

# Chapter 1

## Introduction

*The art of war teaches us to rely:*

- **not** on the likelihood of the enemy's not coming,
  - but on our own readiness to receive him;
- **not** on the chance of his not attacking,
  - but rather on the fact that we have made our position unassailable.

—*The Art of War, Sun Tzu*

# Cybersecurity

- Cybersecurity is the protection of information that is stored, transmitted, and processed in a networked system of:
  - computers, other digital devices, and network devices, and transmission lines, including the Internet.
- Protection encompasses confidentiality, integrity, availability, authenticity, and accountability.
- Methods of protection include organizational policies and procedures, as well as technical means such as encryption and secure communications protocols.

# Cybersecurity

- **Information Security**
  - preservation of confidentiality, integrity, and availability of information. In addition to:
  - authenticity, accountability, nonrepudiation, and reliability
- **Network Security**
  - Protection of networks and their service from unauthorized modification, destruction, or disclosure, and
  - assurance that the network performs its critical functions correctly and there are no harmful side effects.

# Standards Organizations

- National Institute of Standards & Technology (**NIST**)
- Internet Society (**ISOC**)
- International Telecommunication Union  
Telecommunication Standardization Sector  
(**ITU-T**)
- International Organization for Standardization (**ISO**)
- **CERT**: Computer Emergency Response Team

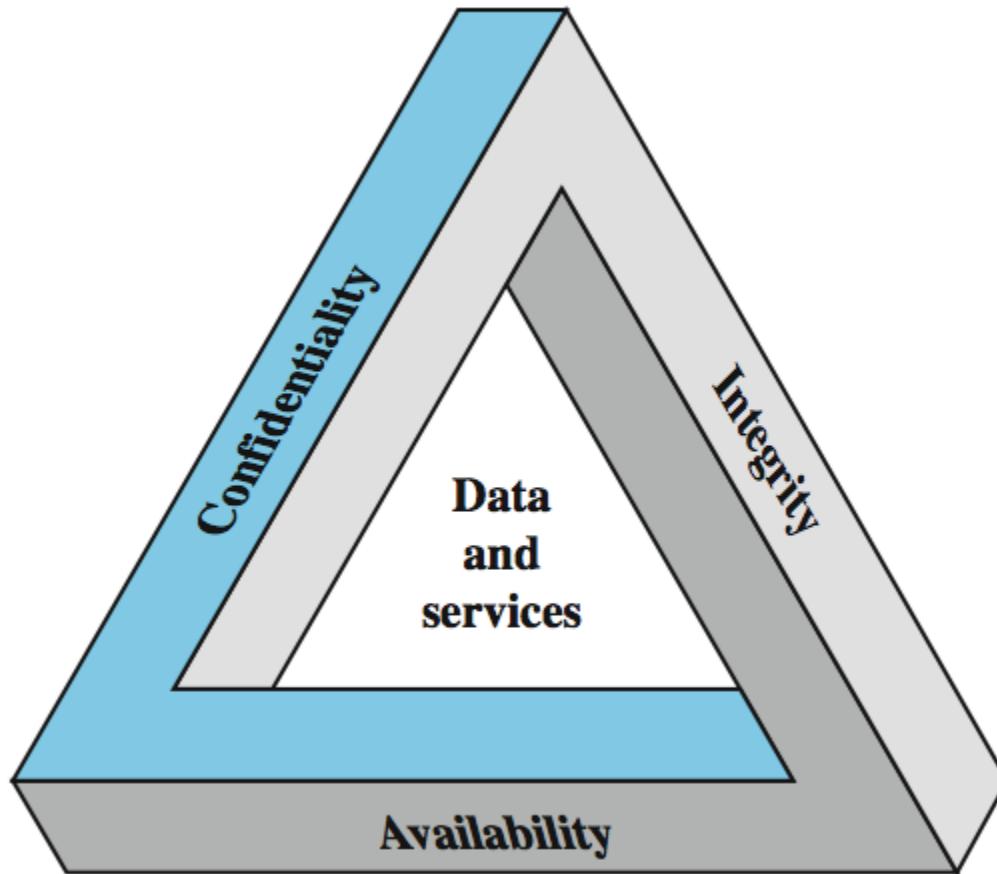
# Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

# Aim of Course

- our focus is on **Internet Security**
- which consists of measures to:
  - Deter, prevent, detect, and correct security violations
  - Transmission & storage of information

# Key Security Concepts



# Objectives of Cybersecurity

## 1. Confidentiality

- **Data Confidentiality:** assures that private or confidential information is not made available or disclosed to unauthorized individuals (e.g., *student grades*)
- **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

# Objectives of Cybersecurity

## 2. Integrity

- **Data integrity:** assures that data (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner (e.g., Patient information)
- **System integrity:** assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

## 3. Availability

- Assures that systems work promptly, and service is not denied to authorized users (E.g., Authentication service)

# Objectives of Cybersecurity - extended

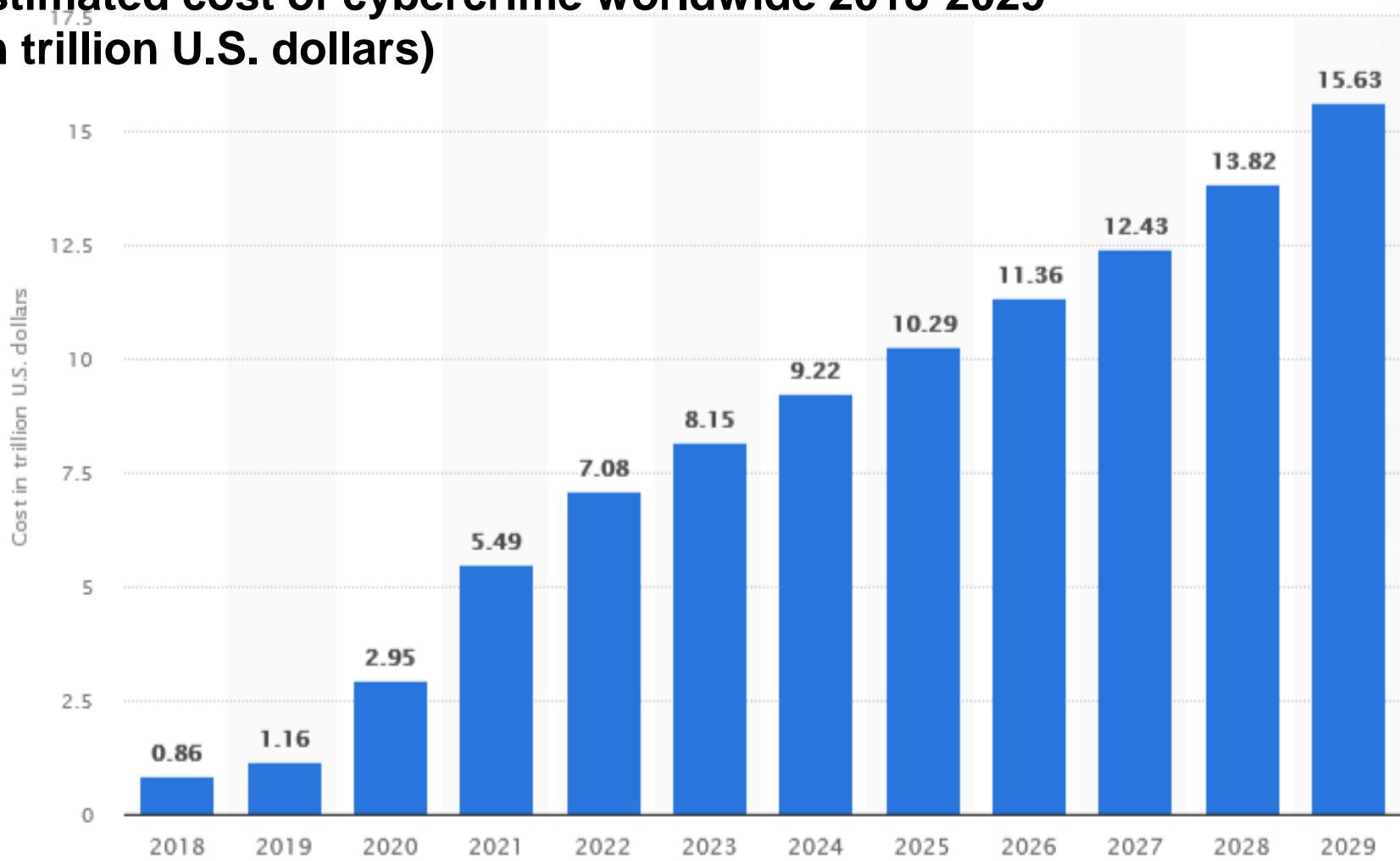
- **Authenticity:** the property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
  - e.g., verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- **Accountability:** the ability to trace an entity. This supports
  - nonrepudiation, fault isolation, intrusion detection and prevention, and after-action recovery.
  - The ability to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis.

# Challenges of Information Security

- It is not simple! The mechanisms are complex
- Typically, there are unexpected weaknesses in the mechanisms.
- Once designed, in which layer do we place them?
- Security mechanisms typically involve secret information to be shared.
  - How do we generate them, distribute them and protect them?
- Security is still too often an afterthought to be incorporated into a system after the design is complete

# Cyber Crime

Estimated cost of cybercrime worldwide 2018-2029  
(in trillion U.S. dollars)



© Statista 2024

[Additional Information](#)

[Show source](#)

# Security Violations

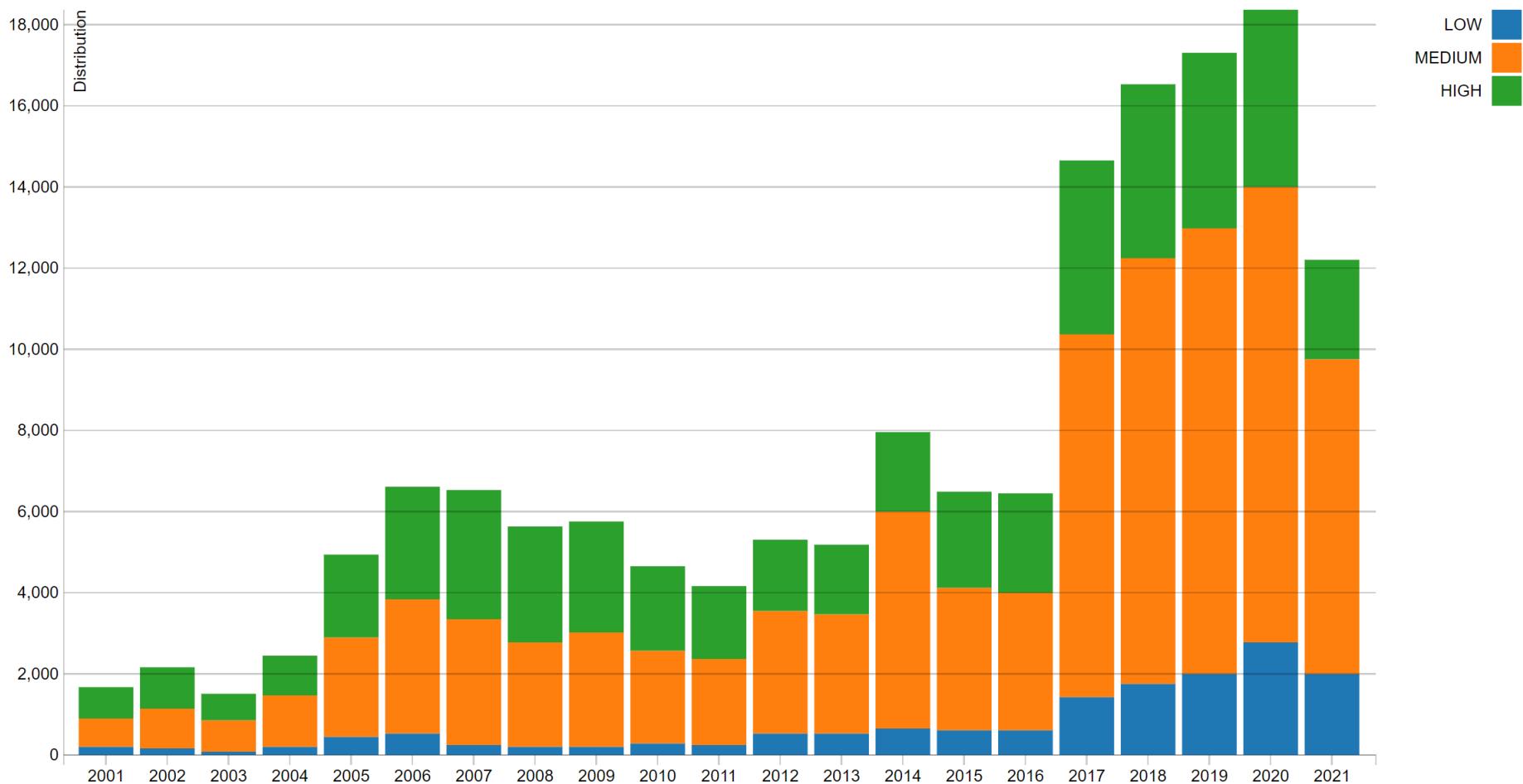
- A transmits a file to B. User C who is **not** authorized to read this file captures a copy (**confidentiality**)
- A network manager D transmits a message to a computer, E, containing entries for new users to be given access to E.
  - F intercepts the message and alters it and then forwards it to E which accepts it and performs the updates (**integrity and man-in-the-middle**)

# Security Violations

- F constructs its own message and sends it to E as if it is coming from D (**forgery, spoofing, masquerading**).
- An employee is fired and a message is sent to deactivate his account. He intercepts the message, delays it and performs a final access to sensitive information (**man-in-the-middle**)
- A customer denies that he sent his stock broker a message about transactions (**repudiation**)

# Security Trends

- CERT reports the security weaknesses in operating systems and in Internet routers and other network devices



# Security Trends

## ▪ Vulnerabilities Reported in 2024 per Operating System

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Linux Kernel</a>	<a href="#">Linux</a>	OS	<a href="#">1705</a>
2	<a href="#">Windows Server 2022</a>	<a href="#">Microsoft</a>	OS	<a href="#">400</a>
3	<a href="#">Windows Server 2019</a>	<a href="#">Microsoft</a>	OS	<a href="#">384</a>
4	<a href="#">Windows 11 22h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">370</a>
5	<a href="#">Windows 11 23h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">370</a>
6	<a href="#">Windows 11 21h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">362</a>
7	<a href="#">Windows 10 21h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">356</a>
8	<a href="#">Windows 10 22h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">356</a>
9	<a href="#">Windows 10 1809</a>	<a href="#">Microsoft</a>	OS	<a href="#">339</a>
10	<a href="#">Windows Server 2016</a>	<a href="#">Microsoft</a>	OS	<a href="#">339</a>
11	<a href="#">Macos</a>	<a href="#">Apple</a>	OS	<a href="#">309</a>
12	<a href="#">Windows 10 1607</a>	<a href="#">Microsoft</a>	OS	<a href="#">293</a>

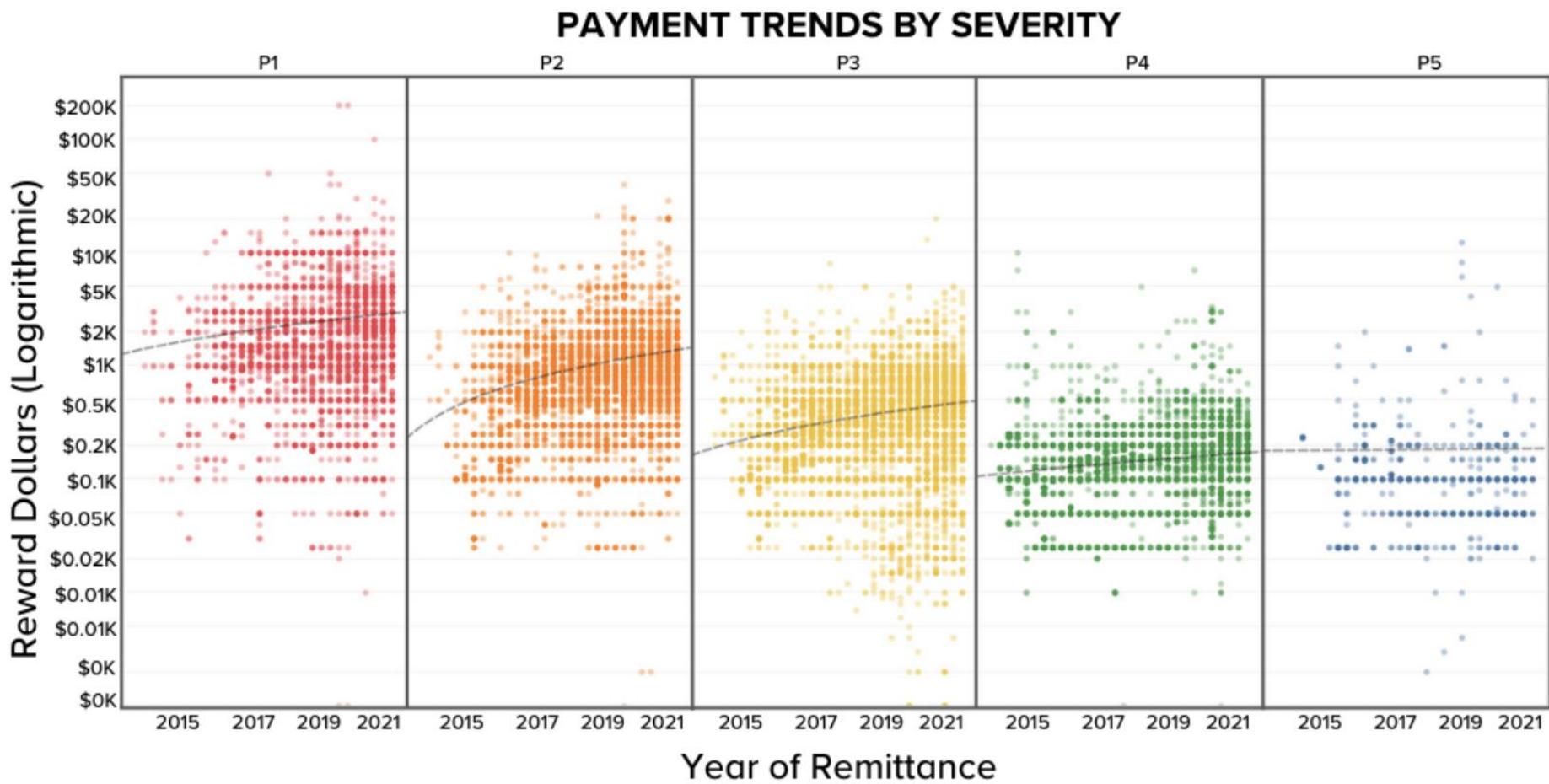
# Security Trends

## ▪ Vulnerabilities Reported in 2024 per Operating System

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
13	<a href="#">Kernel</a>	<a href="#">Linux</a>	OS	<a href="#">285</a>
14	<a href="#">Windows Server 2012</a>	<a href="#">Microsoft</a>	OS	<a href="#">278</a>
15	<a href="#">Android</a>	<a href="#">Google</a>	OS	<a href="#">278</a>
16	<a href="#">Windows 10 1507</a>	<a href="#">Microsoft</a>	OS	<a href="#">276</a>
17	<a href="#">Windows Server 2022 23h2</a>	<a href="#">Microsoft</a>	OS	<a href="#">231</a>
18	<a href="#">Experience Manager</a>	<a href="#">Adobe</a>	Application	<a href="#">220</a>
19	<a href="#">Iphone Os</a>	<a href="#">Apple</a>	OS	<a href="#">207</a>

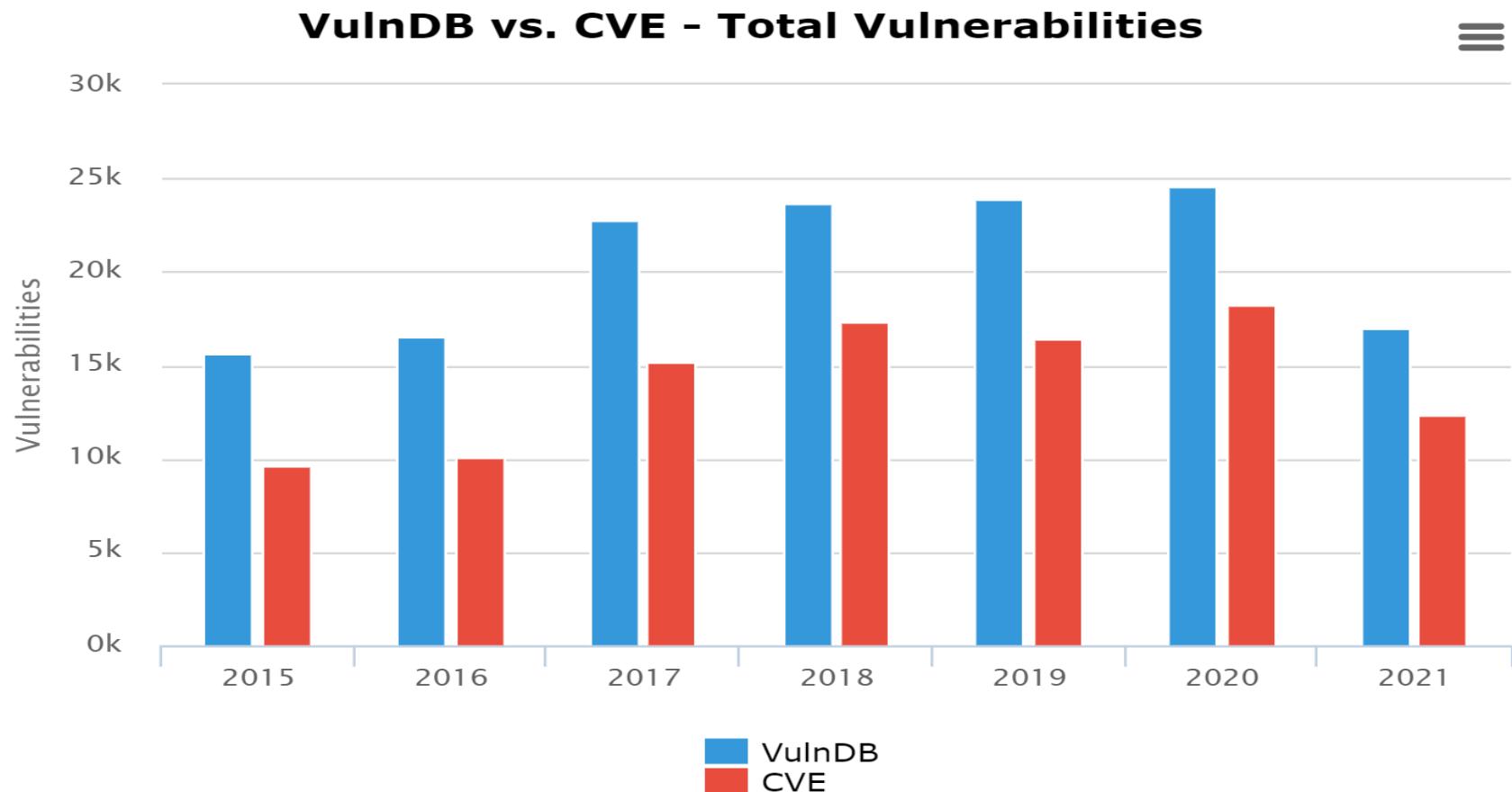
# Vulnerability Reporting Rewarded

- Vulnerability reports are on the rise, and the crowd is rising to the challenge of a changing Internet.
  - Total payouts are growing steadily by about **15-20% per quarter**.



# Vulnerabilities vs CVE

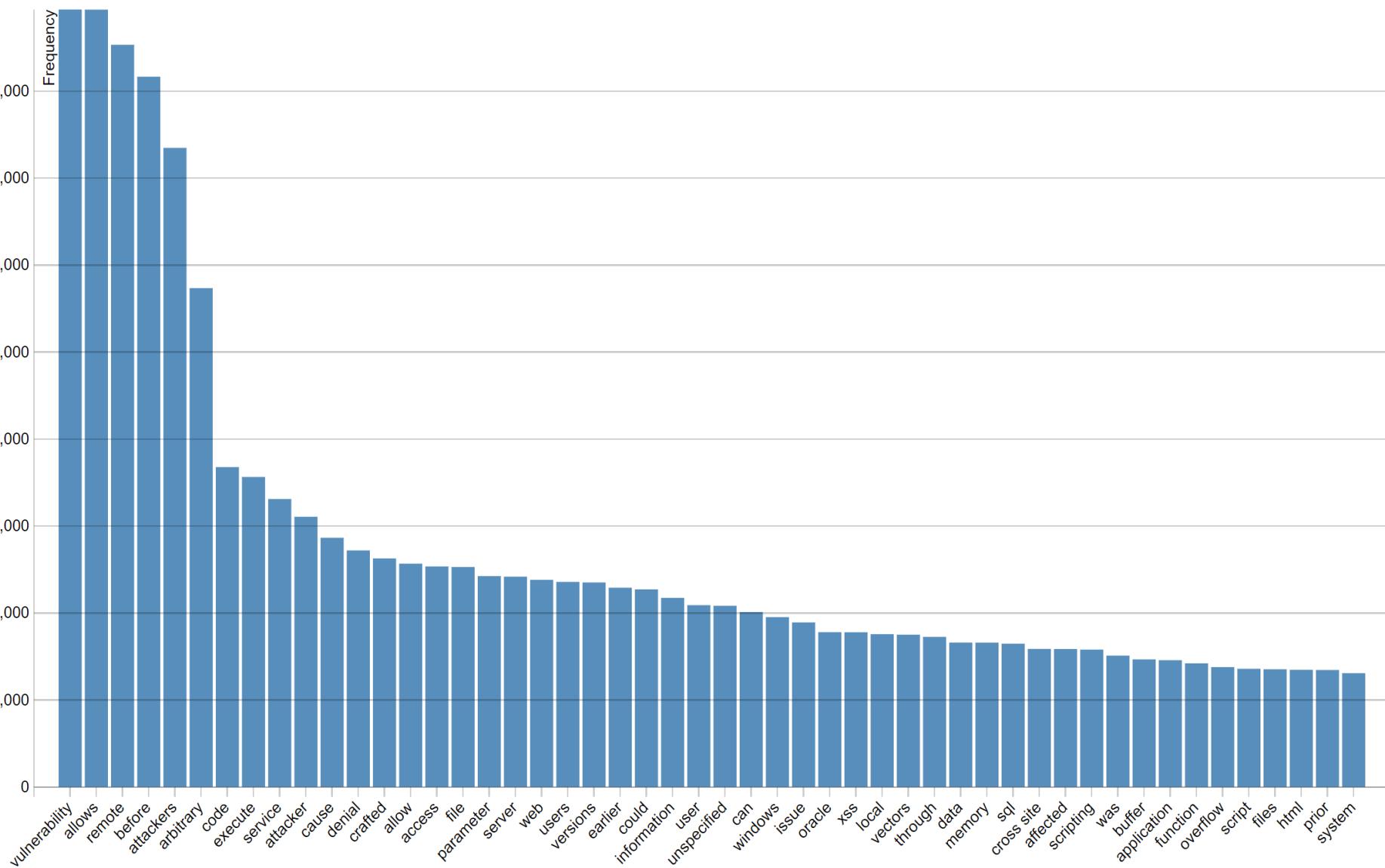
- Common Weakness Enumeration (**CWE**) has to do with the **vulnerability**—not the instance within a product or system.
- Common **Vulnerabilities** and Exposures (**CVE**) has to do with the specific instance within a product or system—not the underlying flaw.



# Vulnerability by Categories

- The six most common vulnerability categories:
  - Buffer overflow.
  - Denial of service
  - Remote file include
  - SQL injection
  - Cross-site scripting
  - Cross-site request forgery.
- All are potentially remotely exploitable.

# Vulnerability by Categories



# Buffer Overflow

- This is an anomaly where a program, while writing data to a buffer, **overruns** the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory **safety**

# Denial of Service (DoS)

- In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users.
- Distributed denial-of-service attacks are sent by two or more persons, or **bots**, and DoS attacks are sent by one person or system.

# Denial of Service (DoS)

Facts about DDoS attacks frequency include:

- The frequency of DDoS attacks increased more than 5 times between 2014 and 2024.
- In 2023, DDoS growth is 120%.
- The cost of a DDoS attack averages between \$20,000-\$40,000 per hour.
- Based on CloudFlare the total number of attacks of this type globally 8.5 million in 2024 Q1/Q2.
- The longest DDoS attack lasted 6,459 minutes; more than 100 hours.

# Remote File Include (RFI)

- It allows an attacker to include a remote file, usually through a script on the web server.
- The vulnerability occurs due to the use of **user-supplied input without proper validation**. This can lead to simple to serious events:
  - output the contents of a file
  - Code execution on the web server
  - Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (**XSS**)
  - Denial of service (**DoS**)
  - Data theft/manipulation

# SQL Injection

- Code injection technique, used to attack data-driven applications
- Malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- It exploits a security vulnerability in an application's software, for example, when user input is incorrectly filtered.

# Cross Site Scripting (**XSS**)

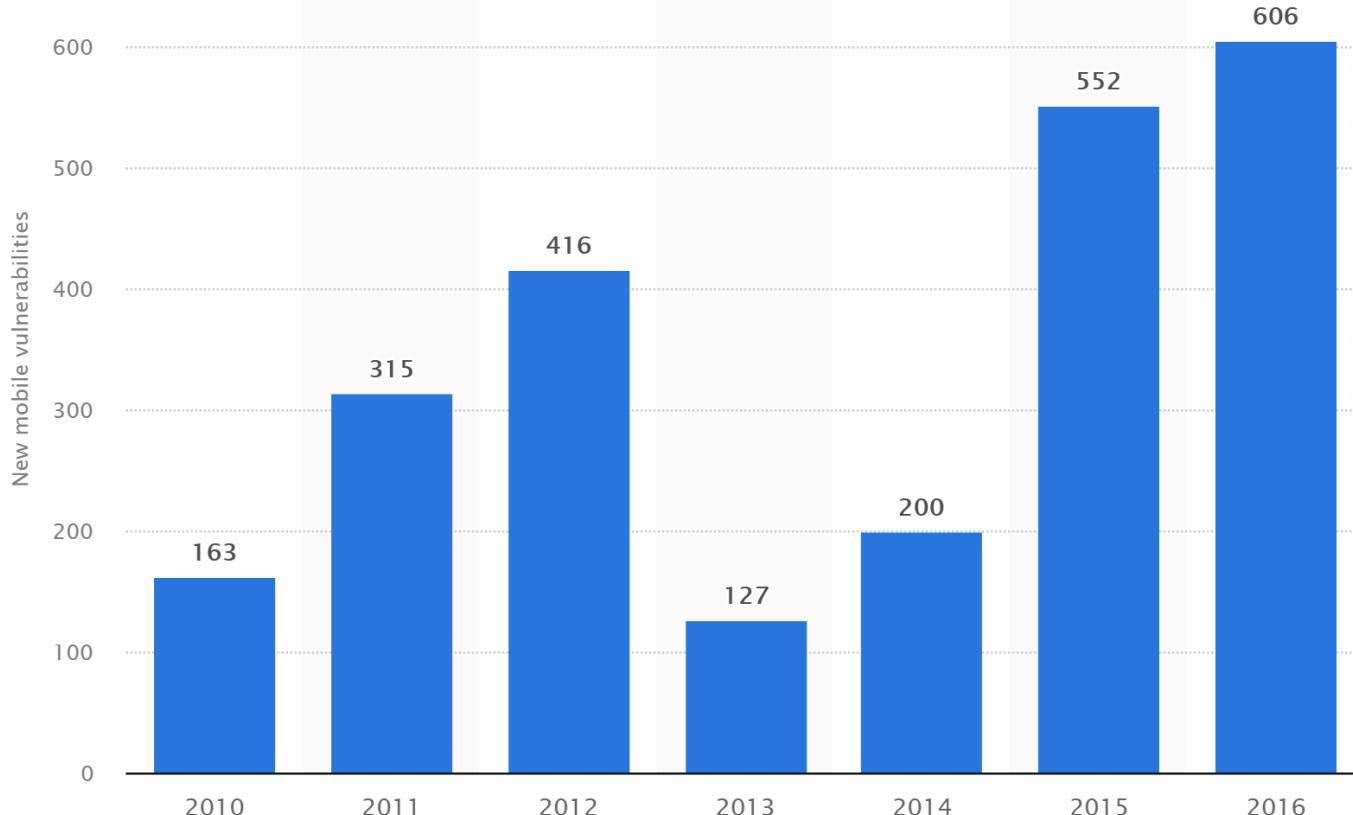
- For example, suppose there is a dating website where members scan the profiles of other members to see if they look interesting.
- For privacy reasons, this site hides everybody's real name and email. These are kept secret on the server. The only time a member's real name and email are in the browser is when the member is signed in.
- Suppose that Mallory, an attacker, joins the site and wants to figure out the real names of the people she sees on the site.
- She writes a script designed to run from other people's browsers when they visit her profile.

# Cross Site Scripting (**XSS**)

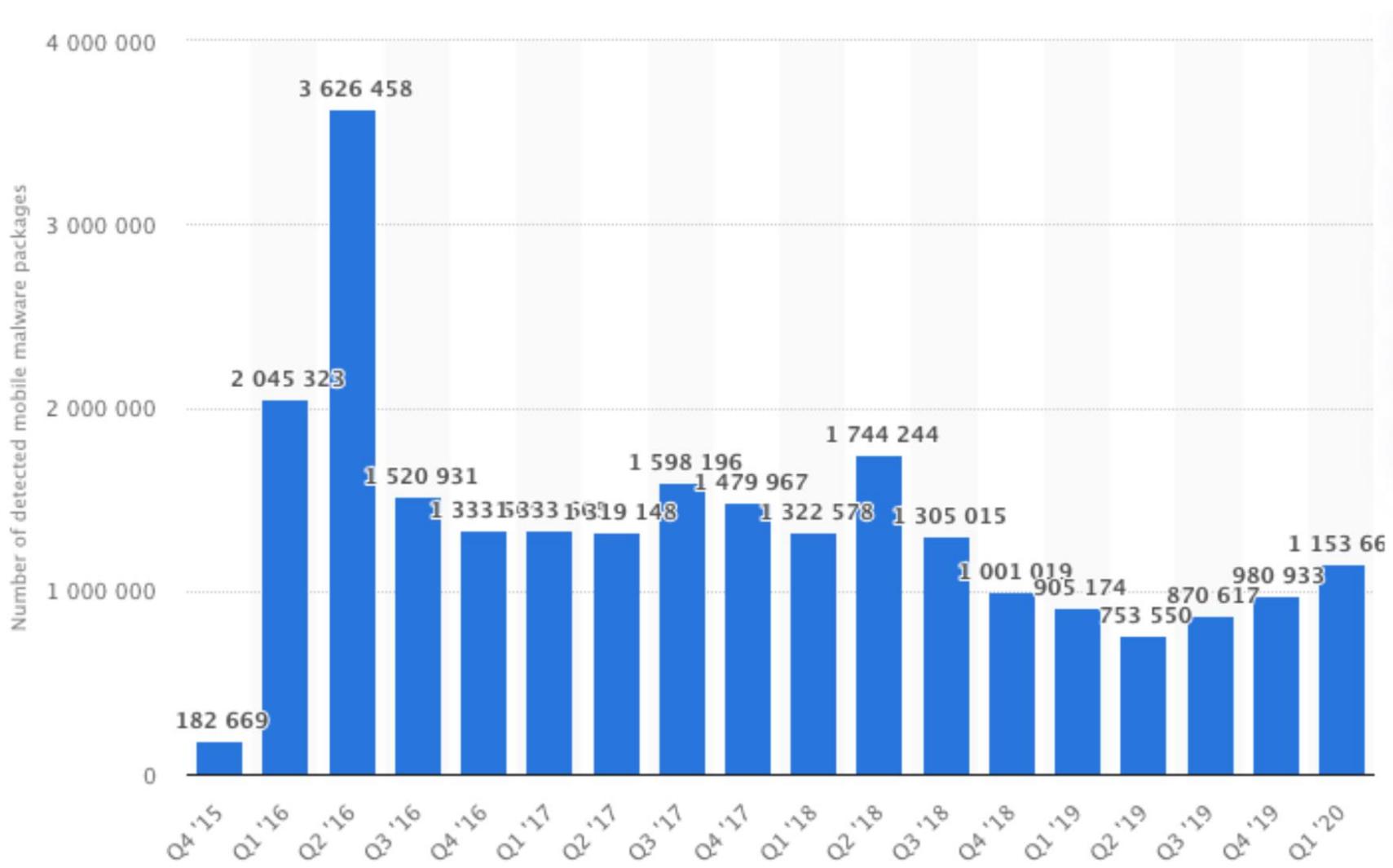
- The script then sends a quick message to her own server, which collects this information.
- To do this, she answers "Describe your Ideal First Date", by a short answer and puts at the end her script to steal names and emails.
- Then suppose that Bob, a member of the dating site, reaches Mallory's profile, which has her answer to the First Date question. Her script is run automatically by the browser and steals a copy of Bob's real name and email directly from his own machine.

# Mobile Vulnerabilities

- Statistics in 2020 and 2021 showing over 1.5K new mobile vulnerabilities each year
- **Android:** Attack likelihood rose from 34% in 2023 to 84% in 2024.
- **iOS:** Attack likelihood increased from 17% in 2023 to 29% in 2024.
- zero-day *vulnerabilities count* for May month: 169.

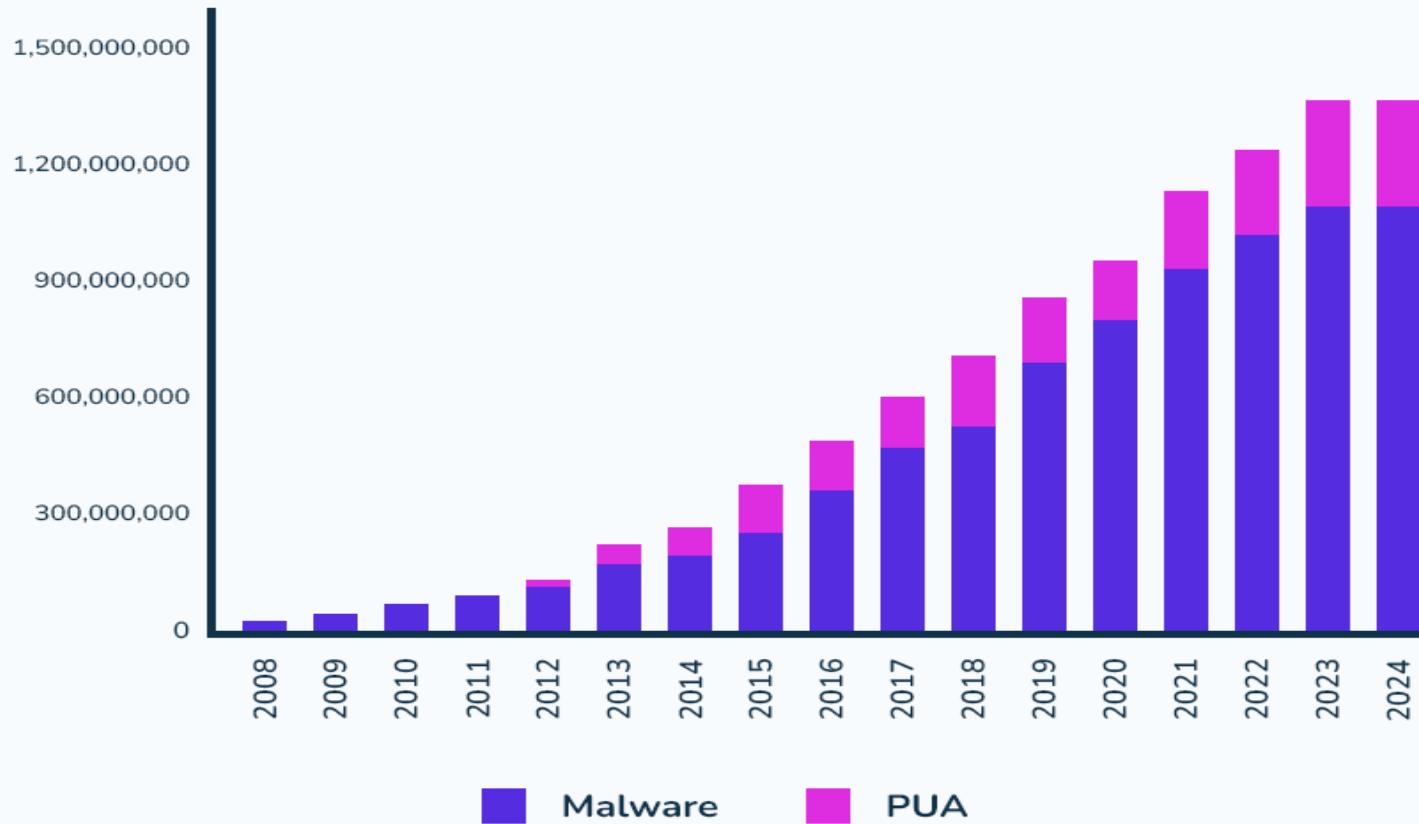


# Mobile Malware Packages



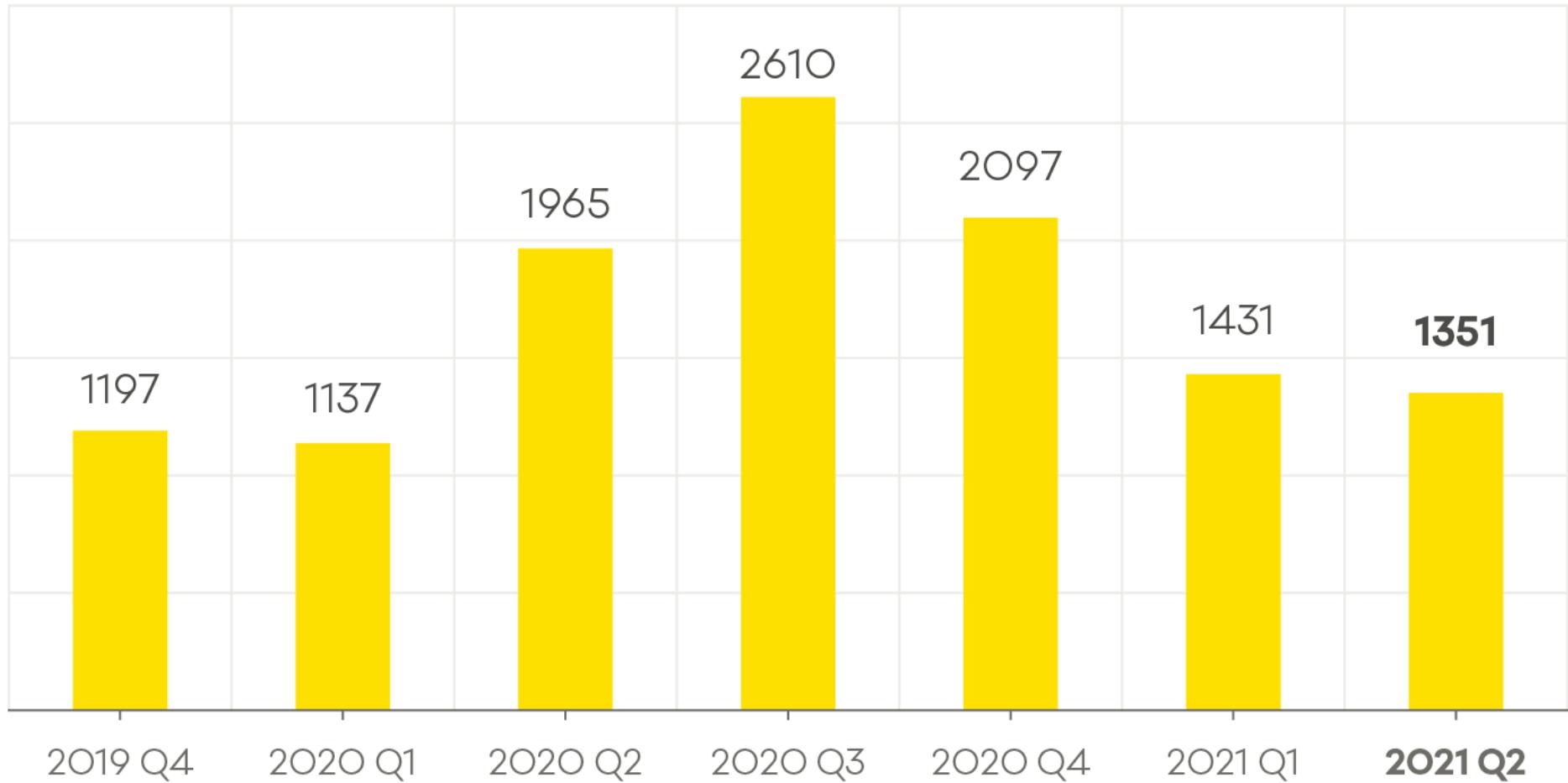
# Malware and PAU Statistics

## Total Amount of Malware and PUA (by year)



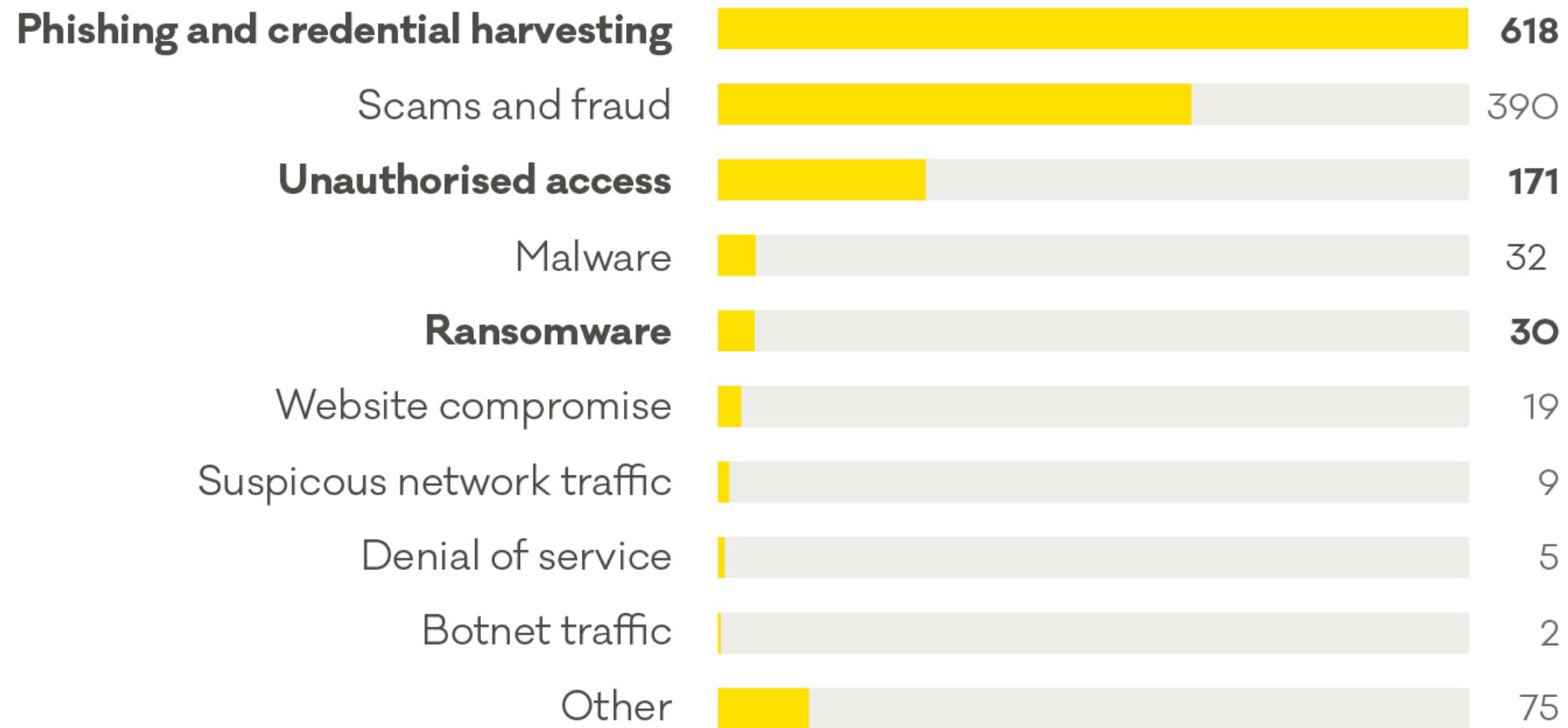
# Security Trends

- Incidents reported to **CERT** (per country / 2024) such as denial of service attacks, IP spoofing, eavesdropping and packet sniffing.



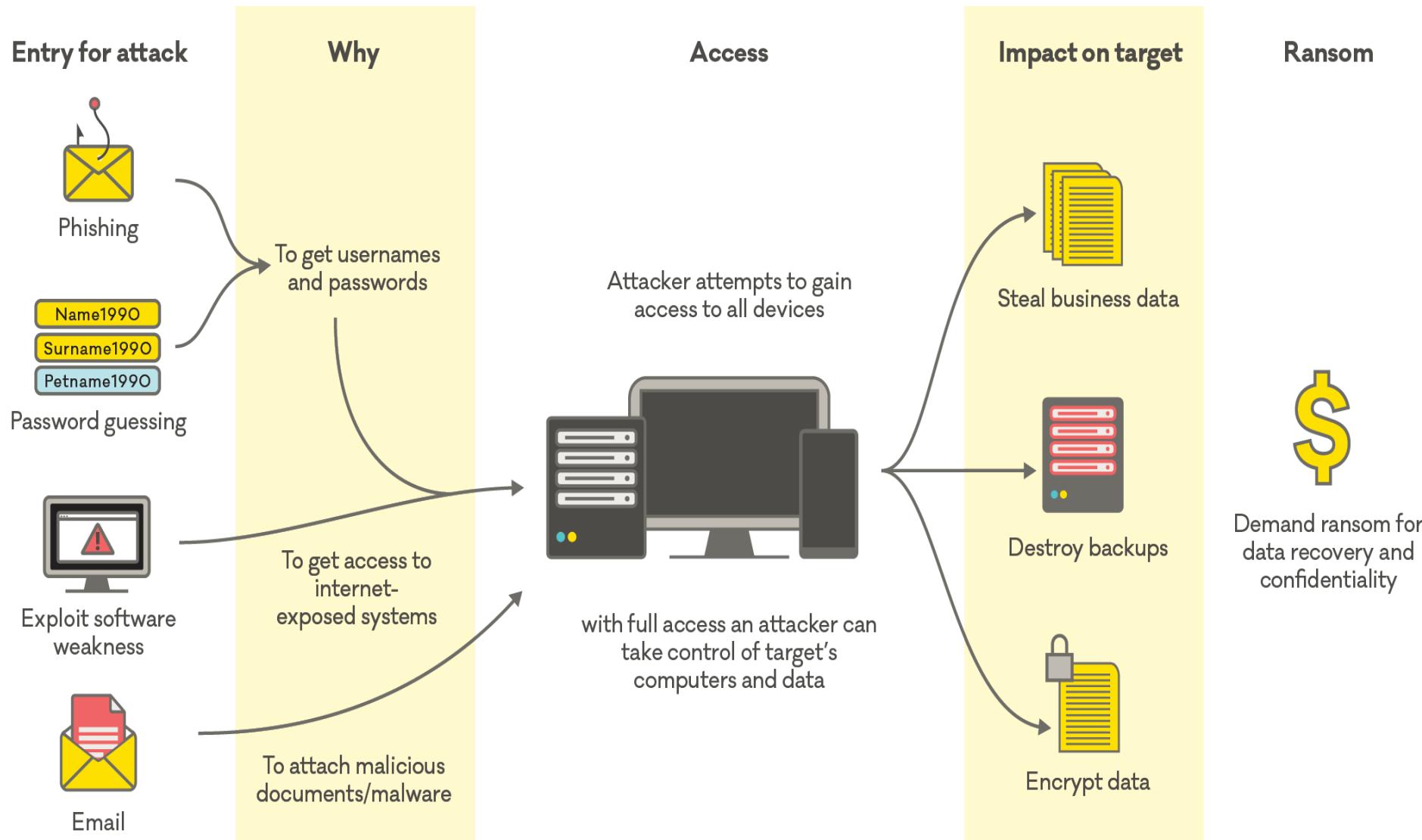
# Security Trends

## Breakdown by incident category



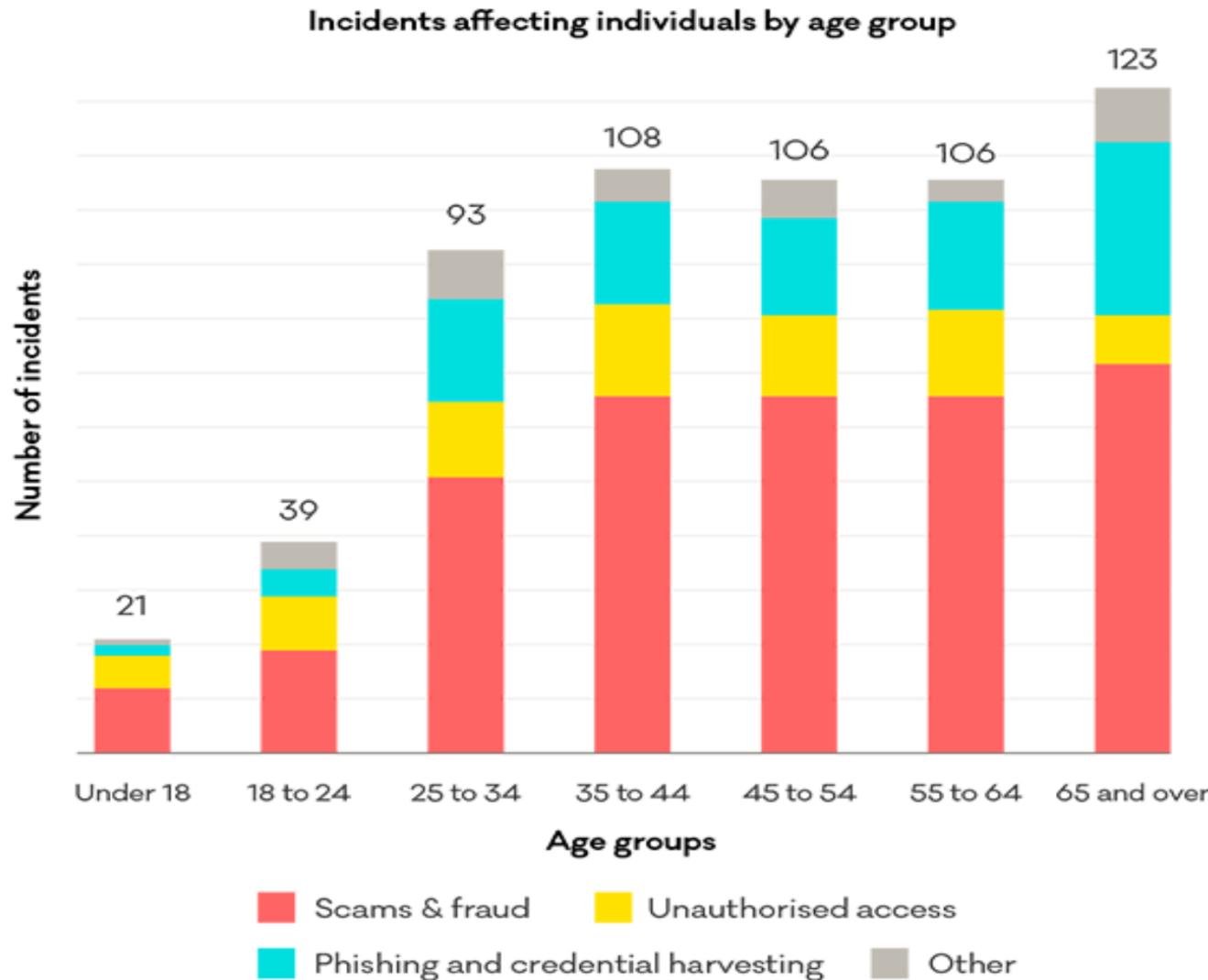
# Security Trends

## How ransomware works



# Security Trends

## Incidents affecting individuals by age group



# IBM X-Force Threat Reports (2024)

- 71% Year-over-year increase in cyberattacks that used **stolen or compromised credentials**.
- 32% Share of cyber incidents that involved **data theft and leak**, indicating that more attackers favor **stealing and selling data**, rather than encrypting it for extortion.
- 50% The **AI market** share milestone that will incentivize cybercriminals to invest in developing cost-effective tools to attack AI technologies.
- Cybercriminals are increasingly ***logging in*** rather than ***hacking into*** networks through valid accounts, which became the most common entry point into victims' environments in 2023, representing 30% of all incidents X-Force® responded to.

## Global number of cyber attacks per day

Nearly 4000 new cyber attacks occur every day. Every 14 seconds, a company falls victim to a ransomware attack, which can result in devastating financial losses while 560,000 new pieces of malware are detected every day

# OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- Defines a systematic way of defining and providing security requirements.
- Computer and communications vendors have developed security features for their products compliant with this architecture.
- For us it provides a useful, if abstract, overview of concepts we will study

# Aspects of Security

- The OSI security architecture focuses on 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**
- Often **threat** & **attack** used to mean same thing
  - Threat is a potential for violation of security
  - Attack is an assault on system security that derives from an intelligent threat

# Security Attacks

- Any action that compromises the security of information owned by an organization.
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
- Have a wide range of attacks.
- We can classify attacks generically as:
  - passive
  - active

# Attacks

## Passive Attacks

Release of message contents

Traffic analysis

## Active Attacks

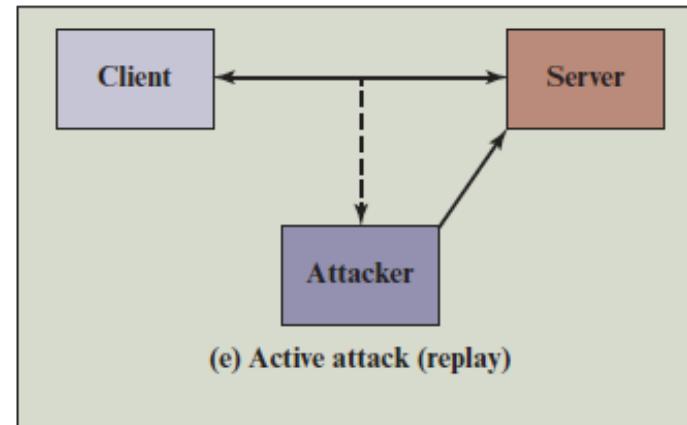
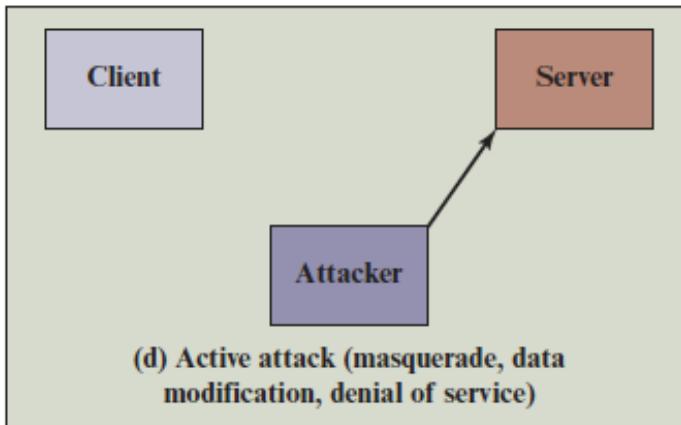
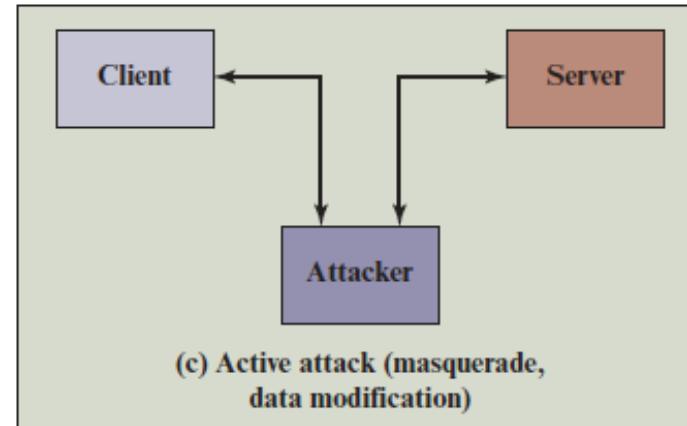
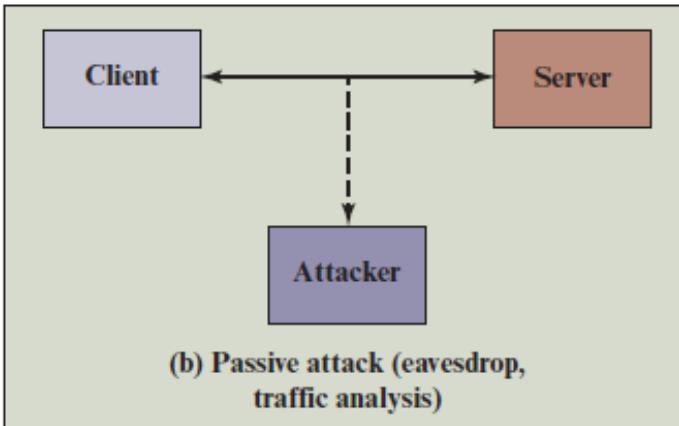
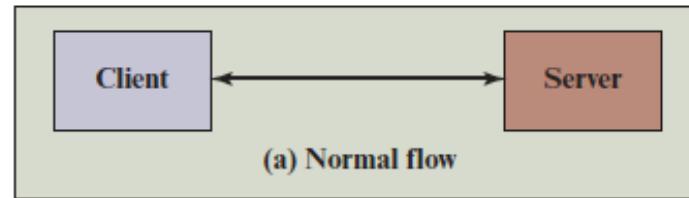
Replay

Masquerade

Data modification

Denial of service

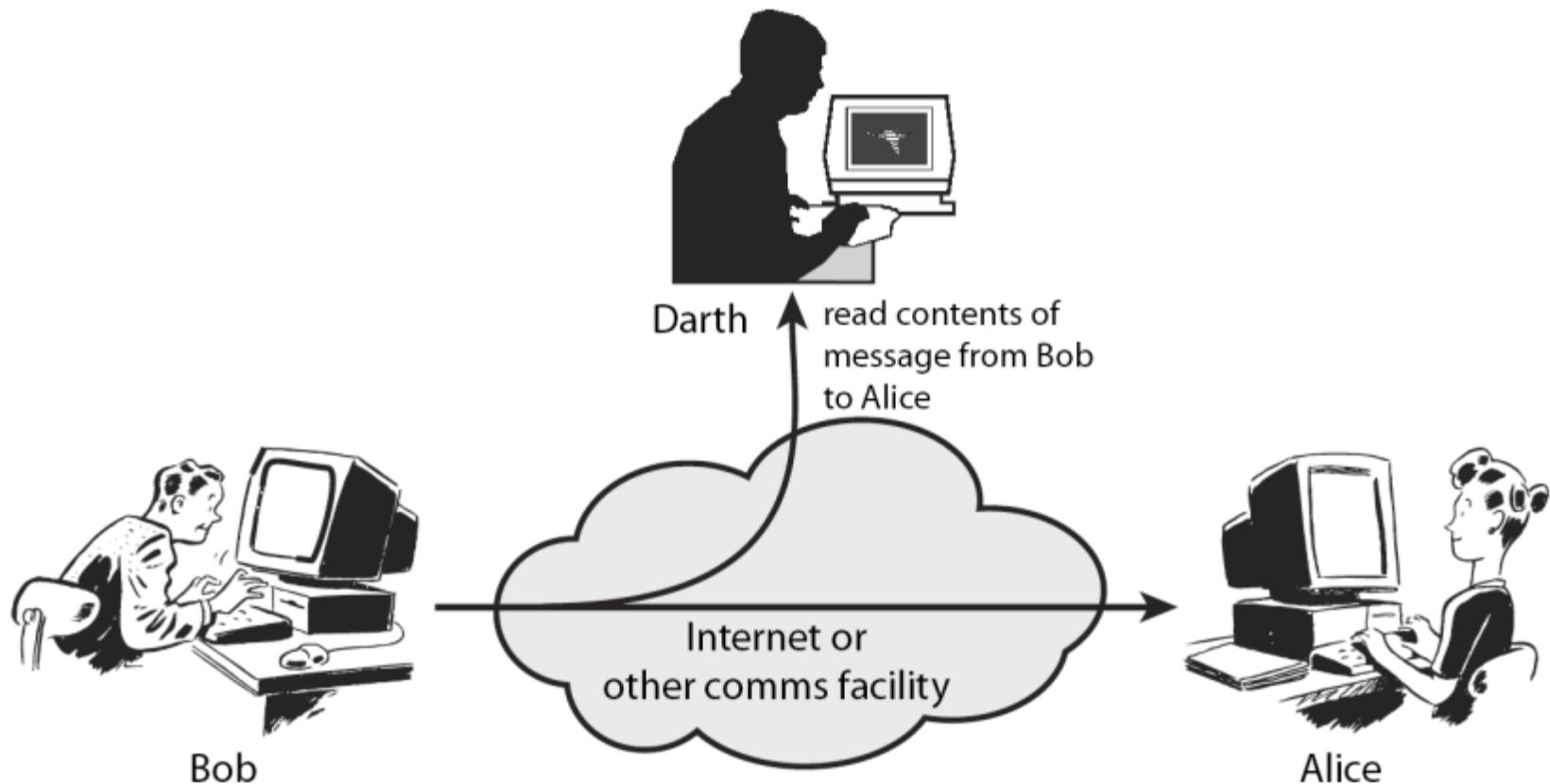
# Security Attacks



# Passive Attacks

- They are in the nature of eavesdropping on or monitoring of transmissions.
- Two types of passive attacks are release of message and traffic analysis.
- Passive attacks are difficult to detect because they do not alter the data.
- To prevent the success of such attacks, usually encryption is used.

# Passive Attacks



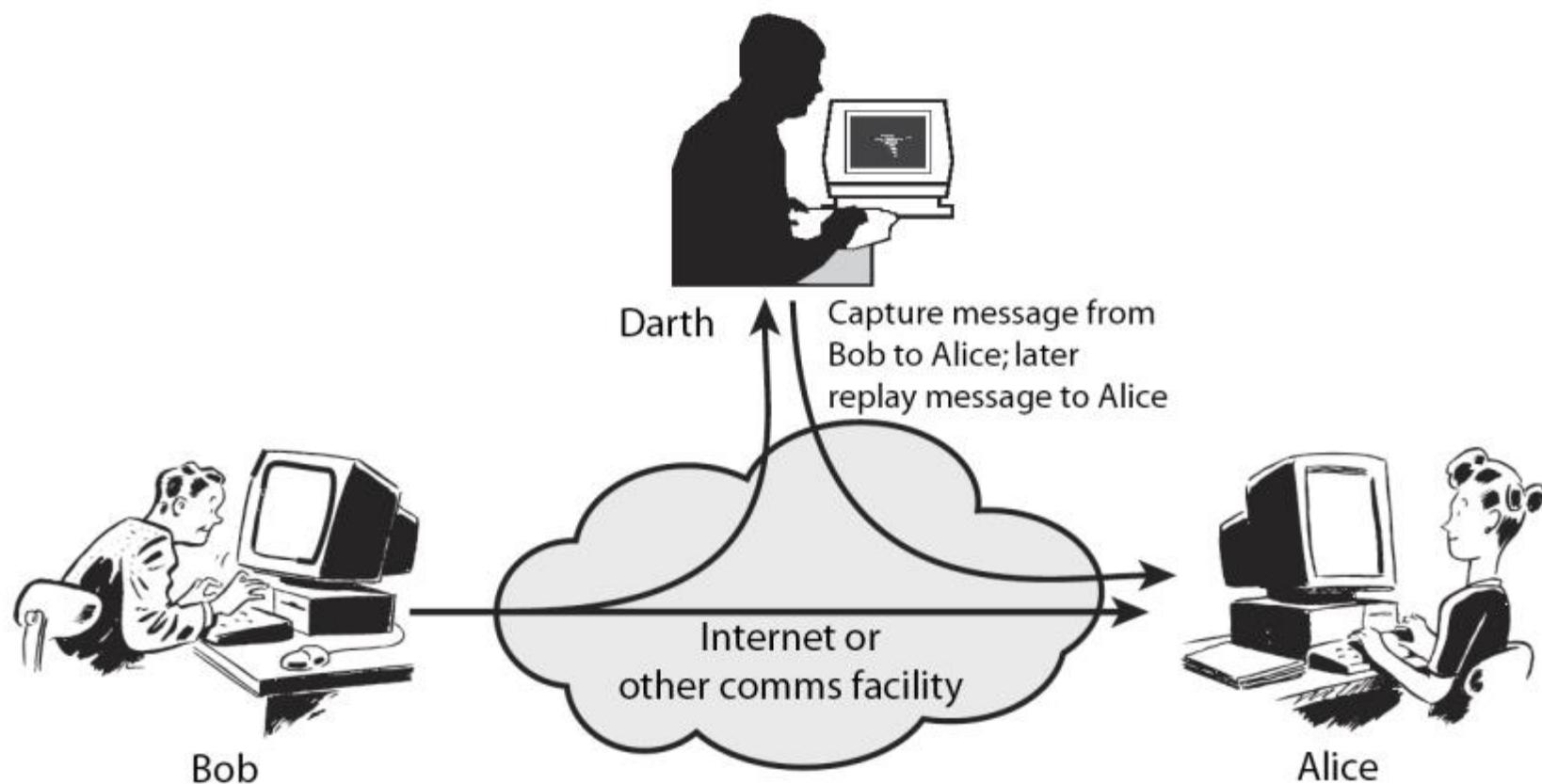
# Active Attacks

- They involve alteration of the data stream or the creation of a false stream. They can be subdivided into 4 categories:
  - Masquerade takes place when one entity pretends to be a different entity by capturing and replaying an authentication sequence
  - Replay is the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

# Active Attacks

- Modification of messages
- Denial of service prevents the normal use or management of communications facilities
  - Suppress all messages directed to a destination
  - Overloading the network with messages to degrade its performance
- It is difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities
- It is important to detect active attacks and to recover from them

# Active Attacks



# Security Services

- Enhance security of data processing systems and information transfers of an organization
- Intended to counter security attacks
- Using one or more security mechanisms
- Often replicates functions normally associated with physical documents
  - Which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Security Services

- X.800:  
“A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”
- RFC 2828:  
“A processing or communication service provided by a system to give a specific kind of protection to system resources”

# Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

# Security Mechanisms

- Features designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However, one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**
- Hence our focus on this topic

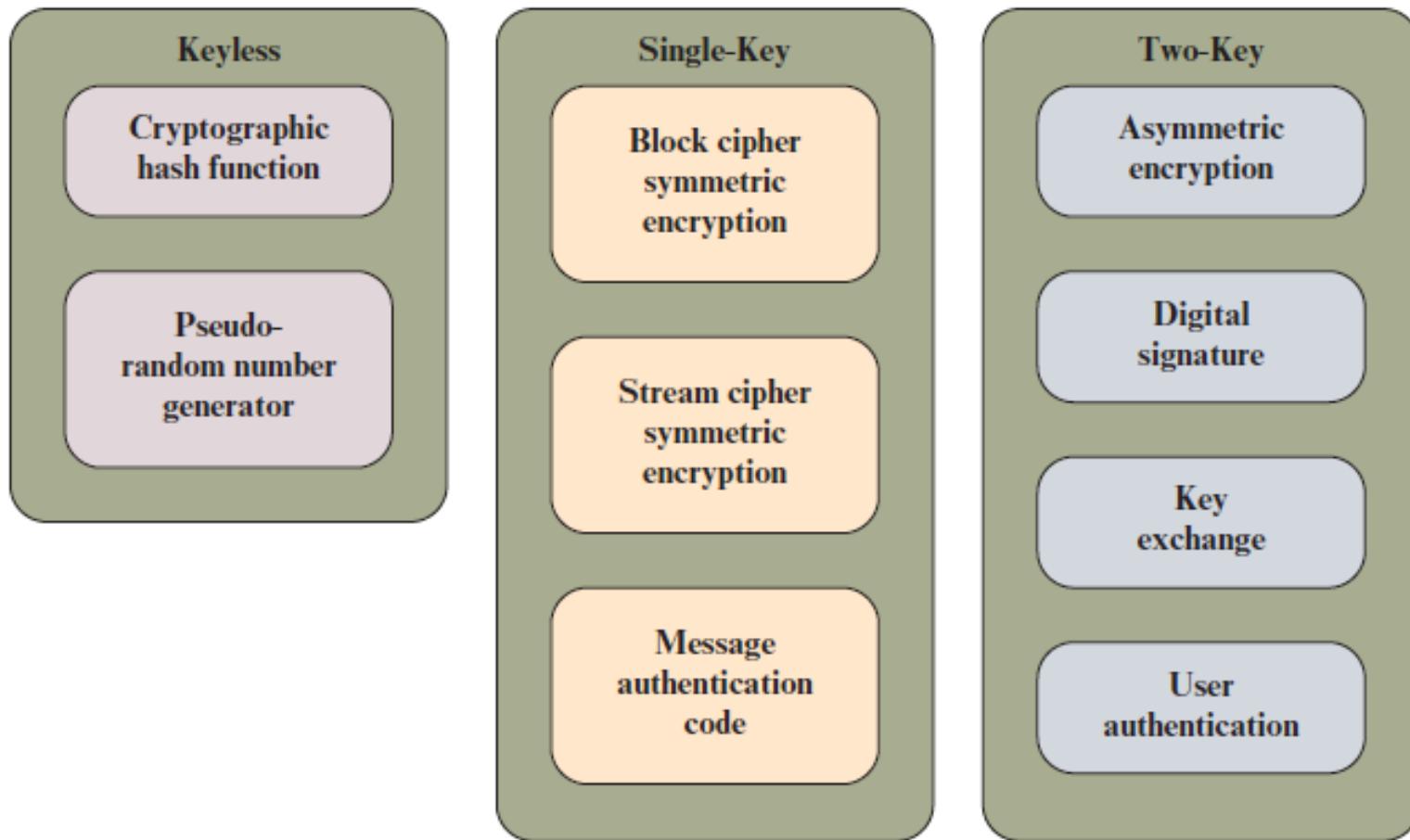
# Security Mechanisms (X.800)

- Specific security mechanisms provide some of the OSI security services:
  - Encipherment
  - Digital signatures (appending to prevent forgery)
  - Access controls
  - Data integrity
  - Authentication exchange
  - Traffic padding (insertion of bits to frustrate traffic analysis)
  - Routing control (selection of secure routes and possibility of route change)
  - Notarization (make use of a trusted third party)

# Security Mechanisms (X.800)

- Pervasive security mechanisms are not specific to any OSI security service or protocol layer:
  - Trusted functionality (perceived to be correct with respect to some criteria)
  - Security labels (designate a security attribute)
  - Event detection (detection of security-relevant events)
  - Security audit trails (data collected for security audit)
  - Security recovery (deals with requests from other mechanisms and takes recovery actions)

# Cryptographic Algorithms



# Cryptographic Algorithms

- Cryptographic algorithms can be divided into three categories:
  1. **Keyless**: Do not use any keys during cryptographic transformations.
  2. **Single-key**: The result of a transformation is a function of the input data and a single key, known as a secret key.
  3. **Two-key**: At various stages of the calculation, two different but related keys are used, referred to as a private key and a public key.

# Keyless Algorithms

- Keyless algorithms are deterministic functions that have certain properties useful for cryptography:
  - **Cryptographic Hash function** turns a variable amount of text into a small, fixed-length value, hash value, hash code, or digest.
  - **Pseudorandom Number Generator** produces a deterministic sequence of numbers or bits that has the appearance of being a truly random sequence.

# Single-key Algorithms

- They depend on the use of the secret key:
  - Protecting stored data that is only going to be accessed by the data creator.
  - Commonly, two parties share the secret key so that communication between the two parties (or a group of users) is protected.
  - Encryption algorithms that use a single key are referred to as **symmetric encryption** algorithms

# Symmetric Encryption

- **Block cipher**
  - A block cipher operates on data as a sequence of **blocks**.
  - A typical block size is **128 bits**.
  - In modes of operation, the transformation depends not only on the current data block and the secret key but also on the content of preceding blocks.
- **Stream cipher**
  - A stream cipher operates on data as a sequence of **bits**.
  - Typically, an **exclusive-OR** operation is used to produce a bit-by-bit transformation.
  - The transformation depends on a secret key.

# Symmetric Encryption

## ■ Message Authentication Code (MAC)

- A MAC is a data element associated with a data block or message.
- The MAC algorithm takes as input a message and secret key and produces the MAC.
- The recipient of the message plus the MAC can perform the same calculation on the message
- if the calculated MAC matches the MAC accompanying the message, this provides assurance that the message has not been altered.

# Two-key Algorithms

- A private key is known only to a single user or entity
- The corresponding public key is made available to a number of users.
- Asymmetric encryption can work in two ways:
  - An encryption algorithm takes as input some data to be protected and the private key and produces an unintelligible transformation on that data.
  - A corresponding decryption algorithm takes the transformed data and the corresponding public key and recovers the original data.
  - Only the possessor of the private key can have performed the encryption and any possessor of the public key can perform the decryption.
- An encryption algorithm takes as input some data to be protected and a public key and produces an unintelligible transformation on that data.
- A corresponding decryption algorithm takes the transformed data and the corresponding private key and recovers the original data.
- Any possessor of the public key can have performed the encryption and only the possessor of the private key can perform the decryption.

# Two-key Applications

## 1. Digital signature

- A value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
- Typically, the signer of a data object uses the **private key** to generate the signature, and anyone in possession of the corresponding public key can verify that validity of the signature.

## 2. Key exchange

- The process of securely distributing a symmetric key to two or more parties.

## 3. User authentication

- The process of authenticating that a user attempting to access an application or service is genuine and, similarly, that the application or service is genuine

# NETWORK SECURITY

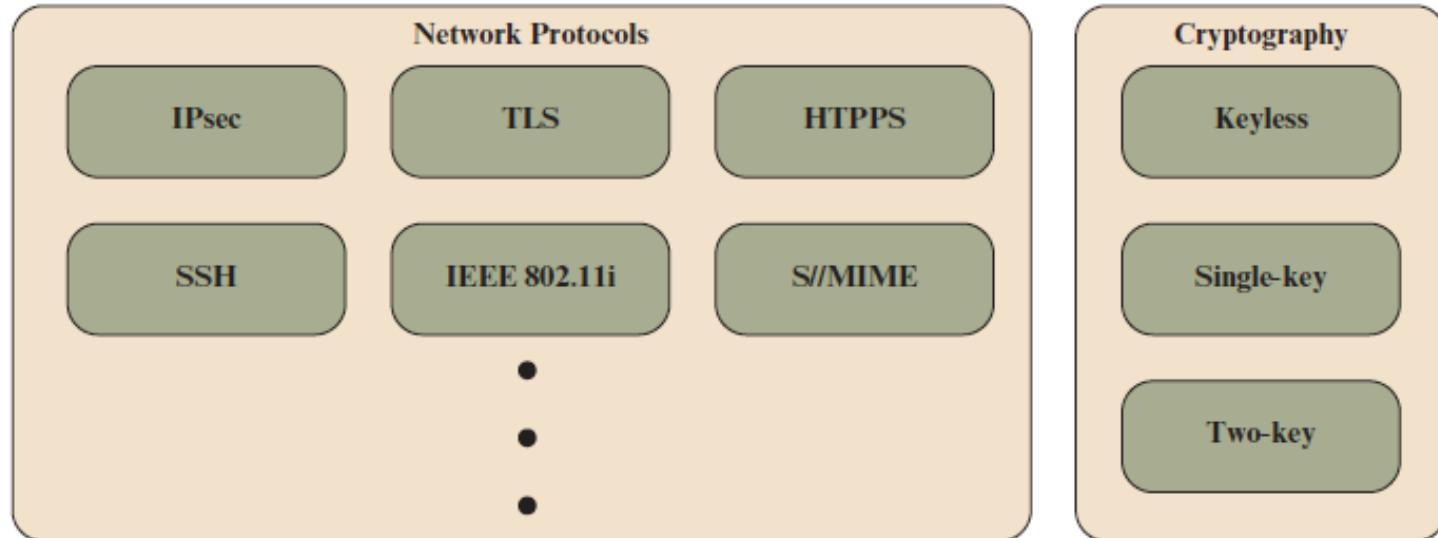
- **Communications Security**

- It deals with the protection of communications through the network, including measures to protect against both passive and active attacks
- It is primarily implemented using network protocols, the format and procedures that governs the transmitting and receiving of data between points in a network.
- A security protocol may be an enhancement that is part of an existing protocol or a standalone protocol.
  - IPsec, part of the Internet Protocol (IP)
  - IEEE 802.11i, part of the IEEE 802.11 Wi-Fi standard. Examples include the Transport Layer Security (TLS) and Secure Shell (SSH).
- One common characteristic of these protocols is that they use cryptographic algorithms as part of the mechanism to provide security

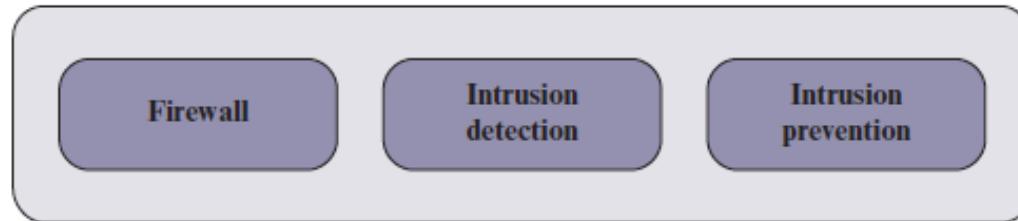
# NETWORK SECURITY

- **Device Security**
  - The protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers.
  - The primary security concerns are intruders that gain access to the system to perform unauthorized actions, insert malicious software (malware), or overwhelm system resources to diminish availability.
  - Important types of device security:
    1. **Firewall**: A hardware and/or software capability that limits access between a network and devices attached to the network, in accordance with a specific security policy. The firewall acts as a filter that permits or denies data traffic, both incoming and outgoing, using a set of rules based on traffic content and/or traffic pattern.
    2. **Intrusion detection**: Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding and providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner.
    3. **Intrusion prevention**: Hardware or software products designed to detect intrusive activity and attempt to stop the activity, ideally before it reaches its target.

# Elements of Network Security

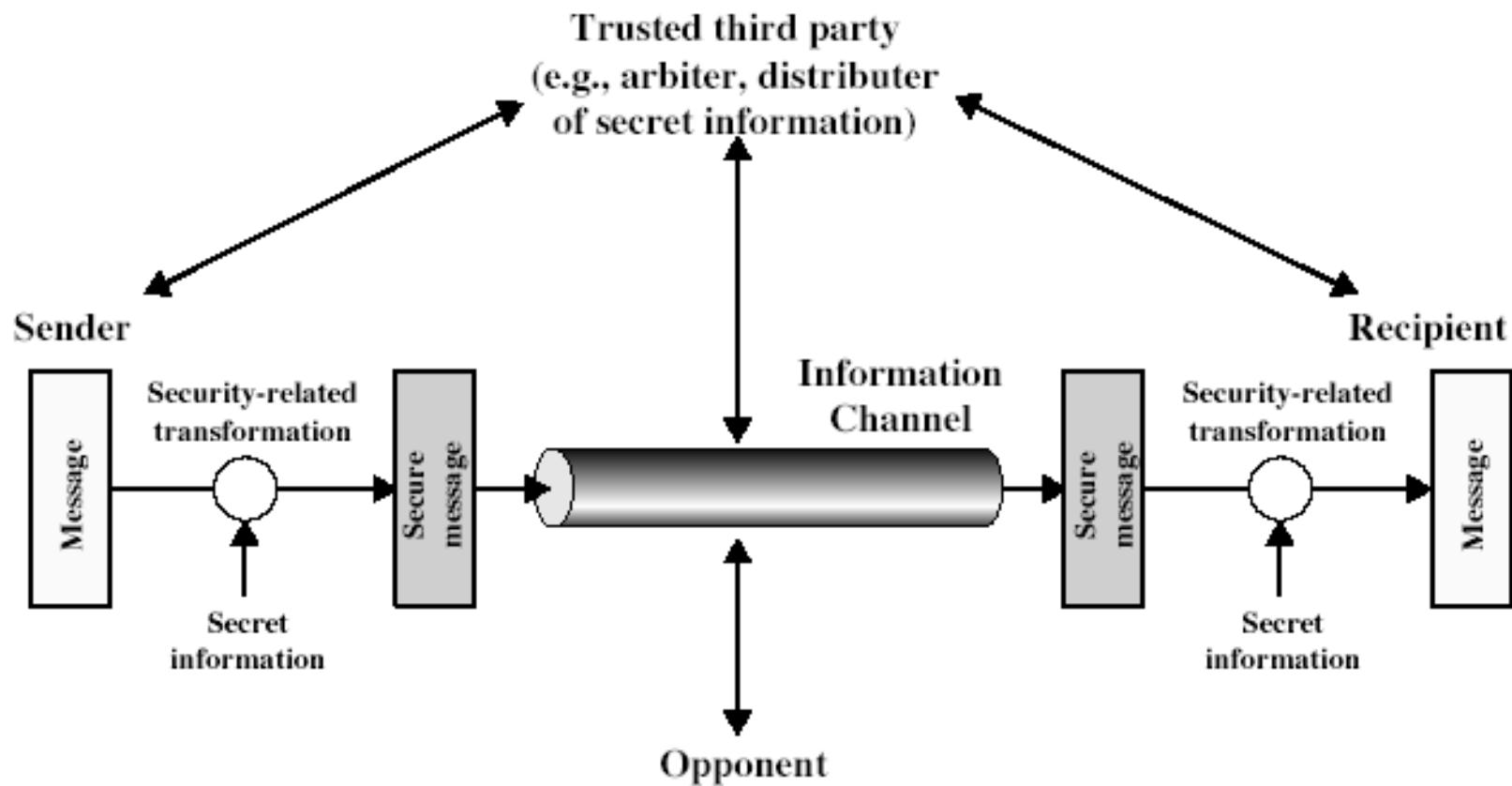


(a) Communications Security



(b) Device Security

# Model for Network Security



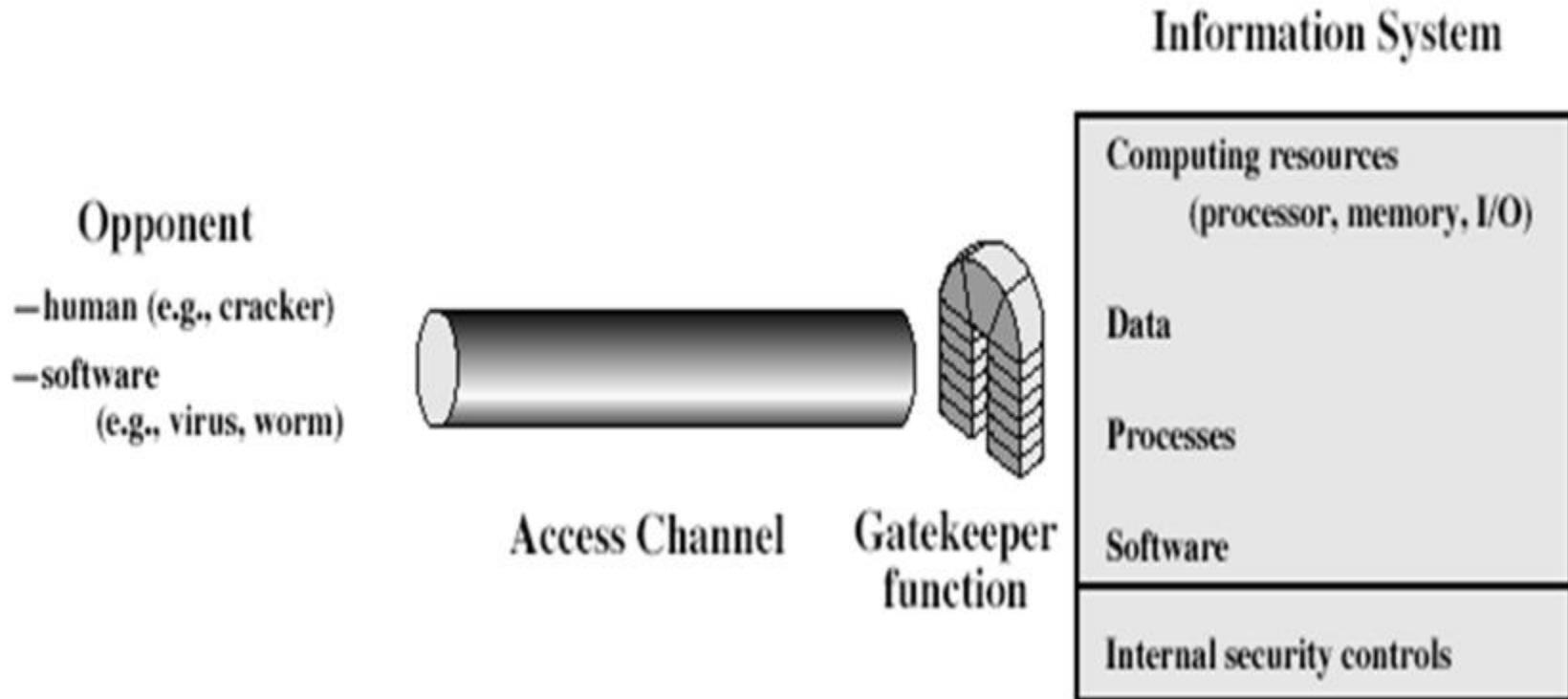
# Model for Network Security

- All the techniques for providing security have two components:
  - A transformation on the information such as encryption and the addition of a code based on the contents of the message to verify the sender.
  - Some secret information shared by the two principals and hopefully not known to the opponent such as an encryption key.

# Model for Network Security

- There are 4 basic tasks in designing a security service:
  1. Design a suitable algorithm for the security transformation.
  2. Generate the secret information (keys) used by the algorithm.
  3. Develop methods to distribute and share the secret information.
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service.

# Model for Network Access Security



# Model for Network Access Security

- Using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users (password-based)
  2. Implement security controls to ensure only authorised users access designated information or resources

# Summary

- Have considered:
  - definitions for:
    - computer, network, internet security
- X.800 standard.
- Security attacks, services, mechanisms.
- Models for network (access) security.