جامعة الملك سعود
King Saud University

1213سبر
Network Defense

Lecture #10 Part 1

Understanding Cryptography and PKI

Topics

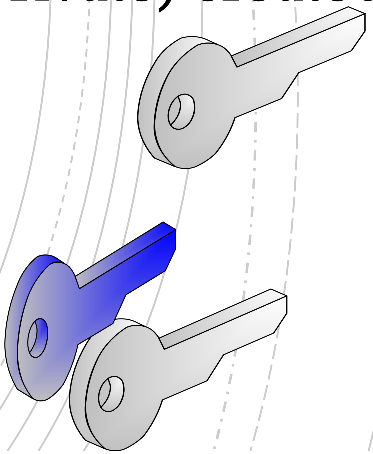
- Introducing Cryptography Concepts
- Providing Integrity with Hashing
- Understanding Password Attacks
- Providing Confidentiality with Encryption
- Using Cryptographic Protocols
- Exploring PKI Components

Cryptography Concepts - Integrity

- Provides assurances that data has not been modified
- Hashing ensures that data has retained integrity
- A hash is a number derived from performing a calculation on data
- If the data is unchanged the hash will always be the same number
- Common hashing algorithms include MD5, SHA, HMAC
- Each algorithm creates a fixed-size string of bits
  - Example: MD5 creates a hash of 128 bits

Cryptography Concepts - Confidentiality

- Ensures only authorized users can view data
- Encryption protects the confidentiality of data
- Encryption ciphers data to make it unreadable
- Encryption normally includes algorithm and key
- Symmetric encryption
  - Uses the same key to encrypt and decrypt data
- Asymmetric encryption
  - Uses two keys (public and private) created as a matched pair



Cryptography Concepts

- Authentication validates an identity
- Non-repudiation
  - Prevents a party from denying an action
- Digital signatures
  - Provide authentication, non-repudiation, and integrity
  - Users sign emails with a digital signature
    - Digital signature is a hash of an email message encrypted with the sender’s private key
    - Only the sender’s public key can decrypt the hash
    - Provides verification it was encrypted with the sender’s private key

Providing Integrity with Hashing

- Hashing provides integrity for data
  - Email, downloaded files, files stored on a disk
  - A one-way function that creates a string of characters

A hash is a number

  - Sometimes called a checksum
  - You cannot reverse the hash
  - You cannot re-create the original data from the hash
  - Created with a hashing algorithm
    - Message Digest 5 (MD5)
    - Secure Hash Algorithm (SHA) family
    - HMAC

Hashing Protocols

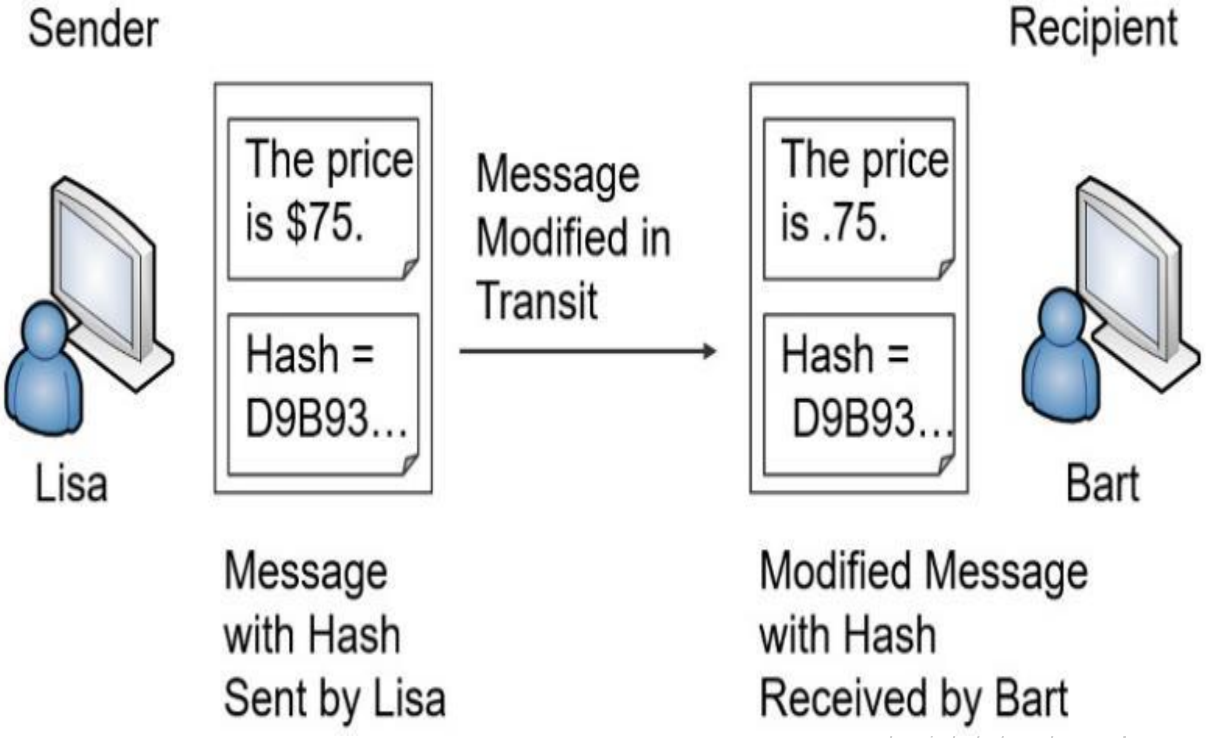
- To verify integrity
  - MD5 (use is discouraged)
  - SHA (SHA-3 previously known as Keccak)
- To verify integrity and authenticity
  - HMAC (HMAC-MD5 and HMAC-SHA1)
    - Uses a shared secret
    - IPsec and TLS use HMAC-MD5 and HMAC-SHA1

Hashing Passwords

- Passwords often stored as hashes
- Password attacks attempt to discover passwords
  - Guess a password
  - Hash the guessed password
  - Compare the hash to the original hash

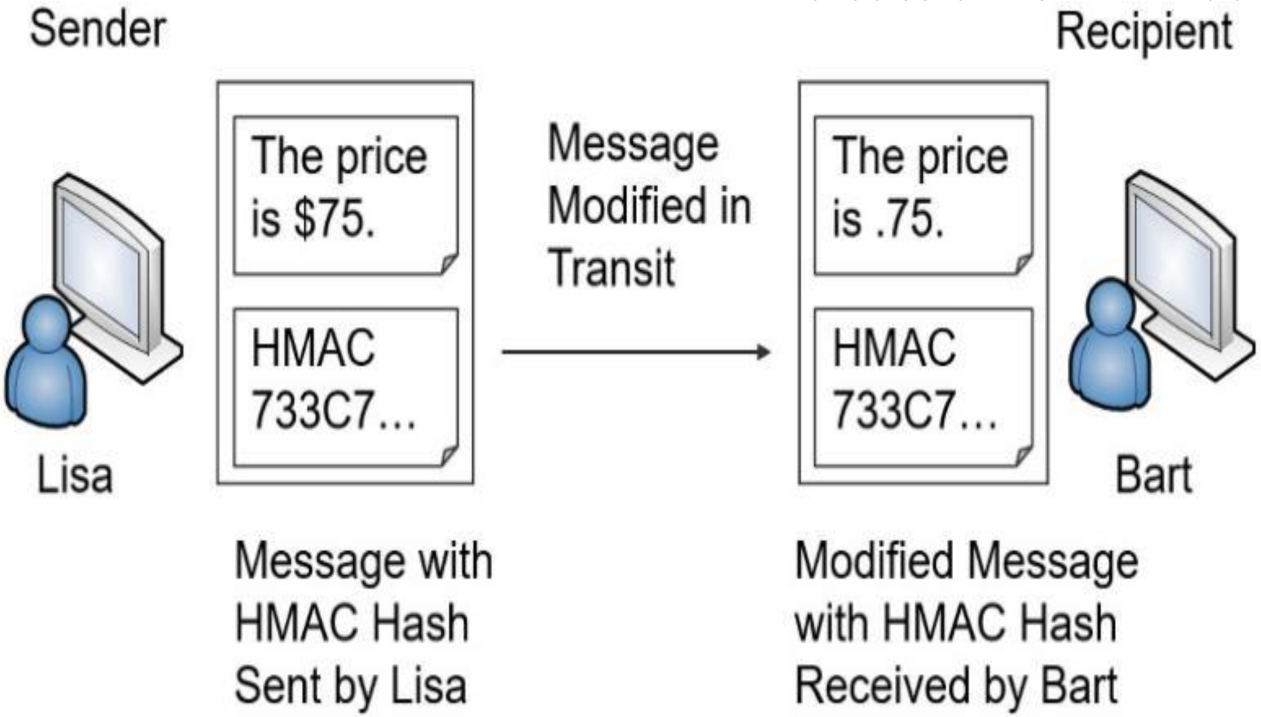
Hashing Messages

- Hashing detects modified message


Sender
Recipient
The price is $75.
Hash = D9B93...
Message Modified in Transit
The price is .75.
Hash = D9B93...
Lisa
Bart
Message with Hash Sent by Lisa
Modified Message with Hash Received by Bart

Hashing Messages with HMAC

- HMAC prevents attacker from modifying hash



Sender
Recipient
The price is $75.
HMAC 733C7…
Message Modified in Transit
The price is .75.
HMAC 733C7…
Lisa
Bart
Message with HMAC Hash Sent by Lisa
Modified Message with HMAC Hash Received by Bart

Hash Collisions

- Hashing algorithm creates the same hash from different inputs
  - MD5 (highly susceptible)

Understanding Password Attacks

- Attempt to discover, or bypass, passwords used for authentication

  - Online password attack (guess the password of an online system)

  - Offline password attack (guess the password stored within a downloaded file, such as a database)

Password Attacks

- Dictionary attacks
  - Uses a dictionary of words
  - Attempts every word in the dictionary to see if it works

- Brute force
  - Attempts to guess all possible character combinations

Password Attacks

- Spraying attacks
  - Special type of brute force or dictionary attack designed to avoid being locked out
- Pass the hash
  - Attempts to use an intercepted hash to access an account
- Birthday attacks
  - Attempts to create a password that produces the same hash as the user’s actual password

Password Attacks

- Rainbow table attacks
  - Attempts to discover the password from the hash
- Salting passwords
  - Prevent rainbow table attacks, along with other password attacks
- Key stretching
  - Used to increase the strength of stored passwords (Bcrypt, PBKDF2, and Argon2)

Providing Confidentiality with Encryption

- Encryption provides confidentiality
  - Helps ensure only authorized users can view data
  - Applies to any type of data
    - Data-at-rest (files, in a database, and so on)
    - Data-in-transit or data in motion (sent over a network)
  - Data-in-processing (sometimes called data in use_
    - Not encrypted while in use
    - If sensitive should be purged after use