视洞摄像头安全白皮书

V1.0 版本

杭州视洞科技有限公司

目录

1 背景

近年来随着物联网、智能家居等行业的快速发展，安防设备也增长迅速。随着安防设备产业规模的逐渐扩大，这些设备带来的安全问题也逐渐凸显，不久前，《财经》杂志刊登《失控的摄像头》和央视频道播出的《第一时间》针对基于智能摄像头引发的安全问题作了详细报道。越来越多的实际案例在提醒大众，安防设备若自身出现安全问题将会造成很多风险，如远程控制，隐私监视等，安防设备的安全加固也是迫在眉睫。

我司专注做民用安防摄像机，因此我们更为注重个人隐私，我们通过对摄像机软件的整体架构设计，针对摄像机操作系统安全、账号管理、数据安全、网络传输安全、固件系统安全全方位考虑，充分保证了客户的数据隐私。

2 文档范围

本白皮书要求规定了网络摄像头安全能力技术要求包括物理硬件层、固件系统层、网络通信层、应用数据层等安全能力，并对安全能力的具体技术实现方式和方法进行了详细的说明和设计。

本白皮书中的安全标准适用于视洞所有摄像机产品，包含视洞P30、视洞P60、视洞U30.、视洞U60-POE、视洞U50、视洞U50-4G、视

洞P62、视洞P90等。

3 缩略及术语说明

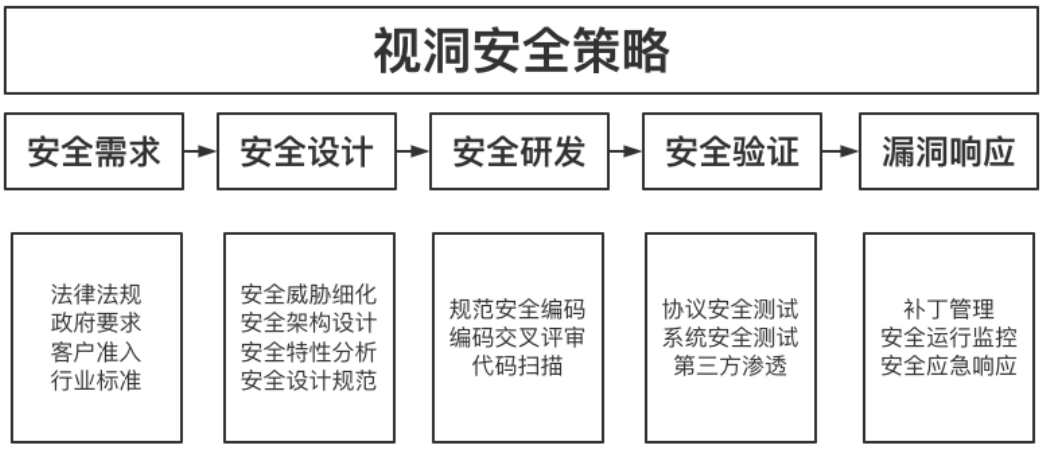
表 1-1 缩略及术语说明表

序号	术语	说明
1	TLS	传输层安全协议(Transport Layer Security)
2	DTLS	数据包传输层安全性协议(Datagram Transport Layer Security)
3	RTSP	实时流传输协议(Real Time Streaming Protocol)
4	CNNVD	国家信息安全漏洞库(China National Vulnerability Database of Information Security)
5	CNVD	国家信息安全漏洞共享平台(China National Vulnerability Database)
6	TEE	可信执行环境(Trusted Execution Environment)
7	SoC	系统级芯片（System on Chip）
8	IPL	初始程序加载器（Initial Program Loader）

9	IPL_CUST	用户级 IPL （Initial Program Loader for Custom）
10	eFuse	一次性可编程存储器
11	HW Key-RSA	硬件 RSA 公钥
12	CUST Key-RSA	用户级的 RSA 公钥

4 安全策略

结合视洞研发并参考业界最佳安全实践，如 OpenSAMM、BSIMM、CSDL、MSDL 以及客户的反馈，融合安全设计、安全开发、安全测试等，制定了符合视洞的产品研发安全策略，保证产品安全的有效落地，提升产品机密性，增强隐私数据保护，为客户提供更安全的产品。



- **安全需求**

首先，把产品安全强制纳入需求列表。产品安全是保障安全目标实现或将风险控制在可接受水平的最基本要求，来源于法律法规、政府要求、客户准入、行业标准等，其目标是确保产品安全合规、保护用户隐私和敏感数据、加强系统访问控制、增强系统防攻击能力。其次，要对该产品未来在客户现场的使用场景进行威胁分析，识别出有针对性的安全需求。威胁分析是针对产品的具体使用场景找到所有可能的威胁来源、类型以及攻击点，以便我们评估风险，确保相关的应对和防范措施纳入到了产品需求列表中。

- **安全设计**

安全设计与功能设计融合，在对产品进行功能设计的同时进行功能级别的威胁识别，并制定对应的缓解措施。对收集或识别的安全需求进行详细的分析与设计，并且公司有专门的安全架构师为各个产品在安全设计中提供专业的技术支撑。所有产品在设计过程中都会做攻击面最小化分析，降低产品总体的安全风险。

- **安全研发**

产品研发人员必须遵循安全编码规范进行编码并进行交叉评审，通过自动代码扫描工具快速、准确地查找高复杂度代码中的危险函数和缺陷问题，降低代码安全缺陷率，识别需要进一步检查的范围。通过自研的针对公司业务场景的代码缺陷分

析和扫描工具，能够通过代码特征识别到已知缺陷，告知研发人员各个分支的缺陷存在情况，评估缺陷同步工作是否到位，并在持续构建活动中进行拦截，实现已知代码问题在源码阶段得到控制，大大降低修复成本。

- **安全验证**

为了防止由于研发过程中可能会导致产品出现的各种安全问题，我们在产品研发的每个阶段都进行相关安全测试，确保产品的安全。在产品安全测试中加强协议安全测试力度，引入协议安全测试工具。对所有产品进行网络协议安全性、健壮性、可靠性分析以及未知漏洞挖掘；在系统安全测试中引入漏洞扫描工具及时跟踪 CVE 漏洞库信息，能够全面发现系统存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞。

- **漏洞响应**

公司有专门负责接收、处理和披露产品和解决方案与安全相关漏洞的应急响应部门，其职责还包括：响应和处理客户提交的安全事件、响应和处理行业协会公布的安全事件、制定公司信息安全事件管理策略和安全事件处理方案、分析系统软件提供商和专业安全厂商发布的漏洞及补丁等。对于安全事件的执行效率，管理规范有明确的规定，如安全事件初步确认时间不超过 24 小时，高危以上级别的安全漏洞修复期限为 30 天。

5 安全设计框架

网络视频监控系统面临着视频信息窃取,控制信令窜改,设备非法接入等多种安全威胁,为提供安全,可信,可靠的视频服务,需要在视频监控系统的各个环节设计安全机制,是视频监控系统安全的重要组成部分.以下图 1-1 是整个系统安全设计框架。

图 1-1 系统安全设计框架

- 在物理硬件层面保障智能摄像头安全，提出相应的安全要求，从硬件接口、安全启动、抗攻击等层面保护智能摄像头；
- 固件与系统安全能力：在固件与系统层面保障智能摄像头安全，提出相应的安全要求，从固件升级、密钥安全等层面保护智能摄像头；
- 网络与通信安全：在网络与通信层面保障智能摄像头安全，保障智能摄像头采用有线、无线通信协议安全能力满足相应的国家标

准或标准组织规定；

- 应用数据安全能力：在应用数据层面保障智能摄像头安全，摄像头需保证数据的完整性、可用性、机密性。

6 安全设计详细说明

6.1 物理硬件安全设计

6.1.1 物理安全

终端设备应该满足以下的物理安全。

- 应具备数据的物理保护机制，防止攻击者通过去除芯片表面封装层而获取存储器数据；
- 应具备在受到暴力移除或拆卸时的防护预警机制。

6.1.2 可调式接口安全

终端硬件设备对于可调式接口安全应该满足以下要求：

- 具有本地硬件调试接口或通信接口的硬件设备，需要支持接口访问控制或关闭的能力，并出货设备需要关闭。
- 具有本地硬件调试接口或通信接口的硬件设备，接口登录认证不能为弱口令，必须要设置为强密码
- 需要禁用闲置的外部设备接口
- 需要禁用外接存储设备引导启动系统自启动功能

6.1.3 安全启动

终端硬件设备的主控SoC支持安全启动，逐级验证和加密功能，支持eFuse存储功能。支持使用TEE执行环境或独立的安全芯片进行密码运算，用于固件的解密和验证。

6.1.4 身份唯一标识

终端硬件设备具有明确的标识以及支持防篡改的唯一识别码的能力。唯一识别码存放在独立区域的设备信息分区。

6.2 固件系统安全设计

固件系统安全设计主要从固件安全，系统安全、OTA 安全、漏洞修复、秘钥存储及证书安全几个方面考虑。

6.2.1 固件安全

终端设备的固件保护需要要求包含以下两点：

- 支持安全启动，并逐级验证；
- 支持固件加密功能，使用前解密

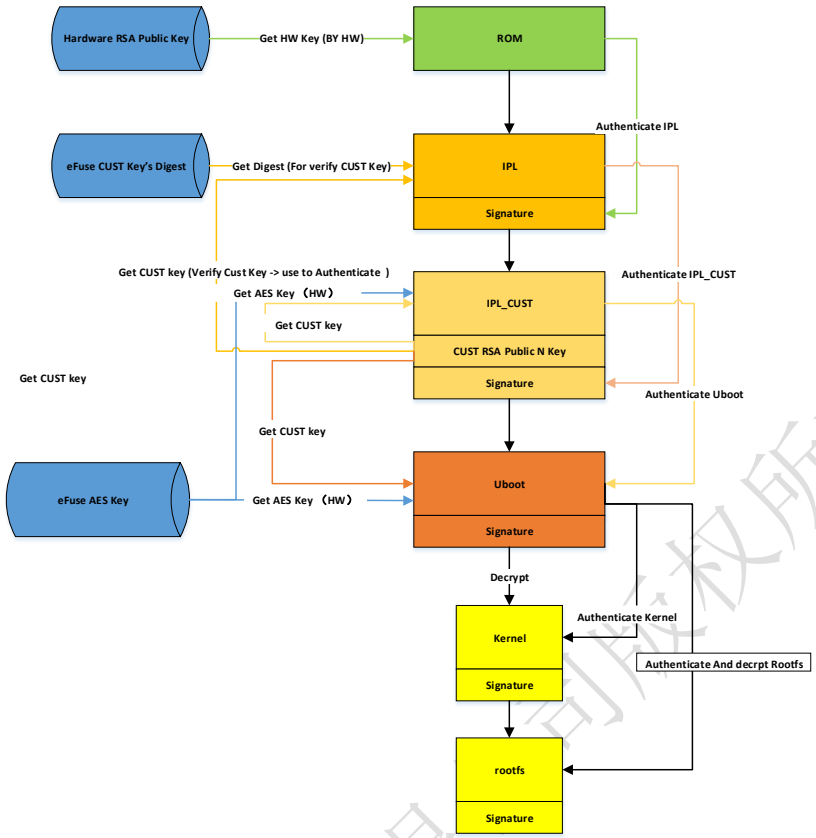


图 1-2 固件系统安全启动流程

该1-2图解为从ROM到Linux Kernel的模块结构，其中Signature为签章数据部分，每个模块的Signature均会嵌入到相应bin文件的最后，每个模块均包含Get Key和Authenticate的动作直到Linux Kernel和Linux Rootfs。Get Key有2种，HW Key-RSA由硬件获取，CUST RSA Key由软件获取。另外，需要注意IPL_CUST是插入CUST RSA Key后才进行签章的，所以其Signature嵌入在CUST RSA Key后面。

- 通过公钥HW Key-RSA验签 IPL

该流程为ROM阶段使用硬件(SoC)中的RSA公钥(RSA Public Key)对IPL进行签章的验证。由于HW Key是不可被改写和替换的，从而保证了IPL不会被篡改。

- 通过公钥HW Key-RSA验证CUST Key-RSA

该流程为IPL对事先已烧录至eFuse中CUST Key-RSA的摘要（Digest，即CUST Key-RSA的SHA-256计算值）和当前软件取到的CUST Key-RSA的摘要进行比对，若一致则证明当前软件取到的CUST Key-RSA是合法的Key。通过这个设计来确保CUST Key-RSA不被篡改。

- 通过公钥CUST Key-RSA 验签IPL_CUST

该流程为IPL读取事先嵌在IPL_CUST里的CUST RSA Public Key，对IPL_CUST进行签章的验证。由于CUST RSA Public Key不会被篡改，从而保证了IPL_CUST也不会被篡改。

- 通过公钥CUST Key-RSA 验签U-Boot/kernel/rootfs

该流程为IPL_CUST读取事先嵌在IPL_CUST的公钥CUST RSA Public Key后，对U-Boot进行签章的验证和解密。同样U-Boot也读取这把Key对下一阶段的Linux Kernel和Linux Rootfs进行签章验证和解密，从而保证uboot、kernel、rootfs等固件的验证和安全。

图1-3为固件镜像的签名、验签、加密、解密图。任何烧录的固件镜像模块都需要先加密，然后对加密后的镜像文件做签章。在设备

启动时，先对加密的镜像文件做验签，验签通过后，加密镜像文件，然后加载在内存启动。

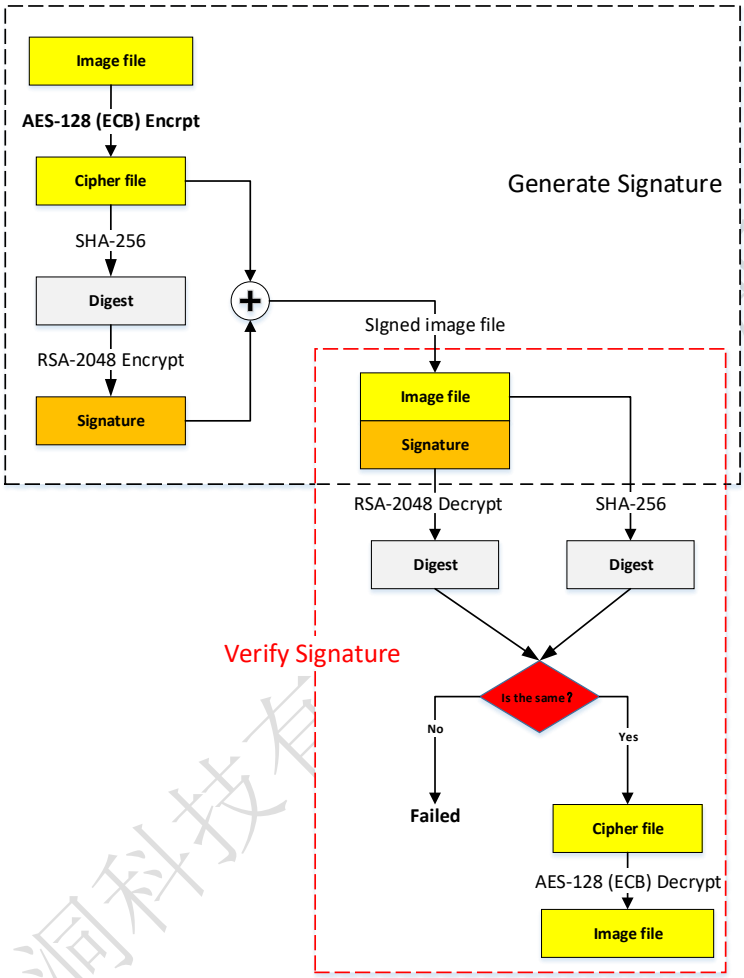


图 1-3 签章和验签图

6.2.2 系统安全

终端设备操作系统最小化安装，仅安装必要的组件和应用程序的能力。

为了满足调试维护的要求，设备支持通过安全的串口和telnet调试，但是在设备上telnet服务默认关闭的，同时串口也是默认禁止

输出。只有管理员才有权限开启和关闭。

6.2.3 OTA 安全

设备需要支持系统远程升级，对于 OTA 安全设计要求如下：

- 设备 OTA 时，应支持对升级软件包进行数字签名验签
- 支持升级包更新之前进行完整性校验的能力，防止升级包传输过程被篡改。
- 设备进行系统与固件更新，当发生因更新包缺陷而导致更新失败时，不应出现系统不可用的情况。

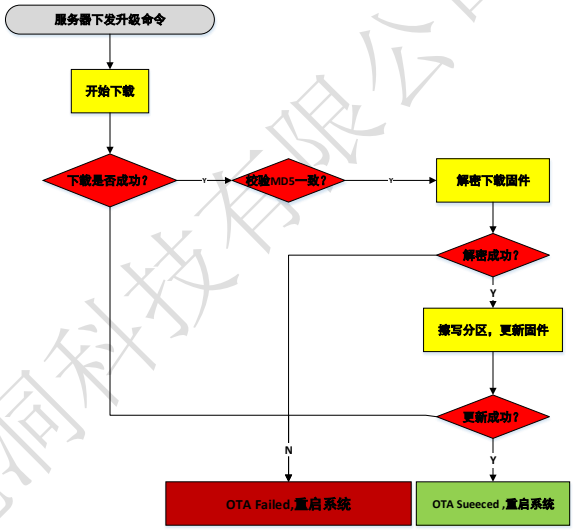


图 1-4 OTA 升级流程

图 1-4 OTA 升级流程。当服务器下发升级命令之后，设备进入 OTA 流程。设备首先解析命令获取和保存链接地址 URL 和 MD5，然后开始下载固件。

- 为了保证固件的完整性，需要检测固件的 MD5 值，当 MD5 值比

对一致后进入下一步操作。

- 为了保证固件的安全，放在服务器的固件一般为加密和签名固件，因此在固件下载下来之后，先需要解密验签处理；一旦解密成功，就开始擦写 flash 更新固件；
- 固件更新成功之后，重启系统，进入正常系统启动流程，即 OTA 成功。

如果 OTA 过程中，由于断电或者其他异常导致擦写不成功时，重新启动后会自动进入备份系统流程，并恢复固件系统。

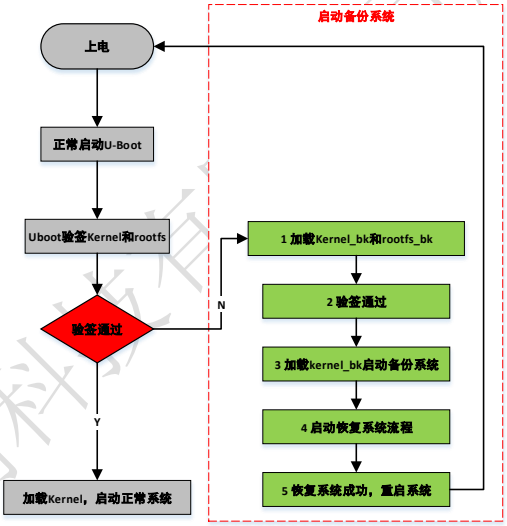


图 1-5 备份系统恢复流程

图 1-5 为备份系统启动流程，当 U-Boot 验签内核 Kernel 和文件系统 Rootfs 分区不通过后，启动备份系统。从备份升级保障设备可恢复，固件的加密和签名保证不被篡改，MD5 校验固件的唯一性；

6.2.4 漏洞修复

6.2.4.1 漏洞原则

对于漏洞修复，支持以下三点：

- 不使用包含CNVD、CNNVD已公布90天以上的高危及以上等级未处置漏洞的第三方库和开源组件。
- 关注漏洞公布，具备根据新曝光漏洞自动或手动安装升级补丁的功能。
- 在编译过程采用安全编译选项，降低内存攻击漏洞的影响。

6.2.4.2 漏洞修复应急响应

视洞建立一套漏洞修复应急响应方案，包括 3 个阶段：

- 漏洞研究与收集：通过客户、外部 CERT、安全研究人员或相关安全网站发布的资讯获取漏洞信息。同时内部团队不断发现潜在安全威胁并鼓励负责任的披露，即外部漏洞发现者应该在公开披露之前，给一段合理的时间去处理和解决问题。
- 安全漏洞评估、分析和验证：不论是疑似漏洞还是已经确认的漏洞，内部都会快速完成漏洞的真实性及相关风险的评估。
- 跟踪与解决：一旦漏洞确认，内部会立即把信息传递给漏洞提交者，然后积极跟踪反馈解决进展。还会对漏洞进行

排查，从而确保该问题在所有产品版本和产品模型中都得到解决，且确保对漏洞的及时响应。

在这个流程的各个阶段，保护客户和漏洞信息的机密性对视洞来说至关重要。

6.2.5 密钥存储及证书安全

对于密钥存储及证书安全，支持以下五点：

- 本地密码做AES加密存储，不以明文存储；对设备密码、设备认证信息等关键安全信息进行加密处理，不应在日志和配置文件中明文记录关键安全信息。
- 摄像头与平台交互的业务数据的加解密密钥由安全的密钥生成算法生成
- 流媒体密钥由服务端分配，密钥与设备ID绑定，密钥和加密向量保存在设备端。设备用该密钥负责对实时码流、回放码流和上传云存的码流加密
- 摄像头证书AES加密保存在安全的存储区域，不可篡改。
- 设备一机一密配置，密钥与设备唯一ID绑定，防止设备伪造。

6.3 网络通信安全设计

传输安全要求包括应采取安全措施，保证设备与应用服务平台之间数据传输的安全性，相关传输加密功能应默认开启；如采用加密措

施，应保证所采用加密算法不存在已被证实的安全风险；设备与应用服务平台之间进行通信前应完成双向身份认证；主要包含了网络接入认证、网络访问控制、通信保护、服务端口禁用、会话控制、无线通信等。

6.3.1 网络接入认证

网络接入认证满足两个要求：

- 接入网络中具有唯一网络身份标识。
- 接入网络证明其网络身份，应支持基于对称或非对称密码机制的鉴别。

6.3.2 网络访问控制

网络访问控制要求：

- 对远程登陆的用户具备身份认证能力
- 应对远程用户的访问进行访问控制管理，管理不同用户所能访问的数据、访问权限和访问时效性
- 支持对应用层访问控制的能力
- 支持网络端口最小化暴露原则，并禁用闲置的通信端口
- 设置口令复杂度和禁止弱口令
- 支持终端设备与接入网络间双向认证的能力

6.3.3 通信保护

支持终端设备与接入网络间，以及对终端设备远程管理时采用通信机密性保护机制，实现鉴别数据、隐私数据和重要业务数据等数据的机密性保护，使用TLS，安全通信协议，加密算法符合国家密码相关规定。 另外，支持终端设备与接入网络间，以及对终端设备远程管理时采用通信完整性保护机制，实现鉴别数据、隐私数据和重要业务数据等数据的完整性保护。视洞所有产品的网络通信都支持安全传输协议：HTTPS、TLS。安全使用各类安全协议，包括：

- 安全的证书管理、验证机制；
- 默认关闭不安全协议，如 SSLv3.0、TLSv1.0、SNMPv2等；
- 私有协议均支持基于 TLS 传输，无明文数据直接传输；
- 支持 HTTPS 访问，保证网络传输安全；
- Syslog 协议支持基于 TLS传输，无敏感数据泄漏；
- 使用安全的算法套件。

6.3.4 服务端口禁用

服务端口安全要求包括端口开放应遵循最小化原则，默认关闭非必须使用的端口。对于必须使用的端口，使用后应立即关闭；系统提示用户所有开放的端口，并告知对业务影响。视洞的所有产品默认关闭各类服务端端口，并支持安全协议版本，以减小设备威胁面，其中包括：

- 不支持 Telnet 服务；
- 不支持 FTP 服务，支持 SFTP 服务；
- 默认关闭 SSH 服务；
- 默认关闭 SNMP 服务，并支持安全的 SNMPv3；
- 默认关闭 NTP 服务；
- 默认关闭 UPNP 服务。
- 不支持web服务

6.3.5 会话控制

视洞产品的所有网络连接会话均具有统一的安全措施：

- 会话超时自动断开：会话超时时间可设置；超时无操作，自动退回登录状态，需要重新身份认证；
- 会话数量限制：会话数量可设置；可限制同时接入的数量，防止非法接入；
- 会话锁定：身份认证失败次数超过预设的次数后，自动锁定该用户后续尝试，有效避免暴力破解。失败次数可配置；
- 会话锁定时间：会话锁定时间可设置；用户可自行配置身份认证失败超限后的锁定时间，在安全的基础上提供良好用户体验。

6.3.6 无线通信

支持工业标准的无线局域网协议，包括“WPA2 企业级”，可针对公司无线网络提供访问认证服务。“WPA2 企业级”使用安全 AES 加

密算法，为用户提供最高级别的安全保障：在通过无线局域网络连接发送和接收通信时，确保用户的数据始终受到保护。

6.4 应用数据安全设计

数据安全要求包括机密性、数据安全两个方面考虑。保证用户隐私数据、个人信息、关键密钥等敏感数据在本地存储的安全性；用户生物特征信息如人脸等特别敏感的数据，进行操作应在安全内存进行，防止数据被第三方恶意获取。

6.4.1 数据机密性

设备缺省关闭web服务功能，不允许用户通过web进行控制。利用密码技术对用户数据进行防护，用户数据主要包括用户配置数据和用户隐私数据。数据加密密钥在设备中实现一机一密方案，每台设备都是随机的密码。即设备上用户数据被强行拷贝走后，无法获取设备随机密钥的攻击者不能解密数据。用户数据主要包括用户的账号密码信息，用户对设备的配置参数等；用户隐私数据包含音视频数据，AI信息但不限于人脸比对图片、模型等。

6.4.1.1 密钥机密性

设备上的密钥存储在硬件安全区，并采用分层的密钥架构。通常情况下密钥体系结构分为三层，主密钥保护密钥加密密钥，密钥加密密钥保护业务密钥，业务密钥按照用途可分为文件密钥、数据加密密

钥等。设备可以根据业务应用的场景，对密钥体系架构进行裁剪和扩充。设备最少要支持两层的密钥架构。

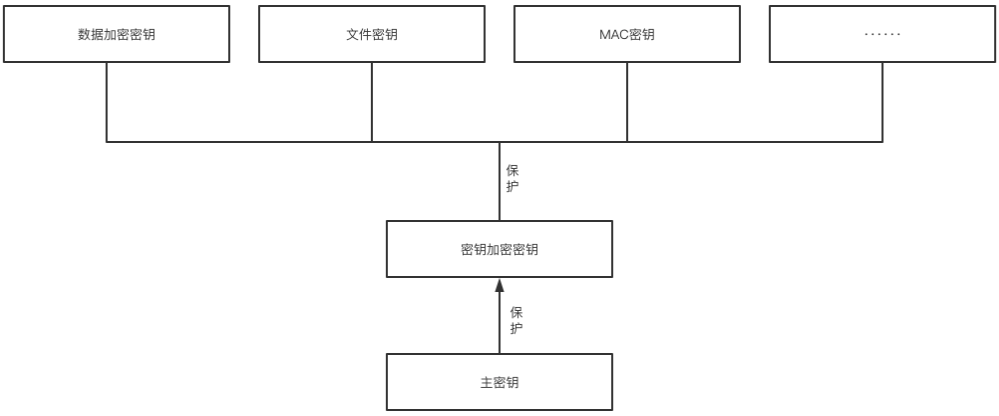


图 1-6 密钥机密性图

6.4.1.2 音视频数据机密性

音视频数据安全是视频监控系统的重点，数据都存在被篡改和非法查看的风险。视洞所有设备支持分别在音视频编码阶段和网络传输阶段进行了安全保护。

- 编码：支持音视频数据在编码过程中进行加密，以密文形态传输、存储。有效避免非法查看；支持音视频数据在编码层进行数字签名，音视频数据带数字签名一起传输、存储。有效避免非法篡改；
- 传输：音视频数据在进行网络传输时，支持 HTTPS/TLS 方式传输。有效防御各类网络攻击。

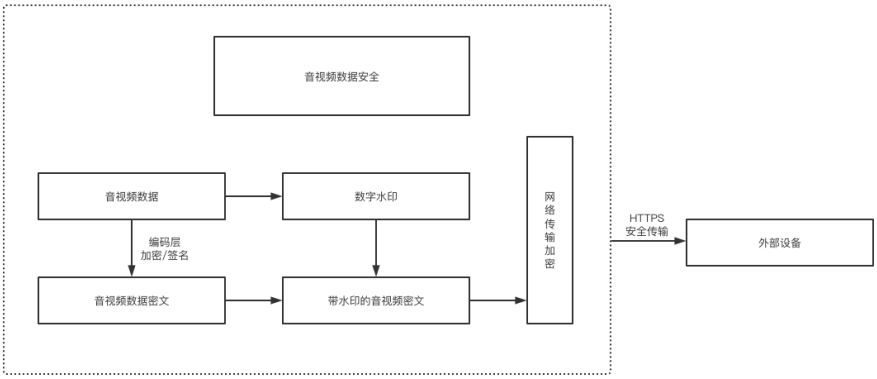


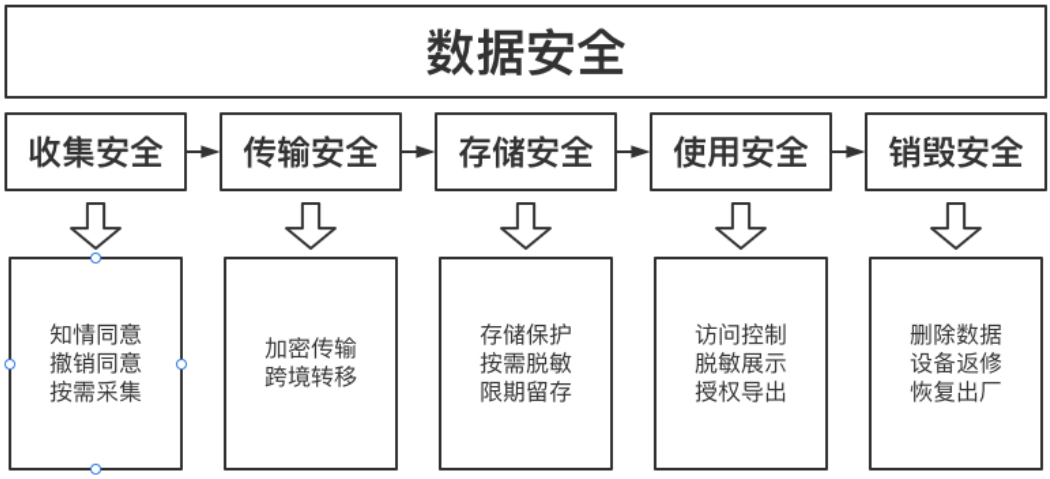
图 1-6 音视频安全图

6.4.1.3 本地存储机密性

支持对于各类存储介质上的各类数据进行加密，避免数据泄漏。尤其是可插拔本地存储上的关键数据（如音视频数据）进行加密。可插拔存储介质包括 TF/SD 卡、U 盘等。在设备中实现一机一密方案，每台设备都是随机的密码。即设备上用户数据被强行拷贝走后，无法获取设备随机密钥的攻击者不能解密数据。

6.4.2 数据安全

- 支持对终端上的重要数据（如所有的密钥和私钥、身份验证和其他安全配置）和重要业务数据实施完整性保护，确保这些数据在存储和传输中的完整。当用户网络设备时，用户的个人信息可能会被直接或间接地采集、传输、存储与使用。数据安全是网络设备应用中至关重要的工作之一。



- 作为硬件设备供应商，在大多数情况下不接触或收集用户个人数据。视洞根据所适用的法律法规将收集必要的个人数据，遵循用户同意的原则，并在隐私政策中明确列明收集范围和使用目的。
- 产品保证隐私数据加密传输，在进行跨境数据转移时，会依据信息所在。
- 对于本地存储个人数据，采取充分的安全措施进行保护，包括但不限于加密存储、访问控制、日志记录等。产品会根据其收集、使用目的来确定存储的个人数据的存留期。