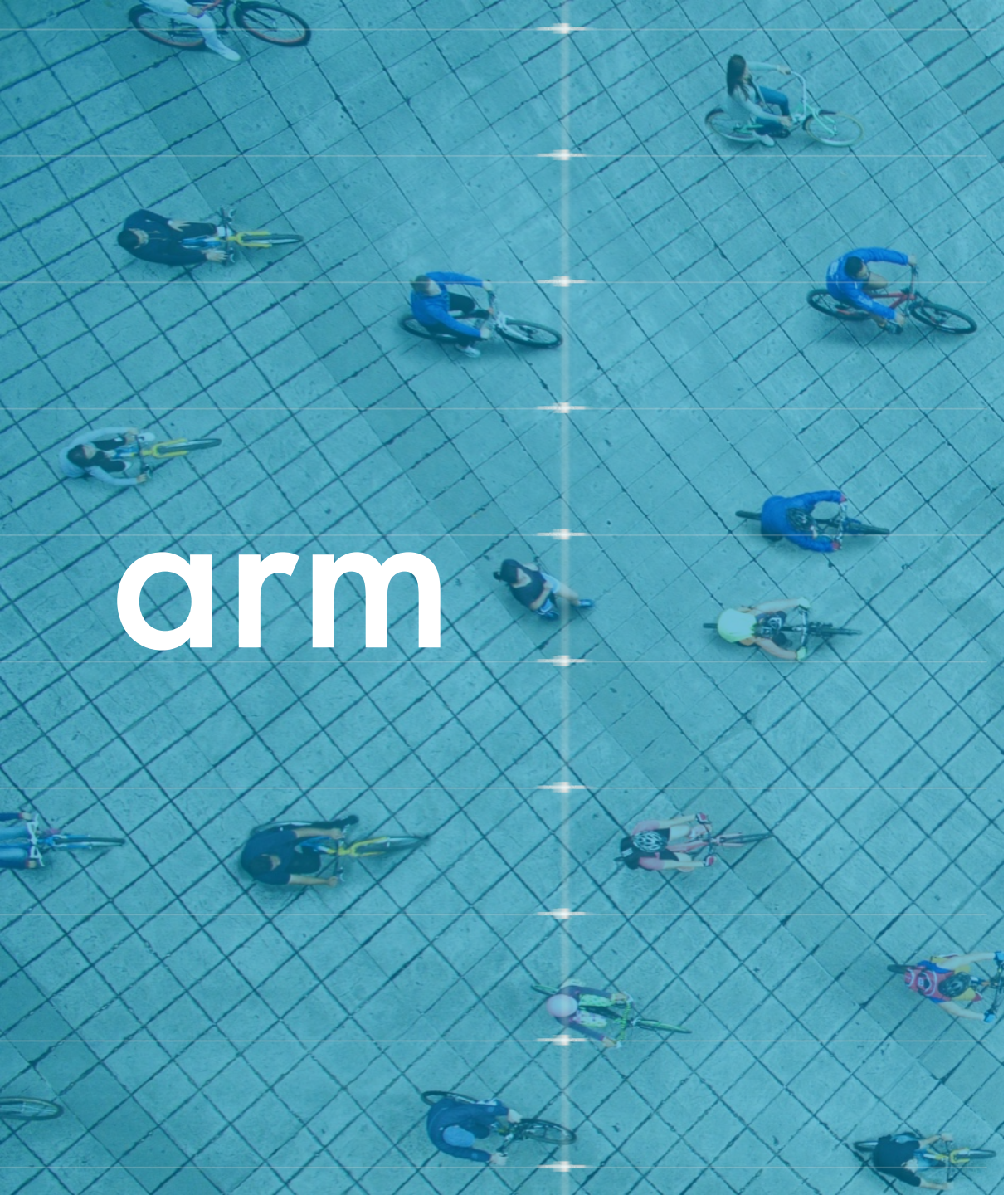


Securing IoT Devices – Closing the gaps

Hugo Vincent

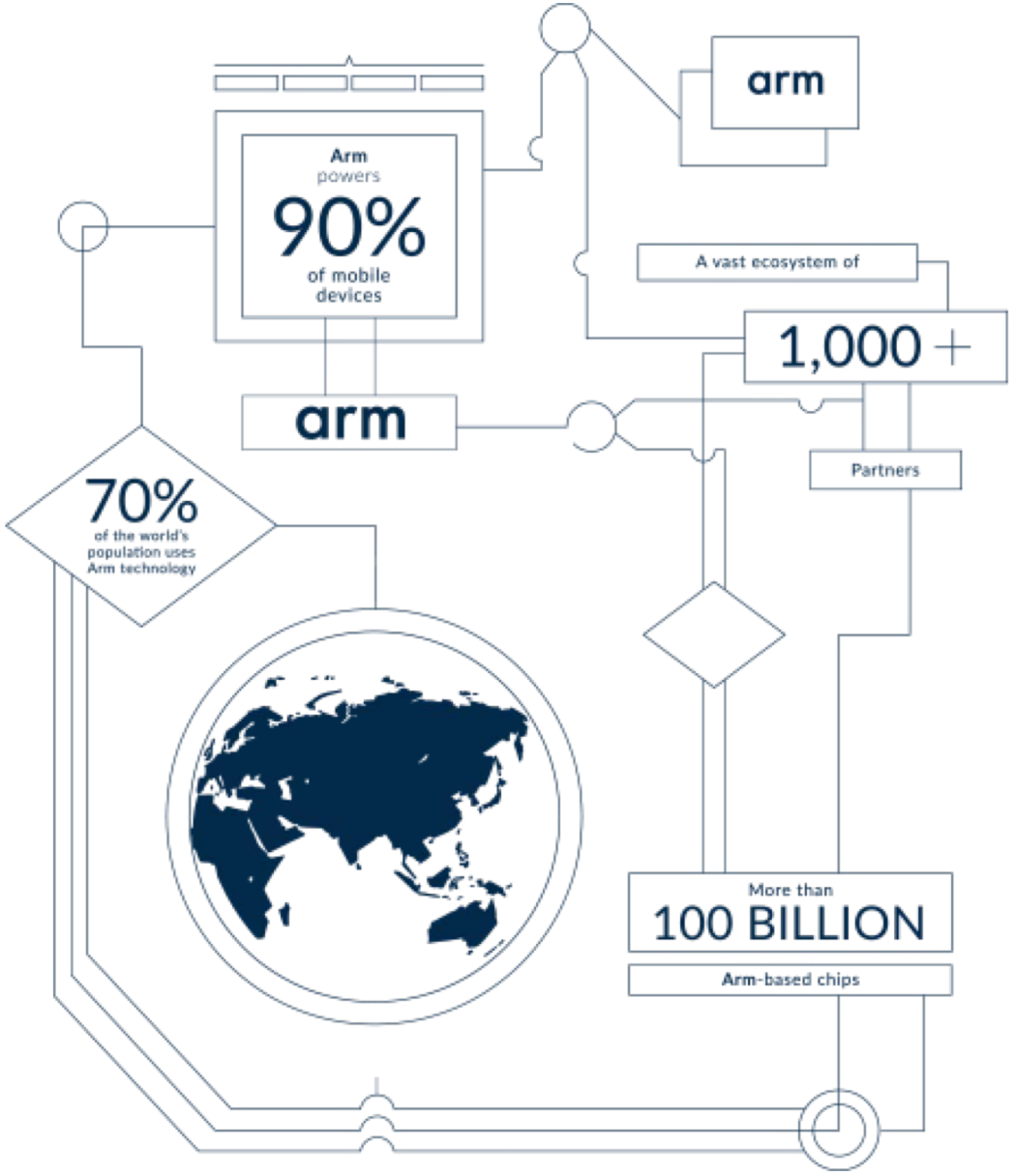
Security Group, Arm Research

RIPE 76, Marseille

17 May 2018

About Arm

- Processor IP company, founded in 1990
- HQ in Cambridge, UK
- Wholly owned subsidiary of SoftBank
- Originally, designed and licensed CPU cores, around which our partners build chips
- Now also do GPUs, ML accelerators, interconnect, subsystems, tools, software…
- … and IoT web services and a platform for IoT devices



arm

About me

- Background in embedded systems, microcontrollers, operating systems, security / trust
- ~7 years at Arm
- Helped set up Arm's IoT research group in 2011, then with our first steps into the IoT business
- Currently leading the security research group & working on computer architectural support for security

arm

Security for devices

Security Principles

Security is a system design problem, not a “feature”

100% security doesn’t exist; need to think in terms of risks and mitigations

As a system designer, you need to defend against any conceivable attack, whereas an attacker only needs to find one

Security measures are often highly un-intuitive

Attackers are unimaginably crafty

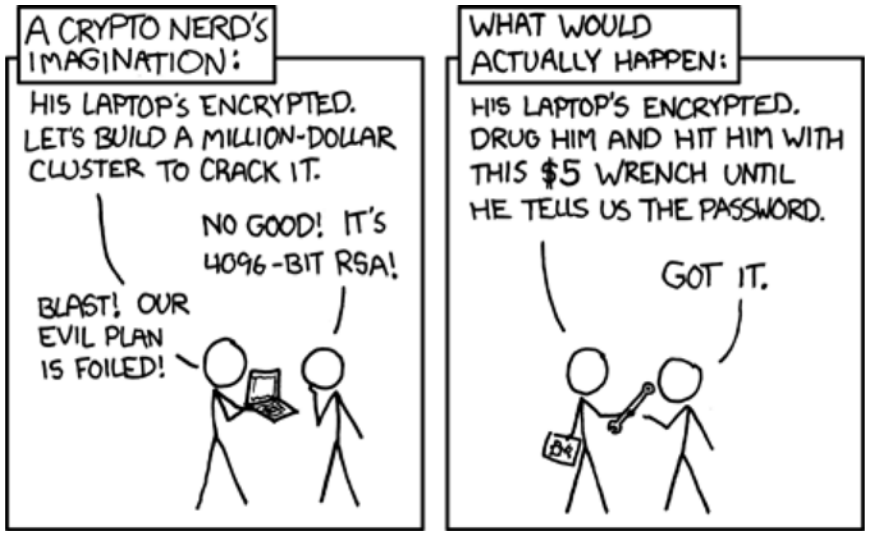
Security is (mostly) not about the maths of crypto

The arms race

IoT devices often low power, low bandwidth, low cost, long deployment lifetime

Components from a complex global supply chain, incorporated into a distributed system

Picture: Wikipedia

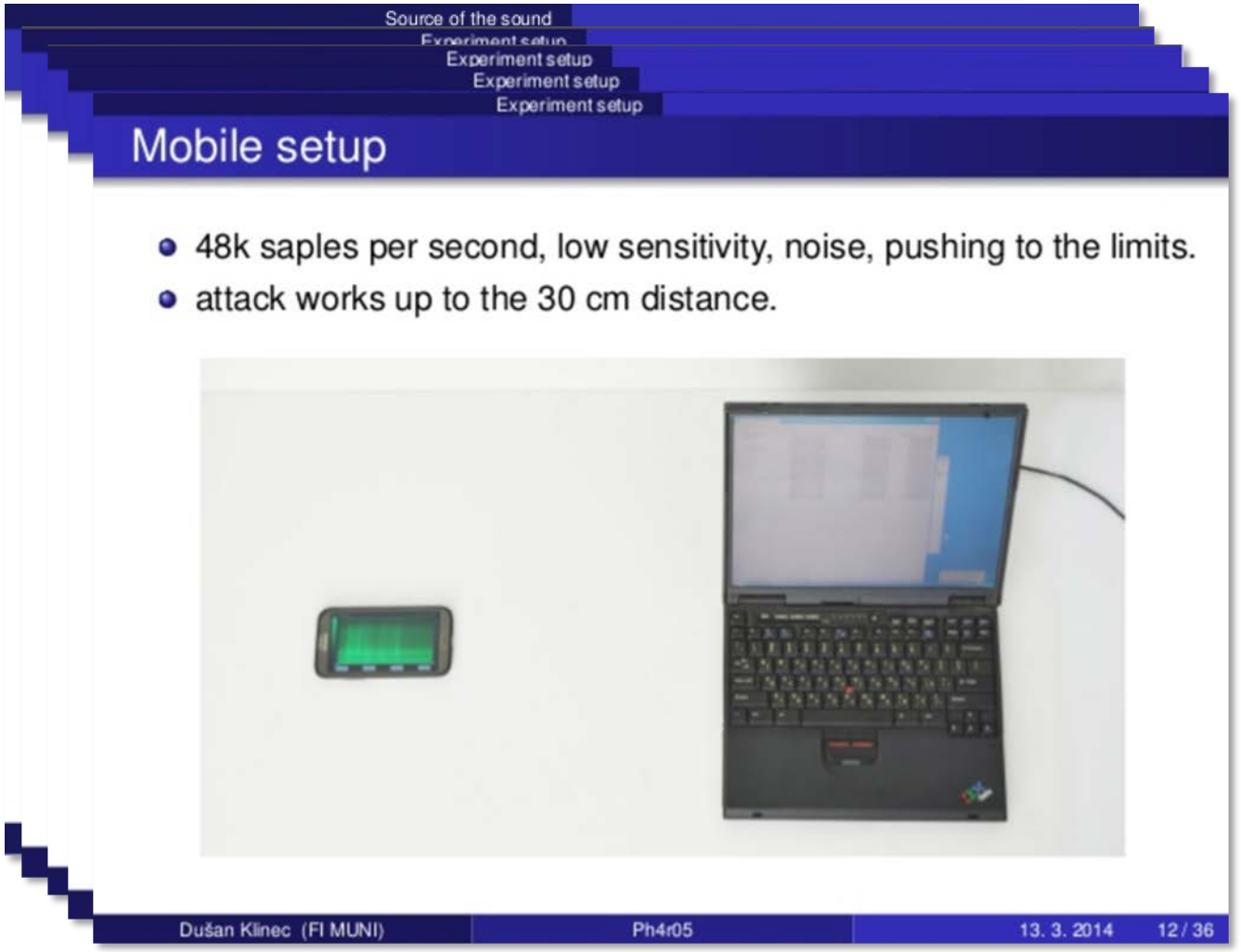


Picture: XKCD

arm

Example: Acoustic Cryptanalysis

Slide credit: Dusan Klinec, Masaryk University



Security Economics

What motivates the attacker?

Many factors, but money is often an excellent proxy

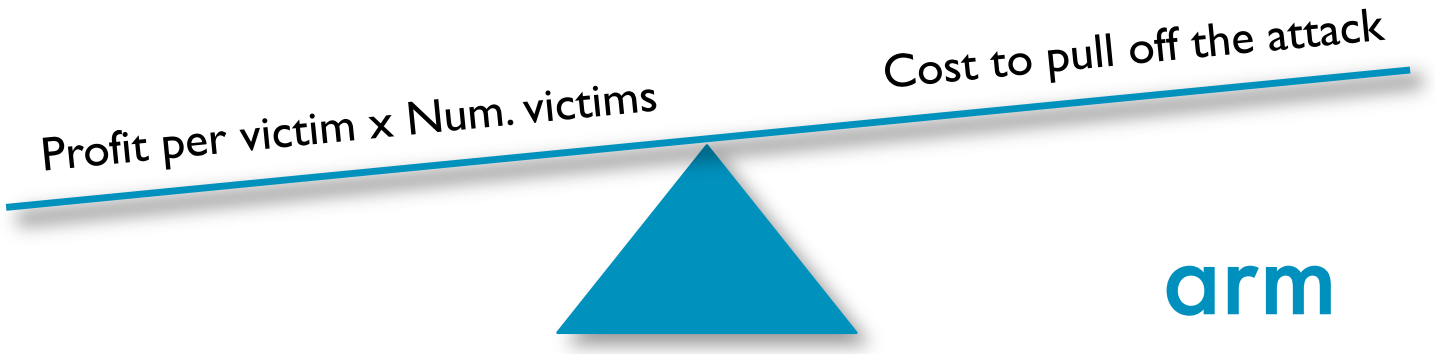
- Attacker wants cheapest possible attack, at the lowest risk of getting caught

Defense is about making it economically infeasible to perform attack

- Or to scale the attack up to multiple victims (one-off break vs class break)

Costs of attack almost always drastically reduce over time

- Tools, automation, knowledge dissemination



arm

Risk & Threat Modelling

Most (all?) security defense has a cost

Need to be rational in what we defend against:

- What attacks do I worry about? What risks am I comfortable with?
- Local or remote access?
- Physical access? Physically invasive access? (shack attack vs lab attack?)
- Motivation: curiosity / ego vs personal gain vs commercial gain vs nation-state
- Deployed lifetime vs undiscovered attack classes?

Not just the system itself:

- How will the data be used? Is the data sensitive / private? Could it become sensitive in the future?
- Are their perceived sensitivities? Could the data be used as a proxy for sensitive data?
- What is the strategy for aggregating and/or pseudonymizing the data? Differential privacy?

Security features, as with all other aspects of the system, may themselves create risks

Isn’t Patching the answer?

Patching has been surprisingly successful as the primary means of dealing with security vulnerabilities in PC/server/mobile, and probably the single most important security capability

IoT things are often different:

- No UI, no means of recovery, so updates have to be fail-safe and bulletproof
- Much less commonality, more bespoke work to deploy patches, more testing, more risk
- Resource constraints limit extent of patchability, and over time may lead to unpleasant choices between functionality improvements or security fixes
  - Of note: on battery powered sensors, a FOTA patch can consume a large chunk of the lifetime energy budget
- OS and linkage model often require full firmware image to be updated, not just component/package affected
- Remote forced update mechanism could itself be a powerful attack vector without strong mutual identity and authentication capability

Recent example

THE VERGE TECH SCIENCE CULTURE MORE

SCIENCE TECH CYBERSECURITY

Almost half a million pacemakers need a firmware update to avoid getting hacked

You may need to take grandma for an update

by Natt Garun | @nattgarun | Aug 30, 2017, 7:27pm EDT

FDA U.S. FOOD & DRUG ADMINISTRATION

Search FDA

back to Safety Communications

Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's)

As with any firmware update, there is a very low risk of an update malfunction. Based on St. Jude Medical's previous firmware update experience, installing the updated firmware could potentially result in the following malfunctions (including the rate of occurrence previously observed):

- reloading of previous firmware version due to incomplete update (0.161 percent),
- loss of currently programmed device settings (0.023 percent),
- loss of diagnostic data (none reported), or
- complete loss of device functionality (0.003 percent). (Exp. ~14 patients in the US)

Medical Specialties

Cardiac Electrophysiology, Cardiology, Cardiothoracic Surgery, Heart Failure

Devices

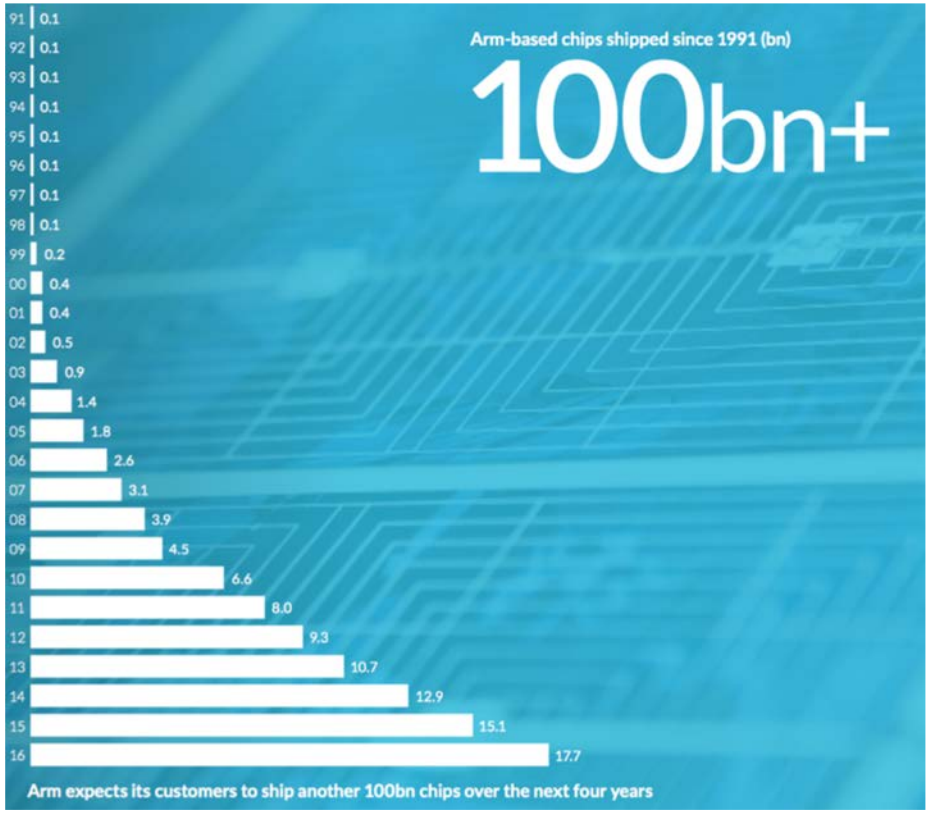
arm

arm

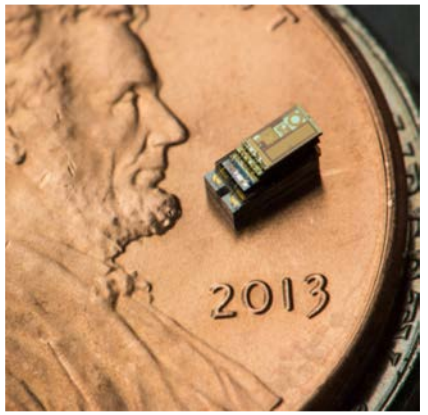
Arm in the IoT

Arm IPG

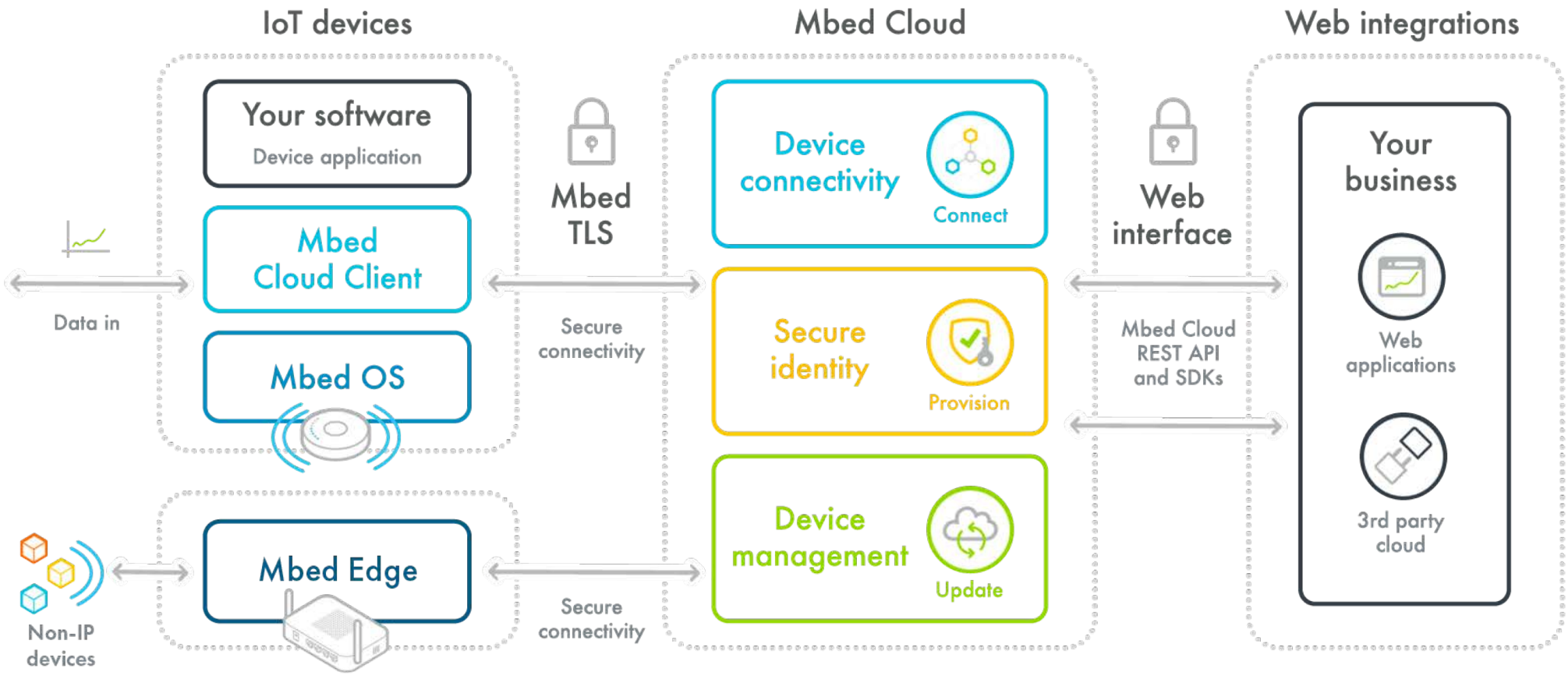
- The Arm Architecture (ISA) – contract between HW & SW
- Arm and architecture partners build cores implementing the architecture
- Partners build chips containing cores



- A-profile: origins in mobile, pushing into automotive, server and HPC
- M-profile: microcontrollers, deeply embedded / low power / low cost, ubiquitous



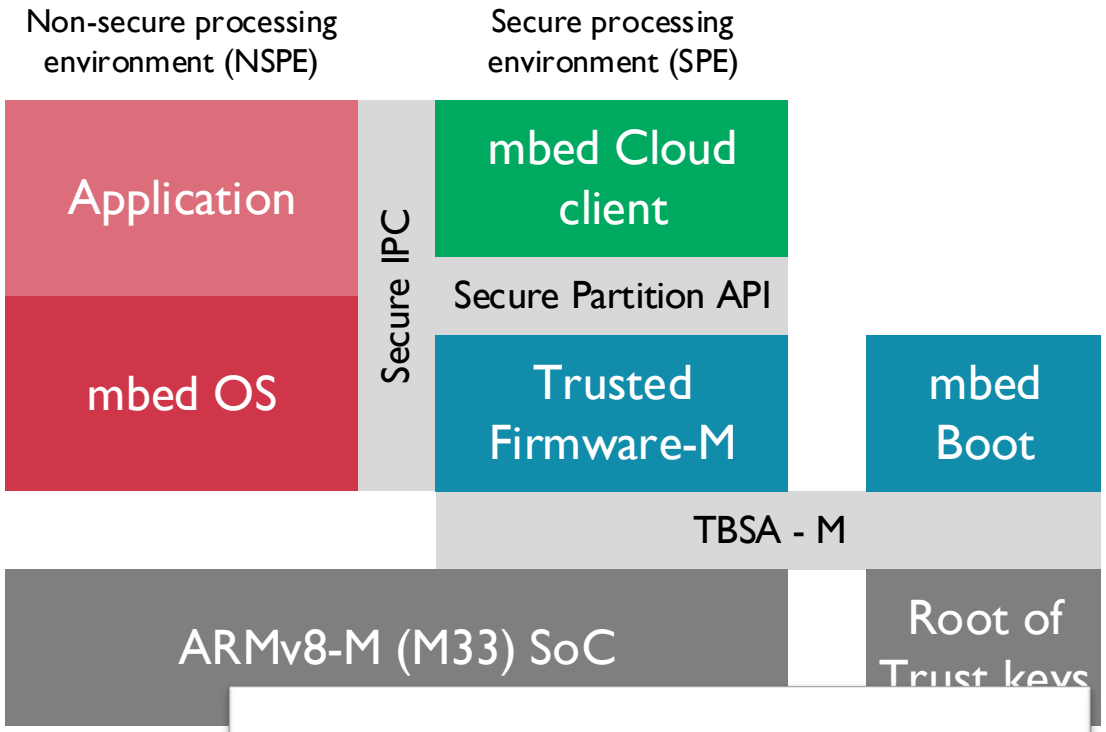
Arm ISG



arm

Our IoT strategy

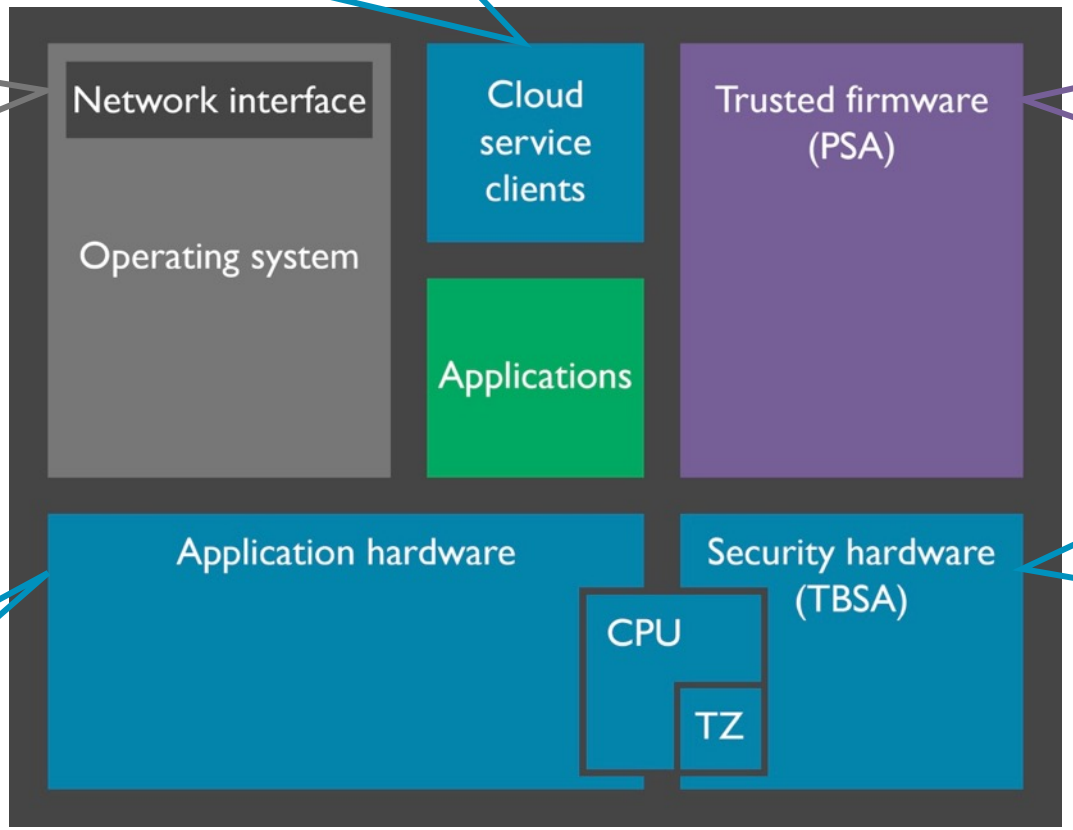
- Unique synergy between IPG and ISG – especially around security
- Put features into hardware and base architecture to enable secure IoT device management at scale (roots of trust, TRNG, isolation mechanisms etc)
  - Platform security architecture (PSA) – common base platform to enable scale
- Offer web services that can rely on these hardware features to offer differentiated security and device management
  - Secure, efficient connectivity to the cloud (native IP, or via a middlebox)
  - Strong device identity and provisioning of secrets
  - Management and update



Anatomy of a secure connected device

Applications that securely connect to cloud services to access device
- Secrets stored in security hardware

Main interface to the 'world' and key point of vulnerability
- Uses firmware and hardware to manage keys and secure communications



Interface between security hardware and OS/applications
- Trusted boot
- Code integrity
- Secure storage
- Firmware update

Other functions
- CPU
- Memory
- Communications

Storing secrets and accelerating cryptography
- CPU extensions
- Secure memory
- Random number generation
- Cryptographic accelerators
- Key stores
- Security island

arm

Conclusion

Securing connected IoT devices is still fairly difficult, and as such, still mostly done quite badly

However, there is hope on the horizon!

- Many of the challenges are analogous to known ones, have known solutions, just need productionizing
- Moore's Law in embedded space continues to give us more capability (PKI, isolation mechanisms, etc) – for now
- Trends towards platformization, subsystems, modules, and generally increasing commonality and re-use will improve security, create economies of scale, and reduce development costs
- Increasingly widespread understanding of the problems and solutions from manufacturers, consumers, and governments will improve market pull for security – or regulators will intervene
- Many IoT devices don't (directly) have fallible human users, and are relatively simple – ultimately, will be more secure and reliable than general purpose machines

Arm and our partners are working to enable a vision of a trillion connected devices by 2035, potentially unlocking a productivity improvements across all industries amounting to ~3% global GDP

- More info: https://community.arm.com/iot/b/blog/posts/white-paper-the-route-to-a-trillion-devices