Web Application Security

Tessema Mengistu (Ph.D.)
Department of Computer Science
Virginia Tech
Mengistu@vt.edu

Outline

- Introduction
- An Overview of Cryptography
- Web Security

Computer System Security?

- The protection of data, networks, and computing power
- Refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization
- **The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)**

Factors of Computer Security

- **Confidentiality:**
  - Preserving authorized restrictions on information access and disclosure
  - Two concepts
    - **Data confidentiality**: Assures that private or confidential information is not made available or disclosed to unauthorized individuals
    - **Privacy**: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Factors of Computer Security

- **Integrity:**
  - Guarding against improper information modification or destruction
  - Two concepts:
    - **Data integrity**: Assures that information and programs are changed only in a specified and authorized manner
    - **System integrity** : Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Factors of Computer Security

- **Availability:**
  - Assures that systems work promptly and service is not denied to authorized users
- Additional
  - **Authenticity:**
    - The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator
  - **Accountability:**
    - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
    - This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action


Cryptography
important
data
message
sophisticated
computer
secret
Cryptology
encryption
cryptanalysis
messages
many
cope

An Overview of Cryptography

- Cryptography:
  - The principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity
- Cryptography guarantees:
  - Confidentiality
  - Integrity
  - Authenticity
  - Non-repudiation
  - Access Control

An Overview of Cryptography

Plaintext:

- A message in its natural format readable by an attacker

Ciphertext:

- Message altered to be unreadable by anyone except the intended recipients

Key:

- Sequence that controls the operation and behavior of the cryptographic algorithm

Keyspace:

- Total number of possible values of keys in a crypto algorithm

Encryption (ciphering) algorithm:

- An algorithm that changes plaintext to ciphertext

Decryption(deciphering) algorithm:

- An algorithm that changes ciphertext to plaintext

An Overview of Cryptography

- An encryption scheme is **computationally secure if**
  - The cost of breaking the cipher exceeds the value of the encrypted information
  - The time required to break the cipher exceeds the useful lifetime of the information
- Cryptographic systems are generically classified along different dimensions:
  - The number of keys used
    - Symmetric (Secret Key)
    - Asymmetric (Public Key)

An Overview of Cryptography

- Symmetric encryption
  - A single key is used for both encryption and decryption
  - Also called Secret key
- Asymmetric Encryption
  - Two different keys are used for encryption and decryption
    - One key is public – used for encryption
    - Another one secret – used for decryption

An Overview of Cryptography

- There are two general approaches to attacking an encryption scheme
  - **Cryptanalysis**
    - Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used
  - **brute-force attack**
    - Try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
    - On average half of all possible keys must be tried to achieve success

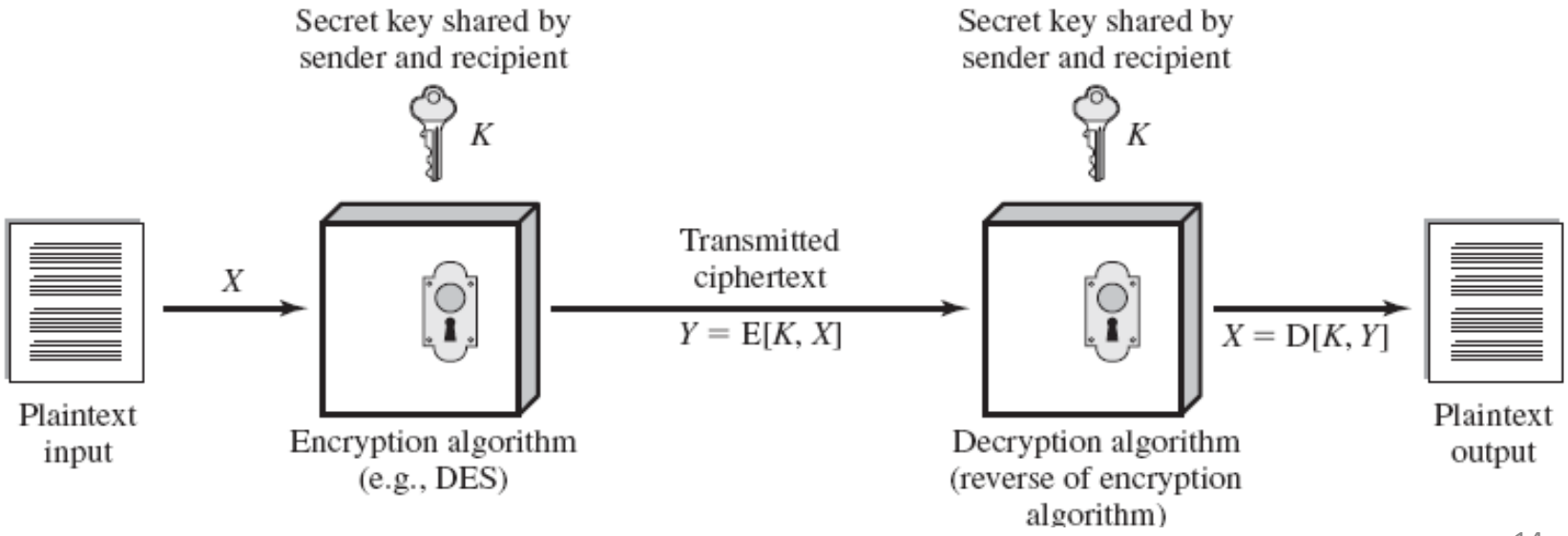
An Overview of Cryptography

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

Source: Computer Security Principles and Practices(2nd Edition),

Symmetric Key Encryption

- Also referred to as conventional encryption or single-key encryption
- A single Key - called Secret key - is used
- Sender and receiver must have obtained copies of the secret key in a secure fashion



Source: Computer Security Principles and Practices(2nd Edition),

Symmetric Key Encryption

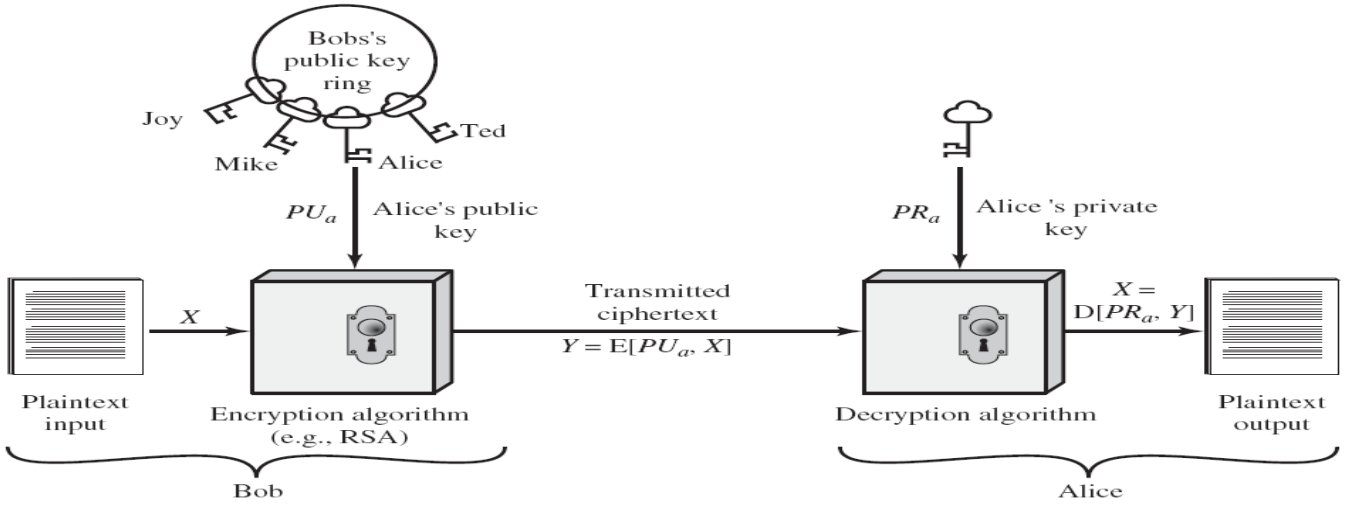
- There are two requirements for secure use of symmetric encryption
  - A strong encryption algorithm
  - Sender and receiver must have obtained copies of the secret key in a secure fashion
    - Must keep the key secure

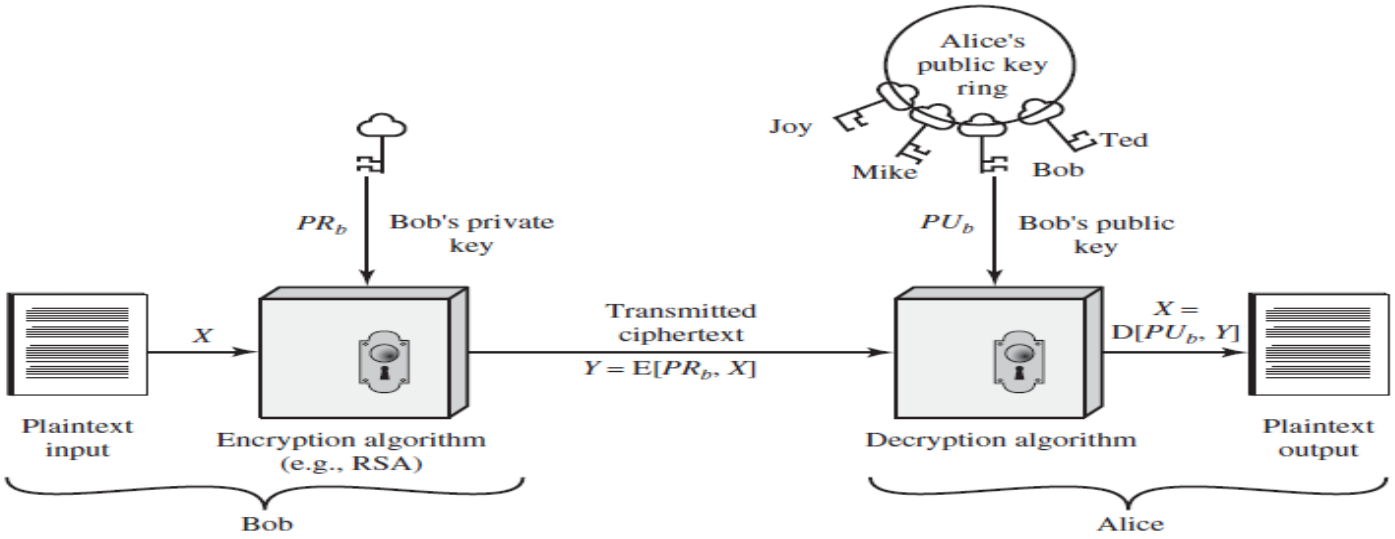
	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

Source: Computer Security Principles and Practices(2nd Edition)

Asymmetric Key Encryption

- Also called **Public Key Encryption**
- Based on mathematical functions rather than on simple operations on bit patterns
- Uses two separate keys
  - **Public**- known publicly
  - **Private** – known only by the owner
- Different algorithms
  - RSA, Diffie –Hellman, Elliptic Curve, etc.





Source: Computer Security Principles and Practices(2nd Edition),

Public Key Certificate

- Is a set of data that binds an identity to a particular public key value
- It contains:
  - **Name of owner**
    - Could be a person, device, or even role
    - Should uniquely identify the owner within the environment in which the public key will be employed
  - **Public key value**
  - **Validity time period**
    - Identifies date and time from which the public key is valid, and more importantly the date and time of its expiry.
  - **Signature**
    - Creator of certificate digitally signs all data that forms the public key certificate. This binds the data and acts as a guarantee that the creator of the certificate believes the data is correct

Certificate Authority

- The “creator” of a public key certificate
- Responsible for ensuring that the information on a certificate is correct
- Revoke the key if necessary
- Example:
  - DigiCert
  - Verisign
  - Let’s Encrypt

Asymmetric Key Encryption

- Can be used for
  - Symmetric key distribution
    - Encryption of secret keys
  - Digital signature

Message Authentication

- Message or data authentication is a procedure that allows communicating parties to verify that received or stored messages are authentic
  - The contents of the message have not been altered
  - The source is authentic
- Different techniques
  - Message Authentication Code (MAC)
  - One Way Hash Function

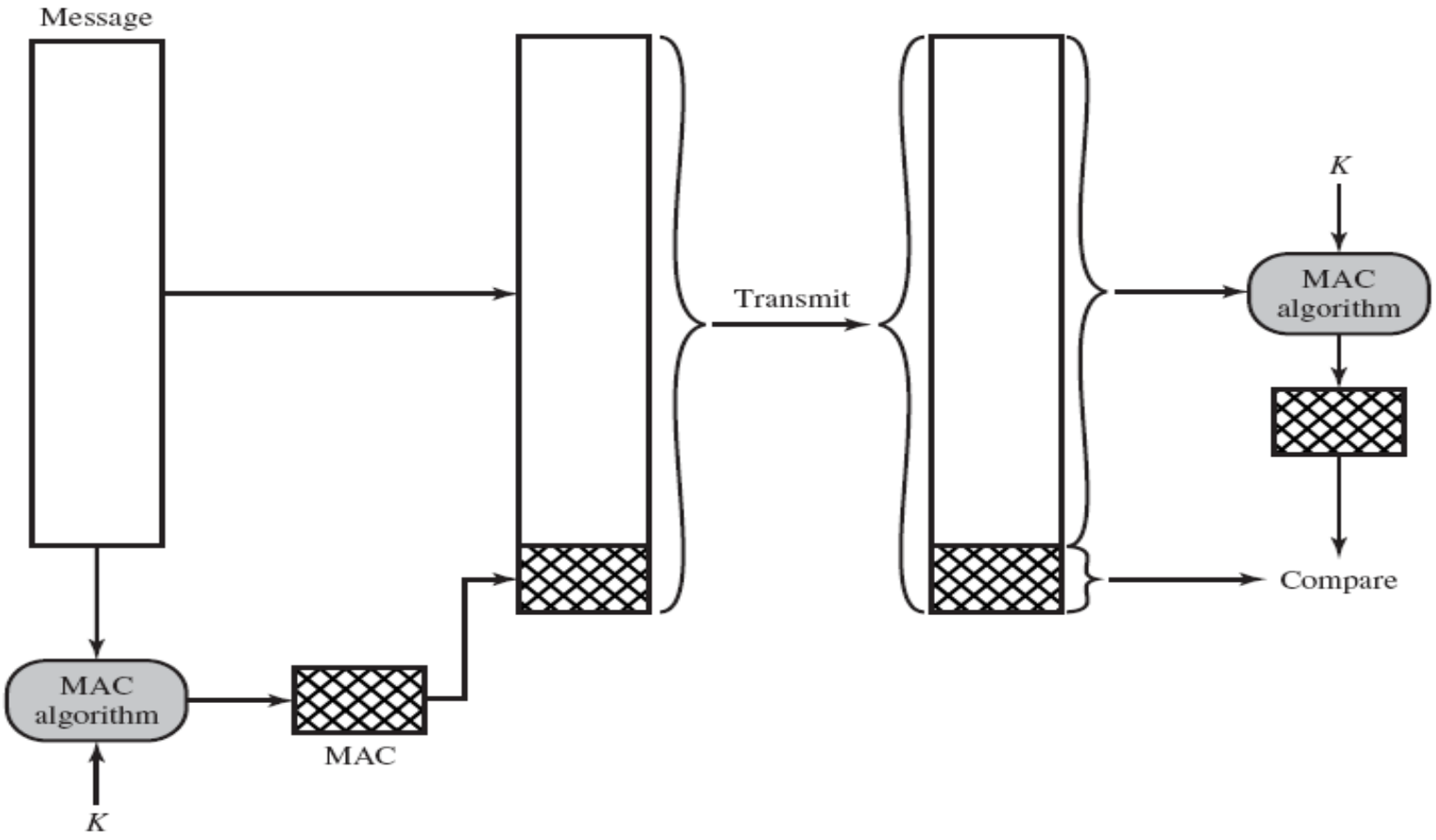
Message Authentication Code (MAC)

- Two communicating parties, say A and B, share a common secret key K_{AB}.
- Generate a small block of data - message authentication code

$$MAC_M = F(K_{AB}, M)$$

- Appended to the message and sent
- The recipient performs the same calculation on the received message

Message Authentication Code (MAC)



Source: Computer Security Principles and Practices(2nd Edition),

Hash Function

- Accepts a variable-size message M as input and produces a fixed-size message digest **H(M)** as output
- Requirements:
  - H produces a fixed-length output
  - For any given code *h, it is computationally infeasible to find x such that* H(*x) = h*
    - *one-way or preimage* Resistant
  - For any given block *x, it is computationally infeasible to find y ≠ x with* H(*y) = H(x)*
    - *second preimage* resistant/ weak collision resistant
  - It is computationally infeasible to find any pair (*x, y) such that H(x) = H(y)*
    - collision resistant / strong collision resistant

Digital Signature

- Is a number dependent on some secret known only to the signer, and, on the content of the message being signed
- How?
  - Sender
    - Generates the hash value of the message – SHA-512
    - Encrypts the hash code with private key
    - Digital signature
    - Send the message together with the digital signature
  - Receiver
    - Calculates the hash of the accepted message
    - Decrypts the digital signature with sender's public key
    - Compare the two

Digital Signature

- Security goals
  - Message integrity
  - Non-repudiation of origin of the message
  - Does not provide confidentiality

Symmetric vs. Asymmetric

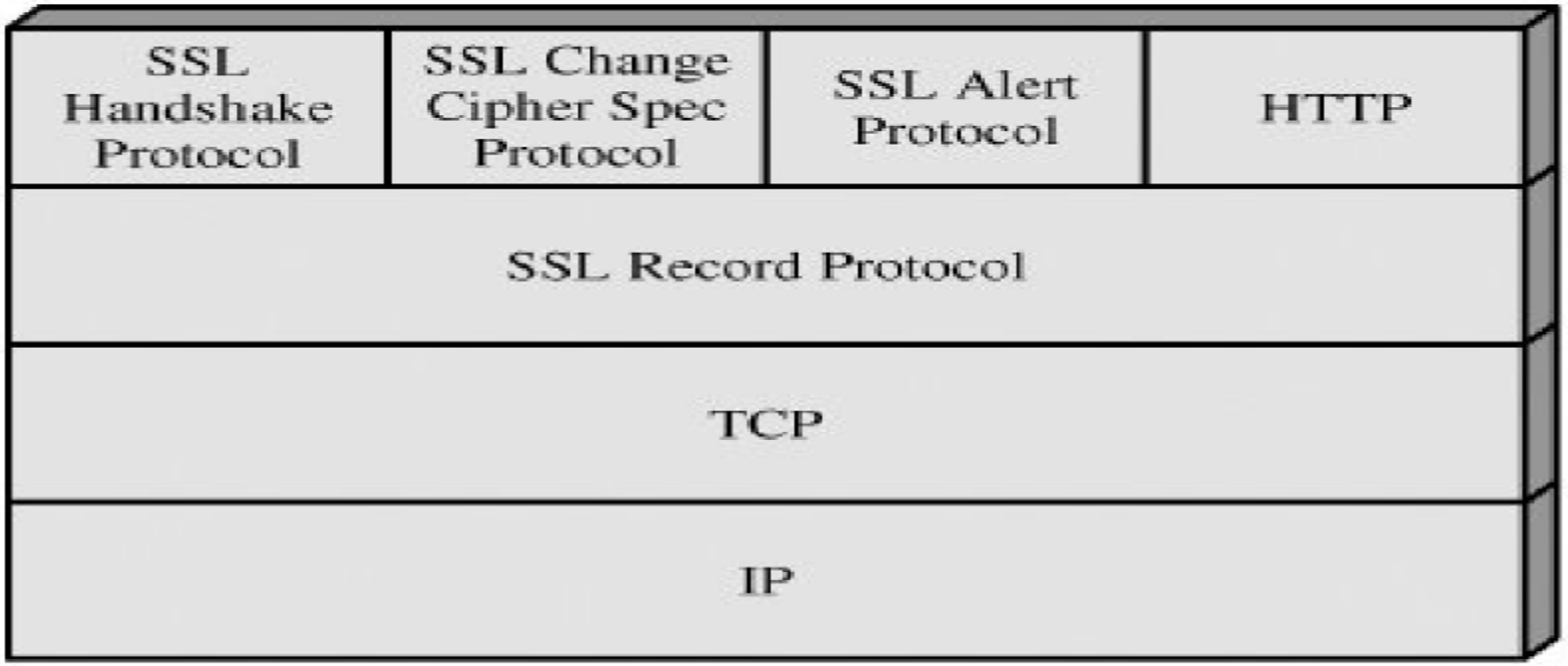
- **Symmetric cipher for confidentiality**
  - + Good performances
  - - Key delivery problems
- **Asymmetric cipher for confidentiality, integrity and authentication**
  - - Poor performances
  - + No key delivery problems

Web Security

- The World Wide Web (Web) is fundamentally a client/server application running over the Internet and TCP/IP intranets
- Over HTTP or HTTPS
- Web security threats location:
  - Web server
  - Web browser
  - Network traffic between browser and server
- Web security can be implemented at different layers of OSI
  - Network Layer – IPSec
  - **Transport Layer – SSL/TLS**
  - Application Layer – Kerberos

SSL/TLS

- Secure Socket Layer / Secure Transport Layer
- Netscape originated SSL
- Designed to make use of TCP to provide a reliable end-to-end secure service



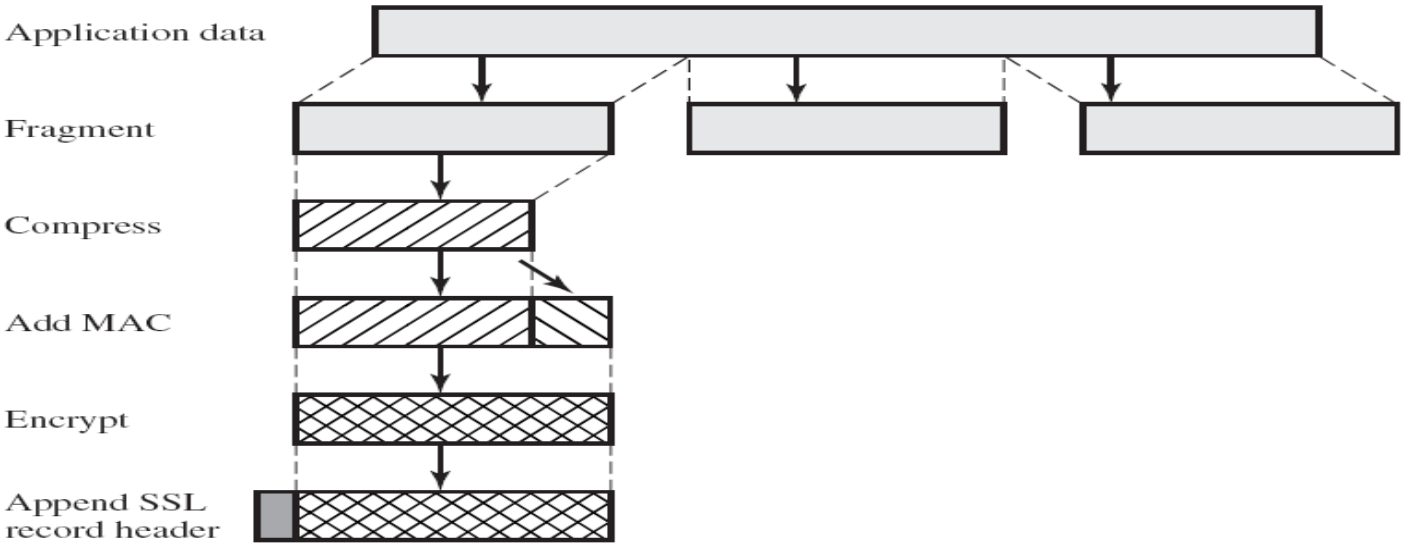
Source: Computer Security Principles and Practices(2nd Edition),

SSL/TLS

- Two important SSL concepts
  - Connection
    - A transport that provides a suitable type of service.
  - Session
    - An association between a client and a server that defines a set of cryptographic security parameters, which can be shared among multiple connections.
    - Has associated parameters:
      - Session ID
      - Compression methods
      - Cipher spec
      - Sequence numbers
      - Keys
      - etc.

SSL/TLS

- **SSL Record Protocol**
  - The SSL Record Protocol provides two services for SSL connections
    - Confidentiality
    - Message Integrity - MAC



SSL/TLS

- Handshake Protocol
  - Allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an SSL record
  - Used before any application data are transmitted
  - Involves message exchanges in 4 phases

SSL/TLS

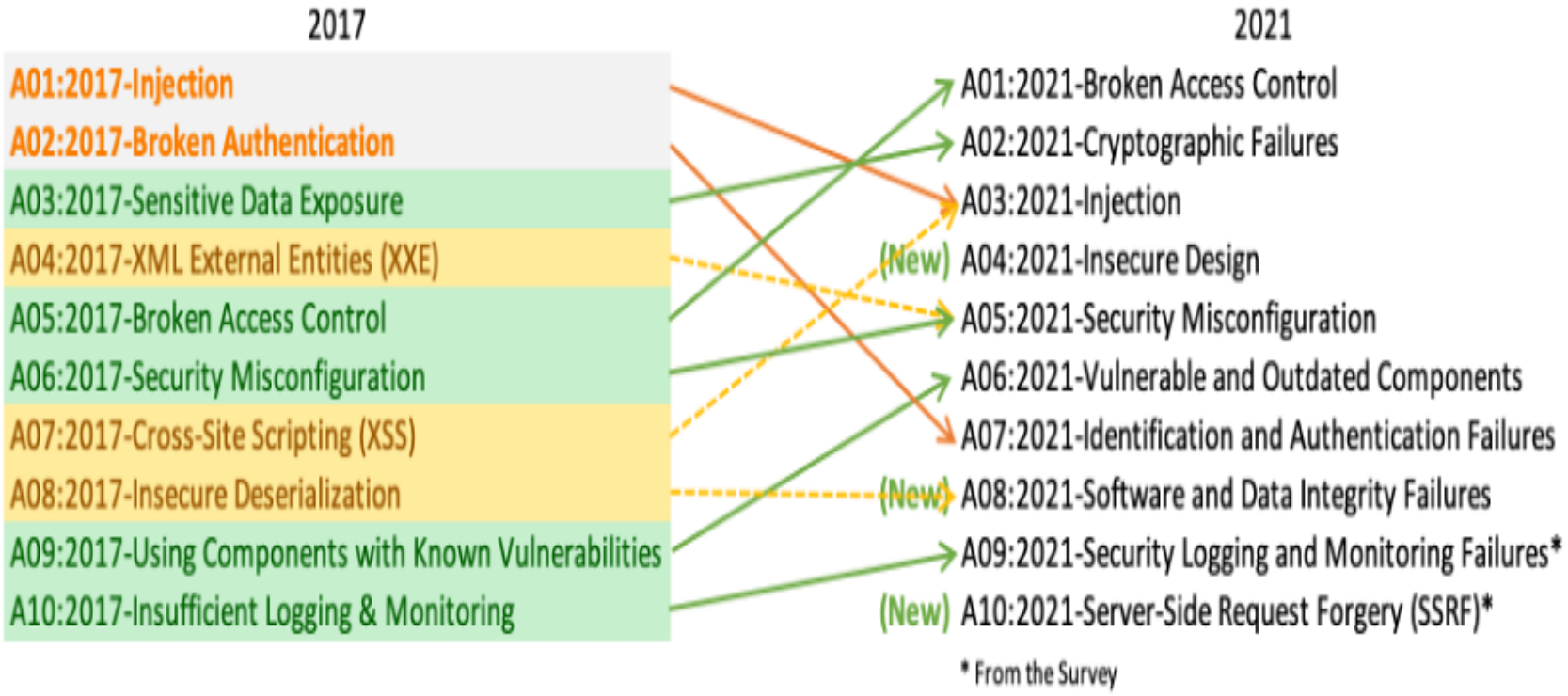
- Phase 1
  - Initiate a logical connection and to establish the security capabilities
  - The message includes
    - Session ID
    - CipherSuit
    - Compression methods
- Phase 2
  - The server passes a certificate to the client and a request for a certificate from the client
  - Server-Done message- always required

SSL/TLS

- Phase 3
  - The client should verify that the server provided a valid certificate if required
- Phase 4
  - Completes the setting up of a secure connection
  - The client sends the finished message under the new algorithms, keys, and secrets.

HTTPS

- HTTP over SSL
- Uses port number 443
- The following elements of the communication are encrypted:
  - URL of the requested document
  - Contents of the document
  - Contents of browser forms (filled in by browser user)
  - Cookies sent from browser to server and from server to browser
  - Contents of HTTP header



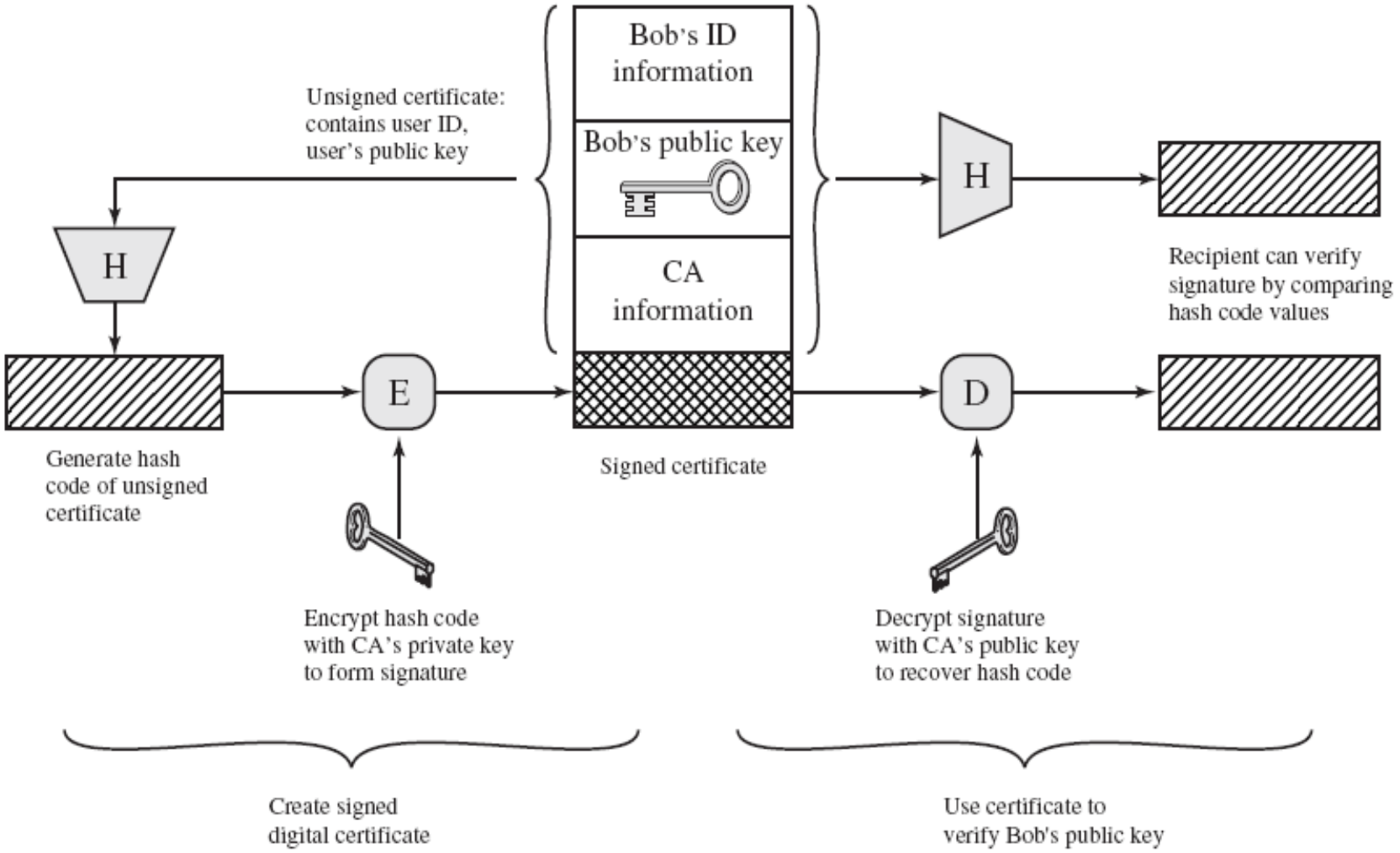
Source: https://owasp.org/www-project-top-ten/

References

- William Stallings and Lawrie Brown. Computer Security Principles and Practices(2nd Edition), Pearson, 2012
  - Ch. 1, 2, 22(22.3 & 22.4)
- https://owasp.org/www-project-top-ten/

Supplemental Slides

Public Key Certificate



Source: Computer Security Principles and Practices(2nd Edition),

Cross Site Scripting (XSS)

- Occur whenever an application takes user supplied data and sends it to a web browser without first validating or encoding that content
- XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, possibly introduce worms, etc

Injection

- Occurs when user-supplied data is sent to an interpreter as part of a command or query
- The attacker's hostile data tricks the interpreter into executing unintended commands or changing data
- Example
  - SQL injection
    - **String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";**
  - Using system calls to in turn make calls to the operating system
- Protection
  - Input validation
  - Use language specific libraries to perform the same functions as shell commands and system calls

Broken Authentication and Session Management

- Attackers compromise passwords, keys, or authentication tokens to assume other users' identities
- You may be vulnerable if:
  - User authentication credentials aren't protected when stored using hashing or encryption.
  - Credentials can be guessed or overwritten through weak account management functions (e.g., account creation, change password, recover password, weak session IDs).
  - Session IDs are exposed in the URL (e.g., URL rewriting).
  - Session IDs don't timeout, or user sessions or authentication tokens, particularly single sign-on (SSO) tokens, aren't properly invalidated during logout.
  - Session IDs aren't rotated after successful login.
  - Passwords, session IDs, and other credentials are sent over unencrypted connections

Broken Authentication and Session Management

- Example Attack Scenarios
  - Scenario #1:
    - Airline reservations application supports URL rewriting, putting session IDs in the URL:

      http://example.com/sale/saleitems;jsessionid=2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii
    - An authenticated user of the site wants to let his friends know about the sale. He e-mails the above link without knowing he is also giving away his session ID. When his friends use the link they will use his session and credit card.
  - Scenario #2:
    - Insider or external attacker gains access to the system's password database. User passwords are not properly hashed, exposing every users' password to the attacker

Broken Authentication and Session Management

- Scenario #2:
  - Application's timeouts aren't set properly. User uses a public computer to access site. Instead of selecting "logout" the user simply closes the browser tab and walks away. Attacker uses the same browser an hour later, and that browser is still authenticated.

- Protection
  - Entire session should be transmitted via HTTPS to prevent disclosure of the session ID. (Not just the authentication)
  - Avoid or protect any session information transmitted to/from the client.
  - Session ID should expire and/or time-out **on the Server** when idle or on logout.