TM256-24B Home > Welcome > **TM256 Glossary**

This item is also available in Resources: section 1.

TM256 Glossary

Wednesday, 31 Jan 2024, 11:27

3

3 Digital Encryption Standard (3DES)

A symmetric block cipher with a key length of 112 or 168 bits. An extension of the original Digital Encryption Standard (DES).

A

AAA (Triple-A, 'The three As')

A widely-used abbreviation for the related cyber security concepts of **authentication**, **authorisation** and **accounting** which are often discussed together in the literature.

(See also: Authentication, Authorisation and Accounting)

Access Control List (ACL)

A list of entities who have permissions to access an object in a Discretionary Access Control (DAC) system.

Accountability

Any process for identifying usage of system resources.

The functional process of a system that enables tracing a set of actions on a system, of an entity (typically a user of the system), uniquely to that specific entity. Such processes are part of the operating systems functions in a computer system.

This is sometimes called accounting.

Accounting

Any process for identifying usage of system resources.

The functional process of a system that enables tracing a set of actions on a system, of an entity (typically a user of the system), uniquely to that specific entity. Such processes are part of the operating systems functions in a computer system.

This is sometimes called accountability.

Active attack

An attempt to make changes in a system – such as by stealing or destroying data – or to impact its operation – such as a denial-of-service attack.

(Cf. passive attack)

Active employment

One of the three main phases of employment, the others being recruitment, and termination.

Advanced Encryption Standard (AES)

A symmetric block cipher widely used across the internet and in Wi-Fi networks. Also known as the Rijndael algorithm.

Advanced Persistent Threat (APT)

A form of attack using multiple attack vectors over a prolonged period.

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

A model for describing attacks in which the attacker's goals are divided into twelve tactics, each of which contains several techniques for achieving that goal.

Also known as MITRE ATT&CK ®

Air-gapped network

A physically isolated network which is not interconnected with any other network.

Application layer

Layer above the TCP/IP protocol stack (in general, any communication layer) that sends and receives data for particular applications such as DNS, HTTP, and SMTP

ARPANET

A packet-switched network developed by the United States Advanced Research Projects Agency between 1966 and 1969 which demonstrated many of the concepts and protocols used by the modern Internet. ARPANET was officially decommissioned in 1990.

Asset

Something that is of value to an organisation or individual.

(See also intangible asset and tangible asset)

Asymmetric cryptography

A cryptographic method that uses two distinct keys – one public and one private.

Attack

Any form of unauthorised access affecting the confidentiality, integrity or availability of an asset.

(See also active attack, passive attack, targeted attack and untargeted attack)

Attack surface

The sum of all the vulnerabilities in a system through which an attack could be made.

Attack vector

The method by which a threat is realised.

Audit

An evaluation of an organisation’s security preparedness.

Auditd

A feature that is native to the Linux kernel that is used to audit events within the system.

Authentication

Any process by which an identity is assigned to an entity.

Authentication Header (AH)

Information added to an IP packet to provide a means to check for data integrity and data.

Authenticity

Authenticity is the quality of being Authentic. It is a security measure that establishes the validity of the data/information exchanged and its originator. It is also a means of verifying the identity of a user to authorise the user to access data/perform a task on a system.

Authorisation

This is the process of granting a user of a system the permission to access and utilise a resource on it. The resource could be a specific file, ability to view/modify it, store it on a drive, execute a process or program, or initiate/receive messages. Typically, this function is a part of the operating system functions on a computer.

Availability

A key concept in the CIA Triad, availability is the property of being accessible and usable on demand by an authorised entity.

(Cf. confidentiality and integrity)

B

Base64

A common method (or set of methods) used for encoding data on the World Wide Web.

Basic Input/Output System (BIOS)

The basic input and output system is the program used to start the system up and load the operating system (OS) when it is powered on. It also manages the connections between the OS and attached devices.

Basic operating system

A simple operating system architecture which places all elements (hardware access, applications etc) within a single trust environment such that once authorised a user has unrestricted access.

BCP life cycle

The phases of continuous cycle of improvement and validation for a Business Continuity Plan (BCP). The main phases are analysis, design, implementation, and validation. As a continuous process, the output of validation phase feeds into the analysis phase.

Birthday attack

A type of cryptographic attack, which exploits the mathematics behind the birthday problem in probability theory. The birthday problem, also known as the Birthday Paradox, states that in a random group of 23 people, there is about a 50 percent chance that two people have the same birthday.

Black box

A term used to describe any unknown system where there is an input and an output.

Blacklist

This blocks access to known bad entities, such as some websites. For example, a school may block access to YouTube.

Block cipher

A cryptographic method in which the data is broken into smaller blocks for encryption and decryption using a cryptographic key and a cryptographic algorithm. The cipher text is of the same size of the original data block. The number of bits in a block is referred to as the block size.

Blowfish

A symmetric encryption method designed by Bruce Schneier in 1993 and uses a 64-bit block size with a variable length key**.**

Breach

A security event resulting in the confirmed compromise of an asset.

(Cf. incident)

Bring Your Own Devices (BYOD)

Policies that allow employees to access organisational data or resources through their own personal computers or mobile devices.

Brute-Force Attack (BFA)

A cryptanalytic method that uses an exhaustive approach to recover a key. It attempts to use every possible key or password combination until one that works is found.

Business continuity

The capability of an organisation (including non-IT resources, such as staff, buildings, supply chains and delivery capability) to continue delivering its products and/or services to a satisfactory level, following a disruptive incident.

Business continuity management (BCM)

The process applied by an organisation’s management, who identify and review the mission-critical components of an organisation. Threats, their impact, and strategies to improve the organisation’s resilience to these are typically performed as part of BCM. BCM is made up of three layers: Business continuity programme, Business continuity readiness and Business continuity operations.

Business continuity management plan (BCMP)

A collection of plans, designed to operationalise the BCM. A BCMP typically contains an emergency response plan, a crisis management plan, and a recovery/restoration plan.

Business continuity operations

One of the three layers of business continuity management (BCM) which contains three overlapping phases of activity performed by an organisation to maintain business continuity. These three phases are emergency response activity, crisis management activity, and recovery/restoration activity.

Business continuity programme

One of the three layers of business continuity management (BCM) which focuses upon ongoing governance processes to initially identify and then review the objectives for business continuity.

Business continuity readiness

One of the three layers of business continuity management (BCM) which focuses upon a collection of strategies and procedures designed to better prepare an organisation to respond to an incident and maximise its business continuity capability.

Business impact analysis (BIA)

An activity designed to understand the organisation and where it may be vulnerable in the event of an incident, regardless of whether this is cyber security-related or not.

Business resilience

The state where an organisation is able to to quickly adapt to disruptions whilst maintaining continuous business operations and safeguarding people, assets, and overall brand equity.

C

Caesar cipher

An example of ancient cryptography, said to have been used by Julius Caesar. A Caesar cipher is a mono-alphabetic substitution cipher in which the alphabet in the plain text is shifted by a fixed number.

Certificate authority

A trusted institution who will authenticate the ownership of a public key.

ChaCha20

A symmetric stream encryption method used in some https website pages.

Chain of custody (CoC)

A written record of how evidence has been handled and by whom between its initial discovery and subsequent analysis.

See also continuity of evidence

Checksum

Data that can be used to compare against other data to verify authenticity.

Chosen Ciphertext Attack (CCA)

A cryptanalyst gathers information by choosing a ciphertext and attempts to obtain its decryption. There is no knowledge of the key used for the decryption. This type of attack is applicable to public-key cryptosystems.

Chosen Key Attack (CKA)

A key is known in part or in full and the cryptanalyst attempts to understand the structural property of the cipher to be able to compromise the capability of the entire system that uses the cipher.

Chosen Plaintext Attack (CPA)

A scenario in which the attacker has the ability to choose plaintexts and to view their corresponding ciphertexts.

CIA Triad

A security model composed of three concepts used in the development of security policies:

The concept of confidentiality holds that data can only be accessed by authorised users. Integrity is the concept that data must not be changed without authorisation. Availability is the concept that data should be available whenever it is needed.

Cipher

An algorithm used in the encryption and decryption of data. Alternative spelling: cypher.

Ciphertext

This is the output of an encryption algorithm. (The input is the plaintext).

Ciphertext attack

Another name for a dictionary attack where a hacker has a list of possible passwords which are tried one at a time.

Ciphertext-Only Attack (COA)

The attacker can only monitor the encrypted communication and therefore has access only to ciphertext, but not the corresponding plaintexts.

Civil justice

Civil justice is a system of law used to resolve disputes between individuals and organisations.

Common Vulnerabilities and Exposures (CVE)

A database hosted by the MITRE Corporation containing standardised identifiers for publicly disclosed vulnerabilities.

Compliance

Compliance provides an organisation, or auditors, with the information needed to determine if the system is operating in accordance with the relevant standards, regulations, or internal policies.

Compliance fatigue

Tiredness and frustration created amongst users by a requirement to conform to burdensome rules, regulations and processes.

See also **security fatigue**.

Confidentiality

A key concept in the CIA Triad, confidentiality is the property that information is only made available or disclosed to authorised individuals, entities or processes.

(Cf. availability and integrity)

Contemporaneous note

A note or notes that are taken at the time of an event or very shortly thereafter, *not* notes that are written after an event, based on recollection.

Content delivery network (CDN)

A globally distributed network of servers that function much like a distributed internet cache. The main purpose of a CDN is to provide high availability and performance by locating content geographically closer to end users.

Continuity of evidence

A written record of how evidence has been handled and by whom between its initial discovery and subsequent analysis.

See also chain of custody (CoC)

Coprime numbers

Also known as relative primes, these are numbers which don’t share any common factors.

Criminal justice

Criminal justice is a general term that refers to the laws, procedures, institutions and policies that exist within a particular jurisdiction and that aim to both control crime and enforce the imposition of penalties for crime.

Critical asset

A subset of assets without which an individual or organisation cannot function.

Cryptanalysis

Shortened from crypto analysis, this is the study of encryption and other cryptographical techniques and solutions.

Cryptanalytic attack

An attack that uses cryptanalysis, that is, attempting to recover plaintext without the knowledge of the key used to produce the ciphertext, which the attacker has access to.

Cryptographic algorithm

A Cryptographic algorithm is used for important tasks such as data encryption, authentication, and digital signatures. It is a well-defined computational procedure that takes variable inputs, such as plain text and a cryptographic key, and produces an output termed as ciphertext. Often, a cryptographic algorithm is referred to as a cipher.

Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)

An algorithm that produces a number that is sufficiently 'random' that it can be used in cryptographic applications. Such generators may rely on an environmentally changing parameter from which they can derive entropy.

Cryptographic key

A key is a numerical value which acts as an input to an encryption or decryption algorithm.

Cryptography

Cryptography is a term used to define a collection of methods for protecting information and communications. Information is encoded to ensure that it is read or processed by only those who it is intended for. Cryptography uses formal mathematical methods to encode and decode information and is used primarily for secure communications. Cryptography provides the means to achieve two components of the CIA triad – Confidentiality and Integrity.

Cryptology

The science of secure communication.

Cryptosystem

Cryptographic system that uses cryptographic methods to secure a system or device.

CVE Numbering Authorities (CNAs)

Trusted organisations, authorised to add information to the Common Vulnerabilities and Exposures (CVE) system.

Cyber Kill Chain®

A methodology developed by Lockheed Martin for identifying and combatting an Advanced Persistent Threat (APT)

Cyber-physical-social system

Extension of the cyber-physical system (CPS), which seamlessly integrates cyber space, physical space and social space**.**

Cyber resilience

A defence strategy that acknowledges cyber security attacks will happen and therefore it is better to develop the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.

Cyber security

The protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

D

Data carving

Data carving is a data recovery procedure which involves locating and extracting fragments of files that have been lost or deleted from unallocated space.

Data Encryption Standard (DES)

A symmetric block cipher with a key length of 546 bits. This is no longer used (deprecated).

Data loss prevention (DLP)

This is a term used to describe a collection of technologies and techniques that examine and identify different types of information that is **at rest** (e.g. in a file on a disk), **in motion** (e.g. a network packet) or **in use** (e.g. data within memory).

Decryption

The process of changing a coded message or coded data (ciphertext) to the original message or data (plaintext).

Default access control policy

A policy allowing or denying access to a resource when no specific access control rule applies to the request for the resource.

Denial Of Service (DoS) attack

An attack which consists of a high level of requests over a network which flood the target machine or network such it can not provide responses or fails entirely.

Dependency confusion attack

This occurs when a software installer script is tricked into pulling a malicious code file from a public repository instead of the intended file of the same name from an internal repository.

Dictionary attack

An attempt to break into a password protected system by systematically attempting entry using a list of well-known words or phrases. The attempt is exhaustive and the attacker could even try using all words in a dictionary, sometimes with additional characters added to the word.

Differential cryptanalysis

Differential cryptanalysis attack involves using pairs of plaintext and corresponding ciphertext to derive a secret key that encrypted them. It uses a set of ciphertext and related plaintext that are encrypted with the same key and attempts to decipher the key.

Differential–linear attack

A differential and a linear attack used together.

Differential SCA

Differential SCA involves monitoring side channel parameters of a device during the process of encryption, using normal power and with power variations. The ‘differences’ in the side channel parameters observed in normal and power varied conditions are statistically analysed to guess the encryption process. In addition to varying power, side channel parameters are monitored by introducing faults as well.

Diffie–Hellman (DH)

A key exchange, mathematical algorithm whereby two people or machines can share a symmetric key remotely.

This algorithm is sometimes referred to as Diffie–Hellman–Merkle, as it was influenced by the work of the US computer scientist Ralph Merkle.

Digital certificate

Proof of ownership of a public key.

Digital Encryption Standard (DES)

An alternative name for Data Encryption Standard (DES).

Digital forensics

A branch of forensic science that centres on the recovery, investigation, examination and analysis of digital data.

Digital forensics may be used following unauthorised access to a system, network or data to support reporting of evidence that may be reliably used in legal proceedings.

Digital Rights Management (DRM)

A method or set of methods used to help protect copyrighted material.

Digital signature

A method of authenticating the authorship of a message.

Discovery

A pre-trial procedure which obliges all parties to disclose case-relevant information, including physical and electronic documents and records.

Discretionary Access Control (DAC)

A widely-used method of access control where entities have discretion to grant or withhold access permissions to objects. Permissions are usually stored in the Access Control List (ACL).

c.f. Mandatory Access Control (MAC)

Document management systems (DMSs)

Systems designed to keep track of document information, such as authors, versions, locations, changes, amongst others.   Document management systems are particularly useful where multiple people are working on documents at the same tie or in close succession.

DomainKeys Identified Mail (DKIM)

An Internet standard which uses digital signatures and hashing to authenticate email headers.

Domain Name System (DNS)

A naming system for networked devices using a decentralised hierarchy of servers. A core function of DNS is to translate human-readable domain names into IP addresses.

E

Edge cloud

A decentralised and distributed approach to processing data, where less resource hungry processing is performed at the edge of a cloud network (ie: on client computers and devices). Examples include IoT devices, such as Amazon’s Echo Dot device or self-driving vehicles.

Electro Magnetic Radiation (EMR)

Electromagnetic radiation (EMR) is a form of energy that is all around us and takes many forms, such as radio waves, microwaves, X-rays and gamma rays. All electronic hardware emits EMR when they operate. It is possible to use equipment to pick up EMR from electronic devices that correlate to hidden signals or data and recreate these signals or data. This forms the basic input of side-channel attacks.

Electronic discovery

See Discovery

Elliptic-Curve Diffie–Hellman (ECDH)

A key exchange, mathematical, algorithm whereby two people or machines can share a symmetric key remotely. In this case the mathematics involves extrapolating from points on a geometric curve – the elliptic curve.

Emanations Security (EMSEC)

Also known as Emissions Security, EMSEC is a collection of measures designed to prevent the means to access/intercept and analyse compromising emanations (EMR, typically) from cryptographic equipment.

Emissions Security (EMSEC)

Also known as Emanations Security, EMSEC is a collection of measures designed to prevent the means to access/intercept and analyse compromising emanations (EMR, typically) from cryptographic equipment.

Employment life cycle

The phases an employee passes through as a result of employment at an organisation. The lifecycle comprises of three main phases: recruitment, active employment, and termination.

Enabling task

Any task required of a user that does not directly result in a product or service.

c.f. **production task**

Encapsulating Security Payload (ESP)

Like Authentication Header (AH) this provides data origin authentication, integrity, and an anti-replay service. In addition, it provides confidentiality in the form of encryption. The integrity protection is optional. Unlike AH, ESP only provides authentication for the payload.

Encryption

A method for obfuscating a message or data so that it can only be read by the intended recipient.

Encryption key

A ‘key’ is a piece of information used in combination with an algorithm (a 'cipher') to transform plaintext into ciphertext. A key is a string of bits and of a specific size, depending upon the cipher.

Endpoint security

Security measures taken to secure end devices and nodes attached to a network.

Enforced TLS

A feature of the STARTTLS ESMTP service extension where servers require email clients send and receive email messages over a secure channel.#

See also: ESMTP, STARTTLS, services extension.

c.f. Opportunistic TLS.

Entity

Any user (human or otherwise) that requests access to, and uses resources of, a system.

Euler’s totient function

A mathematical operation which has as it’s output the number of coprime numbers a given number will have (the ones that are smaller than itself). Euler is pronounced 'oiler'.

Exclusive-OR function

Exclusive-OR, often abbreviated to XOR (and sometimes EOR), is a mathematical operation equivalent to binary addition without carry. It compares two input bits and generates one output bit. If the bits are the same, the result is 0. If the bits are different, the result is 1. It therefore preserves randomness. XOR is used in cryptography since it allows easily encryption and decryption of a string, which the other logic operations don't.

Exif data

EXIF (Exchangeable Image File Format) is a standard that defines specific information about an image or other media that is stored within the content of a digital file.

Expert witness

A professional person whose training and experience, in the opinion of a court of law, supports the claim to be an expert.

Extended SMTP (ESMTP)

A modernisation of SMTP formulated in 1995 to reflect changing email usage including the straightforward sending and receipt of pictures, audio and video; as well as support for services extensions that provide authentication of senders.

See also: Simple Mail Transfer Protocol, services extensions.

F

Fabrication

The action or process of manufacturing or inventing something. In cyber security, it refers to fabricating messages when masquerading as a sender or receiver.

Factor

Any credential supplied to authenticate an identity.

Fault Attack (FA)

Induce faults in a cryptographic circuit, typically voltage, clock glitches, varying the temperature around the device, vibration, infrared light, and wrong input data so that it behaves abnormally and/or delivers incorrect results. These results could reveal some information about the secret key.

Fear, Uncertainty and Doubt (FUD)

A technique widely used in public relations, politics and cyber security sales which aims to influence decision-making through negative messaging describing the frequency of severity of threats or by raising questions over the effectiveness of existing security measures.

File Allocation Table (FAT)

1. A file system developed for personal computers, most notably used by the MS-DOS operating system developed for the original IBM PC. The file system uses an index table (known as the File Allocation Table) to locate data held on individual disks.
2. An index table used by MS-DOS and early versions of Microsoft Window containing a list of clusters where data is stored on a disk.

File extension

A suffix appended at the end of a filename that indicates what type of file it is.

File signature

A unique identifier that specifies what the data content of a digital file is.

File system

A data structure created by operating systems to organise computer files and folders.

Firmware

Sometimes equated with BIOS but sometimes thought of as the hardware read-only memory that holds BIOS to boot a machine. There are also firmware instances such as in network and video cards. There are other types of programme which are stored in firmware for other types of device.

Forensically sound

To be forensically sound, evidence needs to be reliable. Persons gathering or processing evidence must be able to show that items produced in evidence have not altered or been changed in any way.

Forensic Readiness

Planning for data breaches and cybersecurity attacks before they occur with the aim of preserving any inquiry relevant digital data and maintaining business continuity.

Forensic science

The application of scientific methods and techniques to matters under investigation in criminal or civil proceedings.

Frequency analysis

Frequency analysis is the study of the count and distribution of the letters in a text, typically the ciphertext. Analysing the frequencies helps in cryptanalysis for decrypting substitution-based ciphers.

Freshness

A measure of how recent a message or portion of data is.

G

General Data Protection Regulation (GDPR)

A legal framework drafted and passed by the European Union (EU) that came into effect in 2018. This privacy and security law sets out what personal information can be collected from individuals living in the EU and regulates how this data can be processed or stored. The regulation applies regardless of where a company is based and a violation of privacy and security standards carries substantial penalties.

H

Hash digest

The output of a hash function ─ e.g., hash(data) = digest. Also known as a message digest, digest or harsh value.

Hashing

The operation of taking a long input and creating a short mathematical value which is (almost) unique to that input.

Heartbleed vulnerability

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This vulnerability enables compromise of information encrypted by the SSL/TLS encryption algorithm that is used to secure the Internet.

Host layer

The hardware of the computing device (computer) that hosts the operating system and applications.

Human factors

A specialisation within cyber security concerned with the interaction of humans and security technologies.

Hybrid cryptosystem

A cryptosystem that uses asymmetrical and symmetrical encryption methods.

Hypervisor-based operating system

A hypervisor manages Virtual Machines (VM) and other virtual resources (networks, routers, security rules, IP addresses). Also ensuring a user has permission to start and run a particular VM and supporting access, pause and termination of VMs. A hypervisor may also perform an accounting function over the usage of resources.

I

Identity

A unique characteristic of an entity that distinguishes it to a system.

Identity and Access Management (IAM or IdAM)

Processes ensuring entities have appropriate access to resources — including identification, authentication and authorisation.

Also known as Identity Management (IM or IdM)

Identity Management (IM or IdM)

Processes ensuring entities have appropriate access to resources — including identification, authentication and authorisation.

Also known as Identity and Access Management (IAM or IdAM)

Impact

The consequences, or effects of a cyber security incident.

Implementation attack

A threat to cryptographic devices, aiming at recovering secret data exploiting implementation inherent characteristics.

Incident

A security event resulting in the potential disclosure of an asset.

(Cf. breach)

Incident management

A process spans the entire life cycle of an incident. Typical activities that take place during this process include liaising with incident response teams and external stakeholders, such as senior managers, news media, lawyers and regulatory authorities.

Incident response

A process that focuses upon detecting, reporting, assessing, responding, dealing with and learning from incidents.

Information classification

The practice of protecting sensitive information by marking it to one of several hierarchical levels of sensitivity.

Information classification policies

Policies concerned with ensuring that sensitive information is secured in appropriate manners.

Information collection

One of the four types of harmful activities described by Solove in his taxonomy of privacy. It collectively describes the practice gathering data through techniques such as surveillance and interrogation.

Information dissemination

One of the four types of harmful activities described by Solove in his taxonomy of privacy. It collectively describes the practice of propagating information through actions such as disclosure, blackmail, and breaches of confidentiality.

Information handling

Rules and guidelines that describe how information should be processed, communicated, stored and destroyed (if required).

Information processing

(a) In a general context, this refers to the act of performing routine actions on information, such as removing duplicates from a dataset.

(b) In a security context, this is one of the four types of harmful activities described by Solove in his taxonomy of privacy. It collectively describes the practice of performing harmful actions on information, such as aggregation where more complete information about an individual can be determined by combining information from multiple sources.

Information system

Information system (IS) is a term used to denote a set of computing equipment that are used to process, generate, exchange, and store information. Such equipment is typically interconnected by means of a data network.

Information technology

The various technologies used in an information system that comprise both hardware and software technologies are collectively termed as Information Technology (IT). Another common term used in the context, which is generic, is Information and Communication Technology (ICT). These terms are often used synonymously in literature.

Initialisation Vector (IV)

A value required in the generation of a block or stream cipher. This value should not be easily predicted.

Insider threat

A threat to a system coming from within an organisation (such as a careless or malicious employee).

(See also Unintentional Insider Threat)

Intangible asset

A type of asset that cannot be touched or experienced. Examples including intellectual property and reputation.

(Cf. tangible asset)

Integrity

A key concept in the CIA Triad, integrity is the property of safeguarding the accuracy and completeness of assets against unauthorised access or modification.

(Cf. Availability and Confidentiality)

Interception

Receiving electronic transmissions before they reach the intended recipient.

Interface

A common point through which two systems, communications layers, etc. interact.

Internet of Things (IoT)

Physical devices which communicate across a network often used for sensing and recording.

Internet Protocol Security (IPsec)

A system used to protect data on a virtual private network.

Inter-Process Communication (IPC)

This is a mechanism, managed by the operating system to ensure security, whereby two or more processes are allowed to communicate, for example to provide notice of an event or to pass data.

Interruption

To stop or hinder communications by breaking into an ongoing communication.

Invasions

One of the four types of harmful activities described by Solove in his taxonomy of privacy. It collectively describes the practice intruding upon the privacy of an individual through actions such as intrusion or interfering with their freedom to make decisions.

K

Kerckhoffs' Principle

The principle that the mathematics behind a cryptographical system should be public rather than kept secret. The idea is that the security of the data depends on the security of the key and the robustness of the mathematical algorithm.

Kernel

This component is the core of an operating system (OS) which manages the lower level tasks of the OS such as memory management, disc access and task scheduling.

Key Derivation Function (KDF)

A key derivation function is used to generate one or more cryptographic keys from a private (secret) input value.

Key space

A key space, or keyspace, is the set of all valid, possible, distinct keys of a cryptosystem. Simply put, it is the total number of possible values of keys in a cryptographic algorithm. For example, a 32-bit key would have a key space of 4,294,967,296.

Known plaintext attack (KPA)

An attacker has access to the ciphertext and its corresponding plaintext. The objective is to guess the secret key or to engineer a cipher which would decrypt any ciphertext in that system.

L

Latent evidence

Evidence that has to be processed from other data before it becomes apparent (e.g. fingerprints).

Least privilege

The practice of giving a user account or automated process the minimum rights (privileges) necessary for it to perform its intended purpose.

Legacy system

Old software, hardware or methods that are still in use despite newer alternatives being available. It may be used pejoratively suggesting the system is out-of-date or requires replacement.

Likelihood

A measure of the possibility that a threat will successfully exploit a vulnerability to produce an undesirable outcome.

Linear cryptanalysis

Cryptanalysis based on finding related approximations to the action of a cipher. The probabilistic linear relations (called linear approximations) between parity bits of the plaintext, the ciphertext, and the secret key are studied in the process of guessing the different bits of the secret key.

Locard’s principle

A concept formulated by the French criminologist Edmund Locard in the nineteenth century. Locard held that it was impossible for a person to commit a criminal act without leaving some trace of their presence at the scene.

Log

A record (such as a file or database) of events within a system (e.g. log-in attempts, network connections, reboots and crashes).

Logical image

A logical image contains all data that is visible to the file system of the device concerned. Deleted files and fragments will not normally be captured using this imaging method.

Logical topology

Defines the logistical elements of a network such as the transfer of data and methods of communication, regardless of physical location.

M

Malware

Intrusive software that is designed to cause damage or take control of a computer or network. This software usually is unintentionally given access or downloaded to a machine.

Mandatory Access Control (MAC)

Access to resources is strictly controlled by the operating system (OS) as specified by the system administrator. This control is strict and does not observe role, like Role-based Access Control (RBAC), or user discretion, like Discretionary Access Control (DAC).

Man-in-the-middle (MITM) attack

A man-in-the-middle (MITM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify the information being exchanged between the two parties.

Master Boot Record (MBR)

A Master Boot Record (MBR) consists of a program and information stored on the first sector of a main hard disk that identifies how and where the operating system is located so that it can be loaded into the computer's memory. It also includes information about disc partitions.

Master File Table (MFT)

A table that stores information about, and data for, every file on a Microsoft Windows NT-based operating system. MFT is a replacement for the older FAT.

See also: File Allocation Table.

Meet-in-the-middle attack (MitM)

Meet-in-the-middle is a known plaintext attack that can greatly reduce the number of brute-force permutations required to decrypt text that has been encrypted by more than one key. This attack targets the cryptographic function and brute force technique is applied to both plaintext and ciphertext block.

Metadata

Data that describes other data. For example, metadata contained in a picture file will typically describe how large the picture is and the date and time that it was created, as well as other information.

MITRE ATT&CK ®

A model for describing attacks in which the attacker’s goals are divided into twelve tactics, each of which contains several techniques for achieving that goal.

Also known as Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

Modification

Making changes, without being permitted to or without authorisation, in the case of an attack.

Modulo division

A mathematical operation in which one number is divided by another to leave a remainder. The remainder is the output of the operation.

Mono-alphabetic substitution cipher

A substitution cipher using a single alphabet. Eg: Caesar Cipher

Monolithic operating system

This operating system model separates breaks the system down into several trust zones, a central kernel and user applications which are managed by the kernel.

Multi-Factor Authentication (MFA)

Any form of authentication requiring an entity to successfully present more than one authentication factor before being granted access.

Multi-server operating system

This operating system model breaks the system down into components such as applications, file store, networking, drivers, etc and provides each with a trust boundary, connected using inter-process communication and accessed with authentication.

Multi-step authentication

A form of Multi-Factor Authentication (MFA) where authentication factors are requested and evaluated in sequence.

N

Network layer

The Layer 3 in the seven-layer networking protocols stack, the Open Systems Interconnection (ISO) reference model, which deals with routing packets across a network. Routing protocols determine the type of routing strategy deployed. In the context of the TCP/IP protocol stack, the IP layer performs the network layer functions.

New Technology File System (NTFS)

NTFS is a file system developed by Microsoft for its Windows software and introduced in 1993 in order to improve operating system functionality for the storage, organisation and retrieval of files on digital media.

Next-Generation Encryption (NGE)

An encryption system which is expected to be viable for the next 30 years.

NIS Regulations

The **NIS Regulations** ensure that all critical infrastructure organisations, such as telecommunication operators and transport and energy providers, are now required by law to demonstrate they have appropriate processes and capabilities before an incident occurs.

Nonce

An arbitrary mathematical value which is used in various cryptographical algorithms.

Non-repudiation

In general, *non-repudiation* is agreeing to adhere to an obligation. In the context of cyber security, it refers to a property that a sender of a message cannot deny that the message was originated by them.

O

Open mail relay

An email server using SMTP that transfers messages to other servers without requiring any form of authentication. Early email servers were all open mail relays, but their use by email spammers has meant that open relays are now usually due to configuration errors.

OpenSSL Heartbleed

A flaw that was exposed in the OpenSSL cryptographic software, whereby attack victims (systems) could be tricked into revealing sensitive information.

Operating system (OS)

An operating system is a collection of software programs that provide an interface to use the computer. The programs manage the computer system's components (storage drives, memory, processing, etc.) and peripherals (displays, printers, audio, etc.).

Opinion evidence

Verbal or written testimony given by a professional e.g. a medical doctor, who is accepted by a court as being an expert in their field, based on their opinion.

Opportunistic TLS

A feature of the STARTTLS ESMTP service extension where an email client requests that a server enters into a secure session for the exchange of email.

See also: ESMTP, STARTTLS, services extension.

c.f. Enforced TLS.

Organisational vulnerability

A weakness in the operation of a system caused by people, or shortcomings in procedures and processes involved in data handling.

(See also technological vulnerability, vulnerability and window of vulnerability)

Out-Of-Band Authentication (OOBA)

An authentication process where some or all of the authentication factors are exchanged using a different communication channel (e.g. SMS).

P

Packet-sniffing

The act of monitoring network traffic on wired or wireless networks to capture packets, using software and/or specialised hardware.

Parity bits

A parity check is the process that ensures accurate data transmission during communication. A parity bit is appended to the original data bits to create an even or odd number of bits of a value 0 or 1, typically, value 1.

Passive attack

An attempt to learn, understand or make use of information without directly impacting the state of a system resource**.**

(Cf. attack, active attack)

P-box

An algorithm used in encryption which involves the permutation of data according to a strict rule.

Penetration testing

A collection of cyber security processes for testing a computer system, or users of a system, in order to identify vulnerabilities.

Also known as pentesting.

Pentesting

A collection of cyber security processes for testing a computer system, or users of a system, in order to identify vulnerabilities.

Also known as penetration testing

Permissions

A type of access control granting entities the right to read, write or execute objects. Permissions are usually stored in Access Control List (ACL).

This term is most often associated with Discretionary Access Control (DAC).

Persistent data

Data that is stored on a storage device (e.g. a hard drive).

Physical evidence

Case-relevant documents or other tangible evidence that can be observed and measured. Sometimes also called *real evidence*.

Physical image

A physical image is a bit-for-bit replica of all the data contained on a digital device. Making a physical image will capture all live and deleted data.

Physical topology

The actual physical arrangement and layout of devices on a network (PCs, cabling, networking equipment, etc.).

Plaintext

A message or data which is to be encrypted.

Plan-Do-Check-Act (PDCA) cycle

An iterative approach to managing continuous improvement through change. The method is designed to be cyclic with no end.

Policy Administration Point (PAP)

This component keeps track of the set of Policy Decision Points (PDPs) and the deployment of policies across groups of PDPs.

Policy Decision Point (PDP)

This component makes decisions, according to a policy deployed by the Policy Administration Point (PAP), as to whether a request for some resource(s) should be allowed or denied.

Policy Enforcement Point (PEP)

This component implements the decision made by a Policy Decision Point (PDP) and provides a response either accepting or rejecting a request for a resource.

Policy Information Point (PIP)

This component is responsible for providing additional information to a PDP to support the decision-making process. The information typically concerns policies and contextual information (user role, etc.).

Poly-alphabetic substitution cipher

A substitution cipher using a multiple substitution alphabets. Eg: Vigenère cipher

Positive security

An approach to developing security cultures that encourages stakeholders to consider the benefits of behaving in a secure manner rather than concentrating on the negative consequences caused by security threats, and where security incidents are treated as opportunities for learning rather than for blaming individuals.

Pretty Good Privacy (PGP)

A system for exchanging messages in which users have the access to the public keys of those to whom they wish to send messages. Trust in keys is established through a web of trust.

Probing Attack (PA)

An invasive attack that directly accesses the internal wires and connections of a targeted device to extract/tap sensitive information. It is an invasive method to observe the physical silicon implementation of a chip or an on-board device.

Production task

A task performed by a user which results in the production of a product or service.

c.f **enabling task**

Public key

A person’s public key in an asymmetrical cryptography system is available to anyone. It is related to the person’s private key but neither can be easily derived from the other.

Public Key Infrastructure (PKI)

A system whereby public keys can be authenticated and distributed by a trusted institution.

R

Rainbow attack

A rainbow attack or a *rainbow table attack* involves the use of a rainbow hash table to guess the passwords stored in a database system. A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes.

Real evidence

Case-relevant documents or other tangible evidence that can be observed and measured.

See Physical evidence.

Record management systems (RMSs)

A system that controls the creation, storage, retrieval, dissemination and disposal of records created or received by an organisation in the course of its business.

Reference monitor

This component enforces access control rules specified to control access to resources and actions. It ensures rule priorities are followed and if no rule applies a default is applied.

Related-key attack

Any form of cryptanalysis where the attacker can observe the operation of a cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the attacker.

Relaxed model

A relaxed model involves the use of mathematical functions and like in a Chosen Ciphertext Attack (CCA), some preliminary guesses of a key are known in advance.

Render

In this module, the term ‘render’ refers to how a computer OS displays a digital file to the user.

Replay

An occurrence which closely follows the pattern of a previous event. In the context of cyber security, it signifies an attack in which the attacker is able to replay previously captured messages (between a legitimate sender and a receiver) to masquerade as that sender to the receiver.

Replay attack

An attack on a communication session in which an intruder repeats or replays a message that they had previously recorded (but not necessarily understood).

Reverse engineering

A term used to describe using the output of a device or system to work out how the device or system works.

Reverse Engineering Attack (REA)

Reverse engineering attack involves analysing a hardware, software, or a hybrid implementation of a cryptographic algorithm, which is unknown to the attacker and to discover its function.

Rijndael

A family of ciphers with different key and block sizes. Rijndael is the original name of the Advanced Encryption Standard (AES).

Risk

The potential negative effects of achieving an objective caused by uncertainties.

Risk management

Processes for identifying risks within an organisation and developing processes to avoid the risks entirely or to minimise their impact.

(Also see risk)

Rivest Cipher (RC) series

A series or set of symmetric encryption methods invented by Ron Rivest.

Rivest–Shamir–Adleman (RSA)

An asymmetric encryption method named after its three inventors: Ronald Rivest, Adi Shamir and Leonard Adleman.

Role-Based Access Control (RBAC)

A form of access control where users are assigned to roles. Objects in the system can only be accessed by users with the appropriate roles.

Root

The default most privileged user account with access to all resources including all user accounts, files and configuration settings.

Root directory

The root directory is the first or top level directory in a hierarchical file system. All other directories and subdirectories, plus any associated files, are contained within it

Rubber hose attack

Rubber hose attack is extracting secrets from people by use of torture or coercion. Other means are governmental and corporate influence over other sub-entities.

S

Salsa20

A symmetric stream encryption method.

Salt

Salt is a unique, random string of characters known only to the process generating the hash of a plaintext such as a password. Typically, this ‘salt’ is placed in front of the plaintext or each password. The same salt has to be used when verifying the hash of an input string from the user, as in the case of a password, during authentication.

Saltzer and Schroeder Principles

A collection of good practice principles proposed by Jerome Saltzer and Michael Schroeder in their 1975 article, The Protection of Information in Computer Systems. The principles are designed to improve the protection of information through a series of policies on how information is stored and accessed. The principles include concepts, such as 'fail-safe defaults’, which promotes the idea that access to resources (such as a directory) should be based upon the initial assumption that no access is authorised. To gain access, explicit permission must be authorised.

Sanitisation

Processes for destroying data held on storage devices after they are no longer needed. Sanitisation may erase data on media beyond the point where it can be reasonably recovered – in which case the device can be reused, or it may involve the physical destruction of the device itself.

S-box

An algorithm used in encryption which involves the substitution of data according to a strict rule.

Search space

A search space is the set of all values that must be searched in order to find the one you want.

Secure by Default

An approach to the design of hardware, software and services promoted by the UK NCSA based on a few fundamental principles. Secure by Default encourages developers to consider the fundamental causes of security vulnerabilities and to resolve those issues using known security techniques.

See also. Secure by Design.

Secure by Design

A software and design principle that security is designed into a project from its inception and is based on well-founded and understood security concepts; rather than security features being added later or security being reimplemented when there are existing security solutions.

See also. Secure by Default.

Secure Hash Algorithm (SHA-1)

A method for generating a hash – now deprecated (out of date).

Secure Shell (SSH)

A technique used for securing any network service and typically used for remote command-line, login, and remote command execution.

Secure Sockets Layer (SSL)

An encryption-based internet security protocol used on https sites – now largely replaced by TLS.

Security awareness

The lowest level of security learning which aims to persuade users that it is in their interests to engage with security.

Security champion

A role within an organisation responsible for facilitating communications between security professionals and end users. Champions convey and explain policies to end users and solicit information from those users which is fed back to the security team.

Security control

Any safeguard or countermeasure used to protect the confidentiality, integrity or availability of data or infrastructure against risk.

Security education

The highest level of security learning where users acquire specialised cyber security skills with the intention of becoming a cyber security professional.

Security event

Any observable event (malicious or benign), such as a user connecting to a network share, an employee opening a door using a Radio-Frequency Identification (RFID) card, or a website being taken offline.

Security fatigue

Security fatigue is an example of **compliance fatigue**.

Security hardening

The use of various methods to make a system less vulnerable to attack.

Security Operations Centre (SOC)

A facility comprised of a people, processes, and technologies whose main function is to oversee the detection of and response to threats, increase the resilience or an organisation, and identify and address criminal or negligent behaviour.

Security Parameter Index (SPI)

Part of the Authentication Header (AH) or Encapsulating Security Payload (ESP) this contains information about security associations.

Security training

The process of acquiring new skills in order to behave in secure manner.

Seed

A seed is a random sequence or number used to initialise, or help initialise, a function.

Sender Policy Framework (SPF)

A form of email authentication. SPF checks if the IP address of a server in an email envelope’s sender field has been authorised to send mail by the administrator for that domain. If the IP address is not valid, the email is rejected as spam.

See also: Domain Name System, ESMTP, services extension.

Separation of privilege principle

One of the Saltzer and Schroeder Principles. The principle states that wherever possible, multiple conditions should be met in order for an action to be successful. An example of this would be the need for authorisation from two signatories to allow an employee to have access to a restricted area.

Server hardening

A process applied to a server with many facets which involves actions to make data, hardware, applications and accounts as secure as possible using configuration, firmware, hardware and segregation as well as intrusion detection and logging.

Services extensions

Additional features supported by SMTP that are not part of the core protocol. Individual servers can be configured to support a range of features including non-alphabetic email addresses and a range of anti-spoofing and security features.

See also: Extended SMTP.

Session key

A symmetric key used to encrypt information during a single communications session. To be discarded after the session is over.

Shadow security

A process by which users develop and implement their own security policies to replace institutional policies that they find unduly burdensome, inappropriate or ineffective.

Side-Channel Attack (SCA)

Side channel attacks monitor patterns in the information exhaust that computers constantly give off as EMR – the electric emissions from a computer's monitor or hard drive. The emissions vary depending on what information is being processed, what is displayed on the screen or being read by the drive's magnetic head.

Signature

The information that defines the footprint of a virus.

Simple Mail Transfer Protocol (SMTP)

The dominant protocol used to send and receive Internet email. Original SMTP has largely been replaced by the more modern Extended SMTP however, the term ‘SMTP’ is still widely used in the literature.

See also: ESMTP.

Simple SCA

Simple SCA involves an attacker directly measuring the electromagnetic activity. For these attacks to succeed, attackers require to have a complete understanding of the targeted algorithm and its implementation.

Single-Factor Authentication (SFA)

Any form of authentication where an entity only needs to present one authentication factor before being granted access.

(Cf. Multi-Factor Authentication (MFA))

Single Sign-On (SSO)

With an SSO the system uses an Multi-Factor Authentication (MFA) mechanism to check the identity of the user once, then grants them a special token that can be used instead of a password to authenticate themselves to other services provided by the organisation.

Slack space

Slack space is any area of data storage which remains between the end of a file and the end of the disk cluster it is stored in.

SMTP AUTH (SMTP authentication)

A security service extension supported by ESMTP that authenticates message envelopes by requiring users to authenticate themselves with an email server.

See also: ESTMP.

Social engineering

A range of human factor attack techniques aiming to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes or to obtain access to a computer system.

Social engineering attack

A method used by a hacker to obtain information by deceiving a person that will allow them to gain access to a system.

Socio-technical system

Socio-technical systems bring communities of humans together with technology. Typical examples are social online networks such as Facebook and LinkedIn.

Software-optimised encryption algorithm (SEAL)

A stream cipher (encrypts one bit or one byte at a time).

Spoken evidence

Evidence given verbally, usually in a courtroom setting, by witnesses of an event. Sometimes also called testimonial evidence.

SQL Injection attack

A technique whereby malicious SQL statements are sent to a server, typically by inserting commands into fields normally used to accept data as part of the query.

Stakeholder engagement

Any process in which an organisation communicates with all of its stakeholders in order to develop and achieve agreed outcomes.

Standard Operating Procedure (SOP)

A set of step-by-step instructions specific to an organisation to assist employees to perform routine or emergency processes. The main benefit of SOPs is their focus on efficiency, quality output and consistency of performance. SOPs also benefit from reducing miscommunication and helping to spot any non-compliance with industry regulations.

STARTTLS

A service extension for ESMTP that allows messages to be securely exchanged using the Transport Layer Security protocol.

See also: ESMTP, services extension, Transport Layer Security.

Steganography

The study of hiding information inside other information – often in a picture or audio file.

Stream cipher

A symmetric method of encryption where bits are encrypted one at a time. Used for streaming audio or video.

Substitution cipher

Substitution ciphers encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol as directed by the key (e.g., a Caesar Cipher).

Symmetric cryptography

An encryption method in which the sender and receiver share the same key.

System

A set of things working together as parts of a mechanism or a platform with an interconnection between its components, with a goal of providing services.

System hardening

Sometimes taken as synonymous with server hardening but often take to be encompassing further components such as networking, routers, backup devices, etc.

Systems security

Process that captures and refines security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.

T

Tangible asset

Any type of asset that can be seen, handled or experienced – including buildings, hardware and software.

(Cf. intangible asset)

Targeted attack

An attack aimed at a specific organisation, in which the attacker(s) posing the threat(s) has interests

(Cf. untargeted attack)

Technological vulnerability

A weakness in the design, implementation or configuration of hardware or software.

(See also vulnerability. Cf. organisational vulnerability)

Tenant

A cloud technology term used to denote a single user account or project account which is managed by the hypervisor which insures appropriate use of resources and that the account is kept secure and isolated from others.

Testimonial evidence

Evidence given verbally, usually in a courtroom setting, by witnesses of an event.

See spoken evidence

Threat

A potential cause of damage to an asset utilising a vulnerability.

Transient Electromagnetic Pulse Emanation Standard (TEMPEST)

TEMPEST is a set of standards and countermeasures that was set up by the US Government to protect classified intelligence from being intercepted via spurious electromagnetic emissions from telecommunications equipment such as computers, scanners, and any device that uses a transistor or a microchip.

Transmission Control Protocol (TCP)

A communications protocol which primary function is to transport data segments. It resides as layer four in the seven-layer networking protocols stack, the Open Systems Interconnection (ISO) reference model.

Transport Layer Security (TLS)

An encryption-based internet security protocol used on https sites. This has replaced SSL. It is also used on in email, instant messaging, and voice over IP.

Triple Data Encryption Algorithm (TDEA)

Also known as 3DES, TDEA is a cipher suite based on the DES that was introduced during the transition between the DES and the AES.

Trust boundary

A security measure which limits access to some system component, hardware or software, to those who can authorise for such access.

Two-Factor Authentication (2FA)

A form of Multi-Factor Authentication (MFA) requiring two different authentication factors.

U

Unallocated space

Unallocated space is space that has not been allocated to ‘live’ or active files on digital media.

Unified Extensible Firmware Interface (UEFI)

Similar to Basic Input-Output System (BIOS) but with extended capabilities where initialisation information is stored in a file such that it can be updated more easily, larger discs can be supported and booting is faster and more secure.

Unintentional Insider Threat (UIT)

A type of insider threat to an organisation inadvertently created by an authorised user through negligence or ignorance, such as responding to a phishing email.

Untargeted attack

An indiscriminate attack on organisations.

(Cf. targeted attack)

Usability

Measures used to assess the ease of use of technology.

V

Virtual Private Network (VPN)

A secure connection between two devices over a network in which the IP address is hidden and the data is encrypted.

Volatile data

Any data that is stored in the memory of an active device or data that exists in transit.

Volume Boot Record

The Volume Boot Record or sector is typically the first sector of a partition. It defines the file system and records information about how the volume is set up in terms of how many bytes there are in a sector and how many sectors there are in a cluster.

Vulnerability

A weakness in an asset, (or group of assets), or a weakness in the security of a system, that can be exploited by a threat.

(See also technological vulnerability, organisational vulnerability and window of vulnerability)

W

Web of trust

An arrangement of people or machines where there is a relationship of trust such that encryption keys can be authenticated.

Whitelist

This is a list of entities that are known to be benign and therefore to be approved for use in an organisation or network.

Window of vulnerability

The interval between the moment a technological vulnerability is exploited by attackers and the time the vulnerability is eliminated.

Wired Equivalent Privacy (WEP)

An encryption a protocol developed for Wi-Fi – now deprecated (out of date) and replaced by WPA (Wi-Fi Protected Access).

Write blocker

A write blocker can be either a physical device or a piece of software that can be downloaded onto a computer. The purpose of both is the same: to stop the read/write process that normally occurs automatically when a digital device is connected to a computer or some other device.

X

XOR

XOR (exclusive-OR) is a mathematical operation equivalent to binary addition without carry. It compares two input bits and generates one output bit. If the bits are the same, the result is 0. If the bits are different, the result is 1. It therefore preserves randomness. XOR is used in cryptography since it allows easily encryption and decryption of a string, which the other logic operations don't.

Z

Zero day

A vulnerability in an application that is unknown to its authors but that has been discovered by hostile actors.