Secure Solutions for IoT Nodes

- Cloud Connectivity Out-of-the-Box
- Why should you add a Secure Element?
- Secure Platform
- Prototyping with STSAFE
Cloud Connectivity Out-of-the-Box

- Ultra-low-power STM32L475 Arm® Cortex®-M4, 1 Mbyte Flash memory, 128 Kbytes of SRAM
- Firmware example for IoT end node connected with Wi-Fi®
  - 802.11 b/g/n compliant Wi-Fi® module
- Low Power Communications
  - Bluetooth 4.1, Sub-GHz, Dynamic NFC Tag
- Multiway Sensing
  - 3D Accelerometer, 3D Gyroscope, 3D Magnetometer, Temperature/Humidity, Pressure, Time of Flight, Microphones
• **X-CUBE-AWS**
  - Cloud Connector: set of libraries and application examples, MCU acting as end devices.

• **FP-CLD-AWS1**
  - Based on X-CUBE-AWS provides a companion AWS-based web dashboard for an easy sensor data visualization and device control.

• **Amazon FreeRTOS**
  - STM32’s port of the operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage.
• X-CUBE-AZURE
  • Cloud Connector: set of libraries and application examples, MCU acting as end devices.

• FP-CLD-AZURE1
  • Based on X-CUBE-AZURE provides a Web Dashboard with full support for Azure device management primitives and sample implementation for firmware update over the air (FOTA).
• X-CUBE-GCP
  • Cloud Connector: set of libraries and application examples, MCU acting as end devices.
  • Web Dashboard: telemetry functionality with data plotting and commands from the cloud.
• X-CUBE-WATSON
  • Cloud Connector: set of libraries and application examples, MCU acting as end devices.
  • IBM Quickstart and Registered Mode support.

• FP-CLD-WATSON1
  • Includes pre-integrated FFT algorithms for the processing of accelerometer data which can be used to detect vibration from devices such as motors, fans and pumps.
  • Maximum frequencies and tear/wear conditions of the device under test are reported together with raw sensor data to IBM Watson IoT thus enabling solutions for industrial condition monitoring and predictive maintenance.
Classes of Attacks

How would you defend from these?

- **IoT Device**
  - Internet

- **Cloud Service**
  - Misuse of network protocols
    - Exploit communication protocol errors
    - Flaws in software design / implementation

- **Software Attack**
  - With the case opened / removed
    - Test / debug port access
    - Inter device bus and IO probing
    - Reset, clock attacks
    - Power analysis
    - Temperature / electrical attacks (glitch, overvoltage)

- **Board Level Attack**
  - Device de-packaged
    - Circuit analysis and probing
    - Fault injection
    - Laser beam

- **Silicon Level Attack**
  - Circuit analysis and probing
  - Fault injection
  - Laser beam
Secure Platform

STSAFE enhances the tamper-resistance of an IoT Device throughout its lifecycle.
Secure Platform

STSAFE supporting secure boot, firmware updates and communications

- A Secure Element is designed to thwart silicon invasive attacks
- Independently assessed, achieving very high standards like EAL5+ Common Criteria Certified chip
- Protects keys and performs cryptographic functions (ECDH, ECDSA, AES)
  - For Secure Communications, Secure Boot and Secure Firmware Updates
- Provides up to 6K bytes of Secure Data Store
- Devices shipped with secure keys and certificates which are provisioned during ST’s manufacturing process reduces production cost and complexity
  - Trusted device identities don’t require hardware security modules (HSM) in the supply chain, and their presence cannot be bypassed
- STSAFE may be combined with STM32, or other semi-vendors devices
Secure Solutions

STSAFE enables end-to-end security

- **STSAFE-A Optimized** authentication solution
  - Authentication
  - Secure communications, Secure data storage
  - Secure key provision service
  - EAL5+ Common criteria certified chip

- **STSAFE-J Flexible** Java based solution
  - Trusted network access with Authentication
  - Secure Data storage, Secure communication
  - Personalization services
  - Common criteria and BSI certification

- **STSAFE-TPM Standardized** solution
  - Platform integrity, Authentication
  - Secure Boot, Secure Firmware upgrade
  - Secure data storage and Secure communication
  - Solution CC EAL4+ and TCG 1.2 / 2.0 certified
Secure Boot uses cryptographic functions to confirm the authenticity of firmware before allowing it to run.

A multi-stage boot process is where each stage authenticates the next.
Secure Boot

Utilizing STM32L4’s security features and STSAFE

• Performed after a RESET, using a Public Key stored in the device
• It is a stateful process for predictable behavior

Code Authentication

- Code
- Hash
- Public Key
- ECDSA Verify
- Hash Value
- Calculated Hash Value
- Compare
- Trusted
- OK
- Run Code
- NOK
- Reload

Secure Process

Reset
Immutable code
Secure Firmware Update

The ECDSA verify process off-loaded onto the STSAFE

- This is a stateful process for predictable behavior
- A file is downloaded containing the new firmware image and corresponding certificate
- The code image is then authenticated using a Public stored in the device
- If successful, the new firmware image is stored, ready for use
Connecting to the Cloud

Recommendations for handling TLS assets

- Make use of the security mechanisms provided by the MCU to protect code, cryptographic functions and protect the keys (especially the Private Key 🗝️)
- Store certificates and credentials in such a manner they cannot be easily replaced
Handling TLS Assets

- The Elliptic Curve cryptography is off-loaded to the STSAFE from the MCU
  - Reducing the amount of SRAM needed by the MCU
- The IoT Devices Private Key is stored securely in STSAFE tamper-resistant memory
Performance Benchmarking

STSAFE-A100 improves TLS performance

STSAFE integrated with WolfSSL

Benchmark - Time

- ECC 256 key gen
- ECDHE 256 agree
- ECDSA 256 sign
- ECDSA 256 verify

Faster is better!
STSAFE-A100 tamper proof IoT Device identity without production HSMs

• Has been verified to protect the ECC private key used as the basis for TLS to common criteria EAL5+; your device using STSAFE-A100 is infeasible to clone

• An OEM specific CA is registered with AWS to allow devices to be authenticated on first connection, using the JITR process

• ST provides STSAFE devices pre-loaded with certificates signed by this CA

• When connecting to AWS IoT devices presenting these certificates will be accepted and automatically associated with the OEM’s account

• MoQ
Quick Prototyping with STSAFE-A100

STM32 Discovery Kit IoT Node + X-NUCLEO-STSA100

- Ready-to-use printed circuit board STSAFE-A100 secure element.
- STSAFE-A100 pre-personalized with an evaluation configuration
- ARDUINO® connectors for connection to ARDUINO®-compatible microcontroller boards
- HE10 Aardvark™ connector for connection to a Total Phase Aardvark™ adaptor.
- Voltage selector to select the 3.3 V or 5 V power supply
- Chip reset jumper to force the chip reset stage
- User LED for use in applications