ECE 473/573
Cloud Computing and Cloud Native Systems
Lecture 14 Introduction to Cloud Security

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

October 1, 2025

Outline

Cryptography

TCP/IP Network Security

Reading Assignment

- This lecture: Introduction to Cloud Security
- Next lecture: Web Security

Outline

Cryptography

TCP/IP Network Security

CIA: Basic Components of (Computer Cyber) Security

- A king need to send messages to a general fighting in a war.
- Confidentiality
  - Only the king and the general can read the messages.
- Integrity
  - The general should only accept messages sent by the king.
- Availability
  - Some of the messages must be able to reach the general.

Additional Security Services

- Nonrepudiation: sender can not deny creation of message.
  - Can the general provide a proof to a third party that the command is from the King?
  - But who is the King?
- Authentication: who are you?
  - A.k.a. entity/user authentication, or identification
  - Within the context of computer cyber security, shall be built on top of a nonrepudiation service (but usually is not!).
- Access control/authorization: decide who can do what.

Symmetric Cryptography

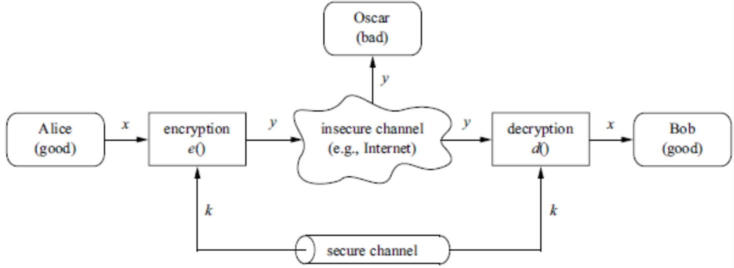

Fig. 1.5 Symmetric-key cryptosystem

(Paar and Pelzl)

- A mechanism for confidentiality
  - plaintext x, ciphertext y, and the key k
  - $e()$: encryption such that $y = e_k(x)$
  - $d()$: decryption such that $x = d_k(y)$
  - "Symmetric": both Alice and Bob know k.
- No "security by obscurity": Oscar knows everything except k

Hash Functions

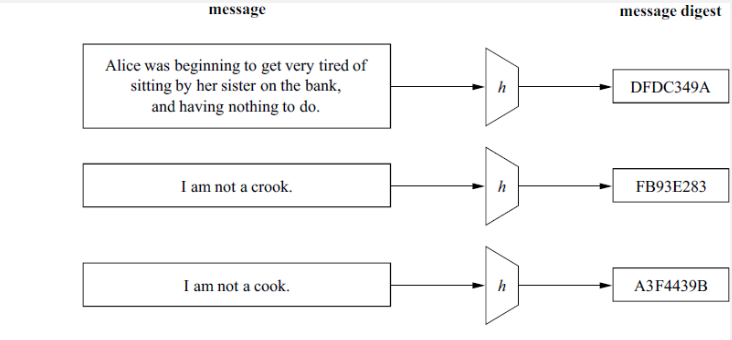

Fig. 11.3 Principal input–output behavior of hash functions

(Paar and Pelzl)

- Input x: messages of arbitrary lengths
- Output $z = h(x)$: <u>message digest</u> or hash, with fixed size.
- A strong hash function for use with cryptography prevents to find $x \neq x'$ such that $h(x) = h(x')$.

Authenticated Encryption with Associated Data (AEAD)

- Symmetric ciphers along cannot guarantee integrity.
- With the secret, hash functions can be augmented into message authentication code to validate integrity.
- Authenticated encryption combines the two to achieve both confidentiality and integrity.
- Very tricky to implement them together securely.
  - Use a well-defined AEAD algorithm like GCM, where software packages and hardware accelerations are widely available.
- AEAD cannot provide nonrepudiation service.
  - Neither Alice nor Bob can provide a proof that the message is encrypted by the other because they both know the secret.

Key Establishment

- To establishing a shared secret between two or more parties.
  - Which could be used later for AEAD.
- How can we solve this problem without a shared secret to begin with?

Public-Key Cryptography

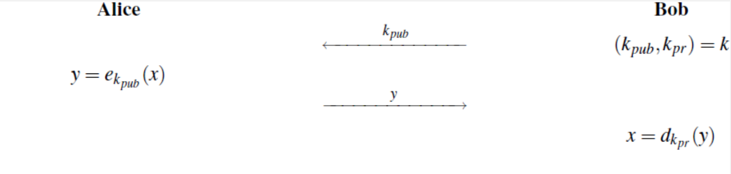

Fig. 6.4 Basic protocol for public-key encryption

(Paar and Pelzl)

- Key pair k: a public k_{pub} and a private (secret) k_{pr}.
  - No one should be able to derive k_{pr} from k_{pub}.
- Alice only need to obtain Bob's k_{pub} before they could share the secret x
- Such algorithms exist, e.g. RSA
- But how could Alice be sure that k_{pub} is from Bob?

Digital Signatures

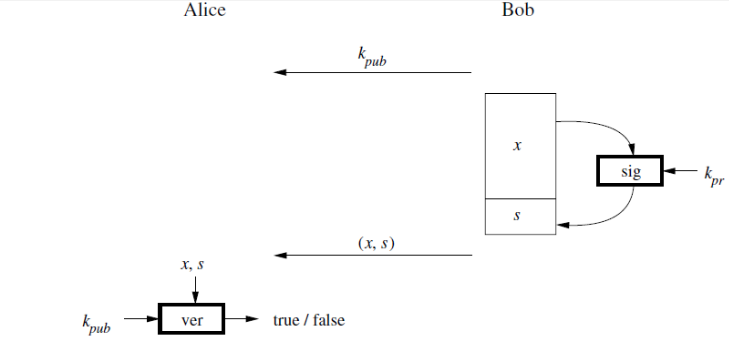

Fig. 10.1 Principle of digital signatures which involves signing and verifying a message

(Paar and Pelzl)

- Nonrepudiation: no shared secret
  - Bob signs with his private key k_{pr}.
  - Alice verifies with Bob's public key k_{pub}.
- Such algorithms exist, e.g. to run RSA reversely.
- Still, how could Alice be sure that k_{pub} is from Bob?

Public Key Infrastructure (PKI)

- A service to connect public keys to physical identities.
  - People, hosts, services, etc.
- Certificate Authority (CA): a trusted third-party.
  - Make use of public-key cryptography: $k_{pub,CA}$ and $k_{pr,CA}$.
  - For digital signatures only.
- Everyone knows $k_{pub,CA}$ to verify digital signatures from CA.
  - But how?
- How Bob proves to Alice $k_{pub,B}$ is from Bob?
  - Bob sends $k_{pub,B}$ to CA and ask CA to sign $(k_{pub,B}, ID_B)$.
  - CA returns Bob his <u>certificate</u>:
    $Cert_B = ((k_{pub,B}, ID_B), sig_{k_{pr,CA}}(k_{pub,B}, ID_B))$.
  - Bob presents Alice $Cert_B$ that Alice can verify with $k_{pub,CA}$.
- Authentication: in other words, Bob proves to Alice that he is Bob, with the help from CA.

Outline

Cryptography

TCP/IP Network Security

Security in TCP/IP Network

- TCP/IP network is created to address availability concerns.
  - Confidentiality and integrity are expected to be addressed through a layered approach.
- How to protect TCP/IP communications?
  - For efficiency reasons, many widely used TCP/IP protocols like HTTP do not address confidentiality and integrity by default.
  - The attacker may see packets, requests, responses and etc., and modify them to inject malicious code.
- Compromised systems communicating via TCP/IP further complicate the security issuses
  - How to monitor and control TCP/IP communications?
- How to achieve security without requiring substantial changes to existing infrastructures?

Internet Protocol Security (IPsec)

- A secure communication protocol at IP layer.
  - Any other service on top of IP, like TCP, obtains the same security guarantees automatically.
  - Encapsulate IP packets to be protected in AH and ESP IP packets – literally, no change is needed to route them.
- Authentication: host
- Modes of operation
  - Transport mode: protect host to host communication, e.g. among a group of servers within a data center.
  - Tunnel mode: protect router to router communication, e.g. a VPN across Internet that interconnects groups of servers at different geographic locations.
- Widely available, but usages are limited to professionals or specific applications like VPN due to its complexity.

IPSec: Internet Key Exchange (IKE)

- Service running on IPSec hosts that establishes security associations (SA) among communicating parties.
  - Similar to key establishment.
  - Also include negotiation of ciphers, hash algorithms, and other security properties like lifetime.
- Authenticate hosts and establish session key by
  - Manual configurations of pre-shared keys or public keys.
  - Certificates signed by a trusted CA.
  - Delegation to other protocols like Kerberos.

IPSec: AH and ESP

- Authentication Headers (AH)
  - IP protocol number 51
  - Provide integrity/message authentication
  - Optionally support sequence number to resist replay attacks.
- Encapsulating Security Payload (ESP)
  - IP protocol number 50
  - Provide confidentiality only (not recommended), or confidentiality and integrity (recommended).
  - Also resist replay attacks.
- Note that you can't hide/encrypt destination IP addresses; otherwise intermediate routers don't know where to route the packets.

Transport Layer Security (TLS)

- Successor of Secure Sockets Layer (SSL)
  - SSL has been deprecated because of security concerns.
  - However, the name 'SSL' remains in use, e.g. when mentioning TLS as TLS/SSL, or using Java API.
  - You should use TLS 1.1 or above, and avoid SSL 1.0,2.0,3.0, as well as TLS 1.0 .
- Provide confidentiality and integrity over TCP connections.
  - Client connects to server via TCP, then negotiates via a handshaking procedure to determine cipher parameters and to perform authentication and key establishment.
  - Finally the byte streams are protected by authenticated encryption and sent over the TCP transport.

TLS Authentication

- Via Public-Key Infrastructures (PKI).
- Server authentication
  - Server provides its certificate.
  - Client verifies the server certificate using the corresponding CA's public key.
- Client authentication
  - Server provides a list of CAs that it would trust.
  - Client provides one of its certificates that is signed by one of server's CAs.
  - Server verifies the client certificate using the corresponding CA's public key.
- Usually server authentication only.

TLS: Certificates Management

- CA certificates (public key) distribution.
  - Usually as part of your OS installation.
  - Can be updated manually.
  - Only install OS from legitimate sources and be careful to provide others with root accesses to servers.
- Certificate revocation list (CRL)
  - Each certificate has an expiration date. An expired certificate won't be accepted.
    - Could attackers change that expiration date?
  - CAs will provide a list of all revoked certificates that are not expired, which should be refered when verifying certificates.
  - Clients and servers need to get this list on a timely basis.

Firewalls

- Monitor and control network traffic with predefined rules.
  - Deny or allow network traffics based on source and destination addresses, protocol, content, etc.
  - Redirect packets by transforming their headers.
- Connectionless rules
  - Stateless: evaluate packets independently
  - Simple to implement efficiently.
  - E.g. to prevent all packets from a host B to reach a host A.
- Connection-based rules
  - Stateful: track packets within a stateful protocol like TCP.
  - Require resources to track protocol states.
  - E.g. to prevent a host B to initiate a communication to a host A while allowing A to initiate a communication with B.

Summary

- Public-key infrastructures combine symmetric cryptography and public-key cryptography to establish secure communication over insecure networks and to provide authentication.
- TCP/IP network is not secure. But we can protect it with proper system setup and choice of protocols.
  - Without breaking existing network infrastructure and applications.