NET – 332

NETWORK SECURITY LAB

Lab 4. Authentication & Message Authentication

What is Authentication?

- Short answer: establishes identity
  - Answers the question: To whom am I speaking?
- Long answer: evaluates the authenticity of identity proving credentials
    - Credential – is proof of identity
    - Evaluation – process that assessing the correctness of the association between credential and claimed identity.
- Usually for a purpose
- Policy driven (what constitutes a good cred.?)

Why Authentication?

- World of rights, permissions, and duties?
- Authentication establishes our identity so that we can obtain the set of rights/products and services

  E.g., we establish our identity with Tiffany's by providing a valid credit card which gives us rights to purchase goods ~ physical authentication system.

- Q: How does this relate to security?

Authentication in Computer World

- The Customer and Vendor are not physically located in same place.
- Prove the repudiation of what we are.
  - Ex: Buying something online using a credit card:
  - Authentication needed:
    - Credit Card number
    - CVV
    - OTP
    - Personal Details (Name, Email, Age, etc.,)

Proving Identity

- How to verify “Who am I”?
- Documentary resembling proofs;
  - Driver’s license
  - Credit Card
  - Signature Verification
  - Biometric Verification

Proving Identity (2)

- Other methods of verifying Identity are:
  - Something I know
    - Mother's maiden name, First school, Fav. Actor etc.,
  - Something I have
    - Smart chip cards, valid photo ID cards, etc.,
  - Something I am (Bio-Metric)
    - Fingerprints
    - Iris
    - Face Recognition

Message Authentication

- What confirms Message Authentication?
  - A Received message from source that claims it sent it.
  - Message that hasn’t been altered in anyway.
  - Message sequence is unchanged
  - Message timing is unchanged
    - Relay
    - Delay
    - Replay
  - Non-repudiation by sender
  - Non-repudiation by recevier

Authentication Functions

- Lower level Functions
  - Authenticator or Value
  - Ex: Getting an OTP or verification message
- Higher level functions
  - Authenticator to verify authenticity of message
  - Ex: Getting OTP only after attempting login in bank site
- Functions to produce authentication
  - Message Encryption (Ciphertext, AES, DES, RSA, etc)
  - Message Authentication Code (Checksum, MAC, etc)
  - Hash functions
    - Mapping messages to value

Message Authentication Code

- Also known as cryptographic checksum
  - MAC = $C_K(M)$
  - M = Message
  - K = Key shared between sender and receiver
  - $C_K(M)$ = Fixed Value authenticator
- MAC is readied at source after the message is ready.
- The receiver of the message can verify the authenticity of message by:
  - Re-computing the MAC of the message

MAC is vulnerable to attacks

- Encryption in MAC
  - Dependent on length of the key
  - Brute force attacks: 2^{K-1} combinations of K bit key
- MAC is many-to-one function.

MD5 – Message Digest 5

- Step 1: Appending padding bits
  - All block size are of 512bits
  - Padding bits: 1000…512th(0)
  - (Msg + pad bits + 64 bit for length) = n X 512
- Step 2: Append length
- Step 3: Initialize MD Buffer
- Step 4: Process message in 512 bit blocks
- Step 5: output 128 bit checksum

MD5 – Hands-on

- Refer to student lab manual for hands-on

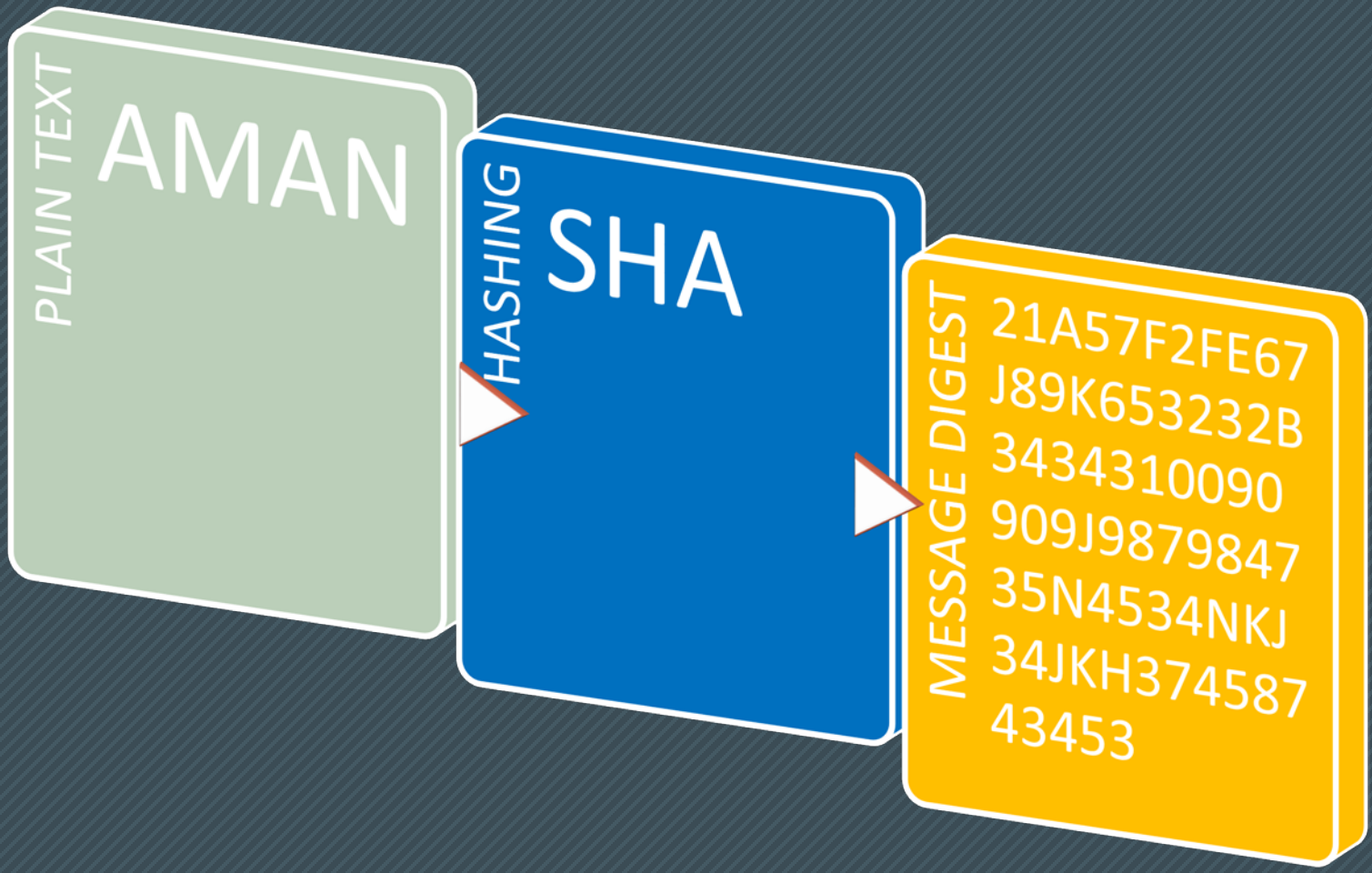
Secure Hashing Algorithm (SHA)

- Secure Hashing Algorithm
  - MD5 -Dead
  - SHA -1
  - SHA -2
  - SHA -3

Secure Hashing Algorithm (2)

- SHA based algorithms are used for authentication.
  - Iterative one way hashing algorithm that process a message to produce a condensed representation called a “Message Digest”
  - Message digest ensures integrity:
  - That means if a message changes, the message digest will also change.

Secure Hashing Algorithm (3)



Why different versions of SHA?

- Based on the Algorithm that is applied to the text/file the block size of the message digest will change.
  - Example if SHA-1 is applied the message digest will result in a 512 block OR 160 Bit
  - SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words.
  - SHA-3: A hash function formerly called Keccak, It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.

How SHA Works?

- Step 1 - Preprocessing
- A Two step procedure
  - Step 1.1 : Setting the initial hash value (consisting of five 32 bit words in Hex)
  - $H_0^{(0)} = 67452301$
  - $H_1^{(0)} = efcdab89$
  - $H_2^{(0)} = 98badcfe$
  - $H_3^{(0)} = 10325476$
  - $H_4^{(0)} = c3d2elf0$
- Based on algorithm of SHA, the initial values will also change

How SHA Works? (2)

- Step 1.1 – Padding message
- The binary representation of the message

A	M	A	N
01000001	01001101	01000001	01001110

  - Message Contains 8X4=32 bits

How SHA Works? (3)

- Remaining Steps:
- Step 2: Compute Message digest
  - Identify the binary value of the message after padding
  - Iterate the message schedule from 0-15 (based on algorithm)
  - Initialize the working variable with the $(i-1)^{st}$ hash value
- Step 3:
  - Iterate the function for t=0 to 79
  - Identify the value of ws (as defined in the secure hash standard)
- Step 4:
  - Compute the i^{th} value for intermediate hash value

Report Work

- Using MD5
  - Produce a checksum for:
    - An image
    - A text file
    - A pdf fie
  - Create a text file with the checksums
  - Append the image, text in the file and pdf file
  - Produce the checksum again and submit both the checksums: before and after the changing the file.