DATA-553 Definitions

Dhun Sheth

2023-11-03

Term/Concept	Definition	Example
Ethics	Moral principles that guide behavior and choices	Ethical decision-making in research projects
Human Factor: The user's role in security	The impact of human behavior on security	Employees clicking on suspicious email links
Phishing	A deceptive attempt to obtain sensitive info	Sending fake emails to trick users
Ransomware	Malicious software that encrypts data	Holding data hostage for a ransom
Social Engineering	Manipulating people to reveal confidential info	Impersonating tech support for passwords
Spoofing (e-mail and URL)	Faking the source of an email or website	Sending emails that appear to be from a bank
Denial-of-Service Attack	Overwhelming a system to disrupt its function	Flooding a website with traffic to crash it
Security as a Process, not a Product	Continuous security efforts, not one-time fixes	Regular software updates for vulnerabilities
Privacy	The right to control personal information	Keeping personal details private on social media
Respect	Treating others' data and privacy with care	Not sharing personal information without consent
Anonymity	Remaining unidentified or nameless	Posting comments online under a pseudonym
De-identification	Removing identifying information from data	Removing names from a dataset for research
Explicit identifier (or direct identifier)	Information directly identifying an individual	Social Security Number or full name
Generalization of data	Aggregating data to protect individual privacy	Reporting age ranges instead of exact ages
k-anonymity	Data protection method where individuals are indistinguishable among at least k-1 others	Releasing data where no individual can be singled out
l-anonymity	Similar to k-anonymity but with a stricter threshold	Data with even stronger privacy guarantees
Pseudonymity	Using a fake name or identifier	Authors using pen names for publication
Quasi-identifier (or indirect identifier)	Information that can indirectly identify an individual	ZIP code, birthdate, or occupation
Re-identification	Matching de-identified data with individuals	Combining medical records to identify a patient

Term/Concept	Definition	Example
Sensitive attribute	Information that can be used to harm or discriminate	Medical conditions or ethnicity
Trusted third party	A neutral entity that manages sensitive data	A bank handling financial transactions
Consequence (e.g. harm, benefit)	Outcomes resulting from actions or decisions	Unauthorized data access can harm individuals
Digital Footprint	Online traces of a person's activities	Browsing history, social media posts
Research ethics board	A group overseeing ethical research practices	Reviewing and approving research protocols
End of Privacy (general idea)	The diminishing privacy due to technology	Surveillance cameras everywhere in public
Psychometrics, Psychographics	The study of psychological characteristics and behavior	Analyzing Facebook data for voter targeting
Right-to-be-Forgotten (general idea)	The right to request removal of personal data	Requesting Google to delete search history
Access Control: Identity-Based, Role-Based	Methods to control user access to resources	Only HR can access employee salary data
Authentication	Verifying the identity of a user or system	Entering a password or using a fingerprint
Authorization	Granting permissions to access specific resources	Allowing a user to edit a shared document
Availability	Ensuring resources are accessible when needed	A website being online and responsive
Confidentiality	Protecting data from unauthorized access	Encrypting sensitive medical records
Ciphertext	Encrypted text or data	Encrypted message that can't be read without the key
Dark Web	Hidden part of the internet not indexed by search engines	Illegal online marketplaces and forums
Decryption	The process of converting encrypted data to its original form	Decrypting an email to read its contents
Eavesdropping	Unauthorized interception of communication	Listening to phone calls without consent
Encryption	Converting data into a secure, unreadable format	Encrypting a credit card number for online purchases
Integrity	Ensuring data remains unchanged and reliable	Checking if a downloaded file is unaltered
Man-in-the-Middle Attack	Intercepting communication between two parties	A hacker capturing data between a user and a bank
Metadata	Information about data, not the actual content	Timestamps and location data in a photo
Plaintext	Original, unencrypted text or data	The message before encryption is applied
Symmetric Cryptography	Using the same key for encryption and decryption	AES encryption with a shared secret key
Two-Factor Authentication	Adding an extra layer of security with two verification methods	Using a password and a fingerprint to log in
Access Control Matrix (don't worry about the names: Capabilities List and Access Control List)	Systems specifying who can access what resources	Defining permissions for users in a network

Term/Concept	Definition	Example
Biometrics	Using unique physical characteristics for identification	Scanning a fingerprint for device access
One-Time Pad	A method of encryption using a single-use key	A secret agent using a unique key for each message
Open Design Principle	Security practices that do not rely on secrecy	Revealing the design of an encryption algorithm
Principle of Least Privilege	Giving users the minimum access necessary for their tasks	Employees can only access files they need
Provenance	Documenting the origin and history of data	Tracking the source and changes of a document
Secure Hash Algorithm	A cryptographic method to generate fixed-size hashes	SHA-256 to create unique file checksums
Substitution Cipher (e.g., Caesar Cipher)	Replacing each letter with a fixed number of positions down the alphabet	Shifting letters by 3 positions (ROT13)
Asymmetric Cryptography (aka Public-Key Cryptography, e.g., RSA)	Using a pair of public and private keys for encryption and decryption	Sending encrypted messages with a public key
Brute-Force Search	Trying all possible combinations to find a solution	Repeatedly guessing a password until it's correct
Collisions when Hashing	Two different inputs resulting in the same hash value	Different files having the same hash value
Cryptographic Hash Function (one-way hash function)	Transforming data into a fixed-size hash value that is hard to reverse	Hashing a password before storing it in a database
Message Authentication Code (MAC)	A code used to verify the integrity of a message	A HMAC attached to an email for verification
Password (strength, difficulty to crack, storage)	Creating secure access codes, guarding against unauthorized access	Using a long, complex password stored in a secure vault
Certificate Authority (CA)	A trusted entity that issues digital certificates	Verifying the authenticity of secure websites
Certificate Revocation List (CRL)	A list of invalidated digital certificates	Removing the certificate of a compromised website
Digital Certificate	An electronic document proving the identity of a user or system	SSL certificates for secure website connections
Digital Signature	A cryptographic signature verifying the authenticity and integrity of a message	Signing an email to prove it's from the legitimate sender
Non-Repudiation	Preventing parties from denying their actions or intentions	Digital signatures provide non-repudiation
SQL Injection Attack	Injecting malicious SQL queries into an application	Exploiting a vulnerability to extract data from a database
Backup	Making copies of data to prevent data loss	Regularly saving important files to an external drive