Definitions

Authentication: The process of assuring that the communicating entity, or origin of a piece of information, is the one that it claims to be.

Authenticity: The condition of being assured by supporting evidence that the entity is the one it claims to be (aka authentic).

Availability: To ensure that assets can be used/accessed by any authorized parties and prevent unauthorized withholding of information or resources.

Backdoor: A covert method of bypassing normal authentication.

Black hat: A hacker who violates computer security for personal gain or maliciousness.

Bot (Zombie): A compromised machine

Botnet (Zombie army): A large collection of connected bots, communicating via covert channels.

CAPTCHA: A computer program used to differentiate man from machine. Used to stop spam/automated extraction of data from websites.

Cipher: Encryption Scheme

Clickjacking: Attacker places a transparent layer above a legitimate link so user will click on the transparent layer instead of the hyperlink.

Click Fraud: A program/script that imitates legitimate users and click on advertisements links without any interest. Advertisers will pay webpage owner depending on the number of clicks the advert garners on the website.

Common Vulnerabilities and Exposure (CVE): A reference method for publicly known information security vulnerabilities and exposures.

Confidentiality: To ensure that assets are only viewed by the authorized parties and protect from unauthorized disclosure of information.

Covert Channel: A channel intentionally created to transfer information between processes that are not supposed to allow communication by security policy. Intended for leaking info.

Drive-by Download: Any downloads without user's knowledge (Virus/Malware) OR authorize by user without understanding the consequence (Counterfeit software)

Easter Eggs: Easter eggs are secret responses that occur as a result of an undocumented set of commands.

Exploit: A software/command that make use of vulnerabilities to cause unintended/unanticipated behaviour.

Hardening: The process of securing a system by reducing the surface area of vulnerabilities.

Integrity: To ensure that assets is only modified by the authorized parties and protect from unauthorized modification of information/process.

Logic Bomb: A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Side Channel: An unintentional channel/vulnerability of a computer system that has been taken advantaged by attacker to find out more about target system.

Sniffing: The process of intercepting and logging/monitoring traffic that passes over a network using a packet sniffer.

Spoofing: The act of imitating an entity, usually for malicious purpose.

Threat: A set of circumstances that has the potential to cause loss or harm

Vulnerability: A weakness in the system.

Web bug: A file object used to monitor user's usage pattern. Just like a electronic bug device.

White hat: An ethical computer hacker, or a computer security expert, who specializes in penetration testing and in other testing methodologies that ensures the security of an organization's information systems

Zero-day Vulnerability: A vulnerability that is unknown/unreported/unaddressed by the developers or vendors (Zero day of protection, thus known as zero-day vulnerability)

Authenticity

Entity authentication: To check if **the parties on both ends are authentic** by using password, challenge and response mechanism.

Data origin authentication: To check if **the origin of a piece of information is authentic** using message authentication code (MAC) or digital signature.

General Cryptography

Asymmetric key Cryptosystem: Different, but related, keys are used in for encryption and decryption.

Block Cipher: A deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key.

Confusion: Attacker **should not be able to predict** what will happen to ciphertext when **one character in plaintext is changed**. Input must **undergo complex transformation** during encryption (aka Complex functional relationship between plaintext-key pair and ciphertext).

Control (Countermeasure, Security Mechanism): A way to counter threats

Cryptology: Cryptography + Cryptanalysis

Cryptography: The practice and study of techniques for **securing communication** in the presence of **adversaries**

Cryptanalysis: The study of **analysing information systems** in order to **study the hidden aspects** of the systems. Cryptanalysis is used to **breach cryptographic security systems** and **gain access to the contents of encrypted messages**, even if the cryptographic key is unknown.

Cryptography backdoor: A method, often secret, of bypassing normal encryption in a cryptosystem. Allows intruder to access the plaintext without having correct user credentials.

Decryption Order: An order to force suspects to decrypt their encrypted data or give up their key.

Diffusion: A **change in plaintext** will affect **many parts of the ciphertext**. Information from plaintext is **spread over entire ciphertext** and **transformation depends equally across all bits** of input. Attacker must access much of ciphertext to infer encryption algorithm.

Key escrow: An arrangement(agreement) in which the keys needed to decrypt encrypted data are held in escrow so that under certain circumstances, an authorized third party may gain access to those keys.

Key space: A set of all possible keys

Key space size: The total number of possible keys.

Key size/length: Number of bits required to represent a key. **Log_2(space size)**

Pretty Good Privacy (PGP): A public key encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

(Internet) Privacy: The right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Can entail personally identifying information (PII, eg. Age, physical address) or non-PII information such as surfing behaviour that can be used to identify an individual without explicitly disclosing their name. Compromised when such data was not intended to be shared.

Stream Cipher: A symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream).

Symmetric key Cryptosystem: Same key is used in both encryption and decryption.

Public Key Distribution

Certificate Trust List (CTL): A predefined list of items signed by a trusted entity.

Common Vulnerabilities and Exposures (CVE): A system that provides a reference method for publicly known information security vulnerabilities and exposures.

Nonce: An arbitrary number that can be used just once in a cryptographic communication

Mechanisms

Authenticated encryption (AE)/Authenticated encryption with associated data (AEAD): Forms of encryption which simultaneously assure the confidentiality and authenticity of data.

End-to-end encryption: A method intended to prevent data from being read or secretly modified along the path of transmission. Messages are encrypted by the sender and only decrypted by the receiver. Intermediaries have no means of decryption.

Graphical password: A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). Sometimes also called graphical user authentication (GUA).

Hardware random number generator (HRNG)/
True random number generator (TRNG): A device that generates random numbers from a physical process, rather than algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect, involving a beam splitter, and other quantum phenomena.

Iris scanning: An automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance.

Port Scanning: The process of determining which ports are open on hosts in a network.

Pseudorandom number generator: An arithmetic method of producing random digit.

Quantum random number generator: The random numbers are generated in real-time by measuring the quantum fluctuations of the vacuum.

Retinal Scanning: Due to the complex structure of the capillaries that supply the retina with blood, each person's retina is unique.

Security Information and Event Management (SIEM): Provides real-time analysis of security alerts generated by network hardware and applications

Security Operations Center (SOC): A centralized unit in an organization that monitors the IT systems and deals with security issues.

Single sign-on: A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to any of several related systems.

Attacks

Ciphertext Only Attack: An attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

Exhaustive Search (Brute force): An attack to exhaustively search all possible keys.

Known Plaintext Attack: An attack model for cryptanalysis where the attacker has access to both the plaintext, and its encrypted version.

Pharming: The act of directing users to a bogus website that mimics the appearance of a legitimate one in order to obtain personal information such as passwords/account numbers.

Phishing: Attacker **imitates authorities and ask for password** under some false pretence to **trick user to voluntarily send their password** to the attacker. Typically done through emails or phone calls.

Side Channel Attack: An attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs)

Smishing: SMS phishing. Phishing executed over SMS.

Social Engineering: Psychological manipulation of people into performing actions or divulging confidential information.

Vishing: Voice phishing. Phishing executed over telephone.

Organizations

NSA: National Security Agency. National intelligence agency of the US Dept. of Defence. Responsible for global monitoring, collection and processing of information and data for foreign intelligence and counterintelligence, specialized in signal intelligence (SIGINT)

NIST: National Institute of Standard and Technology. A measurement standards laboratory and non-regulatory agency of the US Dept. of Commerce, who mission is to promote innovation and industrial competitiveness.

People

Whitefield Diffie: Pioneer of public-key cryptography. Co-inventor of Diffie-Hellman key exchange. Won 2015 Turing award.

Ron Rivest: Co-inventor of RSA algorithm. Investor of symmetric-key encryption RC2, RC4, RC5. Inventor of MD2, MD3, MD4, MD5, MD6 crypto hash functions. Co-author of "Introduction to Algorithms" book. Won 2002 Turing award.