THE (ISC)² ICS

LEXICON

An introduction to basic Industrial Control System (ICS) & cybersecurity terminology and concepts

INTRODUCTION

(ISC)², the world's largest nonprofit membership association of certified cybersecurity professionals, is pleased to provide you with the (ISC)² ICS Lexicon. This a follow-up and companion to the (ISC)² Cybersecurity Lexicon, developed with the (ISC)² Advisory Council of North America, industry leaders and technology experts.

The ICS Lexicon provides professionals, journalists, boards of directors and others with a quick reference guide for common ICS 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.

Feel free to contact the (ISC)² Cybersecurity Advocate team at www.isc2.org/cybersecurity-advocates.

A

Active Scans
The use of scanning software to probe information technology (IT) resources and data on a defined set of systems, and check for vulnerabilities, misconfigurations and missing security updates.

Actuator
A component of a machine responsible for moving and controlling a mechanism or system.

Airgap
A network security measure employed on one or more IT systems to ensure they are physically isolated from any other systems or networks.

Antivirus
Software designed to detect and prevent computer viruses and related malware (malicious software) from getting on to a system and causing harm to it, using it for unintended purposes, or rendering it unusable.

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

Asset

Any item, data element or mission-based system that has value to an organization; including both tangible items such as IT systems and physical property, as well as intangibles such as intellectual property and data.

Attack Surface

The aggregate of all points of access to or exposure of systems, with potential to be compromised by, or provide a foothold for an attacker. A smaller attack surface can help make attacks less likely to succeed and reduce 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.

Software Attack Surface

Comprised of the software environment and its interfaces, these are the applications and tools available to authorized (and unauthorized) users.

Network Attack Surface

Ports, protocols, channels, devices (from routers and firewalls to laptops and smart phones), services, network applications and even firmware interfaces.

Human Attack Surface
The totality of all exploitable vulnerabilities within an organization that are created through the activities and decisions of its personnel. Elements of an organization's human attack surface include negligence, errors, illness, death, insider threat and susceptibility to social engineering among many others.

Authentication
The process or action of verifying the identity of a user or process.

Authorization
The process of assigning approved access to specific data to an authenticated user.

Availability
The attribute of data that ensures it is always available to authorized users when required for use. It is part of the "CIA Triad" of essential information security principles (along with confidentiality and integrity).

B

Blacklisting
A basic access control mechanism that allows the passage of all elements (email addresses, users, passwords, URLs, IP addresses, domain names, file

hashes, etc.), except those explicitly defined. The defined items are denied access. The opposite is a whitelist. Both blacklisting and whitelisting are also used with software programs, either denying specific applications on a blacklist the ability to run on a system or allowing only those applications on a whitelist to run.

C

Confidentiality
The attribute of data that ensures information is only being exposed to appropriately authorized parties and systems. Part of the CIA Triad of essential information security principles.

Controller
See Programmable Logic Controller (PLC).

Control Center
A central location for managing, monitoring and interacting with both IT and OT (operational technology) devices that run at industrial sites. Attacks on control centers that manage critical infrastructure, such as power plants that are part of the electrical grid, are a major risk due to the significant potential impact if they are caused to fail or suffer performance issues.

Critical Infrastructure
A term used to describe assets that are essential for the operation of society. This can include (but is not limited to) power generation, electricity distribution, water treatments facilities, oil and chemical refineries, communications, first responders and manufacturing.

D

Discretionary Access Control (DAC)
A system that uses discretionary access controls and allows the owner, creator or data custodian of an object to control and define access to that object.

Distributed Control System (DCS)
Systems that are typically used to control and monitor industrial processes and production systems within the same physical location. They are used in industrial sites such as oil refineries, power plants, automobile manufacturing plants and many others.

Data Diode
Also known as a uni-directional gateway, it is a network appliance or device allowing data to travel only in one direction. They are most commonly found in high-security environments such as defense, where they serve as connections between two or more networks of differing security classifications - also known as a Cross Domain Solution (CDS).

This technology is also found at the industrial control level for such facilities as nuclear power plants, electric power generation/distribution, oil and gas production, water/wastewater, airplanes (between flight control units and in-flight entertainment systems) and manufacturing.

Defense in Depth

The coordinated use of multiple safeguards – which can be administrative, physical and/or technical – to protect the confidentiality, integrity and availability of information assets and systems. A key principle within Defense in Depth is that there should be compensating controls in place to defend a system if one countermeasure fails. One example is making sure that systems that are protected by a firewall also have other security controls (e.g. encryption, access control, endpoint security) in place in case the firewall is compromised.

Demilitarized Zone (DMZ)

Sometimes referred to as a perimeter network, it is a physical or logical subnetwork that contains an organization's external-facing services and allows connections from them to an untrusted network, usually a larger network such as the internet. Security measures, and access controls in particular, on devices within a DMZ are typically stronger than in any other area of a network.

Distributed Network Protocol (DNP3)
One of the most common ICS communication protocols. It was developed specifically for Supervisory and Data Acquisition (SCADA) systems with data acquisition equipment to communicate between Remote Terminal Units (RTUs), Master Terminal Units (MTUs) and electrical components that have a microprocessor and can communicate using a protocol such as fieldbus or other industrial protocols.

E

Electronic Security Perimeter
Commonly referred to as ESP, it is a North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) term for the logical border surrounding a network to which Bulk Electric System (BES) cyber assets are connected using a routable protocol, and for which access is controlled.

Encryption
Used in the protection of data, it is a process of transforming data (in storage or in transit in data communications) in a way that results in it being unreadable by unauthorized users. Mathematical algorithms are used to transform 'plaintext' (normal) data into 'ciphertext', which can only read if it decrypted.

Endpoint

A term that refers to a single computing device – usually a desktop computer, laptop or smartphone and tablet class mobile devices. Not typically used for network servers that provide services to multiple computers.

European Union Agency for Network and Information Security (ENISA)

The center of expertise for cyber security in Europe. Similar to the US-CERT (U.S. Computer Emergency Response Team) organization in the United States.

Exploit

Software, a subset of data or a sequence of commands that exploits a vulnerability to cause unintended and often damaging results to the system being exploited. Common examples include gaining unauthorized and full control of a computer, causing a Denial of Service (using up such a great percentage of resources on a system that it can no longer provide the service/s it is intended to provide) or the unauthorized modification or export of sensitive data.

F

Firewall
A network security device that monitors incoming and outgoing network traffic and allows or blocks specific traffic based on a defined set of security parameters, or rules. Usually the first line of defense in a network.

H

Hacker
A slang term typically used to describe an adversary who is seeking to disrupt, exploit or compromise IT systems. The term 'White Hat Hacker' is used to describe security researchers and others who work with organizations to identify exploitable weaknesses before bad actors do.

Heartbeat
A term that describes a regular communication, or signal, between an intelligent electric device (IED) and a DCS or SCADA system. This is used as a monitoring check that verifies the connection is operational.

Honeypot
A computer system setup to attract and trap would-be attackers. This can serve to delay attacks on real

systems within an organization. It can also provide useful details on the types of attacks being made against the organization, so that defenses can be adjusted where appropriate.

Human Machine Interface (HMI)
The hardware, software or graphical user interface that allows a person to interact with a control system. It may display monitoring information such as alarm or alert conditions and trends.

I

Inter-Control Center Protocol (ICCP)
A client/server protocol for use in transferring data between control centers over wide area networks (WANs). It operates at the application layer (Layer 7) of the Open Systems Interconnection (OSI) Model.

Identity and Access Management (IAM)
The framework for business processes that facilitate the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management.

Industrial Automation (IA)
A category of operational technology systems that use control systems and IT to handle different processes and machineries to replace a human being. It is the second step beyond mechanization in the scope of industrialization.

Industrial Automation Control System (IACS)
A term used within the International IEC 62443 standards program to identify industry automation systems used to access controllers, collect data and monitor network infrastructure.

Industrial Control Systems (ICS)
A term used to cover a broad range of devices and systems used in industrial control and automation systems. It encompasses both IT and OT (operational technology) systems as well as both hardware and software involved in industrial processes.

International Electrotechnical Commission (IEC) 62443
A series of standards, technical reports and related information that define procedures for implementing electronically protected IACS.

Intelligent Electronic Devices (IED)
PA term to describe a controller device with a microprocessor used with power systems like circuit breakers, transformers and capacitors.

Integrity
Part of the CIA Triad, an assurance that data and information are not subject to – intentional or unintentional – unauthorized modification. Supports the principle of Nonrepudiation listed on page 18.

Internet Protocol (IP)
An OSI Model network layer protocol that is synonymous with and at the core of internet communications. It enables the transfer of data from one computing device to another across a single network, or complex interconnected networks like the internet.

Intrusion Detection System (IDS)
Technology that alerts organizations to adverse or unwanted activity; a real-time monitoring of events as they happen in a computer system or network, using audit trail records and network traffic and analyzing events to detect potential intrusion attempts.

Intrusion Prevention System (IPS)
Technology that monitors activity like an IDS, but can automatically take proactive, preventive action if it detects unacceptable activity; any hardware or software mechanism that can detect and stop attacks in progress.

M

Mandatory Access Controls (MAC)
An access control method that is prohibitive rather than permissive. It uses an implicit 'deny' principle; if users are not specifically granted access to data, the system denies them access to the associated data. MAC controls rely on data labels, whereas Role-based Access Control (listed on page 22) are based on users' job functions.

MODBUS
A communication protocol used to establish master-slave/client-server communication between intelligent devices. It is the most widely used network protocol in industrial manufacturing environments and the de facto communication protocol within ICS.

Master Transmission Unit (MTU)
Part of the SCADA system that initiates communication with all remote sites. It communicates mostly with RTU's and PLC's within an ICS network.

Multi-Factor Authentication (MFA)
A method of computer access control that requires two or more ways of establishing identity. It is based on the concepts of something you know, something you are and something you have.

N

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
A set of cybersecurity standards and regulations that registered entities (regional electric power providers) are required to comply with or face potential monetary fines.

Network
System of computers, and/or connected devices, that are interconnected so that they can communicate by exchanging information and sharing resources.

Network Access Control (NAC)
Security solutions that use a set of protocols to implement policies for secure access to networks, using a set of checks against and actions on any device attempting to connect. Checks may include verifying antivirus and endpoint security measures functioning properly on the device attempting to connect. Actions may include quarantining devices that do not meet security standards or forcing the installation or updating of endpoint security software.

Network Segmentation
Network segmentation seeks to compartmentalize network resources (through physical or logical methods) to limit access to sensitive information for only specific applications, servers, and humans, with policy-defined access. This provides effective controls to mitigate network intrusion and limit lateral movement across the network, or programmed propagation of a threat. The use of a DMZ is frequently a part of network segmentation.

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)

A framework of cybersecurity guidance, built on global standards, guidelines and practices, designed originally with the goal of enhancing the resilience of the nation's critical infrastructure. It focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The CSF also provides a common taxonomy and mechanism for organizations to assess their current and target state for cybersecurity.

Nonrepudiation

Nonrepudiation prevents a subject from claiming not to have sent a message, or not to have performed an action, or not to have been the cause of an event. It is established using mechanisms such as digital certificates, session identifiers, transaction logs and others.

Operational Technology

The hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps switches and many others.

Open Platform Communications (OPC)
A platform-independent interoperability standard for industrial automation to allow for real-time, secure and reliable exchange of data between devices from multiple vendors.

Open Systems Interconnection (OSI) Model
A model to identify the communication path of network traffic. It is comprised of seven layers, Physical, Data Link, Network, Transport, Session, Presentation and Application.

P

Passive Scans
A method of device/asset discovery that relies on information gleaned from network data that is captured from a target computer without direct interaction and without adding additional traffic to the network. It is intended to minimize or eliminate any impact to the system(s) being scanned.

Penetration Test
An exercise intended to fully test the effectiveness of an organization's existing security controls and defenses. Penetration testing mimics the actions of an attacker and goes beyond vulnerability testing, in that it attempts to exploit any vulnerabilities identified.

Perimeter-Based Security Model
A technique of securing a network by controlling access to all entry and exit points of a defined IT environment.

Programmable Logic Controller (PLC)
A ruggedized computer used in industrial automation. PLCs can monitor and interact with input and output devices and automate specific processes and machine functions.

Process Field Bus (Profibus)
A standard communication protocol created in Germany and mainly used within Siemens industrial automation products.

Process Field Net (ProfiNET)
An industry standard communication protocol using for transmitting data within an industrial Ethernet network. It was designed to collect data, control systems within demanding time constraints, usually within one millisecond.

Purdue Reference Mode
A framework created by Purdue University to identify the components in the segments (or zones) of a typical ICS network and the various connections and dependencies between them.

R

Red Team Testing
Exercises conducted with the use of adversarial techniques and procedures to identify vulnerabilities in an organization's hardware, software and personnel, and ways to compromise systems. These are often carried out by independent, external security teams to test
how well an organization would fare in the face of a real attack.

Relay
An electrically operated switch used within an electrical system to protect circuits from faults or overloads. Usually classified with protective relays.

Remote Access
The ability to access a network or computer from a different location or an untrusted network, like a home or office or remote location.

Remote Terminal Unit (RTU)
A computer-controlled device in a SCADA environment that connects to physical devicesand sends data to a master device or MTU.

Risk
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 impact on the organization.

Risk Assessment
A process of evaluating relevant threats, vulnerabilities and assets of information systems, as well as existing controls and countermeasures, to determine the likelihood threats will exploit these vulnerabilities and weaknesses and cause adverse impacts. The output of a risk assessment includes recommendations on how to address identified risks, and enables management to make risk-aware decisions.

Risk Management
A detailed process of identifying factors that could damage systems or disclose data, evaluating those factors considering systems/data value and countermeasure costs, and implementing cost-effective solutions for mitigating or reducing risk. This process is used to develop and implement information security strategies. The goal of these strategies is to reduce risk and to support the mission of the organization.

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

Rule-Based Access Control
An access control model that allows or denies requests to resource objects based on a set of rules defined by a system administrator.

S

Safeguard
A process, procedure, technique or feature that mitigates the effects of a risk or vulnerability. Safeguards can be in the form of technology, procedures/policies or human factors.

Safety Instrumented Systems (SIS)
Refers to control systems used in maintaining safe conditions when other systems fail. They are built to run independently from other equipment in a facility and to provide robust safety for critical processes. They can trigger alerts or shutdowns when monitoring detects potentially dangerous conditions.

Secrecy
The condition of being hidden or concealed.

Secure Coding
The practice of designing and developing computer software in a way that guards against the accidental or purposeful introduction of security vulnerabilities.

Substation
A facility that houses a collection of equipment used with generation, transmission or distribution of electricity on the grid. They also contain SCADA systems and have the ability to transform voltage from high to low, or vice-versa.

Supervisory Control and Data Acquisition (SCADA)
SCADA systems are used for unattended monitoring and control of pipelines, water, waste water, and utility grids. The two basic components of a modern SCADA system are the RTU and the central station computer. SCADA functions include data acquisition, data communication, data presentation and control.

Stuxnet
A computer worm discovered in July 2010 which was the first documented use of a program targeted against an ICS. It is believed to have been designed to look for specific PLC's to infect and then damage the nuclear centrifuges at an Iranian nuclear facility.

T

Threat
Any circumstance or event with the potential to adversely impact organizational operations and assets. Threats exploit specific vulnerabilities. A threat must have a matching weakness in a system that it can exploit, or act upon, if it is to be an effective threat.

Threat Agent
Also known as a threat actor, this is something that causes or initiates a threat against a vulnerability. A threat agent may be a malicious person seeking to compromise or do harm to systems or a natural threat, such as a fire that results from faulty fire detection or suppression equipment.

TRISIS/TRITON
The first known attack that was directed at the safety system in an ICS environment. The attack targeted Schneider Electric's Triconex safety system with custom malware. Two of the plant's safety-instrumented systems (SIS) controllers entered a failed safe mode that shut down the industrial process and ultimately led to the discovery of the malware.

V

Variable Frequency Drives (VFD)
A type of adjustable-speed drive used in electro-mechanical drive systems to control alternating current (AC) motor speed and torque by varying motor input frequency and voltage.

Virtual Machine
A software-based computer that fully emulates the functionality of a physical computer. An operating system running as a virtual machine will appear identical to a physical machine to the applications running on it. Virtual machines are often referred to as "guests," and multiple guests can run on one host or physical server.

Vulnerability
A weakness or flaw in hardware, software, technical or administrative controls, or systems as a whole.

Vulnerability-Based Security Model
A risk assessment methodology centered on the presence or absence of vulnerabilities irrespective of the threats or asset value.

W

Whitelisting
A basic access control mechanism that allows the passage of only specific elements (email addresses, users, passwords, URLs, IP addresses, domain names, file hashes, etc.), that are specifically defined. The opposite is a blacklist. Both blacklisting and whitelisting are also used with software programs, either denying specific applications on a blacklist the ability to run on a system or allowing only those applications on a whitelist to run.

Z

Zone
Used to describe a segment of a network. See 'Network Segmentation' on page 17.

ABOUT THE (ISC)² ADVISORY COUNCIL OF NORTH AMERICA

The Advisory Council of North America represent 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 council 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, more than 140,000 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 The Center for Cyber Safety and Education™. For more information on (ISC)², visit **www.isc2.org**, follow us on **Twitter** or connect with us on **Facebook** and **LinkedIn**.

ACKNOWLEDEGMENTS

(ISC)² recognizes **James McQuiggan**, CISSP, **Toni Hahn**, CAP, CISSP and **Patrick Jordan**, CCSP, CISSP for their invaluable support in creating the ICS Lexicon.

NOTES

NOTES

NOTES

Inspiring a Safe and Secure
Cyber World.