产品安全

技术白皮书

V1.0.0

浙江大华技术股份有限公司

法律声明

版权声明

商标声明

- 、、、HDCVI是浙江大华技术股份有限公司的商标或注册商标。
- HDMI 标识、HDMI 和 High-Definition Multimedia Interface 是 HDMI Licensing LLC 的商标或注册商标。本产品已经获得 HDMI Licensing LLC 授权使用 HDMI 技术。
- VGA 是 IBM 公司的商标。
- Windows 标识和 Windows 是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

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。
- 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。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

关于本文档

- 产品请以实物为准，本文档仅供参考。
- 本文档供多个型号产品做参考，每个产品的具体操作不一一例举，请用户根据实际产品自行对照操作。
- 如不按照本文档中的指导进行操作，因此而造成的任何损失由使用方自己承担。

- 如获取到的 PDF 文档无法打开，请将阅读工具升级到最新版本或使用其他主流阅读工具。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。产品部分功能在更新前后可能存在细微差异。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。

前言

概述

为更好的保护用户数据、提升设备的安全性、规范网络设备的应用，大华采用先进的加密算法，对网络设备采取了一系列的安全措施，如设备开机后引导用户设置强密码、加密存储敏感数据、备份重要日志等。

本白皮书主要介绍网络设备所采用的安全技术和策略，包括 Digest 认证、数据包过滤、反 ARP 欺骗、数字信封、安全存储、安全 shell、可信升级和密码防爆破等安全技术，以及用户管理、权限管理、日志管理、会话管理、网络服务和证书导入等安全策略。

符号约定

在本文档中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	表示有高度潜在危险，如果不能避免，会导致人员伤亡或严重伤害。
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

编号	版本号	修订内容	发布日期
1	V1.0.0	首次创建	2017.5.10
2	V1.0.0	首次发布	2017.6.30

目录

1 安全技术

1.1 摘要认证技术

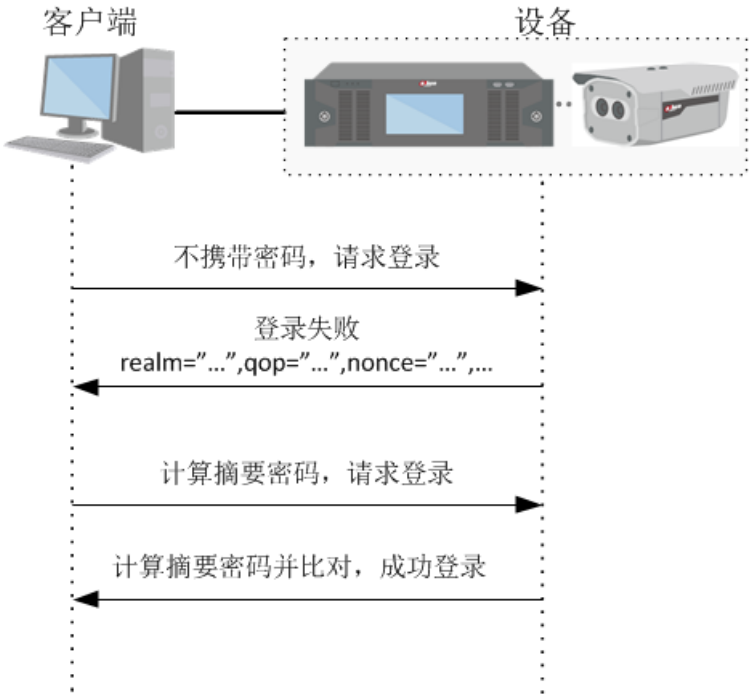
在基本认证过程中，主要的安全问题来自于用户信息的明文传输，而在 Digest 摘要认证中，通过发送密码的摘要信息来取代密码传输，且摘要信息不可逆，从而提高认证交互的安全性。

Digest 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。

Digest 认证技术如图 1-1 所示。

图1-1 Digest 认证技术



摘要密码计算算法如下：

- HA1 = md5("username:realm:password");
- HA2 = md5("method:uri");
- 摘要密码=md5("HA1:nouce:nc:cnonce:qop:HA2");

1.2 数据包过滤技术

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对数据包的 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 包和 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

数据包过滤技术的技术优势如下：

- 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。

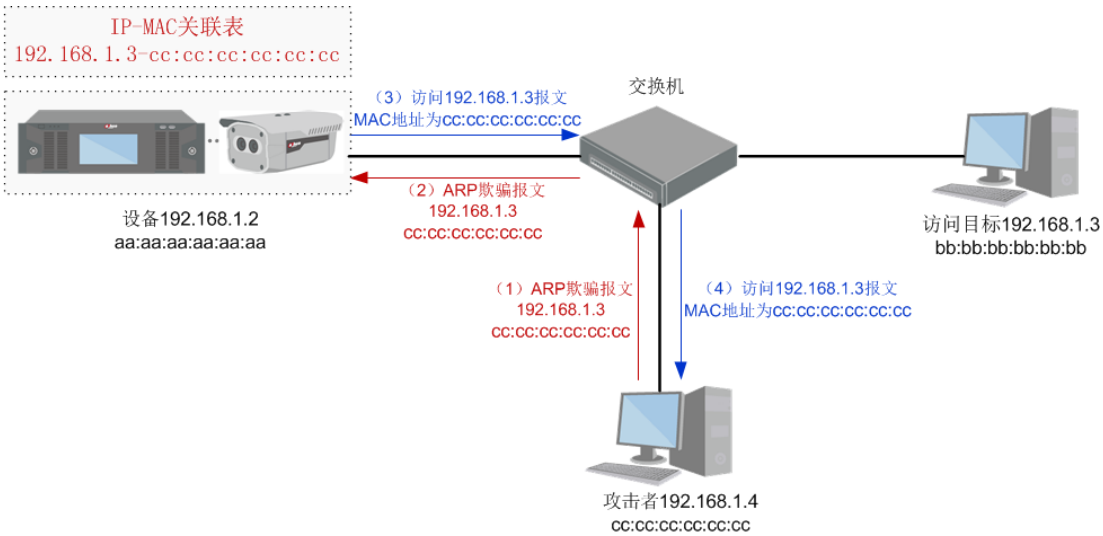
举例说明：黑名单功能就是通过丢弃指定源 IP 的数据包，可以实现拒绝指定 IP 主机对设备的所有访问。

1.3 反 ARP 欺骗技术

ARP 欺骗技术是利用不断发送 ARP 欺骗报文，更新局域网中所有主机的 ARP 表，即 IP 与 MAC 的关联表。

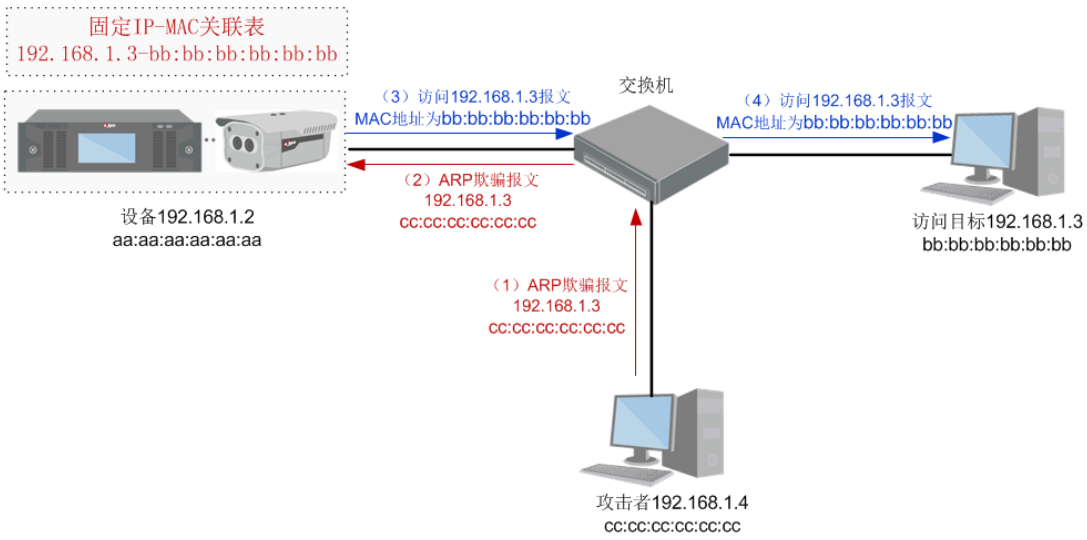
ARP 欺骗报文中填写的 IP 是欺骗的目标 IP，而 MAC 地址填写的是自己的 MAC 地址，实现其他主机对目标 IP 的访问报文被发送到攻击者的主机中，实现流量劫持，如图 1-2 所示。

图1-2 ARP 欺骗技术



反 ARP 欺骗技术是通过固定主机 ARP 表中 IP 与 MAC 的关联关系，防止 ARP 欺骗报文修改 ARP 表中的 IP 与 MAC 的关联关系，从而保证报文发送至正确的 MAC 地址，如图 1-3 所示。

图1-3 反 ARP 欺骗技术

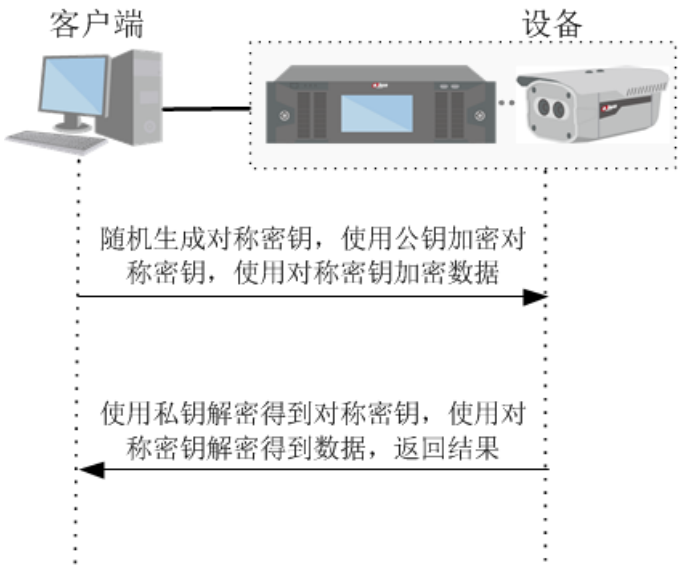


1.4 数字信封技术

数字信封类似于普通信封，普通信封在法律的约束下保证只有收信人才能阅读信的内容；数字信封则采用密钥技术保证了只有规定的接收人才能阅读信息的内容。

- 数字信封中采用了对称密钥体制和公钥密码体制。
- 信息发送者首先利用随机产生的对称密钥加密信息，再利用接收方的公钥加密对称密钥，被公钥加密后的对称密钥被称之为数字信封。
- 在传递信息时，信息接收方若要解密信息，必须先用自己的私钥解密数字信封，得到对称密码，才能利用对称密钥解密所得到的信息，从而保证数据传输的真实性和完整性，如图 1-4 所示。

图1-4 数字信封技术



1.5 本地安全存储技术

设备本地可能存放帐号等敏感信息，本地安全存储技术利用了加密芯片对数据进行加密保存。

- 加密芯片将内部应用软件的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，以保证了本地敏感数据的安全性。

1.6 安全 shell 技术

Shell 是设备的后台，拥有对 Shell 的控制权限，即拥有对设备的完整控制权限，实现查看后台数据、设置设备后台内容等功能。安全 Shell 技术可隐藏设备的完整 Shell（Shell 调试模式），并控制使用者对完整 Shell 的使用时效。

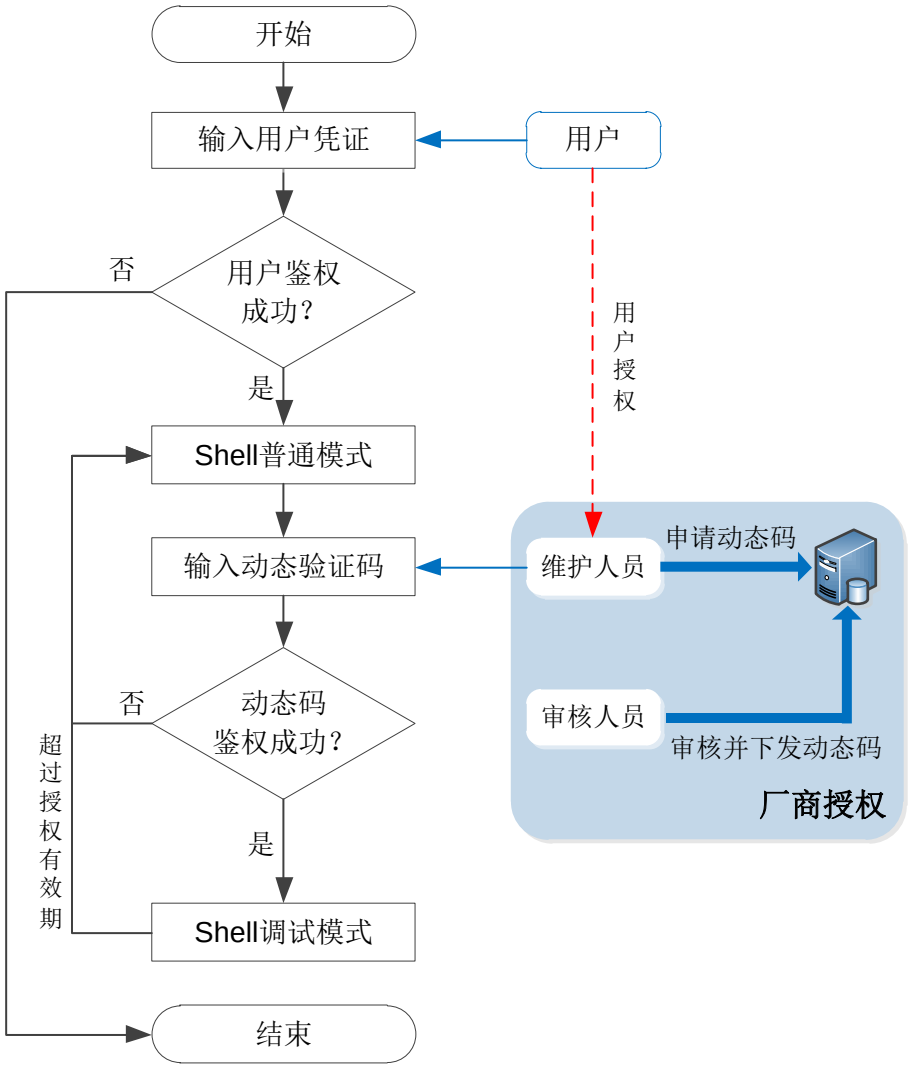
安全 Shell 技术的原理是将安全检测机制通过 hook 技术嵌入到完整 Shell 的入口处，以确保使用者只有通过安全检测机制后，才能进入到完整 Shell。

安全检测机制包括两层授权要求：

- 用户授权：使用用户凭证通过设备的帐户体系认证进入 Shell 普通模式。在 Shell 普通模式下，使用者仅支持查看日期、查看设备基本信息、查看当前模式支持命令等查询操作。
- 厂商授权：使用厂商提供的动态验证码从 Shell 普通模式进入 Shell 调试模式。在 Shell 调试模式下，使用者支持查看后台数据文件、查看进程运行情况、修改设备后台内容等操作。

成功通过两次授权验证进入 Shell 调试模式后，安全检测机制会继续进行监控。当使用者的使用时长超过授权有效期后，安全检测机制将会强制使用者退出 Shell 调试模式，返回 Shell 普通模式。此时如果需要继续使用完整 Shell，使用者必须再次获取厂商的动态验证码进行验证。具体如图 1-5 所示。

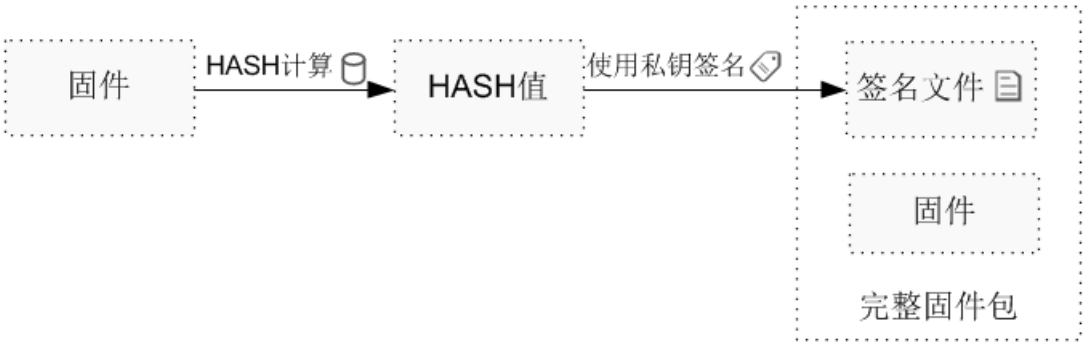
图1-5 安全 shell 技术



1.7 可信升级技术

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，对应的私钥只有厂商拥有并保存，在发布固件包时，利用了私钥的签名技术，如图 1-6 所示

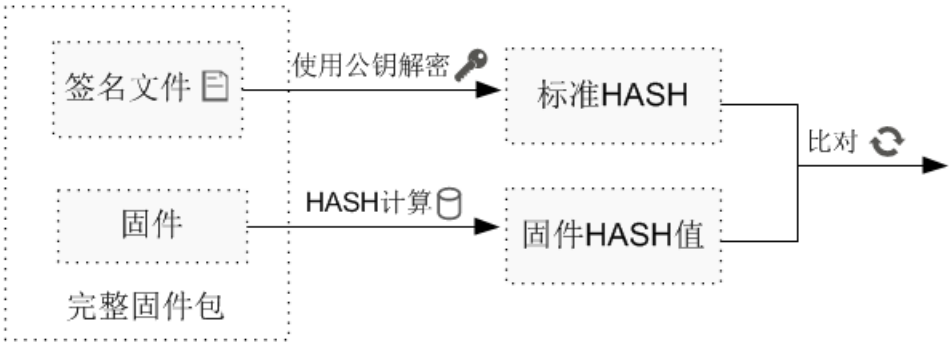
图1-6 打包可信固件



厂商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，

如图 1-7 所示。

图1-7 固件可信校验



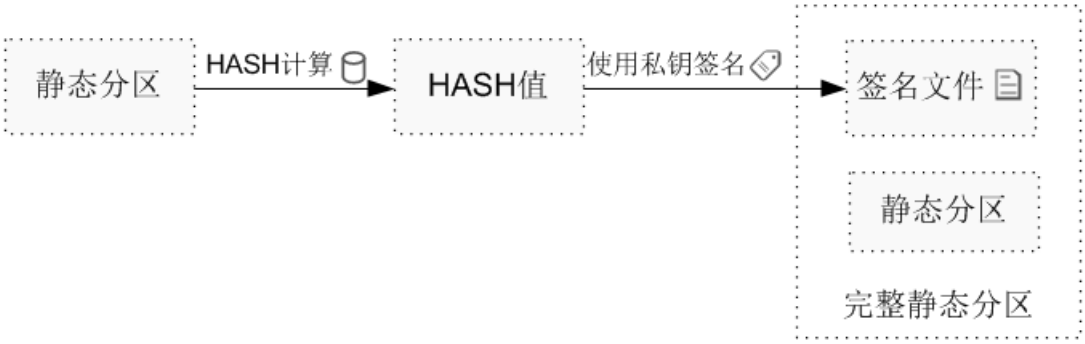
1.8 可信运行环境

可信运行环境包括了静态文件分区数据和反病毒程序两部分的数据内容检测。

1.8.1 静态文件分区数据

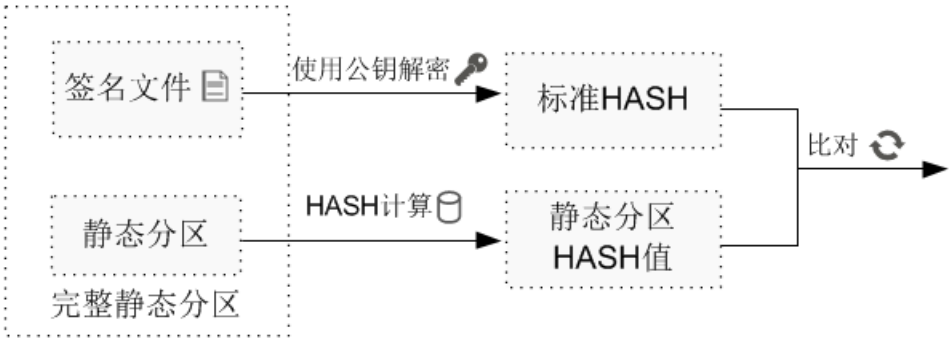
设备的静态文件分区，预先已经完成了签名，如图 1-8 所示。

图1-8 打包可信静态分区



将签名文件与静态分区存放在一起，设备启动完成后，会由内核执行分区签名校验，如图 1-9 所示。

图1-9 静态分区可信校验



如果系统检验发现静态分区数据内容不符合签名，则说明当前程序运行在不可信任的环境下，系统将会终止程序运行、停止提供服务，避免发生更多的损失。

1.8.2 反病毒程序

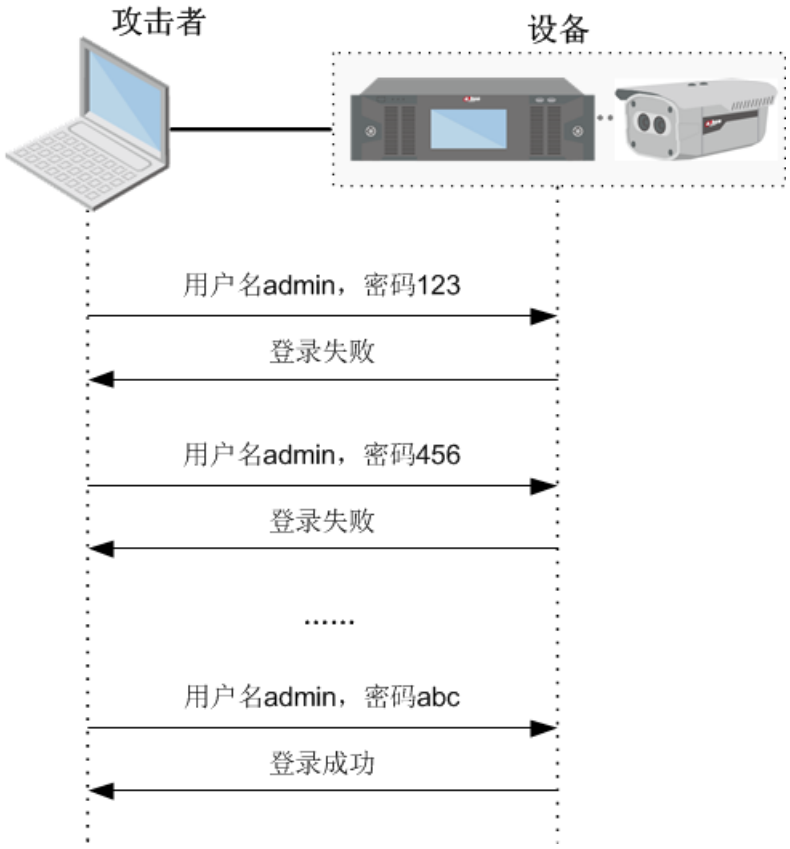
大华设备具备病毒程序识别能力，当设备中被植入病毒程序后，病毒程序尝试运行期间，将会被识别，从而拒绝此类程序的运行。识别病毒技术利用的就是 HASH 签名技术：

- 在合法可执行程序中植入程序签名。
- 程序启动期间，进入内核态调用时，内核会对程序及其签名进行校验认证。
- 判断可执行程序的可信任性，如果内核发现程序不可信任后，终止程序运行，由此达到反病毒程序的能力。

1.9 密码防爆破技术

密码爆破技术是利用高性能主机，不断向目标机的指定用户发起不同的密码尝试，直到找到正确的密码为止，如图 1-10 所示。

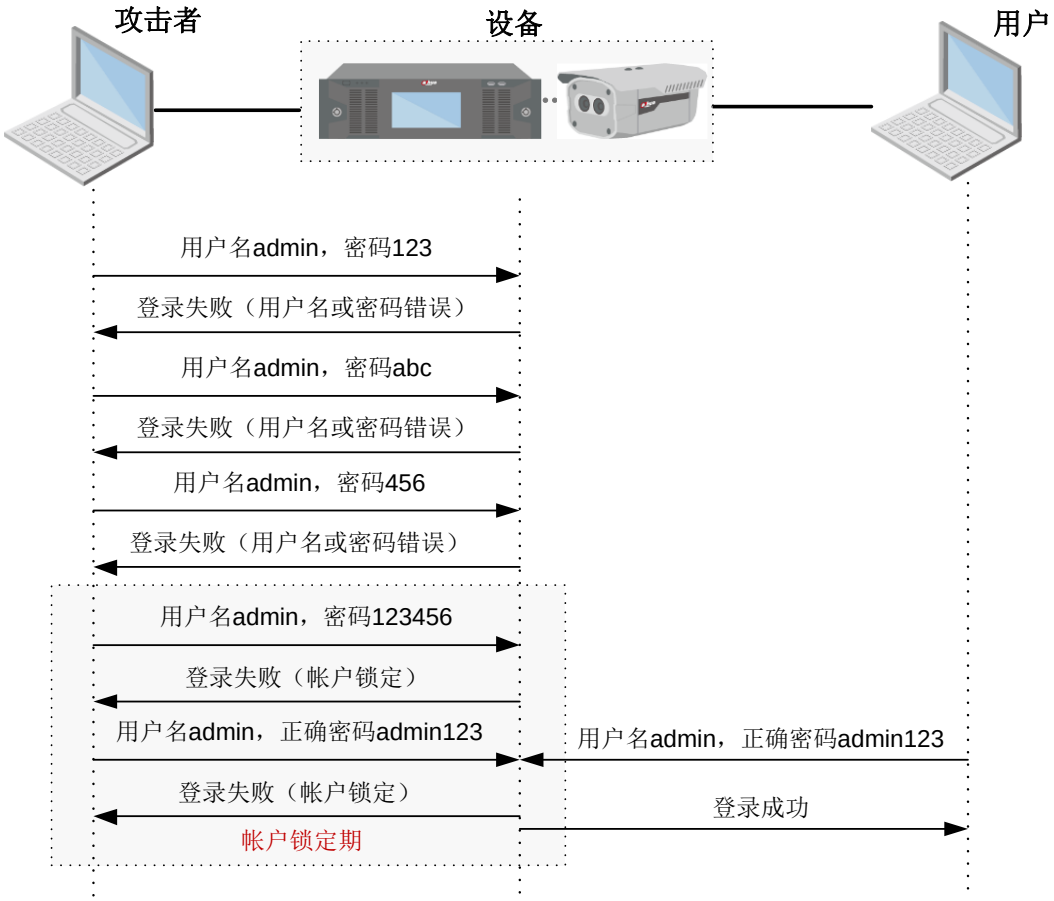
图1-10 密码爆破技术



密码防爆破技术，是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，设备进入帐户锁定期，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，如图 1-11 所示。

图1-11 密码防爆破技术



为防止恶意攻击者利用帐户锁定机制，不停发起恶意登录请求，导致正常用户无法使用设备，密码防暴破技术中融入了主机识别能力，帐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。

2 安全策略

2.1 用户管理策略

设备在出厂状态下，不存在任何的保留帐户，当用户第一次启用设备时，要求用户创建一个属于自己的初始帐户，避免存在用户未知的保留帐户，被攻击者所利用。

设备对用户使用的密码做了最低安全要求限制，引导用户使用强度较高的密码：

- 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：

- 在用户添加帐户、修改密码以及一些帐户展示界面，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。
- 在用户登录时，无论是用户名错误，还是密码错误，设备都会统一返回用户名或密码错误，保证设备帐户的不可猜测性。
- 在用户的密码修改后，设备将会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。

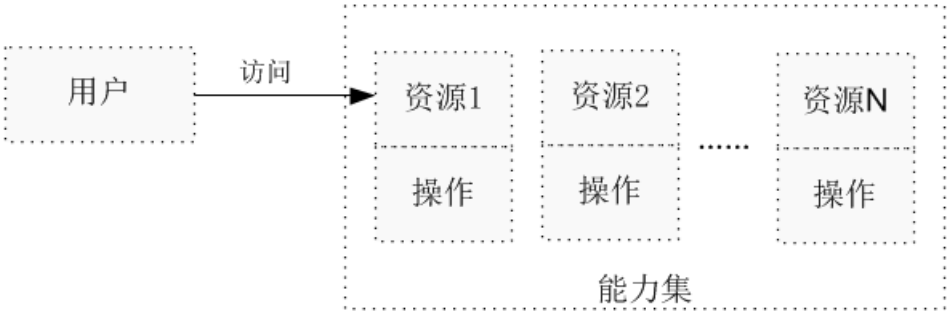
2.2 权限管理系统

大华设备帐户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。

例如，用户 A，是管理员等级用户，可以只为其分配实时预览权限、回放权限、网络管理权限，也可以为其分配管理员等级的所有权限。

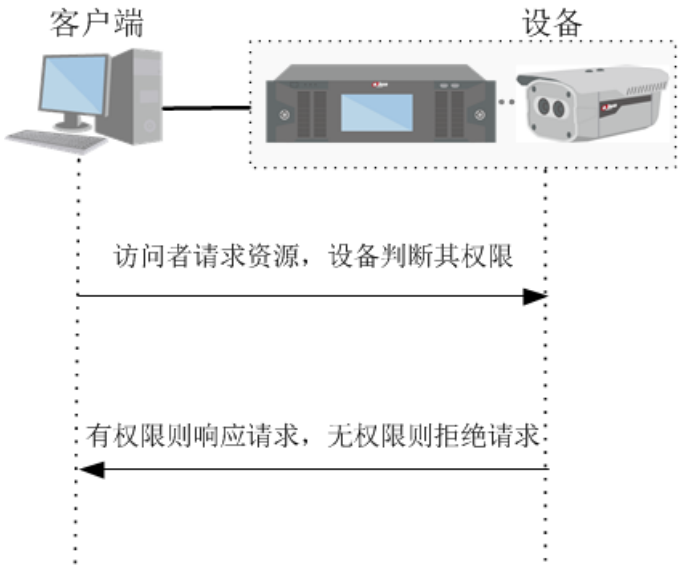
设备权限管理系统，是基于 DAC 权限控制系统实现的，设备集成了用户创建的每一个帐户所拥有的能力集，如图 2-1 所示。

图2-1 权限管理（1）



设备会依据每一个用户拥有的权限范围，控制其操作能力范围，防止越权行为发生，如图 2-2 所示。

图2-2 权限管理（2）



2.3 日志管理策略

大华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（如帐户锁定、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一份到日志服务器中。

2.4 会话管理策略

设备的 web 服务是基于短链接实现的，对此设备做了如下的会话策略：

- 客户端通过成功登录换取会话凭证，用于后续交互的身份评审，此凭证具有较强的复杂度和随机性。

- 会话凭证与登录时的客户端源 IP 绑定，禁止其用于其他主机发起的请求。
- 当设备发现有主机不断的尝试请求，但携带的却是不同的错误凭证，此行为将会被认定为会话凭证爆破行为，设备将会强制注销该主机 IP 相关联的所有会话，以保护其会话的安全性。

2.5 网络服务策略

设备关闭默认状态的部分服务，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，以替代一些较为不安全的网络服务功能：

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

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

2.6 证书导入

设备出厂状态下所拥有的证书是由厂商提供的，为了解决用户的证书信任问题，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的更新证书，更加安全的应用证书。

【社会的安全 我们的责任】

SOCIAL SECURITY IS OUR RESPONSIBILITY

浙江大华技术股份有限公司

地址：杭州市滨江区滨安路1187号

邮政编码：310053

客服热线：400-672-8166

公司网址：www.dahuatech.com