构建基于MCU安全物联网系统

中国软件行业协会嵌入式系统分会 何小庆

面对增长迅速、应用碎片化的物联网系统，安全问题层出不穷。安全是物联网发展的一个热点，已成为物联网产品必备特性。基于MCU的物联网设备多数在节点和边缘，支撑了系统的数据采集和控制，重要性不言而喻。因为系统资源防护能力薄弱，成为黑客的主要攻击对象。可喜的是，基于MCU的IoT芯片的安全机制越来越完善，功能也大幅度增强，技术上正在从外置芯片向MCU内置安全功能的方向发展。

物联网安全旨在保护代码/数据和系统功能

物联网设备与应用虽然多种多样，但其架构本质上与嵌入式系统架构是相似的。今天，使用微控制器（MCU）构建的物联网系统无处不在。安全性首先要保护嵌入式固件不被非法复制或者篡改，设备数据不被盗取以及系统功能安全，即系统功能应稳健可靠。

在物联网世界中，攻击是现实存在的，攻击的本质是黑客利用系统漏洞来访问资产。防止黑客攻击是物联网安全的重要任务。对于环境检测警报设备或监控摄像机等物联网设备而言，拒绝服务攻击（DoS攻击）是一个主要威胁。攻击者希望通过成功的尝试获得经济收益，特别是如果攻击可以像物联网环境那样大规模地传播。联网设备对黑客非常有吸引力，因为它们可以远程访问。联网设备因为协议漏洞提供攻击机会，如果攻击成功，单个被黑客攻击的设备可能会危及整个网络的完整性。

物联网安全旨在保护代码、数据和系统功能。代码保护是保证固件知识产权及其完整性，数据保护（包括加密密钥）是保证用户数据的机密性并避免身份盗用。随着物联网设备访问云资源的数量倍增，设备的访问控制管理变得越发重要，物联网设备资产变得更加敏感。这里资产可以包括传感器数据（健康数据和位置信息）、用户数据（账号和密码）、交易记录和密钥，以及设备和用户身份等。最后，系统功能安全应受到保护，以避免设备故障或服务故障。

四项技术构建安全的物联网架构

构建安全物联网架构是为了应对多种形式的攻击，这样的系统架构必须在单个系统中实现多种类型的安全机制，应在设备硬件和软件应用两个方面考虑整体安全性。

一方面，如果设备没有外部入侵保护（例如开放了调试端口），则无法为机密应用程序运行提供可信计算环境。另一方面，如果设备没有抵御黑客通过应用攻击设备的能力，或者它允许进行完全设备访问，强大的设备自身保护也是无用的。完整的系统安全实现涉及设备保护机制以及一系列稳健性的安全应用，保护机制必须有必要的硬件支撑，还需要在固件开发方面付出巨大努力。它需要良好的软件技能和密码学知识，同时必须权衡开发成本和设备安全，以下是构建物联网安全架构几个关键技术。

一是TrustZone技术。Arm的TrustZone技术在智能手机芯片中被大量采用，为手机安全提供基础保障。今天许多MCU芯片已经在使用基于Trust Zone的IP核，比如Arm Cortex M23/M33，它们内置了TrustZone技术，量产的MCU有Microchip SAM L11、NuMicro M2351、NXP LPC5500和STM32L5系列。

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。为了区分和隔离安全代码，基于TrustZone技术的MCU存储器被分在了不同的区域，每一个区域都由硬件来保护不受软件攻击，任何从非安全区域向安全区域的访问，或者运行的代码和当前的系统安全状态不符，都会导致硬件错误发生。

围绕TrustZone核心技术，Arm联合5家独立安全测试实验室及咨询机构，推出面向IoT安全的“平台安全架构（PSA）”以及相关认证。PSA安全认证有三个级别，不同的认证过程和要求对应被认证产品不同的应用场景。国产芯片公司也在快速跟进TrustZone技术，紫光展锐最近推出基于PSA架构的双核Arm Cortex M33安全MCU。

使用TrustZone的优势是方便建立一个物联网安全生态环境。考虑到自主可控，以及物联网系统中信任硬件（SE）重要性，国内芯片企业在RISC-V开放指令集架构上开发类似安全技术，比如平头哥半导体最近推出的无剑安全平台。

二是安全通信技术。通信安全是物联网系统的重要部分，许多高端的嵌入式系统中已经有了SSL/TLS/SSH和IPSec协议软件，某些云计算服务需要安全的协议支持，比如AWS IoT需要物联网设备端支持TLS，否则无法正常接入。有些资源受限的基于MCU物联网设备无法支持基于TCP的TLS 安全协议，采用UDP的DLS可以提供安全通信链路，云端需要提供响应的接口，比如为Huawei LiteOS和华为OceanConnect IoT提供支持。

安全协议为构建物联网安全提供一个非常好的基础，安全协议的设计目标是为了防止数据报文被窃听（嗅探）、中间人攻击、回放攻击和未经授权与物联网节点通信的请求。

三是安全引导和升级技术。安全引导可以防止在引导过程中将没有授权的软件加载到设备上。安全引导一般分为两个阶段。第一个阶段是放在只读的存储器中，该阶段引导的主要任务是验证第二阶段引导的程序的真实性。第二个阶段引导程序是放在FLASH存储器中，它要验证加载的操作系统和应用程序确实来自可信的来源。

安全引导过程一般要靠数字签名来保护代码的真实性。代码的映像由OEM在设备制造时使用自己的私钥进行签名，然后设备节点使用OEM的公钥来验证代码映像签名。

安全固件升级过程与引导类似，在升级过程中要验证新代码的映像已经是由OEM签名了的。如果验证无效，系统就会丢弃文件并停止升级。只有有效的映像文件才能被接受，而且随后被保存到设备存储器中。

以智能门锁为例，我们看一下升级中的两种安全隐患。第一是智能门锁自身的可靠性，第二是来自对智能门锁的外部攻击。门锁自身的可靠性，比如在升级过程中设备电源掉电了，使得更新后的程序代码无法运行。外部攻击，比如黑客发送早期有缺陷的OTA 升级包，此外还有黑客对于门锁电子部件的物理攻击，比如盗取存储器中的密钥。

物联网操作系统，比如Amazon FreeRTOS与基于云的AWS IoT平台，提供设备管理和远程监测，设备管理服务包括对OTA更新的支持。它利用AWS内置的服务，比如亚马逊用于代码签名的Certificate Management和身份访问管理（IAM）。Amazon FreeRTOS嵌入式软件提供在MCU上执行的OTA代理，协调OTA操作，从云端下载新升级包，验证升级包并处理在下载期间的任何中断。这个升级包的传输借助加密的MQTT通信链路，OTA代理机构为满足MQTT报文格式要求，要对升级包再次封装，好处是不需要另外借助HTTP连接上的TLS 链路。

四是安全工具、软件和服务。基于MCU的物联网安全开发需要软件和工具的支持和服务，MCU公司提供基础安全软件，比如NXP Secure Boot Tool和TEE 配置工具。许多物联网操作系统集成了安全协议，多数支持安全的OTA机制。新出的TencentOS tiny安全框架提供了DTLS和TLS安全协议，加固了COAP及MQTT传输层，可确保物联网终端在对接腾讯云时实现安全认证和数据加密；安全框架还提供与腾讯云IoT Hub配套的密钥认证方案，确保资源受限设备也能在一定程度上实现设备安全认证。

安全操作系统方面，NXP推荐源自FreeRTOS的SafeRTOS，ST与Arm和安全操作系统供应商Prove & Run合作，于2019年10月在Arm TechCon上进行了STM32L5的演示。NXP的LPC55S69-EVK评估板支持MCUXpresso集成开发环境和开发软件，包括外设驱动程序、安全和连接中间件，还包括基于Amazon FreeRTOS的演示和基于Arm TrustZone的安全示例。嵌入式MCU软件工具公司IAR 推出安全IoT设备生命周期管理工具Embedded Trust，Segger公司提供安全编程设备，这些为基于MCU物联网系统安全开发和维护提供了坚实的基础。

中国企业在物联网安全服务上颇具特色，近期360北极星团队、梆梆安全和纽创信安介绍了他们的安全服务和解决方案。从事移动安全的企业也在转向物联网领域，比如国民技术32位高性能安全MCU芯片已经在和阿里IoT云以及中移物联网合作。

物联网安全与行业应用密切相关，某些应用是物联网安全高危区，比如智能家居、网联汽车、智慧城市、智能制造和智慧医疗，物联网上的潜在威胁既可谋财害命，也可对国民经济和生活造成重大危机，这些均需引起企业和主管单位的高度重视。

2019安全型MCU优秀（产品）解决方案奖
瑞萨电子RA6系列MCU

瑞萨电子RA6系列采用Arm Cortex-M4广泛满足从32引脚到176引脚、从256KB到2MB闪存的市场需求。在安全性能上，RA MCU系列基于Arm v8-M TrustZone技术，将其安全加密引擎（SEC）IP与NIST CAVP认证相结合，可为客户带来物联网安全性的同时，还提供篡改检测功能并增强了对侧信道攻击的抵抗力。RA MCU也融合了基于硬件的安全功能。Secure Crypto Engine（安全加密引擎）提供对称与非对称的加密/解密、哈希函数、真随机数发生器（TRNG）和高级密钥处理，包括密钥生成和MCU相关的唯一性密钥封装。如用户未遵循正确的访问协议，访问管理电路将关闭加密引擎内置专用RAM，能确保明文密钥永远不会暴露在任何CPU或外设总线上。

2019智能制造MCU优秀（产品）解决方案奖
赛普拉斯PSoC6 BLE

PSoC6 BLE不但集成物联网/可穿戴设备中的模拟前端、BLE、显示及系统控制等功能，通过可编程模块，用户可灵活定义数字/模拟外设。芯片内部集成领先的电容触控Capsense及智能语音交互I2S/PDM-PCM等特性，可开发出各种强大可靠的基于触控感应和手势控制的用户交互界面。专有的超低功耗40nm SONOS处理技术使PSoC 6 MCU架构能够在Cortex-M4和Cortex-M0+内核上分别以22μA/MHz和15μA/MHz工作电流实现业界领先的功耗水平。此外双核架构为了提高功率效率，可将Cortex-M0+用作待机监测引擎，支持Cortex-M4主内核进入睡眠模式。

支持可信应用的硬件隔离执行环境TEE和硬件加速加密SE操作，将安全元素功能与隔离的加密操作和隔离密钥存储相结合。此外，提供多个加密环境如AES、3DES、RSA、ECC、SHA-512、SHA-256以及真随机数生成器（TRNG）等，不需额外的外部存储或者安全单元即可支持多个同步安全环境。

2019智能家居MCU优秀（产品）解决方案奖
芯科科技Wireless Gecko Series 2

芯科科技Series 2 EFR32MG21和EFR32BG21 SoC是线路供电的物联网产品的理想解决方案，适用于各种智能家居、商业和工业物联网应用。新型xGM210x模块能够为从智能LED照明到家庭和工业自动化的应用提供一站式无线解决方案，改进有线供电物联网系统中的网状网络性能。xGM210L模块可为成本敏感、大批量生产的智能LED灯泡带来完美无线解决方案；xGM210P模块可简化智能照明、HVAC、建筑和工厂自动化系统等空间受限的物联网设计。

Series 2的首批产品是小尺寸SoC器件，具有专用的安全内核和片上无线电，和竞争解决方案相比，可提供2.5倍无线覆盖范围。这些SoC包括支持多协议、Zigbee、Thread和Bluetooth网状网络的EFR32MG21 SoC，以及专用于低功耗蓝牙和蓝牙网状网络的EFR32BG21 SoC。

2019智能汽车MCU优秀（产品）解决方案奖
瑞萨电子RH850/U2A

RH850/U2A采用28纳米制程工艺，32位MCU，配备多达4组采用双核锁步结构、高达400MHz主频的CPU核，每个CPU核都集成了基于硬件的虚拟化辅助功能，同时保持了RH850系列一贯的高速实时性能。支持ASIL D，满足不同ISO26262功能安全级别的多个软件系统在高性能模式下独立运行而免受干扰，同时可降低虚拟化所需的资源占用，以维持实时性，这使客户能够将多个ECU功能集成到单个ECU中，同时保持功能安全、网络安全，以及实时操作要求。结合了高性能、片上安全性能和网联性能的cross-domain、RH850/U2A MCU可广泛应用于包括车身、底盘/安全、域控制和中低端网关等领域。

MCU：“芯”机遇，新挑战

成都锐成芯微科技股份有限公司
CEO向建军

MCU是集成电路中最激发创意和设计灵感的核心元器件。它拥有完整的运算、存储、感知、通信、人机交互等组件，基于具体应用完成功能的配置和调用，即可满足各种各样需求场景的差异化需要。我们现实生活中遇到的每款电子产品里面，都或多或少有MCU身影。

MCU，麻雀虽小五脏俱全

MCU（Micro control unit）即微控制器，国内形象的称之为单片机，是伴随着集成电路同步发展起来的一个产品分支。自20世纪70年代中期，由Intel公司首先推出4bit微处理器以来，已历经8bit、16bit、32bit等多个发展代次，至今已有采用多核架构的32bit MCU产品，拥有强悍的整数和浮点运算能力，具备640KB的eFlash和320KB的SRAM，高达300MHz的主频以及600MHz的DSP工作频率。现在小小一片芯片的运算能力远超当年超大型机的运算能力！

MCU从诞生之初就是以一个完整系统的面貌出现，以丰富的外设见长。随着几十年的发展，不断丰富和拓展自己的外设。

MCU内部的外设一般包括：串口控制模块、SPI模块、I2C模块、A/D模块、PWM模块、CAN模块、SRAM、eNVM、比较器模块等，它们集成在MCU内部，有对应的内部控制寄存器，可通过指令直接控制。

随着MCU在各个应用领域的广泛应用，外设也不断丰富，现已包含了各类高速通信接口如USB1.1/2.0/3.0接口、MIPI接口等，面向有线网络的以太网接口，还有包含LCD屏的驱动和控制接口，Touch pad/panel的接口，一些传感器的专用接口，面向无线应用的蓝牙，Sub-GHz等射频外设等。

在内核方面，除了8051、6502等内核外，32bit的MCU主要采用ARM的cortex-M系列。也有大量的MCU采用RISC内核。同时由于计算量不断增加以及功能不断强化，市场上也出现了多核MCU，集成有多个内核，包含DSP等内核可以对浮点运算提供更快的速度。随着AI的发展和普及，未来的MCU中也会集成一定规模的AI硬件加速模块，面向边缘计算，提供强大的硬件支持。

随着物联网的发展和广泛应用，用户对数据安全也越来越关注，使得MCU中也集成了硬件加密模块，支持各类加密算法。同时，MCU性能和外设不断强化，已经可以运行复杂的片上操作系统。

MCU的主要应用市场

作为嵌入式电子应用领域不可或缺的核心部件，MCU开发的各种嵌入式应用也不断拓展，PC、网络通信、工业控制、汽车电子、消费电子、金融电子、政府身份认证都离不开MCU。

市场研究公司IHS表示，针对连网汽车、可穿戴电子设备、建筑物自动化以及其他有关物联网（IoT）应用的全球微控制器（MCU）市场预计将以11%的复合年成长率（CAGR）成长，从2014年的17亿美元增加到2019年时28亿美元的市场规模。

2017年，国内MCU市场已达403.2亿元，同比增长达12%。据预测，随着中国大陆汽车电子和物联网领域的快速发展，对MCU的需求将越来越大，国内MCU市场将保持12%左右的增速高速增长。

由于国内MCU产品主要面向中低端应用，技术和市场竞争力都不高，与国外厂商差距明显。

目前MCU的应用大致包括：家电类，如电视机、空调、电冰箱、洗衣机等；办公自动化设备，如打印机、复印机、传真机、考勤机、电话等；商业营销设备，如扫码枪、电子称、收款机、条形码阅读器、IC卡刷卡机、出租车计价器以及仓储安全监测系统等；工业自动化控制，如各种测控系统、过程控制、程序控制、机电一体化、PIC等；智能化仪表，如数据处理和存储、故障诊断、联网集控等；智能化通信产品；计量表计，如水、电、燃气表计；集中器和抄表终端等；市政控制，如路灯等公共设施控制；航空航天和国防军工。

芯机遇，新挑战

随着物联网时代的到来，MCU的应用将更加广阔。一些传统的产品将被加入智慧的功能，一些全新的应用场景也将横空出世。这给了MCU应用以极大的想象空间，也不断的改变着MCU的产品形态。

一是物联网。据IDC预测数据，到2020年全球IoT总连接数将达到300亿，市场空间达到1.7万亿美元。物联网将是碎片化的市场，不同场景需要不同的功能外设，这使得ASIC难以兼顾各类场景的需要。MCU拥有良好的通用性，同时具备多种工作模式，其超低功耗模式可以满足300nA以下的待机功耗要求，完全适用于IoT的场景需要。

二是汽车电子。由于电动汽车、混合汽车以及自动驾驶的发展，汽车电子将会成为MCU最大的市场之一。包括车载信息娱乐产品，雨刷、车窗、电动座椅，发动机和车身控制领域，安全监控和自动驾驶等方方面面都会大量采用MCU控制，乐观估计未来MCU在单辆汽车内的用量将有望超过200个。

社长：卢山 社址：北京市海淀区紫竹院路66号赛迪大厦18层 邮编：100048 每周二、五出版 周二8版 周五8版 零售4.50元 全年定价420元（包含手机客户端） 广告部：010-88558848/8808 发行部：010-88558777 京昌工商广登字第20170004号 经济日报印刷厂印刷