国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

X.1352

（09/2022）

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 物联网（IoT）安全

物联网设备和网关的安全要求

ITU-T X.1352建议书

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1350–X.1369**
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	X.1400–X.1429
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1352建议书

物联网设备和网关的安全要求

概要

ITU-T X.1352建议书建立了适用于物联网（IoT）设备和网关的五个安全维度的详细要求：认证、加密、数据安全、设备平台安全和物理安全，这些安全要求基于ITU-T Y.4100建议书中规定的IoT参考模型和ITU-T X.1361建议书中规定的IoT安全框架。

认证维度包括用户认证、认证证书的安全使用和设备认证。加密维度包括安全密码使用、安全密钥管理和安全随机数生成。数据安全维度包括安全传输和存储、信息流控制、安全会话管理和个人可识别信息（PII）管理。设备平台安全维度包括五个要素：软件安全；安全更新；安全管理；日志和时间戳。同样，物理安全维度包括安全物理接口和防篡改。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1352	2022-09-02	17	11.1002/1000/14990

关键词

认证、加密、数据安全、设备平台安全、IoT设备和网关安全、IoT网关、IoT安全评估、物理安全

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1352建议书

物联网（IoT）设备和网关的安全要求

1 范围

本建议书建立了适用于物联网（IoT）设备和网关的五个安全维度的详细要求：认证；加密；数据安全；设备平台安全和物理安全。这些安全要求基于[ITU-T Y.4100]中规定的IoT参考模型和[ITU-T X.1361]中规定的IoT安全框架。

2 参引

下列ITU-T建议书和其他参引的条款，通过在本文本中的引用而构成当前建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参引均面临修订；因此鼓励本建议书的使用者探讨使用下列建议书和其他参引最新版本的可能性。当前有效的ITU-T建议书清单定期出版。在本建议书中引用某个独立文件时，并未给予该文件建议书的地位。

[ITU-T X.1361] ITU-T X.1361（2018）建议书，基于网关模型的物联网安全框架。

[ITU-T Y.4100] ITU-T Y.4100/Y.2066（2014）建议书，物联网的共同要求。

3 定义

3.1 他处定义的术语

本建议书使用了下列他处定义的术语：

3.1.1 认证（authentication） [b-ITU-T X.1254]：对声称的实体身份提供保证。

3.1.2 能力（capability）[b-ISO 16100-1]：一组功能和业务，以及一组用于评估功能提供者绩效的标准。

3.1.3 机密性（confidentiality）[b-ITU-T X.800]：信息不被未授权的个人、实体或过程获得或者泄露给未授权的个人、实体或过程的属性。

3.1.4 证书（credential）[b-ITU-T X.1252]：作为被声称的身份和/或权利的证明的一组数据。

3.1.5 密码质量随机数（cryptographic-quality random number） [b-ITU-T X.667]：通过某种机制生成的一个随机数或伪随机数，它确保重复生成的值的充分传播，以便可用于加密工作（及用于此类工作）。

3.1.6 密码学（cryptography）[b-ITU-T X.800]：由原理、手段和方法等组成的学科，用于数据转换，以便隐藏其信息内容，防止其被不可察觉地修改与/或防止其被未经授权地使用。

3.1.7 数据完整性（data integrity）[b-ITU-T X.800]：数据未被以未授权方式修改或破坏的特性。

3.1.8 设备（device）[b-ITU-T Y.4000]：在物联网中，具有强制性通信能力和选择性传感、激励、数据捕获、数据存储和数据处理能力的一件装备。

3.1.9 密钥管理（key management） [b-ITU-T X.800]：依据安全策略生成、存储、分发、删除、存档和应用密钥。

3.1.10 补丁管理（patch management）[ITU-T X.1361]：包括获取、测试和安装多个补丁到信息系统的过程。

注 – 可以考虑漏洞管理能力。

3.1.11 个人可识别信息（personally identifiable information）（PII）[b-ISO/IEC 29100]：(a) 可用于识别相关信息与之关联的PII主体的任何信息；或者 (b) 直接或间接或者可能直接或间接与PII主体联系起来的任何信息。

3.1.12 物理安全（physical security） [b-ITU-T X.800]：用于为资源提供物理保护以抵御蓄意和意外威胁的措施。

3.1.13 安全配置（secure configuration） [ITU-T X.1361]：配置网络设备的过程，以降低固有漏洞的级别，并仅提供履行其角色所需的业务。

3.1.14 安全网关（security gateway） [ITU-T X.1361]：网络之间或网络内的子组之间的连接点，或者不同安全域内的软件应用之间的连接点，旨在根据IoT环境中给定的安全策略来保护网络。

注 – 该术语有时成为“网关”。该定义改编自[b-ISO/IEC 27033-1]。

3.1.15 威胁（threat）[b-ISO/IEC 27000]：能对某个系统或组织造成伤害的有害事件的潜在起因。

3.1.16 漏洞（vulnerability）[b-ISO/IEC 27000]：可被一个或多个威胁利用的资产或控制的薄弱之处。

3.1.17 漏洞管理（vulnerability management）[ITU-T X.1361]：由识别、分类、修补和缓解漏洞等组成的过程。

3.2 本建议书中定义的术语

本建议书定义了下列术语：

3.2.1 安全维度（security dimension）：系一组旨在解决某一具体网络安全问题的安全措施。

3.2.2 设备平台安全（device platform security）：针对固件及其更新能力和第三方软件管理的一个安全集，以及有关物联网设备和网关的审计能力。

注 – 根据硬件能力，固件被操作系统上的软件所代替。

3.2.3 迷惑（obfuscation）：对程序代码或应用程序数据执行的一种操作的效果，它导致应用程序以某种方式被隐藏或遮掩，而不影响代码的输出。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

API 应用编程接口

CAPTCHA 完全自动化的公共图灵测试以区分计算机和人类

CoAP 受约束的应用协议

DoS	拒绝服务
F/W	固件
FTP	文件传输协议
H/W	硬件
ID	标识符
IDS	入侵检测系统
IMEI	国际移动设备身份
IoT	物联网
IPS	入侵防御系统
LwM2M	轻量级机器对机器
MAC	媒质访问控制
MCU	微控制器单元
MQTT	消息排队遥测传输
OS	操作系统
PII	个人可识别信息
PIN	个人身份识别码
S/W	软件
SD	安全数字
SHA	安全哈希算法
SNMP	简单网络管理协议
SSA	肩窥攻击
SWD	串行线调试
TLS	传输层安全
UART	通用异步接收器/发射器
UID	唯一标识符
UPnP	通用即插即用
USB	通用串行总线

5 惯例

本建议书使用以下惯例：

助动词“应/应该”（should）表明一项建议的、并非需要绝对遵守的要求。

助动词“须”（shall）表明一项必须得到严格遵守的要求，且如果声称遵守本建议书，则不得与该要求有任何偏差。

在本建议的正文中，有时会出现“能/能够”（can）一词，在这种情况下，它们将被解释为“能/能够”（is able to）。

附录一中助动词“应/应该”（should）的出现没有规范意图。

6 概述

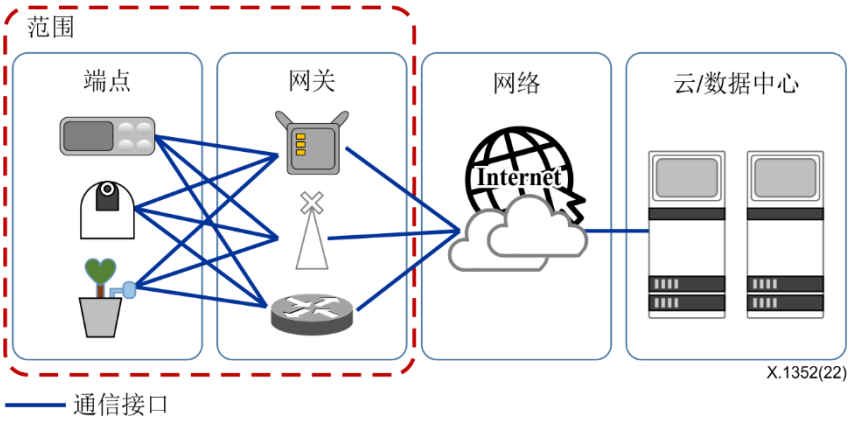


图1 – 安全要求的范围

基于附录二中所讨论的[ITU-T X.1361]和[ITU-T Y.4100]中提出的安全能力，针对五个安全维度规定了应对IoT设备和网关（不包括网络系统和平台）挑战和威胁的安全要求，即：认证；加密；数据安全；设备平台安全和物理安全。

认证维度包括用户认证、认证证书的安全使用和设备认证。

加密维度包括安全密码算法、安全密钥管理和安全随机数生成。

数据安全维度包括传输数据保护和静态数据保护、信息流控制、安全会话管理和PII保护组成。

对于设备平台安全维度，有五个项目：软件（S/W）安全；安全更新；安全管理；日志记录和时间戳。

同样，对于物理安全维度，已经规定了安全物理接口和防篡改。

图2显示了IoT设备和网关的安全维度目标。IoT设备和网关通常由微控制器单元（MCU）、通信模块、存储器和输入/输出端口组成。安全元素以硬件（H/W）或软件（S/W）的形式存在。在MCU中，有固件（F/W）、物理接口和存储器。此处，带有操作系统（OS）的S/W可以被F/W代替。通信模块要求加密，以确保传输数据的安全性。闪存中的数据被安全地存储，用于认证、加密和数据机密性/完整性。通过通用异步接收器/发射器（UART）等物理接口进行访问也需要用户认证。应移除或关闭未使用的H/W接口。

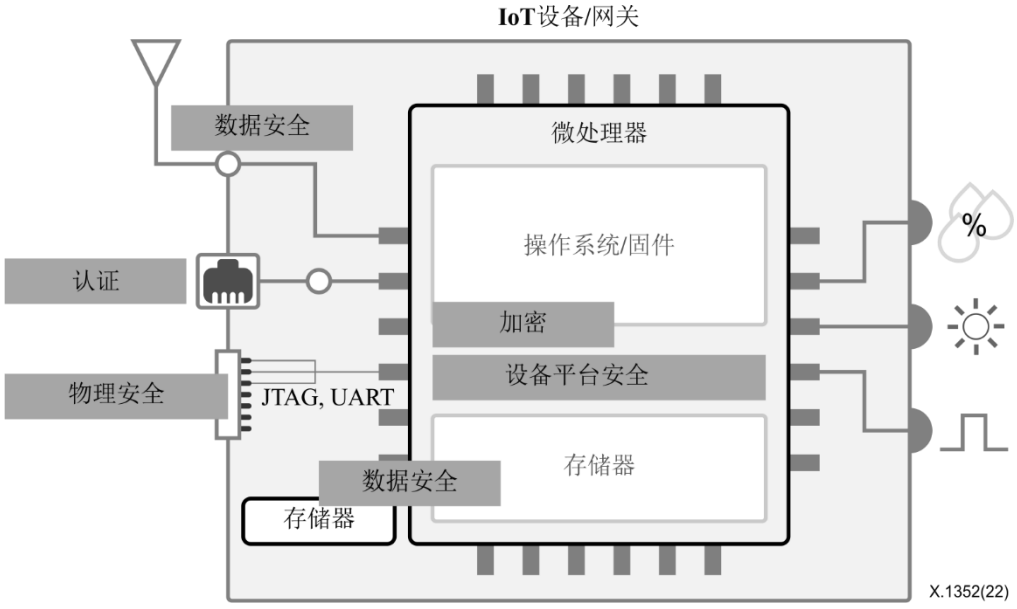


图2 – IoT设备和网关应用安全维度示例

7 IoT设备和网关面临的安全威胁/漏洞

第7.1节和第7.2节描述了IoT设备和网关的安全威胁/漏洞，这些威胁可能使它们成为网络攻击的目标。对网关的安全威胁包括对IoT设备的威胁。

7.1 IoT设备面临的安全威胁/漏洞

设备特定的威胁/漏洞包括以下内容。

– ST-D-1：旁路认证：未经授权的用户得以访问设备，也得以访问关键数据，包括存储在设备中的用户数据和配置文件。

– ST-D-2：未经授权的设备连接：设备暴露于任何未经授权的设备，或者其数据（如用户数据）能被传输到任何未经授权的设备。

– ST-D-3：过度特权：授予过度特权或不必要的特权将使攻击者能够访问所有可接受的操作和受控数据，包括设备的用户数据。

– ST-D-4：无限制的重复认证尝试：重复进行认证尝试的未经授权用户可能会获得真正用户的账号。

– ST-D-5：并发访问导致的错误：多个管理员帐户的并发访问可能会导致关键功能的配置发生不协调的变化。

– ST-D-6：认证信息暴露和猜测：当认证信息（如密码）硬编码或以明文的形式存储时，或者当认证密码或个人身份识别码（PIN）以明文的形式暴露时（也称为肩窥攻击（SSA）），认证信息可能会被攻击者暴露或猜到。

– ST-D-7：弱密码：攻击者可以获得包括默认值或弱密码在内的不安全组合，这可能允许攻击者伪装成真正的用户。

– ST-D-8：弱加密密钥/随机数：密钥不足或可预测的“随机”数可能无法保护好关键数据。

– ST-D-9：弱加密算法：攻击者可以通过分析使用弱加密算法的流量来预测关键数据或发现加密消息（密文）的明文。

– ST-D-10：缺乏输入验证：缺乏输入验证可导致设备故障。

– ST-D-11：数据暴露和数据操纵：通过设备传输或存储在设备上的用户数据、设备配置和密钥等关键数据可能会暴露给攻击者、被攻击者利用或操纵。

– ST-D-12：用户会话劫持：攻击者可能会未经授权地访问一个会话被异常关闭的真实用户帐户，或者利用使用相同密钥的多个设备的有效会话。

– ST-D-13：不安全的更新：预期的更新文件不可下载，或者其来源是未经授权/未经认证的被操纵更新文件可能是可执行的。

– ST-D-14：更新失败：更新期间发生的错误可能会导致设备运行异常。

– ST-D-15：完整性错误：对可执行代码或配置值的非预期操纵可能会导致设备出现故障。

– ST-D-16：恶意软件：具有非预期功能的代码可能会被恶意使用。

– ST-D-17：残留记忆信息利用：用于加密操作、认证和数据传输的密钥、密码和敏感数据保留在内存中，并可能被利用。

– ST-D-18：关键配置中的非预期更改：缺乏设备安全控制可能会导致关键配置中的非预期更改和不安全的业务交付。

– ST-D-19：不安全错误响应：对设备的错误和恶意行为缺乏适当的检测和响应可能会导致不安全的业务交付。

– ST-D-20：不安全的开发：潜在的安全漏洞可能源于设备的设计和实现，在测试过程中可能缺乏对这些漏洞的评估和响应，或者这种评估和响应是不适当的。

– ST-D-21：易受攻击的OS：在易受攻击的OS环境中，设备功能可能会被破坏或旁路。

– ST-D-22：易受攻击的第三方模块或库：易受攻击的第三方模块或库可能允许会攻击者调用那些有风险的模块或库。

– ST-D-23：系统日志中记录的不安全敏感信息：系统日志中记录的敏感信息可能会暴露给攻击者并被其利用。

– ST-D-24：通过调试暴露关键信息：在发布和分发设备时，关键信息可能会通过日志生成和调试暴露给攻击者并被其利用。

– ST-D-25：未经授权的物理访问：设备面临未经授权的物理访问及其配置的非预期更改。

7.2 IoT网关面临的安全威胁/漏洞

网关特定的威胁/漏洞包括以下内容。

– ST-G-1：不可信的数据传输：不可信的数据传输可导致设备故障或恶意代码的传播。

– ST-G-2：拒绝服务（DoS）或分布式DoS：DoS攻击可导致设备失去其可用性。

8 安全要求

本建议书基于第6节中定义的五个安全维度规定了IoT设备和网关的安全要求，并基于威胁模型的规定和IoT的特定功能属性等形成了一套安全要求。安全能力以[ITU-T X.1361]为基础，如附录二所述。

8.1 认证

认证维度由用户认证、认证证书的安全使用和设备认证构成。

8.1.1 用户认证

出厂默认密码须更改（AU-1-1）。

– 密码须在初始认证时或初始认证后需要改动时设置。

– 确保密码不同于初始值或先前的值。

在访问安全管理或敏感数据时，须首先识别和认证用户（AU-1-2）。

– 在访问安全管理，如设置IoT设备、用户账户或权限时，须识别和认证用户。

– 有权访问安全管理或敏感数据的用户须与普通用户分开管理。

须限制认证尝试的次数（AU-1-3）。

– 如果允许重复认证尝试，IoT设备可能易受暴力破解攻击。因此，须提供适当响应连续认证尝试的功能。

– 这项功能可使用以下方法中的一种提供：

a) 限制认证尝试次数，在特定时段内锁定账户或停用认证功能（建议将认证尝试次数限制在五次或以下，且认证功能至少停用5分钟）；

b) 超出认证尝试规定次数视为未经授权的网络流量，用户会被添加至自动锁定名单（建议将认证尝试次数限制为10次或以下）；

c) 执行完全自动化的公共图灵测试以区分计算机和人类（CAPTCHA）。

设备的预置密码应独一无二（AU-1-4）。

应提供管理用户账户和权限的功能（AU-1-5）。

– 应有可能管理IoT设备上使用的所有用户账户（包括管理员账户），例如添加和删除账户以及权限分配。

– 如果使用基于角色的访问控制模式，则明确说明IoT设备所有功能的访问权限并相应分配权限。

最小权限原则应适用于所有用户账户（AU-1-6）。

– 应将基于角色的权限分配给所有用户帐户。

应限制对管理员账户的并发访问（AU-1-7）。

– 应将管理服务的并发访问限制为同一管理员账户，并提供中断之前的访问或限制新的访问尝试的功能。

应提供就长度、周期和复杂程度而言的安全密码（AU-1-8）。

– IoT设备应提供让用户设置考虑到长度、周期和复杂程度的安全密码的功能。

8.1.2 证书的安全使用

不应使用硬编码证书（AU-2-1）。

– 密码（PIN、密文等）不应以硬编码或明文形式存储。

在通过密码进行认证的过程中，应该隐藏密码（AU-2-2）。

– 如果密码以明文显示，可能易遭受SSA。因此，为避免密码在输入时显示，应该隐藏密码的组成字符，例如使用星号（“*”）。

不应提供对认证失败的具体反馈（AU-2-3）。

8.1.3 设备认证

每个硬件设备的唯一标识符（UID）须保留（AU-3-1）。见表 1。

– IoT设备须拥有唯一且固定的标识符（ID）。

表1 – IoT设备的UID

ID	说明
媒质访问控制（MAC）地址	分配给网络接口的唯一标识符，用于在网段的数据链路层通信（48位）。
国际移动终端认证号码 – 国际移动设备身份（IMEI）	智能手机的唯一号码。 手机发售时由制造商分配。 共由15位数字构成，包括：核准码（八位）； 型号序列号（六位）；和验证号（一位）。

在传输敏感数据或出于控制目的将设备互连之前，设备应相互认证（AU-3-2）。

– 相互认证示例如下：

a) 使用基于公钥加密方法的私钥；

b) 使用安全属性（UID、密钥等）和安全芯片；

c) 将传输层安全（TLS）（或数据报TLS）应用于轻量级通信协议，即受约束的应用协议（CoAP）、轻量级机器对机器（LwM2M）协议或消息排队遥测传输（MQTT）。

8.2 加密

– 如果因存储器和存储容量有限而难以使用通用密码算法，则须使用轻量级密码算法。

– 应使用密码算法来防止侧信道攻击。

密钥须在整个生命周期内得到安全管理（CR-1-2）。

– 密钥应以安全的方式生成、更新、分配、使用、存储和销毁。

随机数应在已证明随机性的算法中生成（CR-1-3）。

8.3 数据安全

数据安全维度包括传输数据保护和静态数据保护、信息流控制、安全会话管理和PII保护。

8.3.1 安全传输和存储

传输的数据须加密（DS-1-1）。

– 传输的数据须使用安全密码算法加密（见CR-1-1）。

创建数据或控制信道时应采用安全模式（DS-1-2）。

– 传输数据时，应使用安全协议，确保传输数据的机密性和完整性，并对源方和目的方进行认证。

存储在设备中的数据须加密（DS-1-3）。

– 数据存储设备须使用安全密码算法加密（见CR-1-1）。

已删除的数据不得恢复（DS-1-4）。

– 如果需要废弃、更新或更换设备，须提供删除功能（如出厂初始化），以确保数据无法恢复。

8.3.2 信息流控制

不应允许未经授权的网络流量（DS-2-1）。

8.3.3 安全会话管理

会话应在空闲超时后终止（DS-3-1）。

– 如果在会话终止后再次访问，应重新进行认证。

会话 ID 应为无法预测的数值（DS-3-2）。

– 安全随机数算法应用于会话ID生成。

– 在每个会话认证过程中，会话ID应更改，并且已使用的会话ID应销毁。

8.3.4 PII管理

PII 应在密钥生命周期中得到安全管理（DS-4-1）。

– PII应以安全的方式收集、使用、存储和销毁。

8.4 设备平台安全

在设备平台安全维度，有五项内容：软件安全；安全更新；安全管理；日志记录和时间戳。

8.4.1 软件安全

应采用安全编码（PL-1-1）。

– 软件的设计和运行应考虑安全性。

须检查并消除已知安全漏洞（PL-1-2）。

– 如果软件在开发时使用了含已知安全漏洞的协议、库、应用编程接口（API）、包或开放源，则固件和操作系统中也可能含有这些漏洞。

– 须使用已知安全漏洞的公有领域（如[b-CVE]），检查设备的安全漏洞并予以消除。

应采用代码迷惑（PL-1-3）。

– 这些要求可主要适用于已开发的应用（应用程序），为源代码恢复提供便利。

– 鉴于可以使用开放的反向工程工具提取重要的逻辑或密钥信息，因此需要有适当的保护等级。

应支持配置参数和可执行代码的完整性验证功能（PL-1-4）。

– 为确保IoT设备的有效性，在启动时，应定期以自动模式或手动方式检查配置参数和可执行代码的完整性。

在完整性错误的情况下执行适当响应。

8.4.2 安全更新

更新须由经授权的用户开展（PL-2-1）。

如果更新失败，应支持回滚功能（PL-2-2）。

更新前应检查完整性和认证情况（PL-2-3）。

– 应对执行更新的用户进行认证，对更新服务器地址进行完整性检查，并对更新文件进行上述两种检查。

– 用户的真实性可以通过在更新过程之前立即重新认证用户来确认。

– 授权用户可以通过目视检查来检查更新服务器地址的完整性。

– 通过验证加密数字签名，可以检查更新文件的完整性和真实性。

8.4.3 安全管理

不必要的服务应禁用（PL-3-1）。

– 不必要的服务（Telnet、文件传输协议（FTP）、通用即插即用（UPnP）、简单网络管理协议（SNMP）等）应禁用，设备提供的必要服务应明确。

远程管理应在可靠的环境中进行（PL-3-2）。

应使用安全的第三方库（PL-3-3）。

– 用于开发的第三方库和模块应为最新版本，没有任何已知安全漏洞或缺陷。

应提供自检（PL-3-4）。

– 应提供在IoT设备启动（通电）时或启动后检测主要硬件和软件错误的自检功能。

8.4.4 日志记录

对于安全相关事件应生成日志记录（PL-4-1）。

– 应执行日志记录，并且应有可能检测和跟踪任何异常设备行为。

应提供安全日志记录机制（PL-4-2）。

– 为防止丢失和未经授权更改（包括删除），应有保护日志的机制。

8.4.5 时间戳

应提供可靠的时间戳（PL-5-1）。

8.5 物理安全

物理安全维度涉及保护物理接口和保护IoT设备免受篡改。

8.5.1 安全物理接口

任何不必要的外部接口均应停用（PH-1-1）。

– 所有暴露在外的外部接口（局域网、通用串行总线（USB）、安全数字（SD）卡端口等）的尺寸和功能均应具体说明。

– 如有必要，应控制接入以防止未经授权的接入。

须防止未经授权接入内部接口（PH-1-2）。

– 所有暴露在外的内部接口（联合测试行动小组（JTAG）、串行线调试（SWD）、UART等）的尺寸和功能均应具体说明。

– 如有必要，须实施接入控制以防止未经授权的接入。

8.5.2 防篡改

应支持对未经授权的物理操纵的检测和响应功能（如防篡改密封、锁、篡改响应、归零开关和警报）（PH-2-1）。

附件A

物联网安全要求与安全威胁/漏洞对应清单

（此附件为本建议书不可分割的组成部分。）

安全要求在第 8 节中列出并说明，安全威胁/漏洞在第 7 节中列明。IoT 安全要求与安全威胁/漏洞的对应如表 A.1 所示。

表A.1 – IoT安全要求与安全威胁/漏洞对应清单

要求序号	要求维度	要求说明	安全威胁/漏洞
AU-1-1	认证	出厂默认密码须更改。	ST-D-6
AU-1-2	认证	在访问安全管理或敏感数据时，须首先识别和认证用户。	ST-D-1
AU-1-3	认证	须限制认证尝试的次数。	ST-D-4 ST-D-5
AU-1-4	认证	设备的预置密码应独一无二。	ST-D-1
AU-1-5	认证	应提供一个功能来管理用户帐户和权限的功能。	ST-D-3
AU-1-6	认证	最小权限原则应适用于所有用户账户。	ST-D-3
AU-1-7	认证	应限制对管理员账户的并发访问。	ST-D-1
AU-1-8	认证	应提供就长度、周期和复杂程度而言的安全密码。	ST-D-7
AU-2-1	认证	不应使用硬编码证书。	ST-D-6
AU-2-2	认证	在通过密码进行认证的过程中，应隐藏密码。	ST-D-6
AU-2-3	认证	不应提供对认证失败的具体反馈。	ST-D-6
AU-3-1	认证	每个硬件设备的唯一ID应保留。	ST-D-2
AU-3-2	认证	在传输敏感数据或出于控制目的互连之前，设备应相互认证。	ST-D-2
CR-1-1	加密	在传输或存储数据时须使用安全加密算法。	ST-D-8 ST-D-9

表A.2 – IoT安全要求与安全威胁/漏洞对应清单

要求序号	要求维度	要求说明	安全威胁/漏洞
CR-1-2	加密	密钥须在整个生命周期内得到安全管理。	ST-D-8
CR-1-3	加密	随机数应在已证明随机性的算法中生成。	ST-D-8
DS-1-1	数据安全	传输的数据须加密。	ST-D-11
DS-1-2	数据安全	创建数据或控制信道时应采用安全模式。	ST-D-11
DS-1-3	数据安全	存储在设备中的数据须加密。	ST-D-11
DS-1-4	数据安全	已删除的数据不得恢复。	ST-D-17
DS-2-1	数据安全	不应允许未经授权的网络流量。	ST-G-1
DS-3-1	数据安全	会话应在空闲超时后终止。	ST-D-12
DS-3-2	数据安全	会话ID应为无法预测的数值。	ST-D-12
DS-4-1	数据安全	PII应在密钥生命周期中得到安全管理。	ST-D-11
PL-1-1	设备平台安全	应采用安全编码。	ST-D-10 ST-D-20 ST-D-23 ST-D-24
PL-1-2	设备平台安全	须检查并消除已知安全漏洞。	ST-D-16 ST-D-21
PL-1-3	设备平台安全	应采用代码迷惑。	ST-D-16
PL-1-4	设备平台安全	应支持配置参数和可执行代码的完整性验证功能。	ST-D-15
PL-2-1	设备平台安全	更新须由经授权的用户开展。	ST-D-13
PL-2-2	设备平台安全	如果更新失败，应支持回滚功能。	ST-D-14
PL-2-3	设备平台安全	更新前应检查完整性和认证情况。	ST-D-15
PL-3-1	设备平台安全	不必要的服务应禁用。	ST-D-16
PL-3-2	设备平台安全	远程管理应在可靠的环境中进行。	ST-D-18
PL-3-3	设备平台安全	应使用安全的第三方库。	ST-D-22

表A.2 – IoT安全要求与安全威胁/漏洞对应清单

要求序号	要求维度	要求说明	安全威胁/漏洞
PL-3-4	设备平台安全	应提供自检。	ST-D-19
PL-4-1	设备平台安全	对于安全相关事件应生成日志记录。	ST-D-23
PL-4-2	设备平台安全	应提供安全日志记录机制。	ST-D-23
PL-5-1	设备平台安全	应提供可靠的时间戳。	ST-D-18
PH-1-1	物理安全	任何不必要的外部接口均应停用。	ST-D-24 ST-D-25
PH-1-2	物理安全	须防止未经授权接入内部接口。	ST-D-24 ST-D-25
PH-2-1	物理安全	应支持对未经授权的物理操纵的检测和响应功能（如防篡改密封、锁、篡改响应、归零开关和警报）。	ST-D-24 ST-D-25

附录一

物联网的安全能力

（此附录非本建议书不可分割的组成部分。）

I.1 概述

本建议书仅涉及安全要求，并考虑到服务的可靠性和质量。已对[ITU-T X.1361]中所述的物联网安全能力做了扩充。IoT 架构应包括表 I.1 中所列的一般能力。

表I.1 – 安全要求与安全能力对应表

能力	相关要求
支持安全、可信和保护隐私的通信的安全通信能力	DP-1-1、DS-1-2
支持安全通信的安全密钥管理能力	CR-2-1
提供安全、可信和保护隐私的数据管理的安全数据管理能力	DS-2-1、DS-1-4
认证设备的认证能力	AU-1-1、AU-1-2、AU-1-3、AU-1-4、AU-1-8
授权设备的授权（访问控制）能力	AU-3-1、AU-3-2
基于适当的法律法规，以完全透明、可追溯和可重现的方式，监控数据访问或尝试访问IoT应用的审计能力	PL-4-1、PL-4-2
提供安全、可信和保护隐私的服务的安全服务提供能力	DS-4-1、DS-3-2
整合与各种IoT功能组件相关的不同安全策略和技术的安全整合能力	–
使用公开可用的和标准化的密码算法来执行安全协议的能力	CR-1-1
实施基于轻量级密码算法的安全协议的能力	CR-1-1
更新软件模块或应用的安全、稳健软件更新能力	PL-2-1、PL-2-2、PL-2-3
IoT设备/传感器、网关和平台/服务的身份管理能力	AU-2-1、AU-2-2、AU-2-3、DS-3-2、DS-4-1
漏洞扫描能力	–
以完全透明、可追溯和可重现的方式，监控数据访问或尝试访问IoT应用的能力	PL-4-1、PL-4-2
基于硬件（如可信平台模块）的安全能力，以防止出现因网络和网关虚拟化而带来的物理安全风险	PH-1-1、PH-1-2、PH-2-1
防止选择性转发攻击的多路径路由能力	–
在整个PII生命周期内抵御PII泄漏的PII保护能力	DS-4-1
安全配置能力	–
使用轻量级密码算法的能力	CR-1-1

表I.1 – 安全要求与安全能力对应表

用相关掩模数据加密（EAMD）的简单加密能力[b-ITU-T X.1362]，用于与包括网关在内的其他实体进行通信	–

IoT 架构应包括表 I.2 中所列与密码算法相关的能力。

表I.2 – 针对密码算法的安全要求与安全能力对应表

能力	相关要求
产生用于支持密钥管理的密码质量随机数的能力[b-IETF RFC 4086]	CR-3-1
对广播流所需密钥的定期更新能力	–
使用标准化密码算法的能力	CR-1-1

IoT 架构应包括表 I.3 中所列与情境相关的能力。

表I.3 – 针对情境的安全要求与安全能力对应表

能力	相关要求
抵御旁路攻击的能力	–
支持安全编码实践的能力，在系统和服务、数据库应用和万维网服务中执行严格的数据验证输入	PL-1-1、PL-1-3、PL-1-4
开展有计划的风险评估的能力，以确定工作情境中的风险	PL-1-4

I.2 传感器/设备的安全能力

IoT 传感器/设备应包括表 I.4 中所列的安全能力。

表I.4 – 针对IoT传感器/设备的安全要求与安全能力对应表

能力	相关要求
密钥管理能力	CR-2-1
密码算法协商能力	CR-1-1
数据加密能力，以及在某些情况下指令、控制和管理平面数据，以缓解对通过无线网络传输之数据的机密性的安全顾虑	CR-1-1、DS-1-1、DS-1-2
通过使用适当的完整性保护方案，保证通过无线网络传输之数据的完整性的能力，以确保用户数据或指令、控制或管理数据不被篡改或改变	CR-1-1、DS-1-1、DS-1-2、PL-2-3
数据的来源或IoT传感器/设备的身份以及传感器网络的管理员和维护人员的身份认证能力	AU-1-2、AU-1-6、PL-2-1

表I.4 – 针对IoT传感器/设备的安全要求与安全能力对应表

补丁管理能力，包括更新和升级安全软件模块	PL-2-1、PL-2-2、PL-2-3
执行基于轻量级密码算法的安全协议的能力	CR-1-1
访问控制能力，以确保仅允许经授权的用户或设备可以访问网络元素、存储的信息、信息流、服务和应用	AU-1-2、AU-3-1、AU-3-2
篡改检测或防篡改的能力	PH-2-1
生成密码质量随机数以支持密钥管理的能力	CR-3-1
抵御旁路攻击的能力	–
恶意软件检测和保护能力	–
抵御PII泄漏的PII保护能力	DS-4-1

IoT 设备应包括表 I.5 中所列的安全能力。

表I.5 – 针对IoT设备的安全要求与安全能力对应表

能力	相关要求
使用加密生成的数字签名来验证设备上软件真实性和完整性的能力[b-ISO/IEC 9796-3]	PL-1-4
防火墙、入侵检测、入侵保护或深度数据包检测的能力，以控制将在某个设备上终结的流量	DS-2-1
执行安全配置的能力	PL-1-4

I.3 网关的安全能力

平台/服务应包括表 I.6 中所列的安全能力。

表I.6 – 针对网关的安全要求与安全能力对应表

能力	相关要求
入侵检测系统（IDS）/入侵防御系统（IPS）能力	DS-2-1
密钥管理能力	CR-2-1
执行安全配置的能力	PL-1-4
密码算法协商能力	CR1-1
利用数据中心中IoT设备和组件加密数据以及在某些情况下指令、控制和管理平面数据的能力，以缓解对通过无线网络传输之数据的机密性的安全顾虑	CR-1-1、DS-1-1、DS-1-2
通过使用适当的完整性保护方案，保证通过无线网络传输之数据的完整性的能力，以确保用户数据或指令、控制或管理数据不被篡改或改变	CR-1-1、DS-1-1、DS-1-2、PL-2-3

表I.6 – 针对网关的安全要求与安全能力对应表

从使用安全源代码编码技术、源代码分析测试和漏洞测试，到使用网络或基于主机的IDS/IPS，保证DoS攻击处置技术可用的能力	PL-1-1
认证数据的来源或IoT传感器/设备的身份以及传感器网络管理员和维护人员的身份的能力	AU-1-2、AU-1-6、PL 2-1
访问控制能力，以确保仅允许经授权的个人或设备可以访问网络元素、存储的信息、信息流、服务和应用	AU-1-2、AU-3-1、AU-3-2
IoT设备问责能力，确保任何违反政策的行为将可追溯至特定设备	PL-4-1
更新安全软件模块的能力	PL-2-1、PL-2-2、PL-2-3

I.4 网络安全能力

根据[b-ITU-T X.805]的网络应包括表 I.7 所列的安全能力。

表I.7 – 针对网络的安全要求与安全能力对应表

项目	能力	相关要求
C_NT.1 [b-ITU-T X.805]	通信安全维度确保信息仅在经授权的端点间传送（信息在这些端点之间传送时不会被转移或截获）。	PL-3-1

I.5 平台/服务的安全能力

平台/服务应包括表 I.8 所列的安全能力。

表I.8 – 针对平台/服务的安全要求与安全能力对应表

能力	相关要求
保护用于密码操作的证书的能力，这是一组作为声明身份或权利的证明呈现的数据	DS-2-1
在初始设置期间更改默认用户名和密码的能力	AU-1-1、AU-1-2
执行强密码和细粒度访问控制策略的能力	AU-1-4、AU-1-6
使不必要的端口不可用的能力	PL-3-1、PH-1-1、PH-1-2
支持安全配置的能力，如删除不必要的服务和软件	AU-1-5、PL-3-1
通过使用恶意软件防护软件来防止恶意软件感染的能力	PL-3-4
执行补丁管理策略的能力	PL-2-1、PL-2-2、PL-2-3
漏洞管理能力	PL-1-1、PL-1-2

表I.8 – 针对平台/服务的安全要求与安全能力对应表

更新安全软件模块和应用的能力	PL-2-1、PL-2-3
针对网关与平台/服务之间安全消息传输的密钥管理能力	CR-1-2
在网关与平台/服务之间需要安全消息传输的情况下，在网关与平台/服务之间建立安全隧道的密码算法协商能力；保证DoS攻击处置技术可用的能力	AU-1-5、DS-1-1、DS-1-2
网络监控能力	–
休息时保护PII的能力	DS-4-1
保证应用程序级安全性的能力，以防止[ITU-T X.1361]第8.4节所述的应用程序级威胁和攻击	–
为缓解推理攻击提供支持的能力	–

附录二

对物联网设备和网关适用安全要求的用例

（此附录非本建议书不可分割的组成部分。）

许多 IoT 设备在认证、加密和数据保护方面存在安全漏洞和弱点。此外，其中大多数容易面临物理接口和设备开发平台带来的隐患。本附录介绍了与所建议要求相关的安全开发案例。

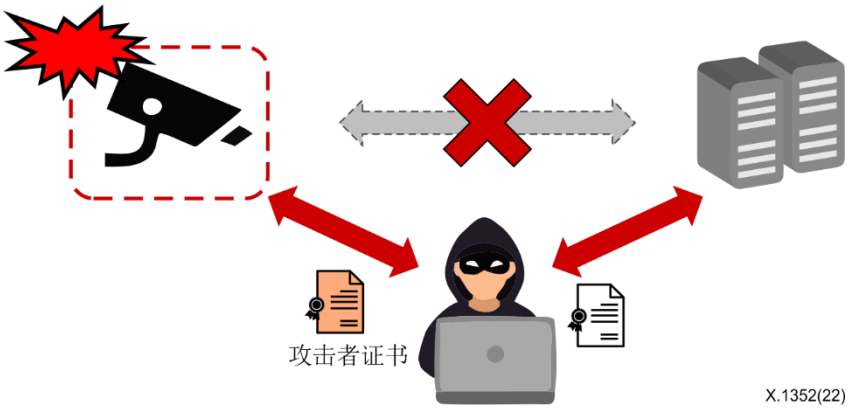
II.1 认证的用例 – 中间人攻击漏洞

服务器和网络摄像机之间的认证程序存在漏洞。网络摄像机在 TLS 握手时不会拒绝无效证书。攻击者窃取重要密钥。见图 II.1。

对抗措施包括：

– 拒绝无效安全套接层证书；

– 使用超文本传输协议公钥锁定。



图II.1 – 认证的用例

II.2 加密领域的用例 – 弱密码算法

见图II.2。

漏洞包括：

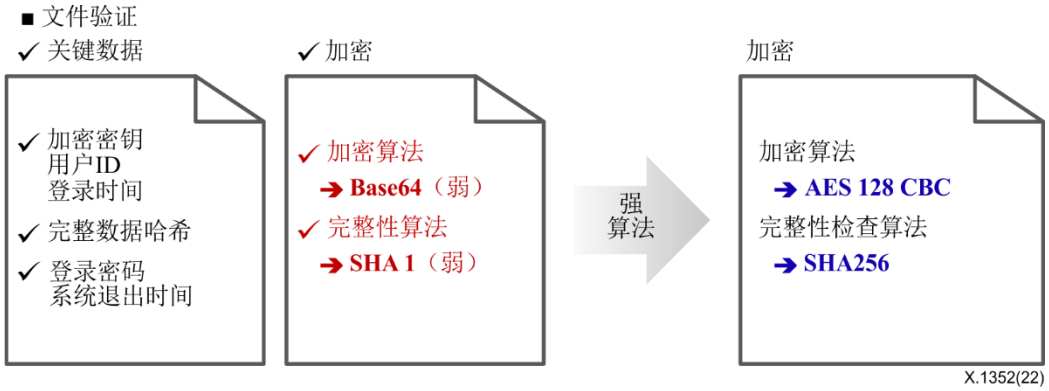
– 弱加密算法：Base64；

– 数据检查方法：安全哈希算法1（SHA1）。

对抗措施包括：

– 高于128位加密算法的安全强度（见[b-ISO/IEC 19790]）；

– 数据检查方法：SHA256 [b-ISO/IEC 10118-3]。



图II.2 – 加密领域的用例

II.3 数据安全和加密领域的用例 – 发送数据的弱完整性检查

见图II.3。

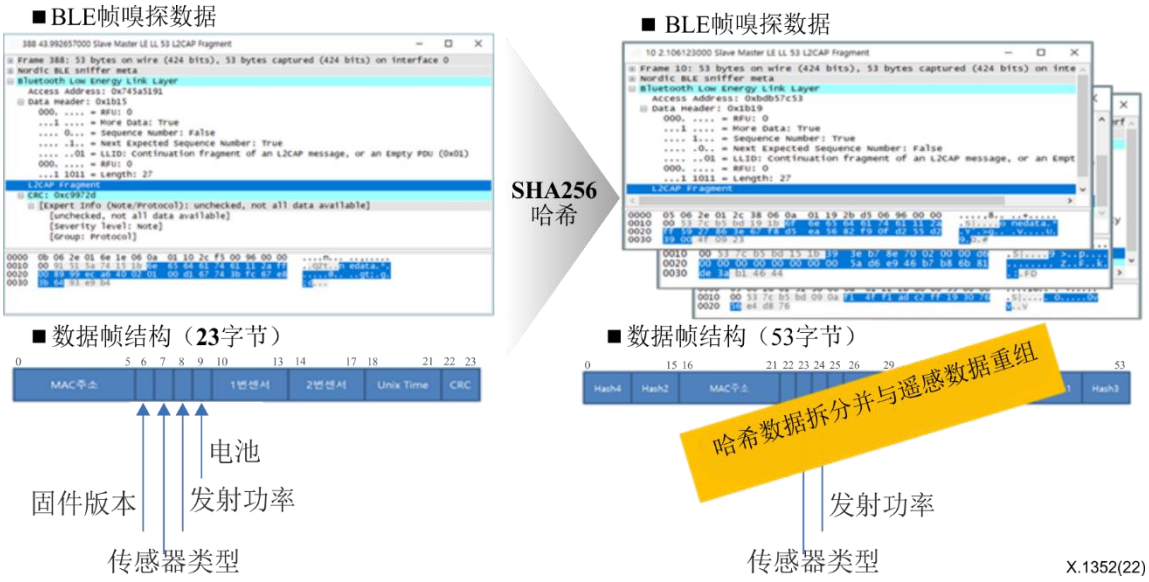
漏洞为：

– 发送数据的弱完整性检查（数据完整性检查方法：循环冗余校验）。

对抗措施包括：

– 数据检查方法：SHA256哈希数据[b-ISO/IEC 10118-3]；

– 总数据拆分和帧重组。



图II.3 – 数据安全和加密领域的用例

II.4 设备平台安全领域的用例 – 对抗利用的弱编码

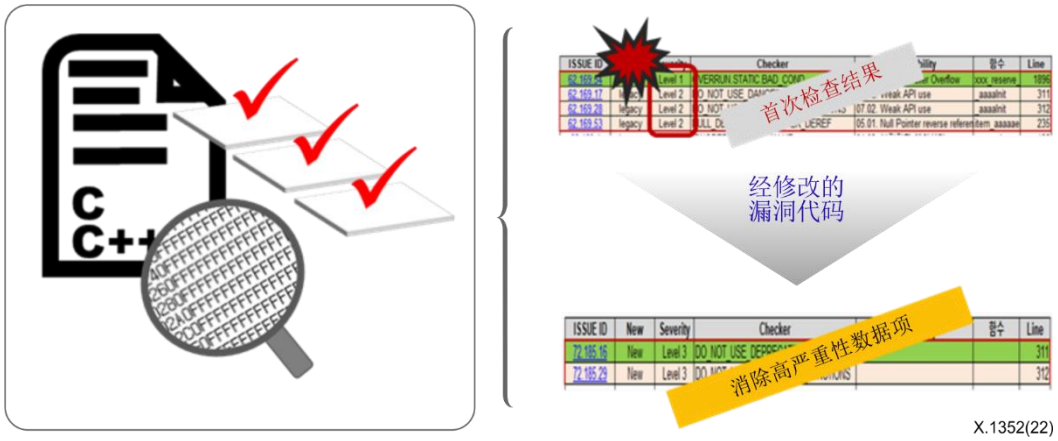
见图II.4。

漏洞为：

– 缓冲区溢出和弱API。

对抗措施为：

– 通过静态分析工具检查安全编码和消除弱代码的建议。



图II.4 – 设备平台安全领域的用例

II.5 物理安全领域的用例 – 印刷电路板的内部接口漏洞

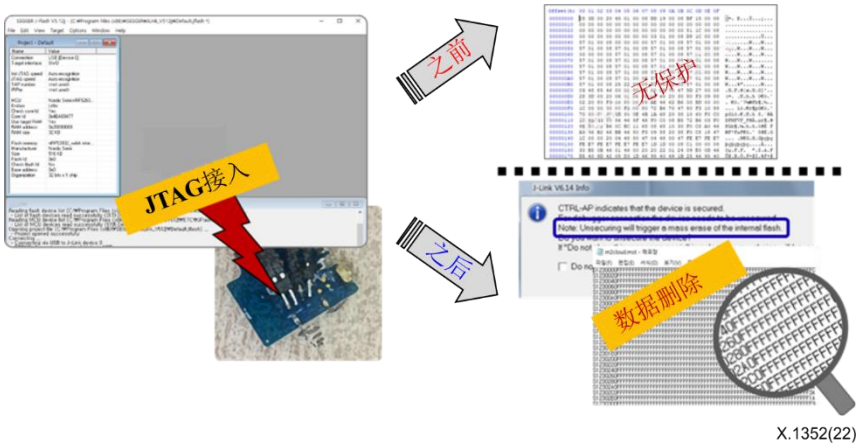
见图II.5。

漏洞为：

– 批量生产的产品提供JTAG端口。

对抗措施为：

– 在MCU中启用存储器存取保护。



图II.5 – 物理安全领域的用例

参考文献

[b-ITU-T X.667] TU-T X.667建议书（2012年），信息技术 – 对象标识符注册机构操作程序：生成通用唯一标识符及其在对象标识符中的使用。

[b-ITU-T X.800] ITU-T X.800建议书（1991年），国际电报电话咨询委员会（CCITT）应用的开放系统互连（OSI）安全架构。

[b-ITU-T X.805] ITU-T X.805建议书（2003年），提供端到端通信的系统安全架构。

[b-ITU-T X.1252] ITU-T X.1252建议书（2021年），基线的身份管理的术语和定义。

[b-ITU-T X.1254] ITU-T X.1254建议书（2020年），实体认证保证框架。

[b-ITU-T X.1362] ITU-T X.1362建议书（2017年），物联网（IoT）环境的简单加密程序。

[b-ITU-T Y.4000] ITU-T Y.4000/Y.2060建议书（2012年），物联网概述。

[b-ISO 16100-1] ISO 16100-1:2009，工业自动化系统和集成 – 针对互操作性的制造软件能力剖析–第1部分：框架。

[b-ISO/IEC 10118-3] ISO/IEC 10118-3 (2018)，IT安全技术 – 哈希函数 – 第3部分：专用哈希函数。

[b-ISO/IEC 19790] ISO/IEC 19790 (2012)，信息技术 – 安全技术 – 加密模块的安全要求。

[b-ISO/IEC 27000] ISO/IEC 27000:2018，信息技术 – 安全技术 – 信息安全管理系统 – 概述和词汇。

[b-ISO/IEC 27033-1 ISO/IEC 27033-1:2015，信息技术 – 安全技术 – 网络安全 – 第1部分：概述和概念。

[b-ISO/IEC 29100] ISO/IEC 29100:2011，信息技术 – 安全技术 – 隐私框架。

[b-ISO/IEC 9796-3] ISO/IEC 9796-3 (2006)，信息技术 – 安全技术 – 具备消息恢复功能的数字签名方案 – 第3部分：基于离散对数的机制。

[b-IETF RFC 4086] IETF RFC 4086（2005年），安全的随机性要求。

[b-CVE] Mitre公司（互联网）。“常见漏洞和暴露”。马萨诸塞州贝德福德：Mitre公司。可参见[2022年10月29日浏览]：https://cve.mitre.org/。

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦