THE (ISC)² IoT

# LEXICON

An introduction to basic terminology and concepts related to the Internet of Things

# INTRODUCTION

(ISC)² – the world's largest nonprofit membership association of certified cybersecurity professionals – is pleased to provide you with the (ISC)² Internet of Things (IoT) Lexicon. Developed with the (ISC)² Advisory Board of North America and with industry leaders & technology experts, this follow up to the (ISC)² Cybersecurity Lexicon is an easy reference guide that can quickly introduce non-technical personnel to key IoT cybersecurity concepts.

The IoT Lexicon provides non-technical professionals, journalists, boards of directors and others with a quick reference guide of common IoT terms. Our goal is to encourage the creation of more effective legislation, standards and policies by encouraging broader understanding of how the accurate use of these terms ensures more effective cybersecurity programs.

We welcome your comments and experiences on using the Lexicon.

For more information, please visit:
www.isc2.org/cybersecurity-advocates.

# A

## Actuator
is a machine or part of a machine which moves or controls another part in response to an input.

## Advanced Encryption Standard (AES)
is a specification for the encryption of electronic data established by the National Institute of Standards and Technology (NIST).

## Agent
is a software component installed on a device (or field gateway) that performs actions on behalf of another program or managing component. In the IoT space, agents are typically controlled and act for components running on the cloud back-end.

## Analytics
is the discovery, interpretation and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming and operations research to quantify performance.

## Antivirus
is software designed to detect and prevent computer viruses and other malware from entering and harming a system.

## Application
is a software program that runs on a computer or device.

## Application Agent
is an embedded program that runs on or near an IoT device and may report the status of the asset or environment. The agent typically reads status from the sensors and applies logic rules.

## Application Firewall
controls input, output, and/or access from, to or by an application or service. It operates by monitoring and potentially blocking the input, output or system service calls that do not meet the configured policy of the firewall.

## Application Security
is the use of software, hardware and procedural methods to protect applications from external and internal threats.

## Architecture
the design artifacts that describe how security controls are positioned in relation to the balance of of the systems. It maintains the system's attributes such as confidentiality, integrity and availability.

Architecture for IoT can include, but is not limited to:

- Applications
- Analytics
- Big Data
- Data Storage
- Networks
- Edge/Fog
- Device Management
- Cloud to Device Management
- Physical Devices

### Artificial Intelligence
is the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making and translation between languages.

### Asset
is any item perceived as having value; includes both tangible items such as information systems and physical property, as well as intangibles such as intellectual property and data.

### Attack Surface
is the sum of the security risk exposure; it is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make your organization less

exploitable, reducing risk. A typical attack surface has complex interrelationships among three main areas of exposure: software attack surface, network attack surface and, the often-overlooked, human attack surface.

### Authenticate
is the process of verifying the identity of an IT system's user.

### Authorize
is the process of defining the specific resources a user needs and determining the type of access to those resources the user may have.

### Autonomous Vehicles
are vehicles capable of sensing the environment and navigating without human input. An example is self-driving cars.

## B

### Big Data
extremely large data sets that may be analyzed computationally to reveal patterns, trends and associations, especially relating to human behavior and interactions.

### Big Data in IoT
refers to the use of predictive analytics, user behavior analytics, or certain other advanced data analytics methods that extract value from data, and seldom to a particular size of data set.

### Blockchain
is a public register in which transactions between two users belonging to the same network are stored in a secure, verifiable and permanent way.

### Bluetooth Low Energy (BLE)
is a wireless technology designed and marketed for applications in healthcare, fitness and home entertainment.

### Business Impact Assessment (BIA)
is a systematic process used to determine and evaluate the potential effects of an interruption to critical business operations as a result of exploitation, disaster, accident or emergency.

## C

### Chirp
is a signal in which the frequency either increases or decreases with time. It works by encoding the data using a series of pitches and tones on the sending device, and then decoded on the receiving device.

## CIA Triad:

**Confidentiality** – The attribute of data that ensures information is only being exposed to appropriately authorized parties and other systems.

**Integrity** – The attribute of data that ensures the information accurately reflects reality. Data and systems/processes cannot be modified without authorization.

**Availability** – The attribute of data that ensures it is always available to appropriate parties when required for use.

## Cloud Computing

is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

## Cloud Gateway

is a system that enables remote communication to and from devices or field gateways, potentially residing at several different sites, connecting across public network space.

## Cloud to Device Management

provides the ability to easily inventory, manage and secure the mobile devices on your network.

### Cold Storage Database
holds data not needed as quickly and/or frequently as warm storage, but still may be necessary to access in the future for reporting, analysis and machine learning use.

### Competing Consumers
denotes a messaging pattern in which more consumers get messages from a common source (i.e. queue), but each message is delivered to only one consumer.

### Connected Devices
are the things (components) that make up the Internet of Things. Many have built-in sensors and/or actuators and collect data to help users or other devices make informed decisions and monitor or affect outside events.

### Connectivity Protection
is a part of the Edge Layer which helps ensure that connectivity does not fail when there is an unreliable connection.

## D

### Data Filtration
reduces the amount of transmitted information while retaining the meaning of the data, typically, at the Edge Layer.

### Data Storage
IoT data storage differs slightly from regular storage as data is stored on back-end devices but also needs to be stored on the device itself. See also Time Series Data.

### Data Visualization
is a technique used to represent data or information using graphs.

### Device
is an object that can connect to the internet. For example, wearable technology that monitors an individual's health.

### Device Management (IoT)
is the process of authenticating, provisioning, configuring, monitoring and maintaining the device firmware and software that provides its functional capabilities.

### Direct Messaging
allows a sender and receiver to be directly connected and allows for the exchange of messages.

### Domains
are the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators and connectivity which enables these things to connect and exchange data.

# E

**Edge Gateway**
is the connecting factor between device analytics, cloud processing and analytics.

**Edge/Fog Computing**
facilitates the operation of computers, storage, and networking services between end devices and cloud computing data centers.

**Edge Layer**
is the first layer of connectivity for devices. Responsible for connectivity of devices and the management of data collection and connection to the server.

**Embedded Agent**
is a proprietary piece of software which vendors install on each device connecting to the cloud.

**Encryption**
is the conversion of electronic data into cipher text that theoretically can only be decoded by authorized parties.

**Endpoint Device**
is a computer or device that is internet capable.

### Exploit
is software, a subset of data or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-of-service (DoS or related DDoS) attack — an event where a human threat successfully takes advantage of a vulnerability for denial or delay of service, exfiltration or unauthorized modification of data.

# F

### Firewall
is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Usually the first line of defense in a network.

### Firmware Over The Air (FOTA)
is technology that allows vendors/manufacturers to wirelessly provide patches or provide software upgrades.

### Flow-Based Programming (FBP)
is a programming paradigm that defines applications as networks of "black box" processes, which exchange data across predefined connections by message passing, where the connections are specified externally to the processes.

# G

### Geofencing
is the use of GPS (Global Positioning System) or RFID (radio-frequency identification) technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area.

### Governance, Risk and Compliance (GRC)
is the process of how an organization manages its information resources. This process usually includes all aspects of how decisions are made for that organization, such as policies, roles and procedures the organization uses to make those decisions. It is designed to ensure the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes, and addresses how expected performance will be evaluated.

### Global Positioning System (GPS)
is a global navigation system that provides location and time information to a receiver anywhere on Earth.

## H

### Hacker
a slang term that can mean a hostile human threat to IT systems, an IT security professional, a vulnerability researcher or an amateur security person.

### Home Automation
is a combination of hardware and software that allows the control/management of applications, electronics and devices in a home. Some examples would be home thermostats or smart speakers.

### Horizontal Business Model
is a system where many companies provide cloud platforms and gateways to many users.

## I

### Industrial Control Systems (ICS)
are IT systems used to control industrial processes such as manufacturing, product handling, production and distribution.

### Information States
refers to the three primary, non-overlapping states of information, which are: transmission, storage and processing. Data is in one of these three states at any given point.

### Ingestion
is the process of uploading data records into storage, through a gateway.

### Intellectual Property (IP)
is a work or invention that is the result of creativity, such as a manuscript or a design, to which one has rights and for which one may apply for a patent, copyright, trademark, etc.

### Internet of Things (IoT)
is the connectivity of physical objects such as vehicles, devices, buildings, and electronics, and the networks that allow them to interact, collect and exchange data.

### IoT Platform
provides service such as Data Storage, Connectivity Services, Analytics and Visualization. All of which provide the glue between devices and the cloud.

### Industrial Internet of Things (IIoT)
is the use of machines with sensors to monitor production systems for various outcomes (including higher quality and efficiency). See also M2M.

### Internet Protocol (IP)
is a set of rules governing the format of data sent over the network.

# L

### Lower-Power Devices
are designed to use less electrical power than conventional devices. These are critical to the future of IoT.

# M

### Machine to Machine (M2M)
are devices that exchange information without human intervention. Typically used in industrial and manufacturing applications.

### Machine Learning
is the application of artificial intelligence (AI) that provides systems with the ability to learn and improve from experience automatically without being explicitly programmed or upgraded.

### Media Access Control (MAC)
is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel.

## Mesh Network
is a local network topology in which infrastructure nodes (i.e. bridges, switches and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data to/from clients.

## Message Protocols
is the way information is transferred and communicated between devices, storage and the cloud.

## Microcontroller (MCU)
is a computer present in a single integrated circuit which is dedicated to performing one task and executing one specific application. It contains memory, programmable input/output peripherals, as well a processor.

## MOTE
*(Short for remote)* is a node in a sensor network that is capable of performing some processing. This term is most common in North America.

# N

**Near-Field Communication**
is a low power, low speed, short range radio communication standard that allows communication between devices in close proximity.

**Network**
is a system of computers that are joined together so that they can communicate by exchanging information and sharing resources.

**Non-Repudiation**
is a method of guaranteeing message transmission between parties via digital signature and/or encryption.

# P

**Penetration Testing**
is a live test of the effectiveness of security defenses through mimicking the actions of real-life human attackers.

**Personal Area Network**
is created through the connection of technology devices (cell phone, etc.) by single users.

**Personally Identifiable Information (PII)**
is information that can be traced back to an individual user through their name, postal address, or email address. Personal user preferences tracked by a website can also be considered personally identifiable when linked to other personally identifiable information.

**Precision Agriculture**
is a farming management concept based on observing, measuring and responding to inter- and intra-field variability in crops using computers and the internet.

**Privacy**
is the right of a human individual to control the distribution of information about themselves; it documents the rights and obligations of individuals and organizations with respect to the collection, use, retention and disclosure of personal information.

**Privacy Impact Assessment (PIA)**
is a decision tool used to identify and mitigate privacy risks. Notifies the public of 1) what PII is being collected, 2) why the PII is being collected and 3) how the PII will be retrieved, shared, accessed and stored.

**Propagator**
manages message routing protocol translation services.

### Provisioning
is a method of using an identity store to create identities for new devices in the scope of the system or to remove devices from the system.

# R

### Radio Frequency Identification (RFID)
is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person.

### Real-Time Operating System (RTOS)
is an operating system (OS) intended to serve real-time applications that process data as it comes in, typically without buffer delays. Processing time requirements (including any OS delay) are measured in tenths of seconds or shorter increments of time.

### Remote Access
is the ability to access a computer from a different location, usually a home or office.

### Risk
is the possibility of damage or harm, and the likelihood that damage or harm will be realized; a function of the likelihood of a given threat source

exploiting a potential vulnerability, and the resulting impact of that adverse event on the organization.

### Risk Assessment
is the evaluation of the threats, vulnerabilities and assets of information systems to determine the likelihood threats will exploit these vulnerabilities and weaknesses to cause adverse effects.

### Risk Management
is the process of designing, developing, sustaining and modifying operational processes and systems in consideration of applicable risks to asset confidentiality, integrity and availability. Applicable risks are those reasonably expected to be realized and to cause an unacceptable impact.

### Role-Based Access Control (RBAC)
is an access control model that bases the access control authorizations on the roles (or functions) that the user is assigned within an organization.

## S

### Secrecy
is attempting to hide information or data.

### Secure Coding
is the practice of developing computer software in a way that guards against the accidental introduction of security vulnerabilities.

### Sensor
is a device that detects or measures a physical property and transform it into an electrical signal.

### Sensor Node
is a node in a sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. Sensor nodes are also known as motes. A mote is a node, but a node is not always a mote.

### Services
are defined as any software component or module that is interfacing with devices through a field gateway or cloud gateway for data collection and analysis, as well as for command and control interactions. Services are mediators.

### Smart Cities
use information and communication technologies to increase operational efficiency, share information with the public and improve both the quality of government and human welfare.

### Smart Buildings
use automated processes to automatically control the heating, ventilation, air conditioning, lighting, security and other systems.

### Special Purpose Devices
are devices that are scoped in purpose (simple temperature sensors to complex factory production lines) and provide some user interface. They can measure and report on various circumstances, control valves, sound alarms, switch lights on and off, or other tasks.

### Store and Forward
is a technique in which data/information is sent to an intermediate station where it is kept and sent at a later time to the final destination or to another intermediate station. The intermediate station verifies the integrity of the message before forwarding it.

## T

### Telemetry
is an automated communications process by which measurements and other data are collected at remote or inaccessible points and transmitted to receiving equipment for monitoring.

### Time Series Data
is a series of data points collected at regular intervals and indexed in time order. One example might include a smart electricity meter in a home. It allows for the storage, analysis and visualization of events to provide insights into trends and anomalies.

### Threat
is a person, event or circumstance with the potential to cause harm for an asset. Threats are either environmental or human-based.

### Threat Actor
is a human-based agent that can negatively impact a systems' IT assets. The threat agent is evaluated on the agent, intent, target and mechanism used.

### Tokenization
is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value.

## V

### Vertical Business Model
is a system where all services are provided and controlled by the same company. Some examples of verticals are Smart Buildings, Smart Cities, Precision agriculture, Health Care, Wearable Technology and Autonomous Vehicles.

### Vulnerability
a weakness or exposure in a technology, protocol or design of an information technology system such as hardware, firmware and software.

# W

### Wearable Technology
can be worn by a consumer and often include tracking information related to health and fitness. Examples include, but are not limited to, watches, fitness trackers and heart monitors.

### Wireless Fidelity (Wi-Fi)
is a facility allowing computers, smartphones, or other devices to connect to the internet or communicate with one another wirelessly within a particular area.

### Wireless Sensor Network (WSN)
refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind and so on.

# PROTOCOLS

### 6LoWPAN
is an acronym of IPv6 over Low Power Wireless Personal Area Networks.

### 802.15.4
is a technical standard which defines the operation of low-rate wireless personal area networks (LR-WPANs). It specifies the physical layer and media access control for LR-WPANs, and is maintained by the IEEE 802.15 working group, which defined the standard in 2003. It is the basis for the ZigBee.

### Advanced Message Queuing Protocol (AMQP)
is an open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.

### BACnet
is a communications protocol for Building Automation and Control (BAC) networks that leverage standard protocols like (ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers), ANSI (American National Standards Institute), and ISO (International Organization for Standardization) 16484-5).

### Bluetooth
is a standard for the short-range wireless interconnection of mobile phones, computers and other electronic devices.

### Constrained Application Protocol (CoAP)
is an application layer protocol that is intended for use in resource-constrained internet devices.

### Hypertext Transfer Protocol Secure (HTTPS)
is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit through a secure socket layer (SSL) or transport layer security (TLS) protocol connection.

### Internet Protocol Suite (TCP/IP)
is short for Transmission Control Protocol/Internet Protocol). A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.

### Internet Protocol Version 6 (IPv6)
is an internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks.

### Low-Power and Lossy Networks (LLN)
are typically optimized for energy efficiency, may use IEEE 802.15.4, and can be applied to industrial monitoring, building automation, connected homes, healthcare, environmental monitoring, urban sensor networks, asset tracking and more.

### Low-Power Wide-Area Network (LPWAN or LPWA or LPN)
is a wireless network that provides long range communication at low bit rates between connected objects. (e.g.: Sensors operated on batteries.)

### Message Queuing Telemetry Transport (MQTT)
is a lightweight messaging protocol for small sensors and mobile devices, optimized for high-latency or unreliable networks. Uses TCP/IP.

### Routing Protocol for LLN (RPL)
is the routing protocol developed specifically for low-power and lossy networks, in which nodes and routers are expected to be power-constrained.

### Secure File Transfer Protocol
is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol.

**Secure Shell (SSH)**
is a network protocol that provides administrators with a secure way to access a remote computer. SSH also refers to the suite of utilities that implement the protocol.

**Secure Sockets Layer (SSL)**
is a standard security technology for establishing an encrypted link between a server and a client.

**Websocket**
provides full duplex communication channels over a single TCP connection.

**ZigBee**
is an open standard for wireless communications specifically designed to use low-power digital radio signals for personal area networks (PAN).

**Z-Wave**
is a wireless communication protocol used primarily in-home automation.

# ABOUT THE (ISC)² ADVISORY COUNCIL OF NORTH AMERICA

The Advisory Council of North America represents a group of senior-level information security professionals in North America who advise (ISC)² on industry initiatives, policies, views, standards and concerns. The goals of the advisory councils are to offer deeper insights into the needs of the information security community in each respective region; discuss matters of policy or initiatives that drive professional development; provide feedback on (ISC)² programs, activities and opportunities; and make introductions to influential organizations, bodies, institutions within government and industry with which (ISC)² should engage.

For more information, please visit:
www.isc2.org/About/Advisory-Council

# ABOUT (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, over 138,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit www.isc2.org.

# AKNOWLEDEGMENTS

(ISC)² recognizes **Diana-Lynn Contesti**, CISSP, CISSP-ISSAP, CISSP-ISSMP, CSSLP, SSCP and a special thanks to **Ercenk Keresteci** of Microsoft for their invaluable support in creating the IoT Lexicon.

Inspiring a Safe and Secure
Cyber World.