物联网设备的安全需求与解决方案

王朋朋
2019年10月

SECURE CONNECTIONS
FOR A SMARTER WORLD

物联网和技术创新带来了新的机遇和挑战

Cloud

Globally available, unlimited compute resources

Secure Connectivity

High secure bandwidth coupled with IoT & edge computing

IoT

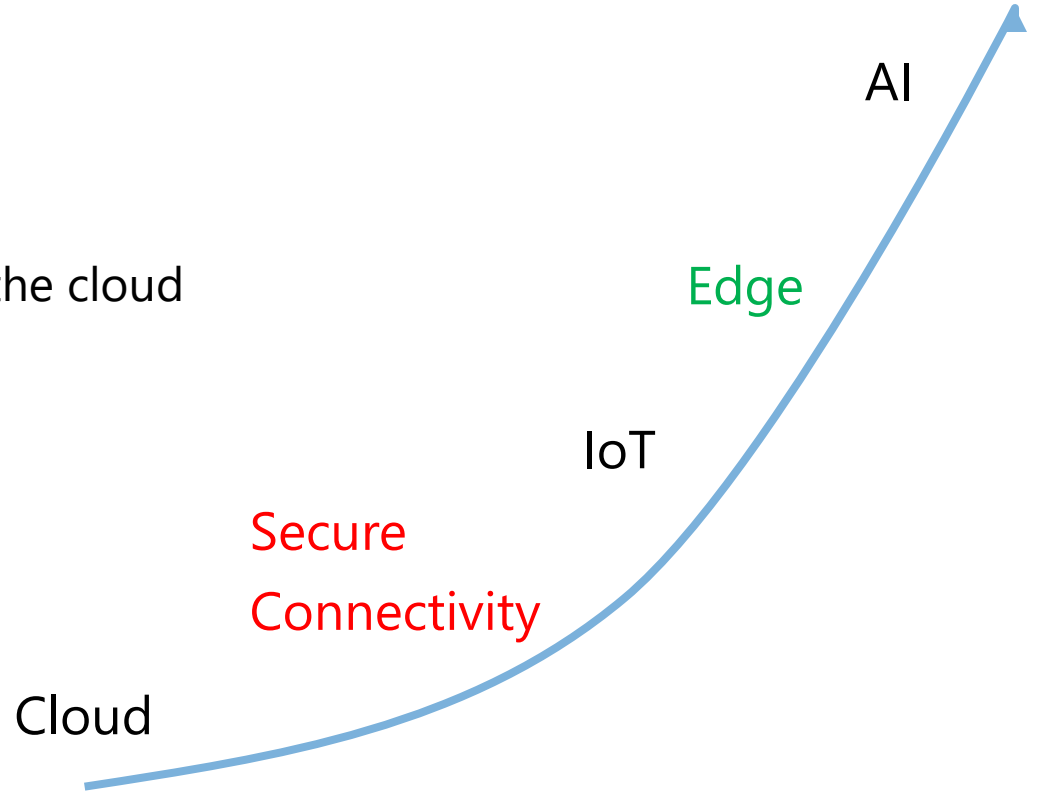
Harnessing signals from sensors and devices, managed centrally by the cloud

Edge

Intelligence offloaded from the cloud to IoT devices

AI

Breakthrough intelligence capabilities, in the cloud and on the edge



物联网缺乏安全性现在是显而易见的

The lack of Security in IoT is now tangible

THE BOTNET THAT BROKE THE INTERNET ISN'T GOING AWAY

Mirai botnet

Disruption of major Internet services

Jeep hack

Loss of control over vehicle via WiFi connection

Casino hack

Overview of high-rollers extracted via thermostat of a fish-aquarium in the lobby

Software bug makes Nest Cams vulnerable to hacks

Nest Hack

Security camera shut down by a simple click on a phone

Target Hack

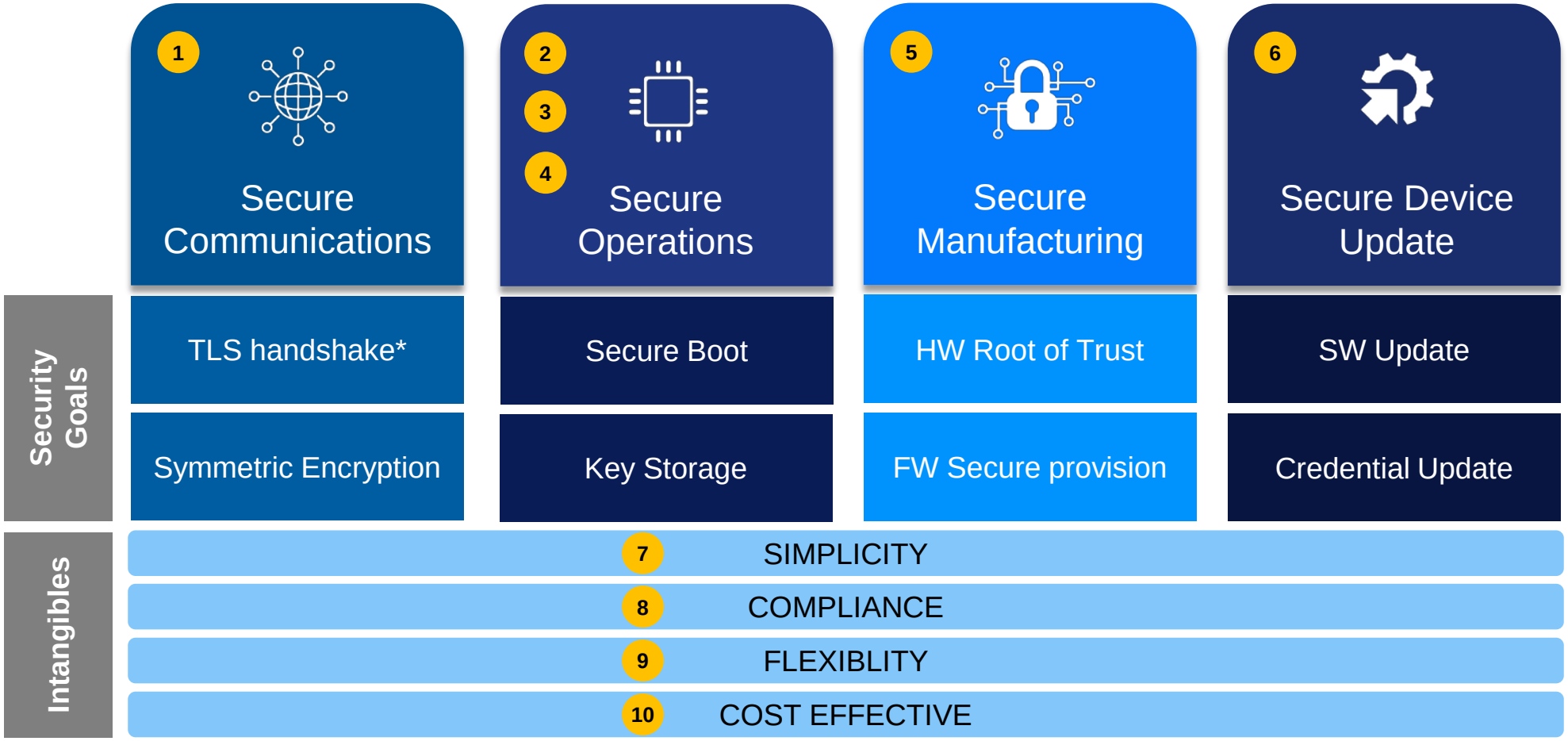
Target declared that the total cost of the data breach had been $202M *NBC news, May 24, 2017*

TARGET

SEPTEMBER 20, 2017 by Manita Badkar in New York

Parcel delivery company **FedEx** said on Tuesday that a June **cyber attack** on its **TNT Express** unit **cost** the company **$300m in the first quarter**, ... the **NotPetya cyber attack**, which originated from tax preparation software in Ukraine and resulted in the disruption of communications systems at TNT Express.

物联网设备的主要安全挑战 -- *解决这四个挑战使OEM能够对应主要的物联网攻击*



TLS handshake* : HW pre-integration of common SSL stacks e.g OpenSSL, mbedTLS..

物联网设备的首要安全问题 -- *客户关于安全需求的声音*

Customer Security Concern	Nr	Concern Description	Business Drivers
Trusted TLS stack	**1**	Customers are looking for standard TLS stack for device to cloud secure communication, i.e OpenSSL, mBdedTLS	Prevent Data breaches ($), IP theft, Protect User Privacy
Secure storage of device credentials	**2**	Customers want protection of device Keys and Identity, against remote and local attacks. Level of prot vary per use	Preserve Brand and business model (protect access to services and against device cloning)
Device FW / OS integrity check	**3**	Customers need protection of device integrity and critical device functions. Prevent unauthorized FW to run.	Avoid mal functions of devices, to deliver best user experience, preserve brand and humans safety.
Device data reset when a tampering event is occurred	**4**	Customers want a way to erase sensitive data from devices at tamper mesh event, either physically or automatically.	Preserve brand and warranty cost, protect infrastructure security, low cost of maintenance
Zero trust on 3rd party manufacturing and supply chain	**5**	Customers don't trust their CM/ODM in China, and wants to implement zero trust model for device manufacturing	Anti-Counterfeit of devices to avoid Business loss. Preserve Reputation, Intangibles : Cybercrime Cyberwar
Secure Update capabilities of FW / OS	**6**	Customers want to keep control on devices OTA to prevent and recover from DDos Attacks, deploy new features, fix bug	Keep innovation by pushing new functionalities, keep security up to date to preserve brand
Zero touch connect to clouds	**7**	Customers want a simple and secure way to register their devices with Clouds, method should not rely on CM.	Fast time to market, less complexity for digital transformation
Compliance with Countries security policies	**8**	Customers are worried about compliance with Country / Segment specific policies and standards i.e GPDR	Preserve access to a market, liability control
Cloud agnostic security solutions	**9**	Customers want to be able to migrate to another cloud with minimum investment, Multi clouds capabilities are required	Keep cloud cost negotiation advantage, preserve competitiveness, new business model
Security cost shall be effective	**10**	Customers are focusing on connectivity of devices and are willing to pay minimum for security in the BoM.	Keep down cost of product BoM for better margin and competitivity

可信安全执行环境 – TEE

将系统资源隔离为安全和非安全两个区域

仅执行经过认证的固件

哈希、加密解密外设

仅允许有授权的开发者进行调试

密钥、代码和数据安全

OTA固件更新、 撤销密钥、固件防回滚

MCU产品安全特性概览 -- *i.MX RT / LPC54S/55S / K(L)81/21*

特性	i.MX RT10xx	i.MX RT1170	i.MX RT600/500	LPC54S0xx	LPC55Sxx	K81/KL81	K21
对称和杂凑算法（DES/3DES, AES, SHA1/256）	✓- DES/3DES	✓+ SHA384/512	✓- DES/3DES	✓- DES/3DES	✓- DES/3DES	✓	✓
非对称算法 ECDSA (up to P521/B571) RSA (up to 4096)	X	✓CAAM	✓Casper	X	✓Casper	✓LTC	X
随机数产生器SA-TRNG	✓	✓RNG	✓	✓	✓	✓	✓RNGA
隔离安全应用 Isolated security applications (e.g. TFM)	X	✓	✓	X	✓	X	X
安全启动 (RSA up to 4096)	✓HAB	✓HAB	✓	✓	✓	✓Flash	✓Flash
加密启动Encrypted Boot	✓	✓	✓	✓	✓	X	X
安全调试Secure Debug	✓	✓	✓	X	✓	X	X
物理不可克隆模块SRAM PUF	X	✓	✓	X	✓	X	X
Always ON domain	✓	✓	X	X	X	✓	✓
安全存储Secure Storage (non-volatile)	✓	✓	✓OTP	✓OTP	✓PFR	✓	✓
防篡改Tamper Detection Signal	X	✓ Active	X	X	X	✓Active	✓Active
电压/温度/频率检测Volt/Temp/Freq Detection	X	✓	X	X	X	✓	✓
在线加密保护Bus Encryption (BEE, OTFAD)	✓	✓ + IEE	✓	X	✓ PRINCE	✓K81 only	X
量产保护Manufacturing Protection	X	✓	✓	X	✓	X	X
资源域隔离Resource Domain Isolation	✓CSU	✓RDC	✓TZ	X	✓TZ	✓SysMPU	✓SysMPU
数字内容保护Content Protection	X	✓	X	X	X	X	X

MCU安全模块提供的安全服务 -- *i.MX RT / LPC54S/55S / K(L)81/21*

安全服务类型	相关的安全模块	抵御的安全威胁
真实性（对信息的来源进行判断，能对伪造来源的信息予以鉴别）	• HAB, CAAM, SRTC, secure ROMBoot, LTC, Casper	假冒,重放
保密性（保证机密信息不被窃听，或窃听者不能了解信息的真实含义）	• DryICE, Tamper detection, CAAM, DCP, LTC secure RAM, TRNG, ZMK, BEE, IEE, OTFAD, PRINCE, HashCrypto, SRAM PUF	信息泄露,窃听,业务流分析,旁路控制,媒体废弃,物理侵入
完整性（保证数据的一致性，防止数据被非法用户篡改）	• CAAM, RTIC, SRTC, HashCrypto, eFuse, PFR	破坏信息的完整性,
可用性（保证合法用户对信息和资源的使用不会被不正当地拒绝）	• TrustZone, (X)RDC, CSU, CAAM, SysMPU, Secure AHB Controller	拒绝服务
不可抵赖性（建立有效的责任机制，防止用户否认其行为，这一点在电子商务中是极其重要的）	• CAAM, eFuse, unique ID. LTC, Casper, SRAM PUF	抵赖,业务欺骗
可控制性（对信息的传播及内容具有控制能力，阻止未经授权的访问）	• TrustZone, CSU, MPU, (X)RDC, Secure Debug, Secure JATG, CAAM, eFuse, unique ID, SRTC, sysMPU, Secure AHB controller, SRAM PUF	非法使用, 授权侵犯,特洛伊木马,陷阱门,计算机病毒,人员不慎,窃取

MCU上的安全子系统 -- *以LPC55S00为例*

安全启动管理

- 来自“可信计算工作组”的基于ROM的设备标识符组合引擎（DICE）

具有专用安全密钥访问权限的加密引擎

- CASPER非对称（RSA / ECC）引擎，可加速WolfSSL / mbedTLS（256位密钥）
- 恩智浦的实时解密引擎（**PRINCE**），用于加密内部闪存代码
- 对称（AES-256）和哈希（SHA-256）引擎
- 具有256位的真随机数生成器（RNG）

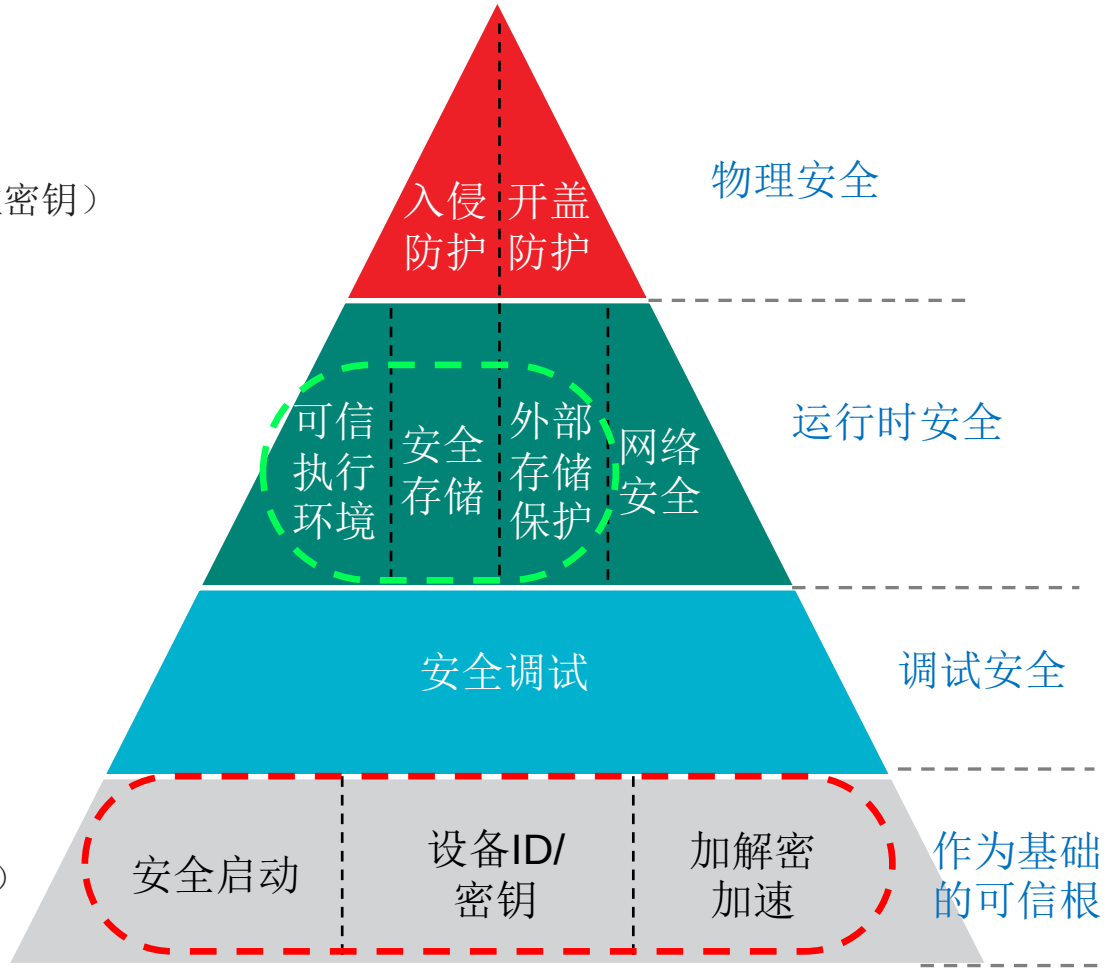
256位硬件保护的安全存储

- 先进的SRAM **PUF**提供了一个不变的，唯一的设备根密钥
- 带设备密钥存储区的受保护的闪存区域（PFR）
  - +符合行业标准的128位通用唯一标识符（UUID）
  - +现场和工厂可编程空间，可提供唯一的设备根密钥和密钥哈希

安全调试身份验证

物理保护和运行时安全

- Armv8-M **TrustZone**，安全归因单元（SAU）和安全内存保护单元（MPU）
- 与恩智浦定义的归因单元和安全总线/ GPIO / DMA控制器结合使用



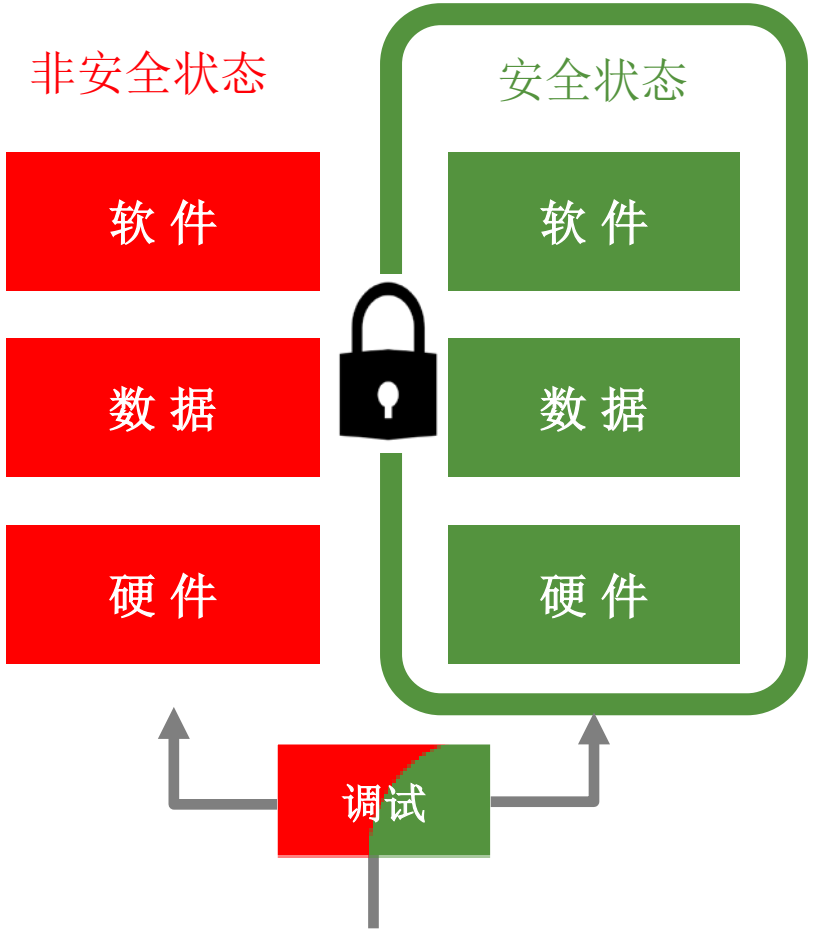
安全启动

想象一下，当系统未开机期间，如果可执行的代码被恶意篡改了，整个系统就会面临巨大的风险。
安全启动功能，就是要在开机上电时，就首先对程序代码进行检查，认证通过后才能执行这些代码。

步骤	基本操作	注释
1	系统上电	在此之前没有任何代码运行
2	第一条指令从ROM里开始执行	假定ROM代码是不能被篡改的，这点由芯片的设计所决定 这是以后安全机制的基本保障
3	ROM程序检查要执行的用户代码的安全性	ROM程序是安全代码，它可以把安全或非安全的代码当成数据来进行运算和校验
4	经过校验确认用户代码的安全性后，CPU开始在安全状态执行用户程序	
-1	用户程序烧录芯片时，可以用私有密钥对程序代码加密	这样可以进一步保证代码不会被盗取和被篡改

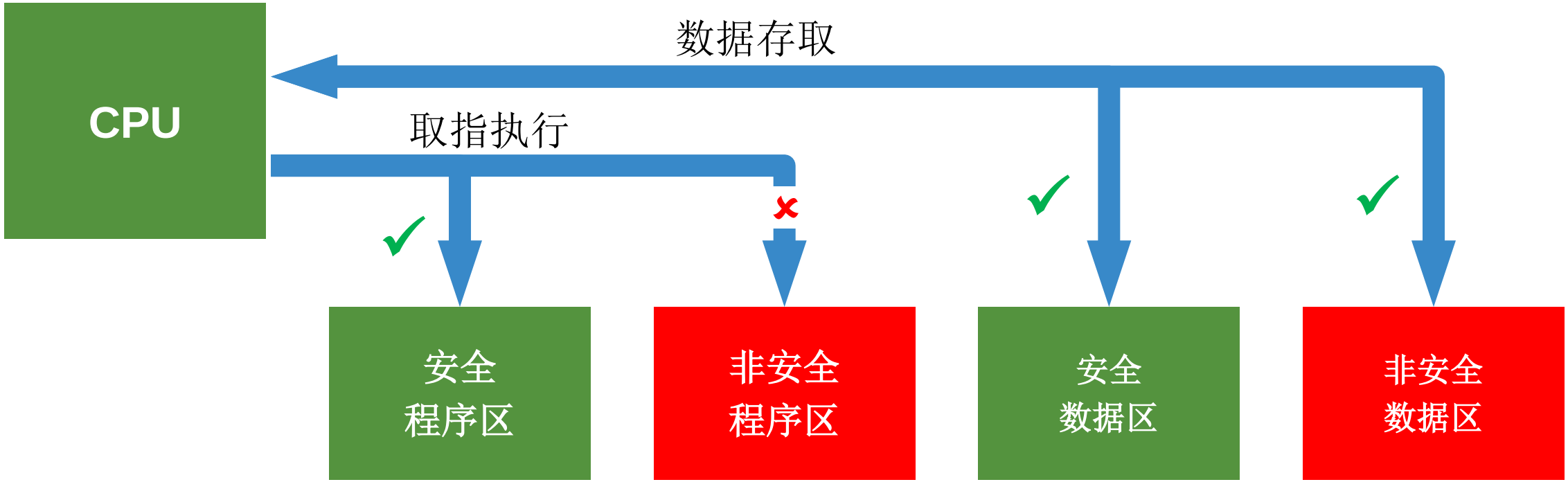
什么是Trust Zone

- Arm的TrustZone技术将系统分为安全和非安全两种状态
- 有特定的命令使CPU在两种状态之间切换



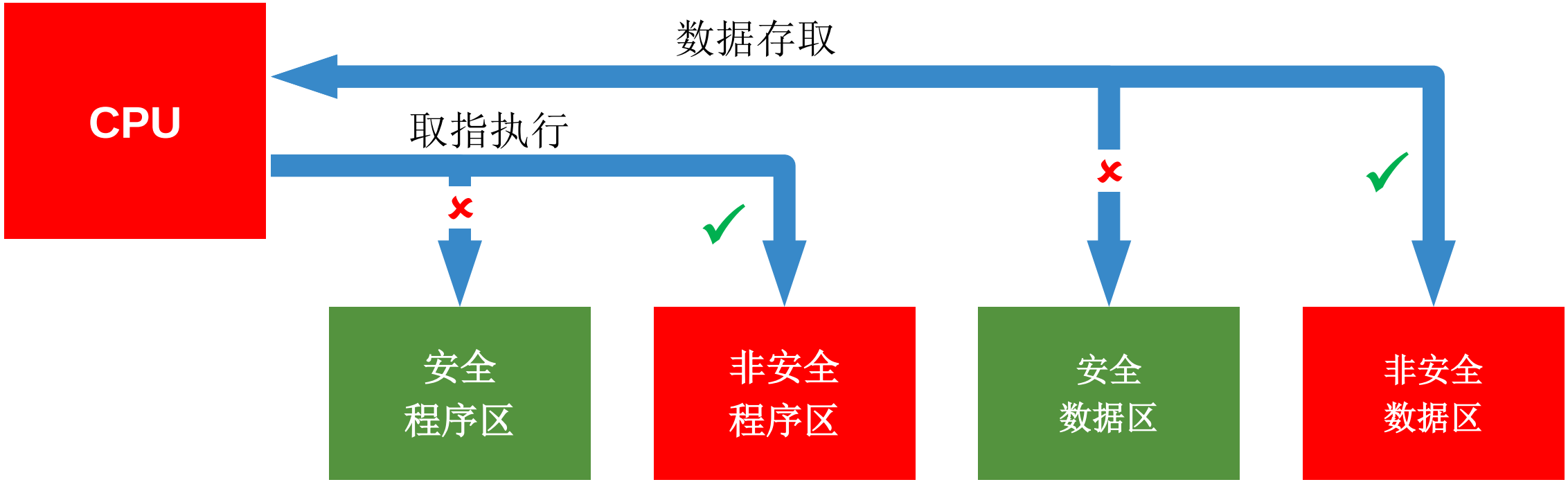
安全的 CPU 状态

- CPU在安全状态时，只能运行处于安全存储区的代码
- CPU在安全状态时，可以访问安全存储区和非安全存储区的数据



非安全的 CPU 状态

- CPU在非安全状态时，只能运行处于非安全存储区的代码
- CPU在非安全状态时，只能访问非安全存储区的数据

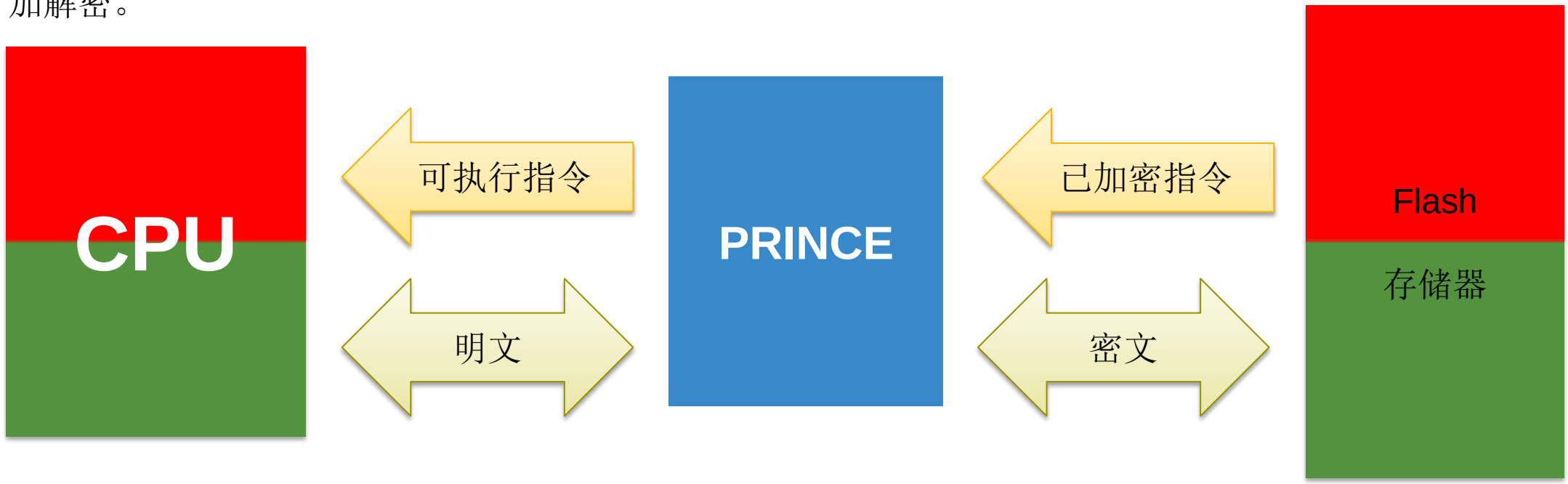


什么是PUF

- 对于安全应用，密钥管理机制至关重要。
- 在传统的通用MCU中，最普遍的做法是将密钥的明文存储在片内的OTP或者Flash中，但是实际上，攻击者只需要通过比较低的代价($200-$5000)就能从片内OTP或者Flash中获取到密钥。
- PUF(Physical Unclonable Functions)是物理不可克隆功能的缩写
- LPC5500内置的PUF是SRAM PUF。由于SRAM的硅结构特征，每个芯片的SRAM的数字特征都是独一无二的，因此每个芯片中读出的内容也是独一无二的。。
- 即使是NXP，也不可能制造出两颗数字特征一模一样的SRAM PUF。所以，我们称芯片内SRAM的独一无二的数字特征为芯片的指纹。利用芯片的指纹，就可以生成根密钥和储存所需的密钥。
- 当芯片断电以后，芯片内的PUF并不保留任何信息，传统的Crack Fuse/Flash手段也就无效了，自然也就避免了传统的片内OTP Fuse和Flash在断电后被暴力读取的风险。

PRINCE

- 一般情况下，我们的程序和数据都是以明文的形式存在于Flash中的。如果通过剖片或者其他技术可以很容易读出Flash里面的内容。这就让我们的程序和数据暴露无疑，技术得不到保护，很容易被他人盗用或者模仿。
- 恩智浦全新一代LPC系列MCU产品LPC55S69包含一个PRINCE模块，它可以在写进Flash数据的时候进行实时加密，读Flash上的内容时实时解密。这些数据既可以是程序，又可以是密钥等信息。
- 你可以把它看做是Flash控制器上面的加密引擎，一旦使能，PRINCE就会过滤Flash读写路径的数据，并进行实时加解密。



安全开发及配置工具

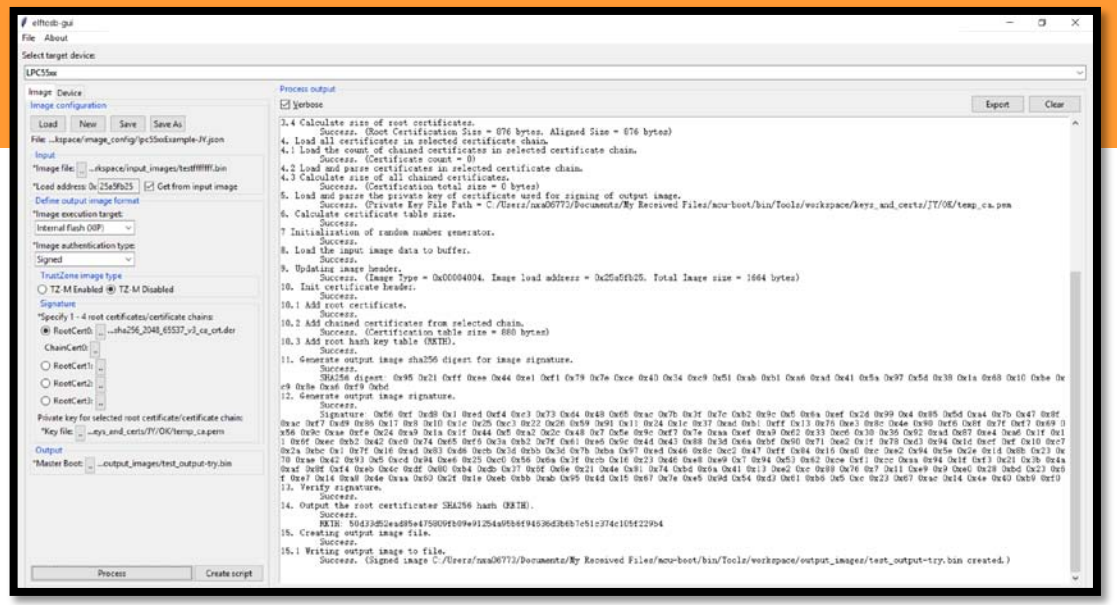
安全应用文档和软件

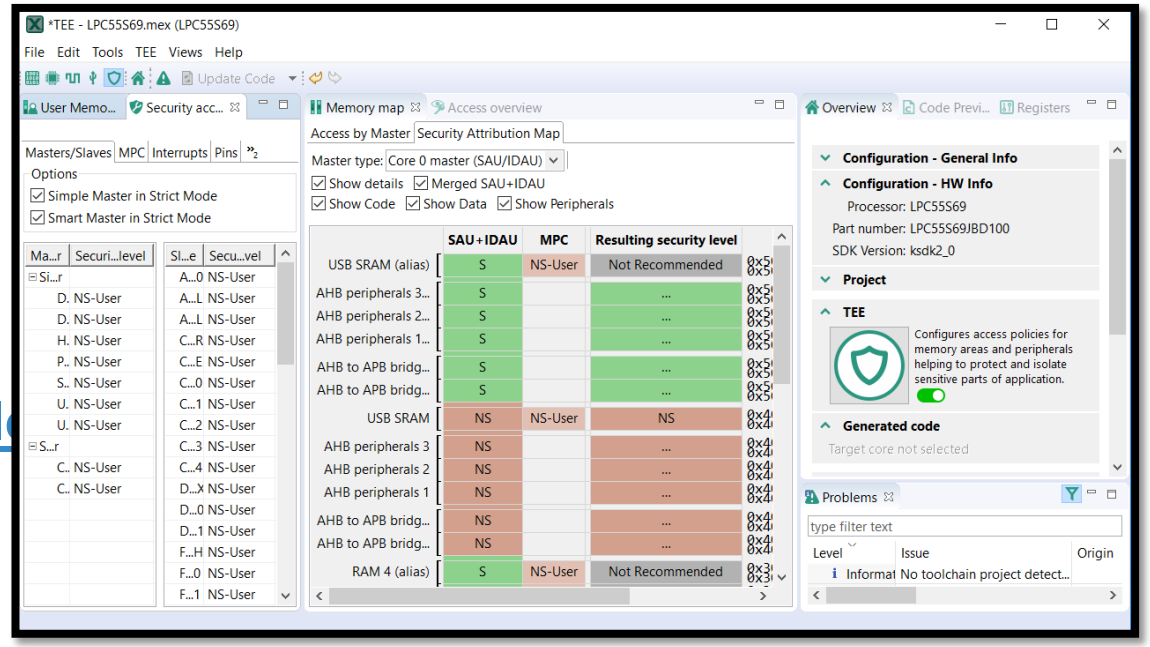
Application Notes	Document Linker	Software Liner
AN12445	Asymmetric Cryptographic Accelerator CASPER	NA
AN12278	LPC55S69 Security Solutions for IoT	NA
AN12324	LPC55Sxx usage of the PUF and Hash Crypt to AES coding	Application note software for AN12324
AN12326	LPC55S6x Secure GPIO and Usage	Application software for AN12326
AN12283	LPC55Sxx Secure Boot	…\SDK_2.6.2_LPCXpresso55S69\middleware\mcu-boot\bin\Tool\elftosb-gui(win).exe

Reference Code	KSDK Position, Request to be selected by downloader when building your SDK
mbedTLS	…\SDK_2.x.x_LPCXpresso55S6x\middleware\mbedtls
Flashloader	…\SDK_2.x.x_LPCXpresso55S6x\middleware\mcu-boot
safeRTOS	https://www.highintegritysystems.com/partners/nxp/
ARM TF-M	…\SDK_2.6.2_LPCXpresso55S6x_MDK\middleware\tfm

安全启动和配置小工具

- **Secure Boot Tool**
  - Part type: LPC55xx, RT6xx, K32W0x
  - Boot type: signed boot, encrypted boot, CRCed boot encrypted XIP boot, encrypted +signed boot
  - Signed/Encrypted/XIP/SB bootable image generation
  - eFuse/OTP/FPR configuration
  - …\SDK_2.6.2_LPCXpresso55S69\middleware\mcu-boot\bin\Tool\elftosb-gui(win).exe
- **TEE Config Tool (CM33 TZ)**
  - Memory (RAM and Flash)
  - Master / Slave IP
  - Interrupt
  - Pins
  - MCUXpresso Config Tools - Pins, Cl… Peripherals

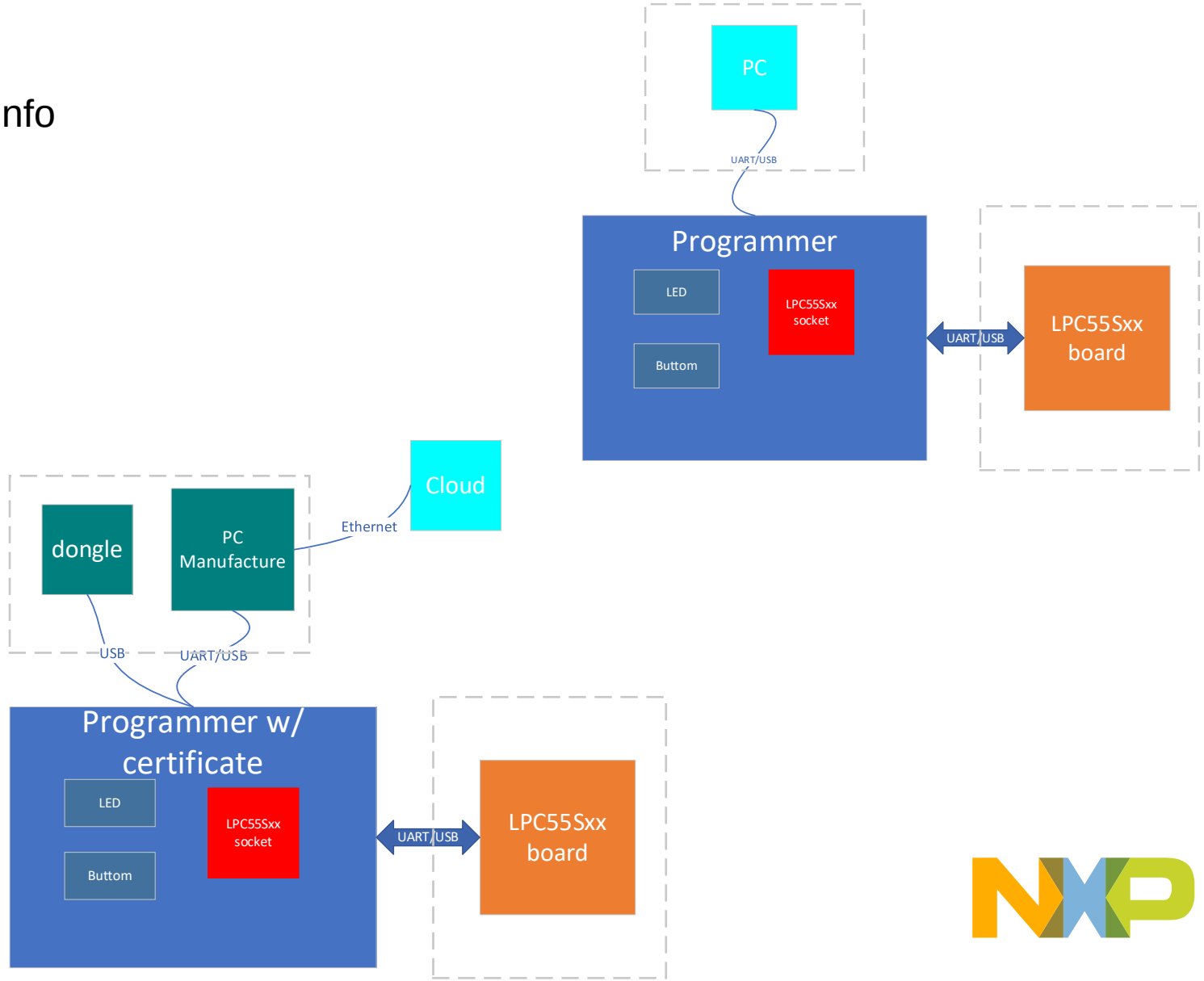




安全编程器

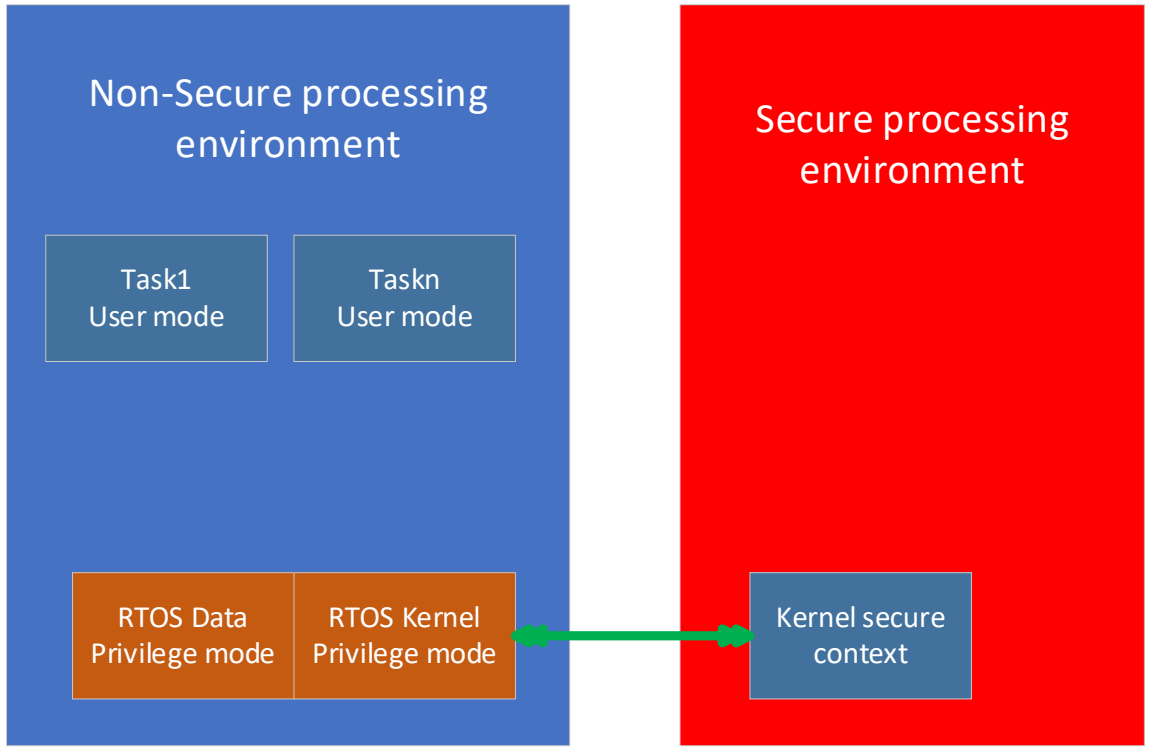
- 通用编程器
  - Program encrypted image/Key/config info
  - Support chip and board programming
  - Programming count

- 具有认证功能的编程器
  - Secure communication
  - Control/protect key by cloud end
  - Support dongle encryption
  - Support chip and board programming
  - Programming count



安全操作系统

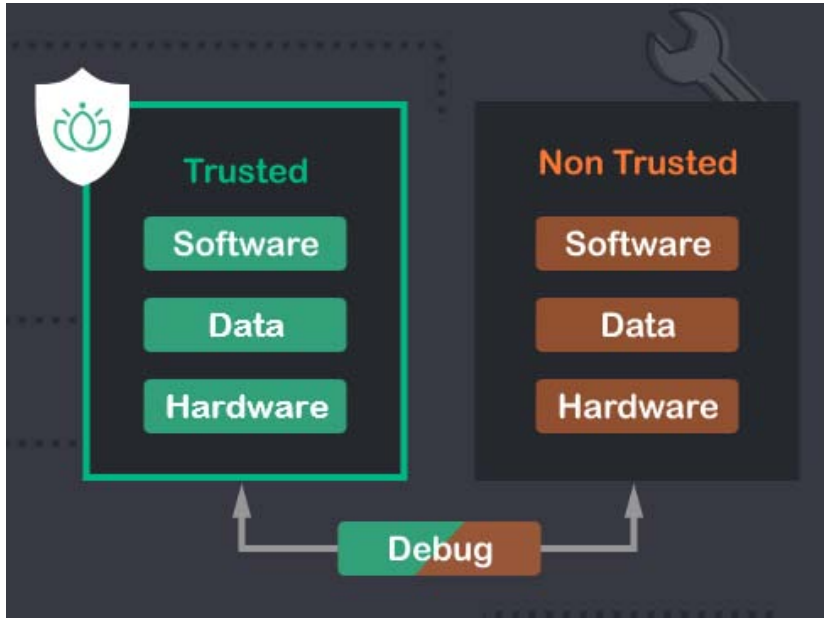
- SafeRTOS
  - Tasks run in Non-secure processing environment
  - Spatial Separation with MMU and Trustzone
  - Key context runs in secure processing environment
  - Demo from https://www.highintegritysystems.com/partners/nxp/



TEE完整解决方案

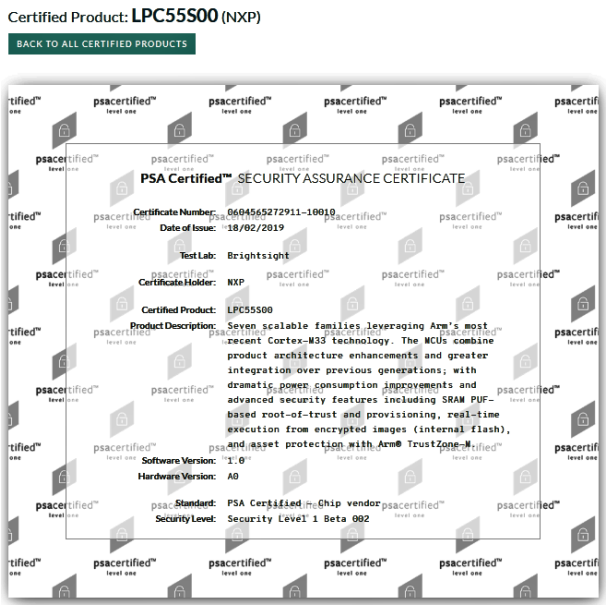
豆荚 Beanpod

青莲云



安全认证

- ARM PSA Certified: building trust in IoT
- SESIP Certified: building trust in IoT
- BCTC Certified: building security in Personal Payment
- TrustedLabs Certified: building trust in IoT/Smart Meter



Certified Product: **LPC55S00** (NXP)

BACK TO ALL CERTIFIED PRODUCTS

PSA Certified™ SECURITY ASSURANCE CERTIFICATE

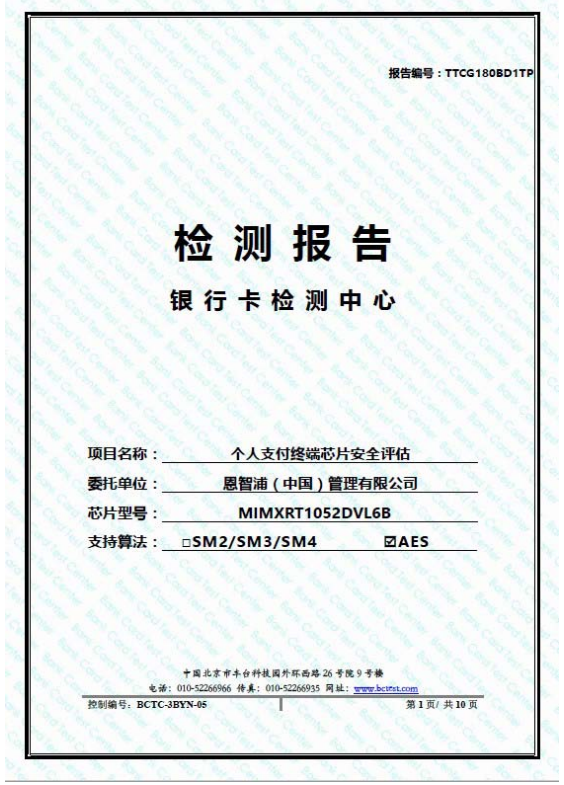
Certificate Number: 0604565272911-10010
Date of Issue: 18/02/2019
Test Lab: Brightsight
Certificate Holder: NXP
Certified Product: LPC55S00
Product Description: Seven scalable families leveraging Arm's most recent Cortex-M33 technology. The MCUs combine product architecture enhancements and greater integration over previous generations; with dramatic power consumption improvements and advanced security features including SRAM PUF-based root-of-trust and provisioning, real-time execution from encrypted images (internal flash), and asset protection with Arm® TrustZone-M.
Software Version: 1.0
Hardware Version: A0
Standard: PSA Certified - Chip vendor
Security Level: Security Level 1 Beta 002

TRUSTCB — TRUST AND VERIFY

Certificate ID: SESIP-1900003-01
TrustCB B.V. declares that
Product: i.MX RT1050/RT1060, version Rev. A and Rev. B
of
Sponsor (and developer): NXP Semiconductors in Hamburg, Germany
complies to the requirements described in the standard and ST
Standard: Common Criteria for Information Technology Security Evaluation (CC) Version 3.1 Revision 5 (ISO/IEC 15408)
ST Reference: i.MX RT1050/RT1060, SESIP Security Target, version 1.1
Summarized:
Assurance Package: SESIP1
Protection Profile: -
As evaluated by:
Evaluation Facility: Brightsight B.V. located in Delft, The Netherlands
Under scheme:
Security Evaluation Scheme for IoT Platforms v1.1
Validity: Date of 1st issuance: 2019-02-27
Date of expiry: 2021-02-26

Wouter Slegers, CEO TrustCB B.V.

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com
Van den Berghlaan 48 | 2132 AT Hoofddorp | The Netherlands



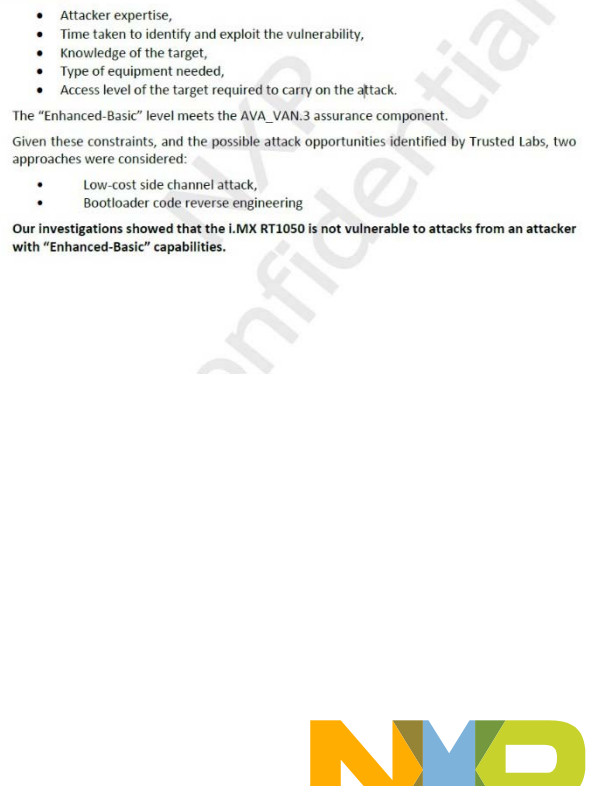
报告编号：TTCG180BD1TP

检 测 报 告

银 行 卡 检 测 中 心

项目名称：个人支付终端芯片安全评估
委托单位：恩智浦（中国）管理有限公司
芯片型号：MIMXRT1052DVL6B
支持算法：□SM2/SM3/SM4 ☑AES

中国北京市丰台科技园外环西路26号院9号楼
电话：010-52266966 传真：010-52266935 网址：www.bctest.com
控制编号：BCTC-3BYN-05 第1页/共10页



This document describes a complementary security assessment to [TLA_IMXRT] conducted on the i.MX RT1050, and targeting the IoT market in general, whereas the initial assessment focused on the Smart Metering market.

Trusted Labs considered in the assessment attacks compatible with the targeted security level of the i.MX RT1050. NXP has designed the i.MX RT family to be used for highly critical security applications in conjunction with more dedicated security technologies (e.g. Secure Element).

Thus, Trusted Labs analyzed potential attack paths, and cover attacks in the range of an "Enhanced-Basic" attacker profile, which is consistent for the use case described by NXP.

The [CEM] documentation details how the definition of the attacker profile is constructed, taking into account:

- Attacker expertise,
- Time taken to identify and exploit the vulnerability,
- Knowledge of the target,
- Type of equipment needed,
- Access level of the target required to carry on the attack.

The "Enhanced-Basic" level meets the AVA_VAN.3 assurance component.

Given these constraints, and the possible attack opportunities identified by Trusted Labs, two approaches were considered:

- Low-cost side channel attack,
- Bootloader code reverse engineering

Our investigations showed that the i.MX RT1050 is not vulnerable to attacks from an attacker with "Enhanced-Basic" capabilities.

NXP Confidential

安全技术相关文章与视频

SECURE CONNECTIONS
FOR A SMARTER WORLD