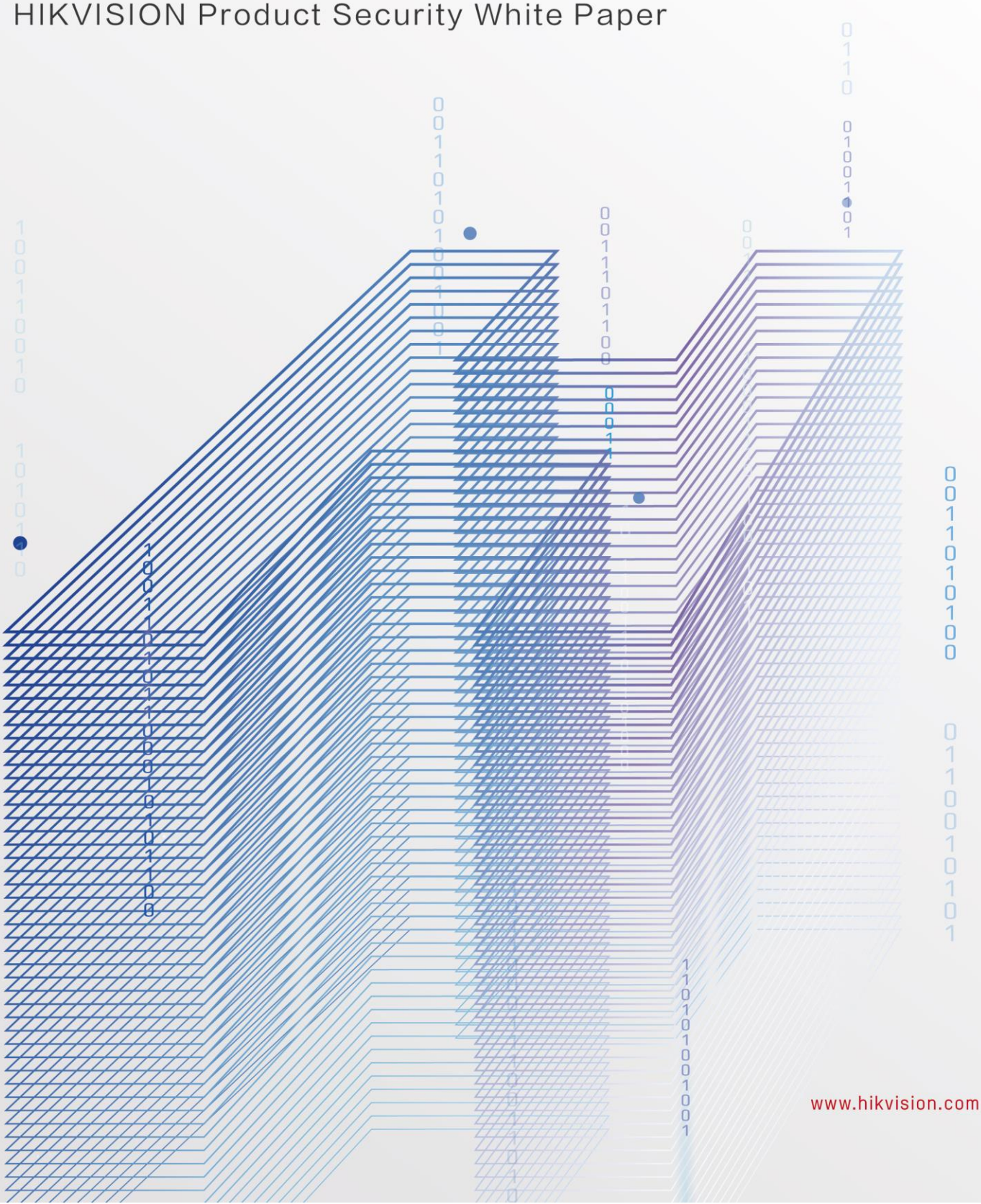
HIKVISION

海康威视产品安全白皮书

HIKVISION Product Security White Paper



www.hikvision.com

关于本文档

海康威视产品安全白皮书，旨在概览海康威视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海康威视的安全能力。

海康威视可能对本文档进行更新，最新版将发布于公司官网（https://www.hikvision.com/cn/）。

版权声明

商标声明

海康威视、HIKVISION为海康威视的商标或注册商标。本文档中提及的其他公司名称或商标由其各自所有者拥有。

责任声明

在法律允许的最大范围内，本文档所述内容均“按照现状”提供，海康威视不提供任何明示或默示保证，包括但不限于适合特定目的、商用性等保证。

海康威视不保证本文档内容的精确性，并保留对其进行纠正或修改的权利，不另行通知。

任何使用或信赖本文档的内容而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 2019 年 5 月，2023 年 12 月第二次修订。

关于海康威视

海康威视成立于 2001 年，是一家专注技术创新的科技公司。

秉承“专业、厚实、诚信”的经营理念，践行“成就客户、价值为本、诚信务实、追求卓越”的核心价值观，海康威视致力于将物联感知、人工智能、大数据技术服务于千行百业，引领智能物联新未来：以全面的感知技术，帮助人、物更好地链接，构筑智能世界的基础；以丰富的智能产品，洞察和满足多样化需求，让智能触手可及；以创新的智能物联应用，建设便捷、高效、安心的智能世界，助力人人享有美好未来。

二十余年来，公司以视频技术为起点，持续拓展和布局可见光、毫米波、红外、X 光、声波等广泛领域，打造了全面、多维的物联感知技术平台；同时，提供的产品从物联感知设备拓展到与人工智能、大数据技术充分融合的智能物联产品、IT 基础产品、平台服务产品、数据服务产品和应用服务产品在内的 5 类软硬产品；从事的领域从综合安防拓展到智能家居、数字化企业、智慧行业和智慧城市。

公司现有员工 58,284 人（截至 2022 年末），其中研发人员和技术服务人员超 27951 人，研发投入占全年营业收入 11.80%（2022 年），绝对数额占据业内前茅。海康威视是博士后科研工作站单位，建立了以杭州为中心，辐射北京、上海、武汉、西安、成都、重庆、石家庄、加拿大蒙特利尔、英国伦敦、迪拜的全球研发中心体系。

公司在中国大陆设有 32 家省级业务中心、300 多个城市分公司，在港澳台地区及海外国家/地区设立了 72 家分支机构（截至 2022 年末），为全球 150 多个国家和地区的客

户提供产品和服务，在杭州亚运会、G20 杭州峰会、北京奥运会、上海世博会、APEC 会议、北京大兴机场、港珠澳大桥等重大项目中发挥了重要作用。

2010 年 5 月，海康威视在深圳证券交易所中小企业板上市（股票代码：002415）。基于创新的管理模式，良好的经营业绩，公司荣获 2022“金责奖”最佳社会（S）责任奖[1]、第四届中国质量奖提名奖[2]、2021 纪念彼得德鲁克中国管理奖[3]、主板上市公司价值 100 强[4]、2022 中国年度最佳雇主 20 强等重要荣誉。

[1] 2022 年 12 月，海康威视荣获由新浪财经颁发的 2022 中国企业 ESG“金责奖”——最佳社会（S）责任奖。

[2] 2021 年 9 月，在中国质量（杭州）大会上，第四届中国质量奖评选结果正式揭晓，海康威视荣获“中国质量奖提名奖”。

[3] 2021 年 12 月，纪念彼得•德鲁克中国管理论坛在线上召开，海康威视获得“2021 纪念彼得·德鲁克中国管理奖”。

[4] 2022 年 9 月，由证券时报主办的第十六届中国上市公司价值评选获奖名单揭晓，海康威视荣获“主板上市公司价值 100 强”。

目 录

关于海康威视 II
1 物联网安全威胁 1
感知层威胁 1
传输层威胁 3
应用层威胁 3
2 产品安全架构 5
2.1 终端安全 5
安全芯片 5
安全启动 6
安全更新 7
口令安全 8
安全 shell 9
IP 过滤 9
2.2 应用安全 9
应用代码签名 9
身份鉴别 10
权限管理 11
访问控制 11
Web 安全 12
组件安全 13
API 安全 13
安全函数 14
2.3 网络安全 14
安全传输协议 14
安全网络服务 15
无线安全 15
端口安全 16
2.4 数据安全 16

数据生命周期安全管理 16
用户数据保护 18
存储介质加密 19
音视频数据安全 19
数字水印 20
白盒加密 21
密钥管理 22
2.5 安全运营 22
安全审计 22
安全加固 23
应急响应 24
3 安全合规 26
商用密码产品型号 26
通用标准认证 CC 26
网络安全标签计划 CLS 27
4 典型安全实践 28
4.1 物联网产品安全设计实践 28
4.2 智能物联网安全管控实践 28
4.3 视频云存储安全实践 30
5 安全性承诺与建议 31

1 物联网安全威胁

物联网（Internet of Things）将任何物体通过网络相连接，给物体赋予智能，实现人与物、物与物之间的沟通和对话。海量设备的互联，使得网络更开放、也更复杂，业务更丰富多样。然而，物联网也面临着巨大的安全挑战。

图 1-1 物联网特点

物联网是由大量的设备或感知节点构成，缺少人对设备的有效监控，并且数量庞大、设备集群度高，除了传统网络安全威胁外，还存在着一些特殊安全问题。物联网的安全威胁可以根据物联网的架构分为感知层威胁、传输层威胁和应用层威胁。

感知层威胁

- 物理攻击

部署在远端的缺乏物理安全控制的物联网设备有可能被盗窃或破坏。物理接口直接暴露在设备外部，没有做安全保护，易被非法访问。

物联网设备在户外分散安装、易被接触又没有纳入管理，导致物理攻击、篡改和仿冒。

- 数据泄露

物联网设备在数据采集和处理等过程中数据未作加密或访问权限控制造成的敏感信息泄露。

- 非法接入

物联网设备访问无认证、认证采用弱口令或者认证机制易被绕过。

物联网设备保留了调试接口，导致攻击者可以获取设备运行信息。

- 非法更新

物联网设备的更新验证机制不健全，攻击者会将存在漏洞或包含恶意文件的非官方固件植入到设备中。

- 过期组件

物联网设备出厂时内置了存在已知漏洞的组件或过期组件，由于过期组件不再被维护，会存在极大的安全风险。

- 恶意软件

物联网设备由于性能限制缺乏安全软件防护，容易被恶意软件感染，影响设备的正常运行。

传输层威胁

- 网络攻击

网络协议本身存在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、重放、篡改和窃听等中间人攻击。

- 数据泄漏

设备、云端以及移动应用端通信传输时，控制命令和采集的数据没有加密，攻击者可通过监听传输信道窃取敏感信息。

- 数据篡改

设备在网络通信时，网络传输数据没有进行完整性校验，控制命令和采集的数据可能会被攻击者篡改。

应用层威胁

- 设备管理

应用层所管理的设备分散、繁多，设备的升级过程和安全状态等难以管理。

- 越权操作

由于应用层权限管理不完善，可能存在越权问题导致重要数据被泄露。

- 系统漏洞

物联网设备的应用软件或操作系统软件存在逻辑设计的缺陷或错误，攻击者通过漏洞植入木马病毒导致设备无法正常运行。

- 数据泄漏

应用层管理大量的数据，如果不做加密处理或访问权限控制容易造成数据泄漏。

- 过期组件

应用层使用了包含已知漏洞的组件或过期组件，如果组件更新不及时，组件本身存在的漏洞易被利用。

- 配置漏洞

对应用程序、框架、容器和操作系统等执行配置时，由于配置不当导致出现安全漏洞，如使用存在安全缺陷的版本、给某些账户过高的权限、对敏感资源未做访问控制等，攻击者可非法获取重要数据。

在深入思考物联网环境中的诸多安全性隐患后，结合物联网设备在软硬件环境、计算能力等方面的复杂性，海康威视设计了以视频为核心的物联网安全解决方案，力求打造出全新的安全架构，建立多维度的安全体系，充分保障终端安全、数据安全、应用安全、网络安全、个人信息保护以及安全合规。

2 产品安全架构

产品安全架构分别从终端安全、网络安全、应用安全、数据安全和安全运营五个维度保障产品安全，在这五个维度中，运用了大量的安全技术手段。同时，所运用的安全技术均符合所在国家的法律法规要求，满足安全合规性要求。

图 2-1 产品安全架构模型

2.1 终端安全

终端安全旨在确保每台海康威视设备的所有核心组件都能为软件和硬件提供安全保护。海康威视设备的硬件和软件实现了紧密集成，可确保系统的每个组件均获得信任，并对系统进行整体验证。从初始启动到软件更新，每个步骤都经过分析和审查。

安全芯片

为满足设备的高安全需求，海康威视充分利用设备主控芯片的安全特性，如 OTP、TrustZone 等，并结合使用高性能安全芯片实现硬件级的高强度安全，为设备的安全启动、安全升级、码流加密等功能提供坚实的基础。

安全芯片所有加密解密动作都在芯片内部进行，密钥不会以明文形式出现在安全芯片外部或暴露给其他组件、软件、程序或个人。

TrustZone 是 ARM 在处理器中提供的安全技术，为设计具有高度安全性的嵌入式系统提供基础。TrustZone 将硬件和软件资源划分为两个执行环境：安全环境（Secure world）和普通环境（Normal world）。通过硬件逻辑进行物理隔离，把敏感资源和机密资源放到安全环境中，降低其受到攻击的可能性。

在物联网设备上，资源和性能至关重要。加密操作非常复杂，如果在设计和实施时未考虑这两个重要因素，可能会带来一些体验或性能方面的问题。海康威视设备配备的密码模块综合考虑这两个因素，可以实现更高效的数据加密，且支持国际密码算法和商用密码算法。

安全芯片自带硬件真随机数生成器，确保设备中的密钥、随机数据等具有较高的随机性。

安全启动

安全启动是终端安全的基石。

安全启动的代码固化在芯片内部，确保起始加载逻辑无法被篡改。设备启动后，会立即执行只读内存（称为 Boot ROM）中的启动代码。Boot ROM 代码使用海康威视固件签名公钥验证底层引导加载程序（Bootloader）是否经过签名，以决定是否允许其加载。启动过程每个步骤包含的组件都经数字签名以确保其完整性，只有在验证通过后，每个步骤

才能继续，形成安全启动链。启动过程包括的程序主要有引导加载程序、内核、应用程序等。安全启动链有助于确保软件未被篡改。

如果该启动过程中某个步骤无法加载或验证失败，启动过程会停止。设备将无法进行工作。

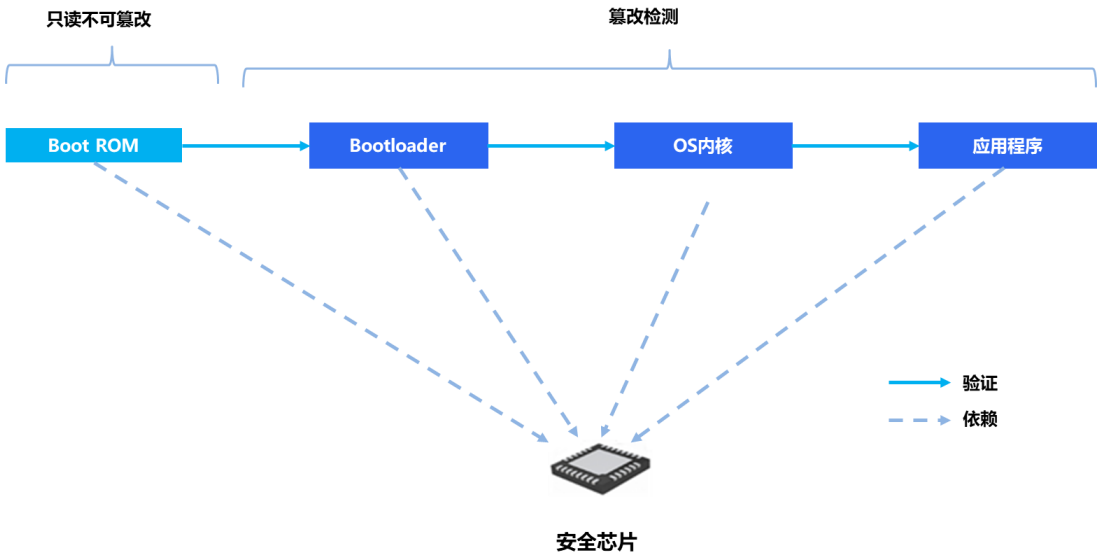


图 2-2 安全启动过程

安全更新

海康威视会及时发布软件更新以解决新出现的安全性问题。用户可在设备上和客户端软件中看到固件更新通知，我们鼓励用户尽快应用最新的固件进行安全性修正。

设备端获取软件更新信息的传输过程采用安全通信机制（如 HTTPS），有效保证固件更新包的数据保密性和完整性。

海康威视在设备固件更新包中携带数字签名，用于设备对固件更新包的来源和完整性进行校验，有效避免非法固件更新包。

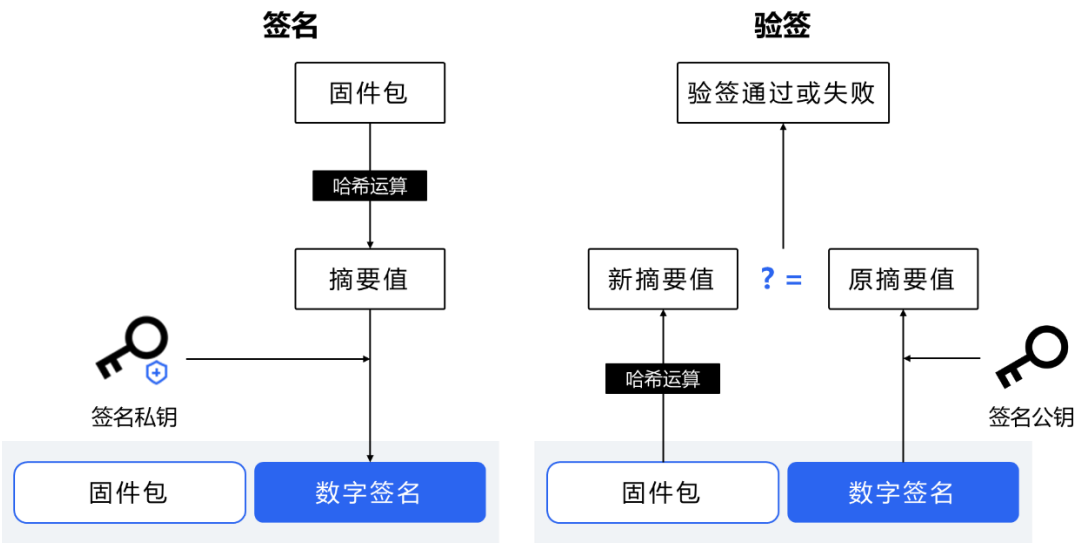


图 2-3 数字签名与签名验证过程

海康威视采用了防降级机制，避免设备降级为可能存在安全风险的早期版本。如果可以将设备降级，攻击者一旦有了设备的控制权，便会安装早期版本的固件，并利用其中未修复的漏洞来进行破坏。

口令安全

海康威视的设备账号安全体系依托于一系列口令策略和访问控制策略，充分保障用户账号安全：

- 用户口令复杂度要求：用户账号的口令具有复杂度要求，至少要求 8 个字符或以上，且包含两种以上不同类型的字符类型(数字、大小写字母、特殊符号)。
- 激活机制：用户首次访问设备时，强制要求设置符合安全要求的口令来激活设备，避免默认口令问题。
- 非法登录监测：监控非法登录尝试，同时提供账户多次登录失败锁定功能，有效阻止暴力攻击；最大连续登录失败尝试次数可配置、锁定时间可配置。

安全 shell

为了满足调试维护的要求，设备支持通过安全的 SSH 协议远程登录，对传输的数据进行加密保护。SSH 协议采用安全机制更完善的 SSHv2。

在设备上 SSH 服务是默认关闭的，只有管理员才有权限开启和关闭 SSH。

IP 过滤

海康威视设备支持 IP 过滤白名单技术：

- 过滤掉非法客户端对象，只允许合法的客户端对象，减小主机面临的威胁。
- 在设备面临攻击时可以完成特定的防御动作，提高设备应对风险能力。

2.2 应用安全

应用代码签名

设备内核启动后，它将控制哪些用户进程和应用可以运行。为确保所有应用均来自批准的已知来源并且未被篡改，要求所有可执行代码均使用海康威视认可的证书进行签名。强制性代码签名将信任链的概念从操作系统扩展至应用，可有效避免非法应用运行。

通过代码签名可以保护设备不受攻击，保证所有运行的代码都是被授权的，保证恶意代码无法运行。相较于互联网，物联网中的代码签名技术不仅可以应用在应用级别，还可以应用在固件级别，所有的重要设备，包括传感器、交换机等都要保证所有在上面运行的代码都经过签名，没有被签名的代码不能运行。

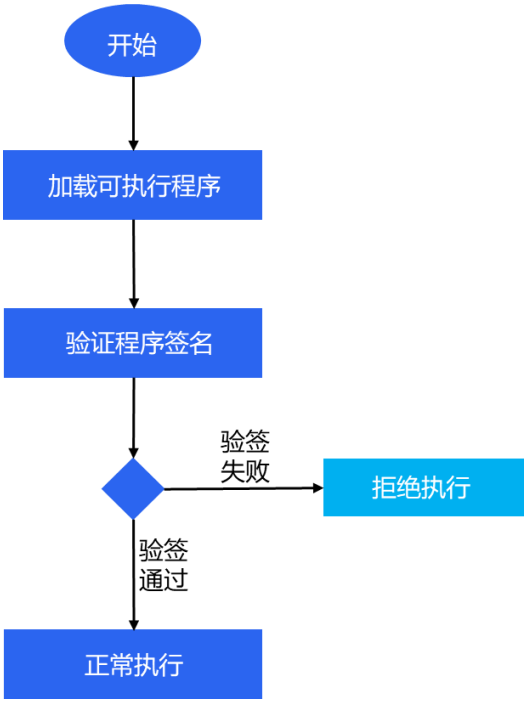


图 2-4 应用代码验证签名过程

由于物联网中的一些嵌入式设备资源受限，其处理器能力，通信能力，存储空间有限，海康威视建立了一套适合物联网自身特点的、综合考虑安全性、效率和性能的代码签名机制。

身份鉴别

身份管理系统定义和管理了每个用户的身份角色及所需资源的访问权限，并根据用户身份角色生命周期，对其所需资源访问权限进行动态管理，实现统一身份管理、统一身份鉴别、统一访问控制和权限合规管理等功能：

- 确保用户身份整个全生命周期内用户标识的唯一性。
- 访问控制：提供访问控制功能，采用角色来分配不同用户的权限，控制登录用户的权限。
- 双因子认证：可选支持基于数字证书的双因子认证，提供更高安全性的身份认证。

权限管理

海康威视对应用的访问权限进行限定，进行权限分类、分级，按业务相关性、最小授权原则配置权限，只有得到授权的用户才能登陆或访问。

访问控制

海康威视的设备均支持用户权限与访问控制管理，提供多维度的用户操作和设备访问控制的安全保障：

- 用户权限分级：设备提供用户权限角色划分，区分管理员、普通用户等不同的角色权限。
- 用户操作控制：针对用户对设备的操作，对用户的敏感行为（比如对设备进行控制、修改设备属性等）进行访问控制，可以有效防止敏感信息被越权访问，敏感操作被越权使用。
- 最小授权：所有操作权限均为细粒度，每个用户的所有操作权限都可以单独设置。避免用户误操作或其身份被假冒而带来的安全风险。

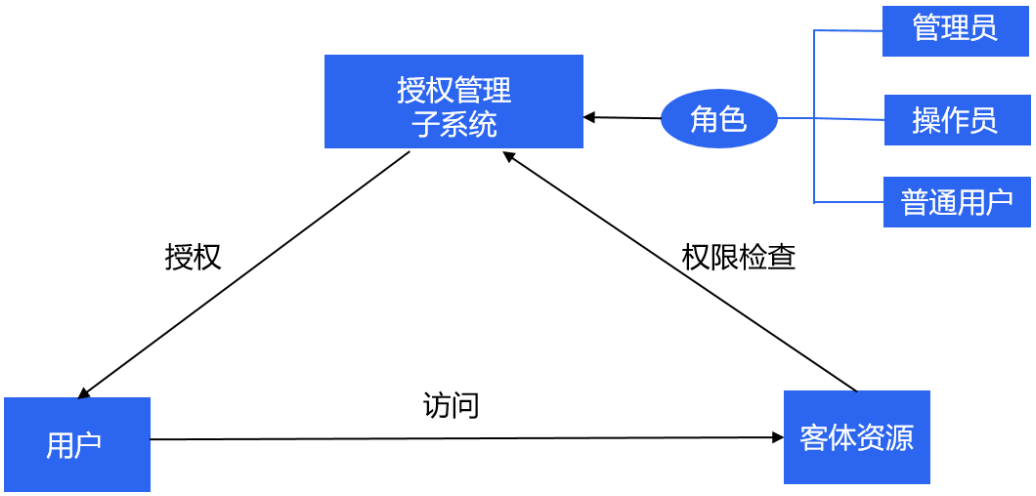


图 2-5 用户权限与设备访问控制管理

Web 安全

海康威视对所有 Web 系统进行全面的安全防御，为用户提供全方位的安全保障，包括但不限于：

- 在服务端对所有来自不可信数据源的数据进行校验，拒绝任何没有通过校验的数据。若输出到客户端的数据来自不可信的数据源，则对该数据进行相应的编码或转义。
- 用户访问/操作权限强校验，防止横向/纵向越权。
- 对上传文件的类型、格式、内容、大小等关键信息进行合法性检测，避免恶意文件上传。
- 敏感信息加密和数据的权限管控，防止未授权访问和信息泄露。
- 对服务端接受的请求进行来源识别和内容检测，杜绝各类请求伪造攻击。
- 根据不同的应用场景，按照安全配置基线严格审计 Web 容器配置，保证配置安全。
- Web 应用程序的会话标识具备随机性、唯一性，身份验证成功后，更换会话标识，防止会话固定。
- 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。

组件安全

海康威视在进行产品架构设计前，会先对产品开发中所涉及的开源及第三方软件进行选型安全分析，包括开源及第三方软件本身所涉及的开源协议是否合规、是否存在未修复的安全漏洞、可能存在的安全风险等情况进行分析，严格遵循“先申请再引入”原则。

在提交测试时，测试团队会对开源及第三方软件的源码一致性进行分析验证，并对软件进行安全扫描，检测设备中是否存在旧的组件或存在未修复漏洞的组件，如早期版本的组件、存在 CVE 漏洞的组件等，并进行相应整改，保证设备发布版本中开源及第三方软件的安全性。

API 安全

在物联网产品中存在各种 API 互相调用访问，应防止接口被滥用。对于 API 安全可以包括但不限于以下功能：

- 在调用 API 时提供认证机制对接入开放 API 的用户进行身份标识和鉴别，并对访问权限进行管理。
- 对于 API 的访问使用基于安全协议的访问，如 HTTPS、SSL/TLS 等安全协议。
- 对 API 访问采用速率限制并设置访问配额。
- 对 API 调用使用输入和输出校验组件，对接口不安全输入参数进行限制或过滤，为接口提供异常处理能力，防止注入攻击。
- 对 API 的调用访问应提供日志用于事后审计。

安全函数

由于 C/C++语言中没有内置边界检查机制，同时标准函数库提供的许多函数并不会检查溢出的情况，如 memcpy()、strcat()、strcpy()、sprintf()、gets()等。当这些函数因为使用不当，或函数的参数由恶意用户以某种形式恶意输入，则很有可能造成缓冲区溢出的漏洞，导致程序运行终止甚至危险代码被执行，带来严重的安全问题。习惯上把这类函数称作危险函数。

为了避免使用了危险函数的代码带来各种漏洞，海康基于标准库的函数进行封装，加上校验和规避的措施，推出海康安全函数库。公司通过自研代码静态扫描平台可以较为完整的对危险函数进行检测，确保安全函数在实际产品中的落地。

2.3 网络安全

物联网发展初期，物联网终端和网络大多都是设计在孤立环境中运行的，安全机制相对薄弱。随着物联网的逐步发展，这些终端和网络将被逐步接入到互联网中，这会引入新的安全问题。

除了用于保护设备上所储存数据的内置安全保护，也有许多网络安全措施可供提升信息在来往于设备时的安全性。为了实现这些安全目标，海康威视集成了经验证的安全技术和最新标准来进行数据网络连接。

安全传输协议

海康威视所有产品的网络传输数据支持安全传输协议：HTTPS、TLS、DTLS。

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
- Syslog 协议支持基于 TLS 或 DTLS 传输
- 使用安全的算法套件

安全网络服务

海康威视所有产品默认关闭各类管理协议，并支持安全协议版本，以减小设备威胁面：

- 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

无线安全

海康威视设备支持工业标准的无线协议，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。由于支持 802.1X，海康威视设备可集成到各种 RADIUS 认证环境中。

端口安全

海康威视对外发布的所有产品默认只开放与客户需求直接相关的端口，关闭其他端口，并在产品通信矩阵中说明可开放的所有端口、端口对应的业务功能、端口对应的认证方式、端口是否默认开启等信息，供客户了解及调整。

2.4 数据安全

数据生命周期安全管理

公司的产品或服务团队应在需求分析和设计阶段考虑个人信息保护，根据具体的业务使用场景，使用适当的技术和管理措施保证个人数据的安全。如海康威视涉及处理个人信息，均在相应的产品界面中提供产品个人信息声明，描述产品涉及所有个人数据类型、目的、处理方式、留存期、风险或建议。

个人数据主体具有知情权、访问权、纠正权、删除权（被遗忘权）、限制处理权、可携带权、拒绝权、不受自动化处理约束等权利。为了合规和更好的保护用户个人信息安全，在设计、实现产品和服务时，应纳入支持个人数据主体行使上述权利的功能。

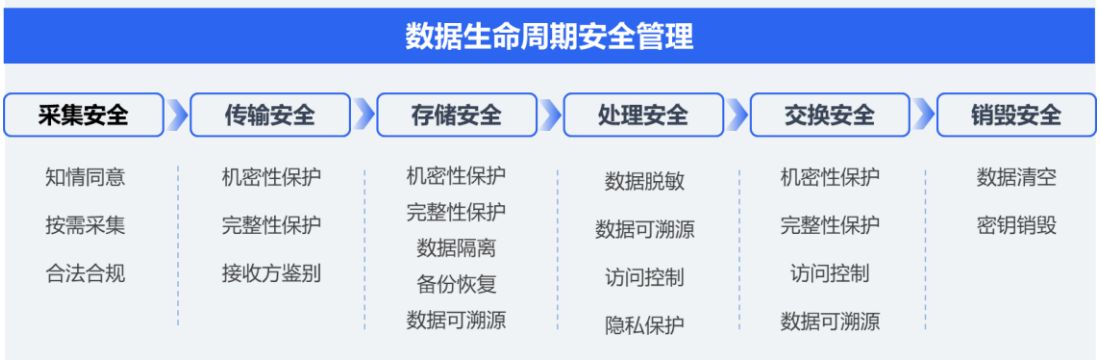


图 2-6 数据生命周期安全管理

1、数据采集安全

按照相应法律法规要求在进行数据采集时，特别是涉及个人数据时，须让用户知情，须遵循用户同意、最小化采集等原则，按需采集所需数据，并且在个人信息政策中明确说明收集范围和使用目的。在用户使用海康威视云服务、IoT 设备等涉及到个人数据的服务或产品时，海康威视会依据所适用的法律法规，在个人信息政策中告知用户收集范围和目的，获得用户授权后按需采集个人数据。

2、数据传输安全

在对采集数据进行传输时，对通信双方进行身份鉴别，确保接收或发送数据的实体是合法用户，此时主要使用摘要认证、数字签名等密码技术来实现身份鉴别。传输过程中通过加密、哈希、数字签名等密码技术确保传输过程中数据内容不被泄露，并保持对数据内容篡改的及时感知。海康威视相关产品在实现数据传输安全时，使用 SSL/TLS 协议保证数据的机密性和完整性。

3、数据存储安全

数据存储时根据数据的敏感级别进行分级隔离存储，可以使用物理隔离、逻辑隔离或虚拟化等相关技术实现不同等级数据所在区域之间的隔离。

数据存储介质可能存在无法正常工作、甚至数据丢失的情况，为了保证存储数据的可用性，需要使用冗余机制对数据进行备份，当数据存储介质重新恢复可用时对数据进行恢复还原。

数据存储后需要支持数据可溯源，根据实际业务场景使用数字水印相关技术保证数据被非法泄露后可溯源，能够追踪到泄露源头并进行相关审计。

数据存储时可使用加密、哈希、数字签名等密码技术来保证数据的机密性和完整性，保证数据被攻击者窃取的情况下也无法获取数据信息，且被非法篡改后能够被感知。

海康威视相关产品实现数据存储安全时，使用标准的密码算法对数据进行机密性和完整性保护，提供商密算法的计算模块使用符合商密规范的密码卡实现。

4、数据处理安全

在对数据进行处理和计算时，需要保证数据的使用者具有对应的权限。使用数据时，应根据业务相关性，基于最小必要原则，对敏感数据进行脱敏处理。在对数据计算时，要保证不能从数据中间结果中得出额外的个人信息，可使用隐私计算相关技术实现数据使用过程中的个人信息保护，例如安全多方计算、同态加密、差分隐私计算等技术。海康威视相关产品对数据处理时会对敏感数据进行数据脱敏、使用密码技术进行加密、使用隐私计算相关技术实现计算过程中的个人信息保护。

5、数据交换安全

在数据进行交互共享时，需要对数据交换渠道进行安全管控，如强制身份验证、严格访问控制等，并采用数据水印等方式实现对数据交换过程中的数据溯源。海康威视相关产品在对数据交互时，使用密码技术保证数据的机密性、完整性和访问控制，使用数字水印技术对数据添加水印实现数据可溯源。

6、数据销毁安全

对数据进行销毁时需要通过逻辑删除、物理销毁等方式，确保数据清除后无法被复原或再次检索到，尤其是口令、密钥等敏感数据。

用户数据保护

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敏感信息。数据加密密钥在设备第一次启动时由随机数生成器随机生成，实现一机一密。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。用户配置数

据主要包括用户的配置参数、使用信息等；用户敏感信息包含但不限于用户口令、密钥等。

存储介质加密

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。尤其是可插拔存储介质上的关键数据（如音视频数据）进行加密。可插拔存储介质包括 TF/SD 卡、硬盘等。

音视频数据安全

音视频数据的安全是视频监控系统的重点，数据在感知层、传输层、应用层都存在被篡改、非法查看的风险。海康威视设备支持分别在音视频编码阶段和网络传输阶段进行安全保护。

- 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。

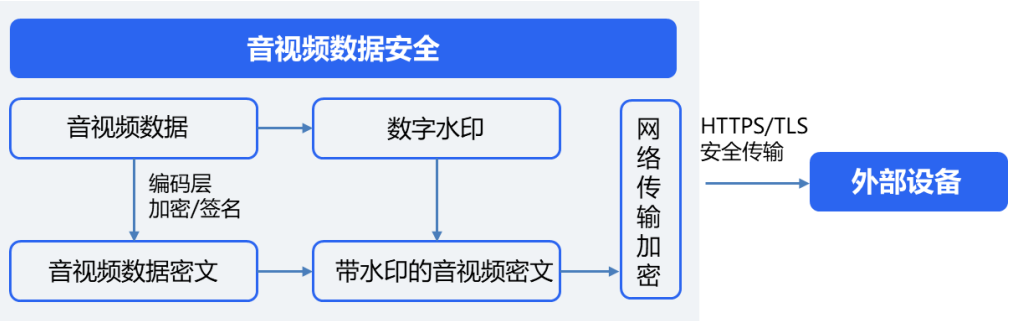


图 2-7 音视频数据加密传输过程

数字水印

数据水印，主要是指基于信息安全、信息隐藏、数据加密等技术，在数据文件(如视频、音频、图片、文档、数据库、模型等)嵌入显式或隐式标记，以应对数据泄露后的溯源查询和版权宣示。

数字水印系统，主要包含嵌入和提取两个阶段。在嵌入阶段，嵌入算法的主要目标是使数字水印在不可见性和鲁棒性之间找到一个较好的折衷点。提取阶段主要是设计一个相应于嵌入过程的提取算法。同时，为了防止攻击者去除水印，目前大部分水印方案都在嵌入、提取时采用密钥，只有掌握密钥的人才能读出水印。

数据水印是抵抗数据泄露的“最后一道防线”。因此从水印技术本身来说，它具有广泛的应用前景和巨大的经济价值。

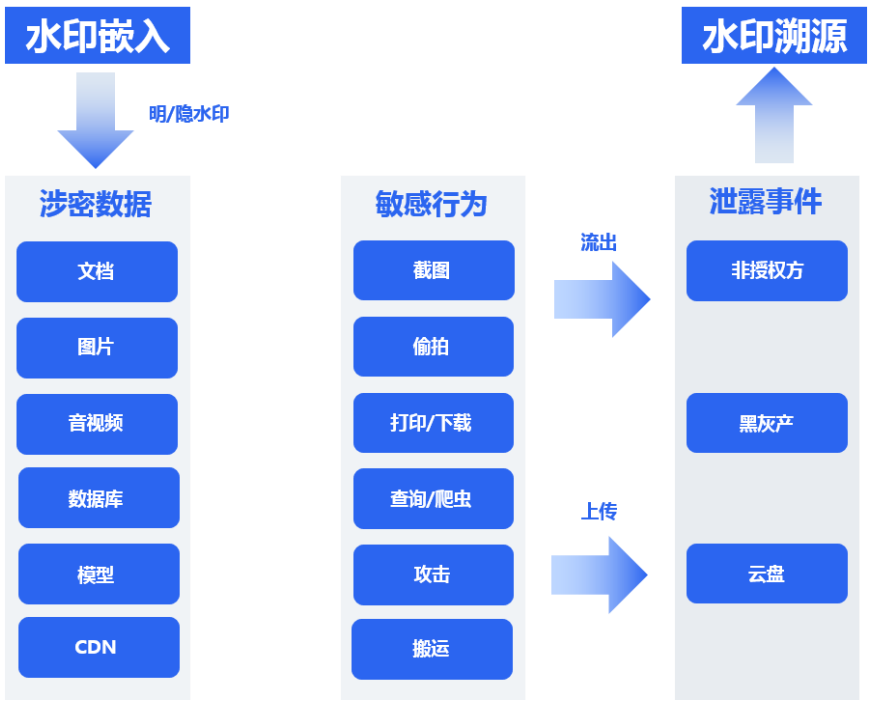


图 2-8 数字水印

白盒加密

白盒加密就是一种抵御白盒攻击的技术，能够保护密钥的安全，使得攻击者难以从中间数据中分析出密钥。白盒加密按照实现方式可分为静态白盒和动态白盒。

静态白盒：密钥经过处理混淆生成查找表，最后得到静态白盒库。使用时直接调用静态白盒库进行加密解密。由于静态白盒库中的运算都是经过查找表方式实现的，所以攻击者无法通过分析中间数据推导出密钥，使用者也无需维护密钥。但是如果更换了密钥，那么静态库也需要重新编译。

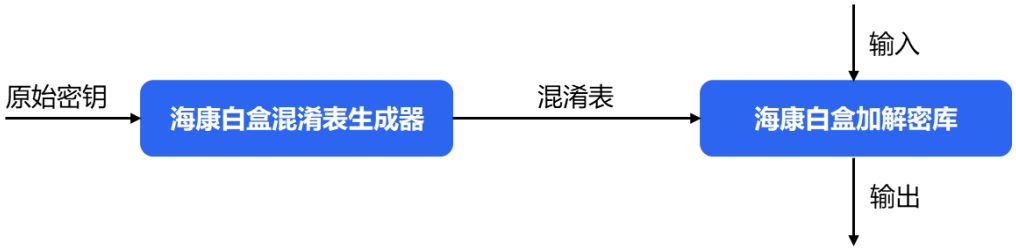


图 2-9 静态白盒使用过程

动态白盒：动态白盒在使用中，如果密钥修改，无需重新生成白盒库。首先需要生成非线性混淆查找表，该查找表供白盒密钥生成工具和白盒库使用。原始密钥经过密钥生成工具产生白盒密钥，使用者只需使用白盒密钥以及白盒库就能进行加密解密。如果要更换密钥，只需在服务端生成新的白盒密钥即可使用，无需更换白盒库。

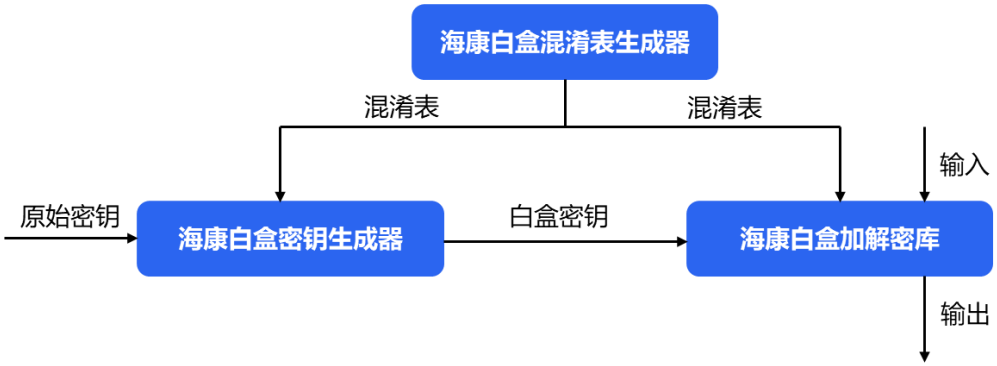


图 2-10 动态白盒使用过程

密钥管理

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。

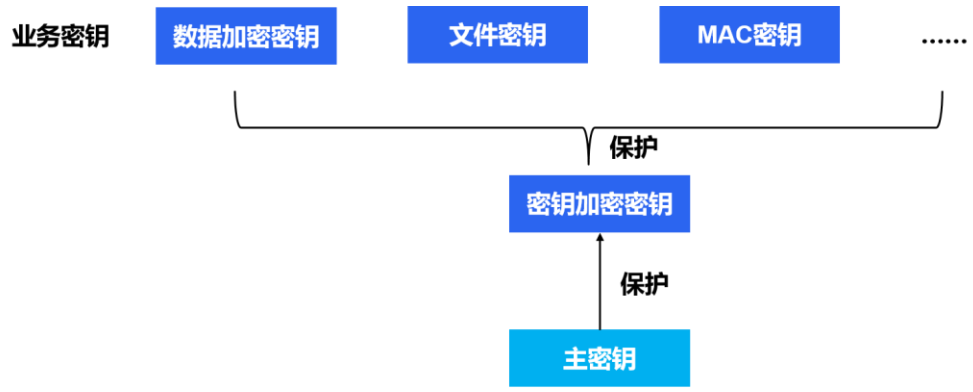


图 2-11 密钥分层管理

2.5 安全运营

安全审计

海康威视的安全审计日志覆盖产品安全活动相关的详细记录，包括审计所需要的信息，识别各类异常事件。生成的结果报表可以使所有数据活动详细可见，比如登录失败、配置变更、用户管理、设备升级维护、接入失败等，并保证所有用户操作可查询。

此外，确保审计进程无法中断，无法删除、修改、覆盖审计记录，同时具备异常事件报警功能。

支持利用密码技术保护设备存储在本地的日志数据，避免非法查看及篡改。设备支持 syslog 协议，实时将日志数据安全上传到日志服务器集中存储。

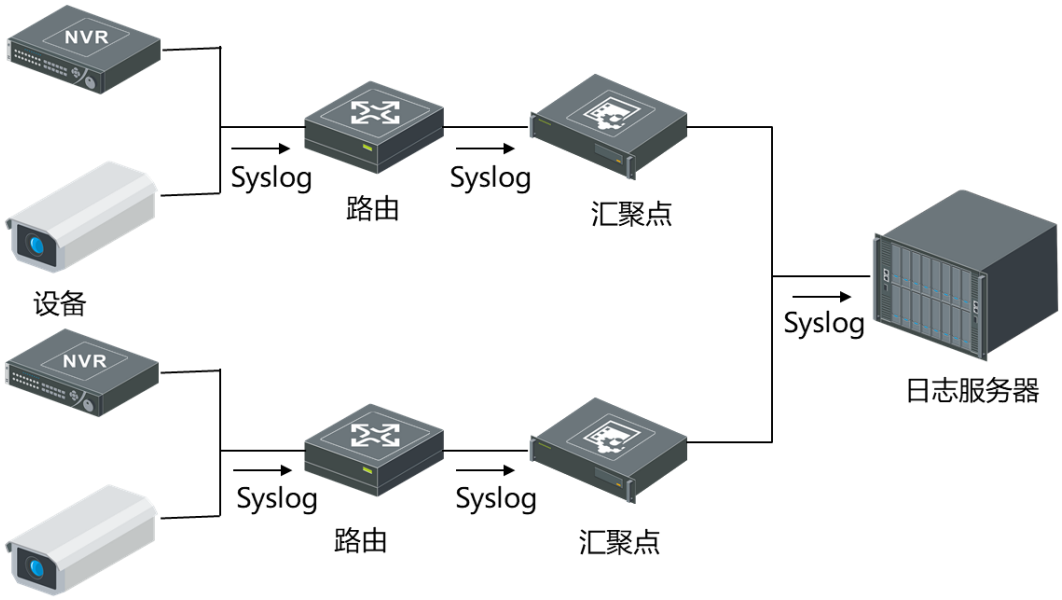


图 2-12 syslog 日志管理服务

日志传输支持通过 TLS 方式对 syslog 协议提供传输层加密及认证，保证网络传输的安全性。

安全加固

应定期对各类设备或系统进行安全加固，如更新配置、安装安全补丁等。遇到紧急事件，应立即采取加固措施，修补漏洞。漏洞扫描可提供操作系统、软件、弱口令、端口等综合漏洞探测服务，检查、评估系统内各个环节运行的系统、应用的安全状态，及时发现可能存在的安全漏洞。

例如，对操作系统的基础安全加固可以包含如下内容：

- 最小化服务：禁用多余或危险的系统后台进程和服务，如邮件代理、图形桌面、Telnet、编译工具等。
- 服务加固：对 SSH、Web 等常用服务进行安全加固。
- 内核参数调整：修改内核参数，增强操作系统安全性，如禁用 IP 转发、禁止响应广播请求、禁止接受/转发 ICMP 重定向消息。
- 文件目录权限设置：结合业界加固规范及应用要求，保证文件权限最小化。
- 账号口令安全：启动口令复杂度检查、口令有效期、登录失败重试次数等。
- 系统认证和授权：禁止 root 远程登录、尽量不用 root 账号安装运行进程。
- 日志和审计：记录服务、内核进程运行日志，可以与日志服务器对接。

应急响应

海康威视成立了安全应急响应中心（Hikvision Security Response Center，以下简称：HSRC），负责接收、处理和披露海康威视产品和业务相关的安全漏洞的应急响应工作，其职责还包括：

- 响应和处理客户提交的安全事件
- 响应和处理外部机构提交的安全事件
- 制定公司安全事件管理策略和安全事件处理方案
- 分析软件供应链和安全机构发布的漏洞预警及安全补丁

另外，公司还规定产品和业务相关安全事件管理的流程和各部门职责，保证产品安全事件管理的质量和效率。管理规范覆盖公司产品安全工作的售前、售中、售后全部过程，包括客户安全专题交流、安全组织合作、应急响应管理、安全公告推送、法律合规的流程和实施细则。

海康威视是国家互联网应急中心、工业信息安全产业发展联盟安全应急服务支撑单位的重要成员，与全球范围内的其他优秀会员单位共享安全应急的最佳实践和处置经验，增进可信沟通和合作，提升公司对安全事件应对的有效性和及时性。

图 2-13 安全应急响应

3 安全合规

商用密码产品型号

海康威视在商用密码算法（SM1、SM2、SM3、SM4、SM7、SM9）使用上，严格遵守国家相关法律法规、标准规范，确保合法合规安全的使用商用密码算法。目前主流产品均已通过商用密码产品认证[5]：

- 网络摄像机（密码模块）
- 网络存储设备（密码模块）
- 视频安全门禁系统
- 软件密码模块
- 视频数据传输加密网关
- 签名验签服务器
- 服务器密码机
- PCI-E 密码卡

同时，海康威视是密码行业标准化委员会会员，积极参与商用密码标准的评审、制定工作。

通用标准认证 CC

通用标准认证 CC(Common Criteria ISO/IEC 15408)是信息技术安全领域认可度最高的国际性认证之一，得到美国国家信息安全保障合作计划的认可（该计划受美国国家技

[5] 商用密码产品认证证书查询： https://www.scctc.org.cn/xxfb/rzyw/rzzscx/jzcxjg/

术与标准研究院监督），同时也被英国、加拿大及其他西方国家所认可。目前全球已有来自 31 个国家的安全认证机构加入了 CC 互认协定（CCRA）。由于 CCRA 成员均为其所在国的政府主管部门或第三方权威机构，因此 CC 认证在全球范围内具有很高的接受度与可信度，成为安全性评估的重要依据。

CC 认证主要用于评估信息技术产品或解决方案的安全性、可靠性，以及对信息隐私的保护。按评估保证级别，该认证分为七个级别，从 EAL1 到 EAL7，对应的验证要求依次增高。

2018 年 9 月，海康威视 2 个系列的摄像机产品成功通过 EAL2+级别认证[6]；2022 年 6 月，3 个系列的摄像机产品成功通过 EAL3+级别认证。海康威视也致力于将 EAL3+的标准适用到所有产品，让公司的安全实践达到新的高度，在安防行业内树立良好示范。

网络安全标签计划 CLS

为了应对日益增长的网络安全威胁，新加坡网络安全局（CSA）在 2020 年启动了网络安全标签计划（Cybersecurity Labelling Scheme，CLS）。CLS 根据消费级物联网设备抵御网络攻击的能力对其进行评级，总共划分为四个安全等级，从 Level 1 到 Level 4 对应的验证要求依次增高。

2023 年 9 月，海康威视 4 个系列摄像机产品成功通过 CLS Level 4 认证。

[6] CC 证书查询： https://www.commoncriteriaportal.org/

4 典型安全实践

4.1 物联网产品安全设计实践

海康威视涉及的产品繁多，以智能摄像机场景为例，智能摄像机作为数据业务的视频数据采集端，从前端的安全防护、云端存储的数据安全管控，始终坚持纵深防御原则，保证产品的安全合规、数据不丢失、信息不泄露、事后可追溯。

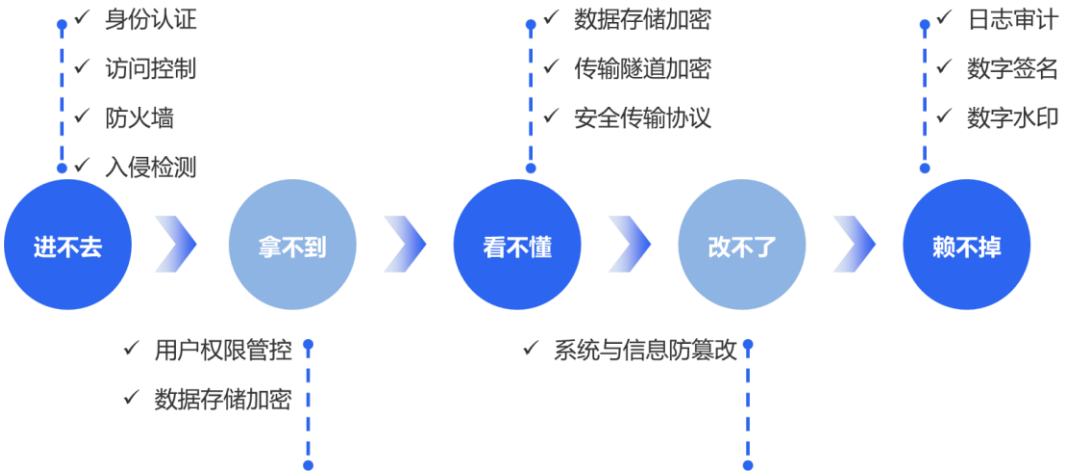


图 4-1 物联网产品安全设计实践参考

4.2 智能物联网安全管控实践

随着物联网的快速发展，物联网安全问题也日益突出：

- 物联终端易存在弱口令、漏洞风险，导致非法侵入、数据窃取等安全问题。
- 物联终端数量多、分布广，终端配置问题难以核查。
- 物联设备自身安全策略管理及口令运维难度大。
- 物联设备部署分散，易被替换和仿冒，成为黑客入侵跳板。
- 物联网设备易被黑客利用，恶意代码、非法入侵防不胜防。
- 安全态势无法感知，异常操作、威胁事件响应不及时，导致安全问题频繁发生。

- 密码设备、密钥等无法实时监测，密码安全态势事件无法集中展示。

海康威视智能物联网防护方案包含物联网安全态势感知平台、物联网全流量威胁探针、视频防火墙、安全准入控制系统、设备安全管控系统、主机安全检测系统。

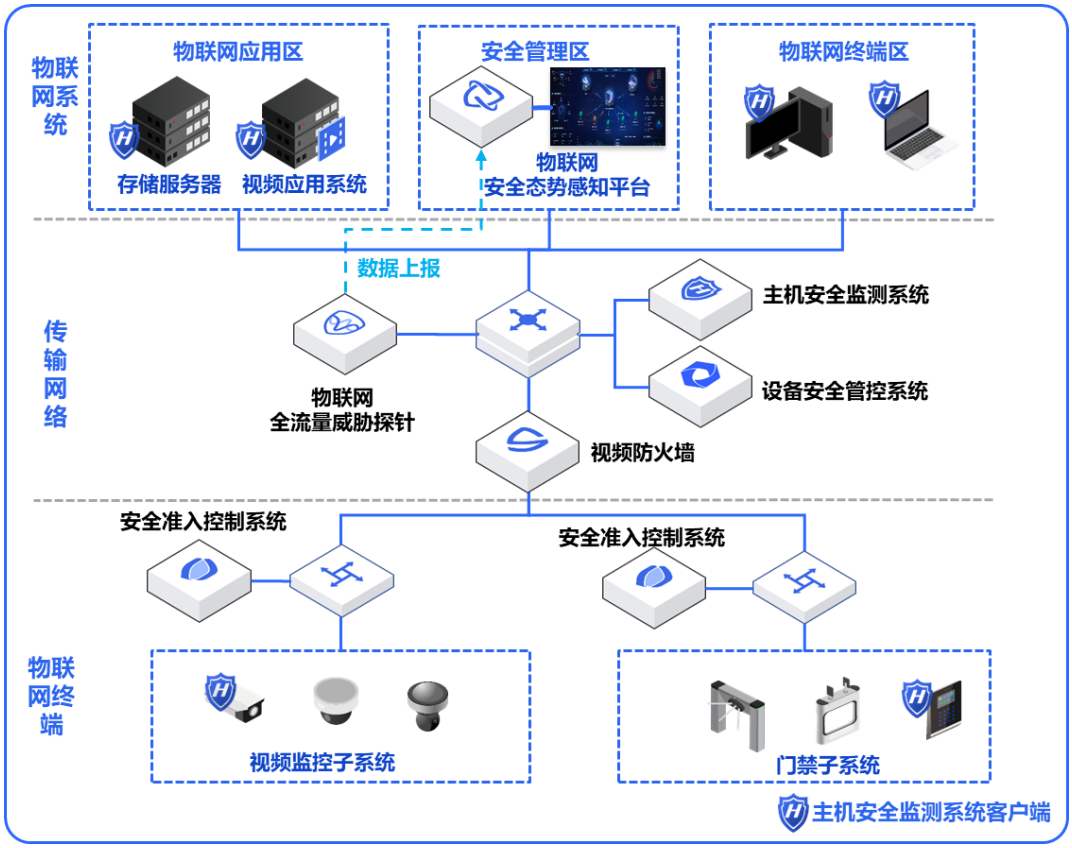


图 4-2 智能物联网安全管控方案

- 物联网安全态势感知平台实现全网资产及威胁可视化分析、安全态势可视化呈现。
- 物联网全流量威胁探针实现视频流量精细化安全审计。
- 视频防火墙实现网络威胁高效检测及响应。
- 安全准入控制系统实现物联终端统一安全管理、实现前端设备安全准入控制。
- 主机安全监测系统实现物联终端基线配置核查、终端漏洞高效检出修复。
- 设备安全管控系统实现终端口令自动化运维、安全策略远程实时下发。

4.3 视频云存储安全实践

海康威视视频云存储是一款以视频存储技术为核心，将云存储技术与安防行业智能应用深度融合，实现视频、图片、文件、对象数据融合存储的云存储设备。海康视频云存储设备有长期和大量行业落地应用经验，目前已服务有上万个安防专用视频云存储项目。在数据存储安全方面，海康视频云存储在链路传输安全、主机系统安全、数据存储安全、系统访问安全等方面保障数据存储的安全性。

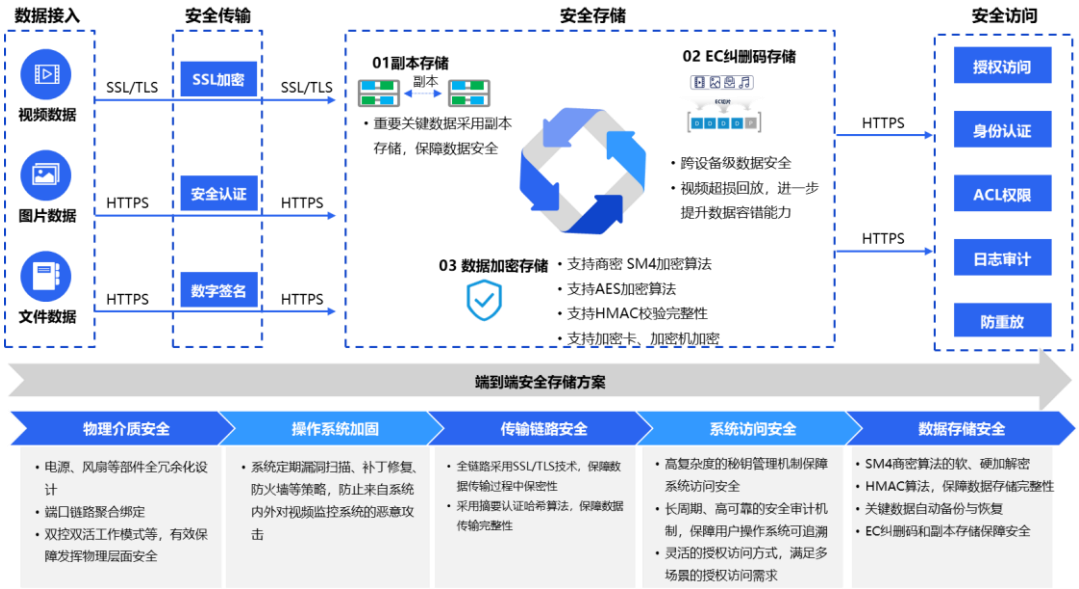


图 4-3 多级数据安全保障

5 安全性承诺与建议

海康威视致力于使用领先的安全及个人信息保护技术来帮助客户保护其个人信息，以及采用全面的方法来保护用户的数据。

海康威视在整个智能物联网应用生态系统中使用统一的集成安全基础架构。海康威视拥有一支专业的安全团队，负责为所有海康威视产品提供支持。该团队为开发中和已发布的产品提供安全审核和测试。安全团队还提供安全培训，并积极监控新增安全问题和威胁的报告。

产品安全不仅需要厂商在研发、生产、交付及维护等环节的持续努力与提升，同时也需要客户的积极参与，持续关注与改善产品的使用环境和使用方式，确保产品交付使用后的安全运营，为此，我们建议用户安全使用设备，包括但不限于：

1、账户安全

- 使用复杂口令，建议口令设置如下：
  - ✓ 口令长度不少于 8 个字符。
  - ✓ 至少包含两种类型的字符类型(数字、大小写字母、特殊符号)。
  - ✓ 不要使用风险口令，风险口令包括但不限于中口令中包含用户名或用户名的倒序、连续四位及以上递增或递减数字、连续四位及以上相同字符。
  - ✓ 杜绝使用默认口令。
- 定期更新口令

  建议您定期更新设备口令，降低口令被泄露或破解的风险。
- 合理分配账号并设置权限

根据实际业务场景，合理新增账户，并基于最小授权原则配置权限。

2、安全配置

- 默认使用安全协议

建议您默认使用 HTTPS 访问 Web 服务。

- 音视频加密传输

如果您的音视频数据内容比较重要或敏感，建议启用音视频编码加密和网络传输加密以降低音视频数据在编码或传输阶段被篡改、非法查看的风险。

- 默认关闭不安全服务

默认关闭各类管理协议如 Telnet 服务、FTP 服务、SNMP 服务、UPNP 服务等，以减小设备威胁面。

- 禁用不必要的功能和服务

许多物联网设备提供了各种功能和服务，但并非所有都是必需的，禁用不必要的功能和服务可以减少设备的攻击面。

- 端口配置安全

建议用户在做安全端口配置的时候仅开启业务必须的端口。

3、及时更新设备软件和固件

遵循行业的标准作业规范，设备软件和固件需及时更新至最新版本，以保证设备能及时修复已知的安全漏洞，提升设备安全性。若设备接入公网时，建议开启在线升级自动检测功能，便于及时获知厂商发布的软件和固件更新信息。

4、安全审计

- 审查在线用户

建议您不定期审查在线用户，识别是否存在非法用户登录。

- 审查设备日志

通过审查日志，可获知尝试登录设备的 IP 信息、登录时间、登录结果及登录用户对设备进行的关键操作信息。

- 配置网络

由于设备本身存储容量限制，日志存储能力有限，建议您启动 syslog 日志管理能力，确保实时将日志数据安全上传到日志服务器集中存储，保证问题可追溯。

5、物理安全

建议您对设备（特别是存储类设备）进行物理防护，比如将设备放置在专用机房或机柜，并做好门禁权限和钥匙管理，防止未授权的人员进行破坏硬件、外界设备等物理攻击。

如需进一步了解如何向海康威视报告问题以及如何订阅安全通知，请参阅 https://www.hikvision.com/cn/support/CybersecurityCenter/

见远 行更远

See Far, Go Further

微信扫一扫
关注海康威视网络安全

海康威视

www.hikvision.com

客服热线：400-800-5998

股票代码：002415

微博：@海康威视hikvision