International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1361

(09/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Internet of things (IoT) security

Security framework for the Internet of things based on the gateway model

Recommendation ITU-T X.1361

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	**X.1360–X.1369**
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1361

Security framework for the Internet of things based on the gateway model

Summary

Recommendation ITU-T X.1361 describes a security framework for the Internet of things (IoT) using security gateways. The IoT is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

This Recommendation analyses security threats and challenges in an IoT environment, and describes capabilities that could address and mitigate these threats and challenges. A framework methodology is provided for determining which security capabilities are required for mitigating and addressing these threats and challenges for the IoT.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1361	2018-09-07	17	11.1002/1000/13607

Keywords

Internet of things, security framework, security requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1361

Security framework for the Internet of things based on the gateway model

1 Scope

This Recommendation describes a security framework for the Internet of Things (IoT) using security gateways.

This Recommendation analyses security threats and challenges in the IoT environment and describes capabilities that address and mitigate these security threats and challenges. A framework methodology is provided for determining which security capabilities are required for mitigating and addressing security threats and challenges for the IoT.

The focus of this Recommendation is on IoT security capabilities using security gateways and considers the reference model described in [b-ITU-T Y.4401] with a focus on technical, not management aspects.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.4100] Recommendation ITU-T Y.4100/Y.2066 (2014), *Common requirements of the Internet of things*.

3 Terms and Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 attack [b-ISO13491-1]: Attempt by an adversary on the device to obtain or modify sensitive information or a service they are not authorized to obtain or modify.

3.1.2 authentication [b-NIST SP 800-53]: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

3.1.3 capability [b-ISO 19440]: Construct that represents the collection of capability characteristics (expressed as capability attributes) of either a Resource (its provided Capability) or an Enterprise Activity (its required Capability).

NOTE – Capabilities can be aggregated.

3.1.4 context [b-ITU-T X.1252]: An environment with defined boundary conditions in which entities exist and interact.

3.1.5 cryptographic algorithm [b-ISO/IEC 19790]: Well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output.

3.1.6 cryptographic-quality random-number [b-ITU-T X.667]: A random number or pseudo-random number generated by a mechanism, which ensures sufficient spread of repeatedly-generated values to be acceptable for use in cryptographic work (and is used in such work).

3.1.7 cryptography [b-ITU-T X.800]: The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

NOTE – Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.1.8 cryptosystem [b-ISO 11568-1]: Set of cryptographic primitives used to provide information security services.

3.1.9 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.10 identity management [b-ITU-T X.1250]: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

– assurance of identity information (e.g., identifiers, credentials, attributes);

– assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and

– supporting business and security applications.

3.1.11 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.12 intrusion detection [b-ISO/IEC 27039]: Formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns, as well as what, how, and which vulnerability has been exploited to include how and when it occurred.

3.1.13 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.14 intrusion prevention [b-ISO/IEC 27033-1]: Formal process of actively responding to prevent intrusions.

3.1.15 intrusion prevention system [b-ISO/IEC 27039]: Variant on intrusion detection systems that are specifically designed to provide an active response capability.

3.1.16 key management [b-ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.17 lightweight cryptography [b-ISO/IEC 29192-1]: cryptography tailored for implementation in constrained environments.

3.1.18 malware [b-ISO/IEC 27033-1]: Malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability.

NOTE – Viruses and Trojan horses are examples of malware.

3.1.19 network monitoring [b-ISO/IEC 27033-1]: Process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis.

3.1.20 personally identifiable information (PII) [b-ISO/IEC 29100]: Any information that a) can be used to identify the PII principal to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal.

NOTE – To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

3.1.21 security association with mask (SAM) [b-ITU-T X.1362]: This is a security-protocol-specific set of parameters. SAM defines the services and mechanisms necessary to protect traffic by applying encryption with associated mask data (EAMD). SAM is referred to by its associated protocol, depending on the protocol layers such as transport layer or Internet protocol (IP) layer. Algorithm identifiers, modes, layer identifier at which EAMD is applied and cryptographic keys can be included in these parameters.

3.1.22 sensor [b-ITU-T Y.4105]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.23 thing [b-ITU-T Y.4000]: With regard to the Internet of things, this is an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks.

3.1.24 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.1.25 vulnerability [b-ISO/IEC 27000]: Weakness of an asset or control that can be exploited by one or more threats.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 cryptographic algorithm negotiation: Mechanism to determine the type of cryptographic algorithm and length of cryptographic keys to use in an encrypted and integrated communications session and to ascertain the most suitable cryptographic algorithm available at both sides.

NOTE – This definition is adapted from [b-ISO/IEC 27033-1] and referred to as 'gateway' in this Recommendation.

3.2.2 patch management: Process which encompasses acquiring, testing, and installing multiple patches to information systems.

NOTE – Vulnerability management capability could be considered.

3.2.3 PII breach: Situation where personally identifiable information is processed in violation of one or more relevant PII protection requirements.

3.2.4 privacy preference model: Model that allows websites to declare their intended use of data they collect about individuals, to give more control of their personal information.

3.2.5 secure configuration: Process by which network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

NOTE – It includes removal or disabling of unnecessary user accounts and unnecessary software, changing any default password to an alternative, strong password, enabling firewall and configuring to disable (block) unapproved connections by default, and disabling of auto-run feature.

3.2.6 security gateway: Point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy in the IoT environment.

3.2.7 side-channel attack: Attack utilizing information obtained from the physical implementation of a cryptosystem.

NOTE – Information about computational timing, power consumption, and electromagnetic leaks can be exploited to break the cryptosystem.

3.2.8 vulnerability management: Process that consists of identifying, classifying, remediating, and mitigating vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DoS Denial of Service

EAMD Encryption with Associated Mask Data

IDS Intrusion Detection System

IoT Internet of things

IP Internet Protocol

IPS Intrusion Prevention System

PII Personally Identifiable Information

5 Conventions

None.

6 Overview

The Internet of things (IoT) is defined as a global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies.

A typical IoT deployment will consist of sensor-equipped edge devices on a wired or wireless network, sending data via a gateway to a public or private cloud. Aspects of the topology will vary broadly from application to application; for example, in some cases the gateway may be on the device. Devices based on such topologies may be built from the ground up to leverage IoT or may be legacy devices that will have IoT capabilities added post-deployment.

7 Functional architecture and framework

This Recommendation is based on the functional architecture of IoT shown in Figure 1.

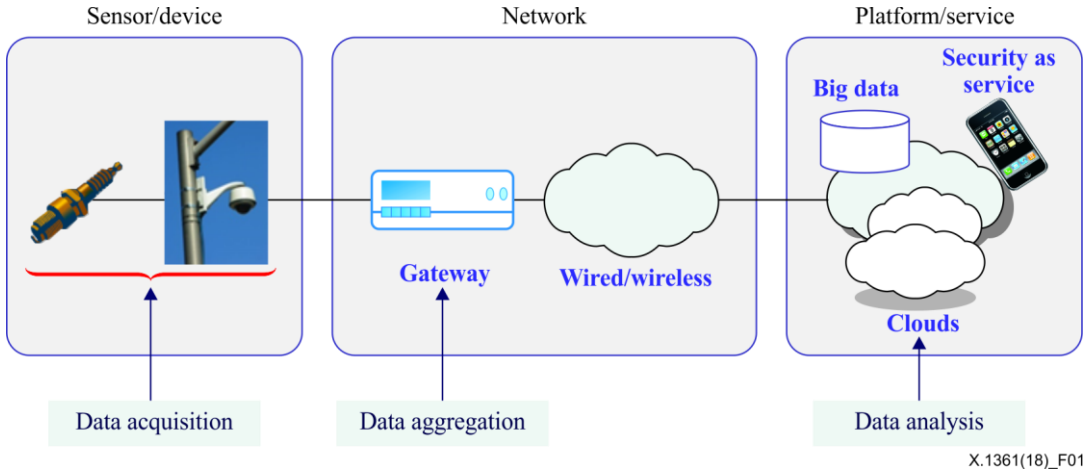

Figure 1 – IoT functional architecture (simplified)

The data between an IoT end-point (sensor or device) and gateway can be communicated over two types of communication networks: Internet protocol (IP)-based network or a non-IP-based network. It is assumed that the communication between the gateway and the IoT component in the IoT platform, deployed in a data center, should be carried out using an IP-based protocol. Therefore, in case of a non-IP network, the communication connection over the non-IP network should be terminated and re-established over an IP network at the gateway.

The functional architecture can be elaborated as shown in Figure 2.

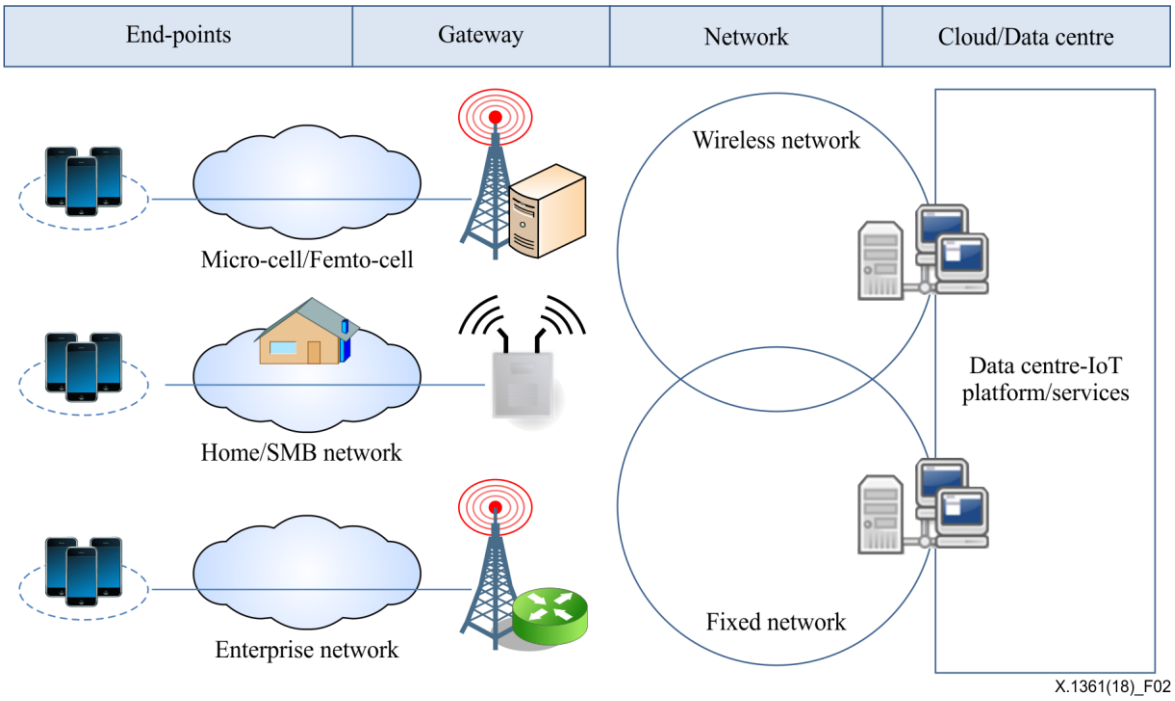

Figure 2 – Practical functional architecture

For example, in an intelligent transport system, the gateway, shown in Figure 2, could act as a vehicle mobile gateway to connect an internal (car) area network and an external open network.

A firewall capability should be in place in the gateway to control traffic that is destined to terminate at the device. Some IoT devices have unique transport protocols, distinct from transmission control protocol (TCP)/IP protocols. Proprietary protocols can be used to govern how IoT devices communicate with one another. Thus, industry-specific protocol filtering capabilities should be in place to identify malicious payloads that could potentially hide in non-IP protocols.

The gateway should implement a function for filtering specific data destined to terminate on that device in a way that makes optimal use of the limited computational resources available.

The gateway participates as a unique element in the functional architecture. The gateway is often the first point of reliable security in an IoT system, because end-points are most vulnerable to physical tampering. The gateway plays a role in IoT that warrants its distinction as a specific security asset, apart from the network. The gateway should consider the constraints of sensor nodes. The gateway can often perform some security functions on behalf of constrained end-points such as: key management, cryptographic negotiation, intrusion prevention.

The gateway will have widely varying security capabilities depending on factors such as: the power and capabilities of the end-points, service design, network design, physical locations and usage context.

8 Security threats to the Internet of things

8.1 Security threats to IoT sensors/devices

Sensor/device-specific threats:

– Device capture: Refers to a device being physically compromised or having its keys lost.

– Sinkhole attack: Refers to an attack in which a compromised device attracts communication traffic to form a black hole or introduce selective forwarding. In a sinkhole attack, an intruder compromises a device or introduces a counterfeit device inside the network and uses it to launch a sinkhole attack. The compromised device tries to attract all data traffic from neighbouring nodes based on the routing metric used in the routing protocol. When this is achieved, the compromised device will launch an attack. Sinkhole attacks are a type of network-layer attack where a compromised device sends fake routing information to its neighbours to attract network traffic to itself. Due to ad hoc networks and the many-to-one communication patterns of wireless networks where many nodes send data to a single base station, wireless networks are particularly vulnerable to sinkhole attacks. Based on communication flows in a wireless network, a sinkhole does not need to target all nodes in the network, but only those close to the base station.

– Sybil attack: Refers to an attack in which a malicious device illegitimately takes on multiple identities. A malicious device's additional identity is referred to as a Sybil node. This attack is launched in conjunction with other attacks, to reduce the effectiveness of fault-tolerant mechanisms, such as distributed storage, multi-path routing and topology maintenance.

– Flooding attack: A flooding attack is a form of a denial of service (DoS) attack in which an attacker sends a succession of 'hello' packets to a targeted device in an attempt to consume enough of the device's resources to make the device unresponsive to legitimate traffic.

– Selective forwarding attacks: In this attack, a compromised node filters randomly received packets and forwards some of them to the next node. If the node filters out (drops) all the packets it receives, it is called a 'blackhole' attack.

– Wormhole attack: Wormhole attacks occur when two malicious/compromised nodes advertise having a very short path between them. A tunnel is a data path between two networked devices which is established across an existing network infrastructure. A network that tunnels data to another network gets the data from one network and replicates it onto another network through the tunnel and that particular network may be confused due to this action. At this time a hacker may easily enter and misuse the network. Used in conjunction with a sinkhole and Sybil attack, can result in selective forwarding or creation of a sinkhole.

– Impersonation of sensor/device. This attack happens when an attacker successfully masquerades as the identity of a legitimate sensor/device.

8.2 Security threats to IoT gateways

Gateway-specific threats:

– Unauthorized access: Unauthorized access to a gateway can cause the disclosure of sensitive information, data modification, DoS and illicit use of resources. For example, once an attacker has accessed a gateway, monitoring of the now unencrypted data can result in user names, passwords and secure configuration data being compromised.

– Rogue gateway: Even if all wireless gateways are secure, it is easy for attackers to deploy a rogue gateway of their own. For example, an overly eager employee might install a wireless access point in their office with no regard for security. This will effectively circumvent many of the security measures in place and perhaps even cause radio interference with the official organization and/or enterprise installation. A rogue, wireless access point may also be deliberately and covertly installed in order to grant easy access to a perpetrator on the network

either locally or remotely. A perpetrator (known as an 'evil twin') could replace an existing wireless access point with one on which they have full configuration and monitoring access or even configure a rogue wireless access point, with similar settings, but with a higher power ratio necessary to overcome the legitimate wireless access point's signal. Once a legitimate device is deceived into connecting to a rogue gateway, confidential connection information can be gathered.

– Denial of service attack: The DoS attack causes a target to significantly slow down or, ideally, stop the services it provides by exhausting the target's memory and/or computing capacity. Targets are kept busy responding to the illegitimate traffic that attackers are sending. The wireless sensor network is particularly vulnerable to DoS attacks due to its features of an open medium, dynamic changing topology, and the lack of a clear line of defence. DoS attacks are a growing problem in networks today. Many of the defence techniques developed for fixed wired network are not applicable to mobile network environments.

8.3 Security threats to the network

Network specific threats:

– Unauthorized access: Unauthorized access to a wireless sensor network can cause disclosure of sensitive information, data modification, DoS and illicit use of resources. For example, once an attacker has accessed a sensor network, monitoring of the now unencrypted data can result in user names and passwords being compromised.

– Packet sniffing: For wireless sensor networks that do not have encryption capabilities it is generally easy for attackers to eavesdrop on network communications. To eavesdrop on such a wireless sensor network, an antenna, along with normal wireless networking tools and a network packet sniffer are required. A network packet sniffer is a tool that sets the network card to "promiscuous mode". This means that the interface will receive and process all traffic rather than only traffic meant for it. A network sniffer will show its user all network packets and decode them for easy reading. All plaintext traffic is easily understood and filters can be defined to look for certain keywords or values.

– Bluejacking: This as an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to users of Bluetooth-enabled devices. The actual messages sent do not cause harm to the targeted device, but may induce the user to respond in some fashion or to add the new contact to the device's address book.

– Bluesnarfing: This attack results in the unauthorized access of information from a targeted wireless device through a Bluetooth connection, often between phones, desktops, laptops, and personal digital assistants (PDAs). A successful attack may result in unauthorized access to private and confidential information on these devices.

8.4 Security threats to platform/services

In the Internet, the main task of the application layer is to collect and process a large number of user data, including users' personal information or confidential information of various transactions. The data are an attacker's main target, stolen, tampered or damaged. It is necessary to protect data using privacy protection mechanisms. Application layer threats include: mass data processing, out-of-control smart devices, unauthorized human intervention, and out-of-control devices unable to recover from disaster.

Platform/services specific threats:

– Profiling: Exploratory process used to gather information on the platform/services.

– Denial of service: An attack in which the platform/service is overwhelmed by massive service requests and becomes too busy to respond to legitimate client requests.

– Arbitrary code execution: An attack that tries to run malicious code on a platform/service to compromise its resources and to then launch additional attacks.
– Malicious code execution: Any part of a software system or script, which is intended to cause undesired effects, security or personally identifiable information (PII) breaches, or damage to a system. Typical example includes viruses, worms, and Trojan horses.
– Elevation of privileges: An attack in which code is executed, using a privileged process account, to elevate the attacker's privileges.
– Structured query language (SQL) injection: An attack that exploits vulnerabilities in an application's input validation and data access code to run arbitrary commands that inject or extract information.
– Network eavesdropping: An attack that captures packets transmitted from the network and reads the data content in search of sensitive information such as passwords, session tokens, or any kind of confidential information.
– Unauthorized access: An attack that gains access to a platform/service using someone else's account or another method of access. For example, if someone keeps guessing a password or username for an account that was not their own until access has been gained; this is considered unauthorized access.
– Brute force: An attack that systematically checks all possible keys until a correct one is found.
– Dictionary attack of usernames/passwords: An attack that systematically defeats cipher or authentication mechanisms by repeatedly trying passwords, using words in a dictionary.
– Use of default usernames and passwords/use of weak passwords: An attack where default usernames and passwords/weak passwords are exploited to gain access to platform/services.
– Inference attack: This attack occurs when a user is able to infer protected information from rightfully accessible chunks of information with lower classification.
– PII leakage: Intentional or unintentional release of PII to an untrusted environment.

9 Requirements for Internet of things

This Recommendation is based on the high-level requirements described in [ITU-T Y.4100], as discussed in Annex A.

10 Security capabilities for the Internet of things

10.1 Overview

This Recommendation only addresses security requirements and takes into account reliability and quality of services. The security capabilities for the IoT are expanded from those described in [b-ITU-T Y.4401].

General capabilities

The IoT architecture should include:

– a secure communication capability for supporting secure, trusted and privacy protected communication;
– a secure key management capability for supporting secure communications;
– a secure data management capability for providing secure, trusted and privacy protected data management;
– an authentication capability for authenticating devices;
– an authorization (access control) capability for authorizing devices;

– an audit capability for monitoring data access or attempts to access IoT applications in a fully transparent, traceable and reproducible manner, based on appropriate regulations and laws;
– a secure service provision capability for providing secure, trusted and privacy protected service provision;
– a secure integration capability for integrating different security policies and techniques related to the variety of IoT functional components;
– a capability to implement secure protocols using publicly available and standardized cryptographic algorithms;
– a capability to implement secure protocols based on lightweight cryptography;
– a secure and robust software update capability for updating software modules or applications;
– an identity management capability for IoT devices/sensors, gateways and platforms/services;
– a vulnerability scanning capability;
– a capability for monitoring data access or attempts to access IoT applications in a fully transparent, traceable and reproducible way;
– a hardware-based (e.g., trusted platform module) security capability to prevent occurrences of physical security risks that come with network and gateway virtualization.
– a multi-path routing capability for preventing selective forwarding attacks;
– a PII protection capability against PII breaches throughout the entire PII lifecycle;
– a secure configuration capability;
– a capability using lightweight cryptography; and
– a simple encryption capability with encryption with associated mask data (EAMD) [b-ITU-T X.1362] for communicating with other entities including the gateway.

Cryptographic algorithm related capabilities

The IoT architecture should include:

– a capability of producing a cryptographic-quality random-number for supporting key management [b-IETF RFC 4086];
– a periodic update capability of necessary cryptographic keys for broadcast streams; and
– a capability using standardized cryptographic algorithms.

Context related capabilities

The IoT architecture should include:

– a capability to resist side-channel attacks;
– a capability to support secure coding practices that enforce rigorous data validation input in systems and services, database applications, and web services; and
– a capability to conduct a planned risk assessment to determine risks across operational contexts.

10.2 Security capabilities for sensors/devices

The IoT sensors/devices should include:

– a key management capability;
– a cryptographic algorithm negotiation capability;
– a data encryption capability and in some cases signalling, control and management plane data to mitigate the security concerns to confidentiality of data transmitted through wireless networks;

– a data integrity capability for data transmitted through wireless networks by using appropriate integrity protection schemes which provide assurances that user data or signalling, control or management data has not been tampered with or altered;
– an authentication capability of the origin of the data or of identities of the IoT sensors/devices and of administrators and maintenance personnel of the sensor networks;
– a capability for patch management, including updating and upgrading secure software modules;
– a capability to implement secure protocols based on lightweight cryptography;
– an access control capability to ensure that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications;
– a tamper detection and/or tamper prevention capability;
– a capability to produce cryptographic-quality random numbers to support key management;
– a capability to resist against side-channel attacks;
– a malware detection and protection capability; and
– a PII protection capability against PII leakage.

The IoT devices should include:

– a capability to verify the authenticity and integrity of software on a device using cryptographically generated digital signatures [b-ISO/IEC 9796-3];
– a firewall, intrusion detection, intrusion protection, or deep packet inspection capability to control traffic that is destined to terminate at a device; and
– a capability for performing secure configurations.

10.3 Security capabilities for gateways

The gateway should include:

– an intrusion detection system (IDS)/intrusion prevention system (IPS) capability;
– a key management capability;
– a capability for performing secure configuration;
– a cryptographic algorithm negotiation capability;
– a capability to encrypt data and in some cases signalling, control and management plane data with IoT devices and components in the data center to mitigate the security concerns to confidentiality of data transmitted through wireless networks;
– an integrity capability of data transmitted through wireless networks by using appropriate integrity protection schemes to provide assurances that user data or signalling, control or management data has not been tampered with or altered;
– an availability capability to handle DoS attacks ranging from using secure source coding techniques, source code analysis testing and vulnerability testing, to using a network or host-based IDS/IPS;
– an authentication capability of the origin of the data or of identities of the IoT sensors/devices and of administrators and maintenance personnel of the sensor networks;
– an access control capability to ensure that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications; and
– an IoT device accountability capability to ensure that any violation of policy will be traceable to a specific device.

The gateway is required to support a capability for updating secure software modules.

10.4 Security capabilities for the network

Security capabilities for the network are out of scope of this Recommendation.

NOTE – Security capabilities to meet security dimensions described in [b-ITU-T X.805] could be used.

10.5 Security capabilities for platforms/services

The platform/service should include:

- a capability to protect a credential for cryptographic operations, which is a set of data presented as evidence of a claimed identity and/or entitlements;
- a capability to change default usernames and passwords during initial setup;
- a capability to implement strong passwords and a granular access control policy;
- a capability to make unnecessary ports unavailable;
- a capability to support secure configuration, for example, to remove unnecessary services and software;
- a capability to protect against malware infection through the use of malware protection software;
- a capability to implement patch management policies;
- a capability for vulnerability management;
- a capability for updating secure software modules and applications;
- a key management capability for secure message transfer between a gateway and a platform/service;
- a capability for cryptographic algorithm negotiations for establishing secure tunnelling between the gateway and the platform/service, in case there is a need for secure message transfer between the gateway and the platform/service;
- an availability capability to handle DoS attacks;
- a capability for network monitoring;
- a capability for PII protection at rest;
- a capability for application level security to prevent application level threats and attacks described in clause 8.4; and
- a capability to provide support for mitigating inference attacks.

Annex A

Security and privacy requirements described in ITU-T Y.4100/Y.2066

(This annex forms an integral part of this Recommendation.)

Security and privacy protection requirements refer to the functional requirements during capturing, storing, transferring, aggregating and processing the data of things, as well as provisioning services which involve things. These requirements are related to all IoT actors.

This annex provides high-level security and privacy requirements described in Annex A of [ITU-T Y.4100] and the bracketed terms given in each clause below refer to the particular element of Annex A of [ITU-T Y.4100].

A.1 Communication security

Secure, trusted and privacy protected communication capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected during data transmission or transfer in IoT [SP1].

A.2 Data management security

Secure, trusted and privacy protected data management capability is required, so that unauthorized access to the content of data can be prohibited, integrity of data can be guaranteed and privacy-related content of data can be protected when storing or processing data in IoT [SP2].

A.3 Service provision security

Secure, trusted and privacy protected service provision capability is required, so that unauthorized access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected [SP3].

A.4 Integration of security policies and techniques

The ability to integrate different security policies and techniques is required, to ensure consistent security control over the variety of devices and user networks in IoT [SP4].

A.5 Mutual authentication and authorization

Before a device (or an IoT user) can access the IoT, mutual authentication and authorization between the device (or the IoT user) and IoT is required to be performed according to predefined security policies [SP5].

A.6 Security audit

Security audit is required to be supported in IoT. Any data access or attempt to access IoT applications are required to be fully transparent, traceable and reproducible according to appropriate regulation and laws. In particular, IoT is required to support security audit for data transmission, storage, processing and application access [SP6].

Appendix I

Security and privacy capabilities described in ITU-T Y.4401/Y.2068

(This appendix does not form an integral part of this Recommendation.)

This appendix provides high-level security and privacy capabilities described in [b-ITU-T Y.4401] and the bracketed terms given in each clause below refer to the particular element of [b-ITU-T Y.4401].

I.1 Communication security capability

Communication security capability involves the abilities of supporting secure, trusted and privacy protected communication [C-7-1].

I.2 Data management security capability

Data management security capability involves the abilities of providing secure, trusted and privacy protected data management [C-7-2].

I.3 Service provision security capability

Service provision security capability involves the abilities of providing secure, trusted and privacy protected service provision [C-7-3].

I.4 Security integration capability

Security integration capability involves the abilities of integrating different security policies and techniques related to the variety of IoT functional components [C-7-4].

I.5 Mutual authentication and authorization capability

Mutual authentication and authorization capability involves the abilities of authenticating and authorizing each device before the device accesses the IoT based on predefined security policies [C-7-5].

I.6 Security audit capability

Security audit capability involves the abilities of monitoring data access or attempts to access IoT applications in a fully transparent, traceable and reproducible way based on appropriate regulations and laws [C-7-6].

NOTE – These security and privacy protection capabilities also include the ability of coping with the security and privacy protection issues for operations across different domains.

Appendix II

Implementation view of the IoT functional framework building over the next generation network functional architecture in ITU-T Y.4401/Y.2068

(This appendix does not form an integral part of this Recommendation.)

Figure II.1 illustrates an implementation view of the IoT functional framework, building over the functional entities described in the next generation network (NGN) functional architecture in [b-ITU-T Y.4401] which is related to the security functional framework in this Recommendation. This Recommendation provides capabilities for the service support layer and device layer described in Figure 7-2 of [b-ITU-T Y.4401].

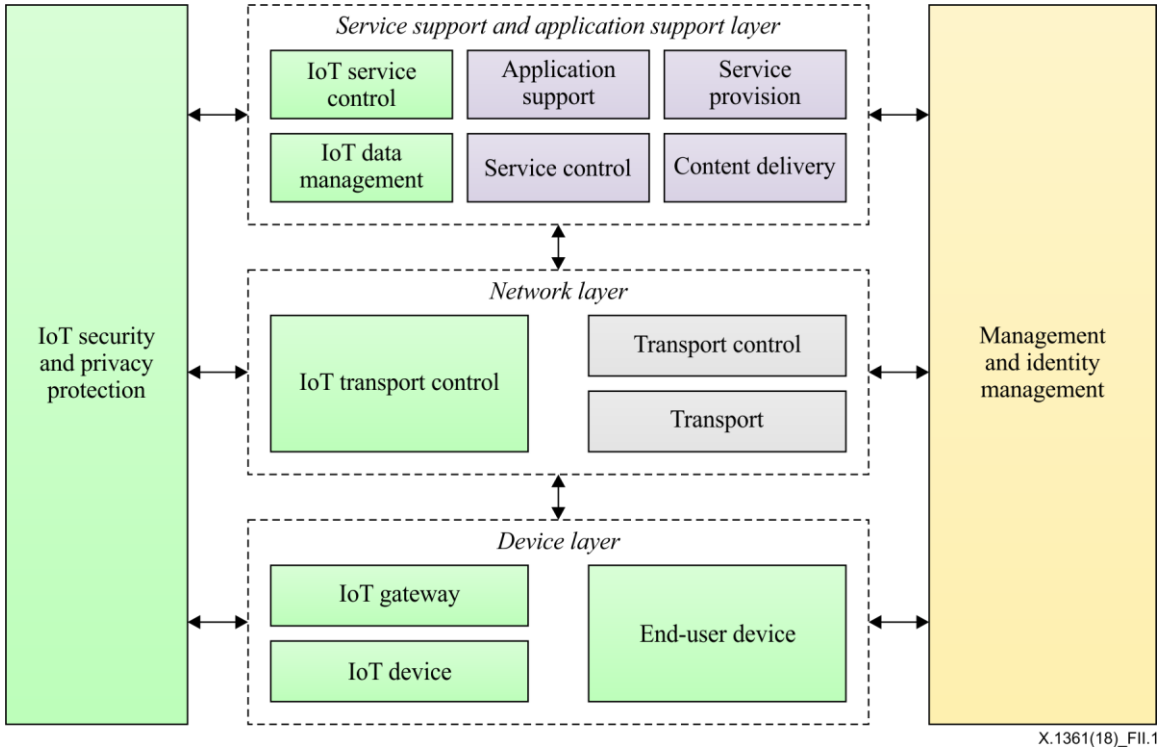

Figure II.1 – Implementation view of the IoT functional framework building over the NGN functional architecture

Bibliography

[b-ITU-T X.667] Recommendation ITU-T X.667 (2012), *Information technology – Procedures for the operation of object identifier registration authorities: Generation of universally unique identifiers and their use in object identifiers*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-IUT-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ITU-T X.1311] Recommendation ITU-T X.1311 (2011) | ISO/IEC 29180:2012, *Information technology – Security framework for ubiquitous sensor networks*.

[b-ITU-T X.1362] Recommendation ITU-T X.1362 (2017), *Simple encryption procedure for Internet of things (IoT) environments*.

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.

[b-ITU-T Y.4050] Recommendation ITU-T Y.4050/Y.2069 (2012), *Terms and definitions for the Internet of things*.

[b-ITU-T Y.4105] Recommendation ITU-T Y.4105/Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

[b-ITU-T Y.4113] Recommendation ITU-T Y.4113 (2016), *Requirements of the network for the Internet of things*.

[b-ITU-T Y.4400] Recommendation ITU-T Y.4400/Y.2063 (2012), *Framework of the web of things*.

[b-ITU-T Y.4401] Recommendation ITU-T Y.4401/Y.2068 (2015), *Functional framework and capabilities of the Internet of things*.

[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.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019