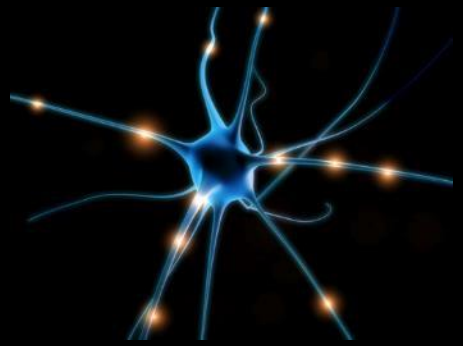


nquiringminds

Why is IOT security so hard and what can we do about it?

IoTSF 6/12/16

Dr Nicholas Allott

WHAT DO THE FOLLOWING HAVE IN COMMON

SmartCities

inds

Industry 4.0

Connected Car

Connected Health

SECURITY BACKGROUND

Trusted Execution Environment TR1/0

Web Application Security Model: W3C/ DAP. WoT Groups

Peer review Most Secure 22 IOT Middleware's –Open Source

Joint project IOT Security University Oxford

Released product addressing “most” of issues raised

nquiringminds

SETTING THE SCENE

IOT COMPONENTS

nquiringminds

Cloud

Switch

IOT Router

Bulb

Almost ALL IOT deployments follow this same basic architecture

IOT NEWORKS

nquiringminds

Cloud

IOT Router

Bulb

Switch

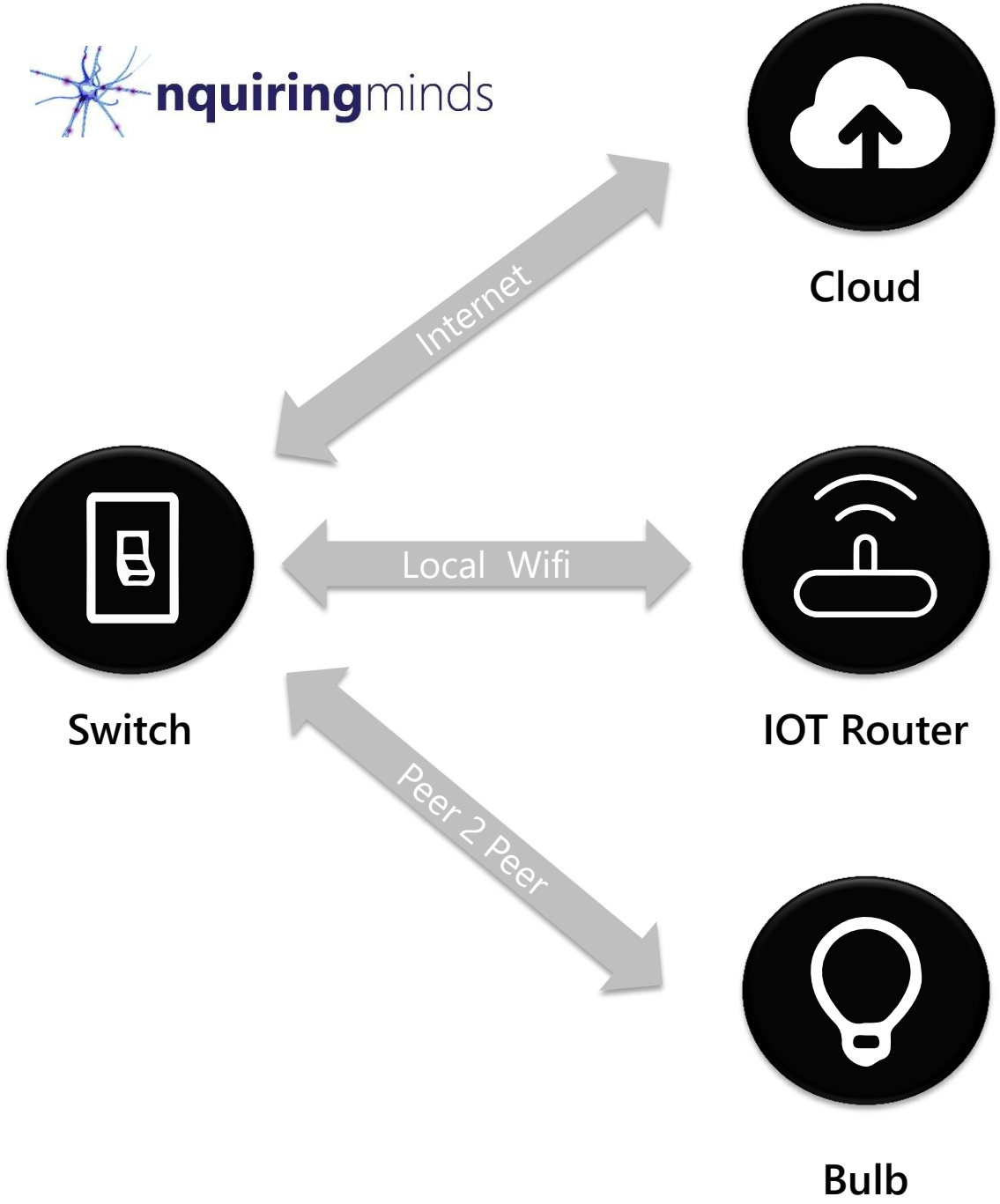
IP NETWORK

IP cloud network could be over fixed or mobile. Note mobile can have different connectivity constraints. Domestic WIFI can be tricky

NON IP

Most real IOT networks do not support IP. 802.15.4, LoRa, SigFox etc.

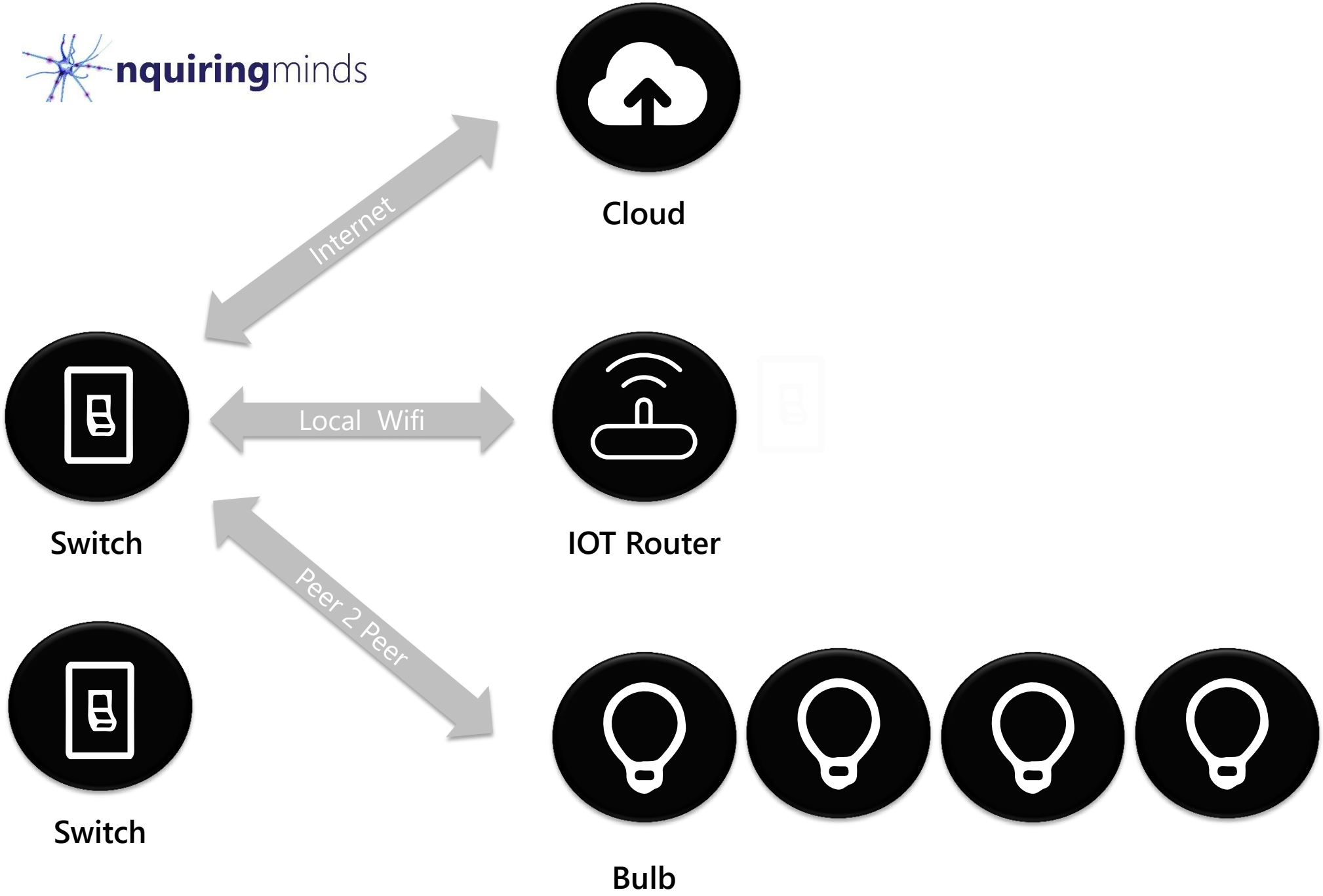
IOT CONNECTIITY SCENARIOS



I want to turn on my lightbulb from my mobile application, at work, my mobile application from home or from built in switch

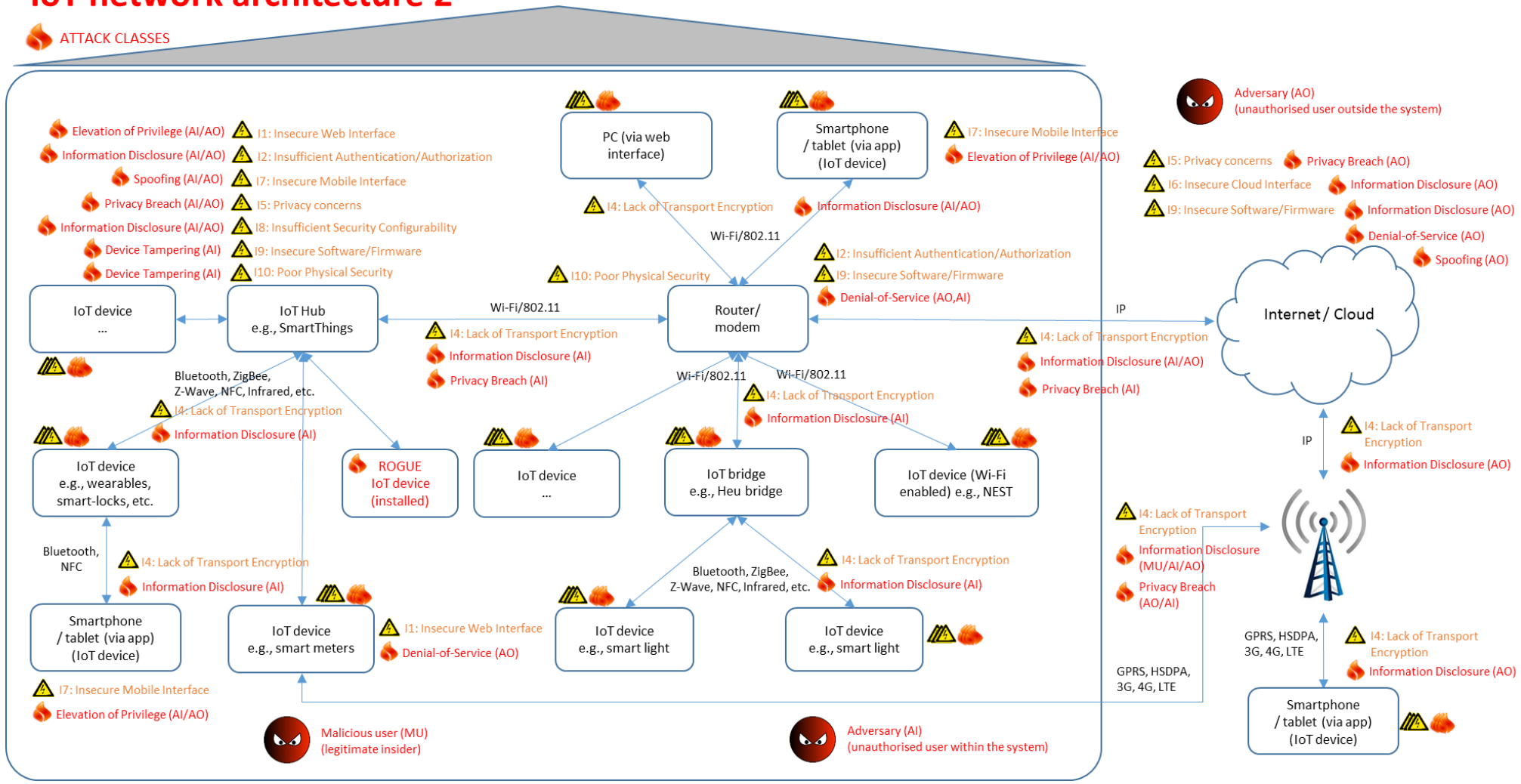
Need consistency of naming/addressing, and transparent routing in all scenarios

THE GROUP PROBLEM



nquiringminds

IoT network architecture 2



THREAT ANALYSIS

nquiringminds

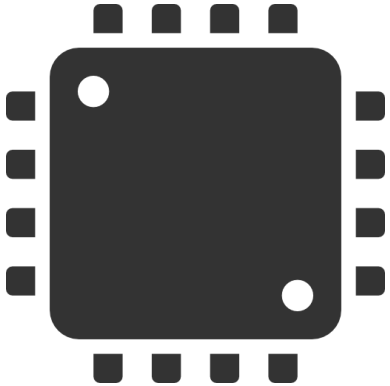
PHYSCIAL CHALLENGES

nquiringminds

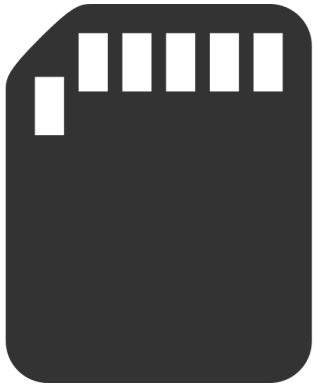
CONSTRAINTS

$2

2 years



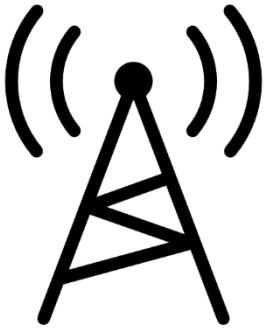
20Mhz



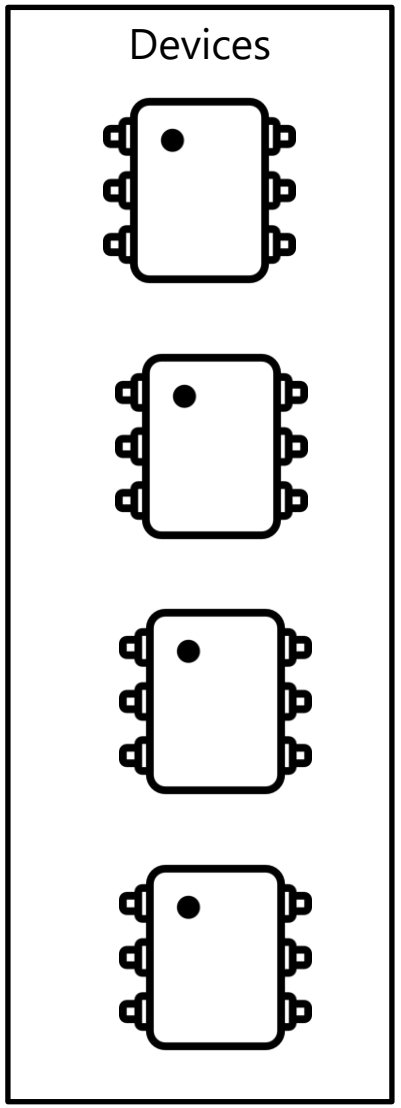
64 Kb

nquiringminds

HETERTOGENEITY



IOTDB	GSM	BluetoothLE
SensorML	Weightless-N	6LoWPAN
Thread	Weightless	ZigbeeIP
OMA	IEEE 1451: ++	Zigbee
MQTT	WirelessHart	802.15.4
CoAP	DigiMesh	2.4 MhZ
SMS - Signal	ISA100.11a	Dash 7
SMS	NFC	SigFox
LTE	ANT	868 MhZ
3GPP	EnOcean	433 MhZ



Cant use bearer level crypto

nquiringminds

IOT NETWORKING

IOT Router

No reliable transmission

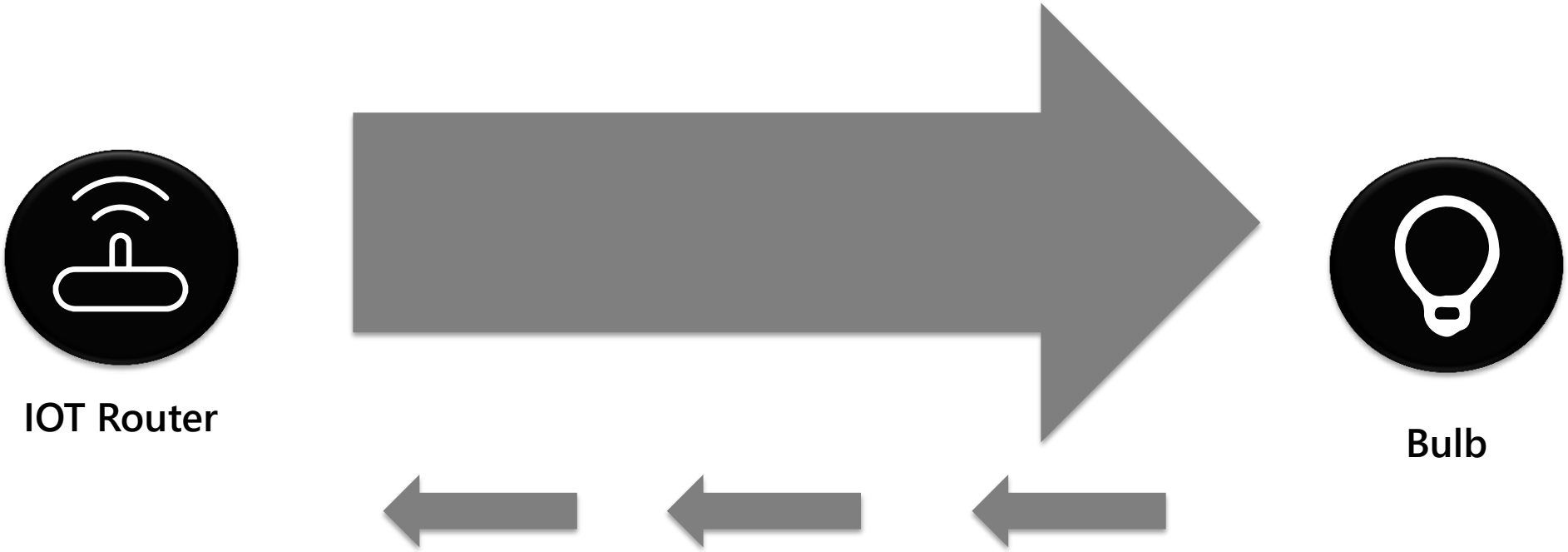
No retries

Tiny packet size

Bulb

NO I IN IOT

nquiringminds



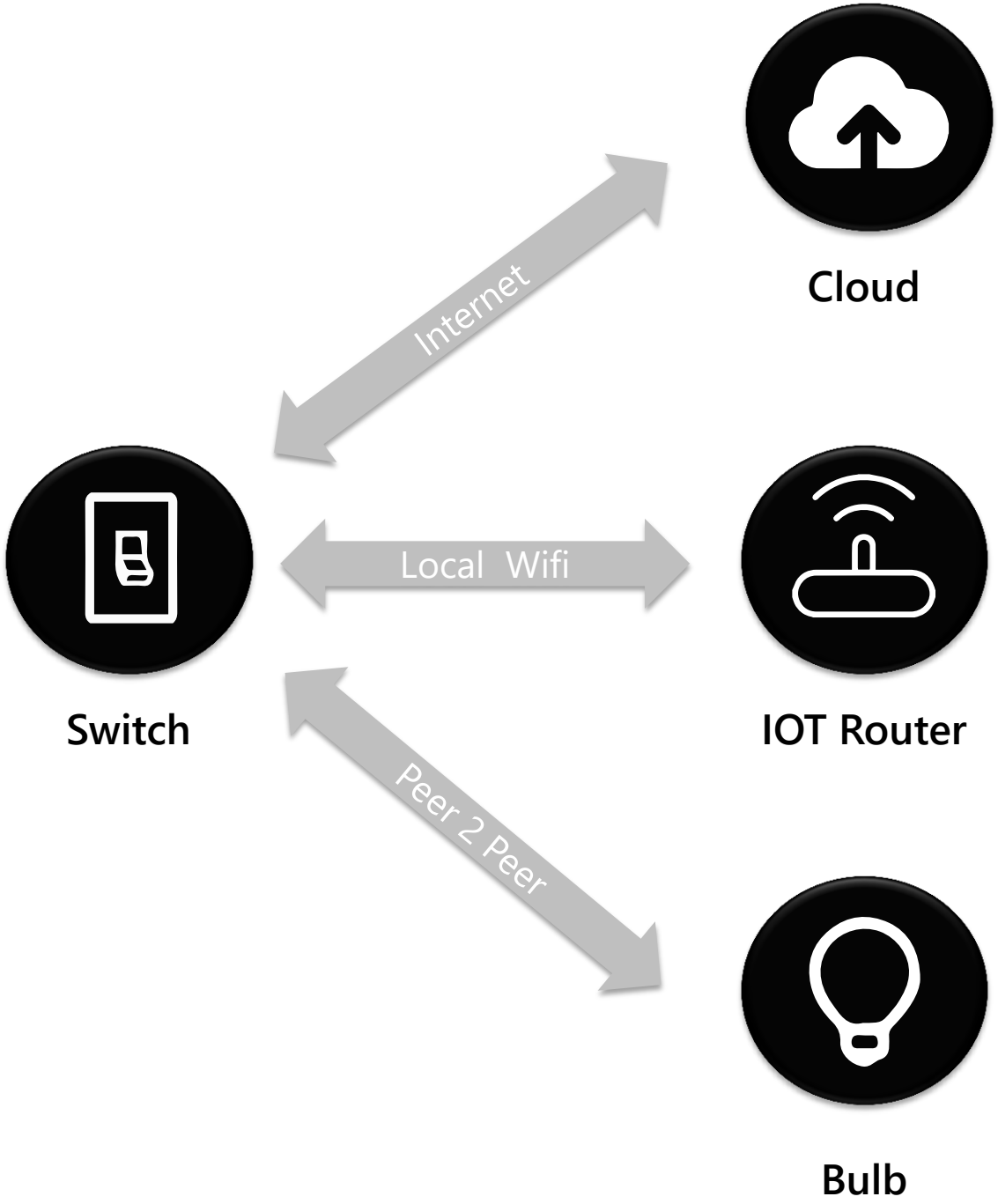
Asymmetry and Asynchronicity

IOT NETWORKING 2

nquiringminds

ADDRESSING

Same connection address?

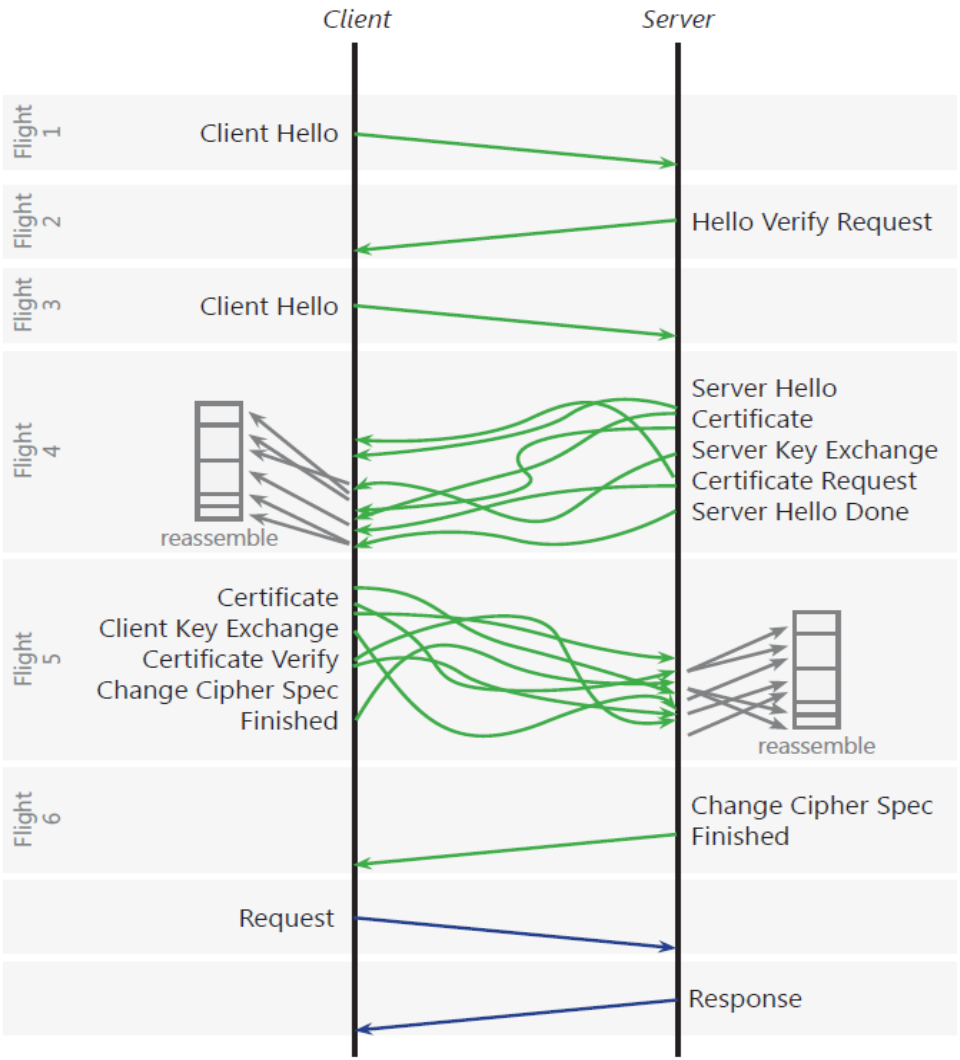


nquiringminds

CRYPTO CHALLENGES

DEVICE IDENTITY

nquiringminds



I-D.hartke-core-codtls

CoAP with DTLS

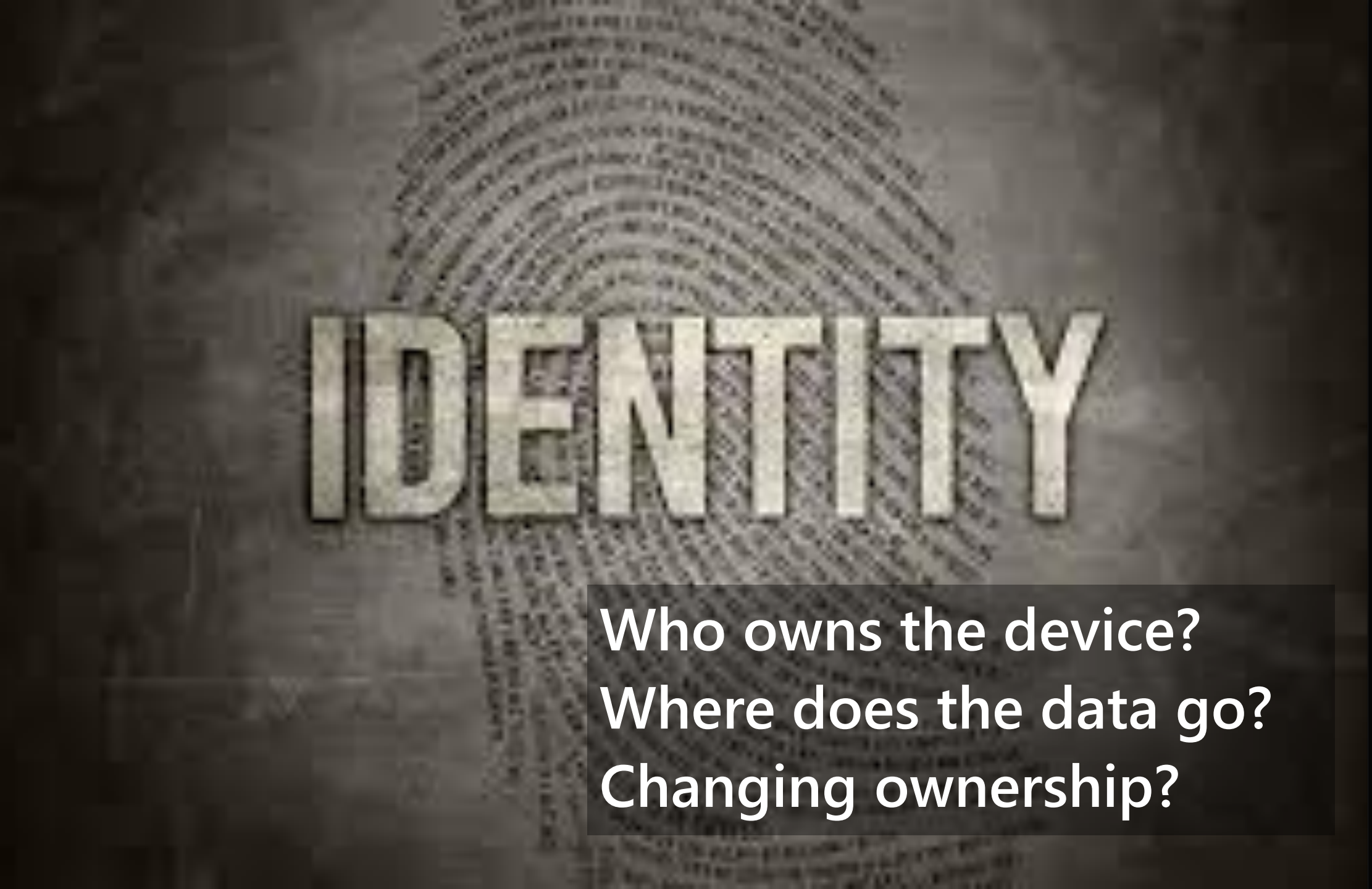
DTLS handshake over 6LoWPAN:
max ~ **30-60 bytes** per fragment

ECDSA P-256: **91 bytes**
ECDSA P-384: **120 bytes**
ECDSA P-521: **156 bytes**

Raw Public Key: Certificate sizes

SESSION HANDSHAKING

IDENTITY PROVISIONING



Who owns the device?
Where does the data go?
Changing ownership?

STORAGE OF SECRETS

Spoofing
Hijacking
Data Theft

Public/private keys
Session IDs
Cached data

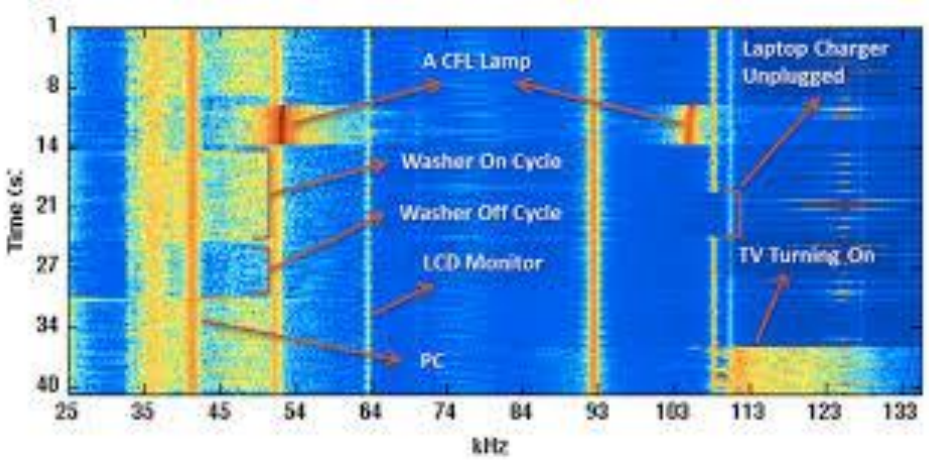
DATA PROVENANCE AND DESTINATION

Where does the data come from?

Where is it going?

OTHER CHALLENGES

nquiringminds



MINIMISATION OF DISCLOSURE

WHO
WHAT
WHEN

Local and
Remote

AUTHORISATION

Device ID
Owner ID
Trusted Party ID
Permission

REVOCATION

nquiringminds

Root certificate impacts

COMMERCIAL ECOSYSTEM

nquiringminds

COMMERCIAL ECOSYSTEM 2

Device cost
vs
Service Value

DEVICE UPDATES

Device update as attack vector

Vs

Unable to fix in the field

ROUTER/BRIDGE PROBLEM

Physically insecure

Terminates two secure connections

DATA SHARING IS THE HALLMARK OF IOT

SHARING

IOT SECURITY CHALLENGES

Who has access to what ? What level of sharing and identity?

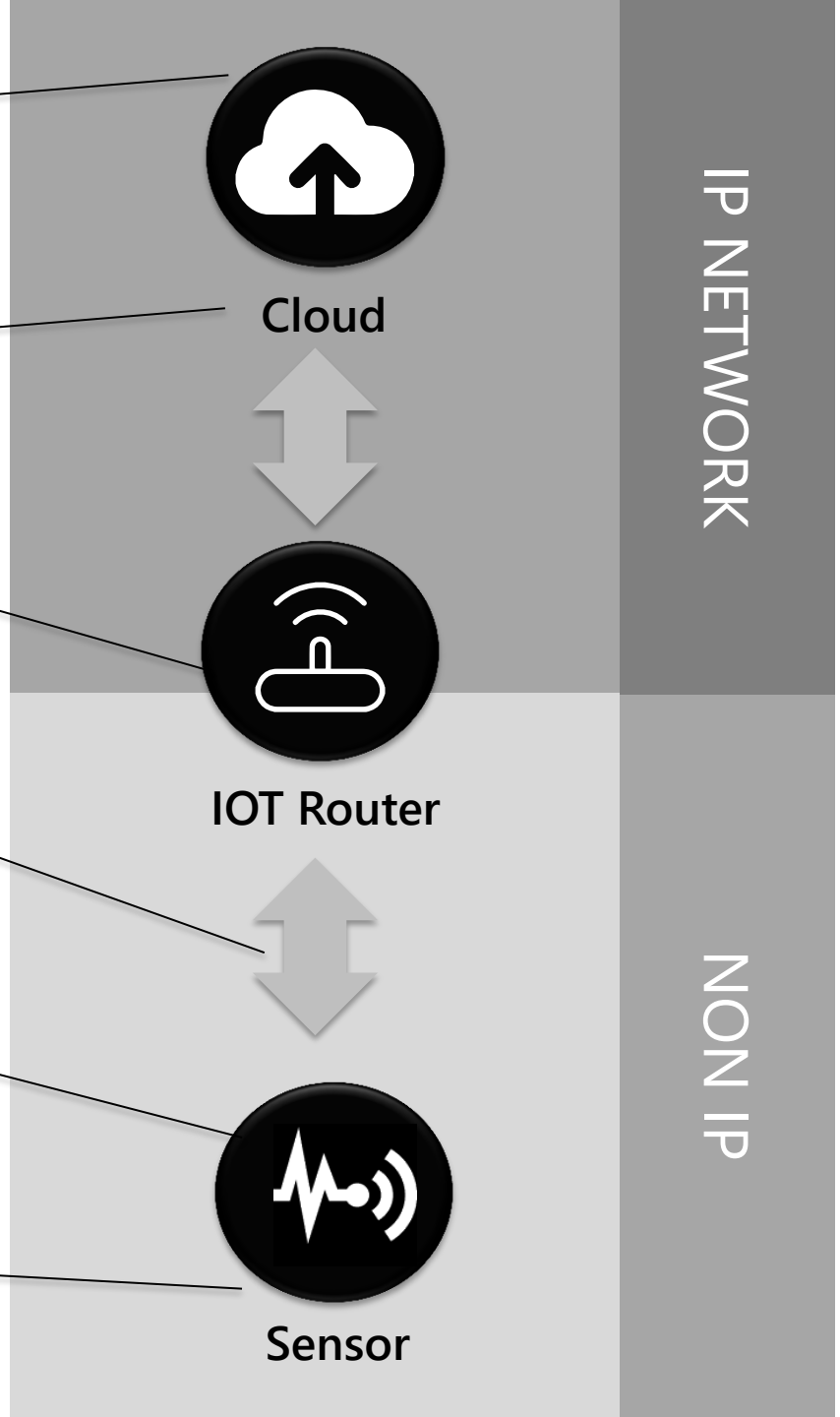
How to flexibly manage IOT devices locally and remotely.

Physically insecure bridging function. Attractive attack target?

Various! Non IP network – what protocol?

Secure storage of secrets – software attack protection?

Low compute power node. Strong enough encryption?

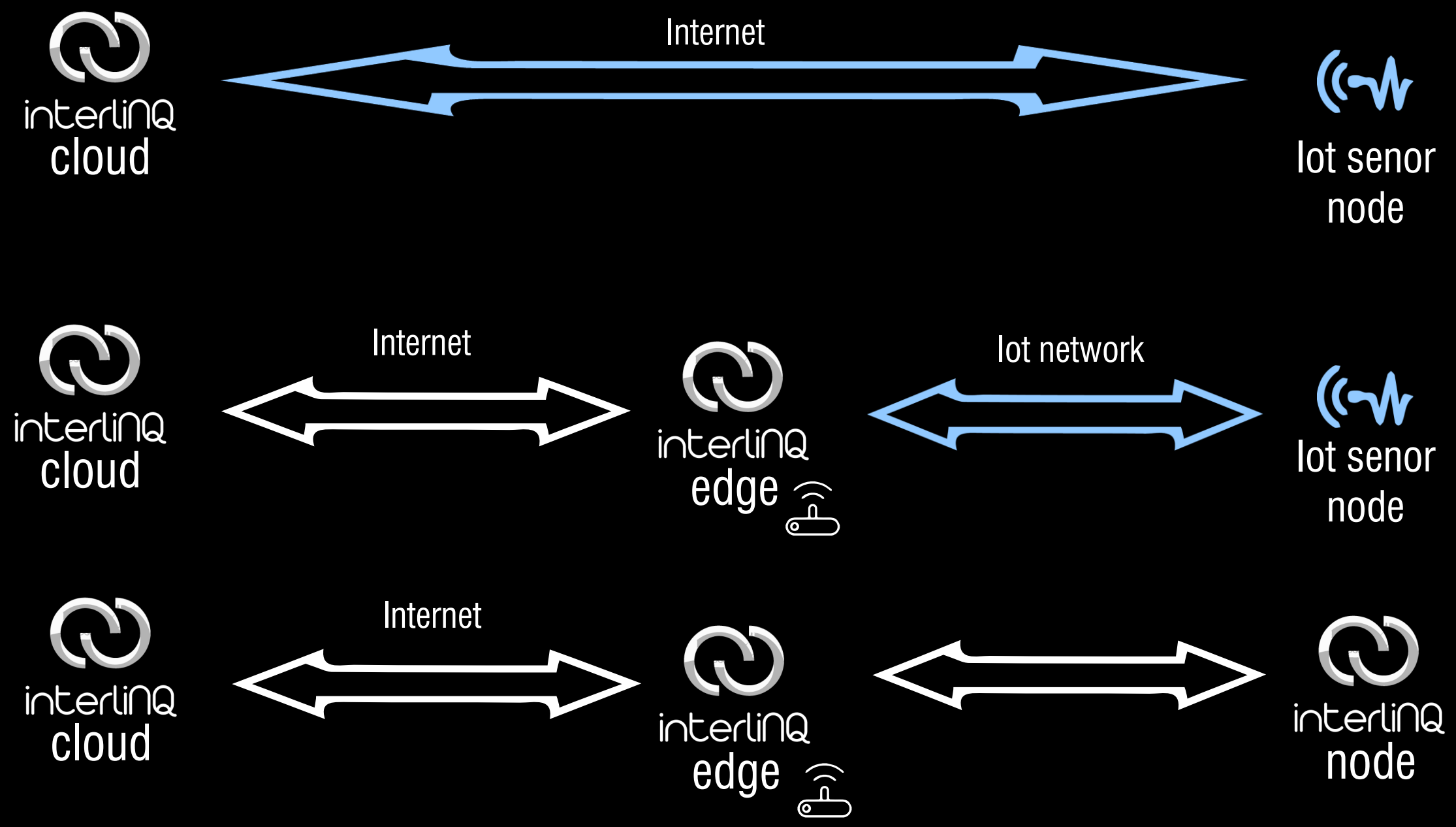


IP cloud network could be over fixed or mobile. Note mobile can have different connectivity constraints. Domestic WIFI can be tricky.

Most real IOT networks do not support IP. 802.15.4, LoRa, SigFox etc.

nquiringminds

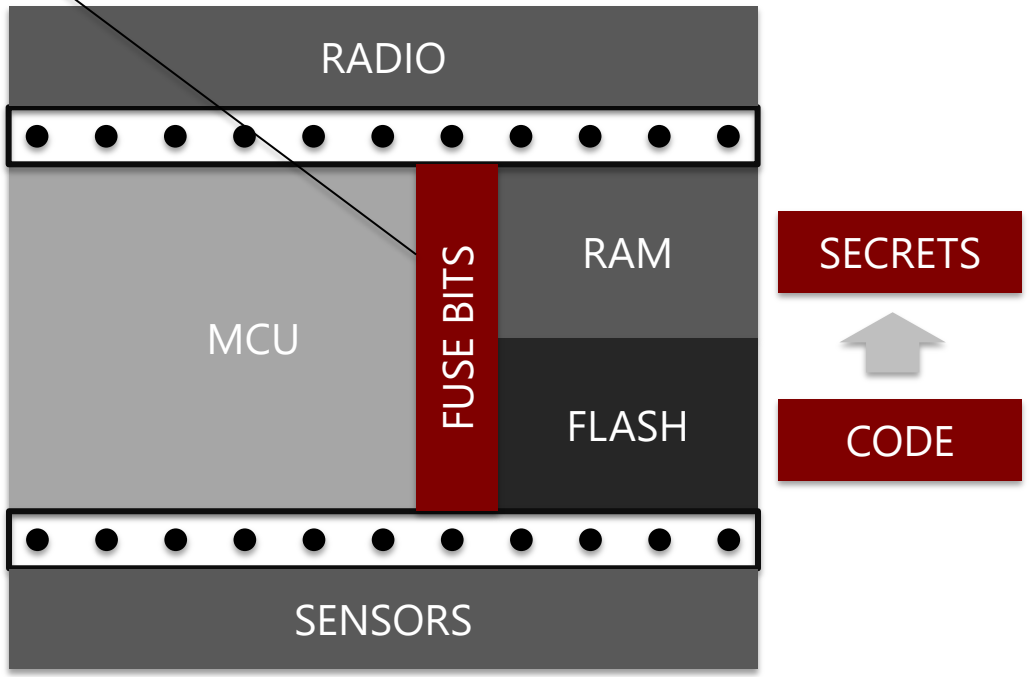
SOLUTIONS

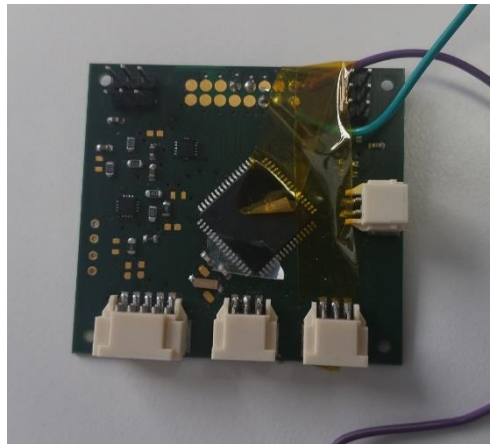

interlinQ
cloud
Internet
Iot senor
node
interlinQ
cloud
Internet
interlinQ
edge
Iot network
Iot senor
node
interlinQ
cloud
Internet
interlinQ
edge
interlinQ
node

STORAGE OF SECRETS

Fuse bits mean any attempt to change code on device will delete secrets. Secrets cannot be discovered by software based attack

Custom "test" board created to implement key features

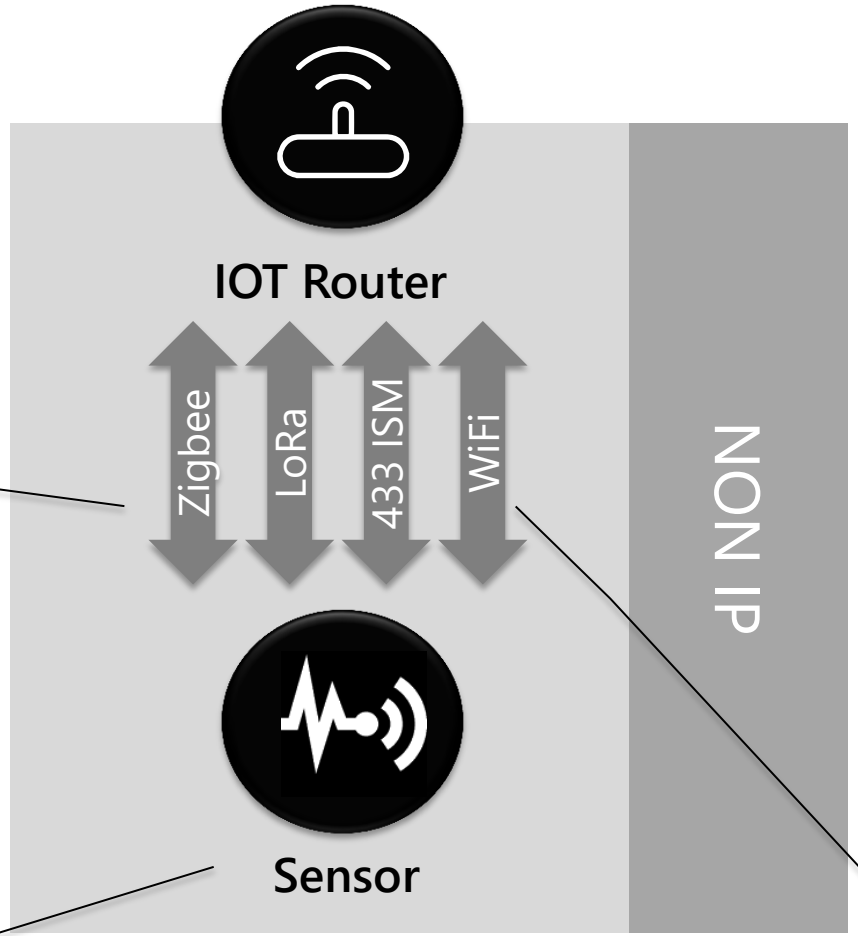




Based on ATxmega384C3 Chip supporting fuse bits

nquiringminds

EFFICIENT SECURE STACK OVER NON IP



Driver layer which maps to multiple different physical networks – none of which support IP – works concurrently

Code base based on MBED DTLS stack stripped down to bare essentials

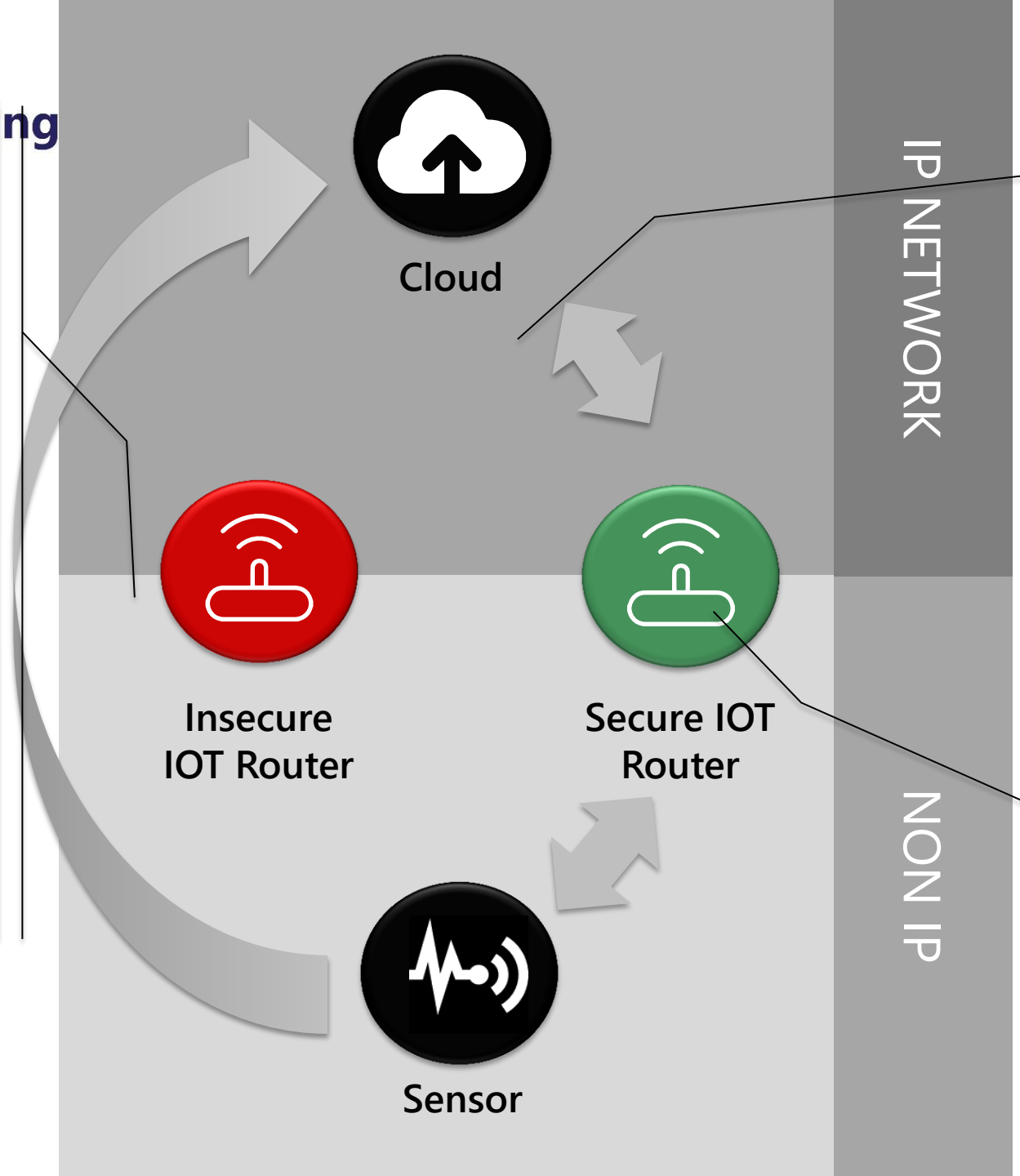
FLASH	RAM
86,590	20,887

Configurable session renew

END TO END OVER HETEROGENEOUS MULTIHOP NETWORKS

New protocols and routing schemas which can negotiate and maintain a secure session over "heterogeneous" networks, consisting of multi hop IP and NonIP legs.

Means physically insecure IOT Hubs store no secrets on device



Either you can trust the router or you cant. A router is physically insecure and possess a lot of secrets – data, keys, session identifiers

Secure IOT Hubs can do "edge" processing . Only secure Hubs can do this. Secure hubs can be build with similar hardware technology to the secure sensor node

SECURE MANAGEMENT OF IOT DEVICES

PKI model means access can be made in "disconnected" state over P2P connections

Internet

Local Wifi

Peer 2 Peer

Flexible Management

Distributed identity model means "different" organisations can share data subject to tokens being granted

IP NETWORK

NON IP

Cloud

IOT Router

Sensor

Model extends to cloud – where separate clouds

IOT "Friendly" IDENTITY and AUTHORISATION model. Based "CLAIMS" signed by PKI infrastructure

COMMANDS can be sent to either HUB or NODE. This allows secure management of a distributed network of devices

ROOT OF TRUST

Trusting what?
Firmware updates
Applications
Identity servers
End users
Signing certificates
Hierarchies thereof

P2P distributed
In factory provisioning
Resurrected duckling

Trusted Data Exchange

Data analytics, sharing and visualisation

- 10 Import any data type
- Inter organisational sharing
- Data visualisation
- AI powered analytics

InterliNQ

Cyber resilient internet of things

interliNQ

- 10 Integrate any sensor
- Any IOT radio
- IOT optimised crypto
- True end to end security
- Edge analytics


BY DEFAULT ORGANISATIONS DON’T SHARE
POWER OF COMBINING DATA

ONE SENSOR – MANY APPLICATIONS

PRIVACY SECURITY CENTRIC

CUSTOMERS

Cambridgeshire County Council

Hampshire County Council

SBRI Future Cities Data Integration

Southampton City Council

Liverpool City Council

Future Solent – Creating a Low Carbon Economy

Centre for Implementation Science

GSMA

[dstl]

Roke – Part of the Chemring Group

SEaB – Make your own green energy – www.seabenergy.com

Liveable Cities

Deutsche Telekom

Wessex Academic Health Science Network

CASE STUDIES

http://nqminds.com/case-studies

AWARDS

Innovate UK – Parlimentary Nomination For Innovation

Cisco pioneers

IOT TOP 15

GSMA Mobile World Congress – Barcelona 22-25 Feb 2016 – Top 10 B2B movers and shakers

Entrepreneurs Unite – CyberSavvy 2016

Cabinet Office – Open Data Champion

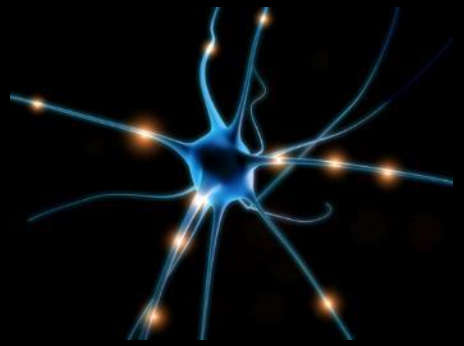
IoT UK Boost – South England – Most Developed Proposition

Best of British – UK Trade & Investment

"NquiringMinds is doing really exciting work through the internet of things to transform urban environments. Harnessing the power of technology and the internet is vital for the future of British prosperity. And I am delighted I will be able to help Nquiringminds seek new opportunities for its business in one of the world's fastest growing markets."

Theresa May, UK Prime Minister
November 7 2016 India-UK TECH Summit

nquiringminds



nquiringminds

@nqminds

www.nqminds.com