BREAKING INTERNET OF THINGS

Nordic Testing Days 2015

Mait Peekma
Clarified Security OÜ

WHO AM I?

Mait Peekma

10 years @ The Most Important Role in product development

testing (security testing)

CLARIFIED SECURITY

- Practical security testing
- „We break security to bring clarity”
- Small, but big testing team concentrated just on security testing

INTERNET OF THINGS

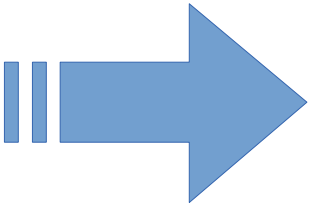
- Embedded Devices - Nodes
  - Sensors, Controllers
- Connected to each other
  - directly or via a Coordinator
- Coordinator connected to Internet

- Building automation, assets tracking, patient monitoring, ...

INTERNET OF THINGS

- Small form factor, cheap
- Low data rate, low power consumption

- Low-Rate
- Wireless
- Personal Area Network



LR-WPAN

BUGS

- Tested the security of ~10 IoT sets
- Independent manufacturers

- Some security weaknesses are present in majority of the IoT sets

REASONS

- Tight time schedule
- Low budget
- Priority: get the IoT working (smoothly)
- Not enough resources to secure the IoT set

ENCRYPTION

- You do not want others to know
  - How much beer is left in your fridge
- Also used to authenticate the owner
  - Open the garage door
  - Turn off the heater (or artificial pacemaker)

ENCRYPTION

- Symmetric encryption
  - e.g. AES-128
- Network Key (NWK)
- Key Transport Key (KTK)
  - Transporting the NWK to all devices

NETWORK KEY

- The same Network Key (NWK) in all networks from the same manufacturer

- Even worse: it is the development NWK
  - Documented in the LR-WPAN specification

KEY TRANSPORT KEY

- With user-friendliness in mind, the same KTK is used in all IoT networks (of a single manufacturer)

- Defence:
  - Out-of-band key transport
  - Lower the transmission power

ENCRYPTION KEY

- Random Number Generator (RNG)
- Works well (according to NSA) on your PC/Mac

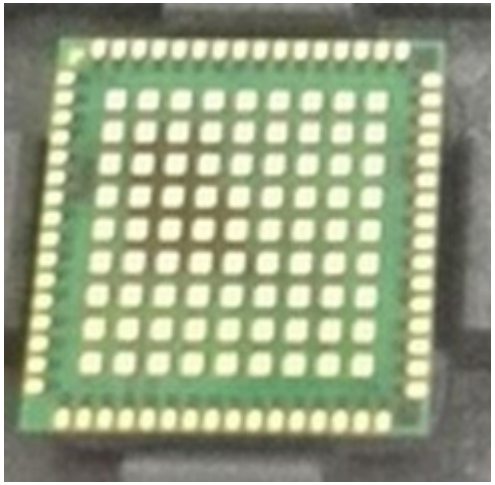
- MCU-s are prone to generate weak randomness
  - unless it is a smart card

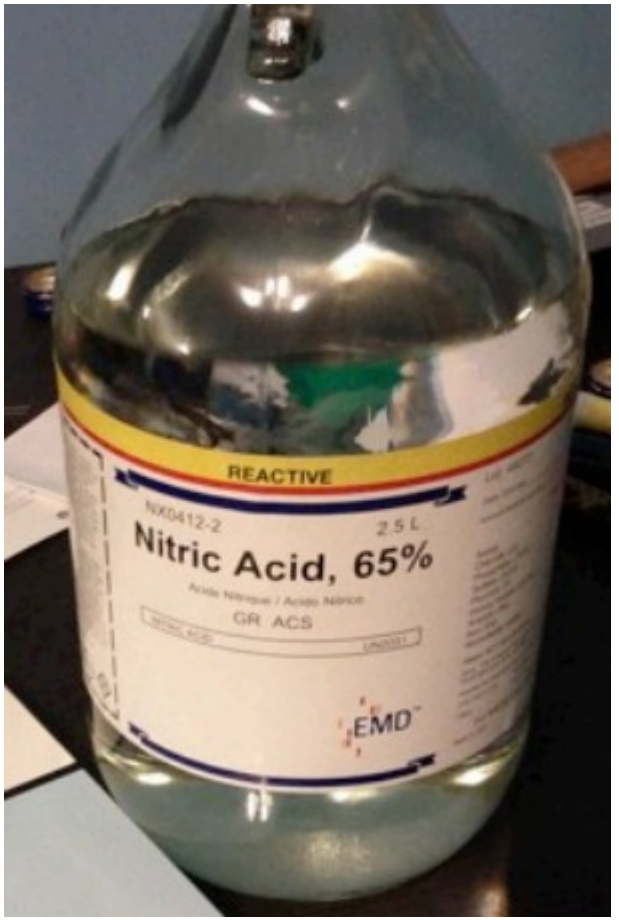
- Alternatively: NWK calculated from Coordinator's network card's serial number

LOCAL KEY EXTRACTION

- Node outside of your premises (building)
  - Moisture sensor in garden, doorbell
- The key is stored in a non-volatile memory
  - and after powering on, also in RAM

CHIP DECAPSULATION





Photos: AliExpress, Travis Goodspeed

CHIP DECAPSULATION

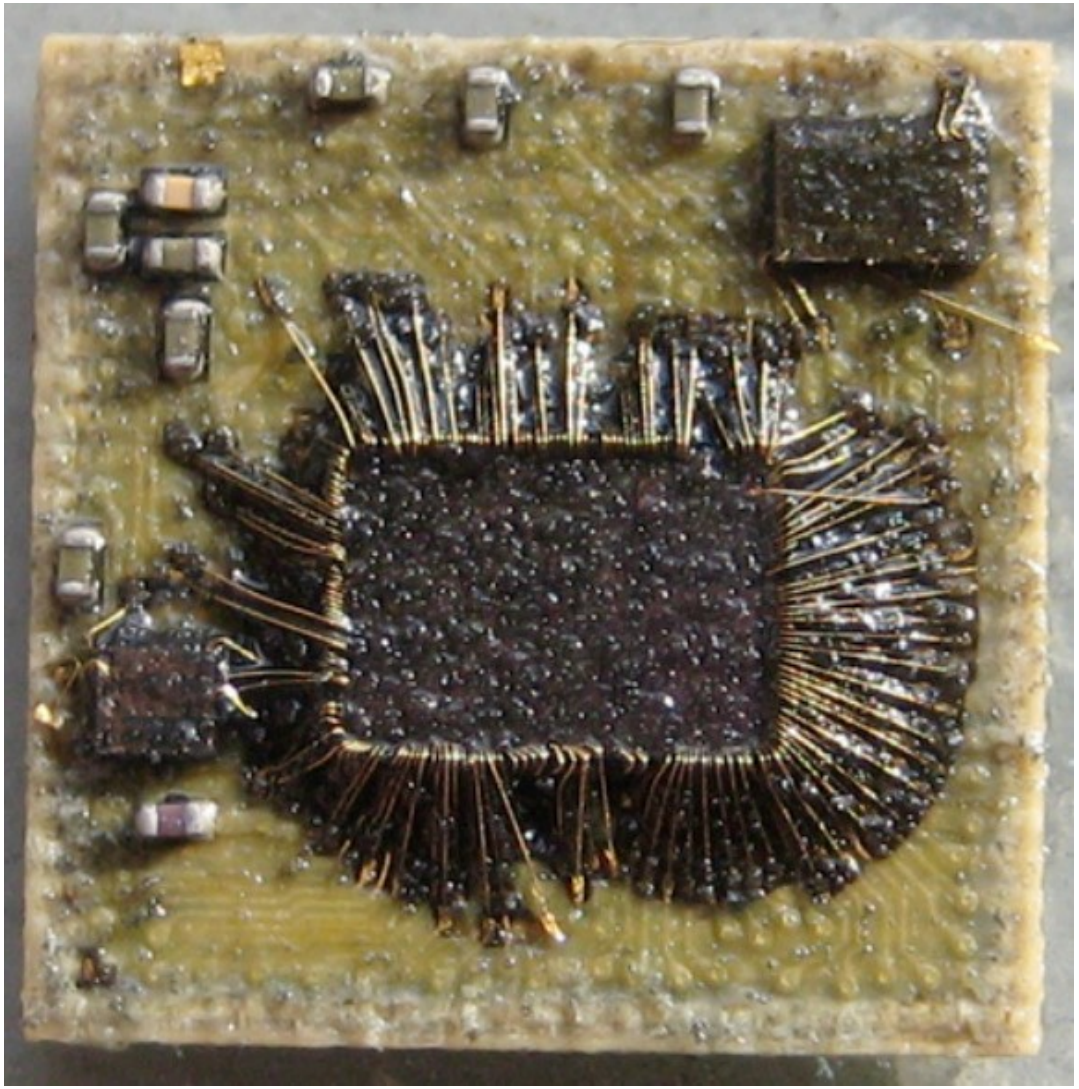


Photo: Travis Goodspeed

DECAPSULATION

- Mechanical
  - cheap, error-prone
- Acid (e.g. sulfuric acid + nitric acid)
  - Dangerous (DNT@home), error-prone
- Plasma/laser
  - Expensive, ~5000€ @ e-bay second-hand

FINDING THE NWK

- 128 kB = 1 Mbit of non-volatile memory.
- NWK length is 128 bits.

- Network Packet has a MIC
  - Message Integrity Code (checksum)

- Try all 128-bit sequences until MIC succeeds

DECAPSULATION

- One of the pins used for powering the non-volatile memory (NVM)
- Chips tries to boot from external memory
  - That is under your control
- Power on the NVM after booting from external memory and then read its contents

LOCAL KEY EXTRACTION

- Firmware is write-only
  - Reading firmware contents not possible
  - Erasing + flashing a new one is possible

- „CHIP-ERASE”
  - Does not erase the contents of RAM
  - NWK in RAM

LOCAL KEY EXTRACTION

- Separate MCU and radio
  - Connected using wires

- 50€ Logic Analyser
  - Read the transmitted signals
  - Find the chip manual
  - Reverse engineer the traffic
  - Read the key

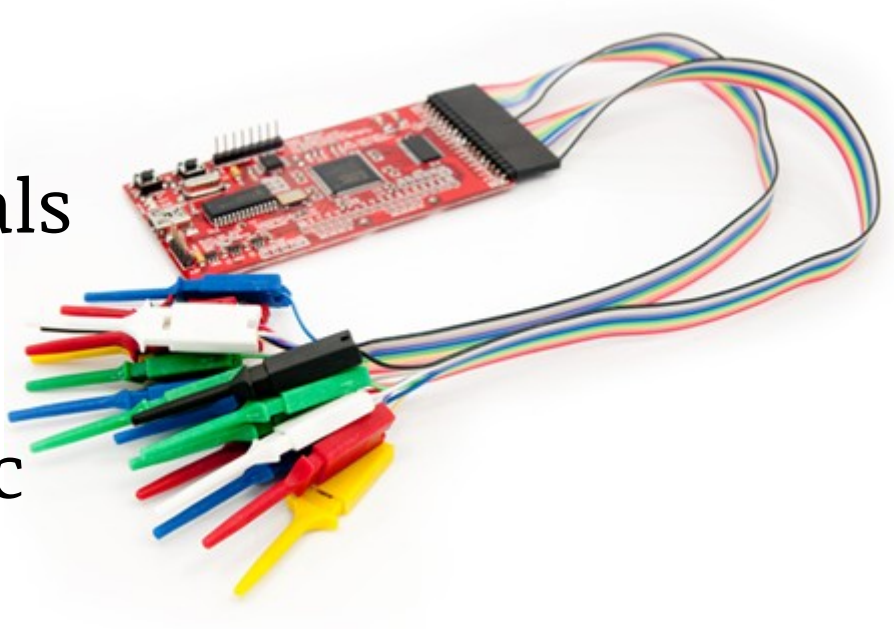


Photo: seeedstudio.com

FRESHNESS

- Replay attack

- Frame counter (FC) – 8bit
  - 256 possibilities
- Frame counter – 32-bit.
  - Packet with FC value 0xFFFFFFFF

RADIO JAMMING

- CSMA/CA
- Transmit is allowed only when the channel is not occupied

- Jamming
- Better: reactive jamming
  - ~20 microseconds required to detect transmission and start jamming

DENIAL OF SLEEP

- Take orders from the Coordinator.
- If there is an order, it must be fulfilled
  - (e.g. change of network key)

- Overhearing
- Idle listening

DETECTION

- Intrusion Detection System
- Uniquely indentify transmitters
  - Transient Signal
  - Radiometric characteristics
    - Tested with 100+ Wifi cards
- Expensive

INTERESTED?

ZigBee - probably the most used LR-WPAN protocol

http://zigbee.luure.info (in Estonian)

http://zigbee.luure.info/test-cases-for-zigbee-security-testing