Juhani Mäkelä

Principal Consultant

Securing Internet of Things

HelSec MeetUp 2019-03-21

NIXU and IoT Security

- IoT is a bit of a buzzword. Often it just means adding IP (v4 or v6) connectivity to already existing devices.
- IoT devices exist both in the consumer and industrial space. Nixu's main interest lies in the latter, because
  - Industry has both the motivation and the means to secure their devices. There are many companies manufacturing investment goods in Northern Europe.
  - Consumer devices are dominated by big Asian and American companies, who seldom feel they need our advice.

NIXU's Track Record

- PKI and general Internet security since early 2000's
- Nokia Mobile platform security
- Huawei device authentication and TEE management
- Danfoss Drives platform security

Not to mention multitide of pentests, device security audits and security architecture work on an ongoing basis

News in March 2019

Connectivity

Triton is the world's most murderous malware, and it's spreading

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents. It was discovered in the Middle East, but the hackers behind it are now targeting companies in North America and other parts of the world, too.

ARIEL DAVIS

Aluminum giant Hydro hit by ransomware

March 19, 2019

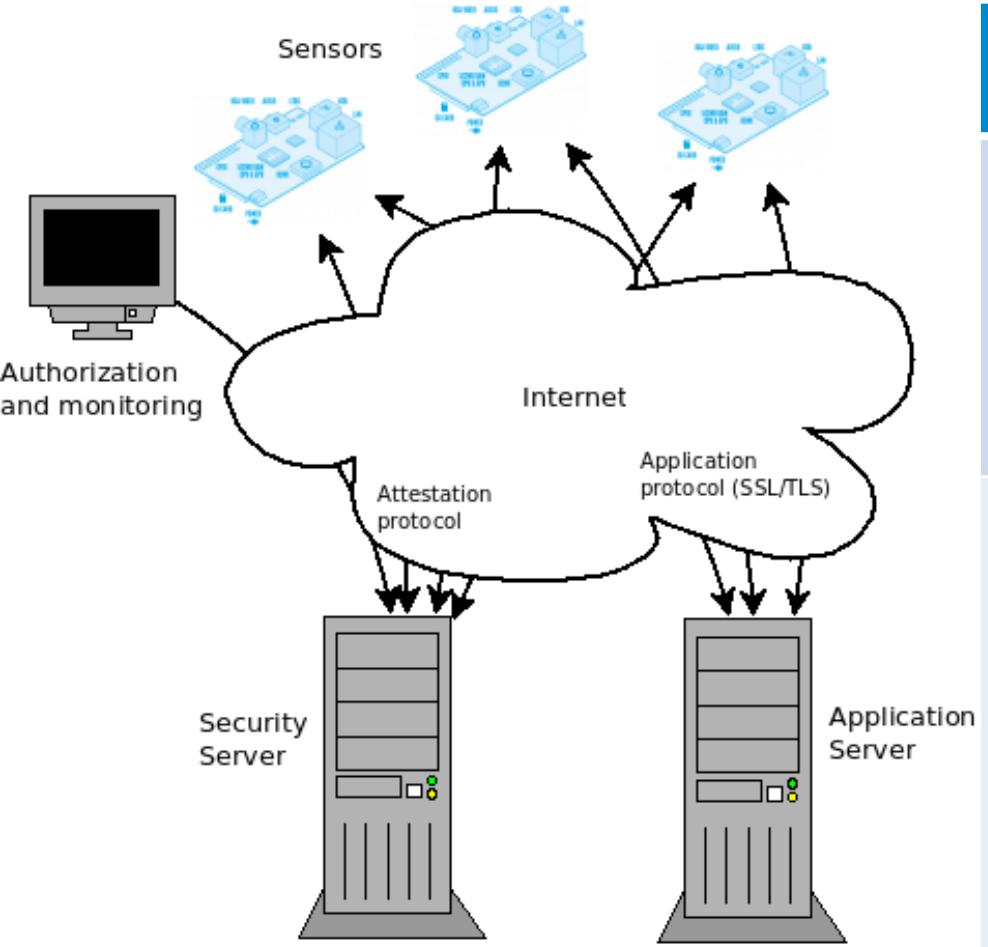
During the last several years we have described multiple incidents with ransomware targeting organizations such as hospitals, municipal transit, or even government computers for an entire county. Then came the age of the wipers, with epidemics of WannaCry, ExPetr, and Bad Rabbit spreading through the world and ruining operations for numerous businesses.

Cyberattacks with the potential to cause loss of lives and damage worth $$$,$$$,$$$

What Makes IoT Devices Special?

- Single-minded appliances, not general purpose computing or communication devices
- Supposed to work mostly autonomously, with little or no local operation or expertise
- Manufactured and deployed in large quantities with the minimum of time and effort
- Computing and storage resources often limited
- Attackers can and will take them apart to analyze and reverse-engineer

Two Lanes of Information Flow



Daily Operation	Fleet Management
The main purpose of the device - Sensors to collect and consolidate measurements - Remotely controlled locks, valves, drives, motors...	Maintenance and support - Security Information and Event Management (SIEM) - OTA updates - Remote diagnostics and control
- Data not necessarily sensitive - High volumes - Low latency - Insecure legacy protocols with no authentication and confidentiality (Modbus, PROFIBUS, CAN, LON...) - Designed for local isolated networks	- Potential to take over the whole fleet in one sweep - Strong authentication and confidentiality is a must - Internet-based from the get-go

Add a Black Box and Be Done With It

NIXU thinks this is a stop-gap solution

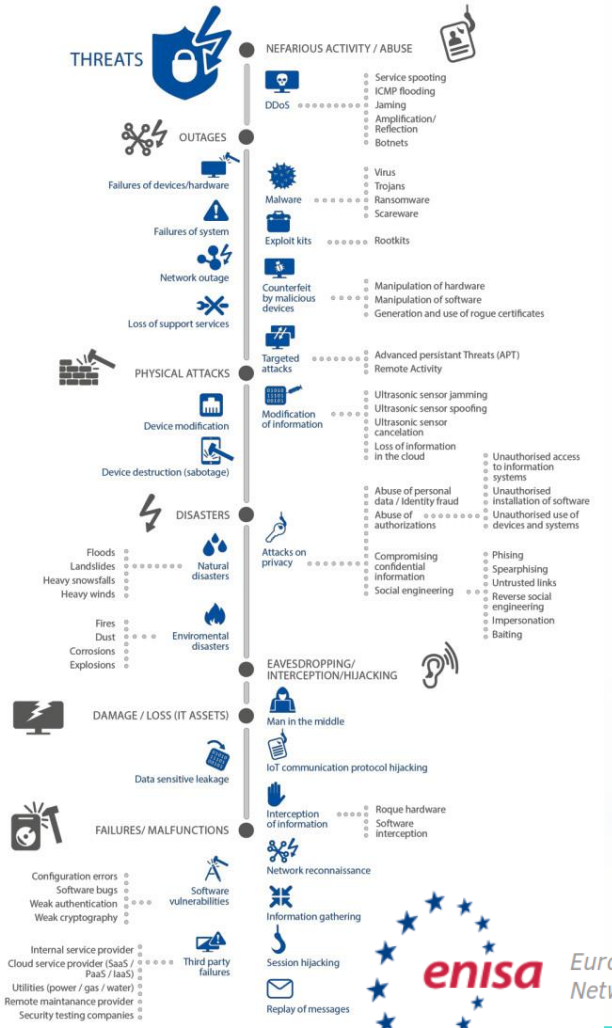
- General Internet security evolved from adding firewalls to defence-in-depth and end-to-end security
- Additional complexity and cost

In practice this is often the quickest and easiest way to go, but our interests lie elsewhere, in applications where it is not good enough or too expensive.

nixucon18

Threats

Enisa – IoT Threat Taxonomy



- Enisa threat taxomony is a mixed bag of bad things: DDoS, Malware, Exploit kits, Counterfeit, Targeted attacks, Modification of information, Attacks on privacy, Man in the middle, Communication protocol hijacking, Interception of information, Network reconnaissance...
- Leading to Loss of Assets, Outages, Failures, Malfunctions, Damage, Disasters...

Basically there are three threats: little, medium and big

enisa *European Union Agency for Network and Information Security*

Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017

Prisoner of War

- Attacker has physical access to a single device and tries to extract secrets by reverse-engineering SW and HW
- Loss: whatever is in the device at the moment and can be deciphered
- Mitigation: HW trust anchor, tamper resistant HW, no shared secrets

Attack of the Clones

- Attacker can create impersonated devices and have them join the fleet
- Impact: loss of confidentiality of downstream material, system stability threatened by bogus input. Loss of revenue by counterfeit products.
- Mitigation: Strong and unique device identity

Loss of Command & Control

- Attacker controls a fleet management server and can can issue malicious commands and/or software updates
- Impact: partial or total loss of the fleet temporarily or permanently
- Mitigation: Proper PKI infra, HW trust anchor, revocation of attacker controlled keys

Excluding the root signing key leak, everything else can be revoked

Protections

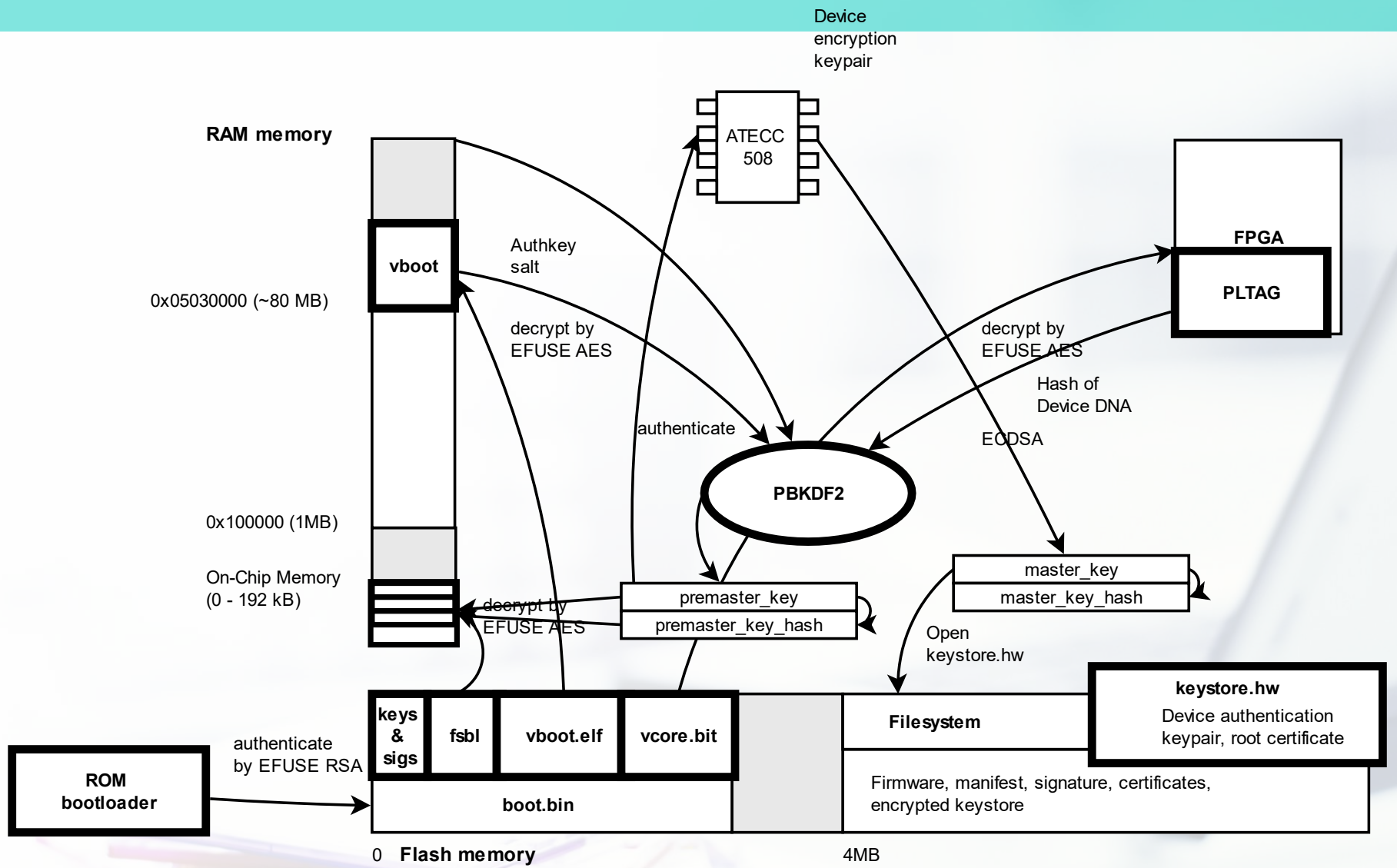
Architectural Principles

- Public key cryptography to minimize the use of shared secrets
- Strong identities everywhere. Not serial numbers, but *certified* serial numbers.
- Mutually authenticated and encrypted communications
- Minimize the risk of *class breaks* by making every device slightly different
- Local and remote attestation

Device Security

- Secure boot by means of software signing and a hardware trust anchor
- Local encryption based on a unique device secret, preferably protected by hardware
- Strong cryptographic identities for devices and users based on asymmetric cryptography (X.509).
- Avoid passwords by all means

Secure Boot by Xilinx And ATECC508



nixucon18

Device Ownership by X.509

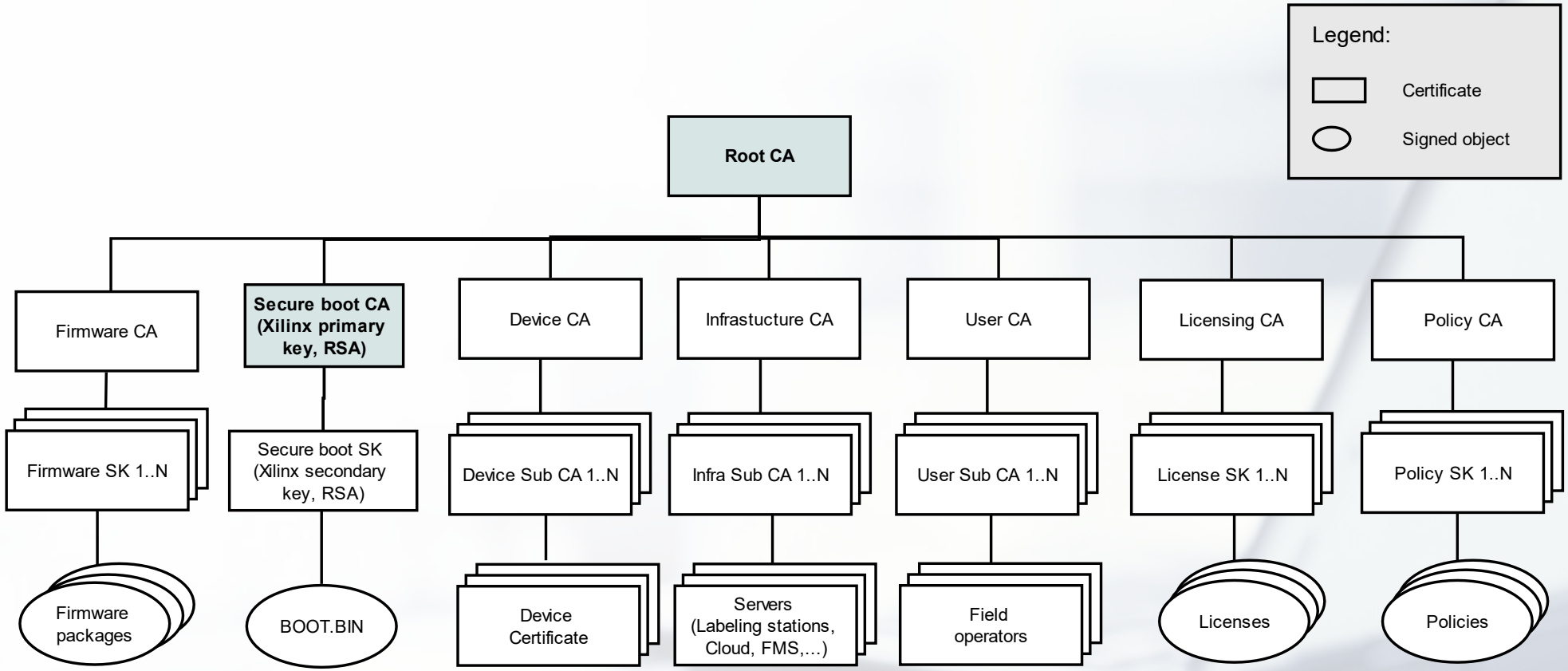
- Device has a strong identity in the form of a signed certificate from factory. Ownership is established in first deployment.
- Owner registers in the cloud service and gets an owner certificate, linking them to the device identified by its own certificate.
- Cloud server issues policy saying this owner certificate owns this device (if not already owned) which is passed to the device.
- Now owner has total control on their own device based on the certificate, policy and possession of related private key.

Requires a safe device to store owner's private key. Privacy not so much of a problem in industrial environment, they have service contracts anyway.

Cloud Security

- Mutually authenticated, encrypted channels
  - TLS and DTLS are battle-hardened,
    Noise Protocol Framework uses modern crypto
- Signing servers for all kinds of purposes
  - Devices, servers
  - Users, authorities
  - Firmware packages, updates, configurations
  - Policies, licenses
- Root private keys are off-line. Automated signing servers use hardware security modules.

Example of a PKI Hierarchy



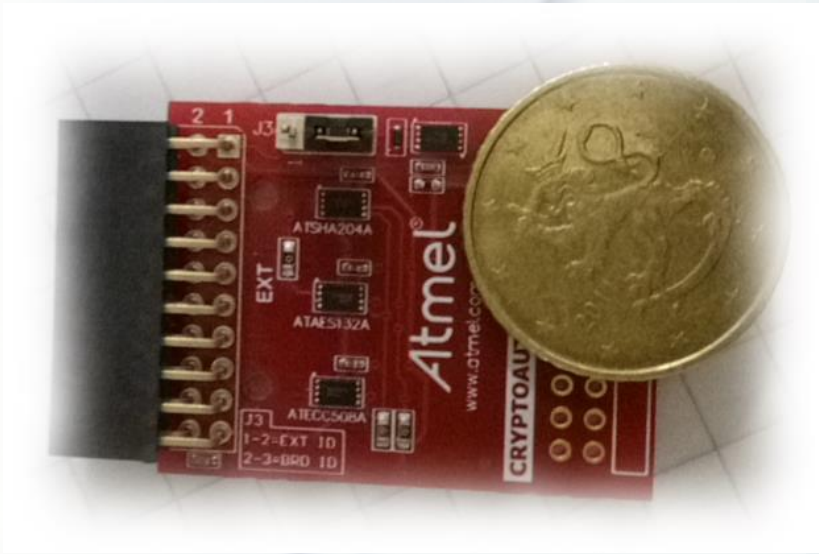
Policy Framework

- Authentication and authorization are two different things
  - Authentication creates persistent identities
  - Authorization says **who** can do **what**, **where, when** and for **how long**.
- Policy statements are signed authorizations using existing identities with an independent duration and scope
- Revocation should not be used as means of access control, only to cancel invalid or stolen identities.
- No established standard for policies yet, everyone does their own. Nixu too.

Hardware

Cryptochips

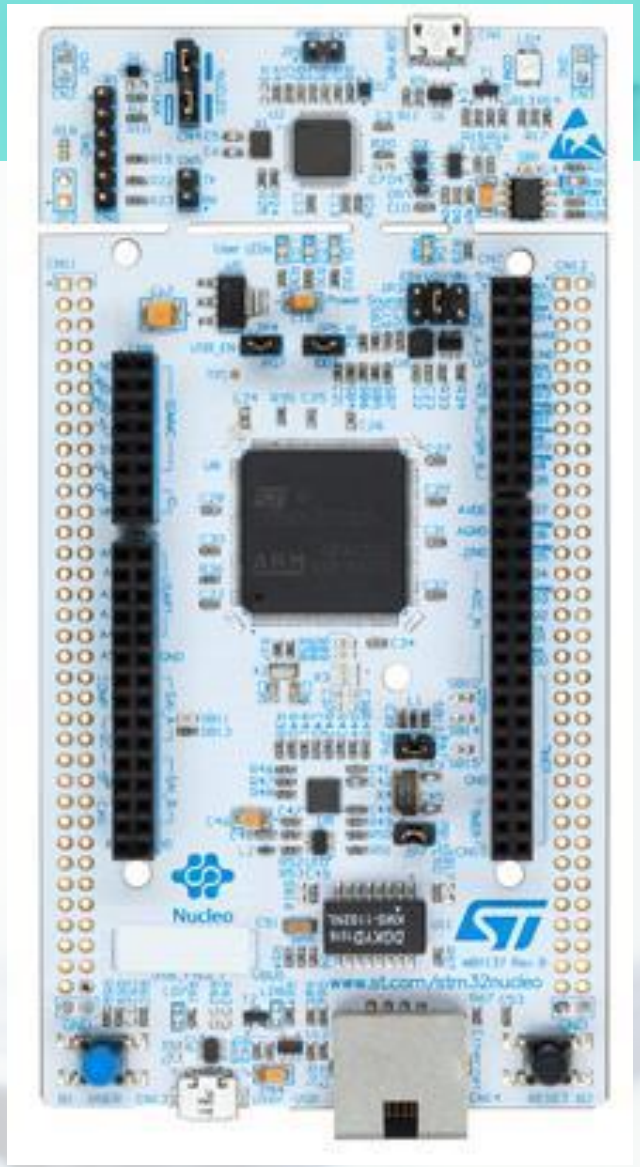
- ATECC508/608
- Cost < 1€
- Asymmetric ECC
- Write-once memory with explicit sealing
- Tamper resistant
- Authenticated and encrypted I^2C communication



nixucon18

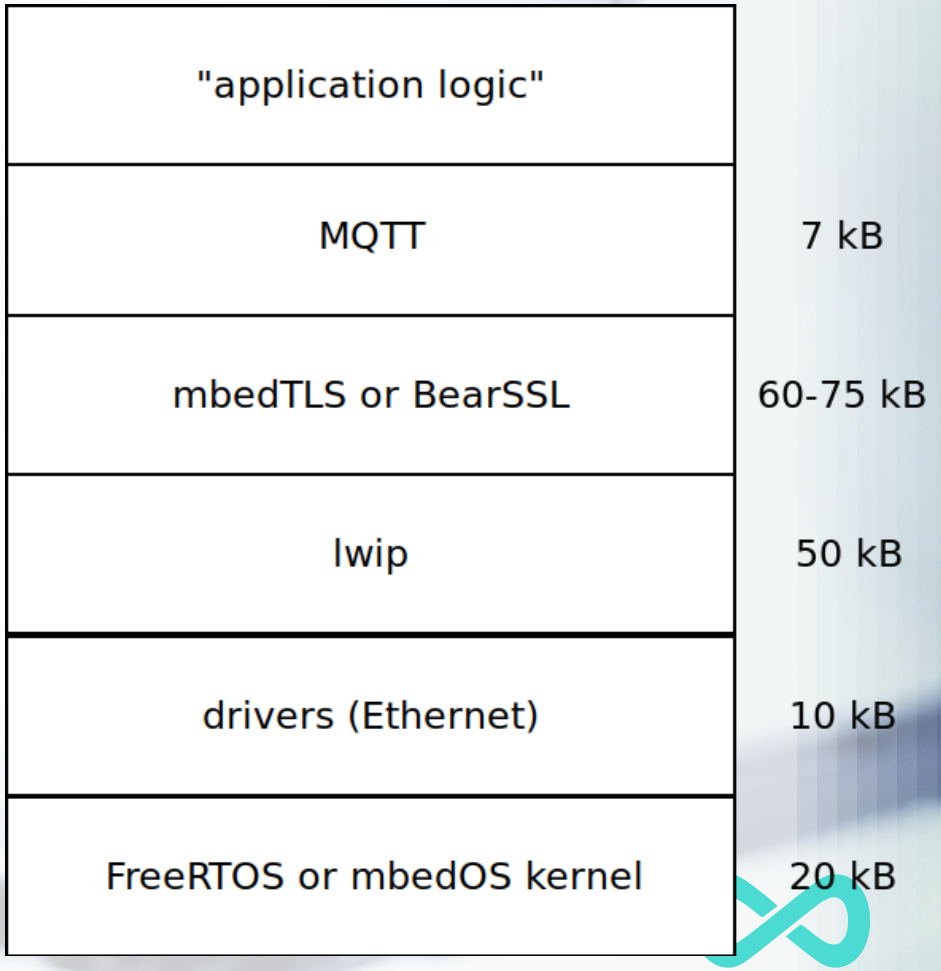
Microcontrollers

- STM32 Nucleo-144
- Cost <10€
- 256 kB SRAM
- 2MB flash memory
- Ethernet, USB, I²C, SPI
- RTOS OS if OS at all



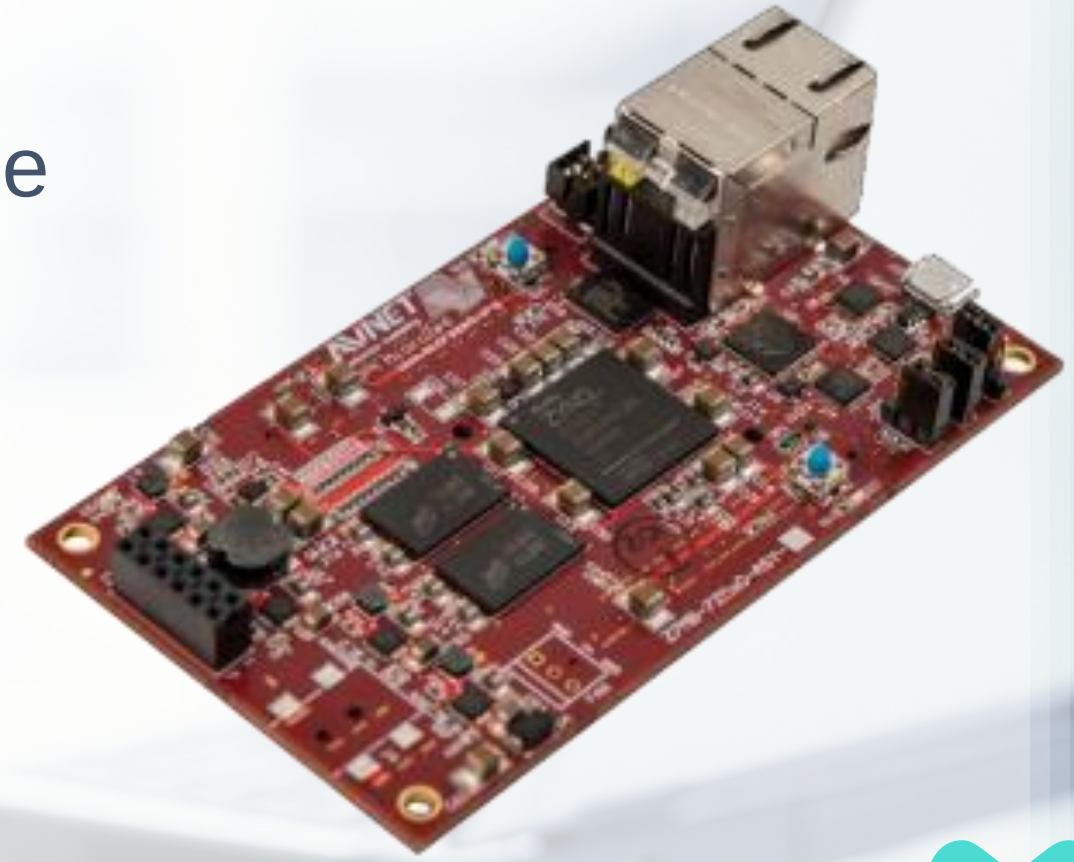
Minimal Security Stack

- How much memory does it take to run asymmetric crypto and TLS?
- We made an experiment last year and managed to squeeze it in 200 kB in a STM32



Raspberry Pi and Smartphones

- Xilinx Zynq SoC
- ARM Cortex with TrustZone
- >512 MB RAM
- >16 MB of Flash
- Secure boot by eFUSES, RSA signing and AES encryption
- FPGA



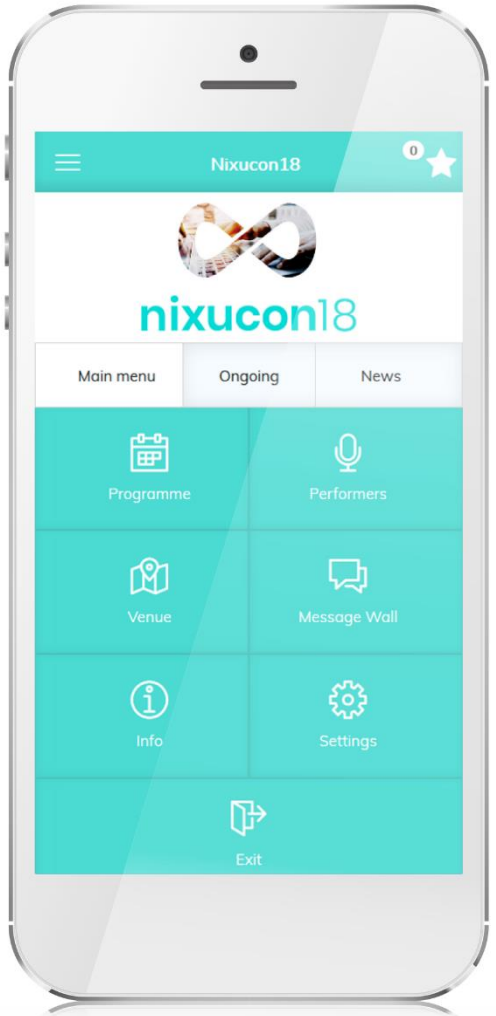
nixucon18

Physically Unclonable Function

- A one-way function based on tiny manufacturing differences in integrated circuits causing undeterministic behavior
- Can be used to derive device-specific secrets or a ’silicon fingerprint’
- Works well with FPGA

Johannes Vainio, *Physically Unclonable Functions as Trust Anchors for Connected Embedded Device Security*, Aalto University 2018

Thank you!



Please, give me Feedback!

Program →
Presentation →
Give feedback

juhani.makela@nixu.com

/in/ juhani-mäkelä-a9702a4

nixucon18