TrustnGo
Plug & Play Security

Secure your IoT & Embedded Products

Hello!

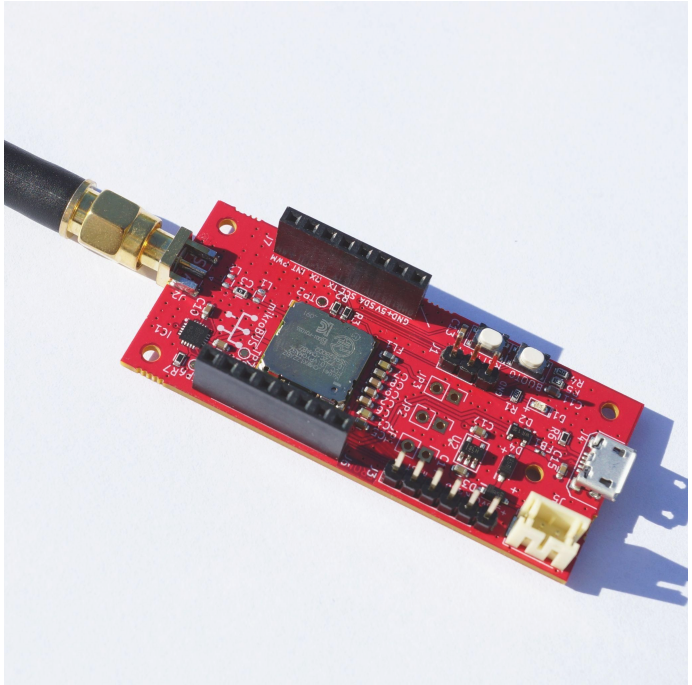
Michael Grand, Founder of TrustnGo

10 years of experience in security assessment of embedded systems.

Former deputy technical manager and R&D manager at Serma Safety & Security

IoT Market in 2021

- How many ?
  - *12,3 billion*
- Usages :
  - *Predictive maintenance*
  - *Smart meter*
  - *Asset tracking*
- Low project maturity :
  - *27% of projects at Proof of Concept stage*



Source : Journal du Net, année 2021

IoT / OT cybersecurity overview (1/2)

68% Sixty-eight percent of security practitioners say management believes IoT/OT innovations are critical to support business development and strategic activities.

60% Sixty percent of security practitioners say IoT/OT security is one of the least secured aspect of their digital infrastructures.

31% Thirty one percent of the IT security practitioners have slowed limited or stopped the adoption of IoT and OT project due to security concerns

Source: The State of IoT/OT Cybersecurity in the Enterprise, Ponemon Institute, November 2021

IoT / OT cybersecurity overview (2/2)

35% Thirty-five percent of organizations have recently observed an IoT device being used to conduct broader attacks.

39% Thirty-nine percent of the organizations have recently experienced an incident where an IoT device was the target of the attack.

63% Sixty-three percent of the organization expects attacks against IoT/OT devices to increase significantly in the years to come.

Source: The State of IoT/OT Cybersecurity in the Enterprise, Ponemon Institute, November 2021

Why your product deserve to be secured ?

- *Protect your customer's assets*
  - E.g. personal data, physical integrity
- *Protect critical IT/OT network infrastructures*
  - IoT should not be an entry point for an attacker
- *Protect your valuable intellectual property*
  - Against theft, counterfeiting and over production

Using a holey umbrella is a bad idea just like developing your own security function.

Why you should outsource cybersecurity to specialists?

- *Foolproof implementation*
  - No homemade suspicious security feature developed by an intern.
- *Add value to your product for a limited cost price*
  - Hiring a skilled team of cybersecurity experts is a way more expensive.
- *Shorten your time to market*
  - No need to learn cryptography or fight with barely understandable datasheets.
- *Stay focus on your core business*
  - Work and improve your strengths, outsource the remainder.

Our Goal: Address six of the Top 10 vulnerabilities (OWASP 2018)

1. **Weak, Guessable, or Hardcoded Passwords**
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. **Lack of Secure Update Mechanism**
5. **Use of Insecure or Outdated Components**
6. Insufficient Privacy Protection
7. **Insecure Data Transfer and Storage**
8. Lack of Device Management
9. **Insecure Default Settings**
10. **Lack of Physical Hardening**

TrustnPlay for MCU : Our *turnkey* security platform

- **Easy to use** secure platform for IoT and embedded systems.
- Based on **Zephyr OS** a widely used open source RTOS.
- Chip vendor and cloud provider **agnostic**.
- **Does not require** the usage of an external *Secure Element*

TrustnPlay for MCU : available plan

Basic

Secure interfaces

- ✅ Secure boot / update
- ✅ Secure communications
- ❌ Secure external storage
- ❌ In-depth security
- ❌ Physical attacker resistance

Standard

Secure interfaces & sw

- ✅ Secure boot / update
- ✅ Secure communications
- ✅ Secure external storage
- ✅ In-depth security
- ❌ Physical attacker resistance

Advanced

Secure interfaces & sw & hw

- ✅ Secure boot / update
- ✅ Secure communications
- ✅ Secure external storage
- ✅ In-depth security
- ✅ Physical attacker resistance

TrustnPlay for MCU : Basic version in brief

- Based on **Zephyr OS** and **MCUboot**
- Supports all ARM Cortex-M based MCUs (ask us for compatibility with other architectures)
- **Fully pre-configured** secure boot / update
  - Firmware authentication with ED25519
  - Firmware encryption with AES-128 and ECIES-X25519
  - **Anti-rollback counter**
  - Power loss resistant and reversible update process
  - Mcumgr update manager (Serial, Bluetooth, USB, UDP)
- Bootloader **isolated from user application** thanks to ARM MPU
- Secure TLS / DTLS network connections with **ATECC608 as optional back-end**

TrustnPlay for MCU : Standard version in brief

- Based on **MCUboot**, **Trusted Firmware-M** and **Zephyr OS**
- Supported platforms :
  - **ARMv7-M MCU** when binded to an **NXP SE05x secure element** (CC EAL 6+)
  - **ARMv8-M MCU** with optional NXP SE05x secure element
- Fully pre-configured secure boot / update
  - All features of basic version backed up by a **secure enclave** (TrustZone and/or NXP SE05x)
- Bootloader isolated from user application thanks to TrustZone (ARMv8-M) or MPU (ARMv7-M)
- All **cryptographic materials** (key and certificates) **securely stored** in a secure enclave
- Secure TLS/DTLS connections relying on TrustZone and/or NXP SE05x back-end

TrustnPlay for MCU : Advanced version in brief

- Based on **MCUboot**, **Trusted Firmware-M** and **Zephyr OS**
- Supported platforms :
  - ARMv8-M MCU with optional NXP SE05x secure element
- All features of Standard version
- Bootloader + Trusted Firmware-M **resistant to fault injection attacks**
- Crypto algorithms **resistants to side-channel attacks** (when executed from SE05x).

TrustnPlay for MCU : What you get

- TrustnPlay SDK
- Getting started documentation
- **1 Year** updates
- **1 Year** technical support*
- **1 Year** CVE monitoring

*May vary according to the selected plan

TrustnPlay for MCU licensing

- Royalty free
- Per project/product license or site license
- Perpetual license with update and support services renewable on a yearly basis

TrustnGo : Additional services

- Risk assessment and security problem definition
- Security architecture and code hardening consulting
- Support on CSPN, SESIP and CC certifications
- Trainings in embedded system security

TrustnGo

Plug & Play Security

37 Cours du Maréchal Georges Clémenceau 33000 Bordeaux - Tel: 06 67 44 01 93 - Mail: contact@trustngo.tech