Securing IoT devices with STM32 & STSAFE Products family

Fabrice Gendreau
Secure MCUs Marketing & Application Managers – EMEA Region
Application Strategic Focus

The leading provider of products and solutions for Smart Driving and the Internet of Things
Secure market & applications

- **Banking, ID**
  - PayTV, Transport & Banking, ID
  - ST31 – STS3921/22 - ST53

- **Authentication**
  - Smart World & Internet of things
  - STSAFE & Custom

- **Mobile security**
  - Mobile & Secure NFC, M2M & Automotive, Wearable
  - ST33 - ST21NFC – ST54
Building a fortified solution is all about risk management

- Understand the value of the Assets you are going to protect, taking into account all stakeholders.
- Understand your Threats and Vulnerabilities.
- Develop a security strategy to reduce Risk, using right level of security for the value of the Assets being protected.
- Make use of the integrity and cryptographic tools available.
Threats

Device Cloning & Counterfeiting
- A cloned device compromises OEM revenues
- A counterfeit device compromises OEM brand
- IoT network or cloud application is polluted by fake devices sending erroneous data

User data corruption & eavesdropping
- Data travel in clear over the network and expose some personal data
- An corrupted measurement is sent to the cloud

Device malfunction
- An erroneous command is sent to an actuator by a fake server
- A malware is injected in a device to modify its behavior

Needs

Resistance against cloning, hacking
- Secure Data storage
- Secure Data communication

Data privacy & confidentiality
- Encryption & signature

Prevent denial of service
- Platform Integrity
- Secure Boot
- Secure Firmware Upgrade

Answer

Device authentication
- Device to device
- Device to server

Authentication and Encryption strength depends on how well keys are protected
Identify the classes of Attacks

Box

Internet

Remote software attack

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

Remote 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

Silicon level attack

- Device de-packaged
  - Circuit analysis and probing
  - Laser fault injection
Identify the classes of Attacks

**Box**

- Internet
- Remote software attack
- Board level attack
- Silicon level attack

**Solutions**

1. Read out protection level
2. Write protection
3. Execute only PCROP
4. Memory Protection
5. Firewall
6. Crypto accelerator engine
7. Secure Firmware install
8. Backup RTC RAM memory

**Attacks**

- Protection against faults injection
- Protection against side-channel attacks
- Monitoring of environmental parameters
- Memory obfuscation, Active shields
- Strong authentication / crypto services
- Secure key storage and handling
- Secure code storage and execution
- Secure key provisioning
Cryptography is the mathematical toolbox providing security services to build secure systems

Whatever Symmetric (AES) or Asymmetric (RSA, ECC) cryptography

Security mechanism rely on secrets

Secrets are keys

Level of Security depends on how secrets are generated, stored, and handled
MCU-based devices: possible architectures

Keys stored in General Purpose MCU or in a key container as a Secure Element

**Use MCU’s embedded security features offering protection against non-invasive attacks**

**Add a Certified (CC EAL5+) Secure Element which guarantees state of the art security protection against physical and logical attacks**
## GP MCU’s embedded security features

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Security Measures</th>
</tr>
</thead>
</table>
| Software Attacks  | - Memory Protection Unit (MPU)  
- Firewall  
- Read Out memory protection  
- Write memory protection  
- Proprietary Code Read-Out Protection (PCROP)  
- RNG, Crypto accelerator, CRC  
- Memory ECC, Parity check  
- Read while write  
- Secure Firmware Install |
| Non-Invasive Attacks | - JTAG Read out protection  
- BOOT from Flash only  
- Tamper pads  
- RTC alarm, registers, SRAM mass erase  
- Power supply integrity monitor  
- Clock security system  
- Temperature sensor |
| Invasive Attacks   | - GP MCUs not designed to resist against advanced security attacks                |
A Secure Element (SE):

- is a tamper-resistant platform (typically a one chip secure microcontroller)
- capable of securely hosting applications and storing their confidential and cryptographic data
- in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities
Secure Element – Trusted Security
Development, Production and Personalization

Non-Invasive attacks
Material & IP Theft
- Secure manufacturing and development environments
- Product lifecycle management

Semi-Invasive attacks
Fault Injection
- Dedicated architecture and design
- Hardware and Software countermeasures

Invasive
Physical Attacks
- Shields
- Intrusion detectors
- Obfuscation

Security evaluated by independent 3rd party laboratories according to defined rules and rankings

Embedded Data, Application (Flash / EEPROM)
Embedded Code (Flash or ROM)
Hardware
Different kinds of Secure Element

**STSAFE-A**
Optimized SE
- Native OS
  - Providing dedicated Crypto Services
- Authentication, Encryption, Signature, Secure Storage

**STSAFE-TPM**
Standardized SE
- TCG compliant OS
  - TPM 1.2 or 2.0 commands set
  - CC EAL4+ certified
  - FIPS 140-2 certified
- Platform integrity measurement and reporting

**STSAFE-J**
Flexible Java Card SE
- Java Card OS 3.0.4
  - Global Platform 2.1.1
  - CC EAL5+ certified
- Running Specific Applications

**Secure Microcontroller**
- Secure Core CPU / ROM or FLASH memory / Hardware Crypto Accelerators RSA, ECC, DES, AES
- CC EAL5+ or EAL6+ certified
Combining Secure Element with local Host MCU
Enabling easy of use security services for IoT developers
Combining STSAFE-A to local Host MCU
Highly secure & cost optimized solution for connected devices

- Authentication (devices to servers)
- Secure communication (Integrity & Confidentiality)
- Secure Data storage
- Signature verification (Secure Boot & Secure Firmware update)
- Secure key provisioning service
- Seamless integration with GP MCU

EAL5+ Common Criteria certified chip
1st Use case example: Peripheral authentication

Remote server
- Requests IOT Certificate
- Uses CA certificate to verify IOT Certificate
- Generates Random
- Verifies signature using IOT certificate
- If signature is verified, IOT device is authenticated

IOT device
- Generates Random
- Signs Random with secret private key
- Verifies signature using IOT certificate
- If signature is verified, IOT device is authenticated

Secure Element
- Provides X509 certificate from data partition Index 0

Wire or wireless connection
USB, WiFi, LoRa...
**2nd Use case example: TLS Handshake V1.2 (RFC 5246)**

**Remote server**
- CA Certificate
- Host Certificate

**IOT device**
- GP MCU
- Secure Element

---

**Processing**
- Verify Server host certificates with CA certificate
- Authenticate server verifying signature
- Generate ephemeral EC key pairs
- Computes shared secret using Remote server public key

---

**Replies algorithms choices**
- Client Hello (client random)
- Server Hello (server random)

**Provides**
- X509 certificate and signed random
- Request IOT device X509 certificate

**Verifies IOT Device certificate and authenticate IOT device**
- Certificate (), signed client random
- Certificate Request ()
- Server Key Exchange ()
- Server Hello done ()

**Computes Diffie-Hellman shared secret**
- Certificate (), signed server random
- Client Key Exchange ()
- Certificate Verify ()
- Change Cipher Spec ()
- Client Finished ()
- Change Cipher Spec ()
- Server Finished ()

**Provides IOT device X509 certificate and signed random**

**Provides ephemeral public key**

**Starts exchange ciphering**

**Wire or wireless connection**
- USB, WiFi, Lora…

**Secure Element**
- CA Certificate

**GP MCU**
- I2C

**IOT Certificate**
- Secure Element

---

**Starts exchange ciphering**
Secure Element personalization service
Securing IoT devices manufacturing
Secure Element seamless integration
A comprehensive set of tools and services

- STSAFE Nucleo Expansion
- STSAFE Toolkit PC application
- Personalization service
- Host library
- Example codes
Scalable Security Platform for IoT Devices
powered by STSAFE, ProvenCore-M & STM32

Ensuring platform integrity

STM32L4 MCU
For faster, reliable and robust applications development

ProvenCore™-M Secure Operating System
For application isolation, stability and integrity of the platform

STSAFE™-A Secure Element
Providing secure storage, crypto-services to strengthen secure boot & firmware update
Secure Cloud Connectivity with STSAFE-A

STSAFE-A100 secure and ease devices registration to Amazon Web Services

- Device by device registration with STSAFE-A100 standard personalization for evaluation
- Devices JIT (just in time) registration to AWS with STSAFE-A100 preconfigured for AWS. Allow mass devices automatic registration to AWS
- STSAFE-A100 TLS secure connection establishment

STSAFE-A100 evaluation Kit
Security for Amazon Web Services
Secure Sigfox Ready™ Connectivity powered by STSAFE-A, S2-LP & STM32

Ultra-low-power Sensor-to-Cloud Connectivity out-of-the-box

S2-LP
Ultra-low power, high performance, Sub-1GHz RF transceiver

STSAFE-A1SX
Plug and play certified security
HW CC EAL5+

STM32L
 Ultra-low-power MCU portfolio
Secure LoRaWAN™ Connectivity
powered by STSAFE-A1LR & STM32L

G+D, Murata, and STMicroelectronics Bring Flexible and Efficient Security Solutions to LoRaWAN™ devices


Flexible solutions for IoT security

The solution consists of:

- G+D’s Key Management System
- STM’s STSAFE-A secure element attached to STM32 general-purpose microcontroller
- MURATA’s LoRaWAN module
Security is becoming a major concern for IoT devices makers
  • A security breach could lead to loss of consumer confidence, loss of brand reputation and loss of businesses!

Start with your own risks assessment, understanding the value of assets for all the stakeholders
  • Perform a Threats analysis to better understand your Risks
  • Remember Confidentially, Availability and Integrity

Define your security policy in order to reduce the risks
  • Hackers will go after the weakest links in the system not necessarily directly to their target

Develop your solution resilient against attacks throughout its whole life-cycle
  • By using MCU’s embedded security features for protection against non-invasive attacks
  • And adding a companion Secure Element which guarantees state of the art security protection
Secure Solutions
Ensuring your peace of mind