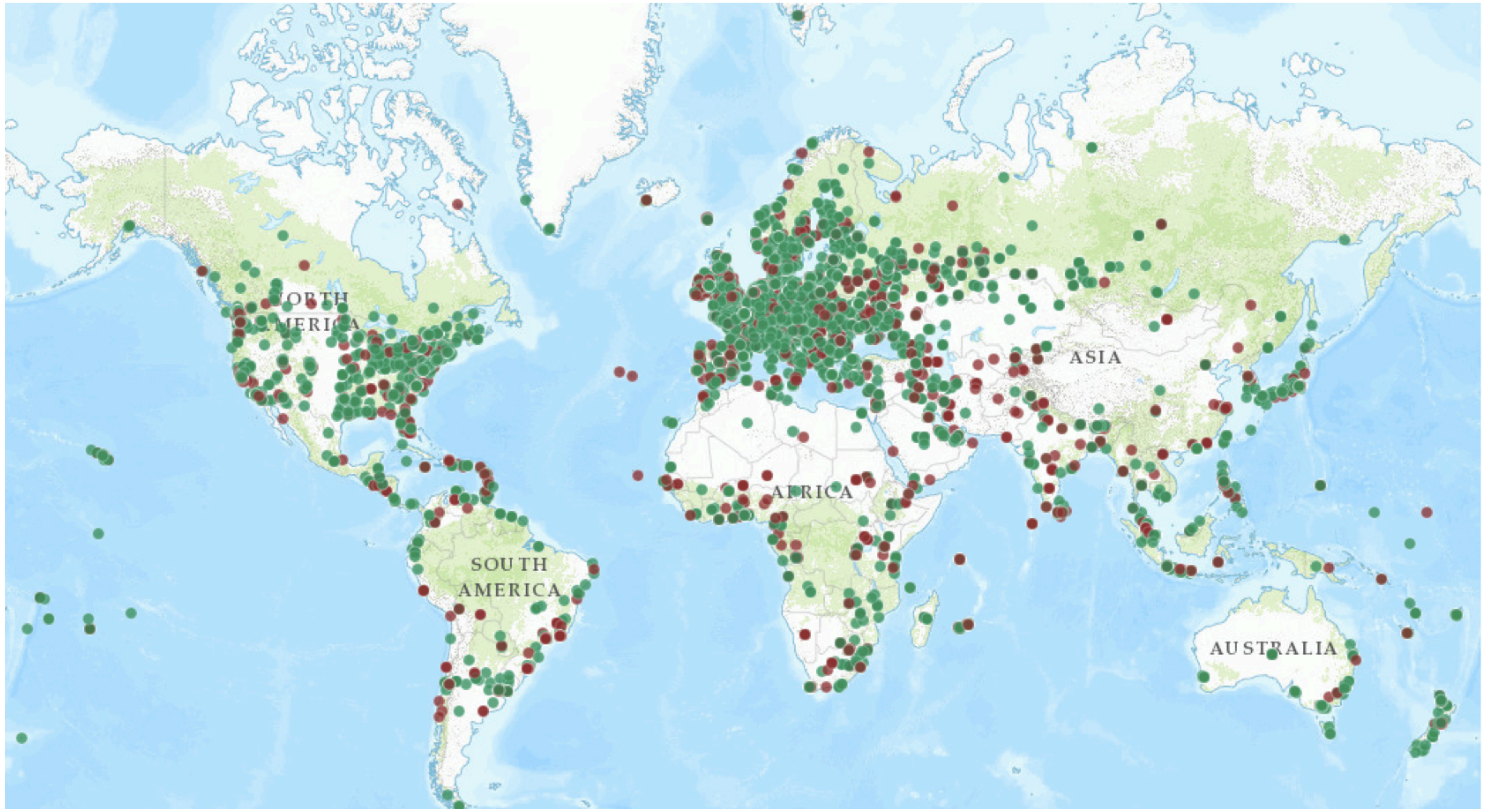
RIPE Atlas

Ethical and Security Aspects of Running an IoT Network

Mirjam Kühne | May 2019 | RIPE 78 Meeting

RIPE Atlas Infrastructure

RIPE Atlas is a **global, open, distributed** Internet measurement platform, consisting of thousands of measurement devices that measure **Internet connectivity** in real time. (wikipedia)



RIPE Atlas Use Cases

- Measuring Internet access disruptions
  - Internet Access Disruptions in Turkey
  - Internet Access Disruption in Gambia
- Measuring DNS censorship and hijacking
  - Using DNS Servers in Iran
  - DNS Censorship
- Monitoring connectivity problems
  - Monitoring Game Service Connectivity
  - Measuring Cloud Connectivity
  - Debugging Network Connectivity Problems

RIPE Atlas in Numbers

- 10,000 probes and 400 anchors connected worldwide
- 5.6% IPv4 ASes and 9% IPv6 ASes covered
- 181 countries covered
- 7,000 measurements per second

Design Principles

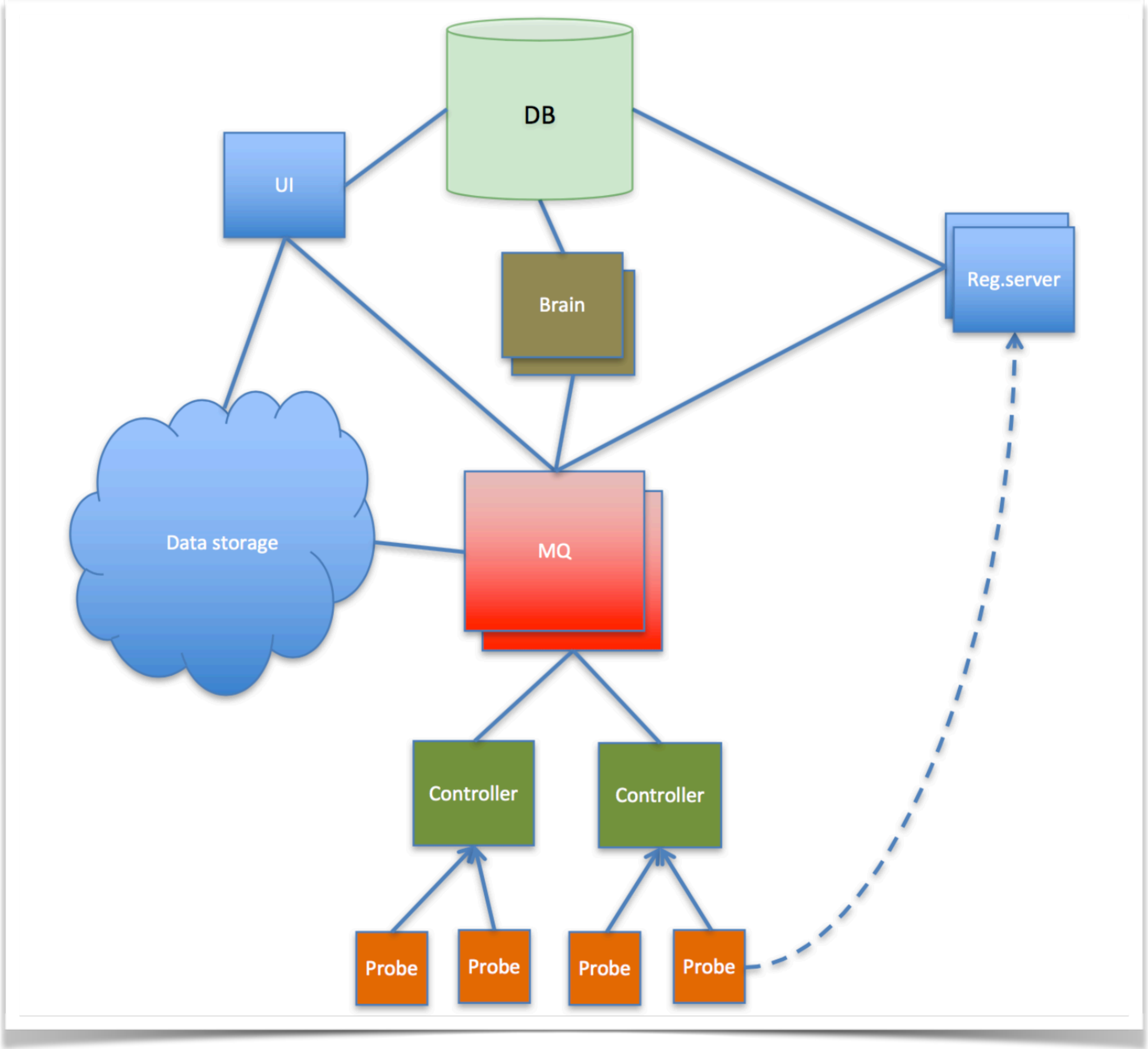
- Low, cheap barrier of entry
- Active measurements only
  - Probes do not observe user traffic
- Data, API, tools, source code: FREE and OPEN
- Set of measurement types limited
  - ping, traceroute, SSL/TLS, NTP, HTTP (limited)
- Strong community involvement from the start

Ethical Considerations

- No bandwidth measurements
  - Other platforms provide that service
- HTTP measurements only towards RIPE Atlas anchors
  - Otherwise it would rely on hosts' bandwidth
  - And might put volunteer at risk
- We encourage users to think about ethical considerations
  - Ethics of RIPE Atlas Measurements

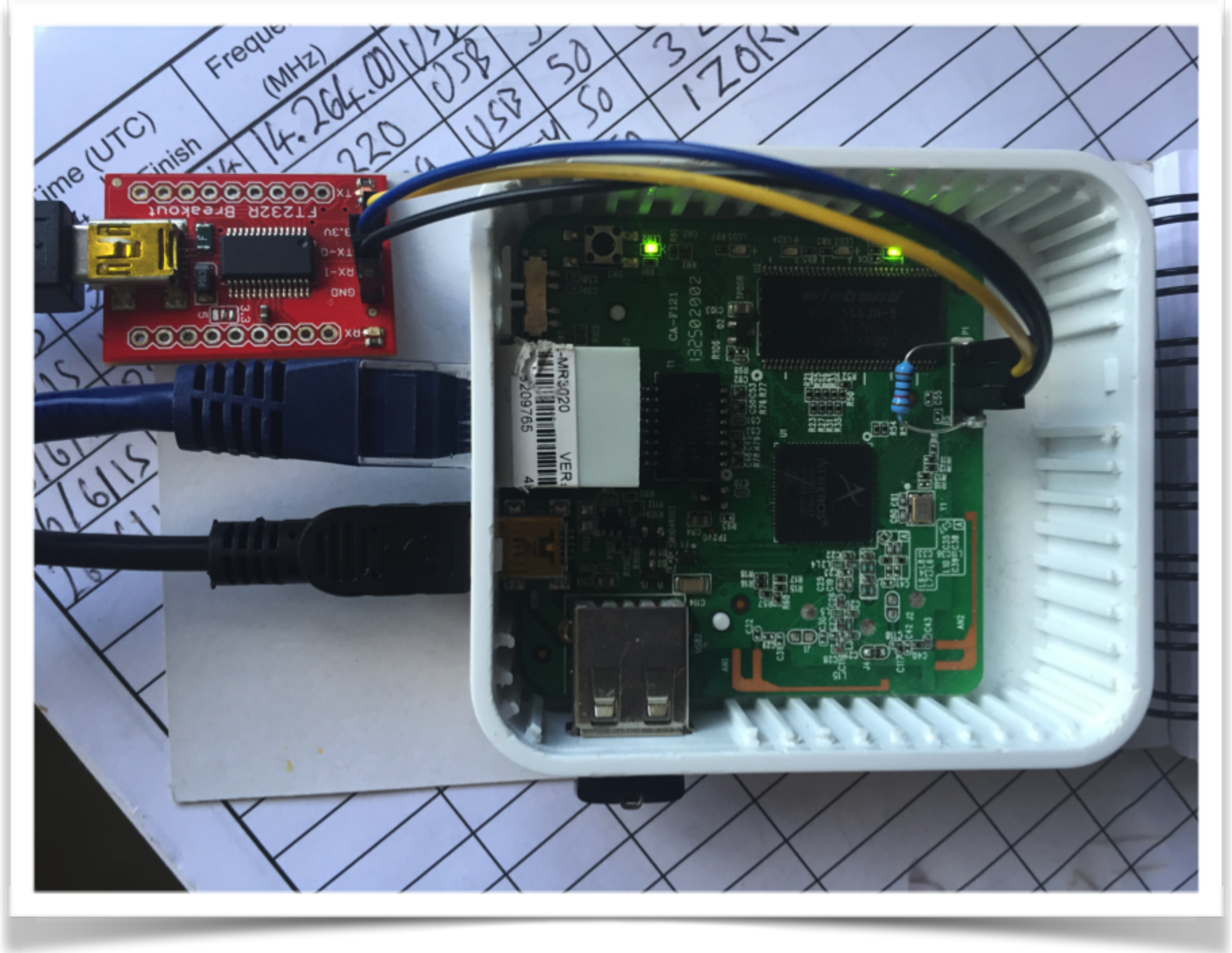
Securing RIPE Atlas

RIPE Atlas Architecture



How We Limit Consequences (1)

- Prevent re-use and re-purposing of probes
  - Decided against Trusted Platform Model (TPM)
  - Instead, we use cheap devices and discourage re-using them
  - Accepting possible loss of probes
- Initialisation procedure before distribution
  - Off-the-shelf firmware gets replaced with RIPE Atlas firmware
  - Generating and registering individual keys
  - Testing



How We Limit Consequences (2)

- Trust anchors installed on all probes
  - Two-way authentication; unique SSH key for probes and for identification
- Regular firmware updates
  - All firmware updates are signed
  - Pre-installed public keys to verify firmware signature before upgrading
- Mechanisms to detect unwanted behaviour
  - We’re looking for outliers or protocol violations
- No direct services to host or network
  - No local configuration possible; reduces network-based attack surface

Firmware Upgrades

- Done in a “lazy fashion”
  - Upgraded next time probes connect to RIPE Atlas infrastructure
  - We have means to force them to upgrade faster
- Each update is cryptographically verified

Best Current Practices

- IETF draft document: BCP for Securing IoT Devices
  - https://tools.ietf.org/html/draft-moore-iot-security-bcp-01

- RIPE Labs: https://labs.ripe.net
  - RIPE Atlas Probes as IoT Devices
  - RIPE Atlas Architecture - How we Manage our Probes