创米科技

创米数联产品安全白皮书

关于本文档

创米数联产品安全白皮书，旨在概览创米数联针对产品安全问题所进行的探索与实践，以开放透明的视角让广大用户了解我们的安全能力。

创米数联适时可能会对本文档进行更新，最新版将发布于公司官网(http://www.imilab.com/)。

版权声明

商标声明

创米科技 为创米数联的商标或是注册商标。

责任声明

在法律允许的最大范围内，本文档所描述内容均“按照现状”提供，创米数联不提供任何明示或默示保证，包括但不限于适合特定目的、商用性等特征。

创米数联不保证本文档内容的准确性，并保留对其进行纠正或修改的权力，不另行通知。

任何使用或信赖本文档内容做出的决定及因此造成的后果由行为人自行承担。

如本文档中所述内容与适用的法律相冲突，则以法律规定为准。

修订记录

首次发布于 2022 年 1 月

关于创米

上海创米数联智能科技发展股份有限公司，成立于 2014 年 4 月，公司总部位于上海,是一家聚焦智能家居，深度融合人工智能，为居家安全与生活提供全方位产品与服务的物联网公司；是小米最早的生态链公司之一，也是首批小米生态链亿元俱乐部成员。

创米小白，是创米科技旗下智能家居品牌。凭借全球领先的 AI 机器视觉技术、深厚的智慧物联行业经验，和智能硬件全链路产研体系，创米小白始终专注于“安全”，不断探索创新，变“前沿黑科技”为“看得见”的“白科技”，让家可看可控，让智慧生活舒心舒适，轻松美好。

安全概述

AIoT 的持续深入发展需要建立在负责、开放、专业、系统的网络安全和隐私保护基础上，创米数联一贯将网络安全和隐私保护作为公司最高纲领之一，持续设立专项资金投入，保障产品安全研发与交付、安全关键技术研究、安全应急响应体系建设得到扎实稳步推进。所有产品发布前，均要经过攻防实验室的严格测试。目前，创米数联已经在可信计算、数据加密、隐私保护、攻防测试等安全技术领域取得丰硕成果，并在全系列产品中集成应用。

本文档旨在通过对创米数联产品安全框架构建、安全基线实践、安全技术应用、安全使用建议的全面阐述，让用户更加深入了创米数联产品的安全能力。

安全名词解释

ESD	Electrostatic Discharge，是一种静电释放技术，为保护设备电子元器件，避免静电带来的损害。
TLS	Transport Layer Security，是一种加密的传输层安全协议。
ARP	Address Resolution Protocol 根据 IP 地址获取物理 MAC 地址的底层网络协议。
AES	Advanced Encryption Standard 高级加密标准算法
RSA	Rivest-Shamir-Adleman 一种非对称加密算法
ECDSA	Elliptic Curve Digital Signature Algorithm 椭圆曲线数字签名算法
Secure Boot	安全系统启动模式

修订记录

编号	版本号	修订内容	发布日期
1	V1.0	首次发布	2022 年 1 月

目录

一、 IOT 存在的安全威胁

IOT（The Intenet of Thing）将任何设备通过网络连接，给设备赋予智能，实现人与设备，设备与设备之间的沟通和交流。海量的设备的互联互通，使得网络更便捷，业务更丰富；同时也使得网络变得更复杂，也面临着巨大的安全挑战。

IOT 设备除了传统的网络安全威胁之外，还存在着一些特殊的安全问题， 这是由于物联网是由海量的设备或是节点组成，缺少了人对设备的有效监控，并且数量庞大、设备集群度高等，物联网的安全威胁还可以根据 TCP/IP 网络的架构分为物理层威胁、传输层威胁和应用层危险

1、物理层威胁

- 物理攻击
  部署在远端的缺乏物理安全控制的设备有可能被盗或破坏。物理接口直接暴露在设备外部，没有安全保护，容易被非法访问。
- 数据泄露
  敏感信息存放在设备中，可能会被读取，更甚的可能会被篡改，造成损失。
- 非法登陆
  部分访问无认证或认证采用默认密码、弱密码，认证机制易被绕过。
  固件中保留了测试调试接口，而且没有相应的安全机制，导致可能被攻击。
- 非法更新
  设备更新验证机制不健全，非官方固件包被直接刷进设备；非官方固件包固件未经验证， 可能存在漏洞，或是其本身就是恶意软件。
- 漏洞
  os 或是软件过时，漏洞没有及时修复。

2、传输层威胁

- 网络攻击
  通过无线接入渗透网络，无线协议本身缺陷如缺乏有效认证可能导致接入侧泄密
  未加密的通信过程容易发生劫持、篡改和窃听等中间人攻击。
  病毒攻击物联网设备，引起僵尸网络，对互联网目标发起 DDOS 攻击。

- 数据泄露
  设备和云端以及移动应用通信传输时，控制命令和采集的数据没有加密，攻击者可能通过监听获取敏感数据。

- 数据篡改
  设备在网络通信时，网络传输数据没有校验机制，控制命令和采集的数据可能会被攻击者篡改。

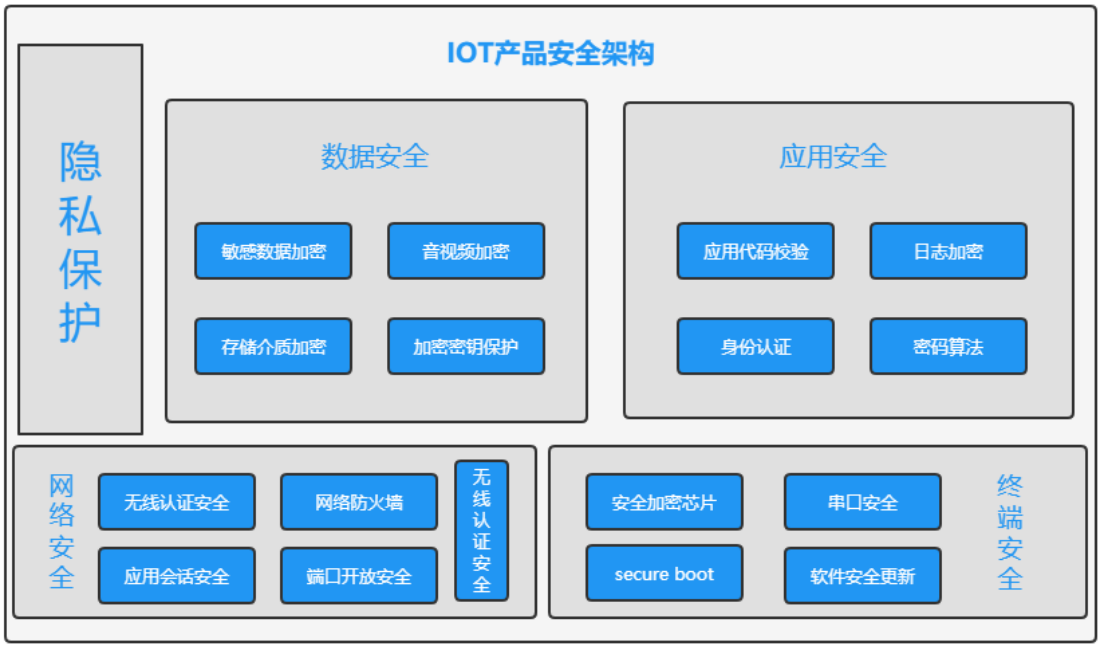
3、应用层威胁

- 设备管理
  平台层面所管理的设备分散、繁多，设备的升级过程和安全状态等难以管理。
- 系统漏洞
  应用层的操作系统，大多为通用系统，如 Linux、windows、Android 等，通常大规模的网络攻击和漏洞利用均是系统漏洞问题。
- 数据泄露
  应用层管理大量的数据，不做加密处理，很容易产生数据泄露，如直接拔走 sd 卡。
- 配置漏洞
  安全配置长期不更新、不核查。较多的网络攻击也是利用配置不合理的问题产生的。

在深入探索 IOT 设备的诸多安全性隐患后，结合 iot 设备在软硬件、计算能力等方面的特性，创米数联设计的以视频为核心的 IOT 安全解决方案，力求打造出安全的架构，建立更加安全的体系，去保障终端安全、数据安全、应用安全、网络安全、隐私保护以及安全合规。

二 、产品安全架构

产品安全架构分别从终端安全、数据安全、应用安全、网络安全、隐私保护等方面去保障，在这些方面运用了很多安全技术手段



1、终端安全

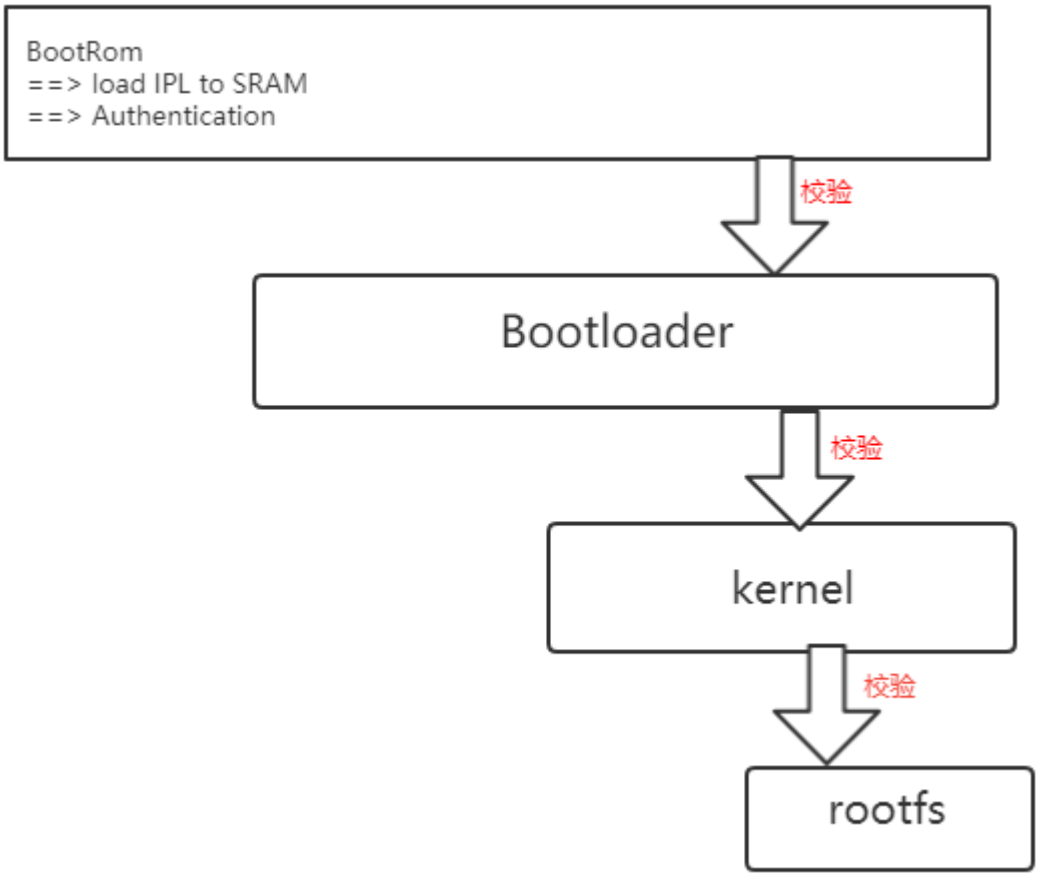
终端安全为了确保每台 IOT 设备的所有核心组件都能为软件和硬件提供安全保护。从系统启动到软件更新，确保每个步骤都进行安全校验。

1.1 secure boot

secure boot 是设备安全的基石。

该方案是通过固化在芯片内部的一段代码（BOOTRom），设备启动后执行这段代码，把保存签章信息的代码 load 到 SRAM 进行认证， 根据认证结果判断系统启动是否进行；验证通过后会继续校验 bootloader、kernel、rootfs 等组件是否合法； 通过各个组件的验证确保软件未被修改。

如果启动过程中任何一个组件校验失败，启动都会停止， 设备将无法继续正常工作。



1.2 软件安全更新

创米数联为了解决产品使用过程中出现的 bug 和产品更新功能迭代；此类更新更新会根据不同的设备分发与之匹配的固件。当软件测试通过后用户会看到固件更新通知，我们鼓励用户尽快更新到最新的固件。

1.2.1 通过 ota 方式升级固件

设备端端获取到新固件的传输过程中采用的是安全的通信机制（https），有效保证固件更新包的数据保密性和完整性。ota 固件的完整性校验有如下两种

1.2.1.1 固件包数字签名

设备固件中携带数字签名，当设备收到固件后可对签名进行验证

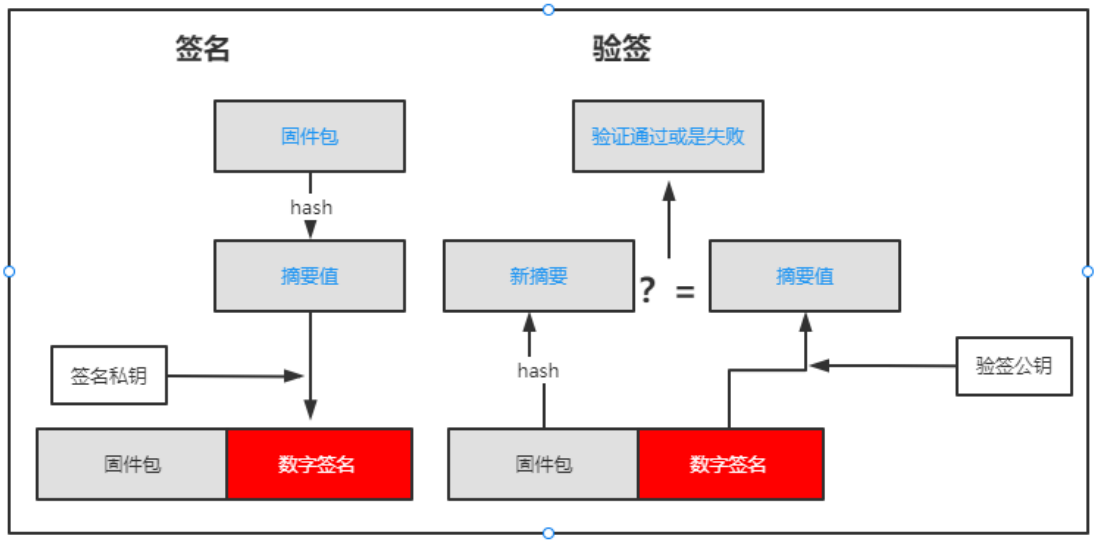
1.2.1.2 固件包加密+摘要验证。

使用高级加密方法，将固件直接加密，当设备端接收到固件后会先对固件进行解密，然后进行固件摘要验证。

签名和加密固件都是为了保证固件包的合法性，避免非法固件更新包。

1.2.2 通过 sd 卡进行刷机

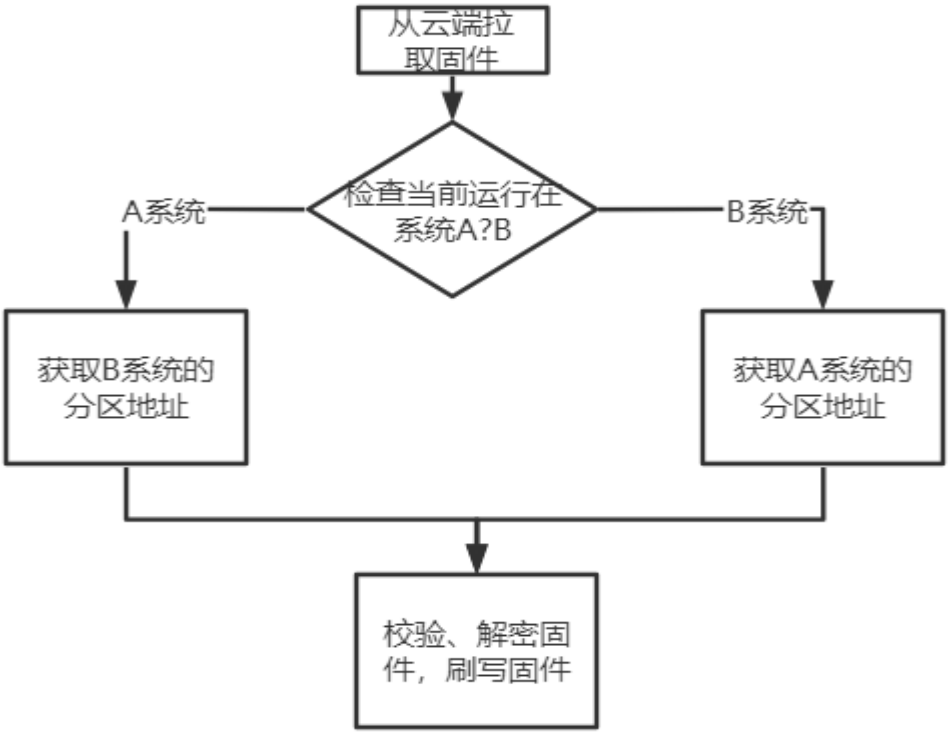
该方法时应对于设备出现异常导致的不能正常运行的固件升级；升级的固件会使用签名的方法去验证合法性。



1.2.3 系统双备份

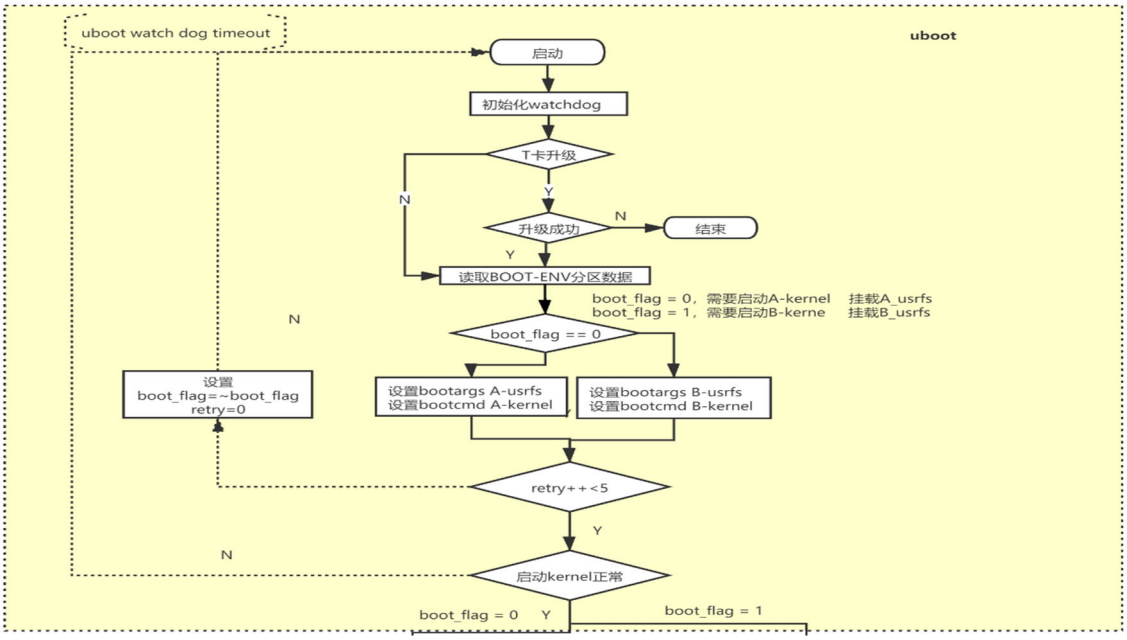
双备份系统可以避免 ota 升级过程中的异常断电、使用过程中的突然掉电引起的 flash 数据损坏导致系统不能启动的问题；

双系统 ota 升级方案：若当前运行在系统 A 上，如果此时需要升级，则直接升级系统 B，当前运行在系统 A 则升级系统 B



双系统启动方案：

在 bootloader 中会标记上次启动的系统，和重试的次数，当系统 A 启动失败达到固定次数后，会启动系统 B， 启动的流程图如下



1.2.4 不允许固件降级

防止设备被降低到老版本，导致已修复的漏洞被继续利用。

1.3 安全加密芯片

为了满足设备的高安全需求，创米数联在设备上增加了一个专门用于签名验证、通信加密的硬件加密芯片，实现了硬件级别的高强度安全，为设备的安全通信，文件加密等功能提供了基础。

安全加密芯片自带硬件真随机数生成器， 确保设备中的密钥，随机数据具有较高的随机性，增强设备的安全。

1.4 串口安全

为了保证设备在出厂后不被暴力破解，在出厂的固件里面关闭了调试接口,同时硬件上也去除了串口引脚。

同时为了在某些场景下的调试方便，对串口登陆进行口令验证，增强了设备的安全性，同时每台设备的口令都不一样， 通过某种规则生成

2、网络安全

IOT 发展初期，IOT 终端和网络大多都是设计在鼓励环境中运行的，安全机制相对薄弱。

随着 IOT 的发展，这些终端和网络被足不接入到互联网中，这会引起新的安全问题。

为了解决这个问题，创米在固件中关闭了不是必须的网络服务，如 telnet、ssh 和 ftp 等，使得设备受攻击的范围更小。

2.1 无线认证安全

创米数联产品支持标准的无线局域网协议，支持 WPA2、 WPA3 级别的无线网络加密，使用安全 AES 加密算法， 为用户提供最高级别的安全保障

2.2 端口开放安全

创米数联所有产品默认只会开辟需要使用的端口， 关闭其他端口，并且已经经过了数家安全机构的测试。

2.3 应用会话安全

所有创米的产品的网络连接会话均按照统一的安全措施。

所有会话使用强口令登陆， 使用高级加密方式通信。

2.4 网络防火墙

创米数联所有产品均配置了网络防火墙，提高安全级别。

3、应用安全

3.1 应用代码安全

- 设备在启动后，会自动按照事先预置好的顺序去挨个启动进程，防止恶意程序或是代码被执行；另外系统在启动的时候会校验固件的完整性，也可以进一步保证程序不被串改。
- 禁止使用不安全的字符串操作函数，避免造成缓冲区溢出异常
- 启用编译器的缓冲区缓解措施，开启 ASLR 保护措施
- 使用带白名单校验的系统调用函数，防止异常的命令注入

3.2 日志加密

设备在运行的过程中会产生日志，为了排查故障，用设备上插有 sd 卡，通常会将日志以一定的机制存放在 sd 卡里面，存放在 sd 卡里面的日志是加密过的，可以避免一些敏感信息被泄露。

排查问题的时候，只要拿加密过的日志去创米数联云端进行解密即可，同时解密时云端自动进行，密钥存储在数据库中，可以保证密钥不会泄露，保证了加密日志安全性。

3.3 身份认证

创米数联的产品账号安全体系依赖于一系列的安全策略，充分保证账号安全。

调试模式下串口登陆口令，使用强口令。

app 账号登陆可以通过短信验证码登陆，提高安全性

3.4 密码算法

在日常的网络通信的过程中，涉及到认证、加解密的时候，使用 sha-256 去替代 MD5、crc32 等， 使用 aes-128/256 代替 DES 等。

4、数据安全

4.1 敏感数据加密

利用密码技术对敏感用户数据进行保护，用户数据主要包括用户配置数据和用户隐私数据。

4.2 加密密钥保护

创米数联的产品的加密密钥分为固件验签密钥、用户日志解密密钥、音视频流解密密钥、用户信息加密密钥等， 这些密钥均保存在云端， 由云端自动生成、管理，不需要人工参与，降低了密钥泄露的风险。

4.3 存储介质加密

对于存储在各类介质上的各类数据进行加密，避免数据泄露。尤其时关键数据如音视频数据、日志等进行加密。

4.4 音视频加密

音视频的数据安全时视频监控的重点，创米数联产品支持音视频帧进行加密和使用加密传输。

编码阶段支持将音视频的每一帧单独进行加密，以密文的形式进行传输或存储，可以避免音视频非法泄露。

网络传输的过程中，使用 HTTPS/TLS 方式，可以防御网络攻击。

4.4.1 音频加密

针对不同的音频格式使用不同的加密策略

g711a：该格式音频帧全是数据，所以得将音频帧全部进行加密

aac：该格式包含了音频数据和枕头部分，所以对 aac 格式的音频使用了一定的策略去加密。

4.4.2 视频加密

对于任何一种流加密方式，都有一个保护块的概念，所有的加密操作只对保护块执行。音频的保护块通常就是一个典型的音频帧，h264 视频的保护块是某些指定 nalu 类型的数据体部分。

视频流加密只在特定的包类型中进行，对于 h264 流而言，并不是所有的 NALU（network adaptation layer units）类型都需要加密，一般情况，NALU 类型为 1 和 5 （slice 和 idr）的都需要加密，而其他的都不需要加密。每一个 nalu 都是以引导码开始，引导码不属于保护块部分，因此不会被加密。 引导码之后的那个字节即表明 nalu 类型的 1 个 byte 以及其后连着的 31 个 byte，也不会被加密。这 32 个 bytes 之后的数据，才是需要加密的保护块。但是，如果任何一个保护块的数据长度小于或等于 16bytes，则也不会被加密。因此，一个 nalu 的长度（不包含引导码）如果小于等于 48bytes，则这个 nalu 不会被加密。对于一个 nalu，将所有的保护块以 16 字节为单位操作，对第一个 16 字节加密，其后的 9 个 16 字节（共 144 字节）不加密，然后接下来 16 字节继续加密。直到剩余的加密数量少于 160.任何一个 nalu，只要其中保护块部分被加密了，那么引导码防竞争机制应该被重复一次。(为了性能，见补充协议)解密操作跟上述描述相反操作即可

5、隐私保护

IOT 的很多应用都与我们的生活息息相关，如摄像头、门锁等。当设备使用物联网设备时，用户的个人信息可能会被直接或间接地收集、传输、存储与使用。数据安全是我们的至关重要的工作之一。创米数联严格遵守相关的法律条规，包括中国的网络安全法。并且每一款产品都有对应的隐私策略，在实际的操作中严格按照隐私策略进行必要的数据收集。

在设备维修、删除等场景下，产品提供了完善的个人数据删除机制。

三、安全合规

1、创米数联的系列产品经通过小米 AIOT 安全实验室的测试，并被评为高安全等级产品；主要参考标准有：

- IoT Security Foundation Security Framework 2.0
- ETSI TS 103645 Cyber Security for Consumer Internet of Things
- OWASP IOT security testing guide
- OWASP Application Security Verification Standard
- CTIA Cybersecurity Certification Test Plan for IoT Devices

2、创米数联的系列产品通过了中国电信、中国移动、中国联通的安全审计

创米科技