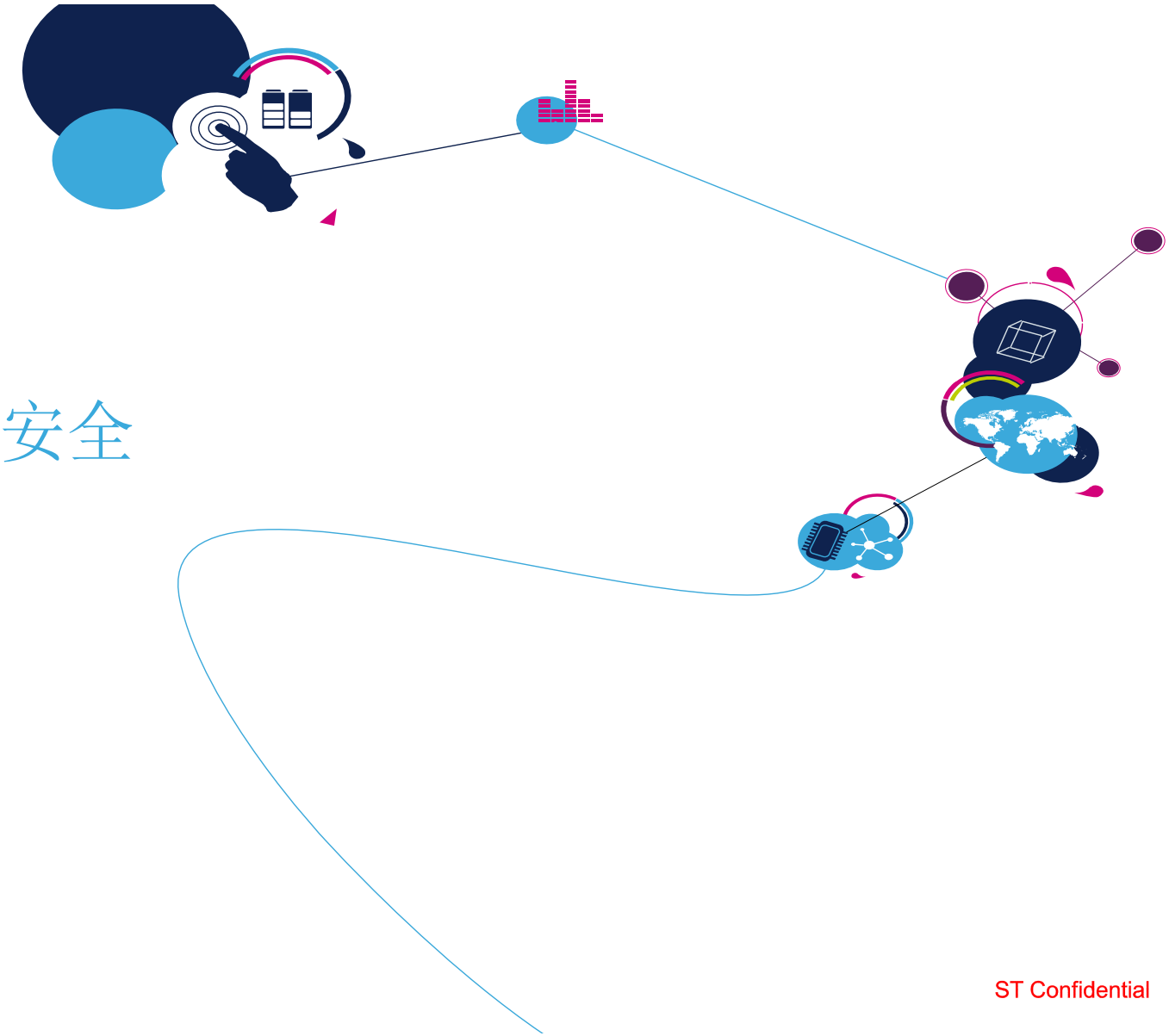


STM32 与 物联安全

STM32 and IoT **Security**

life.augmented

什么是物联安全？

没有安全保障的物联网，
就像驾驶没有安全气囊的汽车一样：

它的价值只有当交通事故发生时
才能体现出来……

但是这已经太迟了！

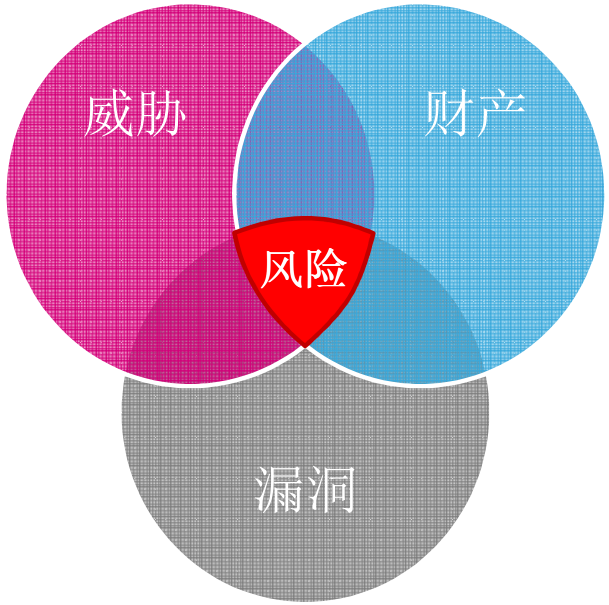
life.augmented

什么是物联安全？

保障物联安全，必须在产品生命周期的早期入手

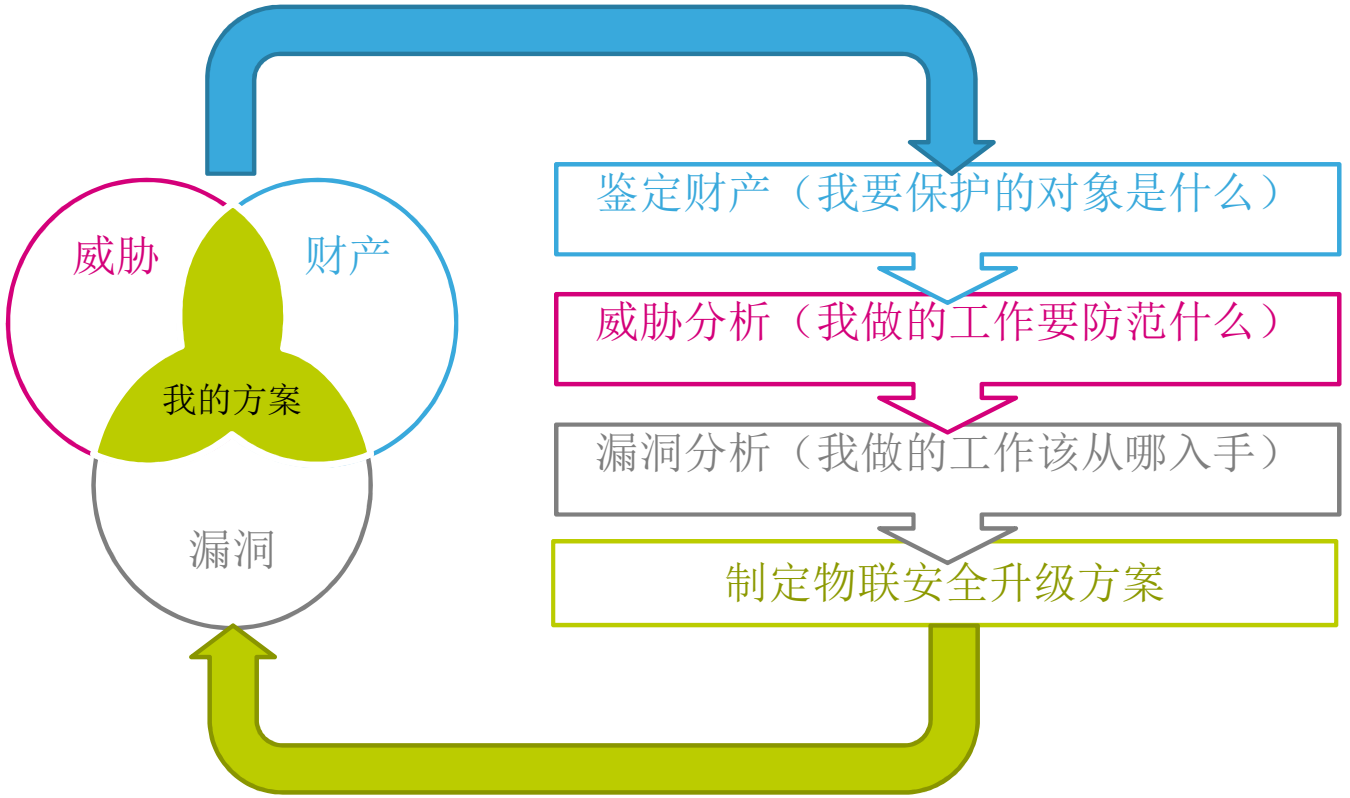
鉴别什么是构成**风险**的三要素

财产，威胁，漏洞



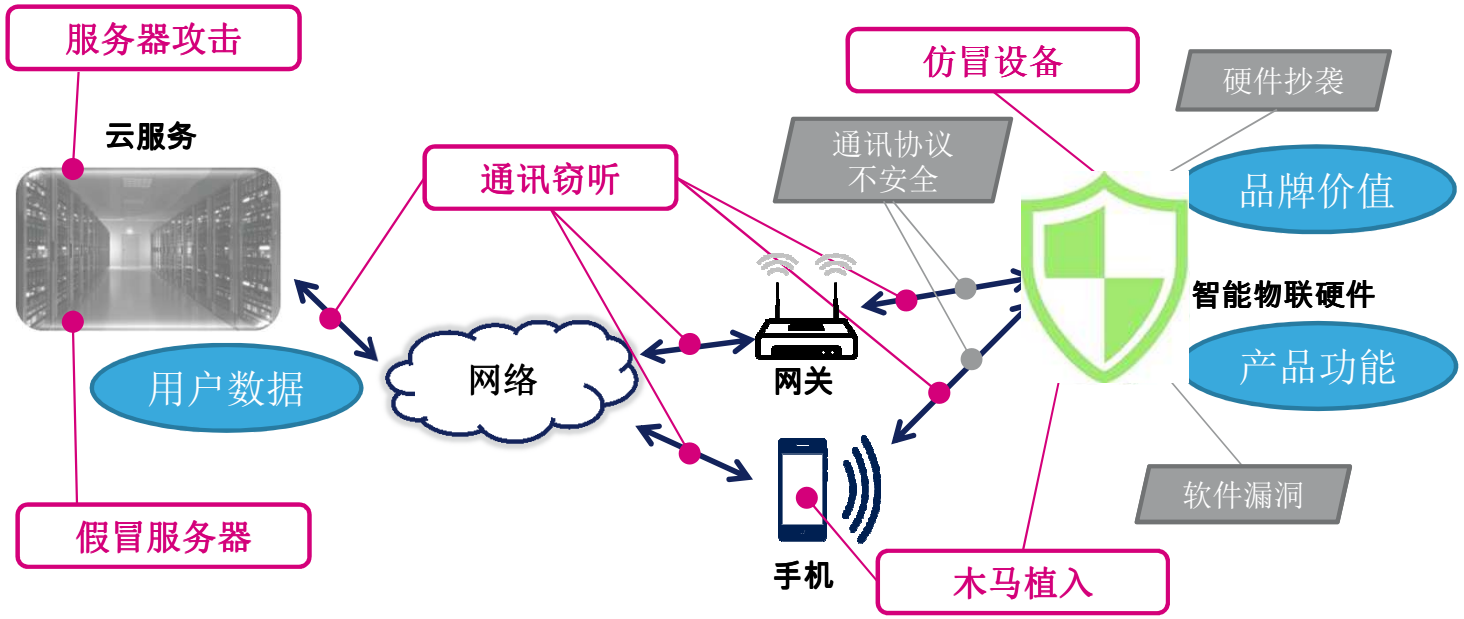
物联安全风险在哪里？

当财产，威胁与漏洞并存时，风险就会存在



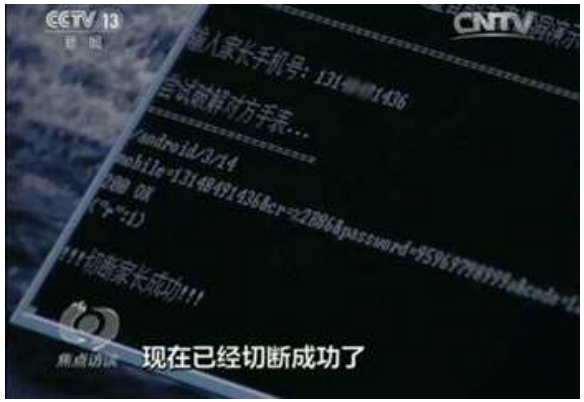
物联安全风险在哪里？

当智能硬件联网时，威胁其实无处不在



物联安全风险在哪里？

物联安全风险其实已经严重影响着我们的生活



Researcher finds huge security flaws in Bluetooth locks

You might want to rethink adding technology to your front door.

Roberto Baldwin , @strngwys
08.10.16 in Security

17 Comments

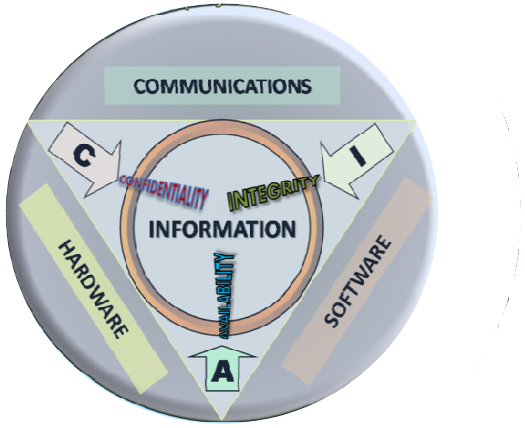
1483 Shares

life.augmented

如何实现物联安全？

信息安全的三大要素（ CIA ）

- 机密性（Confidentiality）
  - 是一种所有权概念，机密信息是不可以对未授权的个人，实体或过程开放或披露的。(摘自ISO27000).
  - 常用方法：加密，动态密钥管理
- 完整性（Integrity）
  - 是指保持和保证数据在其完整有效期内的准确和圆满。这意味着数据不可以被未授权或未被发现的方式所修改。
  - 常用方法：签名认证
- 可用性（Availability）
  - 是指信息必须在它被需要的时候保持对合法对象可用。这意味着在系统存储和处理着每一条信息的过程中，安全机制用于保护这些信息，而通讯渠道必须通过正确的方式存取这些信息。
  - 常用方法：密钥安全传送与存储，设置权限



life.augmented

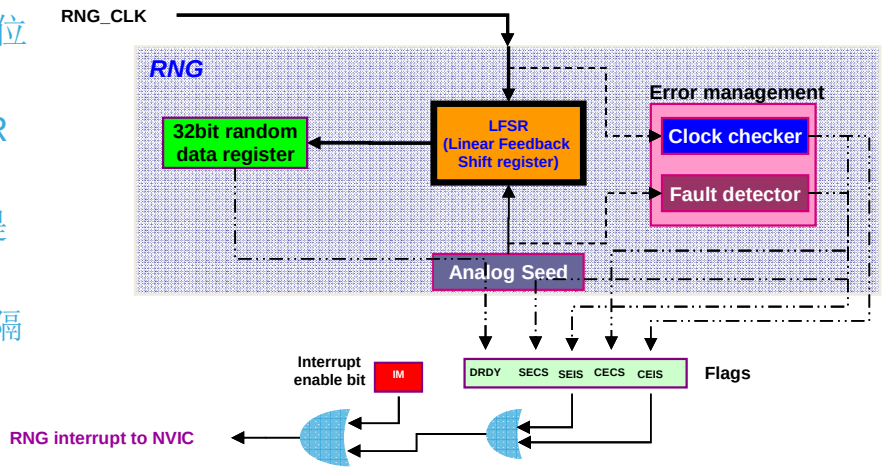
STM32的数据加密与认证

STM32提供一整套硬件和软件的加解密相关功能

功 能			用途
加解密相关 (Crypto)	RNG	软件	片上熵产生。确保强度高的密钥， 防止回放攻击。
		硬件	完全由硬件产生32位真随机数。
	Hash& HMAC	软件	Hash 算法提供了方法来保证信息完整性以及验证数字签名以及消息认证码(MAC). MD5, SHA-1, SHA-224, SHA-256
		硬件	SHA-1, SHA-224, SHA-256 和 MD5
	对称密码	软件	STM32 密码库: ▪ DES/TDES: ECB, CBC. ▪ AES: ECB, CBC, CTR, CCM, CBC-MAC, GCM, CMAC, KEY WRAP
		硬件	DES/TDES:ECB, CBC, 56位密钥 (STM32H7)
			AES 128bit (ECB, CBC,CTR)
			AES 128-256bit (ECB, CBC, CTR, GCM, GMAC, CMAC)
	非对称密码	软件	▪ RSA 符合PKCS#1v1.5的签名函数 ▪ ECC (椭圆曲线密码) 密钥生成, 点乘(ECDH)，ECDSA.

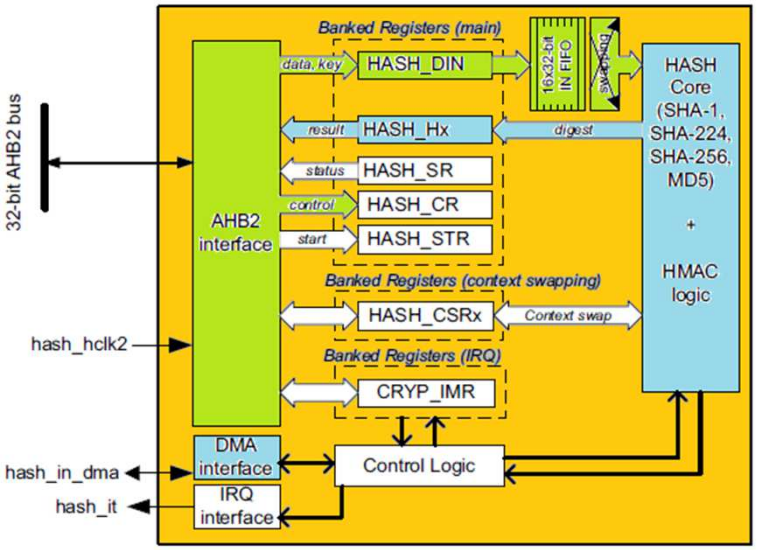
STM32的数据加密与认证

- 硬件真随机数发生器
  - 基于无规律的模拟噪音源产生32位随机数
  - 再经过线性反馈移位寄存器LFSR产生随机序列
  - 由独立PLL时钟源 (PLL48CLK)提供时钟
  - 每两个连续产生的随机数间需间隔40个时钟周期
  - 5 个标志位
    - 1个代表合格随机数就绪.
    - 2个代表模拟噪音源异常时序超过连续64位拥有相同值或连续32位间隔0和1
    - 2 个代表频率异常 PLL48CLK 时钟过慢



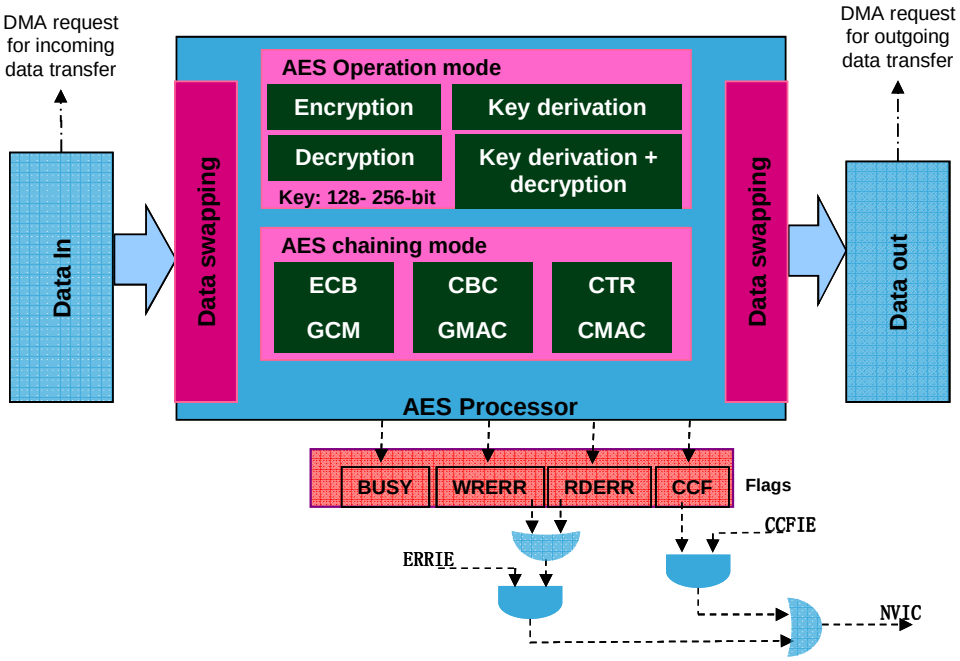
STM32的数据加密与认证

- 硬件哈希模块
  - 运算模式：
    - SHA-1
    - SHA-224, SHA-256
    - MD5
    - HMAC
- 应用场景
  - 散列函数值可以说是对明文的一种“指纹”或是“摘要”，所以对散列值的数字签名就可以视为对此明文的数字签名。
  - 安全散列算法主要适用于数字签名标准（Digital Signature Standard DSS）里面定义的数字签名算法（Digital Signature Algorithm DSA）。



STM32的数据加密与认证

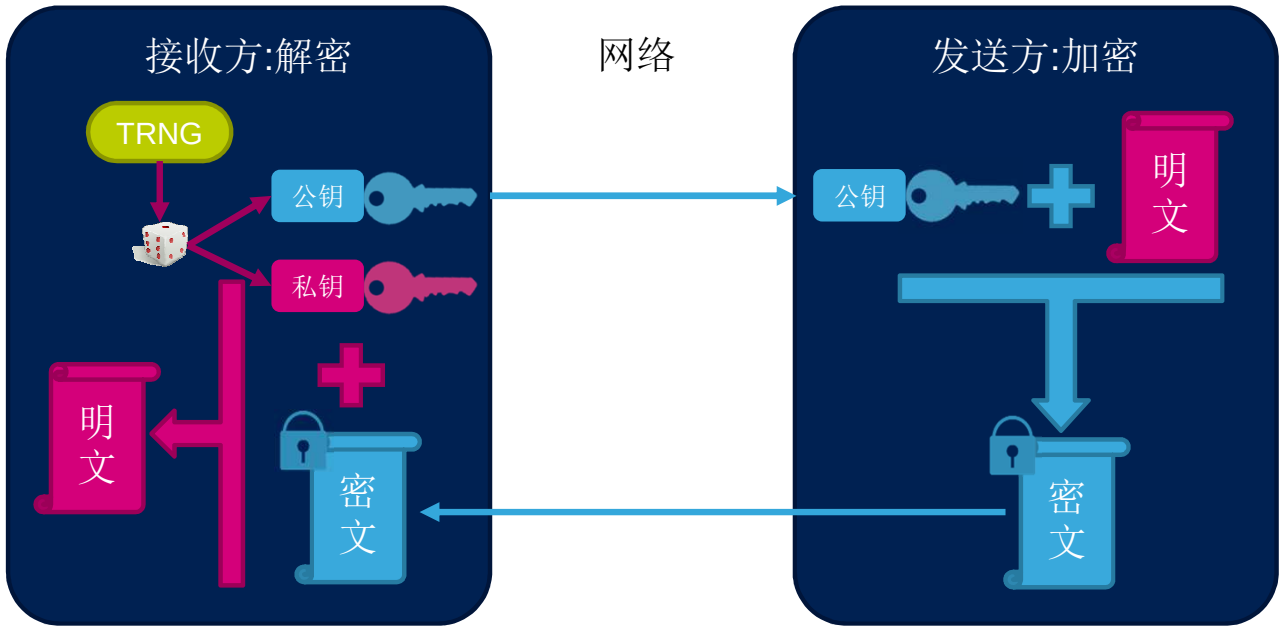
- 硬件AES模块（NIST FIPS 197）
  - 运算模式:
    - 加密
    - 密钥派生
    - 解密
    - 密钥派生+解密
  - 支持128位，192位和256位密钥
  - 128位数据块处理
  - 数据交换逻辑支持1-, 8-, 16- or 32-位
  - 当有优先级更高的消息，正在处理的消息可被打断。
  - 支持DMA
- 应用场景:
  - 加密透传，无线通讯，加密存储，电子商务等



STM32的数据加密与认证

通讯数据的加密

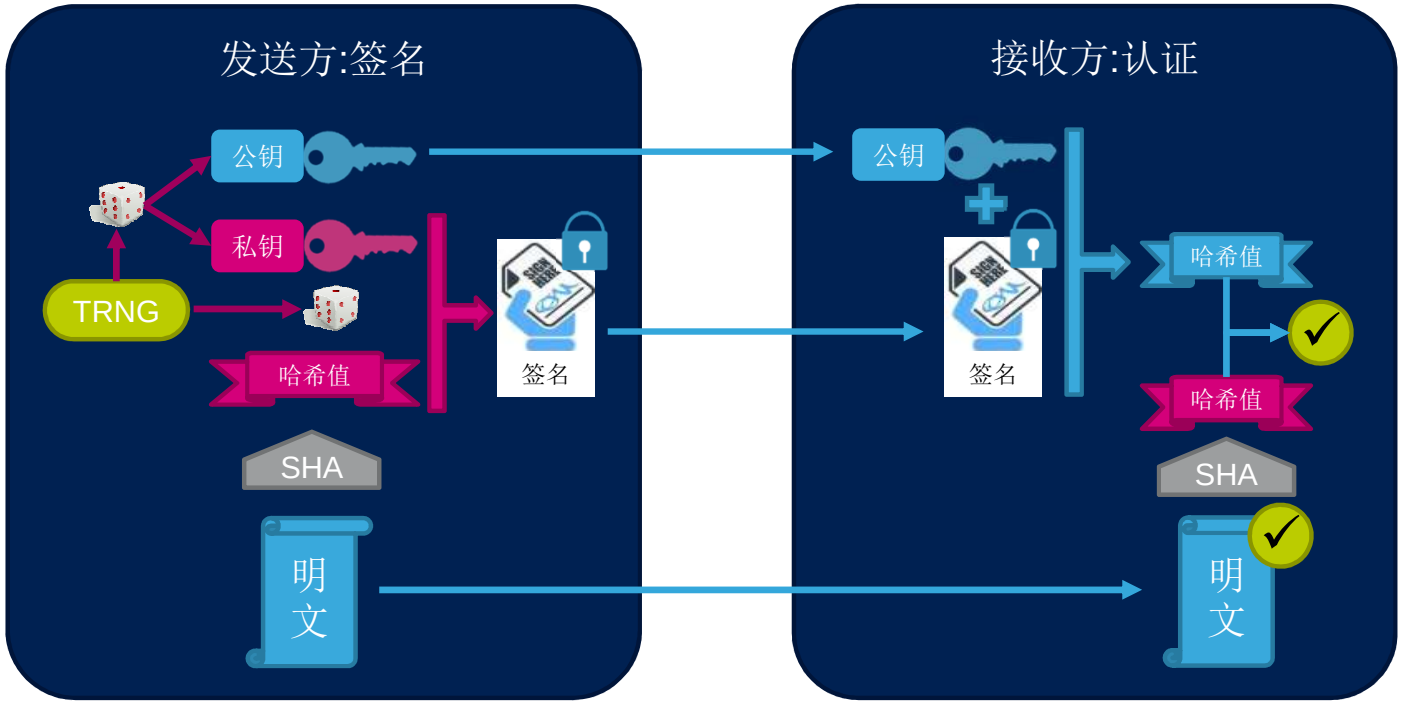
- 非对称加密（公开密钥加密）
  - 可防止密钥通过不安全的途径传播而失去安全性
  - 常见方法：RSA 和 ECC 椭圆曲线密码



STM32的数据加密与认证

通讯数据的签名认证流程

- 非对称加密的另一种常见用法是签名认证
  - 用于认证文件的来源及内容真实可信



STM32的数据加密与认证

- STM32 芯片唯一编码 （UID）
  - ST工厂内预置了唯一设备鉴定码（超值系列产品除外）
  - 对带有该UID的MCU能做到全球唯一性
  - ST的编码规则保证了该编码在几十年内都不会有重复
- 这个唯一编码可用于：
  - 使用算法产生产品序列号
  - 与加密机制使用产生绑定芯片的操作，或用于增强安全性（生成密钥）
  - 在启动引导阶段用于设备签名

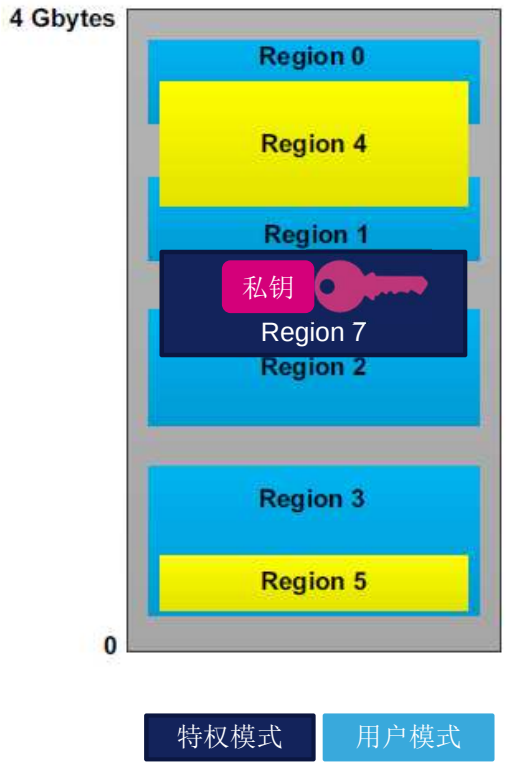
STM32的数据存储与隔离

密钥的管理和保存

- 所有的数据加密和签名认证都依赖于密钥的安全性（尤其是私钥）
- 密钥的管理和保存有哪些方法？
  - 存储器保护单元（MPU）
  - STM32 防火墙（Fire Wall）
  - 私有代码读取保护（PCROP）
  - STM32 读保护 （RDP）

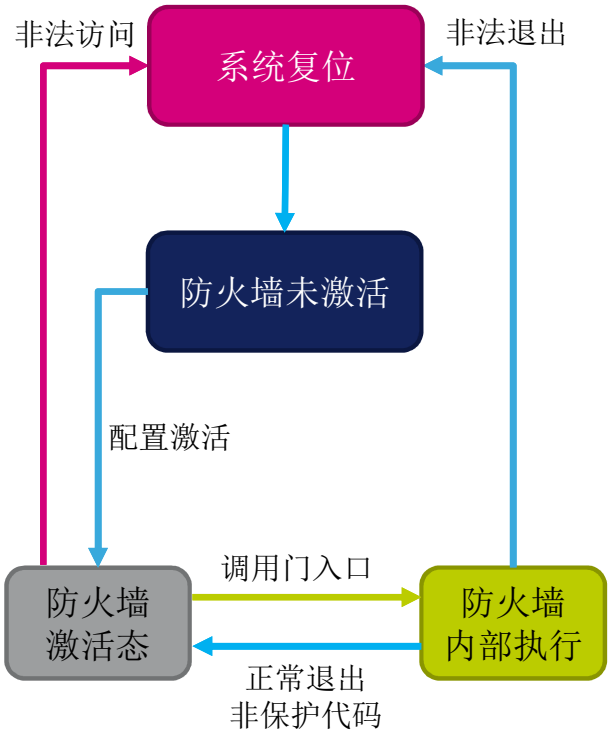
STM32的数据存储与隔离

- 存储器保护单元（Memory Protection Unit）
  - 按区域根据设置的参数进行存储区保护
    - 8个存储区保护区域
    - Region 0优先级最低，Region 7最高
    - Region间可重叠
  - 可设置每个区域对更高或更低优先级（管理员和用户模式）的权限：
    - 只读、读写、只执行或不可访问
  - 如果有非法访问，内核就会产生硬件错误或者锁定
- 如果将密钥放置在设置管理员权限的高优先级区域，并配置其对用户模式不可访问，则所有用户权限区域程序将无法访问密钥。



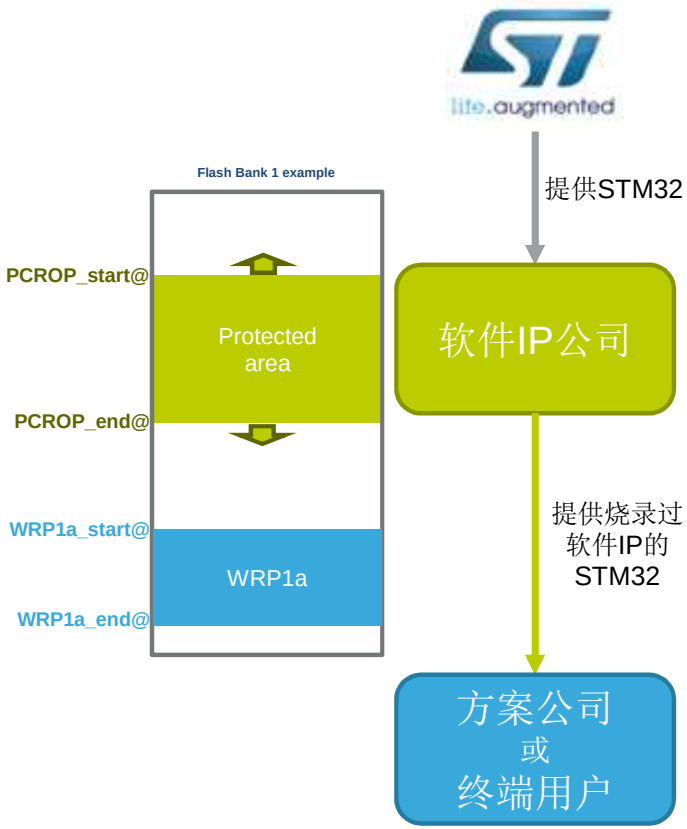
STM32的数据存储与隔离

- 防火墙（Firewall）
  - 对位于Flash或SRAM中的一段敏感数据或代码，构建一个与其它代码隔离的“可信任”存储区域
    - 设置起始地址和长度
  - 当需要使用这个代码或数据时，可从一个唯一的**调用门**进入防火墙，通过从其他任何位置访问防火墙内部，包括DMA和中断侵入，都会导致**系统复位**
- 适用于保护独立于应用的算法，或者有关于安全的敏感操作（例如加解密运算）
  - 启动配置完成后一直保持有效，直到下次系统复位



STM32的数据存储与隔离

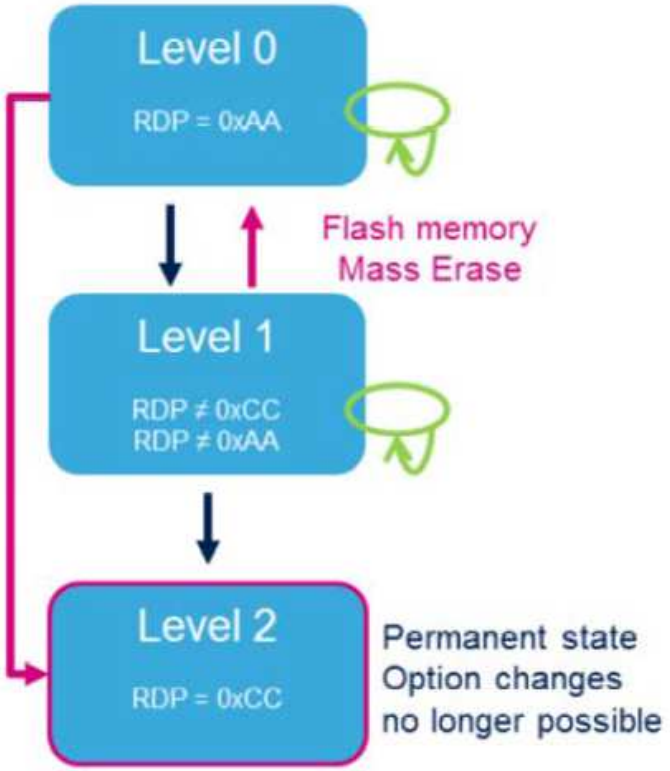
- 私有代码读取保护（PCROP）
  - 基于仅执行(Execute-only)机制的保护措施
    - 受保护代码仅能被执行
    - 受保护代码不能被任何方式读取
    - PCROP可同时提供写保护
    - 执行整片擦除时该区域也可以被保留*
- 可防止软件IP或数据密钥被不可信的第三方窃取，即使系统被入侵后，被保护区域仍可防范被恶意软件窃取。
  - PCROP设置后仅可在解除RDP时被清除，同时会触发整片Flash擦除。



*：部分产品

STM32的数据存储与隔离

- 读出保护（RDP）
  - Level 0 / RDP=0xAA
    - Option byte 允许被更改
    - 可被设置到Level 1和Level 2
  - Level 1 / RDP!=(0xAA|0xCC)
    - Option byte 允许被更改
    - 当被设置回Level 0时，用户程序、备份寄存器、备份SRAM的内容将被清空
    - 可被设置到永久保护Level 2
  - Level 2 / RDP=0xCC
    - Option byte 被冻结
    - 该设置不可逆



STM32的数据存储与隔离

- 读出保护（RDP）的访问权限

区域		读保护等级 (RDP)	从用户程序启动	从SRAM或系统程序启动 或 检测到调试模式
Flash区域	用户程序	1	R/W/E	No Access
		2	R/W/E	-
	系统程序ROM	1	R	R
		2	R	-
	Option bytes	1	R/W/E	R/W/E
		2	R	-
	OTP	1	R/W	No Access
		2	R/W	-
	备份SRAM和 备份寄存器	1	R/W	No Access
		2	R/W	-

R：可读、W：可写、E：可擦除

STM32的硬件安全设计

STM32硬件安全配置表

STM32 系列	安全相关的功能																	
	Debug Port	RESET Register	FLASH WRP	FLASH Mass ERASE	Tamper Pins	CRC Hardware	96-Bit Unique ID	Crypto Library Support	MPU	FLASH RDP Lv2	TRNG	AES Hardware Accelerator	FLASH PCROP	HASH Hardware Accelerator	Firewall	SRAM RDP	Sys Clock (MHz)	ARM Cortex®
STM32 **F1**	■	■	■	■	■	■	■	■	■								72	**M3**
STM32 **F3**	■	■	■	■	■	■	■	■	■	■							72	**M4**
STM32 **F0**	■	■	■	■	■	■	■	■		■							48	**M0**
STM32 **L1**	■	■	■	■	■	■	■	■	■	■	■	■	■				32	**M3**
STM32 **F2**	■	■	■	■	■	■	■	■	■	■	■	■		■			120	**M3**
STM32 **F4**	■	■	■	■	■	■	■	■	■	■	■	■	■	■			180	**M4**
STM32 **F7**	■	■	■	■	■	■	■	■	■	■	■	■	■	■			216	**M7**
STM32 **L0**	■	■	■	■	■	■	■	■	■	■	■	■	■		■		32	**M0+**
STM32 **L4**	■	■	■	■	■	■	■	■	■	■	■	■	■		■	■	80	**M4**
STM32 **H7**	■	■	■	■	■	■	■	■	■	■	■	■	■	■			400	**M7**

Application Note# (AN)/User Manual# (UM)/Reference Manual#(RM) (www.st.com/mcu) (*infocenter.arm.com)

life.augmented

Thank You!

life.augmented