CSIT988/CSIT488
Security, Ethics and Professionalism
Week 11: Protection Mechanisms

Subject Coordinator: *Dr Khoa Nguyen*

School of Computing and Information Technology

Autumn 2025

Learning Objectives

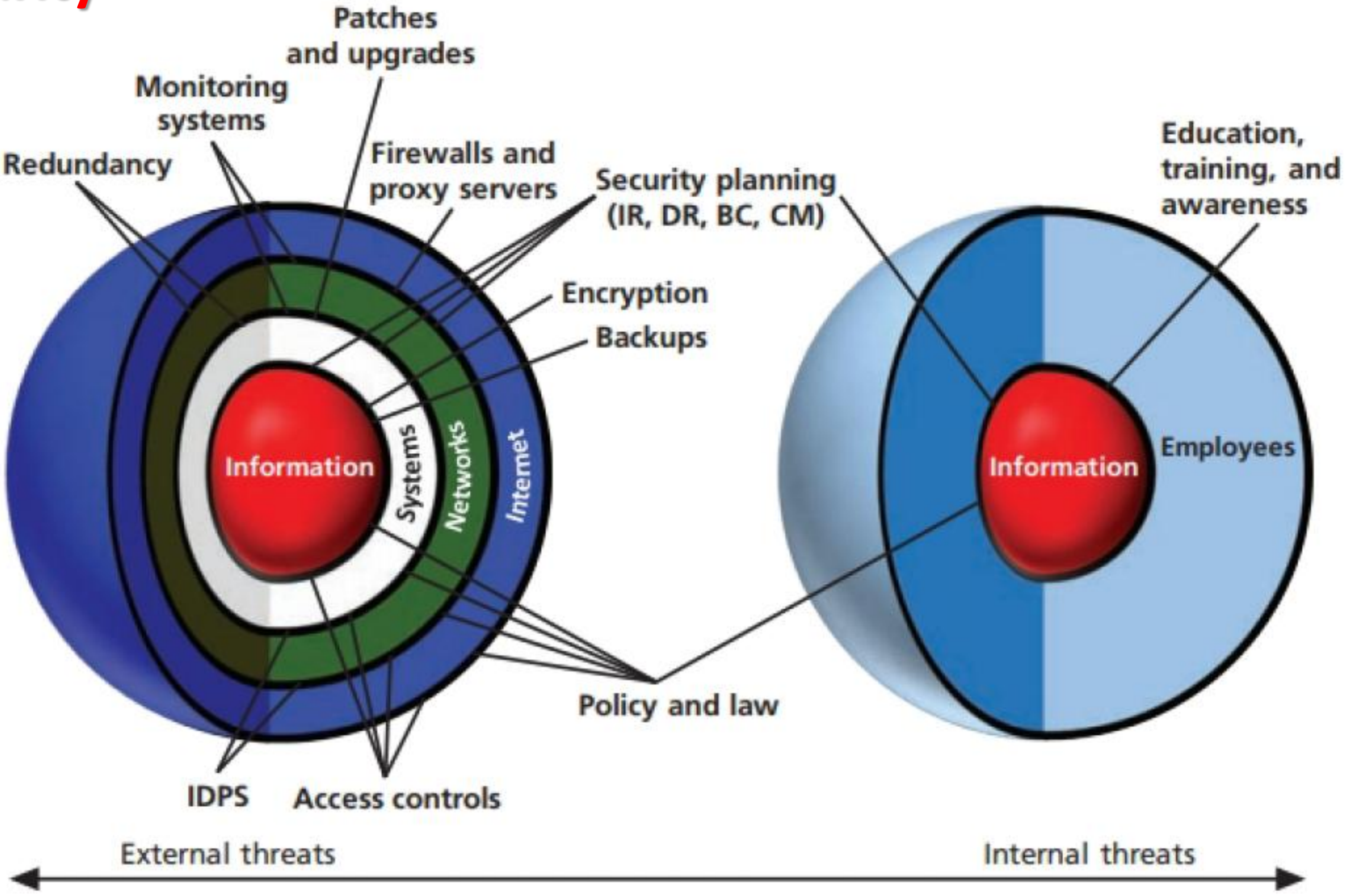
- Describe the various access control approaches, including authentication, authorization, and biometric access controls
- Identify the various types of firewalls and the common approaches to firewall implementation
- Identify and describe the types of intrusion detection systems and the strategies on which they are based
- Wireless network protection
- Explain cryptography and the encryption process, and compare and contrast symmetric and asymmetric encryption

Reference: Chapter 10 of the textbook

Introduction to Protection Mechanisms

- **Technical controls**
  - An essential part of information security programs
  - Insufficient if used alone
  - Must be combined with sound policy and education, training, and awareness efforts
- Examples of technical security mechanisms: access controls, firewalls, dial-up protection, intrusion detection systems, scanning and analysis tools, and encryption systems

Sphere of Security

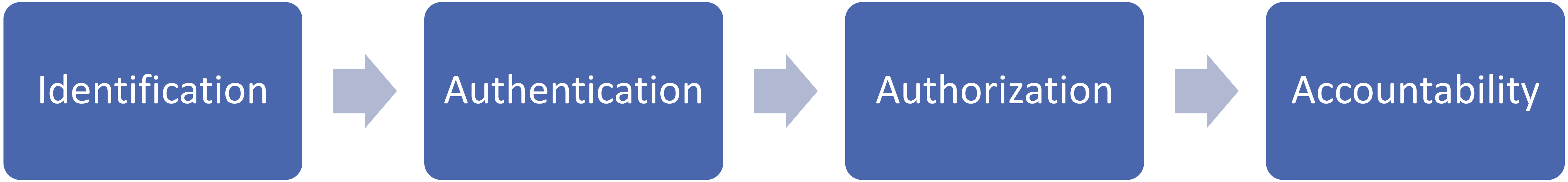


Access Controls

The four processes of access control

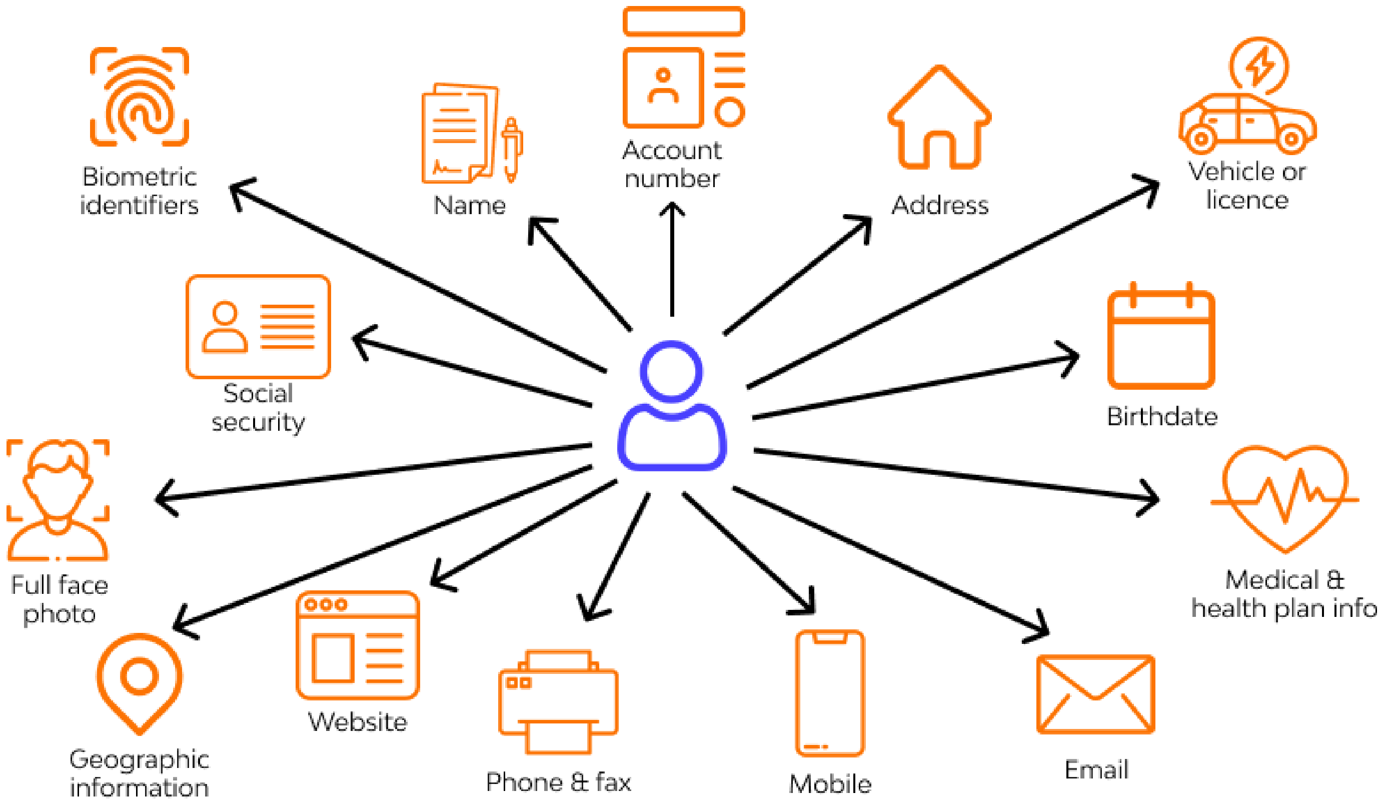
- **Identification**: Obtaining the identity of the entity requesting access to a logical or physical area
- **Authentication**: Confirming the identity of the entity seeking access to a logical or physical area
- **Authorization**: Determining which actions that an entity can perform in that physical or logical area
- **Accountability**: Documenting the activities of the authorized individual and systems

A successful access control approach always incorporates all four elements.



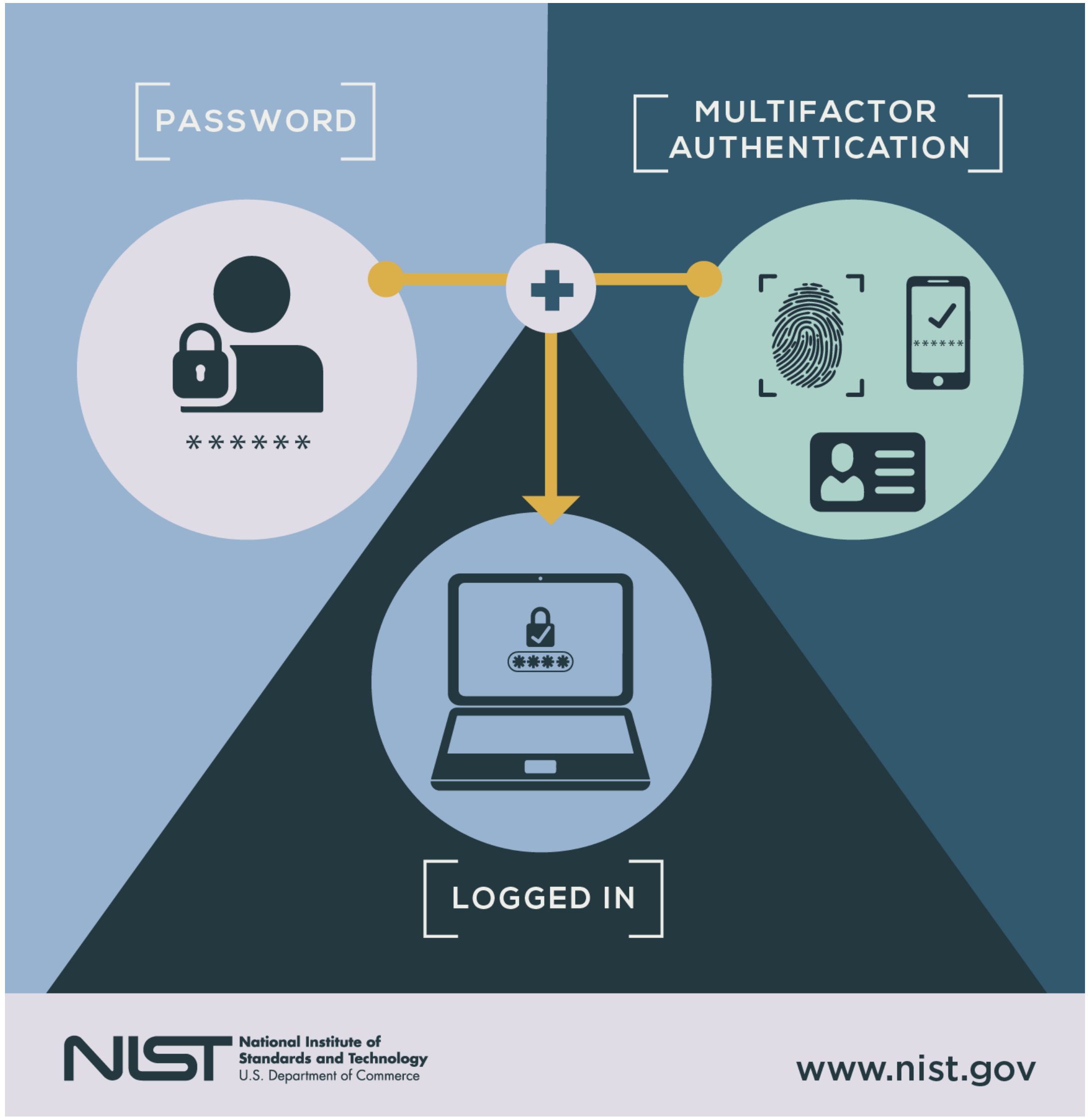
Identification

- A mechanism that provides information about a supplicant that requests access
- **Identifier (ID)**
  - ➢ The label applied to the supplicant
  - ➢ Must be a unique value that can be mapped to one and only one entity within the security domain
- **Examples:** name, first initial and surname



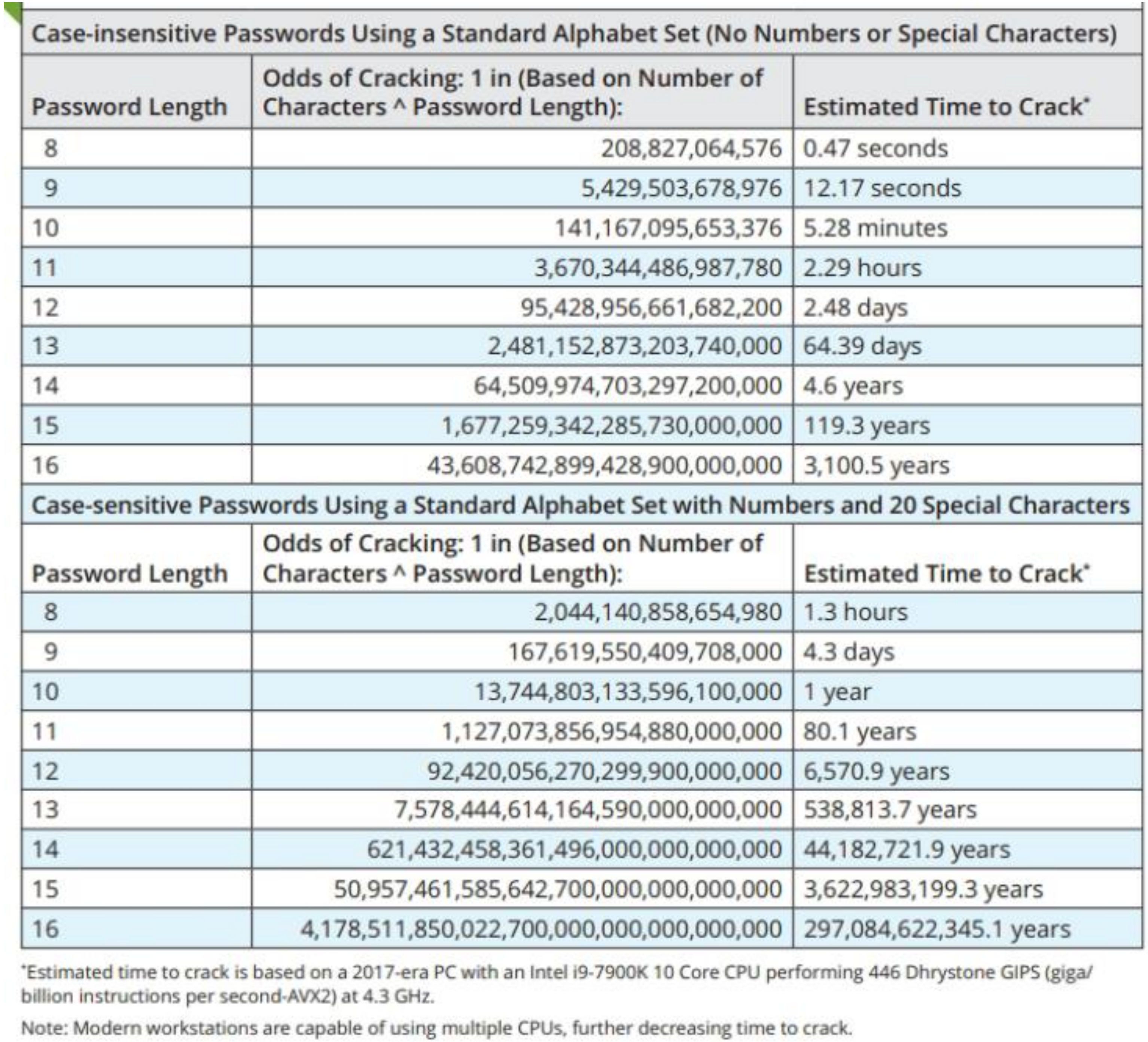
Authentication

- Authentication mechanism types
  - **Something you know:** password, passphrase
  - **Something you have:** cryptographic token or smart card
  - **Something you are:** fingerprints, retina and iris scans
  - **Something you produce:** voice, signature
- Strong authentication: Use at least two different authentication mechanism types (i.e., Multi-factor Authentication)


PASSWORD
******
MULTIFACTOR AUTHENTICATION
******
****
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

Something you know: A password, passphrase, or other unique code

- **Password:** a private word or combination of characters that only the user should know
- **Passphrase:** a plain-language phrase, typically longer than a password, from which a virtual password is derived
- Passwords should be at least 10 characters long and contain at least one number and one special character



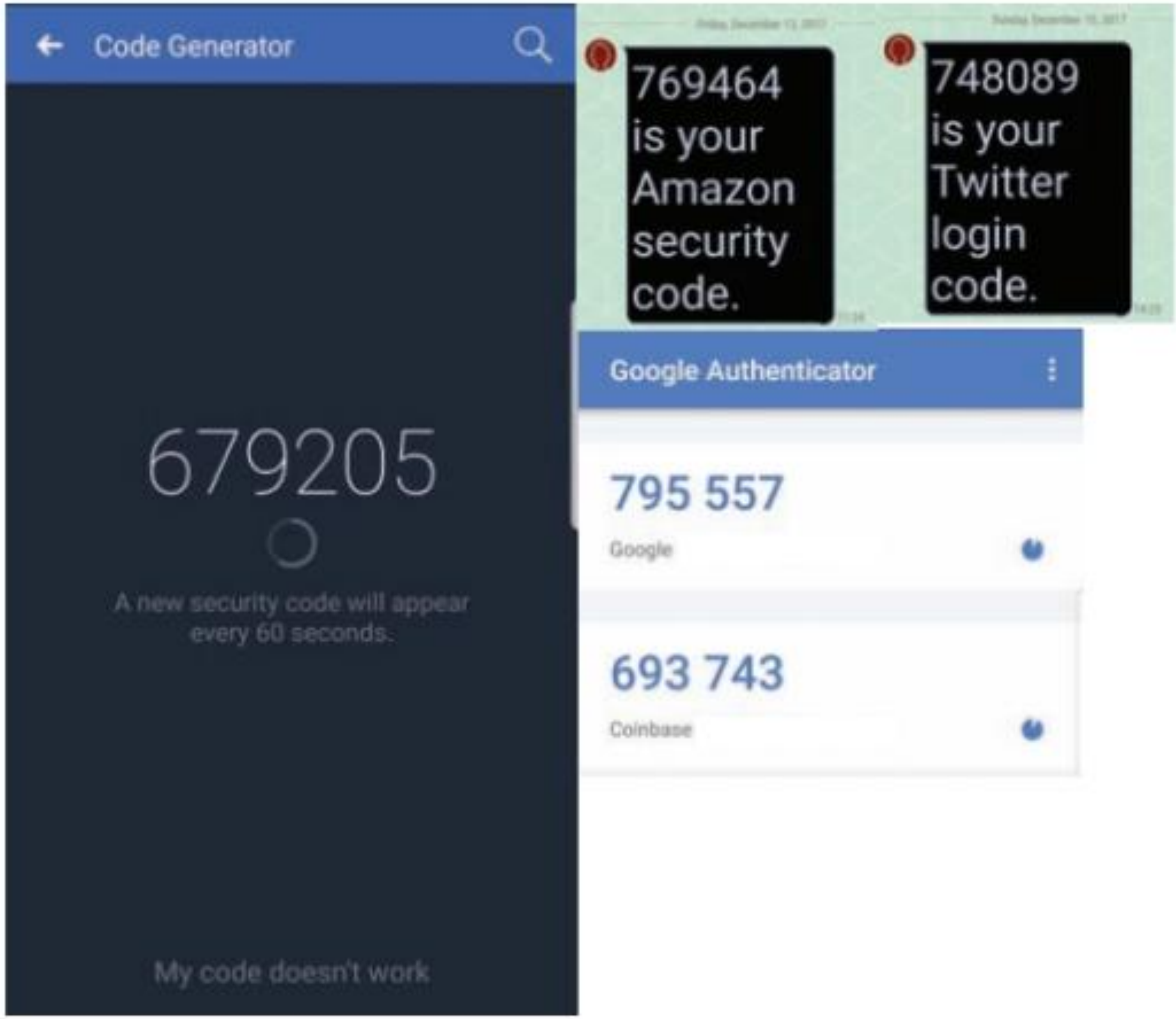
Case-insensitive Passwords Using a Standard Alphabet Set (No Numbers or Special Characters)		
Password Length	Odds of Cracking: 1 in (Based on Number of Characters ^ Password Length):	Estimated Time to Crack*
8	208,827,064,576	0.47 seconds
9	5,429,503,678,976	12.17 seconds
10	141,167,095,653,376	5.28 minutes
11	3,670,344,486,987,780	2.29 hours
12	95,428,956,661,682,200	2.48 days
13	2,481,152,873,203,740,000	64.39 days
14	64,509,974,703,297,200,000	4.6 years
15	1,677,259,342,285,730,000,000	119.3 years
16	43,608,742,899,428,900,000,000	3,100.5 years
Case-sensitive Passwords Using a Standard Alphabet Set with Numbers and 20 Special Characters		
Password Length	Odds of Cracking: 1 in (Based on Number of Characters ^ Password Length):	Estimated Time to Crack*
8	2,044,140,858,654,980	1.3 hours
9	167,619,550,409,708,000	4.3 days
10	13,744,803,133,596,100,000	1 year
11	1,127,073,856,954,880,000,000	80.1 years
12	92,420,056,270,299,900,000,000	6,570.9 years
13	7,578,444,614,164,590,000,000,000	538,813.7 years
14	621,432,458,361,496,000,000,000,000	44,182,721.9 years
15	50,957,461,585,642,700,000,000,000,000	3,622,983,199.3 years
16	4,178,511,850,022,700,000,000,000,000	297,084,622,345.1 years

*Estimated time to crack is based on a 2017-era PC with an Intel i9-7900K 10 Core CPU performing 446 Dhrystone GIPS (giga/billion instructions per second-AVX2) at 4.3 GHz.

Note: Modern workstations are capable of using multiple CPUs, further decreasing time to crack.

Something you have

- Something that the user or system possesses
- Examples:
  - ➢ A card, key, or token
  - ➢ A dumb card (such as an ATM card) with magnetic stripes
  - ➢ A smart card containing a processor
  - ➢ A cryptographic token (a processor in a card that has a display)
  - ➢ Tokens may be either synchronous or asynchronous



A new security code will appear every 60 seconds.

769464 is your Amazon security code.

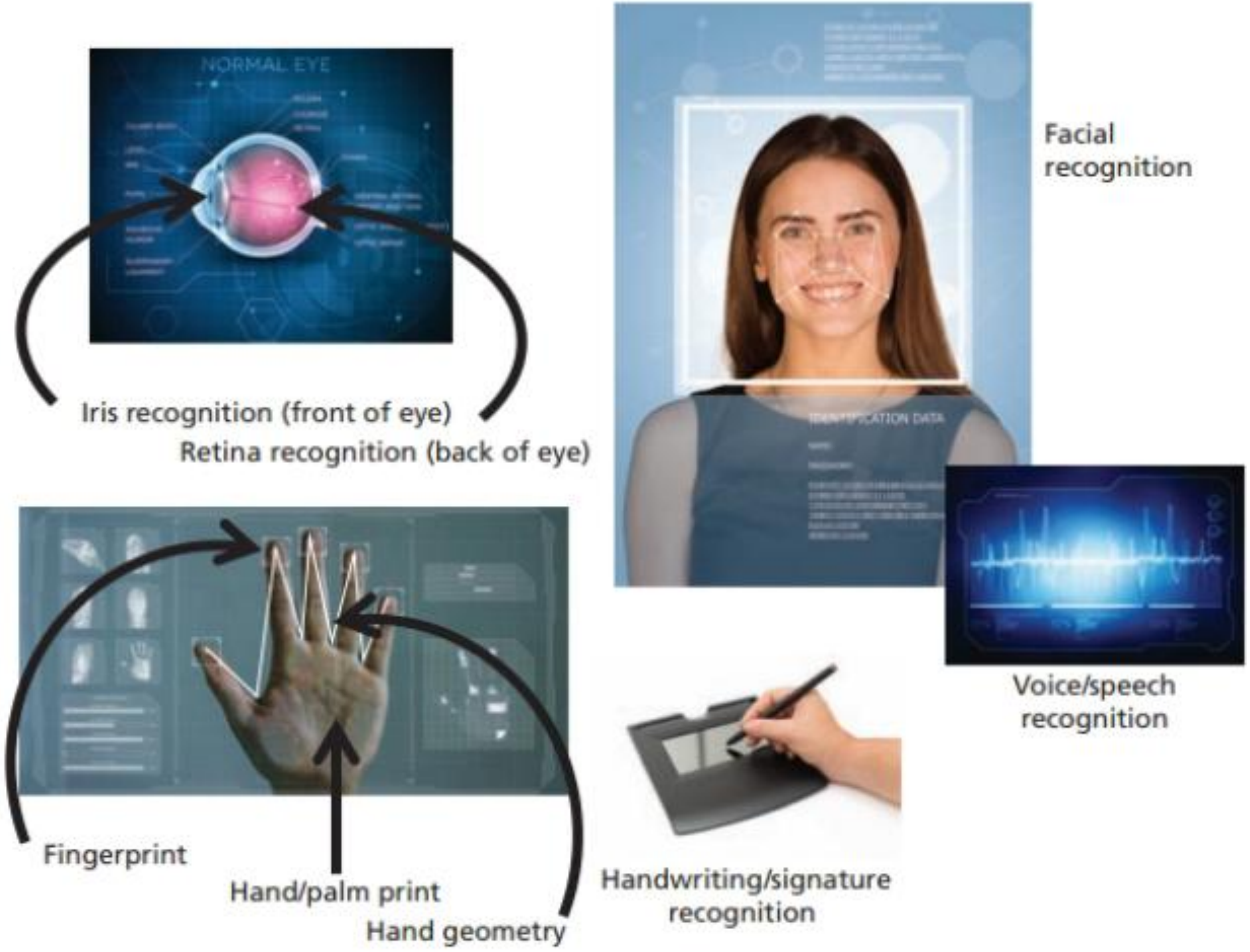
748089 is your Twitter login code.

Something you are: something inherent in the user that is evaluated using biometrics

- ➢Most technologies that scan human characteristics convert the images to obtain minutiae (unique points of reference that are digitized and stored in an encrypted format)

Something you produce: Something the user performs or produces

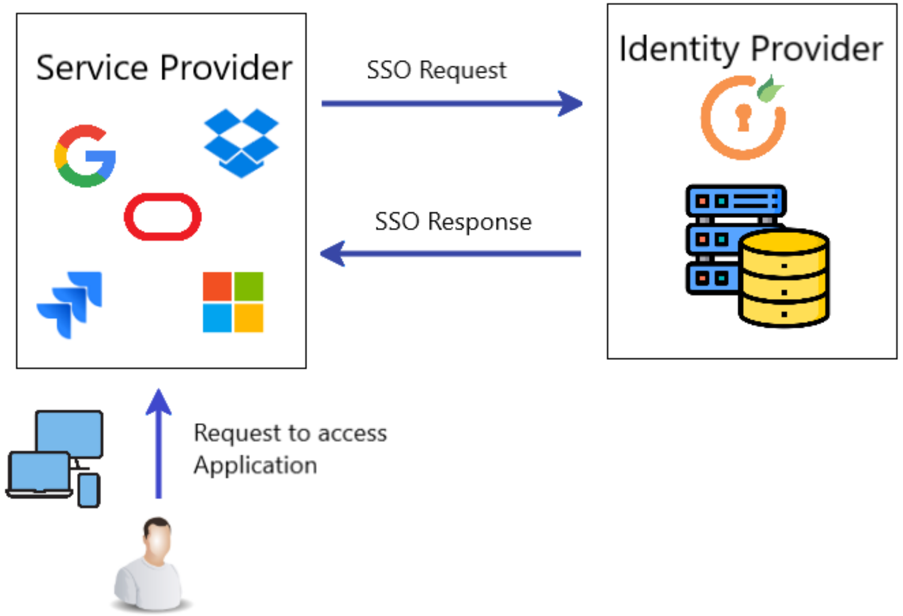
- ➢Includes technology related to signature recognition and voice recognition


NORMAL EYE
Iris recognition (front of eye)
Retina recognition (back of eye)
Facial recognition
Voice/speech recognition
Fingerprint
Hand/palm print
Hand geometry
Handwriting/signature recognition

Authorization

Three common authorization mechanisms:

- Authorization for each authenticated user, in which the system performs an authentication process to verify each entity and then grants access to resources to only that entity.
- Authorization for members of a group: the system matches authenticated entities to a list of group memberships and then grants access to resources based on the group's access rights.
- Authorization across multiple systems, in which a central authentication and authorization system verifies entity identity and grants a set of credentials to the verified entity. Example: Single Sign-On (SSO).



Accountability

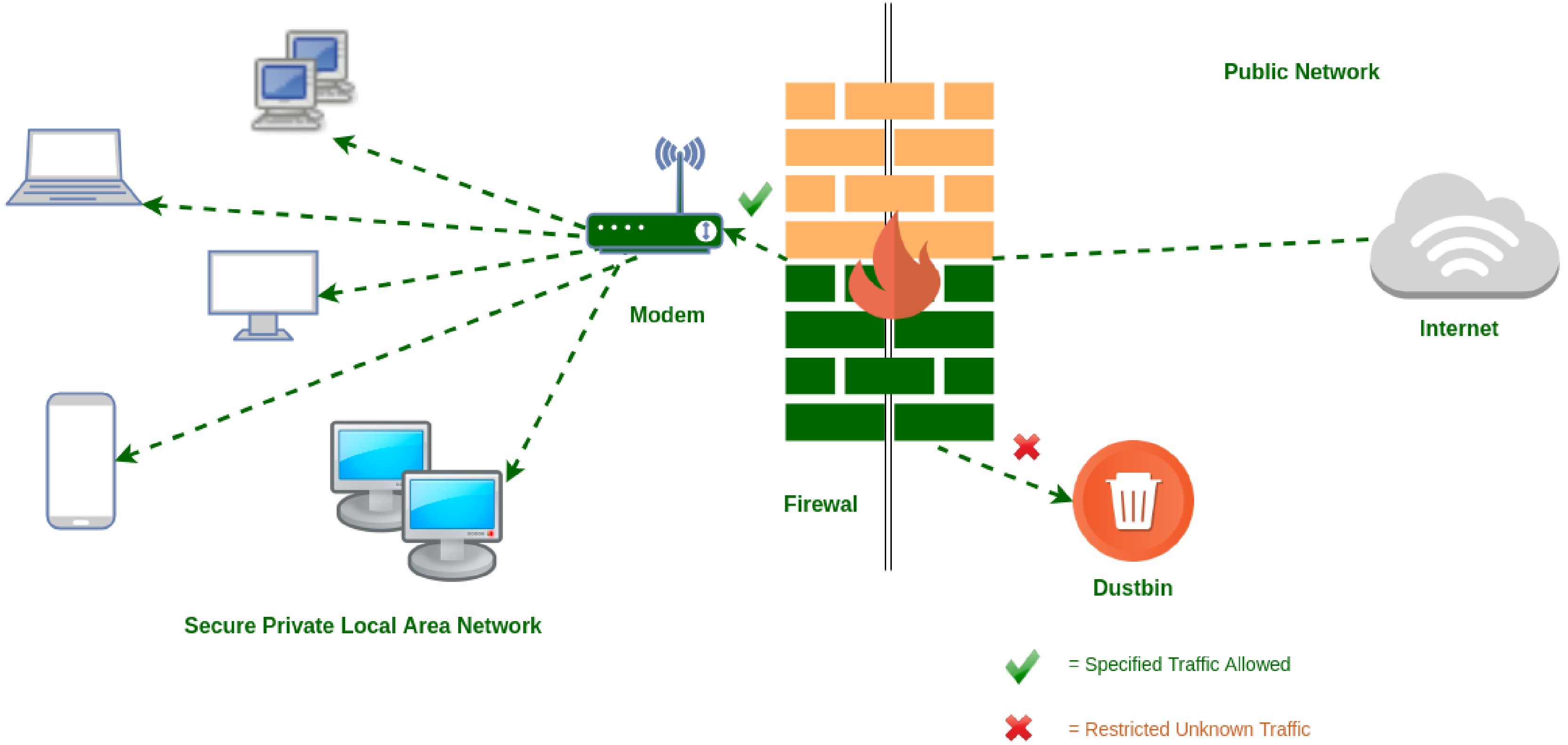
- Accountability ensures that all actions on a system can be attributed to an authenticated identity.
    - ➢These actions could be ones that the entity is authorized for, e.g., looking up or modifying certain data, or they could include unauthorized attempts to escalate privileges or read/modify data that is beyond its access level.
- Accountability is most often accomplished by implementing system logs and database journals and by auditing these records.
- Systems logs are records maintained by a particular system that has been configured to record specific information (e.g., failed access attempts, systems modifications). Logs have many uses, e.g., intrusion detection, determining the root cause of a system failure, tracking the use of a particular resource.
- To protect the log data, you must ensure that the servers that create and store the logs are secure.

Managing Access Controls

- **A formal access control policy**
  - Determines how access rights are granted to entities and groups
  - Includes provisions for periodically reviewing all access rights, granting access rights to new employees, changing access rights when job roles change, and revoking access rights as appropriate

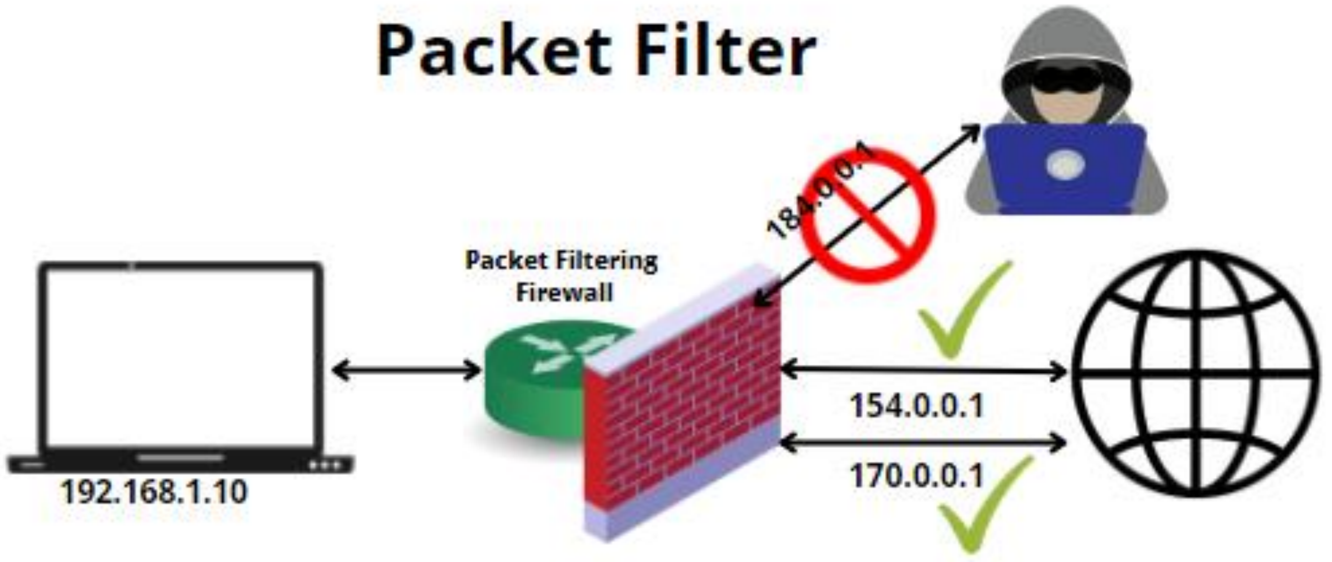
Firewalls

- In Infosec, a firewall is any device that prevents a specific type of information from moving between the untrusted network (e.g., the Internet), and the trusted network
- May be a separate computer system, a service running on an existing router or server, or a separate network with a number of supporting devices


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

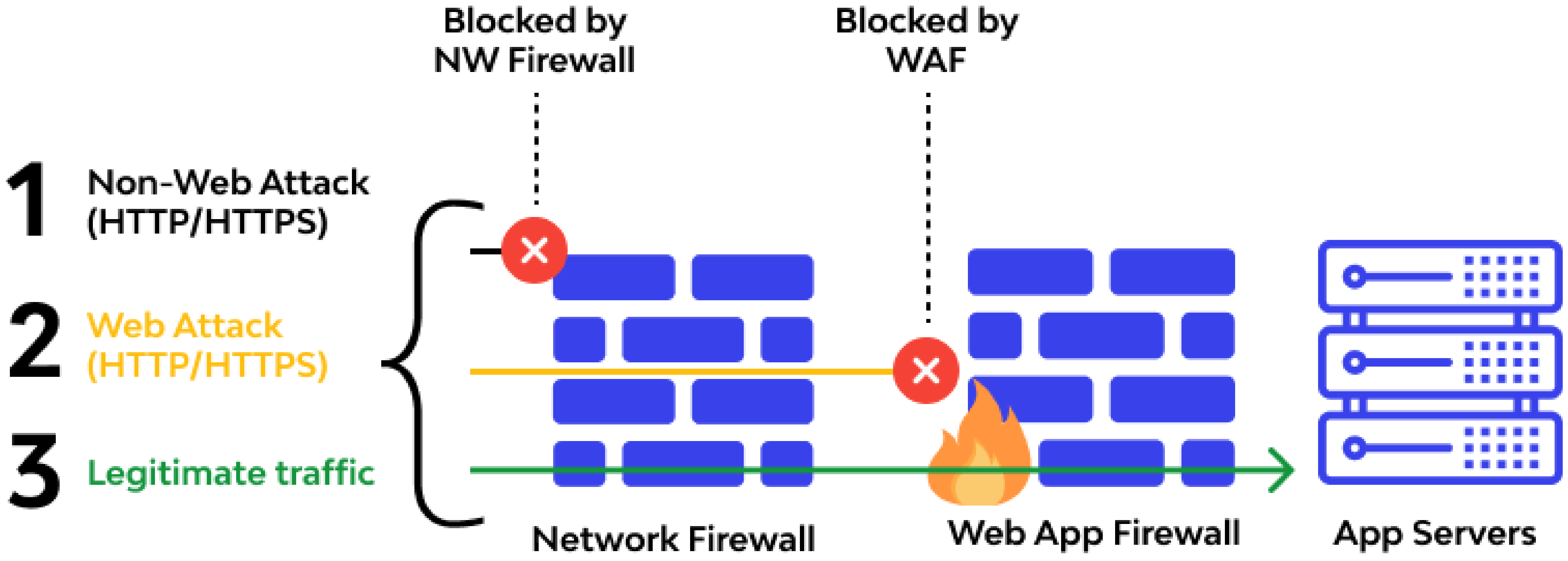
The Development of Firewalls: Packet Filtering Firewalls

- **Packet filtering firewalls:** The first generation of firewalls
  - ➢ Simple networking devices that filter packets by examining every incoming and outgoing packet header
  - ➢ Selectively filter packets based on values in the packet header
  - ➢ Can be configured to filter based on IP address, type of packet, port request, and/or other elements present in the packet



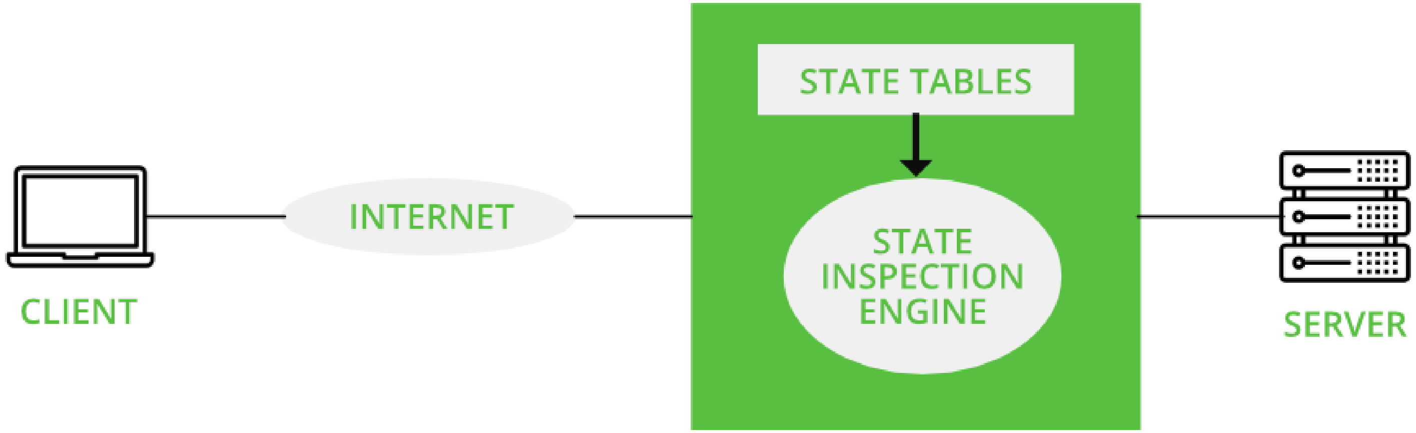
The Development of Firewalls: Application-Level Firewalls

- **Application-level firewalls:** Second generation of firewalls
  - ➢ Work like packet-filtering firewalls, but at the application layer
  - ➢ Commonly used in conjunction with filtering firewalls
  - ➢ Disadvantage: designed for a specific application-layer protocol



The Development of Firewalls: Stateful Inspection Firewalls

- **Stateful inspection firewalls:** Third generation of firewalls
  - ➢ Keeps track of network connections between internal and external systems using a state table. State tables track the state and context of packets exchanged by recording which station sent which packet and when
  - ➢ If the firewall receives an incoming packet that it cannot match in its state table, it defaults to its access control list (ACL) to determine whether to allow the packet to pass.
  - ➢ Disadvantage: additional processing requirements of managing and verifying packets against the state table, which can expose the system to a denial-of-service (DoS) attack

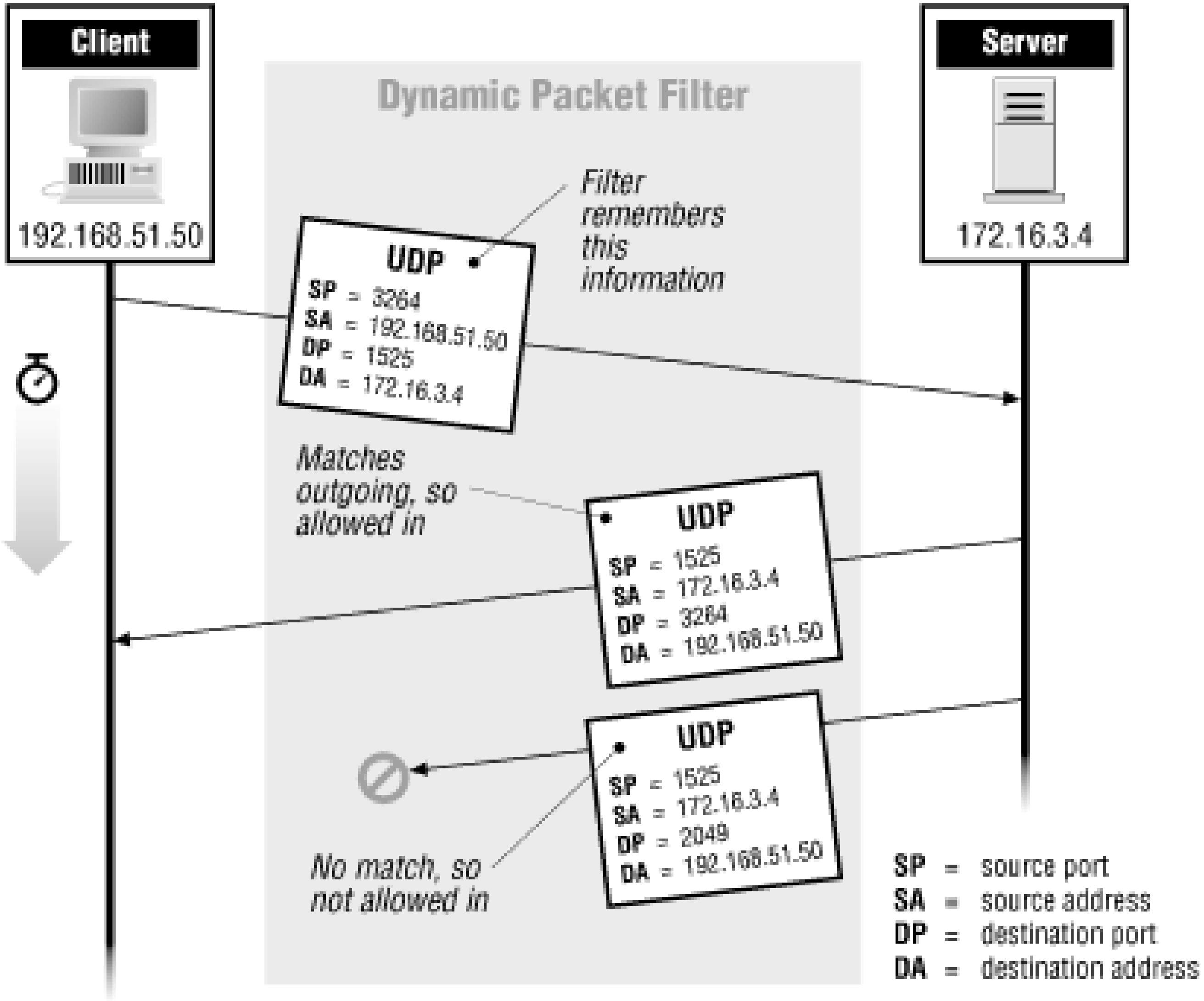


STATEFUL INSPECTION FIREWALL

The Development of Firewalls: Dynamic Packet Filtering Firewalls

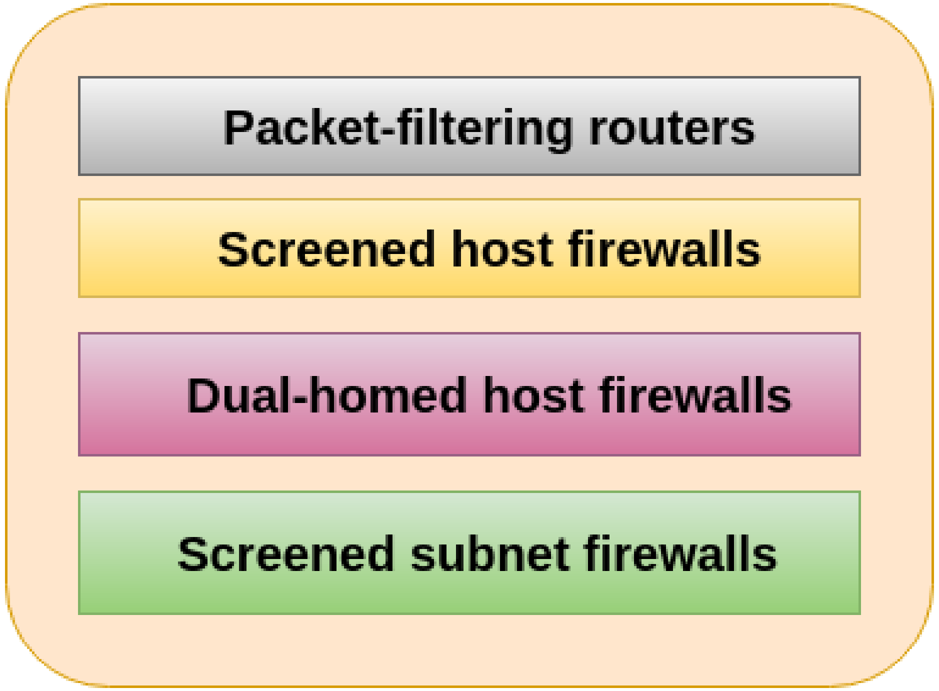
- **Dynamic packet filtering firewalls:** Fourth generation of firewalls
  - ➢ Allows only a particular packet with a specific source, destination, and port address to pass through the firewall
  - ➢ Understands how the protocol functions, and opens and closes firewall pathways

- **Static filter:** each packet is evaluated independently.
- **Dynamic filter:** the decision depends on what packets have already been through the firewall.

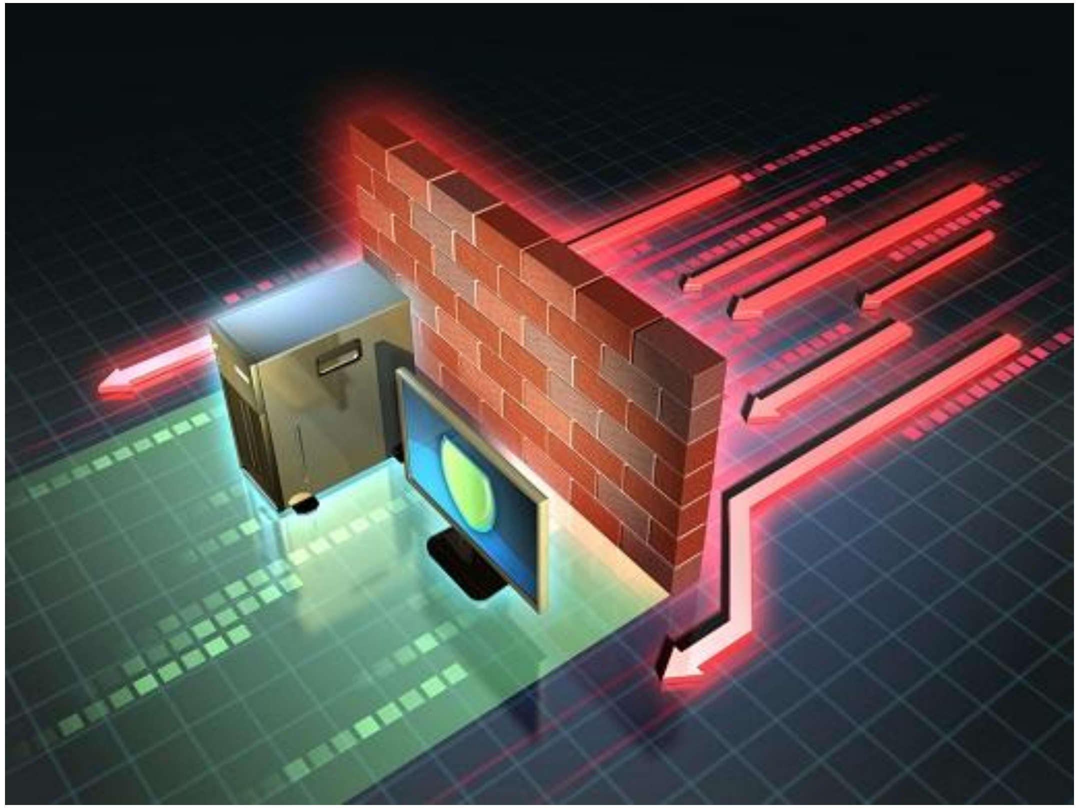


Firewall Architectures

- Each of the firewall generations can be implemented in several architectural configurations, which could be mutually exclusive or be combined
- **Common architectural implementations**

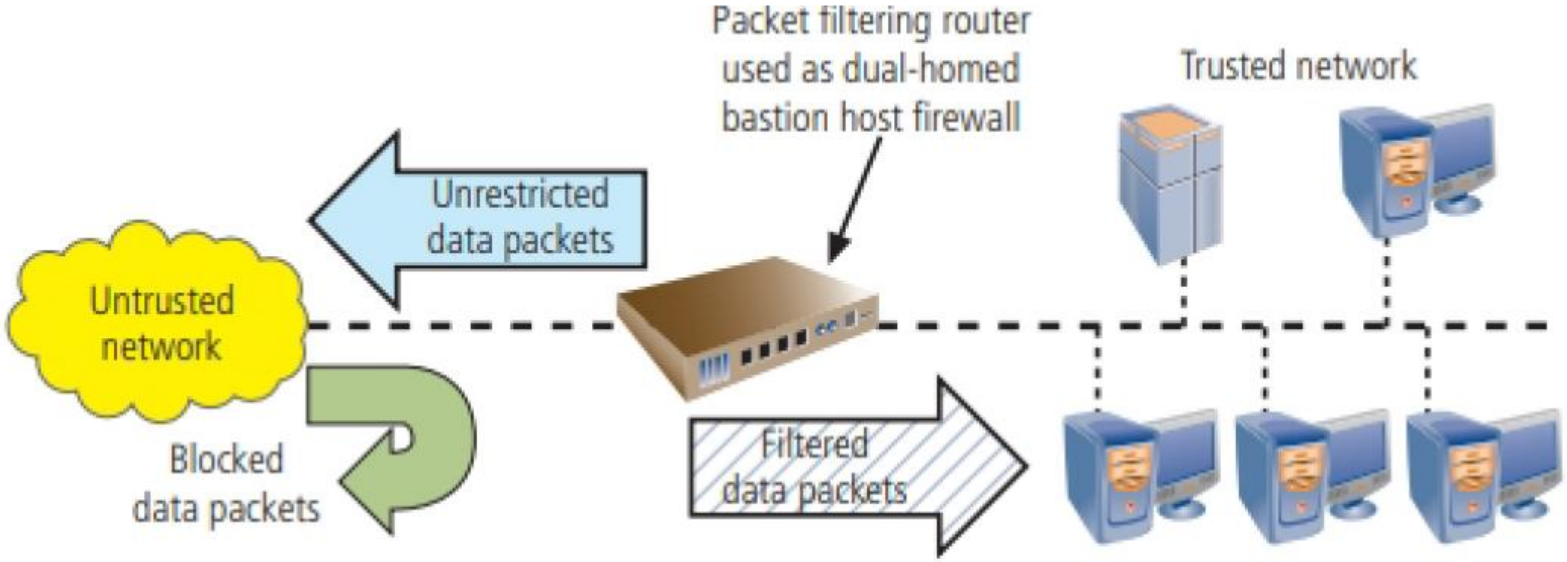


Architectural Implimentation



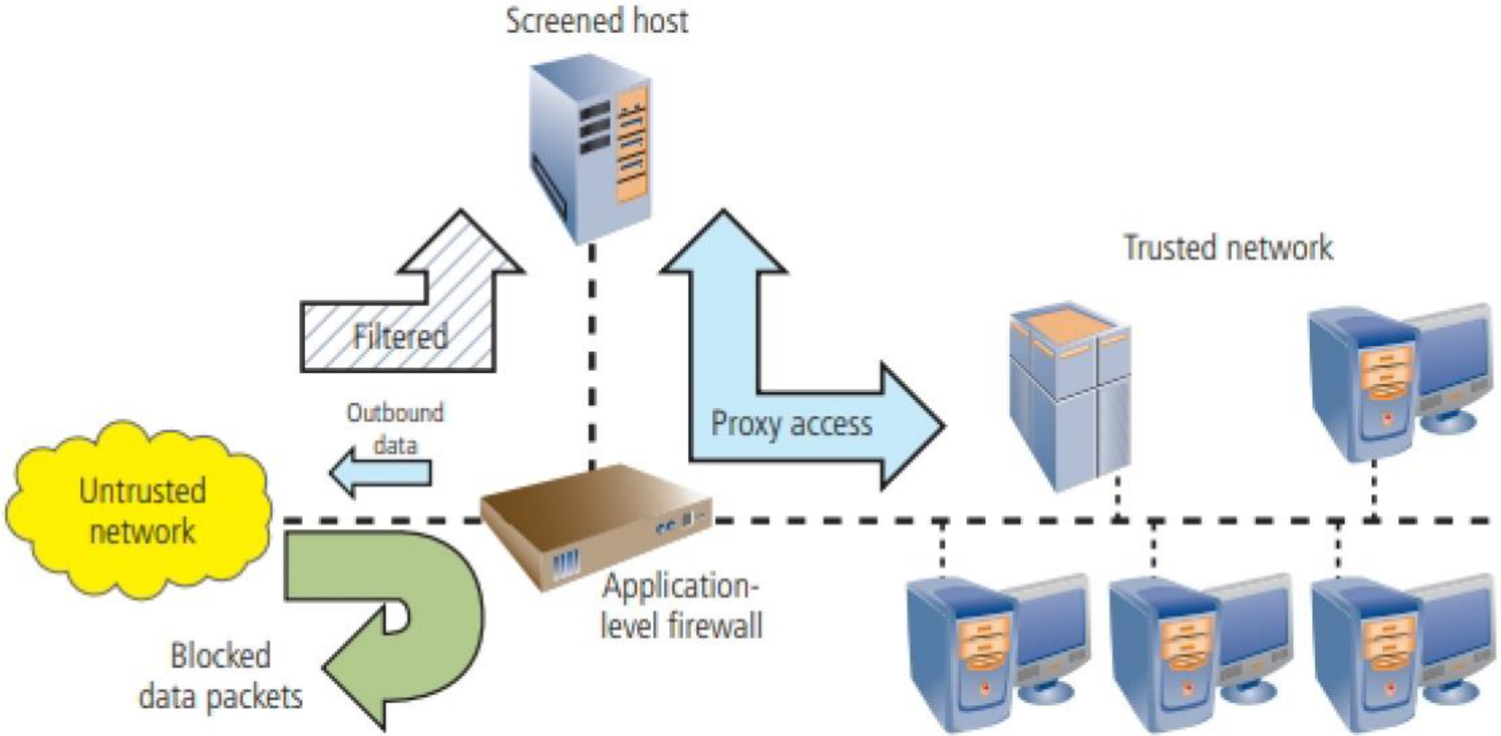
Firewall Architectures: Packet Filtering Routers

- **Packet filtering routers:** Most organizations with an Internet connection use some form of router between their internal networks and the external service provider. Many of these packet filtering routers can be configured to block packets that the organization does not allow into the network.
  - ➢ Simple but effective means to lower the risk of external attacks
  - ➢ Lacks auditing and strong authentication, and the complexity of the ACL used to filter packets can degrade network performance


Packet filtering router used as dual-homed bastion host firewall
Trusted network
Unrestricted data packets
Untrusted network
Blocked data packets
Filtered data packets

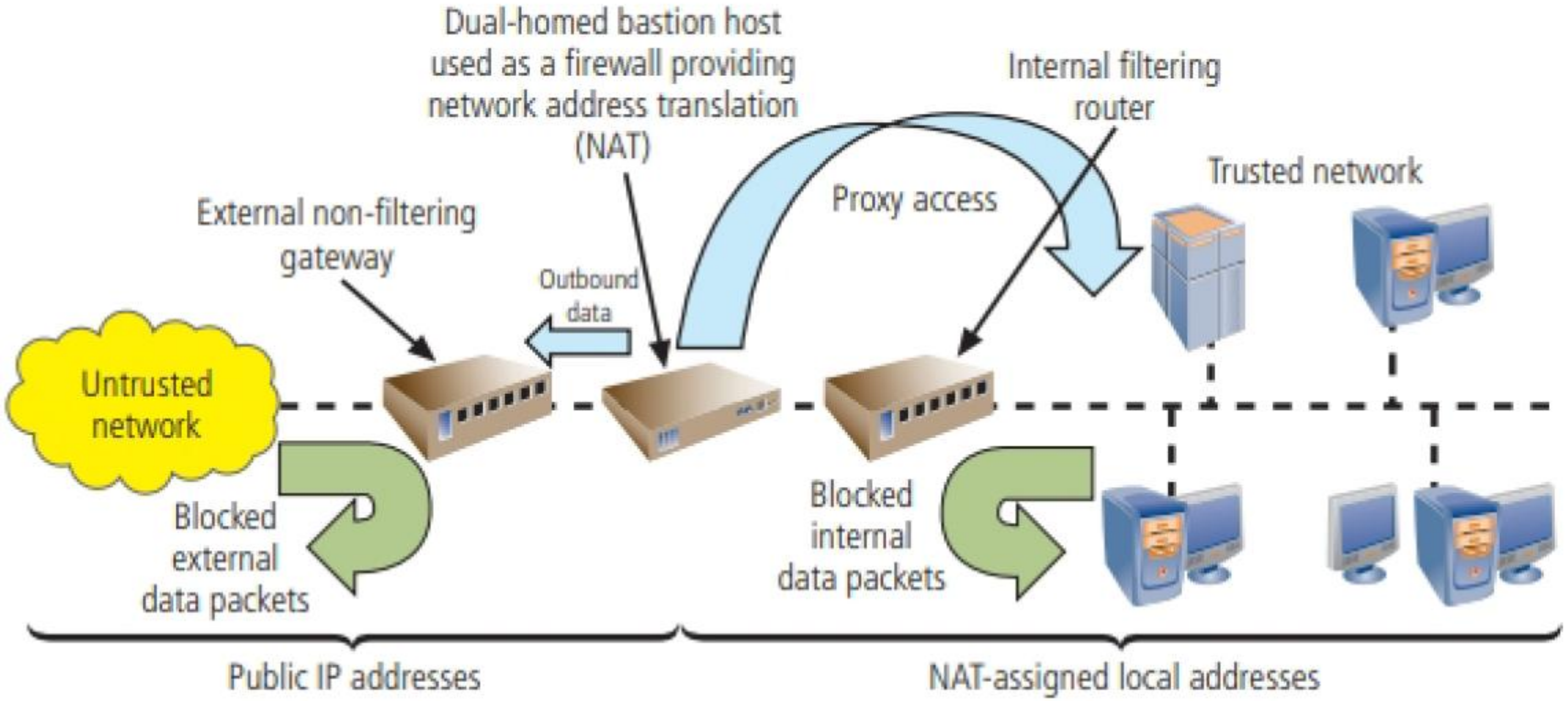
Firewall Architectures: Screened Host Firewalls

- **Screened host firewalls:** Combine the packet filtering router with a separate, dedicated firewall (e.g., an application proxy server). This approach allows the router to screen packets to minimize traffic and load on the internal proxy
  - ➢ The application proxy examines an application layer protocol
  - ➢ The separate host is often referred to as a bastion host



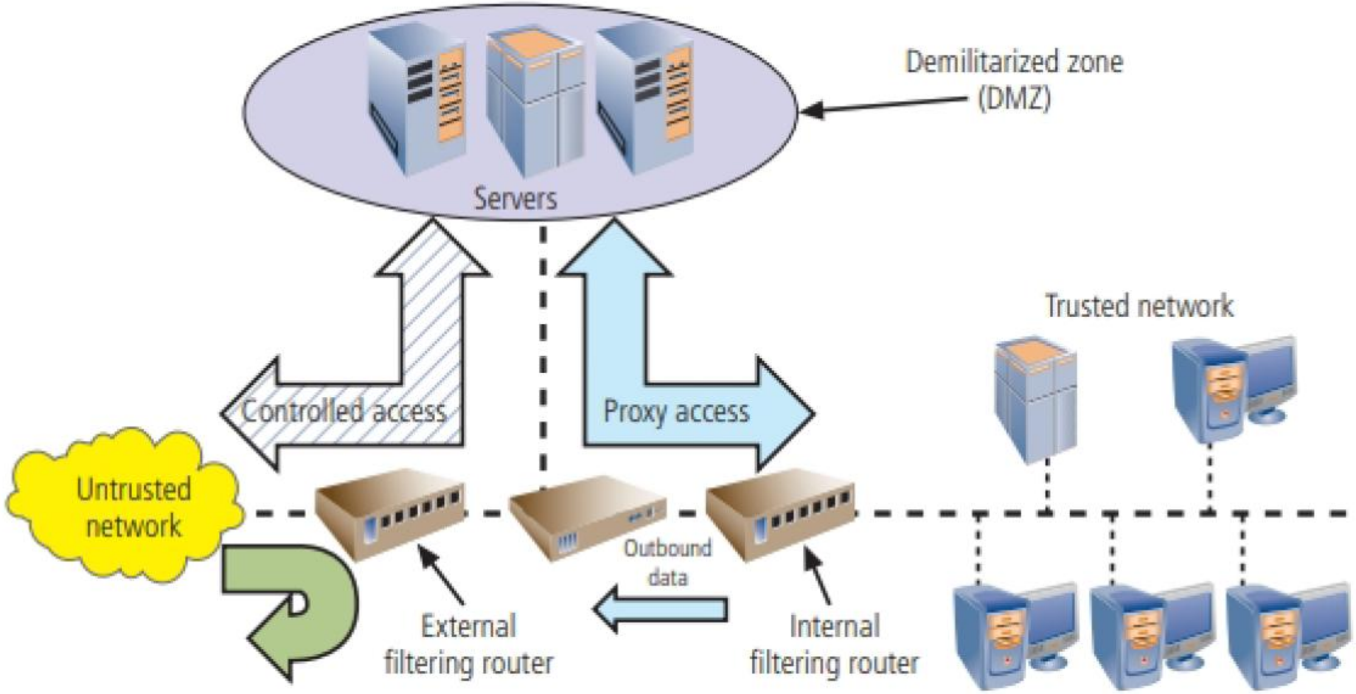
Firewall Architectures: Dual-Homed Host Firewalls

- **Dual-homed host firewalls:** The bastion host contains two network interfaces: one is connected to the external network and one is connected to the internal network. All traffic must travel through the firewall.
  - ➢ Network-address translation (NAT) is often implemented with this architecture, which converts external IP addresses to special ranges of internal IP addresses


Dual-homed bastion host used as a firewall providing network address translation (NAT)
Internal filtering router
Trusted network
Proxy access
External non-filtering gateway
Outbound data
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT-assigned local addresses

Firewall Architectures: Screened-Subnet Firewalls

- **Screened-Subnet Firewalls:** One or more internal bastion hosts located behind a packet filtering router, with each host protecting the trusted network. The first model uses two filtering routers, with one or more dual-homed bastion hosts between them. The second model routes connections as follows:
  - ➢ Connections from untrusted network are routed via an external filtering router
  - ➢ Connections from the untrusted network are routed into—and then out of—a routing firewall to the separate network segment known as the DMZ
  - ➢ Connections into the trusted internal network are allowed only from the DMZ bastion host servers



Selecting the Right Firewall

Questions to ask when evaluating a firewall:

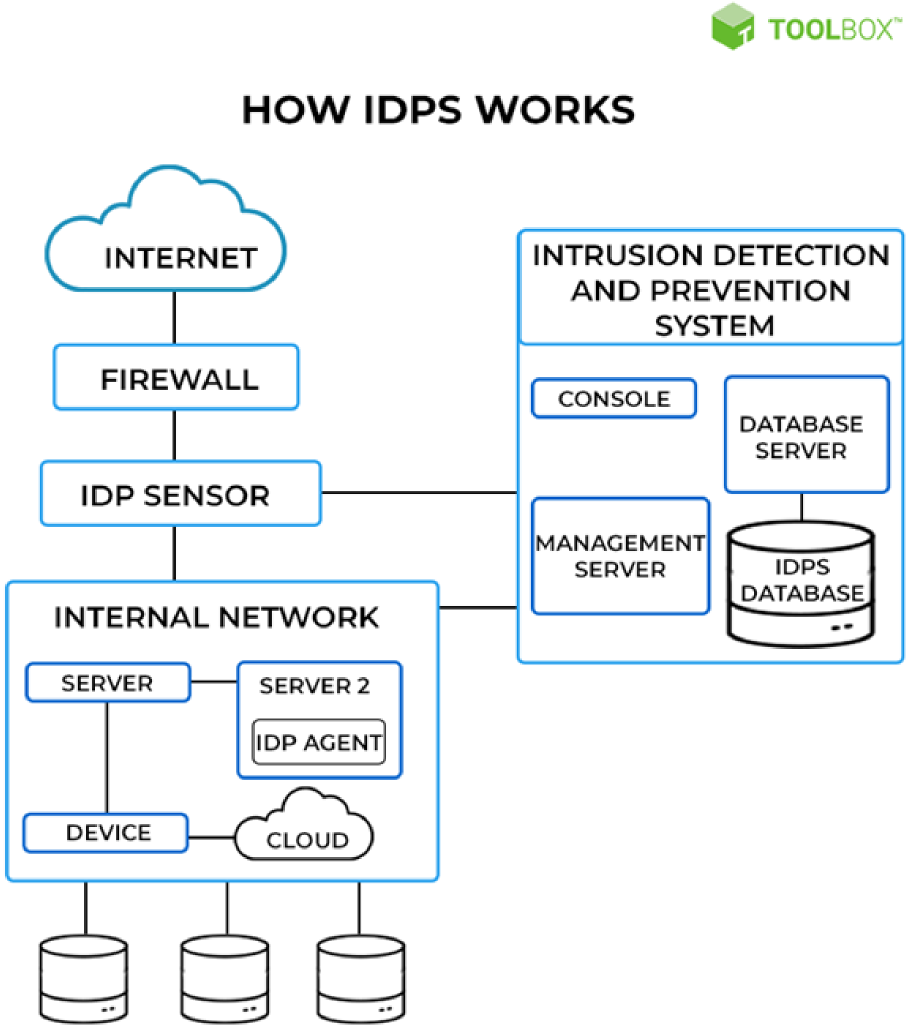
- Firewall technology: What type offers the right balance between protection and cost for the organization’s needs?
- Cost: What features are included in the base price? At extra cost? Are all cost factors known?
- Maintenance: How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
- Future growth: Can the candidate firewall adapt to the growing network in the target organization?

Managing Firewalls

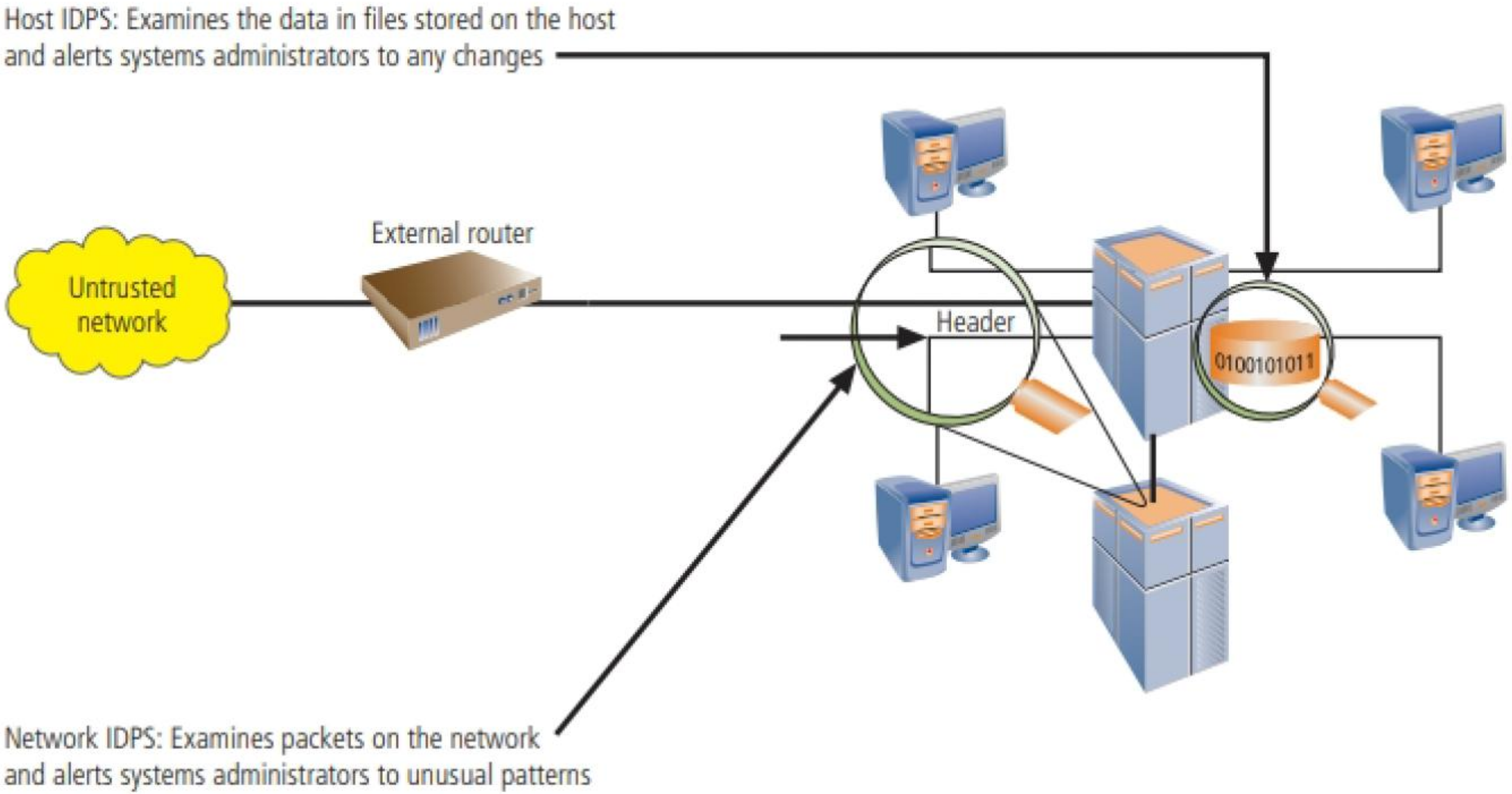
- Any firewall device must have its own set of configuration rules that regulates its actions. A policy regarding the use of a firewall should be articulated before it is made operable.
- Configuring firewall rule sets can be very complicated. Logic errors in the preparation of the rules can cause unintended behavior. Each firewall rule must be carefully crafted, placed into the list in the proper sequence, debugged, and tested.
- The need to balance performance against restrictions imposed by security practices is obvious in the use of firewalls. Organizations are much more willing to live with a potential risk than certain failure.
- Using a computer to protect a computer is fraught with problems that must be managed by careful preparation and continuous evaluation.

Intrusion Detection and Prevention Systems

- IDPSs work like burglar alarms. Administrators can choose the alarm level; Can be configured to notify administrators
- Systems that include intrusion prevention technology attempt to prevent the attack from succeeding by one of the following means: Terminating the network connection or the attacker's user session; Changing the security environment by reconfiguring network devices; Changing the attack's content to make it benign
- Like firewall systems, IDPSs require complex configurations to provide the level of detection and response desired

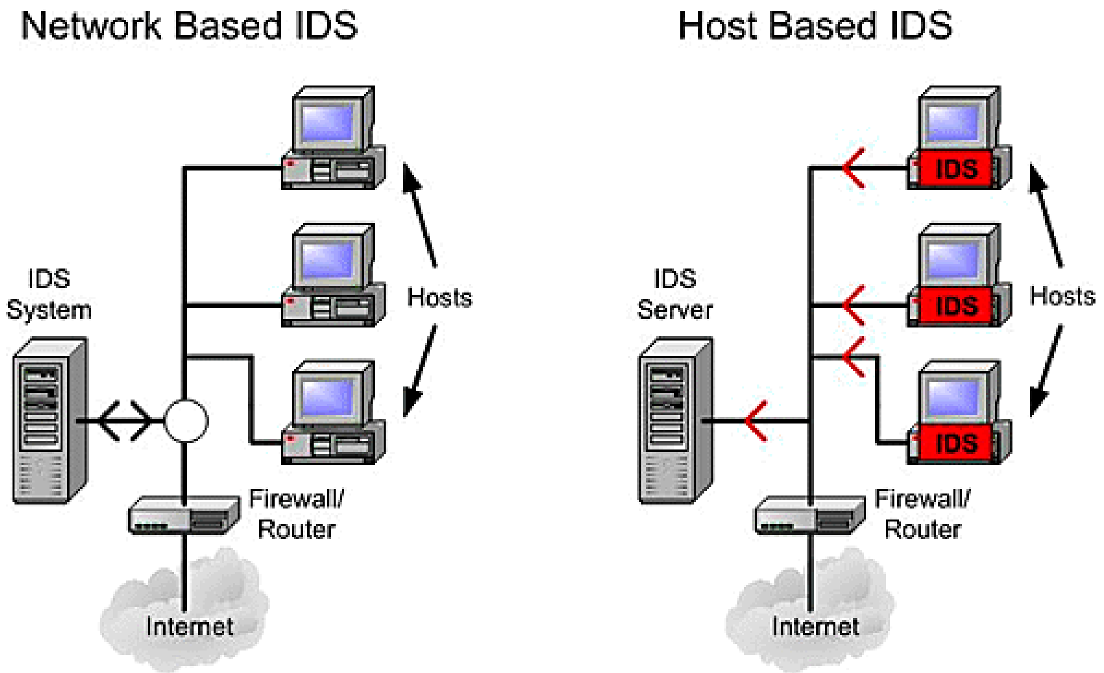


- **IDPSs types:**
  - Network-based to protect network information assets
  - Host based to protect server or host information assets


Host IDPS: Examines the data in files stored on the host and alerts systems administrators to any changes
External router
Untrusted network
Header
0100101011
Network IDPS: Examines packets on the network and alerts systems administrators to unusual patterns

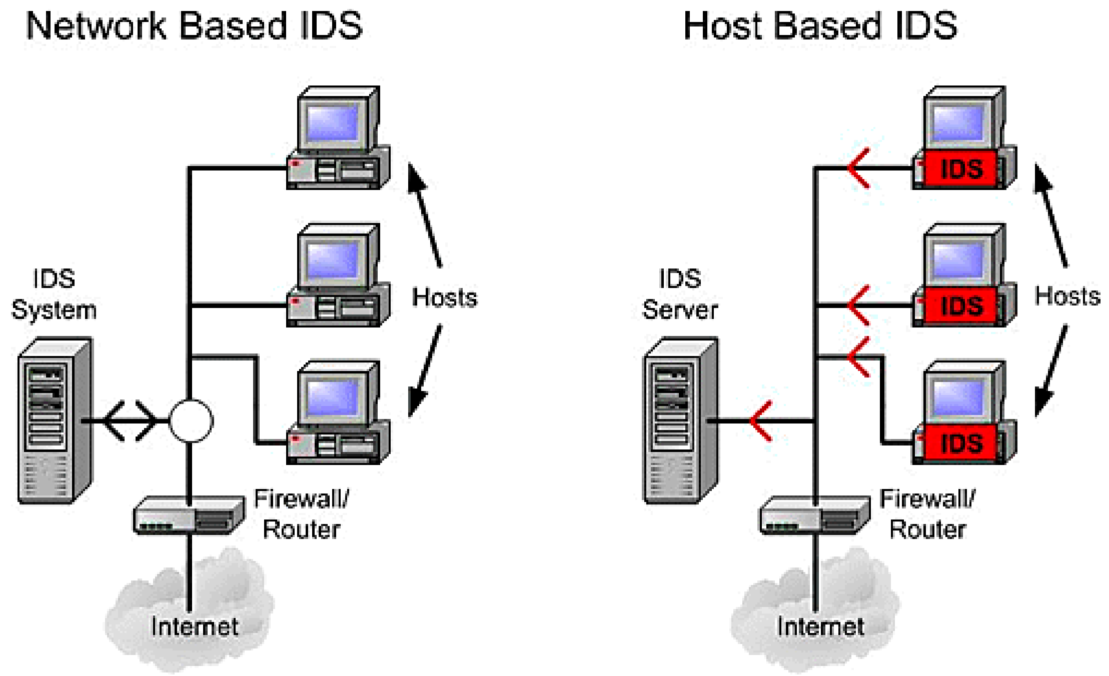
Host-Based IDPS

- Configures and classifies various categories of systems and data files
- IDPSs provide only a few general levels of alert notification
- Unless the IDPS is very precisely configured, benign actions can generate a large volume of false alarms
- Host-based IDPSs can monitor multiple computers simultaneously



Network-Based IDPS

- Monitors network traffic. Looks for patterns of network traffic
- When a predefined condition occurs, notifies the appropriate administrator
- Match known and unknown attack strategies against their knowledge base to determine whether an attack has occurred
- Yield many more false-positive readings than host-based IDPSs



Signature-Based IDPS and Anomaly-Based IDPS

- **IDPS detection methods:** Signature based; Statistical anomaly based

- IDPSs that use signature-based methods work like antivirus software
  - ➢ Examine data traffic for something that matches the signatures (preconfigured, predetermined attack patterns)
  - ➢ Signatures must be continually updated.
  - ➢ Another weakness is the time frame over which attacks occur.

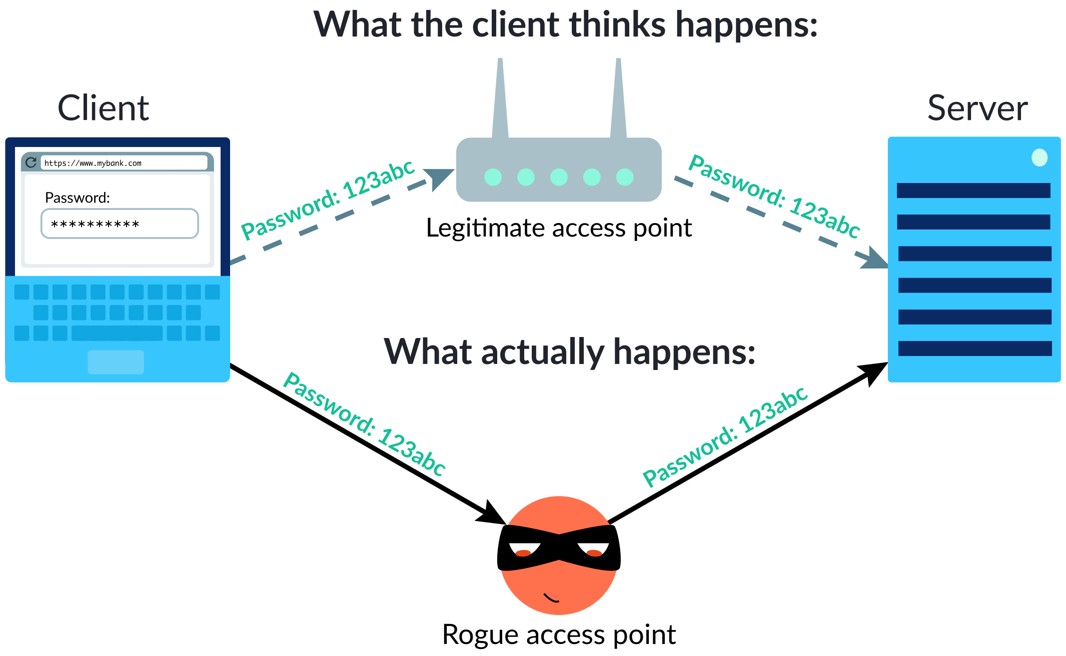
- Anomaly-based IDPSs – also known as behavior-based IDPSs
  - ➢ First collects data from normal traffic and establishes a baseline
  - ➢ Then periodically samples network activity, using statistical methods, and compares the samples to the baseline.
  - ➢ Able to detect new types of attacks
  - ➢ Require large overhead and processing capacity

Managing Intrusion Detection and Prevention Systems

- IDPSs must be configured using technical knowledge and adequate business and security knowledge to differentiate between routine circumstances and threats to the security of the organization's information assets.
- A properly configured IDPS can translate a security alert into different types of notification- for example, log entries for low-level alerts, e-mails for moderate-level alerts, and text messages or paging for severe alerts. A poorly configured IDPS may yield either information overload- causing the IDPS administrator to shut off the pager- or failure to detect an actual attack.
- Most IDPSs monitor systems by means of agents. An agent is a piece of software that resides on a system and reports back to a management server.
- Consolidated enterprise management service: A software allowing the security professional to collect data from multiple host-based and network-based IDPSs and look for patterns across systems and subnetworks.

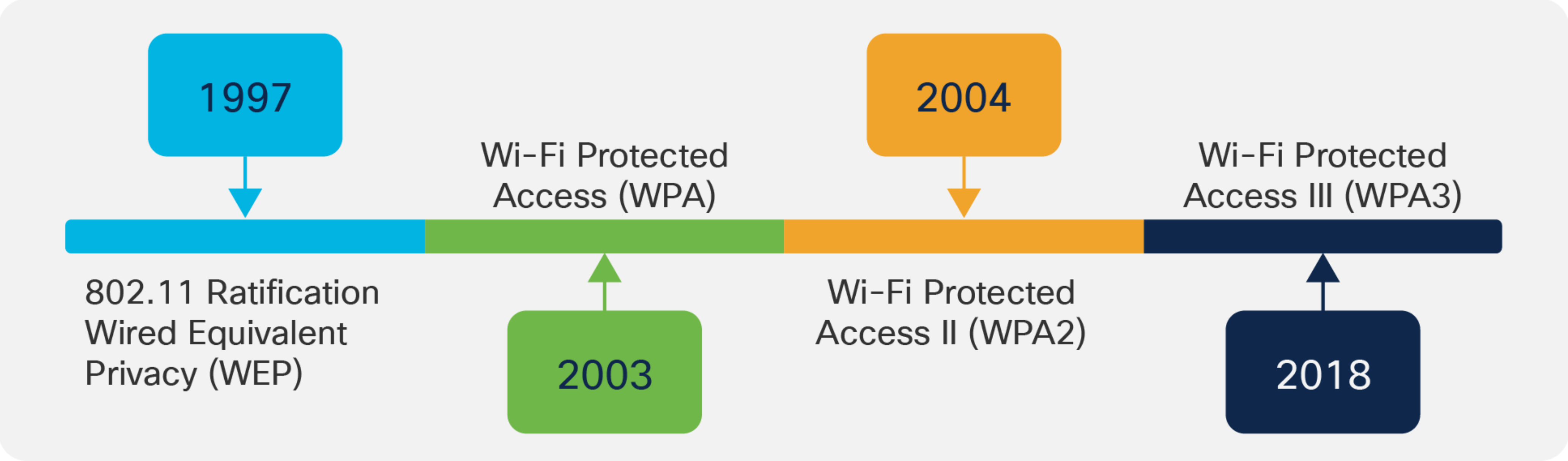
Wireless Networking Protection

- Most organizations that make use of wireless networks use an implementation based on the IEEE 802.11 protocol
- The size of a wireless network's footprint depends on the amount of power the transmitter/receiver wireless access points (WAP) emit
  - ➢ Sufficient power must exist to ensure quality connections within the intended area, but not allow those outside the footprint to connect
- **War Driving, Rogue WAP**
- Protocols used to secure wireless networks
  - ➢ Wired Equivalent Privacy (WEP)
  - ➢ Wi-Fi Protected Access (WPA)



Wired Equivalent Privacy (WEP)

- Provides a basic level of security to prevent unauthorized access or eavesdropping
- Does not protect users from observing each others’ data
- Has several fundamental cryptological flaws, resulting in vulnerabilities that can be exploited, which led to replacement by WPA


1997
802.11 Ratification Wired Equivalent Privacy (WEP)
Wi-Fi Protected Access (WPA)
2003
2004
Wi-Fi Protected Access II (WPA2)
Wi-Fi Protected Access III (WPA3)
2018

Wi-Fi Protected Access (WPA)

- WPA is an industry standard
  - Created by the Wi-Fi Alliance
- Some compatibility issues with older WAPs
- IEEE 802.11i
  - Has been implemented in products such as WPA2
    - WPA2 has newer, more robust security protocols based on the Advanced Encryption Standard
  - WPA/WPA2 provide increased capabilities for authentication, encryption, and throughput

- WP3, with increased security, has started replacing WPA2 since 2018

Cryptography

- Cryptography represents a sophisticated element of control that is often included in other InfoSec controls. Cryptographic techniques can help achieve:
  - Confidentiality: symmetric/asymmetric encryption
  - Integrity: hashing
  - Authentication + Non-Repudiation: digital signatures and MACs
  - Authorization: public-key infrastructure
- **Cryptography** describes the processes involved in encoding and decoding messages so that others cannot understand them
- **Cryptanalysis** is the process of deciphering the original message (or plaintext) from an encrypted message (or ciphertext), without knowing the algorithms and keys used to perform the encryption
- **Cryptology = Cryptography + Cryptanalysis**

Basic Cryptographic Concepts

- **Algorithm:** A mathematical formula or method used to convert an unencrypted message into an encrypted message
- **Cipher:** The transformation of the individual components of an unencrypted message into encrypted components
- **Ciphertext or cryptogram:** The unintelligible encrypted or encoded message resulting from an encryption
- **Plaintext**: The original unencrypted message and results from successful decryption
- **Cryptosystem:** The set of transformations that convert an unencrypted message into an encrypted message
- **Decipher:** To decrypt or convert ciphertext to plaintext
- **Encipher:** To encrypt or convert plaintext to ciphertext
- **Key:** The information used in conjunction with the algorithm to create the ciphertext from the plaintext

- **Steganography:** The process of hiding messages, usually within graphic images

Substitution Cipher

- **Common ciphers:** substitution, transposition, and XOR
- In a **substitution cipher**, you substitute one value for another
  - ➢ A monoalphabetic substitution uses only one alphabet. Example (Caesar cipher):

Input text: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Output text: DEFGHIJKLMNOPQRSTUVWXYZABC

Thus, a plaintext of BERLIN becomes EHUOLQ in ciphertext.

- ➢ A polyalphabetic substitution uses two or more alphabets

Transposition Cipher

- **Transposition cipher (or permutation cipher)**
  - ➢Simply rearranges the values within a block to create the ciphertext
  - ➢Can be done at the bit level or at the byte (character) level
  - ➢ Examples:

Plaintext: 00100101011010111001010101010100

Key: 1 > 3, 2 > 6, 3 > 8, 4 > 1, 5 > 4, 6 > 7, 7 > 5, 8 > 2

How? Bit 1 moves to position 3, bit 2 moves to position 6, and so on, with bit position 1 being the rightmost bit and position 2 being just to the left of position 1.

Plaintext 8-bit blocks: 00100101 01101011 10010101 01010100

Ciphertext: 11000100 01110101 10001110 10011000

XOR Operation

- **XOR cipher conversion:** The bit stream is subjected to a Boolean XOR function against some other data stream, typically a key stream
- XOR works as follows:
  - ‘0’ XOR’ed with ‘0’ results in a ‘0’. (0 ⊗ 0 = 0)
  - ‘0’ XOR’ed with ‘1’ results in a ‘1’. (0 ⊗ 1 = 1)
  - ‘1’ XOR’ed with ‘0’ results in a ‘1’. (1 ⊗ 0 = 1)
  - ‘1’ XOR’ed with ‘1’ results in a ‘0’. (1 ⊗ 1 = 0)
  - If two values are the same, you get “0”; if not, get “1”. Process is reversible: by XOR-ing ciphertext with key stream, you get the plaintext

Plaintext: **0100 0001**

Key stream: **0101 1010**

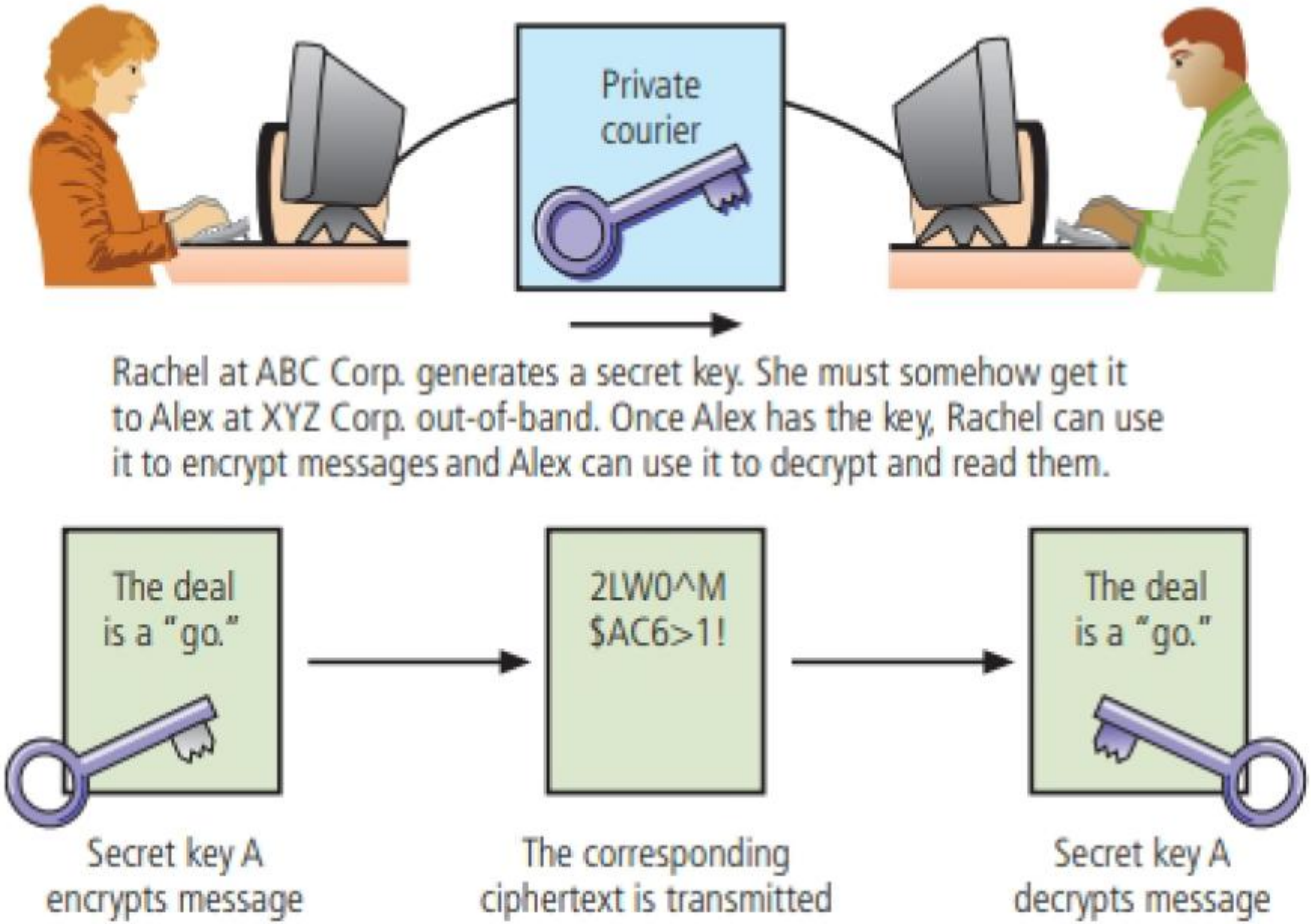
Ciphertext: **0001 1011**

Symmetric Encryption

- **Symmetric encryption**
  - ➢ Known as private key encryption, or symmetric encryption
  - ➢ The same key (a secret key) is used to encrypt and decrypt the message

- Methods are usually extremely efficient
  - ➢ Requiring easily accomplished processing to encrypt or decrypt the message
  - ➢ Challenge in symmetric key encryption is getting a copy of the key to the receiver

Symmetric Encryption



Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out-of-band. Once Alex has the key, Rachel can use it to encrypt messages and Alex can use it to decrypt and read them.

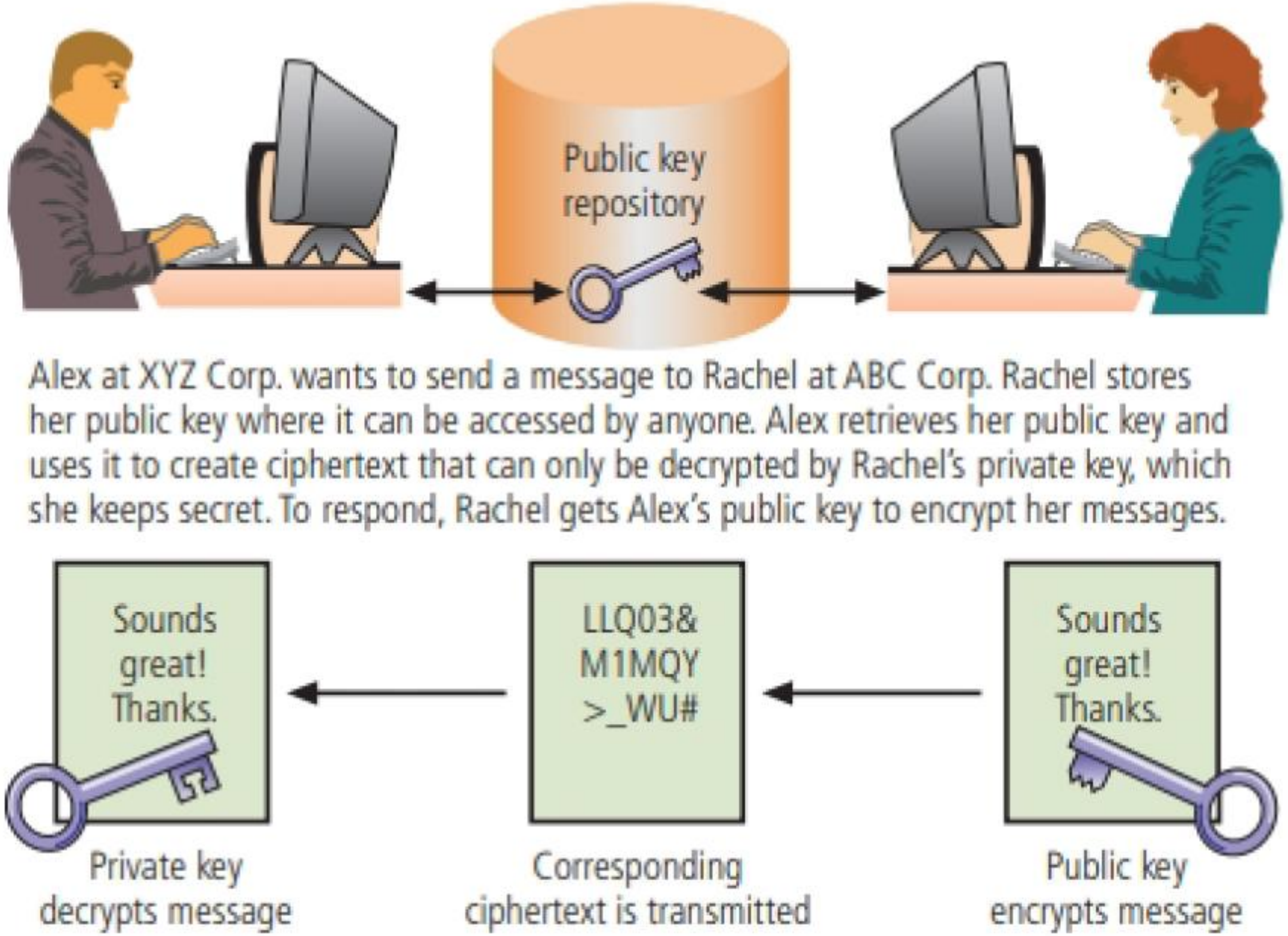
The deal is a "go."
2LW0^M $AC6>1!
The deal is a "go."
Secret key A encrypts message
The corresponding ciphertext is transmitted
Secret key A decrypts message

- Notable algorithms: DES, 3DES, AES

Asymmetric Encryption

- **Asymmetric encryption**
  - ➢ Also known as public key encryption
  - ➢ Uses two different, but related keys
    - ✓ Either key can be used to encrypt or decrypt the message
    - ✓ However, if Key A is used to encrypt the message, then only Key B can decrypt it; conversely, if Key B is used to encrypt a message, then only Key A can decrypt it
  - ➢ This technique is most valuable when one of the keys is private and the other is public
  - ➢ Notable algorithms: RSA, ElGamal, Regev

Asymmetric Encryption



Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves her public key and uses it to create ciphertext that can only be decrypted by Rachel's private key, which she keeps secret. To respond, Rachel gets Alex's public key to encrypt her messages.

- **Problem:** it requires four keys to hold a single conversation between two parties, and the number of keys grows geometrically as parties are added
- Not as efficient as symmetric-key encryption

Digital Signatures

- **Digital signatures**

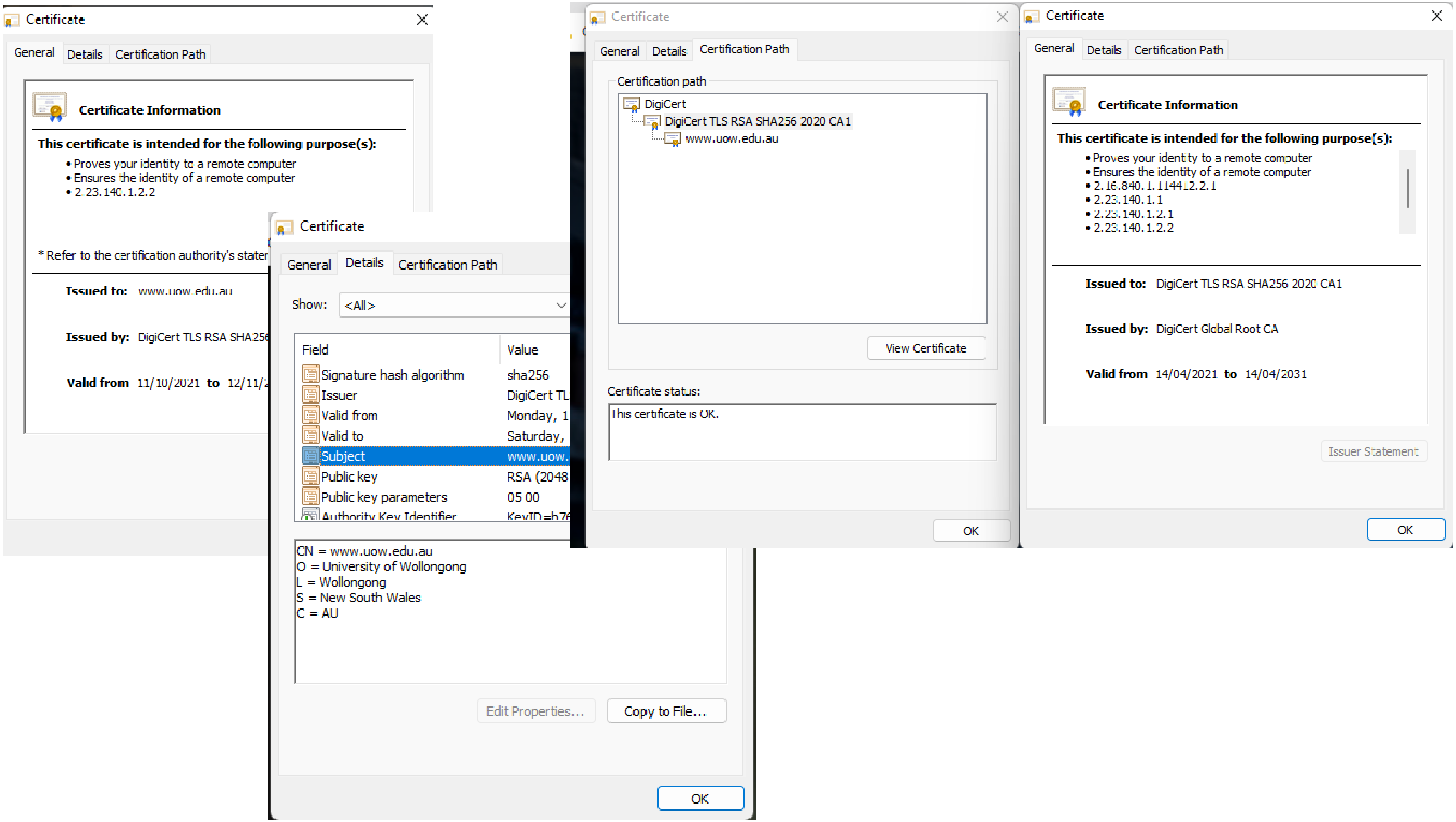
  - ➢ Messages that are independently verified by a central facility (registry) as authentic

  - ➢ When the asymmetric process is reversed, the private key encrypts a message, and the public key decrypts it
    - ✓ The fact that the message was sent by the organization that owns the private key cannot be refuted
    - ✓ This non-repudiation is the foundation of digital signatures

Digital Certificates and CAs

- **Digital certificate**
  - ➢ An electronic document, similar to a digital signature, attached to a file certifying that the file is from the organization it claims to be from and has not been modified from the original format

- **Certificate authority (CA)**
  - ➢ An agency that manages the issuance of certificates and serves as the electronic notary public to verify their origin and integrity



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's stater

Issued to: www.uow.edu.au

Issued by: DigiCert TLS RSA SHA256

Valid from 11/10/2021 **to** 12/11/2

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Signature hash algorithm	sha256
Issuer	DigiCert TL
Valid from	Monday, 1
Valid to	Saturday,
Subject	www.uow.
Public key	RSA (2048
Public key parameters	05 00
Authority Key Identifier	KeyID=b7

```
CN = www.uow.edu.au
O = University of Wollongong
L = Wollongong
S = New South Wales
C = AU
```

Certificate

General | Details | Certification Path

Certification path

```
DigiCert
  DigiCert TLS RSA SHA256 2020 CA1
    www.uow.edu.au
```

Certificate status:

This certificate is OK.

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.16.840.1.114412.2.1
- 2.23.140.1.1
- 2.23.140.1.2.1
- 2.23.140.1.2.2

Issued to: DigiCert TLS RSA SHA256 2020 CA1

Issued by: DigiCert Global Root CA

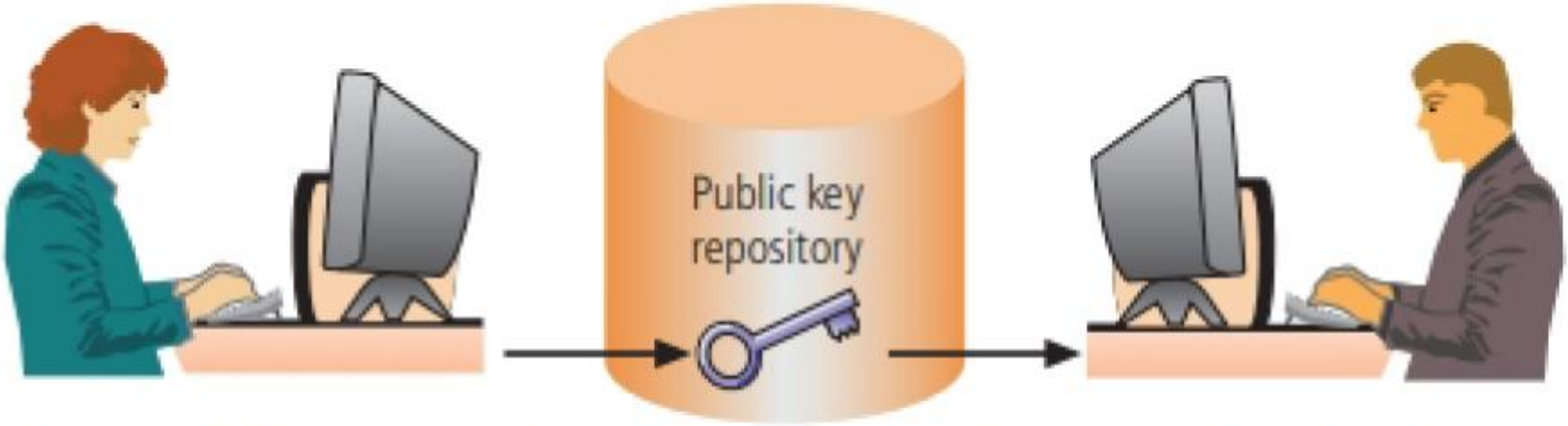
Valid from 14/04/2021 **to** 14/04/2031

Public-Key Infrastructure

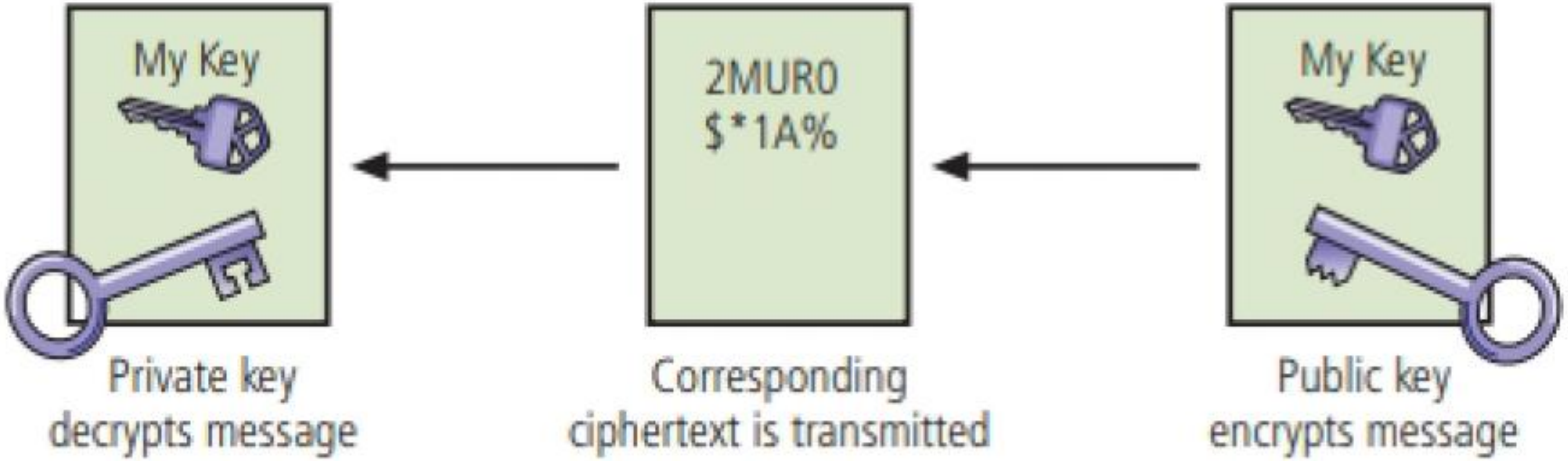
- A **public key infrastructure** (PKI) is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption. PKI systems are based on public key cryptosystems and include digital certificates and certificate authorities
- Common implementations of PKI: Systems that issue digital certificates to users and servers, systems with computer key values to be included in digital certificates, tools for managing user enrollment, key generation, and certificate issuance, tools for managing user enrollment, key generation, and certificate issuance, verification and return of certificates, key revocation services
- An organization can increase its cryptographic capabilities in protecting its information assets by using PKI to provide the following services: authentication, integrity, confidentiality, authorization, non-repudiation.

Hybrid Systems

- Pure asymmetric key encryption is not widely used except in the area of certificates
- It is typically employed in conjunction with symmetric key encryption, creating a **hybrid system**
- The hybrid process in current use is based on the Diffie-Hellman key exchange method, which provides a way to exchange private keys using public key encryption without exposure to any third parties
- In this method, asymmetric encryption is used to exchange symmetric keys so that two organizations can conduct quick, efficient, secure communications based on symmetric encryption
- Diffie-Hellman provided the foundation for subsequent developments in public key encryption



Rachel at ABC Corp. stores her public key where it can be accessed. Alex at XYZ Corp. retrieves it and uses it to encrypt his private (symmetric) key. He sends it to Rachel, who decrypts Alex's private key with her private key and then uses Alex's private key for regular communications.



Using Cryptographic Controls

- Cryptographic controls can guarantee security only when the proper key management infrastructure has been constructed and when the cryptosystems are operated and managed correctly.

- Organizations with the need and the ability to use cryptographic controls can use them to support several aspects of the business:
  - ➢ Confidentiality and integrity of e-mail and its attachments
  - ➢ Authentication, confidentiality, integrity. and nonrepudiation of e-commerce Authentication and confidentiality of remote access through VPN
  - ➢ A higher standard of authentication when used to supplement access control systems

Notable Cryptographic Protocols

- Email Security: **S/MIME** (Secure Multipurpose Internet Mail Extensions) and **PGP** (Pretty Good Privacy)
- Securing the Web: **SSL/TLS** (Secure Socket Layer/Transport Layer Security) and **HTTPS** (Secure Hypertext Transfer Protocol)
- **IPSec** (IP Security)
- **SSH** (Secure Shell)
- **VPN** (Virtual Private Network)
- Secure Authentication: **Kerberos**

Managing Cryptographic Controls

- Don’t lose your keys
- Know who you are communicating with
- It may be illegal to use a specific cryptographic technique when communicating to some nations
- Every cryptosystem has weaknesses
- Do not load cryptosystems on systems that can be easily compromised
- Can the CAs be fully trusted?
- There is no security in obscurity
- Security protocols and the cryptosystems they use are subject to the same limitations as firewalls and IDPSs.