国 际 电 信 联 盟

ITU-T X.1361

(09/2018)

国际电信联盟
电信标准化部门

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

基于网关模型的物联网安全框架

ITU-T X.1361建议书

国际电信联盟

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
网页安全	X.1140–X.1149
安全协议（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.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
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
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

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1361建议书

基于网关模型的物联网安全框架

摘要

ITU-T X.1361建议书描述了使用安全网关的物联网（IoT）的安全框架。物联网是信息社会的一种全球基础设施，基于现有的和正在出现的、可互操作的信息和通信技术，通过（物理和虚拟）之物的相互连接，提供先进的服务。

本建议书分析物联网环境中面临的安全威胁和挑战，并阐明可解决和减缓这些威胁和挑战的能力。本建议书提供的框架方法用于确定在减缓和解决物联网的这些安全威胁和挑战中所需的安全能力。

沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1361	2018-09-07	17	11.1002/1000/13607

关键词

物联网、安全框架、安全需求

* 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识别码，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.1361建议书草案

基于网关模型的物联网安全框架

1 范围

本建议书描述了使用安全网关的物联网（IoT）安全框架。

本建议书分析了物联网环境中面临的安全威胁和挑战，并阐明了可解决和减缓这些威胁和挑战的能力。本建议书提供的框架方法用于确定在减缓和解决物联网面临的这些安全威胁和挑战中所需的安全能力。

本建议书的重点是使用安全网关的物联网安全能力，并考虑[b-ITU-T Y.4401]中描述的参考模型，重点关注的是技术而非管理方面的问题。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITUT-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

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

3 术语和定义

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 **攻击（attack）**[b-ISO13491-1]：对手为获取或修改敏感信息或未被授权获取或修改的服务而对设备发起的进攻尝试。

3.1.2 **认证（authentication）**[b-NIST-SP-800-53]：核实用户、过程或装置的身份，这常常是允许获取信息系统中资源的一个前提条件。

3.1.3 **能力（capability）**[b-ISO 19440]：表示资源（其提供的能力）或企业活动（其需要的能力）之能力特征集合（表示为能力属性）的概念。

注 – 能力可以聚合。

3.1.4 **情境（context）**[b-ITU-T X.1252]：具有实体存在和相互作用的明确边界条件的一个环境。

3.1.5 **加密算法（cryptographic algorithm）**[b-ISO/IEC 19790]：接受变量输入（可包括加密密钥）并生成一个输出的明确定义的计算程序。

3.1.6 **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）。

3.1.7 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。

注 – 密码学确定用于加密和解密的方法。对加密原理、手段或方法的攻击称为密码分析。

3.1.8 密码系统（cryptosystem）[b-ISO 11568-1]：用于提供信息安全服务的密码原语集。

3.1.9 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设备。

3.1.10 身份管理（identity management）[b-ITU-T X.1250]：用于以下目的的一组功能和能力（如行政管理、管理和维护、发现、通信交流、关联和绑定、策略执行、认证和声明）：

– 保证身份信息（如标识符、证书、属性）；

– 保证实体（如用户/订户、组、用户设备、组织机构、网络和服务提供商、网络元素和对象、虚拟对象）身份；以及

– 支持业务和安全应用。

3.1.11 物联网（Internet of Things）（IoT）[b-ITU-T Y.4000]：信息社会的一种全球基础设施，基于现有的和正在出现的、可互操作的信息和通信技术，实现（物理和虚拟）之物的相互连接，以提供先进的服务。

注1 – 通过使用标识、数据捕获、处理和通信能力，物联网充分利用物体向各种各样的应用提供服务，同时确保满足安全和隐私要求。

注2 – 从广义而言，物联网可被视为技术和社会影响方面的一个愿景。

3.1.12 入侵检测（intrusion detection）[b-ISO / IEC 27039]：检测入侵的正式过程，通常包括收集关于异常使用样式的知识，以及哪些漏洞被利用了、它们是如何被利用的、什么时间被利用的等。

3.1.13 入侵检测系统（intrusion detection system）[b-ISO / IEC 27039]：用于识别入侵是否已在尝试、正在发生或已经发生的信息系统。

3.1.14 入侵防御（intrusion prevention）[b-ISO / IEC 27033-1]：积极响应以防止入侵的正式过程。

3.1.15 入侵防御系统（intrusion prevention system）[b-ISO / IEC 27039]：专门设计用于提供主动响应能力的入侵检测系统的变体。

3.1.16 密钥管理（key management）[b-ITU-T X.800]：根据安全策略，生成、存储、分发、删除、归档和应用密钥。

3.1.17 轻量密码算法（lightweight cryptography）[b-ISO/IEC 29192-1]：专门设计用于在受限环境中实施方案的密码算法。

3.1.18 恶意软件（malware）[b-ISO/IEC 27033-1]：旨在专门破坏或干扰系统，攻击其保密性、完整性与/或可用性的怀有恶意的软件。

注 – 病毒和木马是恶意软件的例子。

3.1.19 网络监控（network monitoring）[b-ISO / IEC 27033-1]：持续观察和审查记录网络活动和操作的数据，包括审计日志和告警以及相关的分析。

3.1.20 个人身份识别信息（personally identifiable information）（PII）[b-ISO/IEC 29100]：a) 可用于识别相关信息与之关联的PII（个人可识别信息）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。

注 – 为确定PII主体是否可识别，应考虑持有该数据的隐私利益攸关方或任何其它方可合理使用的所有手段，以识别该自然人。

3.1.21 与掩模相关的安全（security association with mask）（SAM）[b-ITU-T X.1362]：这是一组特定于安全协议的参数。SAM通过采用带有相关掩模数据的加密术（EAMD），来确定保护通信所需的服务和机制。SAM由其相关协议参引，取决于诸如传输层或网际协议（IP）层的不同协议层。在这些参数中，可包括算法标识符、模式以及利用EAMD的层标识符和加密密钥。

3.1.22 传感器（sensor）[ITU-T Y.4105]：传感物理条件或化合物并传递与所观测到的特性相关的电子信号的电子设备。

3.1.23 物（thing）[b-ITU-T Y.4000]：在物联网中，“物”指物理世界（物理事物）或信息世界（虚拟事物）中的一个对象，它可被标识并整合进通信网络中。

3.1.24 威胁（threat）[b-ISO/IEC 27000]：可能对系统或组织机构造成伤害的有害事件的潜在起因。

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

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 加密算法协商（cryptographic algorithm negotiation）：用于确定加密算法类型和加密密钥长度的机制，以便用在加密的和集成的通信会话中，并确定双方都可用的、最适合的加密算法。

注 – 这一定义改编自[b-ISO / IEC 27033-1]，在本建议书中称为“网关”。

3.2.2 补丁管理（patch management）：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。

3.2.3 PII违规（PII breach）：违反一项或多项PII保护相关要求而处理个人身份信息的情况。

3.2.4 隐私偏好模型（privacy preference model）：允许网站声明其对收集之个人数据预期用途的模型，以更好地控制其个人信息。

3.2.5 安全配置（secure configuration）：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服务。

注 – 它包括删除或禁用不必要的用户帐户和不必要的软件，将任何默认密码更改为备用密码、强密码，启用防火墙和配置以默认禁用（阻止）未经批准的连接，以及禁用自动运行功能。

3.2.6 安全网关（security gateway）：网络之间或网络内子组之间的连接点，或者不同安全域内的软件应用之间的连接点，旨在根据物联网环境中给定的安全策略来保护网络。

3.2.7 旁路攻击（side-channel attack）：利用从密码系统的物理实施方案中获得的信息进行的攻击。

注 – 关于计算时序、功耗和电磁泄漏的信息，可被用来破坏密码系统。

3.2.8 漏洞管理（vulnerability management）： 由识别、分类、修补和缓解漏洞等组成的过程。

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：

DoS 拒绝服务

EAMD 用相关掩模数据加密

IDS 入侵检测系统

IoT 物联网

IP 网际协议

IPS 入侵防御系统

PII 个人身份识别信息

5 惯例

无。

6 概述

物联网（IoT）是信息社会的一种全球基础设施，基于现有的和正在出现的、可互操作的信息和通信技术，实现（物理和虚拟）之物的相互连接，以提供先进的服务。

一个典型的物联网部署方案将包括有线或无线网络上配备传感器的边缘设备，通过一个网关将数据发送到一个公共云或私有云。从应用到应用，拓扑结构的各方面都将会有很大差异；例如，在某些情况下，网关可能在设备上。基于这种拓扑结构的设备可以从头开始构建，以充分发挥物联网的作用，或者可以是将在部署后添加物联网功能的传统设备。

7 功能体系结构和框架

本建议书基于图1所示的物联网功能体系结构。

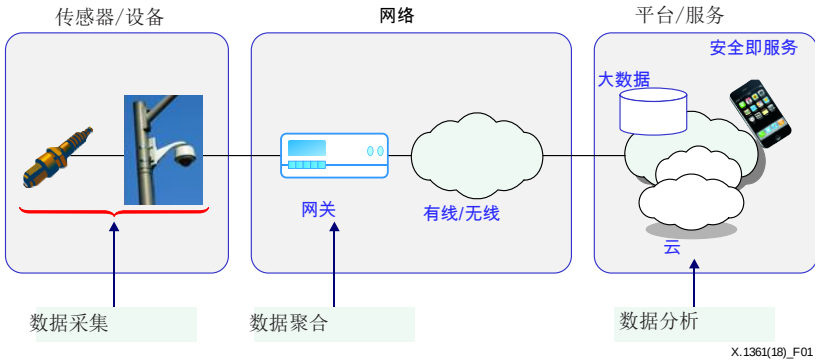


图1 – 物联网功能体系结构（简化）

物联网端点（传感器或设备）与网关之间的数据可通过两种类型的通信网络来通信：基于网际协议（IP）的网络或非基于IP的网络。假设在部署于数据中心的物联网平台中的网关与物联网组件之间的通信应使用基于IP的协议来完成。因此，在非IP网络的情况下，应终止通过非IP网络的通信连接，并通过网关上的IP网络来重新建立通信连接。

功能体系结构可以详述如图2所示。

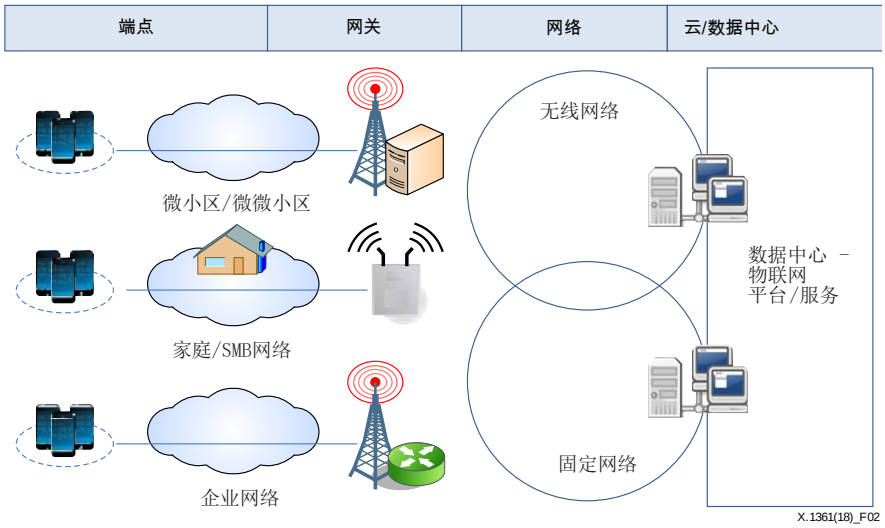


图2 – 实用的功能体系结构

例如，在智能交通系统中，图2所示的网关可以作为车辆移动网关来连接内部的（汽车）区域网络和外部的开放网络。

网关应具备防火墙能力，以控制将要在设备上终结的流量。一些物联网设备具有独特的传输协议，不同于传输控制协议（TCP）/IP协议。专有协议可用于管理物联网设备如何相互通信。因此，应采用行业特定的协议过滤能力来识别可能隐藏在非IP协议中的恶意负载。

网关应执行一种功能，用于过滤将在该设备上终结的特定数据，以最佳使用有限的可用计算资源。

网关作为一个独特的元素参与功能体系结构。网关通常是物联网系统中可靠安全性的第一点，因为端点最容易受到物理篡改。除了网络，网关在物联网中起着重要作用，保证其作为特定安全资产的独特作用。网关应考虑到传感器节点的约束条件。网关通常可以代表受限端点执行某些安全功能，例如：密钥管理、密码协商、入侵防御。

根据以下因素，网关将具有广泛不同的安全能力：端点的功能和能力、服务设计、网络设计、物理位置和使用情境。

8 物联网面临的安全威胁

8.1 物联网传感器/设备面临的安全威胁

特定于传感器/设备的威胁：

– 设备捕获：指设备被物理地破坏或丢失其密钥。

– 天坑（Sinkhole）攻击：指受攻击的设备吸引通信流量形成黑洞或引入选择性转发的攻击。在天坑攻击中，入侵者会损害设备或在网络内部引入伪造设备，并使用该设备发起天坑攻击。被攻击的设备会尝试根据路由协议中使用的路由度量标准，自相邻节点吸引所有数据流量。达到此目的时，被攻击的设备将发起攻击。天坑攻击是一种网络层攻击，当中，受攻击的设备向其邻居发送虚假路由信息，以吸引网络流量至其自身。由于特别（ad hoc）网络和无线网络的多对一通信样式（当中许多节点向单个基站发送数据），因此无线网络特别容易受到天坑攻击。基于无线网络中的通信流量，天坑不需要针对网络中的所有节点，而只需针对基站附近的那些节点。

– 女巫（Sybil）攻击：指恶意设备非法拥有多个身份的攻击。恶意设备的额外身份被称为女巫节点。这种攻击与其它攻击一起发起，以降低容错机制（如分布式存储、多路径路由和拓扑维护）的有效性。

– 泛洪（Flooding）攻击：泛洪攻击是拒绝服务（DoS）攻击的一种形式，当中攻击者通过向目标设备发送一连串的“问候”数据包，试图消耗掉足够多的设备资源，使设备对合法流量无法做出响应。

– 选择性转发攻击：在这种攻击中，被攻击的节点过滤随机接收到的数据包，并将其中的一部分转发到下一个节点。如果节点过滤掉（丢弃）所有接收到的数据包，则称其为“黑洞”攻击。

– 虫洞攻击：当两个恶意/被攻击的节点通告它们之间有一条非常短的路径时，蠕虫攻击就会发生。一条隧道指的是在两个联网设备之间的一条数据路径，它在现有网络基础设施上建立。将数据隧道给另一个网络的网络，从一个网络中获取数据，并通过隧道将数据复制到另一个网络上，由于此操作，该特定网络可能因此而变得混乱。这时黑客可容易地进入和滥用网络。与天坑攻击和女巫攻击结合使用时，它可导致选择性转发或创建一个天坑。

– 传感器/设备假冒：当攻击者成功伪装成某个合法传感器/设备的身份时，会发生这种攻击。

8.2 物联网网关面临的安全威胁

特定于网关的威胁：

– 未经授权的访问：未经授权访问网关会导致泄露敏感信息、数据修改、拒绝服务（DoS）和非法使用资源。例如，一旦攻击者访问了一个网关，对现有未加密数据的监控可导致用户名、密码和安全配置数据受到威胁。

– 流氓网关：即使所有无线网关都是安全的，攻击者也很容易部署一个其自身的流氓网关。例如，一个过度热心的员工可能会在其办公室安装一个无线接入点，而不考虑安全性。这将有效规避许多在用安全措施，甚至可能造成对官方组织与/或企业设施的无线电干扰。一个流氓无线接入点也可能被刻意地、隐蔽地安装，以便在本地或从远程方便地访问网络上的某个作恶者。作恶者（被称为“邪恶双胞胎”）可用一个他们具有完全配置和监控权限的无线接入点来取代现有的无线接入点，甚至可用类似的设置来配置一个流氓无线接入点，但需要更高的功率比，以覆盖合法无线

接入点的信号。一旦一个合法设备被欺骗连接到一个流氓网关，则可以收集机密的连接信息了。

– 拒绝服务攻击：拒绝服务攻击会导致目标性能显著下降，或者在理想情况下，通过耗尽目标的内存与/或计算能力而停止其提供的服务。目标忙于应对攻击者发送的非法流量。无线传感器网络因其开放媒质的特性、动态变化的拓扑结构以及缺乏明确的防线，而特别容易受到拒绝服务攻击。拒绝服务攻击目前在网络中是一个日益严重的问题。许多为固定有线网络开发的防御技术不适用于移动网络环境。

8.3 网络面临的安全威胁

特定于网络的威胁：

– 未经授权的访问：未经授权访问无线传感器网络会导致泄露敏感信息、数据修改、拒绝服务攻击和非法使用资源。例如，一旦攻击者访问了传感器网络，对现在未加密数据的监控可导致用户名和密码被泄露。

– 数据包嗅探：对于没有加密能力的无线传感器网络，攻击者通常很容易对网络通信进行窃听。为了窃听这样的无线传感器网络，需要一副天线以及普通的无线网络工具和网络数据包嗅探器。网络数据包嗅探器是一种工具，它将网卡设置为“混杂模式”。这意味着接口将接收和处理所有流量，而不仅仅接收和处理针对它的流量。网络嗅探器将向其用户显示所有网络数据包，并对其进行解码以便于阅读。所有明文流量都易于理解，可以定义过滤器来查找特定的关键词或值。

– 蓝牙劫持：这是对蓝牙移动设备（如手机）进行的一种攻击。攻击者通过向蓝牙设备的用户发送未经请求的消息来发起蓝牙劫持。发送的实际消息不会对目标设备造成伤害，但可能会诱使用户以某种方式作出响应，或者将新联系人添加到设备的地址簿中。

– 蓝牙窃取：该攻击导致通过蓝牙连接（通常在电话、台式机、笔记本电脑和个人数字助理（PDA）之间）自目标无线设备未经授权地访问信息。一次成功的攻击可导致未经授权地访问这些设备上的私有和机密信息。

8.4 平台/服务面临的安全威胁

在互联网中，应用层的主要任务是收集和处理大量的用户数据，包括用户的个人信息或各种各样交易的机密信息。数据是攻击者的主要目标，企图窃取、篡改或破坏之。有必要使用隐私保护机制来保护数据。应用层威胁包括：大量数据处理、失控智能设备、未经授权的人为干预以及无法从灾难中恢复的失控设备。

特定于平台/服务的威胁：

– 试探：收集平台/服务信息的探索性过程。

– 拒绝服务：平台/服务被大量服务请求淹没的一种攻击，平台/服务因此变得太忙而无法响应合法的客户端请求。

– 任意代码执行：试图在平台/服务上运行恶意代码的一种攻击，以破坏其资源并发起额外的攻击。

– 恶意代码执行：软件系统或脚本的任何部分，旨在导致不良后果、安全性或个人身份信息（PII）遭到破坏或者系统遭到损坏。典型的例子包括病毒、蠕虫和特洛伊木马。
– 特权升级：使用特权进程帐户执行代码的一种攻击，以提升攻击者的特权。
– 结构化查询语言（SQL）注入：利用应用程序输入验证和数据访问代码中的漏洞运行任意命令的一种攻击，它注入或提取信息。
– 网络窃听：从网络捕获传输的数据包并读取数据内容以搜索敏感信息的一种攻击，如密码、会话令牌或任何类型的机密信息。
– 未经授权的访问：使用他人帐户或另一种访问方法访问平台/服务的一种攻击。例如，如果有人一直在猜测某个非其所有的账号的密码或用户名，直至获得访问权限；这被视为未经授权的访问。
– 暴力破解：系统性地检查所有可能的密钥直至找到某个正确密钥的一种攻击。
– 用户名/密码的字典攻击：通过反复尝试密码，使用字典中的单词来系统性地破坏密码或认证机制的一种攻击。
– 使用默认用户名和密码/使用弱密码：使用默认用户名和密码/弱密码来获取平台/服务的一种攻击。
– 推理攻击：当用户能够从合理访问的低分类信息块中推断出受保护的信息时，将发生这种攻击。
– PII泄漏：有意或无意地将PII发布到某个不受信任的环境中。

9 物联网的要求

本建议书基于附件A中讨论的、[ITU-T Y.4100]中描述的高级别要求。

10 物联网的安全能力

10.1 概述

本建议书只涉及安全要求，并考虑到服务的可靠性和质量。已对[b-ITU-T Y.4401]中所述的那些物联网安全能力做了扩充。

一般能力

物联网体系结构应包括：

– 支持安全、可信和隐私保护的通信的安全通信能力；
– 支持安全通信的安全密钥管理能力；
– 提供安全、可信和隐私保护的数据管理的安全数据管理能力；
– 认证设备的认证能力；
– 授权设备的授权（访问控制）能力；

– 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物联网应用程序的审计能力；
– 提供安全、可信和隐私保护的服务的安全服务提供能力；
– 整合与各种物联网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；
– 实施基于轻量密码算法的安全协议的能力；
– 更新软件模块或应用程序的安全且健壮的软件更新能力；
– 物联网设备/传感器、网关和平台/服务的身份管理能力；
– 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物联网应用程序的能力；
– 基于硬件（如可信的平台模块）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；
– 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攻击的PII保护能力；
– 安全配置能力；
– 使用轻量密码算法的能力；以及
– 用相关掩模数据加密（EAMD）的简单加密能力[bITUT X.1362]，用于与包括网关在内的其他实体进行通信。

密码算法相关的能力

物联网体系结构应包括：

– 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]；
– 对广播流所需密钥的定期更新的能力；以及
– 使用标准化的密码算法的能力。

情境相关的能力

物联网体系结构应包括：

– 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；以及
– 开展有计划的风险评估的能力，以确定工作情境中的风险。

10.2 传感器/设备的安全能力

物联网传感器/设备应包括：

– 密钥管理能力；
– 密码算法协商能力；
– 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进行传输之数据的机密性的安全顾虑；

– 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，以保证用户数据的完整性，或者指令、控制或管理数据不被篡改或改变；
– 数据的来源或物联网传感器/设备的身份以及传感器网络的管理员和维护人员的身份的认证能力；
– 补丁管理能力，包括更新和升级安全软件模块；
– 执行基于轻量密码算法的安全协议的能力；
– 访问控制能力，以确保只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；
– 篡改检测与/或防篡改的能力；
– 生成密码质量随机数以支持密钥管理的能力；
– 抵御旁路攻击的能力；
– 恶意软件检测和保护能力；以及
– 抵御PII泄漏的PII保护能力。

物联网设备应包括：

– 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]；
– 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；以及
– 执行安全配置的能力。

10.3 网关的安全能力

网关应包括：

– 入侵检测系统（IDS）/入侵防御系统（IPS）能力；
– 密钥管理能力；
– 执行安全配置的能力；
– 密码算法协商能力；
– 利用数据中心中物联网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进行传输之数据的机密性的安全顾虑；
– 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，以保证用户数据的完整性，或者指令、控制或管理数据不被篡改或改变；
– 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，保证拒绝服务攻击处置技术可用的能力；
– 认证数据的来源或物联网传感器/设备的身份以及传感器网络的管理员和维护人员的身份的能力；
– 访问控制能力，以确保只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；以及
– 问责物联网设备的能力，确保任何违反政策的行为都可追溯到某个特定设备。

网关需要支持更新安全软件模块的能力。

10.4 网络的安全能力

网络的安全能力超出了本建议书的讨论范围。

注 – 可以使用满足[b-ITU-T X.805]中所述安全维度要求的安全能力。

10.5 平台/服务的安全能力

平台/服务应包括：

– 保护用于密码操作的证书的能力，这是一组数据，作为声明之身份与/或权利的证据呈现；
– 在初始设置期间更改默认用户名和密码的能力；
– 执行强密码和细粒度访问控制策略的能力；
– 使不必要的端口不可用的能力；
– 支持安全配置的能力，例如，删除不必要的服务和软件；
– 通过使用恶意软件防护软件来防止恶意软件感染的能力；
– 执行补丁管理策略的能力；
– 漏洞管理能力；
– 更新安全软件模块和应用程序的能力；
– 管理网关与平台/服务之间安全消息传输的密钥的能力；
– 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；
– 保证拒绝服务攻击处置技术可用的能力；
– 网络监控能力；
– 休息时保护PII的能力；
– 保证应用程序级别安全性的能力，以防止第8.4节所述的应用程序级别的威胁和攻击；以及
– 为缓解推理攻击提供支持的能力。

附件A

ITU-T Y.4100/Y.2066中描述的安全和隐私要求

（此附件为本建议书不可分割的组成部分。）

安全和隐私保护要求是指在捕获、存储、传输、聚合和处理物的数据以及提供涉及物的服务期间的功能要求。这些要求与物联网的所有参与者有关。

本附件提供了[ITU-T Y.4100]附件A中所述的高级别安全和隐私保护要求，下面各条款中括号内的术语是指[ITU-T Y.4100]附件A的特定元素。

A.1 通信安全

需要安全、可信和隐私保护的通信能力，以便禁止对数据内容进行未经授权的访问，保证数据的完整性，并在物联网中传输或传送数据期间可以保护与隐私相关的数据内容[SP1]。

A.2 数据管理安全

需要安全、可信和隐私保护的数据管理能力，以便禁止对数据内容进行未经授权的访问，保证数据的完整性，并在物联网中存储或处理数据时可以保护与隐私相关的数据内容[SP2]。

A.3 服务提供安全

需要安全、可信和保护隐私的服务提供能力，以便禁止未经授权的访问服务和欺诈性的服务提供，并可以保护与物联网用户相关的隐私信息[SP3]。

A.4 安全政策和技术的整合

需要整合不同安全策略和技术的能力，以确保对物联网中各种设备和用户网络执行一致的安全控制[SP4]。

A.5 相互认证和授权

在设备（或物联网用户）可以访问物联网之前，需要根据预定义的安全策略执行设备（或物联网用户）与物联网之间的相互认证和授权[SP5]。

A.6 安全审计

物联网需要支持安全审计。任何数据访问或企图访问物联网应用都需要根据适当的法律法规使之完全透明、可追溯和可重现。特别地，物联网需要支持有关数据传输、存储、处理和应用访问的安全审计[SP6]。

附录I

ITU-T Y.4401/Y.2068中描述的安全和隐私功能

（此附录非本建议书不可分割的组成部分。）

本附录提供了[b-ITU-T Y.4401]中所述的高级别安全和隐私保护能力，下面各条款中括号内给出的术语是指[b-ITU-T Y.4401]中的特定元素。

I.1 通信安全能力

通信安全能力涉及支持安全、可信和隐私保护之通信的能力[C-7-1]。

I.2 数据管理安全能力

数据管理安全能力涉及提供安全、可信和隐私保护之数据管理的能力[C-7-2]。

I.3 服务提供安全能力

服务提供安全能力涉及提供安全、可信和隐私保护之服务提供的能力[C-7-3]。

I.4 安全整合能力

安全整合能力涉及整合与各种物联网功能组件相关的不同安全策略和技术的能力[C-7-4]。

I.5 相互认证和授权能力

相互认证和授权能力涉及在设备访问基于预定义安全策略的物联网之前认证和授权每个设备的能力[C-7-5]。

I.6 安全审计能力

安全审计能力涉及依据适当的法律法规监控数据访问的能力，或者尝试以完全透明、可追溯和可重现的方式访问物联网应用的能力[C-7-6]。

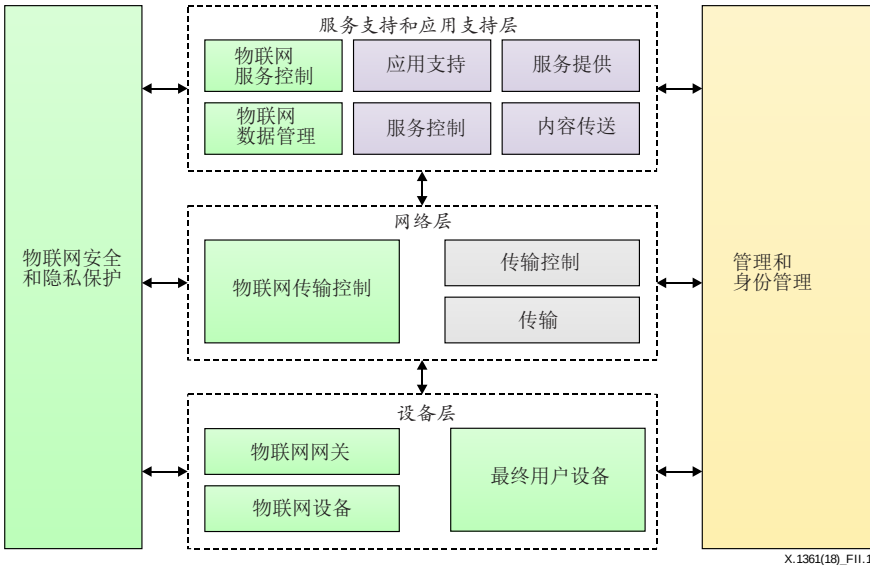
注 – 这些安全和隐私保护能力还包括应对跨不同域工作的安全和隐私保护问题的能力。

附录II

ITU-T Y.4401/Y.2068中建立在下一代
网络功能体系结构上的物联网功能框架的实施方案视图

（此附录非本建议书不可分割的组成部分。）

图II.1说明了物联网功能框架的实施方案视图，它建立于[b-ITUT Y.4401]中下一代网络（NGN）功能体系结构中所述的功能实体上，与本建议书中的安全功能框架相关。本建议书为[b-ITU-T Y.4401]图7-2中所述的服务支持层和设备层提供了能力。



**图II.1 – 在NGN功能体系结构上
建立物联网功能框架的实施方案视图**

参考书目

[b-ITU-T X.667] ITU-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），CCITT应用的开放系统互连的安全体系结构。

[b-ITU-T X.805] ITU-T X.805建议书（2003年），提供端到端通信的系统的安全体系结构。

[b-IUT-T X.1250] ITU-T X.1250建议书（2009年），增强全球身份管理和互操作性的基准能力。

[b-ITU-T X.1252] ITU-T X.1252建议书（2010年），基线身份管理术语和定义。

[b-ITU-T X.1311] ITU-T X.1311建议书（2011年）| ISO/IEC 29180:2012，信息技术 – 泛在传感器网络的安全框架。

[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-ITU-T Y.4050] ITU-T Y.4050/Y.2069建议书（2012年），物联网术语和定义。

[b-ITU-T Y.4105] ITU-T Y.4105/Y.2221建议书（2010年），在下一代网络（NGN）环境中支持泛在传感器网络（USN）应用和服务的要求。

[b-ITU-T Y.4113] ITU-T Y.4113建议书（2016年），物联网的网络要求。

[b-ITU-T Y.4400] ITU-T Y.4400/Y.2063建议书（2012年），物联网框架。

[b-ITU-T Y.4401] ITU-T Y.4401/Y.2068建议书（2015年），物联网的功能框架和能力。

[b-IETF RFC 4086] IETF RFC 4086 (2005), *Randomness Requirements for Security*.

[b-ISO 11568-1] ISO 11568-1:2005,*Banking – Key management (retail) – Part 1: Principles*.

[b-ISO 13491-1] ISO 13491-1:2016,*Financial services – Secure cryptographic devices (retail) – Part 1: Concepts, requirements and evaluation methods*.

[b-ISO 19440] ISO 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.

[b-ISO/IEC 9796-3] ISO/IEC 9796-3:2006,*Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.

[b-ISO/IEC 19790] ISO/IEC 19790:2012,*Information technology – Security techniques – Security requirements for cryptographic modules*.

[b-ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts*.

[b-ISO/IEC 27033-6] ISO/IEC 27033-6:2016, *Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access*.

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework.*

[b-ISO/IEC 29192-1] ISO/IEC 29192-1:2012, *Information technology – Security techniques – Lightweight cryptography – Part 1: General*.

[b-NIST SP 800-53] NIST Special Publication 800-53 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations*.

[b-ZT] Zhang Li, Tong Xin (2013), *Threat Modeling and Countermeasures Study for the Internet of Things,* Journal of Convergence Information Technology (JCIT), *Vol. 8, No. 5, March.*

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
2019年，日内瓦