ICS 33.050

M 30

电信终端产业协会标准

T/TAF XXX-XXXX

物联网设备安全平台技术要求和分级方法

Technical Requirements and Classification Guideline for Security Platform of IoT Devices

XXXX－XX－XX 发布

XXXX－XX－XX 实施

电信终端产业协会 发布

目次

前　言

标准按照 GB/T-2009 给出的规则起草。

本标准中的某些内容可能涉及专利。本标准的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、安谋科技（中国）股份有限公司、中国—东盟信息港股份有限公司、阿里巴巴（中国有限公司）、高通无线通信技术(中国)有限公司、北京豆荚科技有限公司。

本标准主要起草人：魏凡星、路晔绵、国炜、李煜光、张炳华、张晓楠、杜欢、沈伟、黄天宁、崔晓夏、王江胜、杨子光、冯杨森。

引　　言

近年来，物联网的发展进入万物互联的新时代，移动支付，共享单车，智能音箱等等，这些物联网设备给现代生活带来了便捷，但也面临更多的安全威胁。针对种种安全威胁，涌现了不同的安全解决方案，如 TEE、SE 等。基于不同的处理器架构，业界也提出了不同的安全平台框架，但对此没有统一的标准。基于上述考虑，提出物联网设备安全平台技术要求和分级方法，规范物联网设备的安全性要求，为国内该领域的相关产品的测评提供依据，来促进产业的健康稳定发展。

物联网设备安全平台技术要求和分级方法

1 范围

本标准规定了物联网设备安全平台技术要求和分级方法，包括对安全目标分析、安全威胁分析、安全功能要求及分级方法等。

本标准适用于物联网终端安全平台。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

TAF-WG4-AS0008-V1.0.0:2017移动终端安全环境安全评估内容和方法

3 术语、定义和缩略语

3.1 术语和定义

3.1.1

安全平台 Secure Platform

为物联网设备提供安全服务的所有硬件、固件和软件部分。

3.1.2

安全启动 Secure Boot

安全平台在启动过程中对将要执行的软件或固件进行验证，以确保只有合法代码能够在物联网设备上运行。

3.1.3

安全存储 Secure Storage

为安全平台资产提供存储，以确保只有合法代码能够读写安全平台资产。

3.1.4

固件 Firmware

与设备硬件进行交互的软件。

3.1.5

防回滚 Rollback Protection

防回滚机制保证设备只接受新版本的固件和数据，防止设备加载包含已知错误或漏洞的旧版本固件，防止设备加载非法数据。

3.1.6

绑定 Binding

数据的一种属性，绑定到特定的设备。

3.1.7

远程验证 Remote Attestation

是软件证明其身份的一种机制，目的是向远程实体证明其操作系统和应用程序软件的完整性和真实性。

3.1.8

信任根 Root of Trust

包含硬件、代码和数据，能够验证下个 RoT 的完整性和真实性。

3.1.9

生命周期 Life Cycle

生命周期用来标识安全平台在不同生命阶段的状态，包括开发、制造、使用、调试、直到终止使用。在不同的生命阶段，安全平台具有不同的安全属性。

3.1.10

鲁棒性 Robustness

系统正确执行以及处理意外终止和意外操作的能力。

3.2 缩略语

下列缩略语适用于本文件：

DDR	Double Data Rate	双倍速率
HUK	Hardware Unique Key	硬件唯一密钥
ST	Security Target	安全目标
ROM	Read Only Memory	只读存储器
SP	Secure Platform	安全平台
RoT	Root of Trust	信任根
FW	Firmware	固件
SIM	Subscriber Identity Modula	用户识别卡
TEE	Trusted Execution Environment	可信执行环境

TPM	Trust Platform Module	可信平台模块
SE	Secure Element	安全单元
OTP	One Time Programmable	一次性可编程

4　安全平台概述

4.1　安全平台范围

本标准所针对的范围为给物联网设备不可信环境提供基本安全服务的安全平台。评估的范围包括安全平台用来提供安全服务的所有相关的硬件、固件和软件部分。

4.2　安全平台逻辑框架

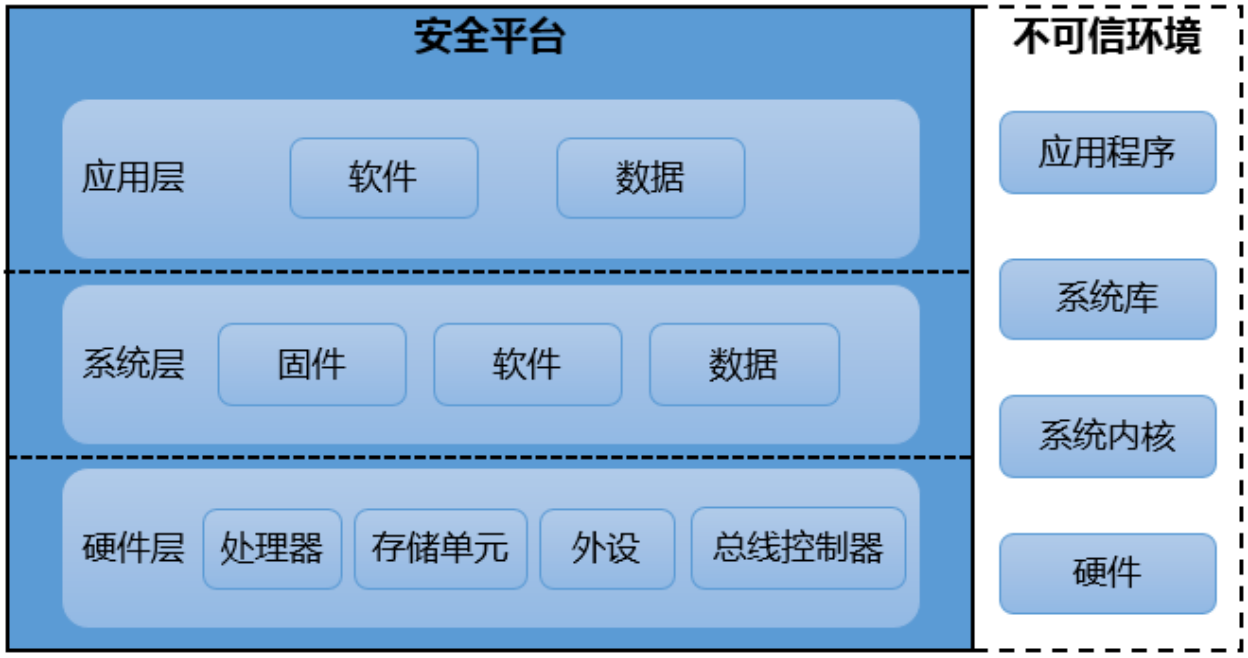

图 1 物联网设备安全平台逻辑框架

物联网设备安全平台逻辑框架如图 1，旨在抽离出安全平台的逻辑架构。逻辑架构分为硬件层、系统层、和应用层；图 1 中不可信环境包括硬件、系统内核、系统库、应用，不可信环境的安全要求不在本规范的范围内。

4.3　安全平台功能框架

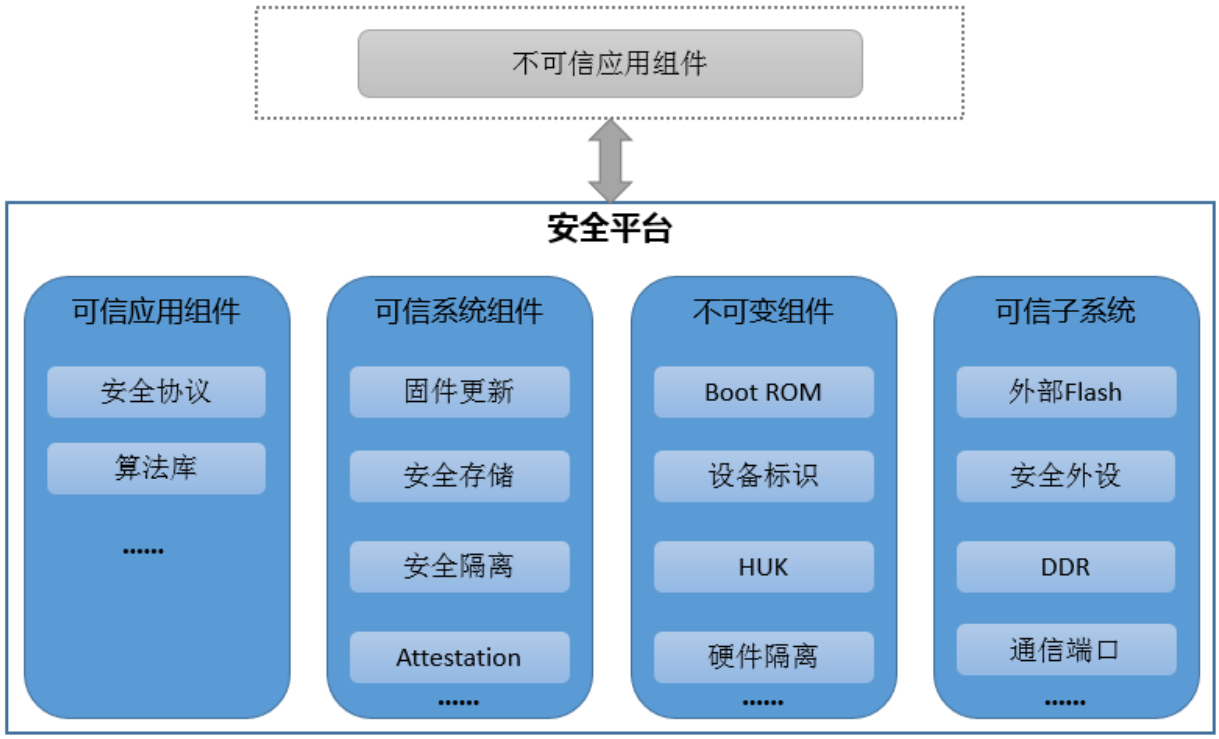

图 2 物联网设备安全平台功能框架

物联网设备安全平台功能框架如图 2 所示，主要包括可信子系统、不可变组件、可信系统组件、可信应用组件四个部分。其中：

可信子系统：通常是拥有独立功能的子系统，例如 DDR 控制器、SIM、TPM 等，自身拥有独立的信任根和安全生命周期，不能直接访问不可变组件、可信系统组件和可信应用组件的代码和数据。子系统可依照相关标准单独认证；

不可变组件：包含两个部分，一部分是是不可更改的、与设备绑定的软件资源；另一部分是防篡改的硬件。例如启动代码、设备标识、HUK、OTP、Boot ROM、硬件隔离的存储单元等；

可信系统组件：是运行在硬件上的固件及服务，例如安全存储、安全隔离、固件更新、远程验证等安全服务；

可信应用组件：是运行在可信环境中，调用可信系统组件，实现特定功能的一组应用软件。

不可信应用组件：是运行在不可信环境中的应用软件，通常包含第三方或开源的库，不能直接访问可信应用组件的资源，也不能直接访问不可变组件和可信系统组件的资源。其安全要求不在本规范的范围内。

5 安全平台的资产

a) HUK 的保密性、完整性和可用性；公共密钥的完整性和可用性；对称密钥和私钥的保密性、完整性和可用性。

b) 启动代码和其数据的完整性和可靠性。

c) 存储的保密性、可靠性、一致性、原子性，存储的权限管理。存储密钥生成机制及密钥的保密性、完整性和原子性。

d) 固件代码的可靠性、一致性和完整性。

e) 可信系统组件运行时数据的完整性。

f) 不可变组件持久化数据的完整性，保密性，与设备绑定。

g) 可信应用组件代码的可靠性和一致性。

h) 可信应用组件的数据和密钥与设备绑定，其数据和密钥保密性、原子性、一致性。

i) 生命周期状态的真实性和完整性。

j) 随机数的随机性，满足一定的熵值。

k) 设备标识的唯一性和不可篡改。

6 安全目标

物联网设备安全平台的安全目标是其具有的安全功能可以防御附录 B 中描述的安全威胁，保证安全平台资产不被非法获取。物联网设备安全平台的安全目标包括：

a) 防止攻击者在安全平台中加载和执行非法代码并破坏安全平台资产；

b) 防止攻击者绕过更新机制篡改或安装旧版本的固件；

c) 防止攻击者通过利用加密算法的漏洞、输入格式错误的参数、绕过生命周期检查、非法访问调试接口等方法篡改安全平台的资产；

d) 防止远程平台把非法的设备识别为合法设备。

7 安全平台安全功能要求

根据不同的安全平台使用的场景和其所支持的安全能力的程度，将安全平台安全的安全技术能力划分为三个级别，每一级别定义了安全平台在相应等级对应的安全能力的最小集合，具体的要求见 7.1 到 7.9 节。

7.1 安全隔离

一级安全功能要求：

a) 安全平台应与不可信应用组件隔离，不可信应用组件无法直接访问安全平台的资源；

b) 如果不可信应用组件和安全平台有共享资源时，不可信应用组件访问共享资源时应有权限访问控制机制。

二级安全功能要求：

a) 可信应用组件应与可信系统组件和不可变组件隔离，可信系统组件应有访问控制机制，可信应用组件需要通过可信系统组件提供的访问控制来访问可信系统组件和不可变组件的资源；

b) 应保证可信应用组件与可信系统组件之间通信的安全性和鲁棒性。

三级安全功能要求：

a) 可信应用组件间应隔离，每个可信应用组件只允许访问自己的资源；

b) 应保证可信应用组件之间通信的安全性和鲁棒性。

7.2 安全启动

一级安全功能要求：

a) 应从不可变代码执行启动。

二级安全功能要求：

a) 应有对可信系统组件、可信应用组件或其他安全子系统的签名验证机制和完整性保护机制；

三级安全功能要求：

a) 应在引导时，计算和验证所有可更新的可信系统组件和可信应用组件并记录其引导状态。

7.3 安全存储

一级安全功能要求：

a) 应有安全平台资产存储的保密性和完整性保护。

二级安全功能要求：

a) 安全存储应与安全平台绑定，只有当前安全平台才能从安全存储中访问和修改资产；

b) 当安全平台执行完安全存储后，安全平台的 RAM 中不应保存处理过的数据。

三级安全功能要求：

a) 安全存储应具备数据防恢复机制，防止新数据被旧数据覆盖。

7.4 密码算法和密钥

一级安全功能要求：

a) 应使用符合国家有关法规规定的加解密算法为安全平台提供服务；

b) 密钥在生成、存储和使用过程中应保证其不被泄露；

二级安全功能要求：

a) HUK 若需存储，则存储在不可篡改区域。

b) 随机数发生器产生的随机数应满足一定的熵，并符合国家有关法规规定。

三级安全功能要求：

a) 安全平台应使用真随机数发生器，应具备防干扰的安全机制，防止攻击者预测出随机数。

b) 安全平台应提供防物理攻击的安全机制，物理攻击包括但不限于侧信道攻击、故障注入攻击、侵入式攻击。

7.5 固件版本控制

一级安全功能要求：

a) 固件应拥有版本标识，实现版本控制；

b) 固件版本控制应支持防回滚；

7.6 固件安全更新

一级安全功能要求：

a) 当固件本地更新或者远程更新时，应在更新安装之前验证其完整性和可靠性，若更新失败则继续运行更新之前的版本。

7.7 安全生命周期

一级安全功能要求：

a) 安全平台在使用阶段应禁用调试端口或提供进入安全调试模式的访问控制机制。

b) 安全平台进入调试模式时，应禁止不可信应用组件访问安全平台资产。

注：安全平台的开发和制造阶段的安全性不在本标准的范围内。

二级安全功能要求：

a) 安全平台进入异常状态时，应擦除所有运行时的安全平台资产，防止资产泄露。

三级安全功能要求：

a) 如果可信应用组件是动态加载的，安全平台应验证其完整性和可靠性。

b) 安全平台进入终止状态时，应擦除所有安全平台的资产，防止资产泄露。

7.8 绑定

二级安全功能要求：

a) 可信系统组件所使用的密钥应与设备绑定，可从 HUK 派生。

三级安全功能要求：

a) 安全平台应向可信应用组件提供密钥和其他敏感信息与设备的绑定服务。

7.9 远程验证

二级安全功能要求：

a) 安全平台应提供初始证明服务，负责上报设备的标识、固件验证结果和设备的运行时状态，由远程实体进行验证；

b) 安全平台在出厂前应内置用于远程验证的密钥和设备标识，并存储在不可变硬件中。

c) 引导程序应对可信子模块的引导状态进行完整性校验，并将结果包含在初始证明中。

三级安全功能要求：

a) 安全平台应提供运行时证明服务，负责上报安全平台的标识和安全平台的运行时状态，由远程实体进行验证。

附录 A

（规范性附录）

标准修订历史

修订时间	修订后版本号	修订内容
2019 年 3 月	草稿	全文格式
2019 年 7 月	征求意见稿	全文格式
2019 年 12 月	征求意见稿	全文格式
2020 年 4 月	送审稿	全文格式

附 录 B
（资料性附录）

本小节定义了安全平台可能受到的安全威胁。

a) 功能滥用

可信系统组件和可信应用组件的功能可能被滥用，修改可信组件的行为以便获取或修改敏感数据、执行非授权的操作；

调试功能滥用，调试功能可能被滥用并破坏安全平台资产。

b) 克隆

将一个设备上的可信应用组件和可信系统组件的代码或数据拷贝到另一个设备上，并在该设备上成功运行。

c) 恶意代码攻击

在可信应用组件和可信系统组件中注入恶意代码，获取或者修改敏感数据，以及执行非授权的操作。

d) 非易失存储攻击

非易失存储介质中可信应用组件和可信根系统组件的代码和数据被读取和篡改。

e) 易失存储攻击

可信 RAM 内数据易被读取，恢复部分或者全部的 RAM 内容。

f) 侧信息泄露

可信系统组件和可信应用组件在操作过程中易受到侧信道、故障注入攻击，从而恢复敏感信息或密钥。

g) 数据回滚

固件、存储数据易受到回滚攻击。

h) 随机数发生器攻击

非授权获取随机数信息；

干扰随机数发生器从而预测出随机数。

i) 接口攻击

攻击者通过使用非法的上下文或者非法的参数实例化安全平台的接口，从而获取敏感数据或执行非法操作。

j) 隐蔽信道攻击

攻击者通过隐蔽信道，以非授权或非法的方式从安全平台获取敏感数据或往安全平台上传输信息。

参 考 文 献

电信终端产业协会团体标准

物联网设备安全平台技术要求和分级方法

T/TAF XXX—XXXX

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn