Huawei LiteOS 安全技术白皮书

文档版本　02

发布日期　2017-09-23

商标声明

 、HISILICON、海思和其他海思商标均为深圳市海思半导体有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

深圳市海思半导体有限公司

地址：深圳市龙岗区坂田华为基地华为电气生产中心　　邮编：518129

网址：http://www.hisilicon.com

客户服务电话：+86-755-28788858

客户服务传真：+86-755-28357515

客户服务邮箱：support@hisilicon.com

前 言

概述

Huawei LiteOS 是华为面向物联网领域的轻量级操作系统，属于单进程多线程的实时操作系统。

结合 Huawei LiteOS 的安全架构，从不同的安全维度阐述 Huawei LiteOS 的安全技术及建议，最后梳理出 Huawei LiteOS 的安全发展趋势。

产品版本

与本文档相对应的产品版本如下。

产品名称	产品版本
Hi3516A	V100
Hi3516D	V100
Hi3518E	V200
Hi3518E	V201
Hi3516C	V200
Hi3516C	V300
Hi3559	V100
Hi3556	V100
Hi3559A	V100
Hi3516E	V100

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师

- 软件开发工程师

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 02 (2017-09-23)

添加 Hi3559V100/Hi3556V100 的相关内容

文档版本 01 (2017-06-12)

产品版本中添加 Hi3516A/Hi3516D 及 Hi3518EV20X/Hi3516CV200

文档版本 00B01 (2017-04-18)

第 1 次临时版本发布。

目 录

插图目录

1 Huawei LiteOS 安全技术白皮书

1.1 简介

Huawei LiteOS 操作系统，是华为面向物联网领域的操作系统，它由自研的 10KB 级实时嵌入式操作系统、文件系统、标准接口库、轻量级网络协议栈、互联互通中间件组成。

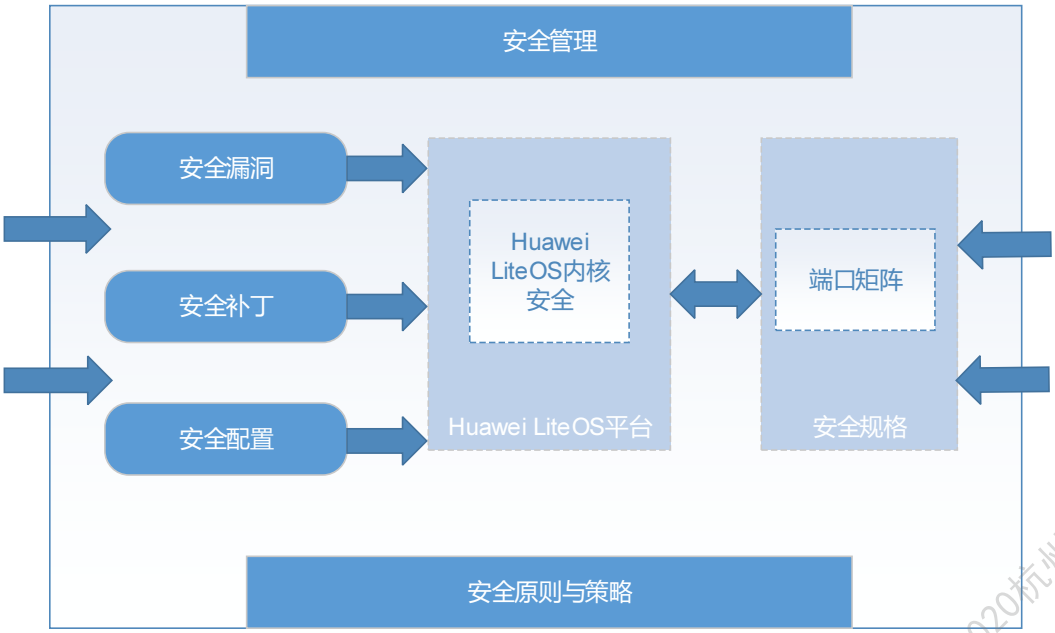
与其他操作系统（服务器操作系统、Linux 嵌入式操作系统等）不同，Huawei LiteOS 操作系统属于单进程多线程的实时操作系统，应用于物联网领域的消费类操作系统，用户面、控制面和管理面三面合一，没有用户态和内核态的概念，也没有用户概念和账号口令安全配置，没有权限控制管理、日志及审计用途。

1.2 Huawei LiteOS 安全解决方案

1.2.1 安全架构

Huawei LiteOS 安全架构如图 1-1 所示。

图1-1 Huawei LiteOS 安全架构图



Huawei LiteOS 操作系统属于嵌入式实时操作系统，是一种单用户单进程的系统，没有用户态和内核态概念，产品的应用程序与 Huawei LiteOS 在一个进程空间内运行。

Huawei LiteOS 操作系统的整体安全框架具有以下几个特点：

- 识别操作系统平台级别的安全漏洞。
- 提供安全加固的处理解决方案。
- 评估 Huawei LiteOS 操作系统的安全级别。
- Shell 和 Telnet 支持可裁剪，用户通过 Shell 和 Telnet 可以查看和修改任意系统数据，执行任意代码。
- Tftp 支持可裁剪，用户通过 tftp 可以上传和下载任意系统数据。

1.2.2 安全维度

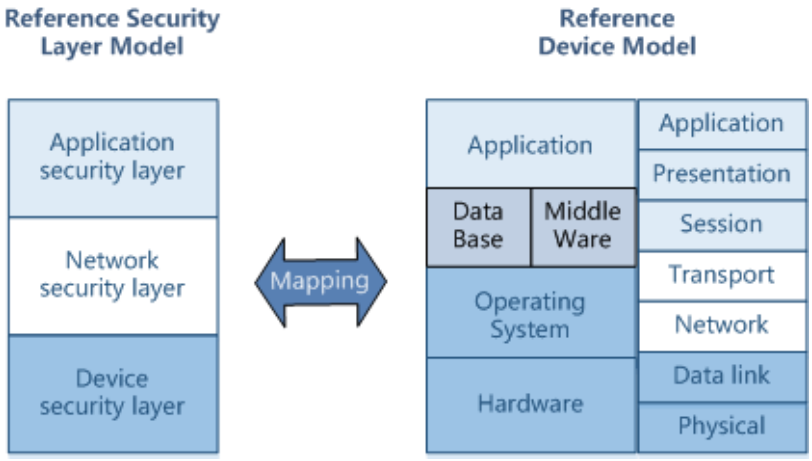
1.2.2.1 隐私

Huawei LiteOS 操作系统本身不涉及隐私数据和敏感数据，Huawei LiteOS 上的应用程序都是出厂前厂家预置好的，用户不可安装，大大减少隐私泄露的风险。

1.2.3 安全层

安全从层次上分为设备安全层、网络安全层和应用安全层，这三层和系统软件映射关系如图 1-2 所示：

图1-2 安全层、网络安全层和应用安全层和系统软件映射关系



下面将分别按照此三层描述 Huawei LiteOS 在这三层的上的安全防范机制。

1.2.3.1 设备安全层

对于设备安全层，Huawei LiteOS 从以下方面进行防护：

Huawei LiteOS 通过安全扫描工具确保系统可以排除任何不安全的漏洞，保证系统没有高风险的漏洞。

1.2.3.2 网络安全层

对于无线网络来说，产品负责采用 WiFi 芯片内置的 WPA 协议来对 Huawei LiteOS 设备的接入进行认证，确保接入端的身份安全可靠。

1.2.3.3 应用安全层

- 建议用户在插入 SD 卡或硬盘前，对存储介质进行病毒扫描；
- 建议厂商对 USB 中的可执行代码有校验（身份或签名），或禁止执行 USB 中的代码；
- 建议厂商的 WiFi 接入协议有认证；
- 建议厂商的应用程序与手机的 APP 之间有认证；
- 建议厂商对账号口令单向加密存储，建议采用安全加密算法；
- 建议厂商评估是否需要审计日志；
- 建议厂商对安全性要求高的业务提供加密传输机制；
- 建议厂商的应用程序对读取的数据进行校验(大小、类型、格式)；
- 建议厂商的应用程序自行考虑权限控制模型；
- 建议厂商配置 watchdog 功能来进行重启机器。

1.2.4 安全准则及策略

Huawei LiteOS 当前安全需求主要为系统安全加固类需求，包括系统接入安全、漏洞修复等，无安全敏感性需求。

Huawei LiteOS 基于新的功能、以及新的安全需求的基础上提供新的版本，这有助于产品是最新的安全级别。

Huawei LiteOS 以标准的操作系统安全测试工具进行安全性评价，如 nessus、nmap 等，提高 Huawei LiteOS 系统的安全能力。

1.2.5 安全管理

1.2.5.1 安全策略管理

通过安全扫描工具确保系统可以排除任何不安全的漏洞，保证系统没有高风险的漏洞。

1.2.5.2 安全威胁和攻击管理

采用端口扫描工具来发现打开的端口是否合理并最小化，关闭不必要的端口来减少安全威胁攻击。

Shell、telnet 和 tftp 等调测功能需禁止在正式产品使用。

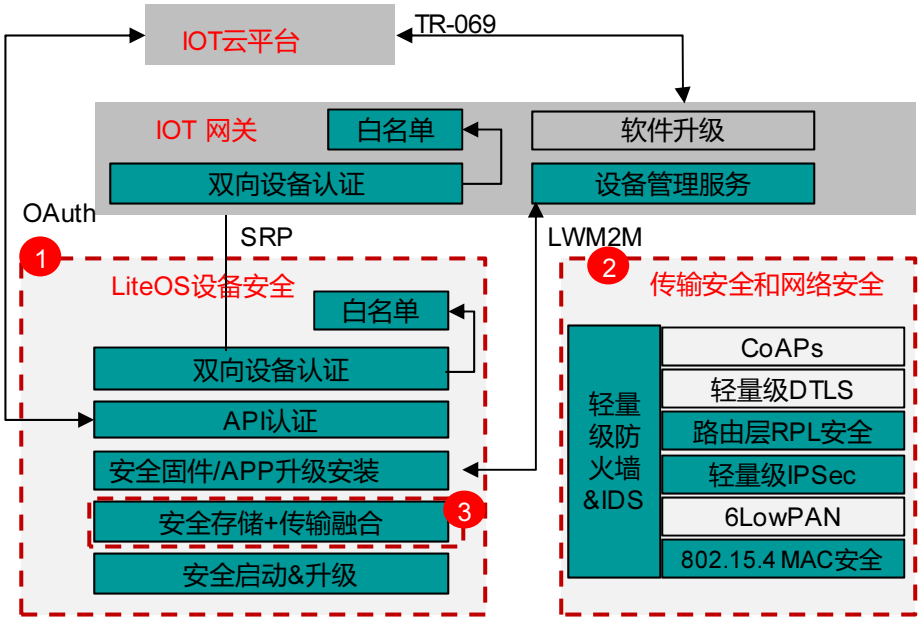
采用 Huawei LiteOS 系统的产品与手机 APP 之间是采用 WiFi 信道进行 WiFi 连接。产品负责采用 WiFi 芯片内置的 WPA 协议来进行 WiFi 接入认证。

Huawei LiteOS 系统可通过 USB 读写 SD 卡的视频和图像等数据，不会执行 SD 卡内的可执行文件，且 Huawei LiteOS 只提供 SD 卡基本读写操作，不涉及加解密。存储的安全部分需要产品去负责。

1.2.6 安全技术发展趋势

当前业界的 IoT 设备侧的安全措施不完备，其中以认证和传输安全为主，缺乏设备级的安全及防攻击措施。Huawei LiteOS 安全技术规划如图 1-3 所示。

图1-3 Huawei LiteOS 安全技术规划



Huawei LiteOS 致力于构建完备的设备侧安全能力、轻量级 E2E 安全传输、以及安全存储与传输结合的差异化能力。

- 轻量级、完备的设备侧安全

  安全启动、Firmware/APP 安全升级，网关设备白名单，安全应用安装。FW 合法性校验，异常自动恢复。

- 跨层及轻量级的网络安全机制

  802.15.4 Security（MAC layer）+Lightweight IPSec+Lightweight DTLS+RPL 安全。轻量级 Firewall、IDS(入侵检测)。

- 存储和传输融合的数据安全机制

  相比分离方式，通过存储与传输相融合的方式，对数据的进行安全处理，使得计算量和功耗大幅降低。

1.3 推广

1.3.1 客户价值

客户的期望价值包括：

- 平台级安全性得到了保证。
- 提供了产品的安全性，有助于微调最终产品的安全性配置选择。

1.3.2 价值体现

- 提供平台级安全性

  - 消除模块在操作系统级别的安全威胁
  - 操作系统级别的安全性评价报告让最终客户产放心
- 提供安全配置机制
  - 使客户可根据自身需求来配置模块的裁剪性