Deployment and Operations for Software Engineers 2nd Ed

Chapter 7—Infrastructure Security

Outline

- **Cryptography**
- Key exchange
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- DNSSEC
- Secure Shell
- Secure File Transfer
- Intrusion Detection

Easy to remember definition of security

- CIA
  - Confidentiality – only authorized users can access data and resources.
  - Integrity – data is not corrupted or modified
  - Availability – information and resources are available to authorized users.

More precise security definition

- **Authentication**: assurance that communicating entity is the one claimed
- **Authorization**: prevention of the unauthorized use of a resource
- **Data Confidentiality** protection of data from unauthorized disclosure
- **Data Integrity** assurance that data read or received is as written or sent by an authorized entity
- **Non-Repudiation** protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

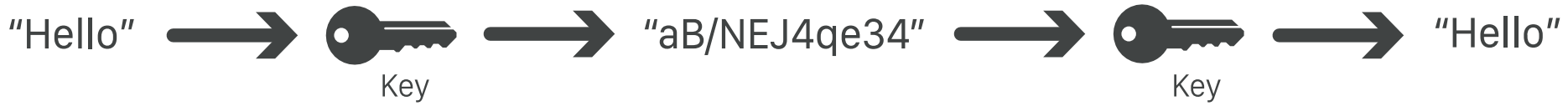
Data

- One more concept – data
  - At rest – on disk or in memory
  - In transit - on the network

Encryption

- Encoding data so that it is not readable without key.
- Three forms of encryption
  - Symmetric – the same key is used for encryption and decryption.
  - Asymmetric- one key is used for encryption and a separate key is used for decryption.
  - One way – hash. Perform encryption but there is no key for decryption.
- NIST (US National Institute for Science and Technology) certifies algorithms and implementations for encryption.

Symmetric encryption

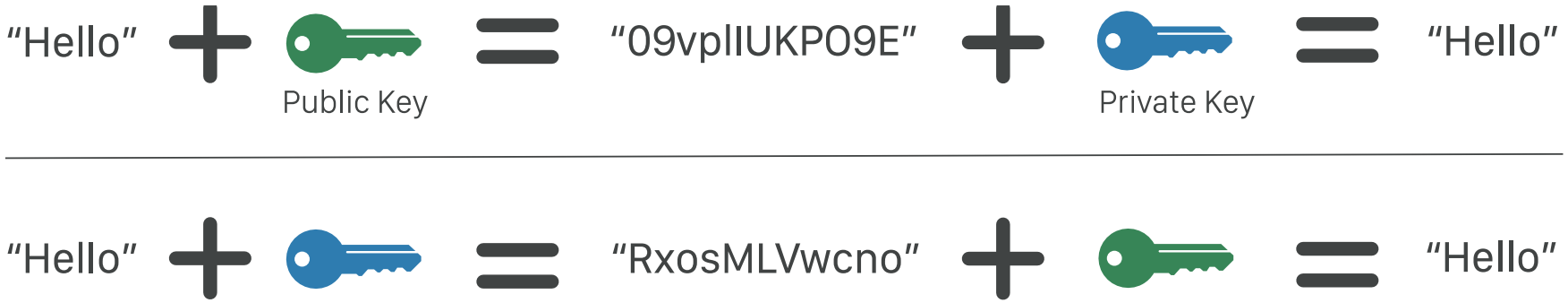


- Use same key for encrypting and decrypting
- Suitable for data at rest
- A portion of solution for data in transit.
- NIST approved algorithm is AES with key lengths of >128 bits

Weakness of symmetric encryption

- If attacker discovers key, they have access to all encrypted data
- No authentication with symmetric encryption

Asymmetric encryption



- Also known as public/private key encryption
- Messages encrypted with public key can be decrypted by private key (and vice versa)
- NIST approved algorithms: DSA, RSA, ECDSA >1024 bits

Hashing for encryption

- A hash is a one way encryption based on a public algorithm with no key
- Not possible (very difficult) to decrypt
- Used to verify integrity of data
- Passwords: save hash of password but not password. When user enters password, compare to hash to verify.
- Downloads: publish hash of software available for download. Compare hash of downloaded software. Verifies that software has not been modified.
- NIST approved algorithm is SHA-3.

Performance comparison of encryption algorithms

- Symmetric encryption is ~4000x faster than asymmetric encryption.
- SHA-3 is notably faster than other hashing algorithms.
  - Measured in cycles per byte of value being hashed.
  - 12.6 cpb on a typical x86-64-based machine

Discussion questions

1. Hashing has other purposes than security. What are these other purposes?
2. How are the keys in an asymmetric encryption developed? What keeps the keys from being discovered?

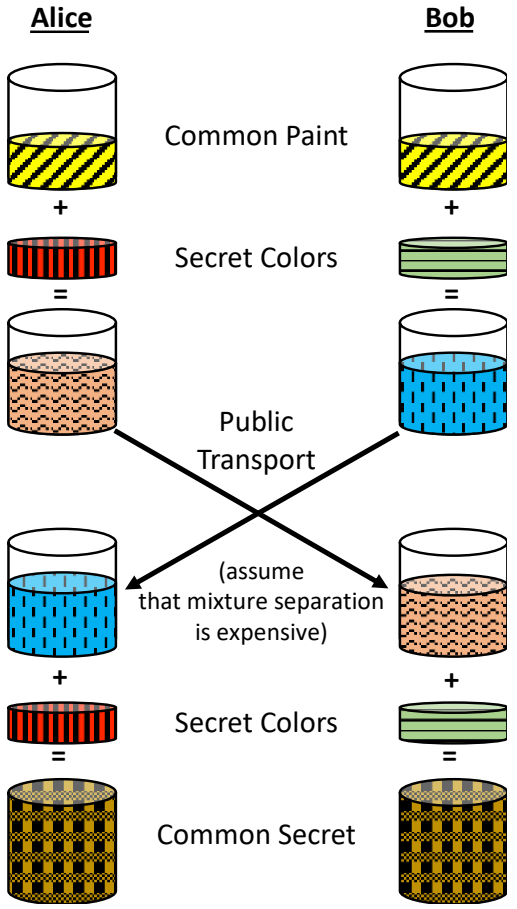
Outline

- Cryptography
- **Key exchange**
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- DNSSEC
- Secure Shell
- Secure File Transfer
- Intrusion Detection

Developing symmetric key

- Suppose Alice and Bob wish to communicate securely.
- Communication over the internet is open to eavesdropping.
- Step 1 is to develop a shared symmetric key.
- The Diffie-Hellman algorithm is a means for Alice and Bob to generate a shared symmetric key even if there is an eavesdropper on their communication.
- Security of the algorithm is dependent on the difficulty of factoring large numbers.
- We present a more intuitive description using colors.

Intuitive explanation of Diffie-Hellman



- Alice and Bob agree on a shared color.
- Alice and Bob both independently choose a secret color.
- Alice mixes the shared color with her secret color and sends the mixture to Bob
- Bob mixes the sharedshared color with his secret color and sends to Alice.
- Alice adds her secret color to the mixture she got from Bob. Bob does the same.
- The resulting color, on both sides, has the same components.

Explanation of algorithm

- Determining the components of a color mixture is hard.
- A common large prime number and secret large prime numbers take the place of the colors in the example.
- Finding the prime factors of a number is NP hard.

Additional implementation issues

- The shared key is ephemeral. Once a session is over, it is cleared from memory. Even if it is leaked, the damage is limited to a single session.
- Generating the secret large primes depends on finding large random numbers.
- This in turn depends on physical phenomenon. E.g. electrical noise from computer components.

Discussion questions

1. What is the difference between a pseudo random number and a truly random number?
2. What are some physical phenomenon used to generate large random numbers?

Outline

- Cryptography
- Key exchange
- **Public Key Infrastructure and certificates**
- Transport Layer Security (TLS)
- DNSSEC
- Secure Shell
- Secure File Transfer
- Intrusion Detection

How do I know with whom I am communicating?

- Asymmetric (public/private) keys can be used to confirm communication between individuals.
- Alice can send a message that guarantees she sent it.
- Alice can receive a message that only she can read
- Alice publishes her public key for the world to see.
- Alice keeps her private key secret.

A message only Alice can have sent

- Now Alice wants to send a message to Bob so that Bob knows it is from her.
- She encrypts her message using her private key.
- It can only be decrypted using her public key.
- It must come from Alice since only she knows her private key.

A message only Alice can read

- Bob encrypts a message to Alice using her public key.
- Alice decrypts it using her private key.
- Only Alice can read the message since only she knows her private key.

Digital Signature

- A digital signature is a means for sending an open signed letter.
- Anyone can read it but it is guaranteed to come from a particular party.
- You wish to send “text”.
- Hash “text” to get a hash value
- Encrypt the hash value with your private key
- The message consists of “text”+encrypted hash value.
- Anyone can read “text”, hash it and get a hash value.
- Using your public key to decrypt the encrypted hash value and comparing it to the current hash will ensure your message has not been altered.

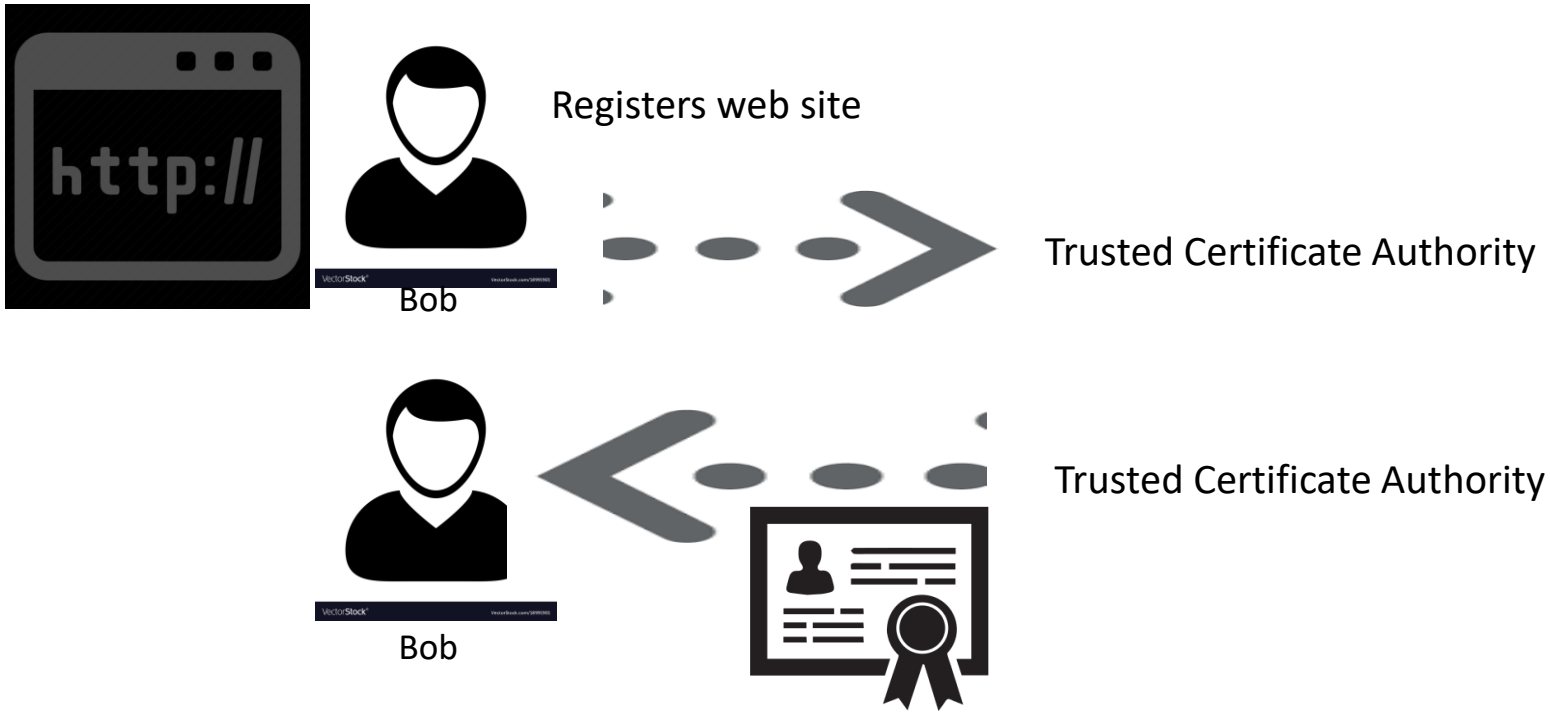
PKI

- Public Key Infrastructure (PKI) is based on a trusted Certificate Authority (CA).
- A CA is an independent organization that will issue a certificate only to a party (called a *subscriber)* that can verify its identity.

Certificates

- Certificates are used to establish that a web site is what it claims to be.
  - You own a web site.
  - You register the web site with a CA.
  - The CA issues you a certificate that attests to your ownership.
- Two important elements of a certificate
  - URL of web site that has been certified
  - Digital signature of a trusted certificate authority

Getting a certificate



Accessing Web Site

Alice verifies using CA's public key (saved in her browser) and knows she is talking to Bob's web site

Discussion questions

1. Why do certificates use digital signatures rather than just being encoded with the CA's private key?
2. How are certificates revoked?

Outline

- Cryptography
- Key exchange
- Public Key Infrastructure and certificates
- **Transport Layer Security (TLS)**
- DNSSEC
- Secure Shell
- Secure File Transfer
- Intrusion Detection

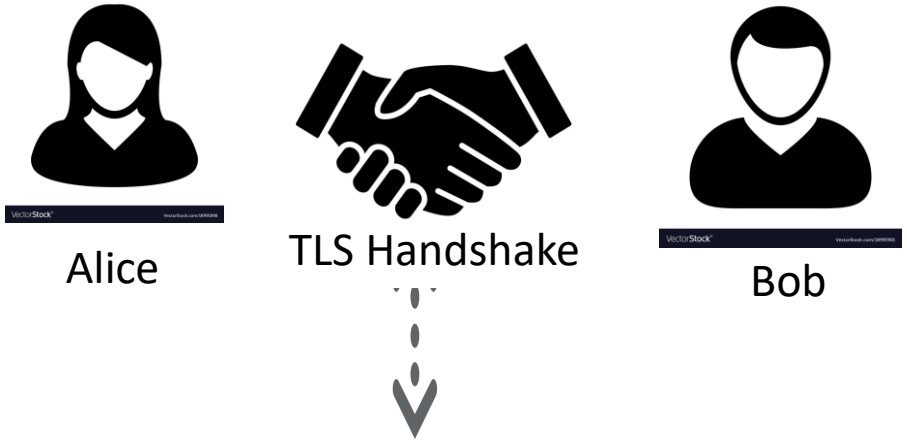
Man in the middle attack

- You are in the airport scanning for an available ISP
- You find “freewifi” and get an IP address from them.
- “freewifi” may be an attacker
- “freewifi” can
  - modify messages to spoof the web site and steal your credentials
  - eavesdrop on your communication with a web site

TLS

- TLS (Transport Layer Security) is the basis for https
- Thwarts man-in-the-middle attacks
- Used in web browsing, email, instant messaging, and voice over IP.
- Starts with a “handshake” that
  - Establishes identity
  - Creates symmetric key

TLS Overview



Symmetric key is output of handshake

- Symmetric key is used to encrypt actual messages
- Discarded after session completes
- Another session will generate a different key

TLS handshake

- Establish identify
- Uses certificates which depend on public/private keys
- Because certificates are digitally signed, they can neither be modified or spoofed
- Use Diffie-Hellman algorithm to create session key for symmetric encryption

Thwarting man in the middle

- Man in the middle may see all messages but
  - Credential is digitally signed so it cannot be modified
  - Diffie-Hellman protects against eavesdropper (the man in the middle)
- Your communication with web site is encrypted using key unknown to man in the middle

Discussion questions

1. What version of TLS is the latest?
2. Suppose the web site you are communicating with has not been updated to latest TLS version. What happens?

Outline

- Cryptography
- Key exchange
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- **DNSSEC**
- Secure Shell
- Secure File Transfer
- Intrusion Detection

DNSSEC motivation

- DNS is protected against
  - Physical intrusion
  - Unauthorized addition of entries
- Suppose, however, that an authorized individual wishes to corrupt some entries
- When you receive an IP from DNS, you have no easy means to verify who entered the IP into the DNS system.
- This is the problem that DNSSEC solves.

DNSSEC

- DNSSEC adds a certificate to the IP entry so that you know who published the information.
- Two t;hings are necessary to utilize DNSSEC
  - Registrants, who are responsible for publishing DNS information, must ensure their DNS data is DNSSEC–signed.
  - Network operators need to enable DNSSEC validation on their resolvers that handle DNS lookups for users.

Outline

- Cryptography
- Key exchange
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- DNSSEC
- **Secure Shell**
- Secure File Transfer
- Intrusion Detection

SSH

- Secure Shell (SSH) is a standard protocol and supporting software that enables the control of one computer remotely from another
- Uses public/private key but SSH is unrelated to PKI and TLS
- SSH has a concept of “known addresses” that allows logging into remote computer without a password.
- SSH is used by tools to provision and manage collections of computers. It is also used in Virtual Private Networks. .

TLS vs SSH

- TLS allows communication between two arbitrary parties using PKI
- SSH allows communication where one party knows the IP address it wishes to communicate with
- Could TLS be used instead of SSH? Yes, but:
  - They have different historical roots and SSH is very embedded in practice
  - Using TLS would require having certificates for many more machines.

Outline

- Cryptography
- Key exchange
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- DNSSEC
- Secure Shell
- **Secure File Transfer**
- Intrusion Detection

File Transfer Protocol (FTP)

- **FTP** is a standard network protocol used for the transfer of computer files between a client and server on a computer network.
- First version standardized in 1971
- FTP is built on a client-server model
- Transfer is not encrypted
- Not secure.

Secure file transfer

- Two families of secure file transfer building on FTP
  - FTPS
  - SFTP

FTPS

- FTPS (FTP+TLS)
- Operating system agnostic
- Can transfer text or binary

SFTP

- SFTP (SSH + FTP)
- Binary transfer only
- Designed for Unix based systems although there are utilities for other operating systems

Discussion questions

1. What are the use cases for SSH? Is it a reasonable tradeoff to not use certificates and PKI?
2. Many browsers support ftp. ftp://URL. Does your favorite browser? What is required to use ftp on a browser?

Outline

- Cryptography
- Key exchange
- Public Key Infrastructure and certificates
- Transport Layer Security (TLS)
- DNSSEC
- Secure Shell
- Secure File Transfer
- **Intrusion Detection**

Intrusion Detection Systems (IDS)

- Host based.
- Network based

Host based IDS

- One type is better known as a virus scanner.
  - Runs on physical or virtual machine under control of an operating system.
  - Looks for anomalous signatures of files
  - Relies on a database of known attack signatures
- Second type is container security scanner
  - Examines manifests of containers to determine whether any dependencies have known vulnerabilities.

Network based IDS

- Specialized machine that monitors all network traffic
- Looks for attack patterns
  - Port scans
  - Failed login
  - Other anomalous traffic patterns
- May generate false positives
- Because network traffic is very diffuse difficult to detect anomalous patterns

Discussion questions

1. Virus scanners look for anomalous signatures. What is an anomalous signature of a file?
2. Who is informed when the network IDS detects a potential intrusion?