

The background of the entire page is a light gray circuit board pattern. It features a complex network of white lines representing traces, with numerous small white circles representing solder pads or vias. The pattern is dense and covers the entire surface, with a slight gradient from top to bottom.

HIKVISION

海康威视产品安全白皮书

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(<http://www.hikvision.com/cn/>)。

版权声明

© 2019 杭州海康威视数字技术股份有限公司。版权所有。

未经海康威视事先书面许可，任何公司或个人不得以任何方式复制、翻译、修改、分发本文档中的任何内容。

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

关于海康威视

海康威视是以视频为核心的物联网解决方案提供商，面向全球提供综合安防、智慧业务与大数据服务。

海康威视全球员工超 34000 人（截止 2018 年底），其中研发人员和技术服务人员超 16000 人，研发投入占企业销售额的 7-8%，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，以杭州为中心，建立辐射北京、上海、武汉以及加拿大蒙特利尔和英国伦敦的研发中心体系。海康威视拥有视音频编解码、视频图像处理、视音频数据存储等核心技术，及云计算、大数据、深度学习等前瞻技术，针对公安、交通、司法、文教卫、金融、能源和智能楼宇等众多行业提供专业的细分产品、IVM 智能可视化管理解决方案和大数据服务。在视频监控行业之外，海康威视基于视频技术，将业务延伸到智能家居、工业自动化和汽车电子等行业，为持续发展打开新的空间。

海康威视在中国大陆拥有 32 家省级业务中心/一级分公司，在境外建立了 44 个分支机构（截止 2018 年底），其产品和解决方案应用在 150 多个国家和地区，在 G20 杭州峰会、北京奥运会、上海世博会、APEC 会议、德国纽伦堡高铁站、韩国首尔平安城市等重大项目中发挥了极其重要的作用。

海康威视是全球视频监控数字化、网络化、高清智能化的见证者、践行者和重要推动者。

2011-2017 年蝉联 IHS Markit 全球视频监控市场占有率第 1 位¹；连年入选“国家重

¹ IHS Markit 是世界著名的三大咨询调查公司之一，官方网站 <https://www.ihs.com/>。

点软件企业”²、“中国软件收入前百家企业”³、a&s《安全自动化》“中国安防十大民族品牌”、CPS《中国公共安全》“中国安防百强”（位列榜首）；2016-2018年，a&s《安全自动化》公布的“全球安防50强”榜单中，蝉联全球第1位。

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，公司先后荣获“2016&2017 CCTV中国十佳上市公司”⁴、“中国中小板上市公司价值十强”⁵、“2016年A股上市公司未来价值排行以及A股最佳上市公司”榜首⁶、“第六届中国上市公司口碑榜最佳公司治理实践奖”⁷、“中国中小板上市公司投资者关系最佳董事会”⁸、“上市公司金牛投资价值奖”和“最佳投资者关系管理奖”⁹等重要荣誉。

海康威视秉承“专业、厚实、诚信”的经营理念，坚持将“成就客户、价值为本、诚信务实、追求卓越”核心价值观内化为行动准则，不断发展视频技术，服务人类。

² “国家重点软件企业”名单由国家发展改革委、工业和信息化部、商务部、国家税务总局等联合公布。

³ “中国软件收入前百家企业”由工业和信息化部发布。

⁴ 2016年12月12日，2016央视财经论坛暨中国上市公司峰会上正式发布了“2016CCTV中国十佳上市公司”榜单，海康威视位列其中。

⁵ 2016年9月，第十届中国上市公司价值评选，海康威视荣获“中国中小板上市公司价值五十强前十强”。

⁶ 2016年11月，第三届“2016A股上市公司未来成长价值排行榜暨行业先进性排序”，海康威视荣登2016年A股上市公司未来价值排行以及A股最佳上市公司榜首。

⁷ 2016年11月，由每日经济新闻主办“第六届中国上市公司领袖峰会”上颁发“中国上市公司口碑榜”九大奖项，海康威视获颁2016“最佳公司治理实践奖”。

⁸ 2016年4月，海康威视荣获证券时报、中国基金报颁发的“中国上市公司投资者关系天马奖——中国中小板上市公司投资者关系最佳董事会”。

⁹ 2017年8月15日，由中国证券报主办的“第十九届中国上市公司金牛奖颁奖典礼暨高端论坛”在贵阳举行，海康威视荣获“2016年度上市公司金牛投资价值奖”和“2016年度最佳投资者关系管理奖”。

目 录

关于海康威视.....	II
1 物联网安全威胁.....	IV
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
2.2 数据安全	9
2.3 应用安全	11
2.4 网络安全	15
2.5 隐私保护	18
2.6 安全合规	20
3 安全性承诺	23

1 物联网安全威胁

物联网（The 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。

物联网除了传统网络安全威胁之外，还存在着一些特殊安全问题。这是由于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、设备集群度高等，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资产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。

终端在户外、分散安装、易被接触到又没有纳入管理,导致物理攻击、篡改和仿冒。

➤ 数据泄露

敏感信息预置在设备中,易被读取或篡改。

基于数据的隐私威胁,物联网中数据采集和处理等过程中的隐私信息泄露。

➤ 非法接入

物联网环境中的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,但由于没有进行正确的安全保护,导致攻击者可以远程访问。调试接口没有限制代码执行的权限,导致攻击者访问该接口服务后就可以完全控制设备。

➤ 非法更新

物联网设备的更新验证机制不健全,非官方固件包易被直接更新进设备。非官方固件包未经验证,可能存在漏洞,或其本身就是恶意软件。

➤ 过期组件

物联网设备,出厂时,其上装载的组件就已经“过期”或即将过期。即使有些设备出厂的时候装载的是最新版本软件,但由于未及时更新,也可能在未来出现漏洞。因此,除非拥有持续的软件更新机制,否则物联网终端设备存在较高的软件漏洞风险。

➤ 恶意软件

OS 或软件过时,漏洞无法及时修复。设备的数量巨大使得常规的更新和维护操作面临挑战。

恶意软件可能会影响物联网设备的操作,获取未授权的访问或者实施攻击。例如引发大规模 DDoS 攻击的 Mirai、Bashlite、Lizkebab、Torlus、Gafgyt 等。

传输层威胁

➤ 网络攻击

通过无线接入渗透到网络，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、重放、篡改和窃听等中间人攻击。

IP 化后面临 IP 体系的安全问题：如来自互联网的攻击和入侵。

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。。

➤ 数据泄漏

设备和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。

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。

➤ 越权操作

权限管理不完善，越权访问导致隐私和安全凭证等重要数据有被泄露的风险。

➤ 系统漏洞

应用层的操作系统，大多为通用系统，如 Linux、Windows、Android 等，通常大规模网络攻击和漏洞利用均是系统漏洞问题。

➤ 数据泄漏

应用层管理大量的数据，不做加密处理，很容易产生数据泄漏。如直接拔走硬盘。

➤ 过期组件

应用层的组件数量，相对物联网设备要多出数倍。如组件更新不及时，组件本身存在的漏洞易被利用。

➤ 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而产生的。

➤ 非法更新

非官方软件未经验证直接更新，可能存在漏洞，或其本身就是恶意软件。

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，海康威视设计的以视频为核心的物联网解决方案，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、隐私保护以及安全合规。下面分 6 个部分详细介绍了安全技术和功能如何在海康威视物联网解决方案中得以实现。

2 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、网络安全和隐私保护五个方面保障产品安全，在这五个方面中，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。



2.1 终端安全

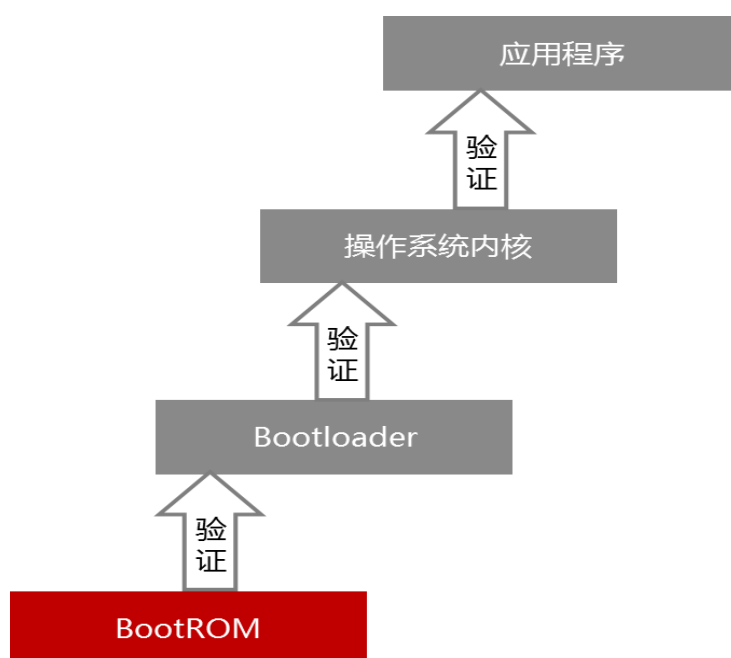
终端安全旨在确保每台海康威视设备的所有核心组件都能为软件和硬件提供安全保护。海康威视设备的硬件和软件实现了紧密集成，可确保系统的每个组件均获得信任，并对系统进行整体验证。从初始启动到软件更新，每个步骤都经过分析和审查。

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，防止启动流程被改动。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。

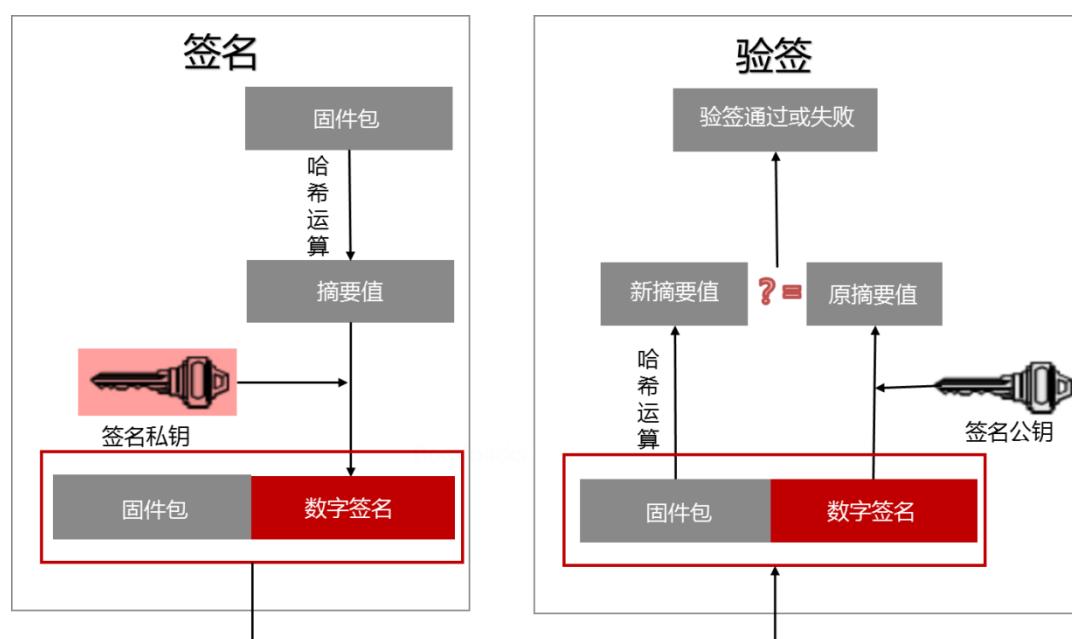


软件更新

海康威视会定期发布软件更新以解决新出现的安全性问题，并提供全新功能；此类更新会同时提供给所有受支持的设备。用户会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可采用安全通信机制（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。



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。

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 TrustZone、OTP 等，并结合高性能安全芯片，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，且支持国际算法和国密算法。

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 shell

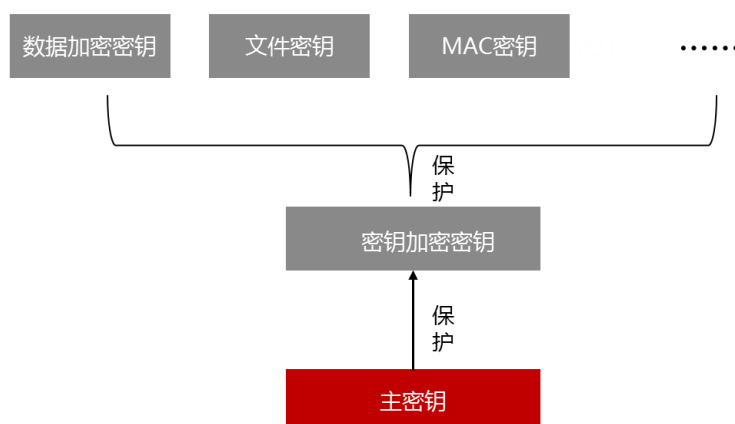
为了满足调试维护的要求，设备支持通过安全的 SSH 协议远程登录，对传输的数据进行加密保护。SSH 协议采用安全机制更完善的 SSHv2。

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。

设备对通过 SSH 建立的控制台输入的 shell 命令进行了裁剪和安全封装，只有通过安全检查后命令才执行。

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。



2.2 数据安全

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隐私数据。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；用户隐私数据包含但不限于人脸比对图片、模型等。

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、U 盘等。

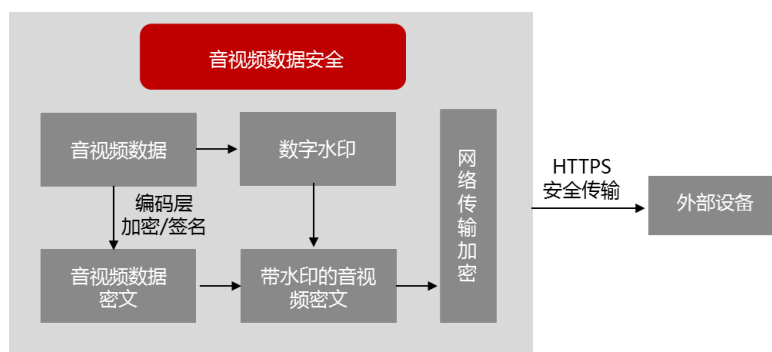
数字水印

数字水印技术是一种信息隐藏技术，它的基本思想是在数字图像、音频和视频等数字产品中嵌入秘密信息，以便保护数字产品的版权、证明产品的真实可靠性、跟踪盗版行为或者提供产品的附加信息。数字水印技术提供了一种隐藏标识的方法，标识信息在原始文件上是看不到的，只有通过特殊的阅读程序才可以读取。在视频流中添加数字水印是解决视频篡改攻击问题的理想途径，通过隐藏水印的状态可以判断视频信息是否被篡改。

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。



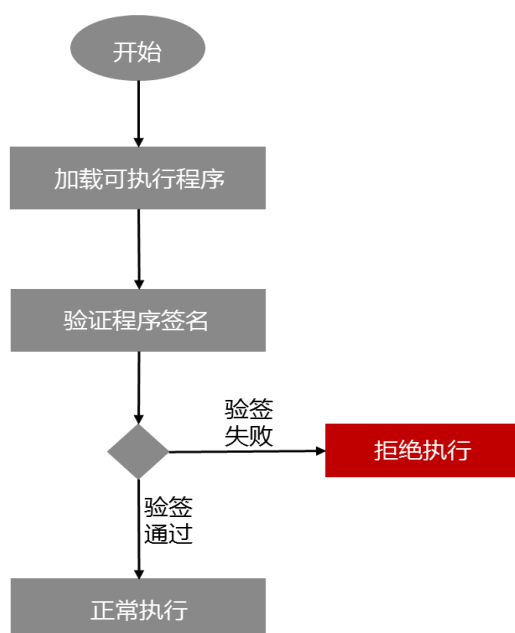
2.3 应用安全

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，保证恶意代码在无法运行。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。

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。



身份认证

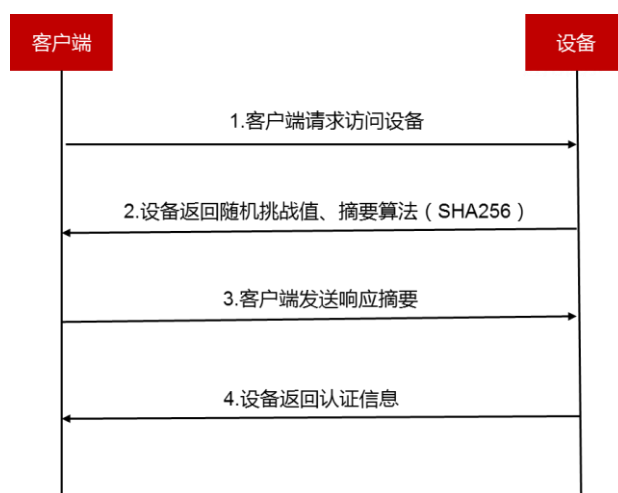
海康威视的设备账号安全体系依托于一系列口令策略和访问控制策略,充分保障用户账号安全：

- 用户口令复杂度要求：用户账号的口令具有复杂度要求，至少要求八位以上，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)；
- 访问控制：提供访问控制功能，采用用户权限分级机制，控制登录用户的权限；
- 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。
- 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。

密码算法

海康威视的密码算法使用均符合国际标准（如 FIPS），以及国内密码行业标准。除兼容第三方系统、或兼容历史标准协议外，密码算法使用均支持安全算法，并且采用安全的运算模式。

在身份认证过程中，大量标准协议，包括 HTTP、ONVIF、RTSP 等，使用 MD5 等不安全算法作为默认摘要认证算法。海康威视设备支持更高安全级别的密码算法，如 SHA256。

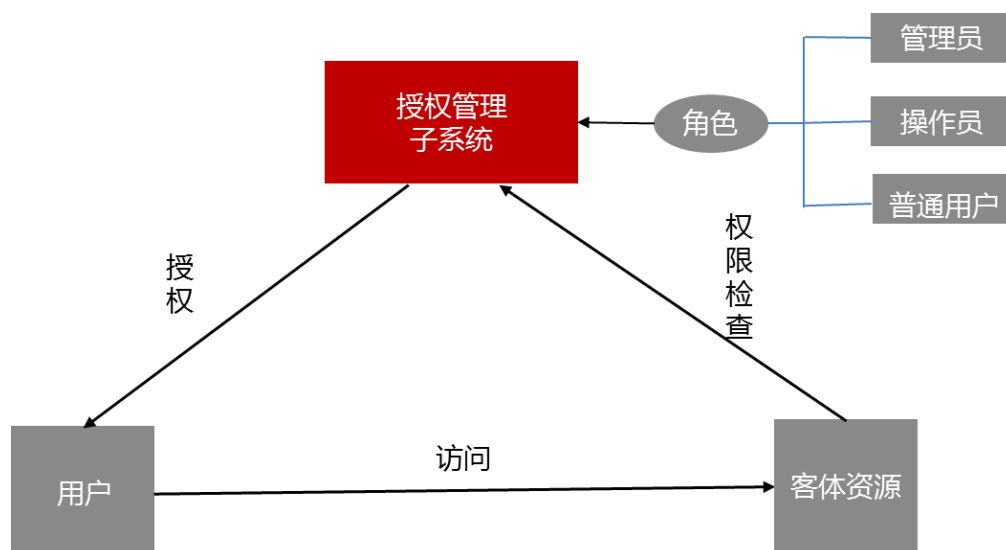


访问控制

海康威视对用户权限与设备访问控制进行统一管理，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。

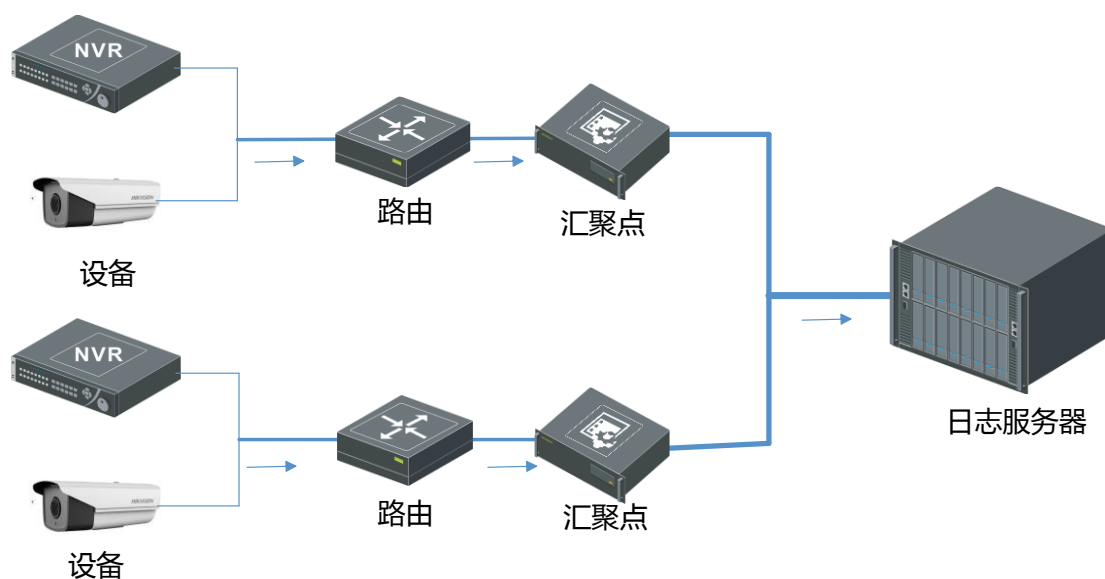


日志审计

海康威视的安全审计覆盖所有数据活动的详细跟踪记录, 从而实现对用户访问行为的主动监控, 生成审计所需要的信息, 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。日志服务器可满足数万台设备日志审计、自动分析预警, 可满足日志永久存档需求。



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。

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 “先安全分析再引入” 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。

2.4 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技术和最新标准来进行数据网络连接。海康威视移除不必要的网络服务(如 telnet 或 ftp 服务器),使受攻击的范围减小。

安全协议

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,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 或 DTLS 传输,无敏感数据泄漏;
- 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。

会话安全

海康威视设备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。

无线局域网安全

海康威视设备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。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。

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。

Web 安全

海康威视对所有 Web 系统进行全面的安全防御，为用户提供高品质、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；
- 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“CIS”规范严格审计 WebServer 配置，保证配置安全。

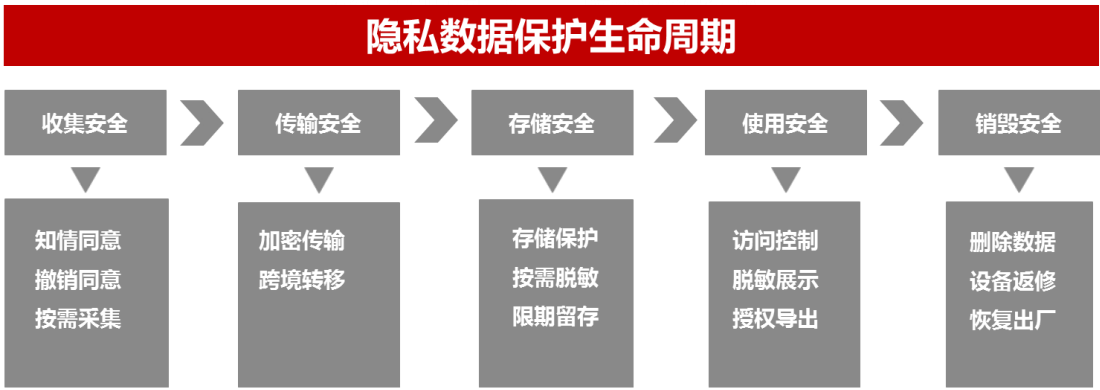
WEB 应用程序的会话标识具备随机性、唯一性，身份验证成功后，更换会话标识，防止会话固定。

2.5 隐私保护

物联网中的很多应用都与我们的生活息息相关，如摄像头，智能恒温器等设备。当用户使用物联网设备时，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

是物联网应用中至关重要的工作之一。海康威视严格遵循所适用的数据保护法律法规，包括中国《网络安全法》、欧盟《通用数据保护条例》等，并参照业内最佳实践，将数据安全与隐私保护要求贯穿于技术研发、产品设计、开发、验证、测试、交付及售后服务的全业务流程。

隐私数据保护生命周期具体保护措施如下：



- 收集安全：作为硬件设备供应商，在大多数情况下海康威视不接触或收集用户个人数据。但如果用户使用海康威视云服务，则海康威视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。
- 传输安全：产品保证隐私数据加密传输，在进行跨境数据转移时，会依据信息所在地区适用的法律法规要求进行处理。
- 存储安全：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。

- 使用安全：产品会对访问个人数据的用户进行身份认证和权限管理，在使用个人数据的过程中，如界面展示或日志记录等需要按照实际业务场景决定是否需要做脱敏处理，并且保证所有个人数据在使用后及时清理。出于业务场景需要，如需将个人数据导出用户网络，产品会依据信息所在地区适用的法律法规要求进行处理。
- 销毁安全：在设备维修、销毁或是云资源回收的场景下，产品提供完善的个人数据删除机制。

2.6 安全合规

商用密码产品型号

海康威视在商用密码（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。至今已取得多种不同类型产品的商用密码产品型号证书：

- SRM1701 安全门禁读卡器；
- SYT1703 密钥管理系统；
- SHT1810 视频监控安全管理系统；
- SJT1809 视频采集加解密系统。

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。

证书查询：

<http://www.oscca.gov.cn/app-zxfw/xzspsx/symmcp.jsp>

加密验证（FIPS 140-2）

美国商务部下属机构美国国家标准与技术研究院(NIST) ,联合加拿大通信安全机构(CSE) ,建立了旨在评测、验证和认证密码模块安全性的 FIPS 140-2 标准 ,该标准"被广泛认可为密码模块的实操标准"。作为一个相对综合和全面的认证标准 , FIPS 140-2 的认证要求不仅仅是密码模块算法及技术 ,还涵盖了正确的环境与密钥管理、物理安全、设计保障、安全实现等诸多方面 ,指定了密码模块需要被满足的安全需求。该标准不仅在美国和加拿大的政府中被普遍采纳 ,在金融、医疗、法律、公用事业等其他领域也被广泛采用。

海康威视于 2018 年 7 月获得了 FIPS 140-2 安全认证 ,证书编号为 3228。

海康威视所有同类产品中的密码模块完全相同 ,符合 FIPS 相关要求 ,并且针对新产品也将提交其密码模块进行验证。

证书查询 :

<https://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>

通用标准认证 (Common Criteria / ISO 15408)

CC(Common Criteria)认证是信息技术安全领域认可度最高的国际性认证之一 ,遵循国际公认的信息安全标准 (ISO/IEC15408)。该认证得到美国国防部下属的美国国家信息安全联盟 (The National Information Assurance Partnership , NIAP) 的认可 ,同时也在英国、加拿大等国家得到认可。目前已有包括美国和加拿大在内的 28 个国家的政府部门或政府代理机构加入了 CC 互认协定 (CCRA) ,因此 CC 认证在全球范围内具有很高的接受度与可信度 ,成为安全性评估方面的重要依据。

海康威视相关产品于 2018 年 9 月成功获得 CC EAL2+级认证 (ALC_FLR.2 增强) , 在安防行业内树立了良好示范。

海康威视将积极参与开发当前还未实施的保护描述文件 (PPs) ,并将继续针对当前已实施的 PPs 新版本和更新版本来评估和开展认证。

证书查询：

<https://www.commoncriteriaportal.org/products/>

3 安全性承诺

海康威视致力于使用领先的安全及隐私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。

海康威视在整个视频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。要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

http://www.hikvision.com/cn/about_593.html。



海康威视
产品安全白皮书

见远 行更远
See Far, Go Further

HIKVISION

杭州海康威视数字技术股份有限公司
地址: 杭州市滨江区阡陌路555号
电话: 0571-88075998