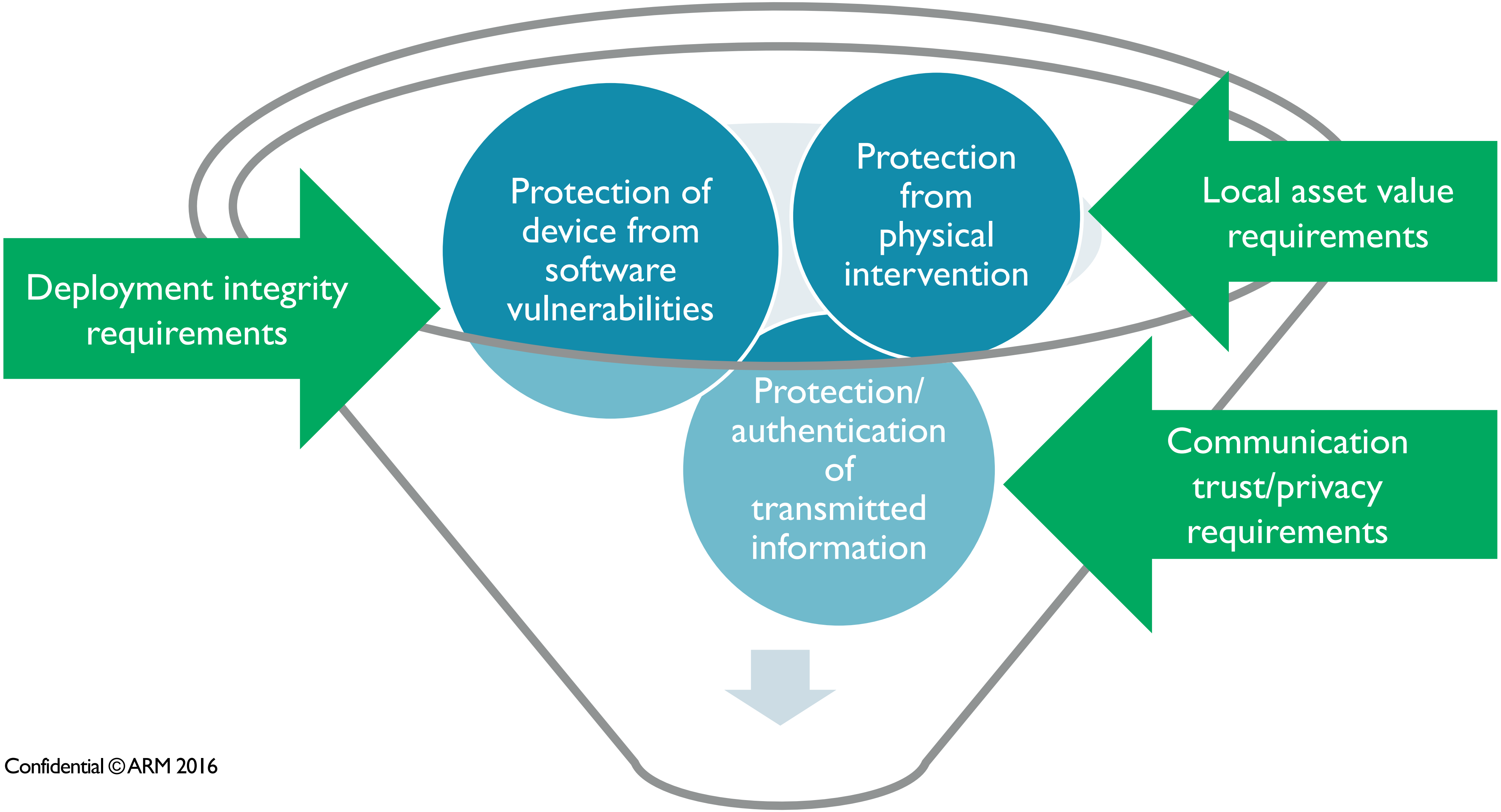
Proportional security to meet the business needs of IoT

Nick Zhou / Senior Field Application Engineer / ARM

mbed Connect Asia / Shenzhen, China
Dec 5, 2016

Invest in IoT security according to business needs



Deployment integrity requirements

Protection of device from software vulnerabilities

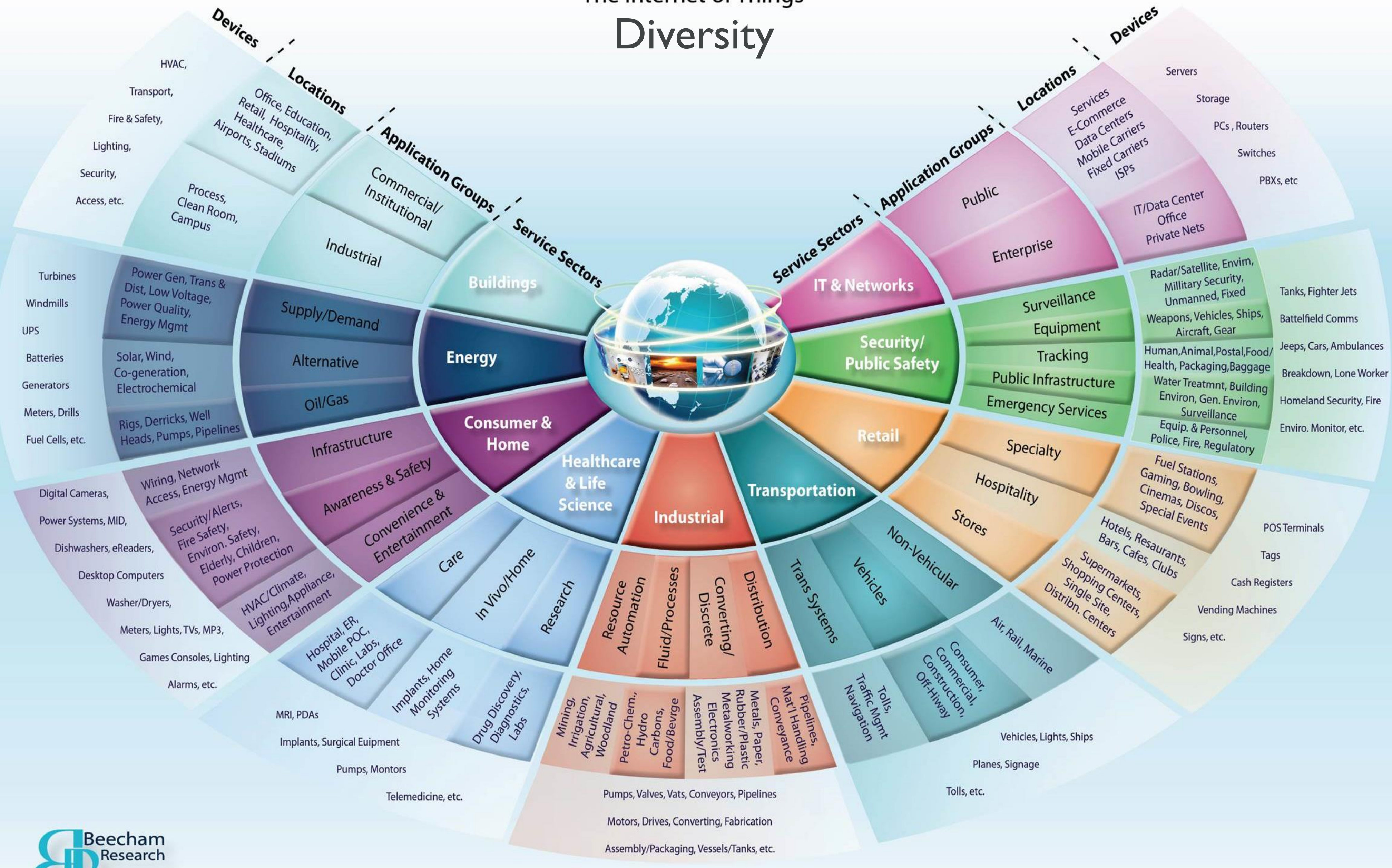
Protection from physical intervention

Local asset value requirements

Protection/ authentication of transmitted information

Communication trust/privacy requirements

The Internet of Things
Diversity



Devices / Locations / Application Groups / Service Sectors

Service Sectors / Application Groups / Locations / Devices

Buildings
- Commercial/ Institutional — Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
- Industrial — Process, Clean Room, Campus
- HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.

Energy
- Supply/Demand — Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
- Alternative — Solar, Wind, Co-generation, Electrochemical
- Oil/Gas — Rigs, Derricks, Well Heads, Pumps, Pipelines
- Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.

Consumer & Home
- Infrastructure — Wiring, Network Access, Energy Mgmt
- Awareness & Safety — Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
- Convenience & Entertainment — HVAC/Climate, Lighting,Appliance, Entertainment
- Digital Cameras, Power Systems, MID, Dishwashers, eReaders, Desktop Computers, Washer/Dryers, Meters, Lights, TVs, MP3, Games Consoles, Lighting, Alarms, etc.

Healthcare & Life Science
- Care — Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
- In Vivo/Home — Implants, Home Monitoring Systems
- Research — Drug Discovery, Diagnostics, Labs
- MRI, PDAs, Implants, Surgical Euipment, Pumps, Montors, Telemedicine, etc.

Industrial
- Resource Automation — Mining, Irrigation, Agricultural, Woodland
- Fluid/Processes — Petro-Chem., Hydro Carbons, Food/Bevrge
- Converting/ Discrete — Metals, Paper, Rubber/Plastic, Metalworking, Electronics, Assembly/Test
- Distribution — Pipelines, Mar'l Handling, Conveyance
- Pumps, Valves, Vats, Conveyors, Pipelines, Motors, Drives, Converting, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.

Transportation
- Trans Systems — Tolls, Traffic Mgmt, Navigation
- Vehicles — Consumer, Commercial, Construction, Off-Hiway
- Non-Vehicular — Air, Rail, Marine
- Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.

Retail
- Specialty — Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
- Hospitality — Hotels, Resaurants, Bars, Cafes, Clubs
- Stores — Supermarkets, Shopping Centers, Single Site, Distribn. Centers
- POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.

Security/ Public Safety
- Surveillance — Radar/Satellite, Envim, Millitary Security, Unmanned, Fixed
- Equipment — Weapons, Vehicles, Ships, Aircraft, Gear
- Tracking — Human,Animal,Postal,Food/ Health, Packaging,Baggage
- Public Infrastructure — Water Treatmnt, Building Environ, Gen. Environ, Surveillance
- Emergency Services — Equip. & Personnel, Police, Fire, Regulatory
- Tanks, Fighter Jets, Battlefield Comms, Jeeps, Cars, Ambulances, Breakdown, Lone Worker, Homeland Security, Fire, Enviro. Monitor, etc.

IT & Networks
- Public — Services, E-Commerce, Data Centers, Mobile Carriers, Fixed Carriers, ISPs
- Enterprise — IT/Data Center, Office, Private Nets
- Servers, Storage, PCs , Routers, Switches, PBXs, etc

Beecham Research

End node device and deployment conditions

- Connected to a network
- May have a long lifetime
- May be physically inaccessible for manual updates
  - Must be able to be managed remotely
- May be physically accessible to third parties
  - Must protect against physical access
- Deployed in enormous numbers
  - Represents a significant investment to protect/maintain

Learn from internet security best practices

- Internet security evolving for decades
  - Leverage this heritage for IoT end nodes

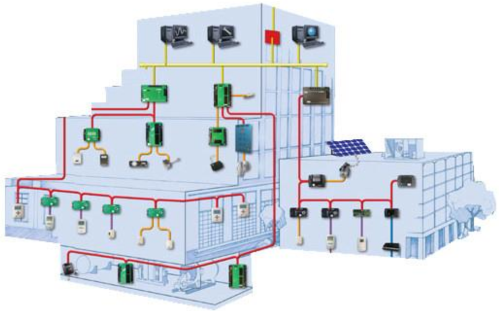
- Low cost, long battery life nodes are capable
  - Think about agility post deployment – security is not a fixed thing

- Security is about the weakest link
  - Look for flaws in protocol and security architecture
  - Avoid deployment mistakes and mismanagement

- Learning applicable to both IP and non-IP IoT communication
  - Find ways to work with existing deployments/technology
  - Drive the future direction of relevant standards

IoT use cases

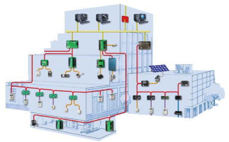
Bluetooth headset linked to cloud service via Smartphone App



Building Automation System OEM covers many client buildings using a diverse set of device types with live connectivity to a cloud service

A few security technology choices

- Protection/authentication of transmitted information

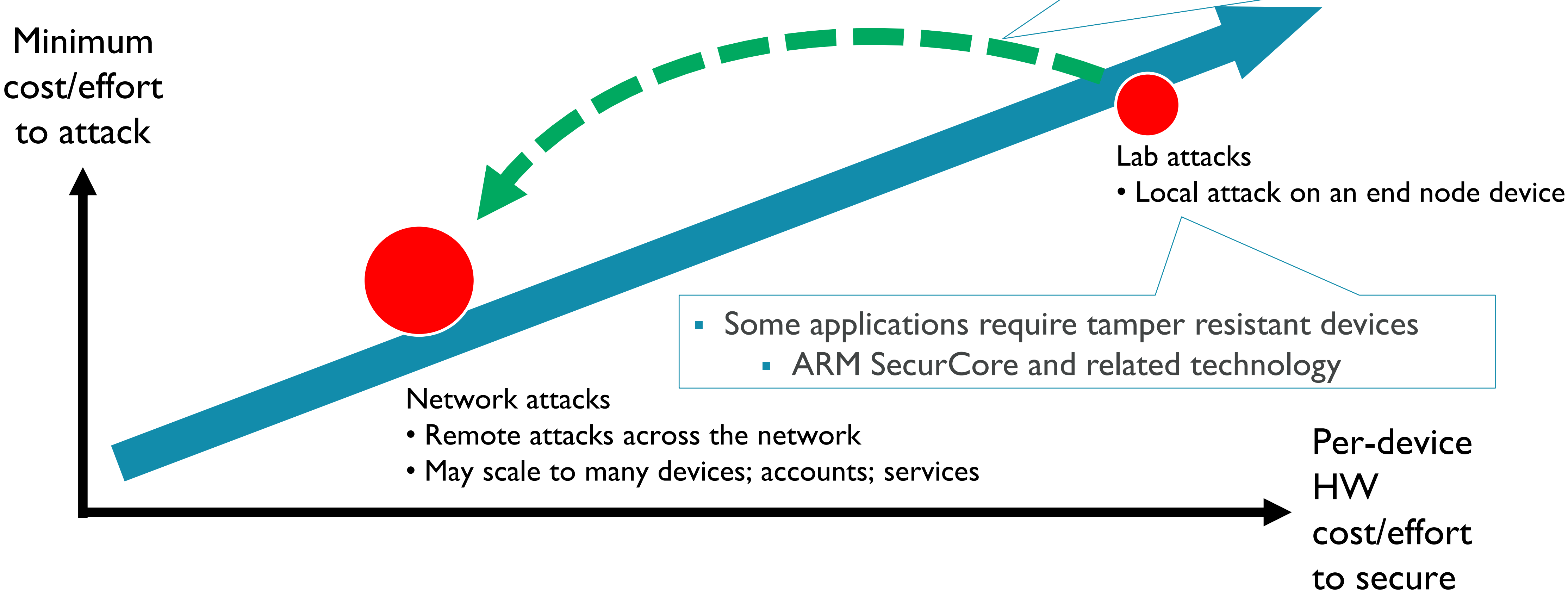


  - Use standard BLE relationship between Smartphone and headset to pair devices and setup link security
  - Treat network as untrusted and use DTLS to establish secure connections based on certified device identities

- Protection of device from software vulnerabilities
  - Device is not directly addressable on the internet
  - Direct attack unlikely if paired device runs trusted SW
  - Strong security to establish/authenticate DTLS sessions (ECC) limits device access
  - Additional device partitioning can vastly reduce local SW attack surface

- Protection from (local) physical intervention
  - Limited local threats
  - Limited device asset value
  - Device identity and (device unique) service keys must be protected
  - Need security in supply chain to prevent installation of cloned devices

Security profiles



Minimum cost/effort to attack
Per-device HW cost/effort to secure

- Where possible devices should not store valuable secrets
  - Local attacks must not enable network attacks on other devices

Lab attacks

- Local attack on an end node device

- Some applications require tamper resistant devices
  - ARM SecurCore and related technology

Network attacks

- Remote attacks across the network
- May scale to many devices; accounts; services

Proportional security

- Threat-models should be informed by business requirements

- Technology applied and cost expended varies according to application needs

- For example
  - Risk environment of application
  - Value of assets to be protected
  - Trust and control over firmware
  - Supply chain structure
  - Lifetime of the device

Application	Security
Short life node	mbed TLS + Connect
Long life node	+ uVisor + Provision + Update
High value asset protection	+ Anti-tamper hardware (ARM SecurCore)

	Ultra-constrained	Constrained	Mainstream IOT	Unconstrained
	BBC micro:bit BT Smart beacon	Rich BT Smart Thread node	Low BW WiFi node Border router	High BW WiFi node Gateway

Device HW resources

Architecture	ARMv6-M ARMv8-M Baseline	ARMv8-M Mainline or ARMv7-M with MPU		A-Class
Acceleration		TRNG + Crypto	TRNG + Crypto	TRNG + Crypto + GPU + VPU

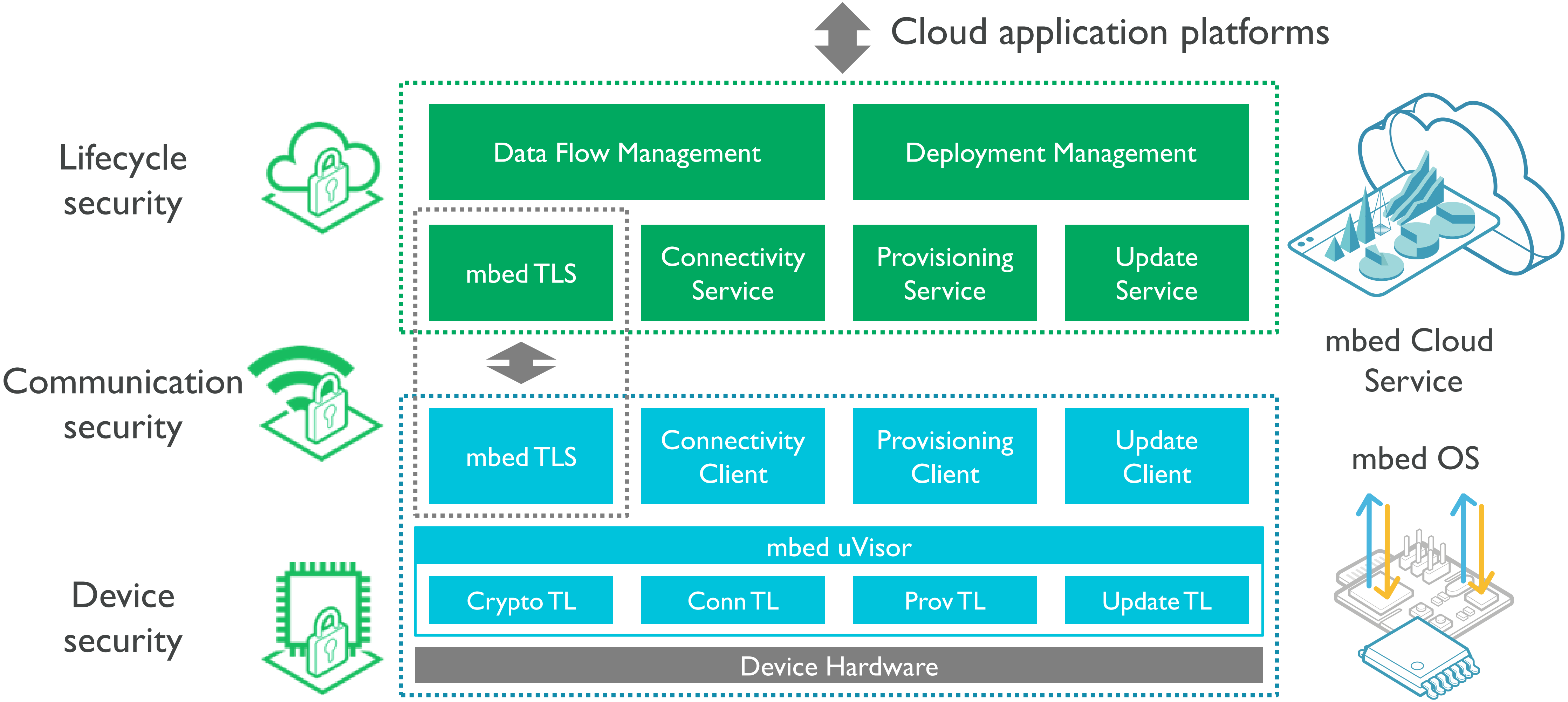
Device SW capabilities

BT Smart	IP + TLS uVisor Lifecycle Security	IP + TLS uVisor Lifecycle Security Firmware over-the-air	IP + TLS OP-TEE Lifecycle Security Firmware over-the-air Rich UI/Multimedia

mbed OS ⟷ (Ultra-constrained to Mainstream IOT)

A-Class + mbed ⟷ (Unconstrained)

mbed security architecture



ARM

Call to action: Better security value proposition

- Avoid selling via FUD
  - Generally unquantifiable: What is value of security investment? What is the ROI?

- Enable reasoning: What security is for, the value it brings
  - Understand threats to business and what key assets are?
  - Measure complete deployment lifecycle value not just BOM cost

- Do not treat Security Technology as a "One Size Fits All"
  - Deploy technology according to business needs
  - Proportional security response according to defined threats/value
  - Factor in agility to cope with evolving security context

- Deliver scalable security choices for IoT driven by clear need/value

ARM