



# 新华三智能终端有限公司安全白皮书

---

## 物联网安全

### 技术白皮书

2021-06-发布

2021-06-实施

---


新华三智能终端有限公司 发布

# 法律声明

## 版权声明

- 版权所有 2003-2021 新华三技术有限公司
- 在未经新华三技术有限公司（简称“H3C”）事先书面许可的情况下，任何公司或人不能以任何形式复制、翻译、修改、传递、分发或存储本文档中的任何内容。
- 本文档描述的产品中，可能包含H3C及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

## 商标声明

-  是新华三技术有限公司的。商标或注册商标。
- 新华三技术有限公司系H3C商标的权利人，同意授权新华三智能终端有限公司（系H3C公司设立的全资子公司，以下简称“新华三智能终端”）在中华人民共和国境内使用H3C商标。

## 责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 新华三智能终端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。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

## 修订记录

- 2021-06-发布并实施

# 前 言

本标准由新华三智能终端有限公司提出。

本标准的起草单位：新华三智能终端有限公司。

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

- GB/T 22239-2019 信息安全技术网络安全等级保护基本要求
- GB/T 28448-2019 信息安全技术网络安全等级保护测评要求
- GB/T 25070-2019 信息安全技术网络安全等级保护安全设计技术要求
- GB/T 36951-2018 信息安全技术物联网感知终端应用安全技术要求
- GB/T 37024-2018 信息安全技术物联网感知层网关安全技术要求
- GB/T 37025-2018 信息安全技术物联网数据传输安全技术要求
- GB/T 37044-2018 信息安全技术物联网安全参考模型及通用要求
- GB/T 37093-2018 信息安全技术物联网感知层接入通信网的安全要求

## 物联网概述

物联网（Internet of Things，简称 IoT）将海量的设备互联，带我们进入一个万物感知、万物互联、万物智能的全新世界，极大地提升了社会运转的效率，方便人们的生活。物联网的应用场景十分广泛，包括智能家居、智能楼宇、智慧医疗、物流运输、交通、警务等领域。据 Gartner 预测，到 2021 年全球物联网设备数量将增至 208 亿台，复合增速高达 34%。物联网将渗透进人们生活的方方面面，广泛进入各行各业。

## 安全问题

物联网作为互联网的扩展和延伸，传统互联网面临的安全问题/安全威胁在物联网中同样存在，例如如何保护的数据机密性、完整性、可用性，如何防窃听、伪造、仿冒、篡改等。此外，物联网由于自身特点不可避免带来了新的安全问题：

- 物联网中大量应用与生活息息相关，如摄像头等设备，通过对它们信息的采集，可直接或间接地暴露用户的隐私信息。
- 由于物联网设备自身资源限制，很多物联网设备缺乏加密、认证、访问控制管理的安全措施，使得物联网中的数据容易被窃取或非法访问，造成数据泄露。
- 物联网设备数量多、分布零散，海量物联网设备的升级过程和安全状态监控存在困难。

## 安全事件

现实生活中因为物联网设备而导致的安全事件已是触目惊心：

- 据外媒报道，2016 年 10 月 21 日，美国东部遭遇史上最严重的 DDoS 攻击，攻击流量超过 1Tbps，近半个美国的网络遭到攻击并瘫痪。造成这次事故的元凶，是日常生活场景却很容易被人们所忽略的摄像头、家庭路由器、数字视频录像机等微型智能设备，这些设备感染了 Mirai 恶意软件，造成的攻击导致 Twitter、亚马逊等百余家知名网站出现数小时的瘫痪。
- 2015 年，HackPWN 安全专家演示了利用比亚迪云服务漏洞，开启比亚迪汽车的车门、发动汽车、开启后备箱等操作。
- 2015 年 12 月 23 日，黑客以 BlackEnergy 病毒为攻击工具，通过远程控制电力控制系统节点下达断电指令，并通过对系统数据擦除覆盖、关机等系列操作阻碍系统恢复，导致乌克兰伊万诺-弗兰科夫斯克地区超过一半区域断电几小时，大量用户受到影响。

物联网安全问题需要引起我们的高度重视，国家实施了如《中华人民共和国网络安全法》、《关于加强公共安全视频监控建设联网应用工作的若干意见》等一系列法律法规来加强网络安全建设。据 Gartner 统计，2016 年全球在物联网安全上的支出达到 3.48 亿美元，比 2015 年的 2.815 亿美元支出增长了 23.7%。2018 年，物联网安全的总支出预计将达到 5.47 亿美元。物联网安全将成为我们必须面对的重要课题。

## 安全威胁

从摄像头、猫眼、门铃等感知设备的终端层，路由器、交换机等数据传输的网络传输层，到运维管理、云端存储管理的平台层，IoT 面临的安全威胁如图 2-1 所示。

图2-1 物联网安全威胁层级图



### 终端层

终端设备的形态千差万别，广泛分布在社会的方方面面、各行各业，从家用安防、智能交通、智能楼宇到平安城市。

从终端设备的个体差异与服务多样性考虑，终端设备会受到如下安全威胁：

- 终端在户外、分散安装、易被接触到又没有纳入管理，导致受到物理攻击、被篡改和仿冒。
- 物联网终端多为小型嵌入式设备，因成本、计算能力等原因，无法将防病毒、内容检测等安全技术应用到终端设备，导致终端自身安全能力较为薄弱。
- 物联网终端设备应用广泛，存在海量设备，终端软件漏洞修复成本高。

### 网络层

设备端采集到的数据，设备的配置信息等数据需要通过网络传输到管理端，数据在网络传输的过程中，面临着网络中无时无刻不在发生的威胁攻击：

- 物联网数据通过 Internet 传输，由于传输协议本身的缺陷或通信过程未使用加密方式容易受到劫持、重放、篡改和窃听等中间人攻击，导致用户数据、个人隐私被窃取。

- 
- IP 化转型，面临 IP 体系的安全问题，如来自互联网的攻击和入侵。

## 平台层

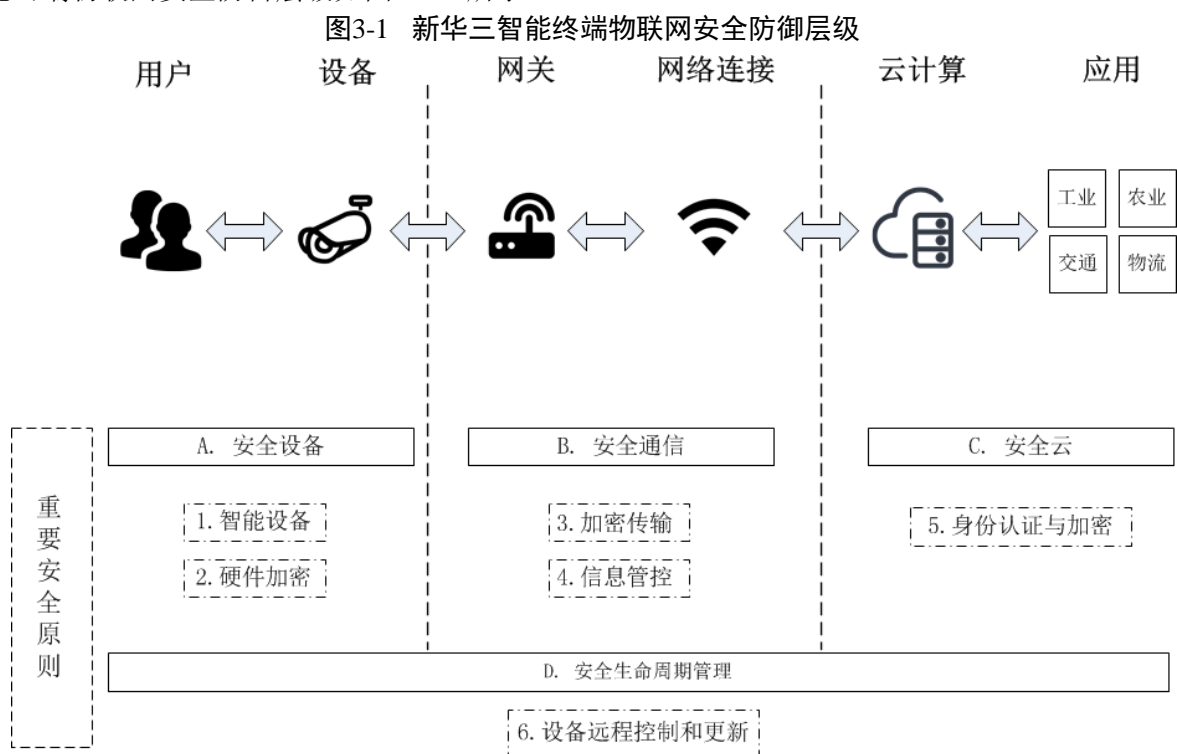
物联网平台层提供企业和用户以可视化的平台管理海量的设备终端，提供不同的应用与服务，与不同地域、不同类型的设备、协议交互，面临的安全威胁如下所示：

- 平台层面所管理的设备分散、繁多且可能出现不同厂家设备，平台需要对接不同厂家型号、不同协议交互的设备，难度较大；同时，海量设备的升级过程和安全状态等难以管理。
- 平台支持不同用户操作，由于权限设置或校验不当而导致的越权访问，使得个人隐私和安全凭证等重要数据存在被泄露的风险。
- 平台提供的应用丰富、数据中心出口多，与对端交互的协议也丰富多样，网络攻击方法层出不穷，如DDoS 等网络攻击风险高。
- 当前众多平台开放自身API 接口可能导致新的安全威胁，如注入攻击。

## 新华三智能终端物联网安全体系

由于物联网分布式的特点，物联网设备可能跨不同区域分布，终端设备通过 Internet 网络连接将信息传输到物联网平台。终端设备的千差万别，传输网络中无处不在的安全风险，物联网平台的隐私数据，使得物联网的不同组件间跨越不同的安全信任区域。因此物联网需要多重端到端的安全防御体系。

新华三智能终端将软件安全开发生命周期管理全过程融入公司协同产品开发流程中，基于完善的的安全管理体系，实现终端层（端）、网络层（管）、平台层（云）的多重端到端安全防御体系，为客户提供安全可靠的物联网安防产品和解决方案，新华三智能终端物联网安全防御层级如图 3-1 所示。



### 安全设备

终端层，部署物联网解决方案时所涉及到的硬件设备。物联网设备分布广泛，数量众多，暴露在外，敏感而脆弱。新华三智能终端在设计 and 生产设备（包括 OEM 设备）时致力于在终端上集成更多的安全功能，如设备的身份认证功能以防止异常设备终端接入网络，提供了硬件加密模块有效保护本地数据安全，固件安全检测、完整性校验等功能以保证升级的固件包安全有效。

### 安全通信

网络层，用于安全传输数据的媒介。物联网设备端的数据只有通过网络传输到服务器

或云端才能被用户查看与使用，而这些数据包含大量的敏感信息，只有通过安全的传输通道才能保证数据不被窃取、篡改。

新华三智能终端解决方案可以提供安全隔离功能，支持隐藏内部网络地址，支持配置过滤流量的属性，实现对流量的严格控制，可以指定可疑流量直接丢弃；所有传输通道都支持加密方式传输，有效地保证了数据的机密性和完整性；针对网络中的不同攻击类型，可以通过部署专业的安全设备来防御网络攻击。

## 安全云

平台层，负责对终端大量数据的分析、存储与处理。平台层对用户开放，支持多用户并发操作，提供多种应用端口，因而更容易遭受网络攻击。同时，海量数据的分析与处理对平台提出了更高的性能要求。

新华三智能终端依托云服务和云存储，提供了新华三智能终端设备的云升级方案，设备可以直接连接云服务，快速高效地更新设备固件，为安全漏洞修复提供了安全便捷的方式。新华三智能终端运维管理平台提供实时监控、视频分析、监控点“户籍化”管理、报表可视化等运维可视化手段，提升了运维效率。

## 安全生命周期管理

除了架构层级划分的三个层级，新华三智能终端着眼于物联网安全的整体架构与解决方案，实现对物联网设备与安全的运维、管控，从设备出厂到安装部署，再到实际应用，动态监控物联网安全，实现完整的生命周期管理，不断加固物联网各个环节的安全特性，以促进物联网安全的不断提升。

新华三智能终端在开发流程中引入安全开发生命周期管理（Security Development Lifecycle, SDLC）流程，并结合企业安全需求及新华三智能终端协同项目开发流程，系统识别产品/解决方案的安全风险，端到端进行项目安全开发生命周期管理。



# 新华三智能终端物联网安全防御介绍

本章节从数据安全、身份安全、网络安全及系统安全的角度，将上述安全技术物联网安全的设备层、网络层及平台层的三个层级的应用情况进行描述，并阐述了新华三智能终端基于产品开发流程的安全开发生命周期管理体系。

## 数据安全

新华三智能终端深刻理解数据安全对客户业务、客户隐私的重要意义，从数据的安全生命周期角度出发，通过对数据产生、数据存储、数据传输、数据使用、数据消亡等各个生命周期阶段制定对应的数据安全策略，保证端到端的数据安全。

### 端到端数据加密

新华三智能终端为物联网提供了端到端数据的安全保护。

### 敏感信息保护

敏感信息如用户名、密码、个人姓名、电话号码、邮箱、地址等的泄漏，会导致攻击者在用户无感知的情况下长期、任意窃取用户信息。

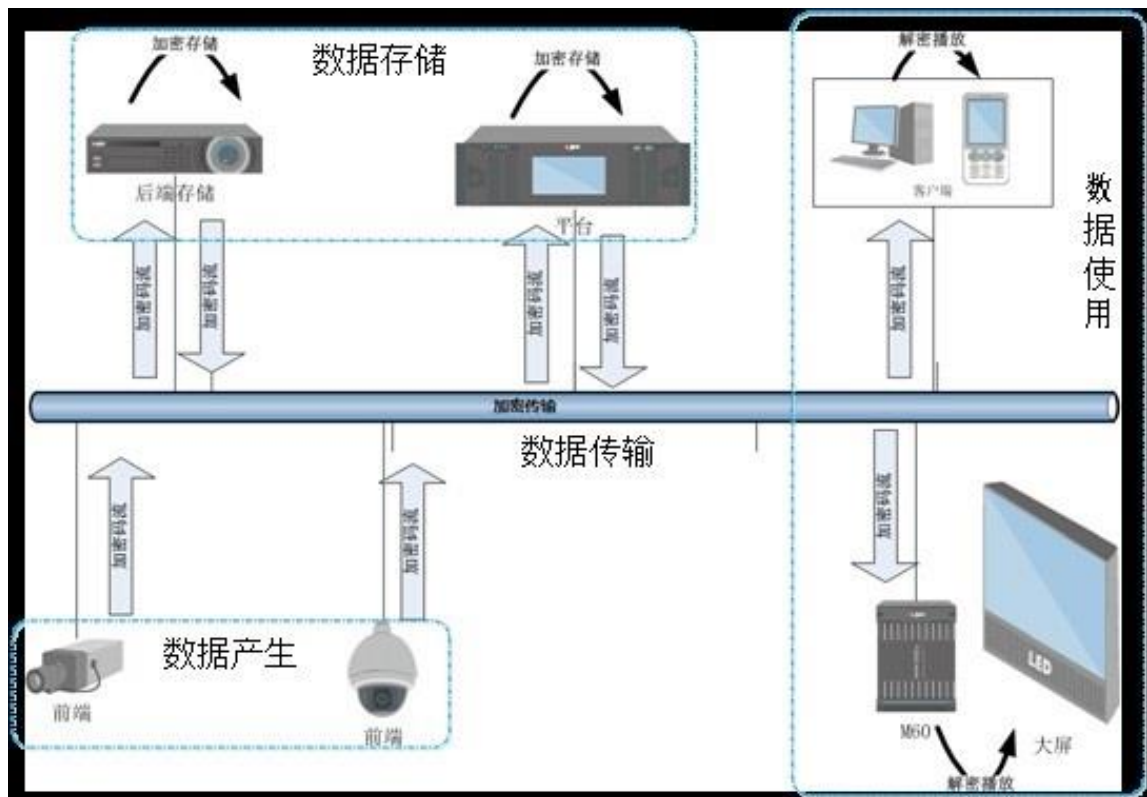
为避免敏感数据泄露，设备对敏感数据实现安全存储。设备对敏感信息加密保存，避免被攻击者通过静态分析固件/登录设备后获取文档等形式获取敏感信息。

### 业务数据保护

在数据产生、传输、存储、使用过程的全程对数据加密，最大程度上保证了数据安全。

业务数据经高强度加密后，从终端传输到后端存储或平台系统，平台直接以加密数据形式保存。当有业务查询请求时，数据仍以加密方式发送到客户端，在客户端本地解密后展现。数据全程以加密状态存在，有效防止数据泄露，业务数据保护流程如图 4-1 所示。

图4-1 业务数据保护



## 数据冗余备份

为减小由于硬件故障、自然灾害或者其它灾难导致的数据丢失或服务中断等情况，新华三智能终端解决方案提供数据存储的容灾备份能力以保证用户的数据安全。

## 数据访问策略

新华三智能终端为企业和用户的数据访问提供安全保障。所有产品所使用的数据，严格控制访问权限。任何第三方应用访问和使用企业或用户数据都必须经过企业或用户的授权，同时操作会被记录在相应的操作日志，以便后续追溯、审计使用。

## 硬件加密模块

硬件加密模块在系统中被用来提供硬件加密功能，密钥被保护在硬件加密模块内部。新华三智能终端通过硬件加密模块提升系统的数据安全保护等级。

- 硬件加密模块将内部应用软件加密算法的密钥安全地移植到芯片的硬件中保护起来。
- 在需要使用时，应用软件可以通过功能调用引擎指令运行硬件中的加密算法并返回结果，协助完成整个软件全部的功能。

由于这些加密算法的密钥在设备端没有副本存在，因此解密者无从猜测或窃取加密算法的密钥，有效地保证了本地敏感数据的安全。

## 用户账号安全

### ● 无保留账户

## ● 密码保护策略

➤ 至少 8 位字符。

- 不少于两种类型字符。

- 对登录提示、密码强度和会话认证上做了安全提示:

- 用户添加账户、修改密码以及一些账户展示界面，明确提示用户当前密码的安全等级，以此提醒用户当前使用的密码安全情况。

- 用户登录时，无论是用户名错误，还是密码错误，设备统一返回用户名或密码错误，保证设备账户的不可猜测性。

- 设备无默认密码，强制用户在初始化阶段设置用户密码。

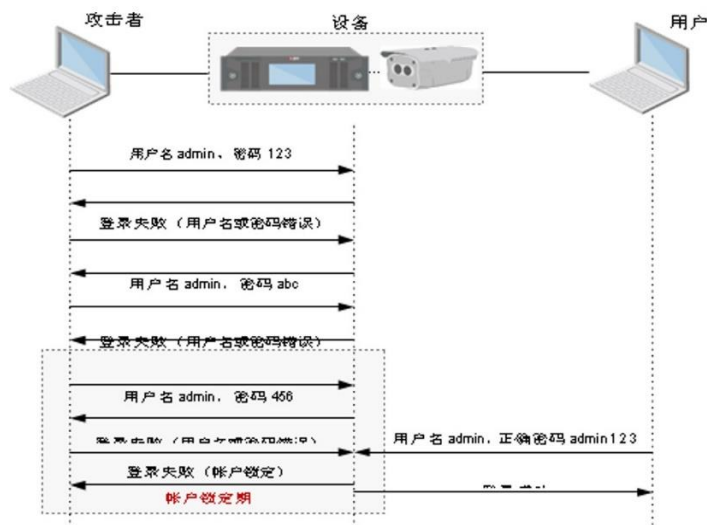
- 在用户的密码修改后，设备强制注销所有该用户的在线会话，要求重新认证登录，避免非法用户保持连接继续操作。

## ● 密码防爆破

为防止帐号密码被暴力破解，新华三智能终端设备采用了密码防爆技术，即基于提高攻击时间成本的思想实现的一种保护密码的安全技术。

密码防爆破的原理是在设备感知到某台主机发起对设备的密码爆破行为时，设备进入账户锁定期，该主机在锁定期内，无论密码正确与否，都会登录失败。攻击者在单位时间能够尝试的密码次数非常有限，以此有效制止密码爆破行为，密码防爆技术如图4-2 所示。

图4-2 密码防爆技术



为防止恶意攻击者利用账户锁定机制，不停发起恶意登录请求，导致正常用户无法使用设备，密码防爆破技术中融入了主机识别能力，账户锁定期只会对发起密码爆破攻击主机生效，但不影响正常用户使用设备。

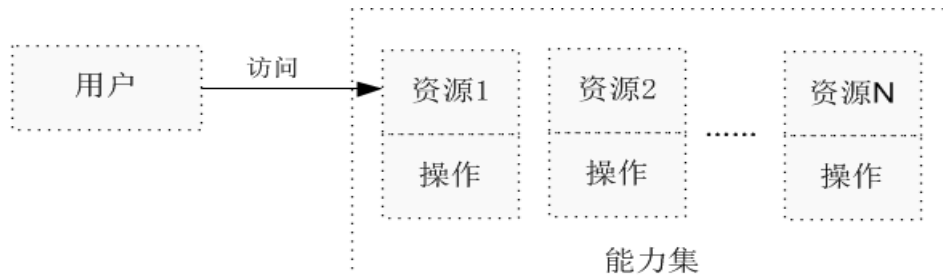
## 帐户权限安全

设备具备一套灵活安全的权限管理系统，用户可被分为管理员和普通用户两个等级，每一个用户等级下，拥有着对应的权限集合；用户在所在的用户等级权限集合范围内，能够被灵活分配所需的最小权限集合。

设备权限管理系统，是基于自主访问控制（DAC）权限控制系统实现的，设备集成了用户创建的每一个账户所拥有的能力集：

- 每个主体（用户）拥有一个用户名并且用户名属于一个组或具有一个角色身份；
- 每个客体（设备）都拥有一个限定主体对其访问权限的访问控制列表（ACL）；
- 每次访问发生时访问控制列表都会检查用户标识以实现用户对设备访问权限的控制，如图4-3 所示。

图4-3 基于用户的能力集权限控制



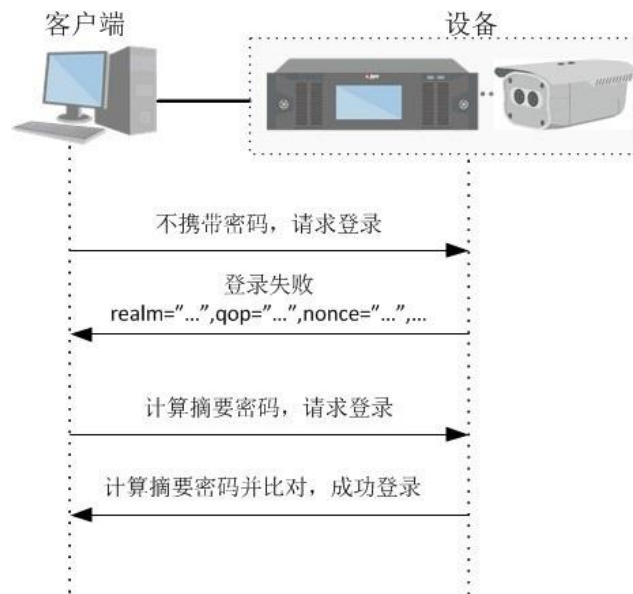
## 会话安全

在会话认证过程中，主要的安全问题来自于用户信息的明文传输，而在摘要（Digest）认证中，通过发送密码的摘要信息来取代密码传输，且摘要信息不可逆，从而提高认证交互的安全性。

摘要认证技术优势如下：

- 不会将密码以明文方式在网络上传递。
- 防止恶意用户捕获并重放认证的握手过程。摘要认证技术图解如图 4-4 所示。

图4-4 摘要认证技术图解



设备通过对用户会话的多重校验保护，确保用户会话安全。

- 会话凭证具备随机性，确保不被外部猜测破解；
- 会话凭证跟登录 IP 地址绑定，避免被其他攻击者利用；
- 增强防暴力破解机制，检测对用户会话的暴力破解行为，并注销受威胁会话，避免被攻击者利用；
- 对会话凭证进行用户权限校验，避免低权限用户越权操作。

## 网络安全

### 安全传输

在网络传输过程中，为了确保物联网中设备与物联网平台之间传输数据的完整性与机密性，新华三智能终端针对网络传输采用了用于安全传输的标准协议（如TLS）。安全传输标准协议中需使用证书用于验证身份，设备出厂状态下所拥有的证书是由厂商提供的。为解决用户的证书信任问题，新华三智能终端设备提供证书导入功能，支持用户使用自己信任的证书，同时也支持用户定期更新证书，更加安全地应用证书。

### 安全隔离

#### 安全设备隔离

物联网数据通过互联网传输，在传输两端的网络出口部署边界安全隔离设备，在安全隔离设备上根据流量的源目 IP 地址、源目端口、使用协议等实施隔离策略，实现对流量的严格控制；并且安全隔离设备可以实现用户网络的 IP 地址对外界隐藏的目的。

除了互联网边界安全，在物联网局域范围内的不同安全区域，部署安全隔离设备可实现不同安全等级区域之间的隔离，保证数据严格按照制定的访问控制策略传输。

## 数据包过滤

新华三智能终端设备支持数据包过滤技术，以达到直接在设备上实现控制数据包通过或丢弃的控制目的。包过滤技术是指根据包过滤规则检查所接收的每个数据包，做出允许数据包通过或丢弃数据包的决定。

数据包过滤技术是通过检查数据包的 IP 头和 TCP 头或 UDP 头的检查来实现的，主要信息如下：

- IP 源地址
- IP 目标地址
- 协议（TCP 包、UDP 包、ICMP 包）
- TCP 或 UDP 包的源端口
- TCP 或 UDP 包的目标端口
- ICMP 消息类型
- TCP 包头中的ACK 位
- 数据包到达的端口
- 数据包出去的端口
- 数据包过滤技术的优势如下：
  - 过滤掉非法的客户端对象，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。新华三智能终端设备支持配置协议端口与转发端口。
  - 更改默认的 HTTP 和 TCP 端口，这两个端口可以设置成 1025~65535 间的任意数字。更改默认端口后，减小了被入侵者猜到您使用哪些端口的风险。
  - 使能 IP 过滤功能，只有指定 IP 地址的设备才能访问系统。
  - 只转发必须使用的网络端口，避免转发一段很长的端口区。不要把设备的 IP 地址设置成DMZ。
  - 关闭客户端（如SmartPSS）的自动登录功能，增加一道防线防止未经授权的人访问系统。
  - 如果已经在路由器上手工打开了 HTTP 和 TCP 端口映射，我们强烈建议您关闭UPnP 功能。启用 UPnP 协议以后，路由器将会自动将内网端口进行映射，虽然方便用户使用，但会导致系统自动转发相应端口的数据。在实际应用场景中，我们强烈建议您关闭此功能。
  - 如果您不使用 SNMP 功能，我们建议您关闭此功能。
  - 我们建议您使用PoE 方式连接到 NVR 的 IP 摄像机，使其与其它网络隔离。



## 流量管控

在网络关键节点部署管控流量的安全设备，针对不同来源、访问不同服务的流量实施不同的流量管控策略，以保证优先级高的流量可以在网络质量较差、带宽较小的情况得到更好的传输保障。

## 攻击防范

网络攻击层出不穷，单一依赖流量管控、安全策略等无法保证对攻击防范的防御。新华三智能终端解决方案可以提供集成部署专业安全设备以防御基于网络协议的攻击和基于系统及应用安全漏洞的攻击，如 DDoS 攻击、异常报文攻击等。

## 系统安全

## 云升级服务

新华三智能终端云升级服务，提供新华三智能终端设备通过定期连接云升级系统或用户手工立即触发的方式，检测版本更新情况，在用户确认授权的情况下，通过安全连接主动到升级服务器下载程序包，完成升级的过程，通过云升级服务实现设备固件 OTA 升级。

新华三智能终端云升级服务部署在公有云上，包括云端服务接口与云端数据存储。企业可以根据自身需要选择连接互联网的公有云升级方式，也可以在企业内网定制新华三智能终端云升级服务，搭建本地升级服务。

通过云升级服务：

- 统一的终端设备升级解决方案，提高新华三智能终端产品程序升级效率。
- 及时推送安全威胁修复解决方案，为可能存在的安全隐患提供快速、及时的解决通道。云升级流程如图 4-5 所示。

图4-5 云升级流程图



## 固件升级安全

终端设备具有固件安全升级能力，对用来升级的固件进行校验，识别非来源于新华三智能终端的固件包或被非法篡改的固件包。新华三智能终端终端设备在升级过程中会对加载的固件包进行安全校验（合法性及完整性校验），只能使用新华三智能终端官方发布的安全固件包进行升级，保证升级的固件包安全有效。

可信升级技术是为了防止固件包被恶意篡改、用户的设备被升级等，利用非对称算法的签名能力，出厂设备已经集成了厂商提供的一份公钥文件，对应的私钥只有新华三智能终端拥有并保存，在发布固件包时，利用了私钥的签名技术，可信固件打包流程如图 4-6 所示。



图4-6 可信固件打包



新华三智能终端利用此私钥对固件包完整签名后，与固件包一起发布。设备在升级固件包时，会使用预先集成设备中的公钥文件进行签名校验，只有通过检验的固件包，才能被真正写入到设备 flash 中，固件可信校验流程如图 4-7 所示。

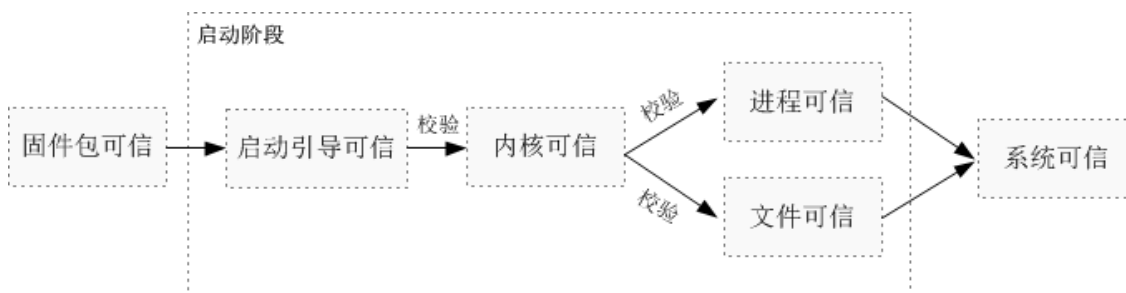
图4-7 固件可信校验



## 安全运行环境

终端设备实现了端到端可信系统，通过建立“信任链”，保证了设备运行环境的安全性，从底层向上，层层认证，保证每一层的调用安全可靠，从而保证整个运行环境的安全可靠。进一步加固了系统层安全，保证设备上不会运行非法程序，降低了设备自身被攻击的风险。安全运行环境示意图如图 4-8 所示。

图4-8 安全运行环境示意图



新华三智能终端设备具备控制病毒、恶意程序运行的能力，即使设备中被植入病毒/恶意程序，病毒/恶意程序尝试运行期间，将会被识别并阻拦，从而拒绝此类程序的运行，有效地防止病毒/恶意程序。

控制非授权程序运行技术通过签名技术实现：

- 在合法可执行程序中增加程序签名。

- 程序启动期间，操作系统内核会对程序及其签名进行校验认证。
- 如果内核发现程序不可信任，则终止程序运行，由此达到反病毒/恶意程序的能力。

## 网络服务策略

设备关闭部分默认状态的服务，以减小设备威胁面：

- 默认关闭Telnet 调试服务。
- 默认关闭 SSH 调试服务。
- 默认关闭 SNMP 服务。

设备支持更加安全的服务，我们强烈建议您设置 HTTPS/SFTP 服务为默认服务以替代一些较为不安全的网络服务功能：

- HTTPS 访问功能，替代HTTP 服务。
- SFTP 服务，替代 FTP 服务。

设备对已经支持的服务，提供了端口配置能力，用户可自由配置端口，达到隐藏端口的目的。

## 日志审计

终端设备具有完善的日志管理系统，为每一个重要或关键的操作做好日志记录。

日志管理系统为日志划分了重要等级，其中安全日志的等级尤为重要，其他任何等级的日志，都将无法覆盖安全等级的日志，以此保障设备安全事件的回溯。

以下操作（但不限于）均有日志记录：

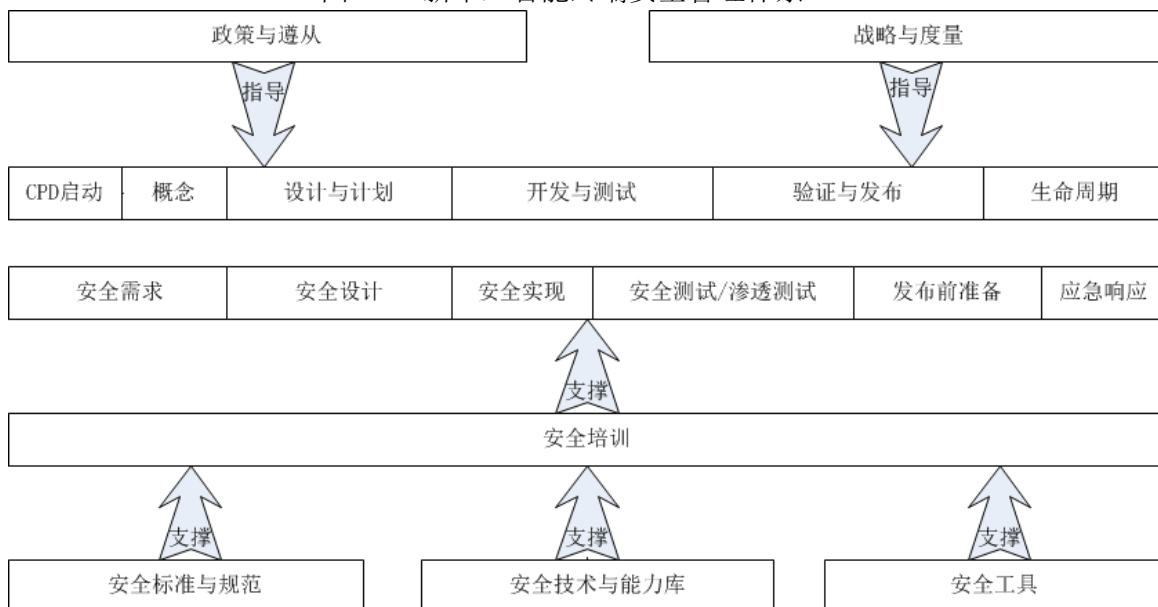
- 用户登录和退出
- 增加、删除、修改用户帐号和密码
- 导入导出系统配置
- 修改系统关键配置（包括报警和录像配置等）
- 上传文件
- 重启和升级设备
- 修改系统时间
- 异常处理（异常事件包括断网、无硬盘、硬盘错误、硬盘容量过低或视频丢失等）
- 非法安全操作（如账户锁定、会话爆破等） 每条日志都包含如下关键内容：
- 操作源，包括用户及源 IP
- 操作内容
- 操作时间

设备配备了网络日志备份能力，可以启用网络日志功能，将重要日志同步保存到日志服务器中。

## 安全生命周期管理

结合新华三智能终端产品协同开发流程，以产品和解决方案最终在客户侧的安全可靠为核心目标，建立新华三智能终端安全开发生命周期管理（SDLC）体系。将新华三智能终端公司产品安全问题作为常态进行管理，在结合历史实践和能力现状的前提下牵引新华三智能终端研发流程体系，不断积累安全技术能力，形成新华三智能终端自己的安全标准与规范、安全技术能力库、安全工具集合，更好地支撑 SDLC 过程，积极响应安全事件，新华三智能终端安全管理体系如图 4-9 所示。

图4-9 新华三智能终端安全管理体系



## 安全开发生命周期管理

### 安全培训

产品开发过程各个阶段，新华三智能终端安全工程师对开发人员进行安全开发规范、安全意识等培训，提高开发人员的安全意识，构筑全员安全开发能力。

### 安全需求

在当前已有安全基线的基础上，不断完善安全与隐私保护的能力基线，在产品设计与开发的前端开始根据业务功能、业务流程、系统架构对安全需求、隐私保护进行分析，评估产品的安全风险，形成安全需求分析文档。

## 安全设计

在安全需求分析完成的前提下，进行安全设计，完善产品攻击面分析，实现安全威胁建模，形成安全需求设计文档，用于指导产品的具体安全能力实现与测试。

## 安全实现

在产品软件开发流程中，安全实现过程符合安全标准与规范，包括但不限于禁用安全危险函数、开源库及第三方软件管理、代码扫描、代码检视。

## 安全测试/渗透测试

软件开发完成后，必须由新华三智能终端专门的测试团队完成对软件的安全测试（包括但不限于 Fuzzing 测试、攻击面再检视、动态分析）以及渗透测试。

## 发布前准备

新华三智能终端产品（包括软件和硬件）在发布前必须经过安全审视，制定安全响应计划，发布操作指导文档与安全操作指南。

## 安全应急响应

物联网设备在使用过程中，会遭遇不同的安全威胁、漏洞风险。新华三智能终端构建的安全应急响应体系实时监控网络安全状况，第一时间响应安全漏洞与风险，执行应急响应计划，实施漏洞修复与管理。

新华三智能终端是 MITRE 成员组织 CNAs (CVE Numbering Authorities) 的重要成员，该组织在发现安全漏洞时会及时主动通报给相关成员，因此新华三智能终端公司可以第一时间获取外部组织发现的安全漏洞并做修复。另一方面，新华三智能终端在发现自身安全漏洞后会维护对应的 CVE (Common Vulnerability & Exposures) 编号及时向客户和公众披露。新华三智能终端发现漏洞的方式包括但不限于本司安全人员发现、外部道德黑客提交、外部安全组织（如CNVD、ZDI 等）通报等。

新华三智能终端专门成立了应急响应中心，由专门的安全观察员从安全组织、漏洞共享平台、个人白帽子等方式获取安全告警，将安全事件上报给网络安全执行小组、安全测试人员进行分析，对事件进行定级处理，出具综合解决方案，并将事件处理结果与方案向社会公布，收集发现的漏洞，编写对应的测试用例，保证该漏洞不会在之后的程序版本里出现。

## 支撑体系

在 SDLC 流程实践中，新华三智能终端建立并持续完善新华三智能终端安全标准与规范，构建安全技术与能力库，引进或开发安全工具以支撑不断变化的安全威胁。

- 安全标准与规范：形成完备的安全标准规范，指导安全需求分析、设计、实现与测试。
- 安全技术与能力库：为新华三智能终端产品实现安全能力提供公共支撑。
- 安全工具：新华三智能终端通过自研与引入的方式提供安全能力测验工具，极大提升安全能力检测的效率。

新华三智能终端专门成立了网络安全产品线，致力于构建安全标准与规范，开发安全能力公共库与测试工具，为程序发布提供漏洞检测、安全测试，监控安全漏洞发布，做好网络安全应急响应，为客户提供及时的安全问题处理方案。

## 政策与遵从

### 安全体系

新华三智能终端依据 ISO27001:2013 建立安全管理体系，确保产品/解决方案的安全管理合规。公司已通过被全球广泛采用的安全标准-ISO27001 信息安全管理体系认证，采用以风险管理为核心的方法来保证公司和客户信息的保密性、完整性和可用性，并通过定期评估风险和控制措施来保证体系的持续运行。

### 政策合规

新华三智能终端根据国家法律、业界标准和行业最佳实践不断完善自身的管理与机制，并通过了一系列标准认证、三方审计和内部安全评估，务求从多维度满足合规需求。

新华三智能终端面对不同角度、不同行业、不同地区的合规需求，可以划分为：

- 管理体系合规
  - 公司成熟的的安全管理机制和遵从行业最佳实践；
  - ISO 27001：信息安全管理体系；
  - BSIMM：构建安全的能力成熟度模型（Building Security In Maturity Modle）。
- 法务合规
  - 符合《中华人民共和国网络安全法》、《关于加强公共安全视频监控建设联网应用工作的若干意见》、《公安视频传输网建设指导意见》（征求意见稿）等法规；
  - 在不同地区经营，需要符合当地的法律法规。新华三智能终端有专业的法务团队评估对应地区的法律、行业法规，确保产品、解决方案的法规遵从。

### 行业标准

遵从所属行业的相关国家标准，积极参与行业标准的制定，跟踪标准更新的进展；遵从网络信息安全等级保护基本要求（等保 2.0）、公共安全视频监控联网信息安全技术要求、公安视频传输网建设指导意见。

## 隐私政策

新华三智能终端制定了严格的隐私保护政策，采用用户授权原则与最小权限原则来收集和传输个人或隐私数据，此操作需提供明确的个人数据和隐私声明以及提前获得授权，数据所有者有权随时撤销其授权。

隐私政策中定义了产品、平台对个人数据收集的范围、用途、存储及保密政策。采集的数据仅用来为用户提供服务，不会向任何无关第三方提供、出售、出租、分享或交易。同时新华三智能终端采用各种技术手段确保客户的个人信息仅存在于新华三智能终端的业务范围。