Glossary of Cyber Security Terms

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

Cyber security is not always easy to understand because it is a constantly changing, complex problem and it is a factor at every point in a system's or device's life cycle. As systems become more complex, successful cyber attacks are increasing and there is renewed focus on security. As you look to protect your system, equipment, assets, or IP, here are some cyber security terms and definitions commonly used in connected systems.

Term	Definition	Source
AES	A U.S. government-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.	NIST CSRC Glossary
Attestation	Issue of a statement, based on a decision that fulfillment of specified requirements has been demonstrated. Applied to security: A cryptographic measurement (measured boot) of the platform from power on to a functional trusted platform. This attestation measurement provides proof that the platform is trusted and will perform its intended function as intended.	ISO/IEC 29109-1:2009 (First sentence only)
Authentication	Provision of assurance that a claimed characteristic of an entity is correct.	ISO/IEC 27000:2016
Availability	Property of being accessible and usable upon demand by an authorized entity.	ISO/IEC 27000:2016
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.	ISO/IEC 27000:2016
Countermeasure	Action, device, procedure, technique, or other measure that is designed to minimize vulnerability.	ISO/IEC 2382:2015
Credential	Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.	CNSSI 4009
Cryptography	Discipline that embodies principles, means, and mechanisms for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.	ISO/IEC 18014-2:2009
Data at Rest	Stored data that is neither being processed nor transferred.	IIC
Data in Motion	Data being transferred from one location to another.	ISO/IEC 27040:2015
Data in Use	Data being processed.	IIC
Data Integrity	Property that data has not been altered or destroyed in an unauthorized manner.	ISO/IEC 27040:2015
Denial of Service (DOS)	Prevention of authorized access to resources or the delaying of time-critical operations.	ISO/IEC 27033-1:2015
ECC	Elliptic curve cryptography, the public key cryptographic methods using operations in an elliptic curve group. ECC is based on the assumption that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible.	NIST CSRC Glossary (First sentence only)
Edge	Boundary between the pertinent digital and physical entities, as delineated by IoT devices.	IIC
Edge Computing	Distributed computing that is performed near the edge, where the proximity is determined by the system requirements.	IIC
Encryption	Reversible operation by a cryptographic algorithm converting data into cipher text so as to hide the information content of the data.	ISO/IEC 9798-1:2010
Endpoint	The point where data is created or consumed. The beginning stage of a process or the end stage of the process.	
Endpoint Identity	Inherent property of an instance that distinguished it from all other instances. When applied to devices, it typically involves using stored secret and cryptographic authentication methods to validate that the device is in procession of the secret.	
Endpoint to Endpoint	The point from where data is created to the point where the data is consumed. When applied to communication, it is the sending of data from where it is created (point A) to the point where it is consumed (point B). It does not take into account how or what form the data flows from point A to point B, only the interaction between point A and point B.	
Entropy	The measurement of how random an event is. In security terms, number of bits of entropy is typically used to define the effective number of random bits used as the key for a cryptographic algorithm.	

Term	Definition	Source
Hardware Root of Trust	Hardware root of trust (HW RoT) forms the basis for the security that is performing the security functions. This basis is rooted in immutable hardware providing cryptographically protected functions. Typical protections include cryptographically strong validation of mutable elements for authentication, integrity, identity, attestation, tamper resistance, and protection of security sensitive data with a well-defined boundary.	
Identity	Inherent property of an instance that distinguishes it from all other instances.	ISO/IEC/IEEE 31320-2:2012
Identity Authentication	Formalized process of identity verification that, if successful, results in an authenticated identity for an entity.	ISO/IEC 24760-1:2011
Identity Verification	Process to determine that presented identity information associated with a particular entity is applicable for the entity to be recognized in a particular identity domain at some point in time.	ISO/IEC 24760-1:2011
Immutable Components	Immutable components are unchangable. Data that can only be written, not modified. For example, hardware mask or one time programmable (OTP). Note: some definitions allow cryptographically protected protection methods.	
Industrial Control System (ICS)	Combination of control components that act together to exercise control in the physical world.	IIC
Industrial Internet	Internet of Things, machines, computers, and people that enable intelligent industrial operations using advanced data analytics for transformational business outcomes.	IIC
Industrial Internet of Things (IIoT) System	System that connects and integrates industrial control systems with enterprise systems, business processes, and analytics. Note 1: industrial control systems contain sensors and actuators. Note 2: typically, these are large and complicated systems.	IIC
Information Technology (IT)	Entire spectrum of technologies for information processing, including software, hardware, communications technologies, and related services. Note: Although information technology (IT) technologies are used in operational technology (OT), information technology (IT) is traditionally considered to be distinct from operational technology (OT) due to a different set of requirements and concerns.	Gartner IT Glossary
Integrity	Property of accuracy and completeness.	ISO/IEC 27000:2016
IoT Actuator	IoT device that can change a property of a physical entity in response to an input.	IIC
IoT Device	Endpoint that interacts with the physical world through sensing or actuating.	IIC
IoT Sensor	IoT device that observes properties of the physical world and converts them into a digital form.	IIC
IT/OT Convergence	Process of interweaving information technology (IT) and operational technology (OT) in order to create Industrial Internet of Things (IIoT) systems.	IIC
Key Store	See secure storage.	
Measured Boot	Attestation measurement of the mutable elements starting with the root of trust and sequenctially measuring all subsiquent executing modules provided evidence of the software running on the platform.	
Mutable	Mutable components are changeable. For example, firmware, software, configuration, calibration.	
Nonrepudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.	ISO/IEC 27000:2016
Operational Technology (OT)	Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.	Gartner IT Glossary
Personally Identifiable Information (PII)	Any information ▶ that identifies or can be used to identify, contact, or locate the person to whom such information pertains, ▶ from which identification or contact information of an individual person can be derived, or ▶ that is or might be directly or indirectly linked to a natural person.	ISO/IEC 24745:2011
Public Key Infrastructure (PKI)	Structure of hardware, software, people, processes, and policies that uses digital signature technology to provide relying parties with a verifiable association between the public component of an asymmetric key pair with a specific subject.	ISO 21091:2013
Privacy	Right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.	ISO/TS 17574:2009
Private Key	A cryptographic key that is kept secret and is used with a public key cryptographic algorithm. A private key is associated with a public key.	NIST CSRC Glossary
Programmable Logic Controller (PLC)	Electronic device designed for control of the logical sequence of events.	ISO 13577-4:2014
Public Key	The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.	NIST CSRC Glossary
Random	Lacking a definite plan, purpose, or pattern. In security terms, a randomizer is typically used to create random numbers that are random sequences of 1s and 0s that are used as keys in cryptographic algorithms.	
Reliability	Ability of a system or component to perform its required functions under stated conditions for a specified period of time.	ISO/IEC 27040:2015
Resilience	Ability of a system or component to maintain an acceptable level of service in the face of disruption.	IIC
Root of Trust	Root of trust (RoT) forms the basis of security functions such as endpoint identity and attestation of software and hardware identity and integrity.	IIC Endpoint Security Best Practices

Term	Definition	Source
RSA	Rivest, Shamir, Adelman; an algorithm approved in [FIPS 186] for digital signatures and in [SP 800-56B] for key establishment. RSA's asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the factoring problem.	NIST CSRC Glossary (First sentence only)
Safety	The condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment.	ISO/IEC Guide 55:1999
Secure Boot	Secure boot is a cryptographically enforced process that starts from immutable or cryptographically protected bootstrap code executed at power up. The boot process requires validation of the immutable hardware platform functionality and cryptographic integrity checks and cryptographic authenticity checks for mutable content (firmware, software, calibration, configuration). It assures that the system is trustworthy and performing its intended functions and has not been compromised.	
Secure Communications	It is how data is shared between point A to point B with varying degrees of certainty that third parties cannot intercept or understand the data. Secure communications includes confidentiality and integrity of the data in transit. It is normally accomplished with a series of steps that include authentication to determine the identity of point A and point B, followed by encryption and integrity checks of the data from point A to point B.	
Secure Debug	Debug interfaces access and functionality are lockable by immutable methods (fuse) or cryptographically protected methods.	
Secure Storage	Provides a protected location for storing security critical data and only allows access by authorized security functions. This is typically implemented using an encryption key that encrypts all the security critical data prior to storage. Sometimes this is referred to as a secure key store.	
Security	Property of being protected from unintended or unauthorized access, change, or destruction to ensure availability, integrity, and confidentiality.	IIC
Security Controls	Management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.	ISO 12812-1:2017
Security Function	Cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, symmetric or asymmetric key algorithms, message authentication codes, hash functions or other security functions, random bit generators, entity authentication, and SSP generation and establishment all approved either by ISO/IEC or an approval authority.	ISO/IEC 19790:2012
Security Policy	Rules, directives, and practices that govern how assets, including sensitive information, are managed, protected, and distributed within an organization and its systems, particularly those that impact the systems and associated elements.	NISTIR 7298, rev 2
Secure Update	Secure update is a cryptographically enforced process that validates the cryptographic integrity and authenticates the source of the update image prior to performing the update process.	
Security Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	NISTIR 7298, rev 2
SHA	A hash algorithm with the property that it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.	NIST CSRC Glossary
Stakeholder	Individual, team, organization, or classes thereof having an interest in the system of interest.	ISO/IEC/IEEE 42010:2011
Trust	Trust is the probability that the intended behavior and the actual behavior are equivalent, given a fixed context, fixed environment, and fixed point in time. Trust is viewed as the level of confidence.	NIST 8222
Trust Boundary	Separation of different application or system domains in which different levels of trust are required.	IIC
Trusted Execution Environment	Secure processing region providing guarantees that code and data will be protected with respect to authenticity, confidentiality, and integrity. This isolated execution environment provides security features such as isolated execution, integrity of applications executing, and confidentiality of data and assets from the rest of the larger system.	
Trustworthiness	Degree of confidence one has that the system performs as expected with characteristics including safety, security, privacy, reliability, and resilience in the face of environmental disturbances, human errors, system faults, and attacks.	IIC
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.	ISO/IEC 27000:2016
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. Note: this could also be called compliance testing.	ISO/IEC 27000:2016
Verified Boot	Boot policies are enforced during the boot process. Starting with the root of trust for verification, the currently executing module verifies the next module against a policy.	Trusted Computing Group
Vulnerability	Weakness of an asset or security controls that can be exploited by one or more threats.	ISO/IEC 27000:2016

AHEAD OF WHAT'S POSSIBLE™

Analog Devices, Inc.
Visit analog.com

For regional headquarters, sales, and distributors or to contact customer service and technical support, visit analog.com/contact.

Ask our ADI technology experts tough questions, browse FAQs, or join a conversation at the EngineerZone Online Support Community. Visit ez.analog.com.

©2019 Analog Devices, Inc. All rights reserved. Trademarks and registered trademarks are the property of their respective owners.

Ahead of What's Possible is a trademark of Analog Devices.

BR21375-5/19