Armaan Shamsaasef

Non-repudiation

Notes: Non-repudiation (SY0-701 - 1.2)

Core Concept: Non-repudiation provides undeniable proof of the origin and integrity of data, preventing an individual from denying (repudiating) their involvement in a transaction or communication.

- Repudiation: "I did not send that message," or "I did not sign that document."
- Non-repudiation: Proof that makes this denial impossible.

How Non-Repudiation Works

Non-repudiation is achieved by combining two processes:

1. Integrity Verification: Confirming the data has not been altered.
2. Origin Authentication: Confirming the identity of the sender.

The primary mechanism that provides both of these is a Digital Signature.

The Digital Signature Process

A digital signature uses asymmetric cryptography (public/private keys) to provide non-repudiation.

1. The Sender:
    - Creates a unique hash of the message/data.
    - Encrypts that hash with their private key. This encrypted hash *is* the digital signature.
    - Sends the original message along with the digital signature.
2. The Receiver:
    - Uses the sender's public key to decrypt the digital signature, which reveals the original hash.

    - Creates their *own* new hash from the received message.
    - Compares the two hashes.
        - If they match, it proves two things:
            - Integrity: The message was not changed (the hashes match).
            - Origin: The message could only have come from the sender, as only their public key could decrypt the hash, which was encrypted with their private key.

Real-World Analogy

- A handwritten signature on a legal document is a form of non-repudiation. It's unique to you and proves you agreed to the document's contents.
- A digital signature is the electronic, cryptographically-secure equivalent.

Key Takeaway

Non-repudiation is a critical security service that provides undeniable proof of an action. It is a core function of integrity and is primarily implemented using digital signatures and public key infrastructure (PKI).