# Cyber Security

RAKSHITH P

Assistant Professor , CSE

JSS SCIENCE AND TECHNOLOGY UNIVERSITY

# What is Computer Security?

- *Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.*
- Computer security is the protection of the items you value, called the assets of a computer or computer system.
- There are many types of assets, involving hardware, software, data, people, processes, or combinations of these. To determine what to protect, we must first identify what has value and to whom

- Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues.
- The Internet has made our lives easier and has provided us with lots of advantages but it has also put our system's security at risk of being infected by a virus, of being hacked, information theft, damage to the system, and much more.
- Technology is growing day by day and the entire world is in its grasp. We cannot imagine even a day without electronic devices around us.
- With the use of this growing technology, invaders, hackers and thieves are trying to harm our computer's security for monetary gains, recognition purposes, ransom demands, bullying others, invading into other businesses, organizations, etc.

- A computer device (including hardware, added components, and accessories) is certainly an asset. Because most computer hardware is pretty useless without programs, the software is also an asset.
- Software includes the operating system, utilities and device handlers; applications such as word processing, media players or email handlers; and even programs that you may have written yourself.
- Much hardware and software is off-the-shelf, meaning that it is commercially available (not custom-made for your purpose) and that you can easily get a replacement.

- Three things—hardware, software, and data
- Other assets—such as access to data, quality of service, processes, human users, and network connectivity—deserve protection, too; they are affected or enabled by the hardware, software, and data.
- So in most cases, protecting hardware, software, and data covers these other assets as well.

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

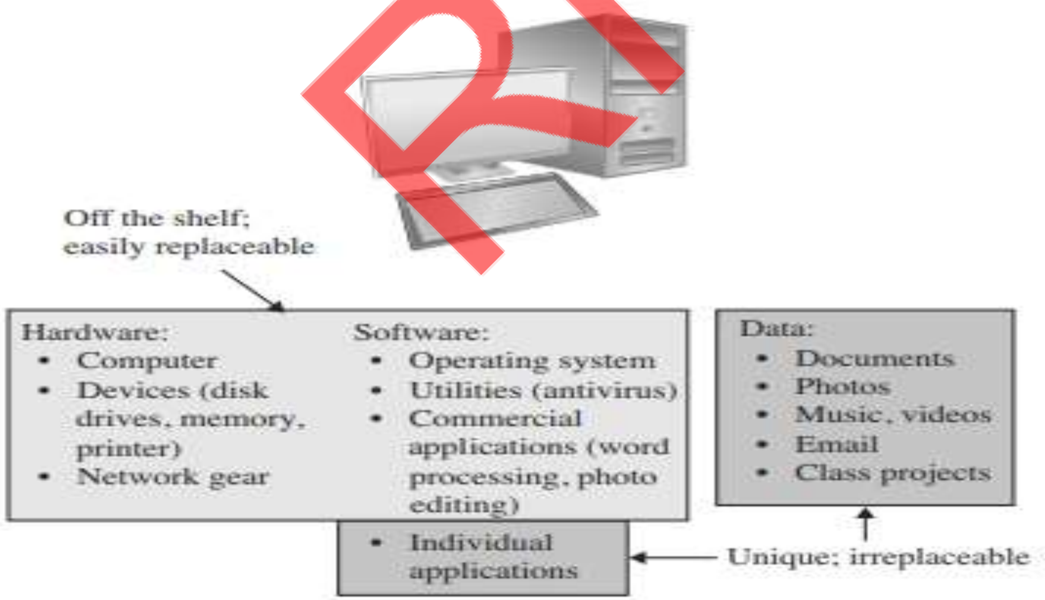
Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

**Computer systems—hardware, software, and data—have value and deserve security protection.**

FIGURE : Computer Objects of Value

# Value of an Asset

- The value of an asset depends on the asset owner’s or user’s perspective, and it may be independent of monetary cost, as shown in Figure



Off the shelf; easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

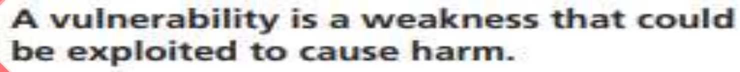
Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

Unique; irreplaceable

**Assets’ values are personal, time dependent, and often imprecise.**

# Vulnerability- Thread-control mechanism

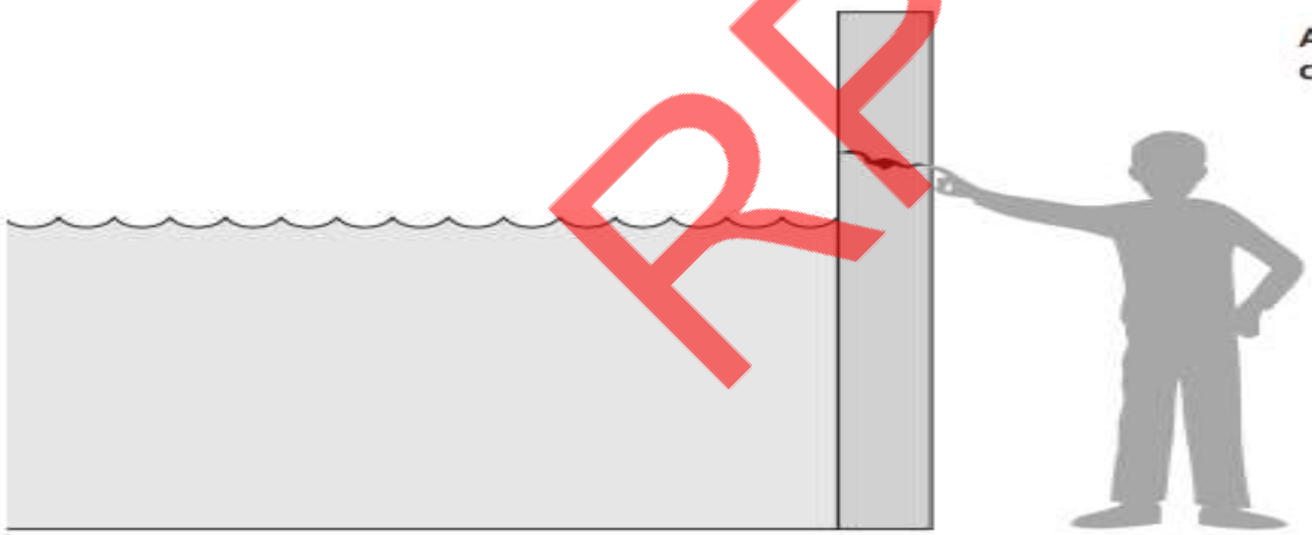
- The goal of computer security is protecting valuable assets. The different ways of protection, we use a framework that describes how assets may be harmed and how to counter or mitigate that harm.



A vulnerability is a weakness that could be exploited to cause harm.

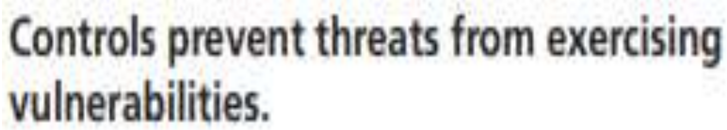
- A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user’s identity before allowing data access.

- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. To see the difference between a threat and a vulnerability, consider the illustration in Figure



A threat is a set of circumstances that could cause harm.

However, we can see a small crack in the wall—a vulnerability that threatens the man’s security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man



Controls prevent threats from exercising vulnerabilities.

- Control or countermeasure as protection. That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability.
- In Figure previous, the man is placing his finger in the hole, controlling the threat of water leaks until he finds a more permanent solution to the problem.
- In general, we can describe the relationship between threats, controls, and vulnerabilities in this way:

A threat is blocked by control of a vulnerability.

# THREADS

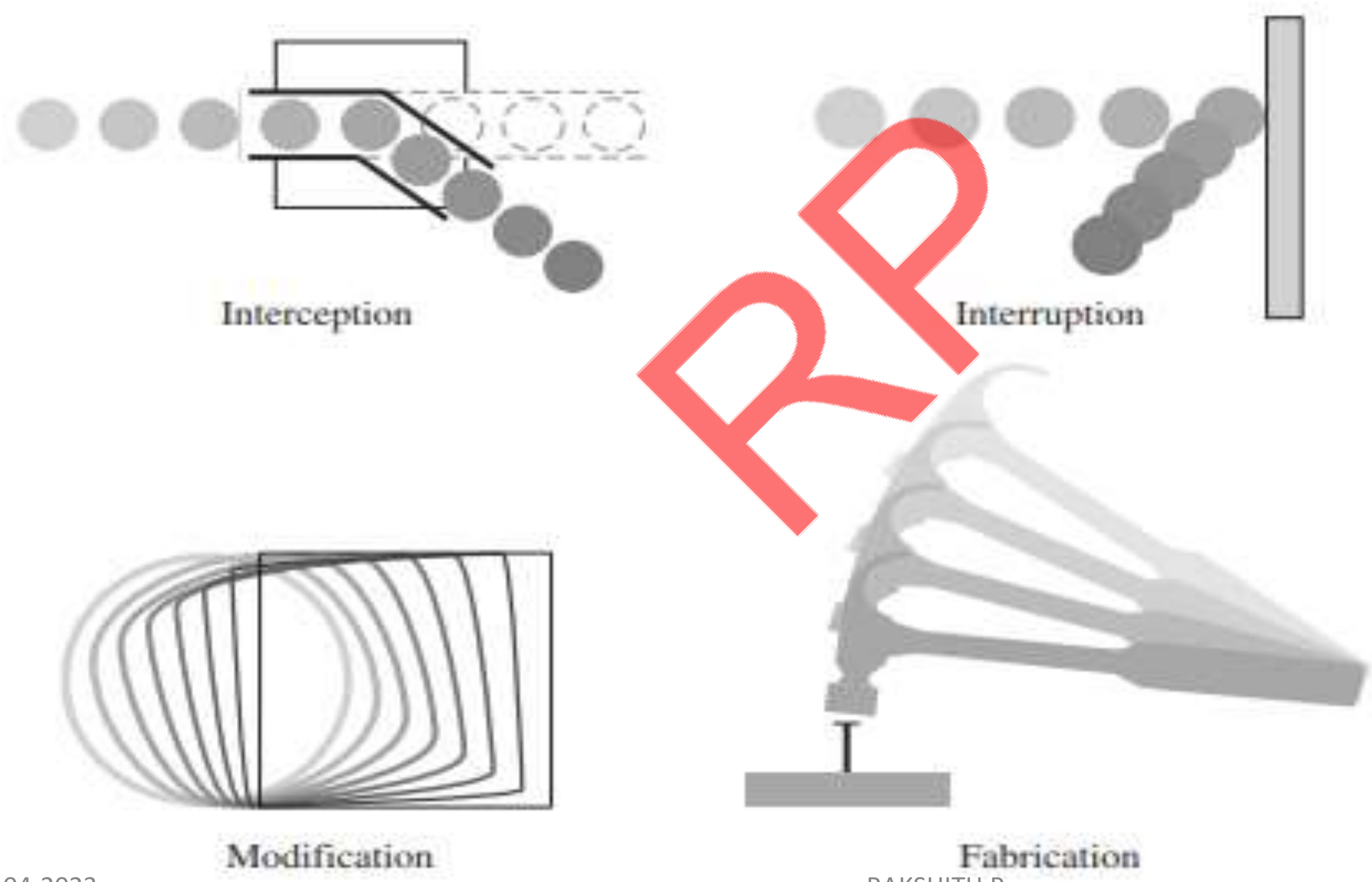
- We can consider potential harm to assets in two ways: First, we can look at what bad things can happen to assets, and second, we can look at who or what can cause or allow those bad things to happen. These two perspectives enable us to determine how to protect assets.
- Three aspects confidentiality, integrity, and availability, make your computer valuable to you. But viewed from another perspective, they are three possible ways to make it less valuable, that is, to cause you harm.
- If someone steals your computer, scrambles data on your disk, or looks at your private data files, the value of your computer has been diminished or your computer use has been harmed.

- These characteristics are both basic security properties and the objects of security threats. We can define these three properties as follows.
- • Availability: the ability of a system to ensure that an asset can be used by any authorized parties
- • Integrity: the ability of a system to ensure that an asset is modified only by authorized parties
- • Confidentiality: the ability of a system to ensure that an asset is viewed only by authorized parties

- Taken together (and rearranged), the properties are called the C-I-A triad or the security triad. ISO 7498-2 [ISO89] adds to them two more properties that are desirable, particularly in communication networks:
- • Authentication: the ability of a system to confirm the identity of a sender • Nonrepudiation or Accountability: the ability of a system to confirm that a sender cannot convincingly deny having sent something
- The U.S. Department of Defense [DOD85] adds auditability: the ability of a system to trace all actions related to a given asset.
- The C-I-A triad forms a foundation for thinking about security. Authenticity and nonrepudiation extend security notions to network communications, and auditability is important in establishing individual accountability for computer activity

C-I-A triad: confidentiality, integrity, availability

# Four Acts to Cause Security Harm



# Confidentiality

- The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Confidentiality** is the protection of information in the system so that an unauthorized person cannot access it. This type of protection is most important in military and government organizations that need to keep plans and capabilities secret from enemies.
- Some things obviously need confidentiality protection. For example, students' grades, financial transactions, medical records, and tax returns are sensitive. A proud student may run out of a classroom screaming "I got an A!" but the student should be the one to choose whether to reveal that grade to others.
- Other things, such as diplomatic and military secrets, companies' marketing and product development plans, and educators' tests, also must be carefully controlled. Confidentiality must be well-defined, and procedures for maintaining confidentiality must be carefully implemented.
- A crucial aspect of confidentiality is user identification and authentication. Positive identification of each system user is essential in order to ensure the effectiveness of policies that specify who is allowed access to which data items.

- Confidentiality relates most obviously to data, although we can think of the confidentiality of a piece of hardware (a novel invention) or a person (the whereabouts of a wanted criminal).

Here are some properties that could mean a failure of data confidentiality:

• An unauthorized person accesses a data item.

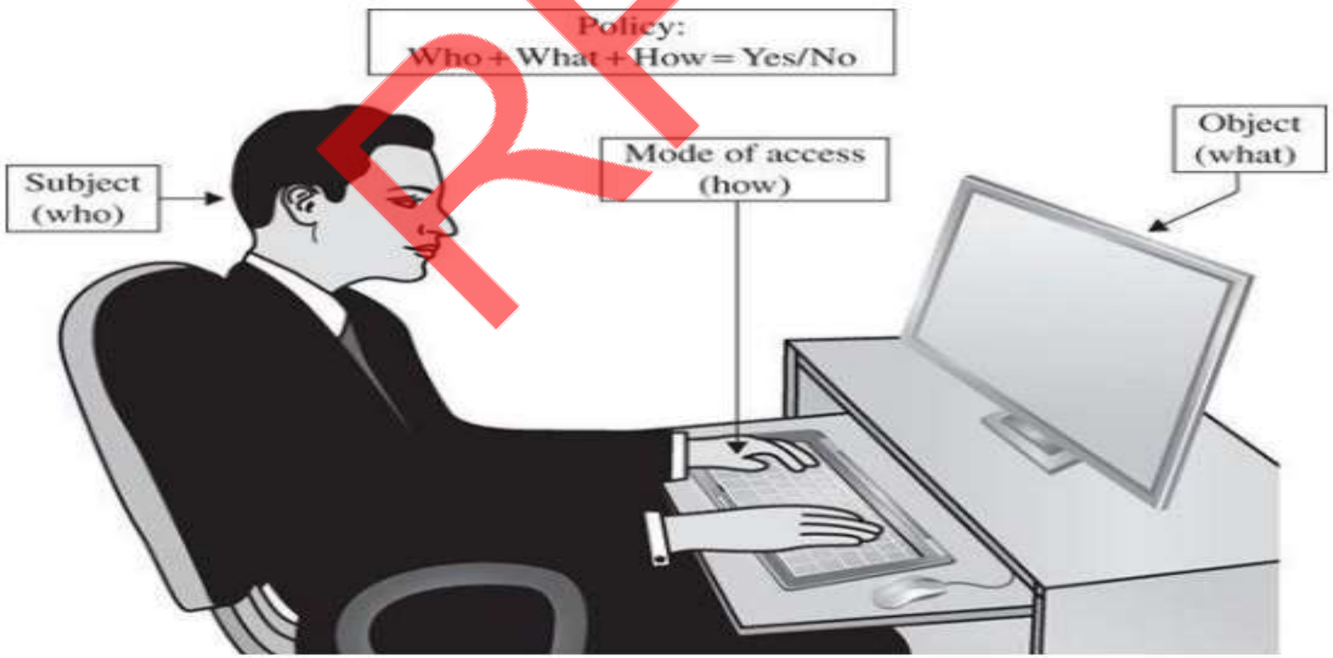
• An unauthorized process or program accesses a data item.

• A person authorized to access certain data accesses other data not authorized (which is a specialized version of “an unauthorized person accesses a data item”).

• An unauthorized person accesses an approximate data value (for example, not knowing someone’s exact salary but knowing that the salary falls in a particular range or exceeds a particular amount).

• An unauthorized person learns the existence of a piece of data (for example, knowing that a company is developing a certain new product or that talks are underway about the merger of two companies).

- A person, process, or program is (or is not) authorized to access a data item in a particular way. We call the person, process, or program a subject, the data item an object, the kind of access (such as read, write, or execute) an access mode, and the authorization a policy, as shown in Figure
- These four terms reappear throughout this book because they are fundamental aspects of computer security.



# Integrity

C
Confidentiality
The Information Security Triad
I
Integrity
A
Availability

- The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Integrity is the protection of system data from intentional or accidental unauthorized changes. The challenges of the security program are to ensure that data is maintained in the state that is expected by the users.
- Although the security program cannot improve the accuracy of the data that is put into the system by users. It can help ensure that any changes are intended and correctly applied. An additional element of integrity is the need to protect the process or program used to manipulate the data from unauthorized modification

- For example, if we say that we have preserved the integrity of an item, we may mean that the item is
- • Precise
- • Accurate
- • Unmodified
- • Modified only in acceptable ways
- • Modified only by authorized people
- • Modified only by authorized processes
- • Consistent
- • Internally consistent
- • Meaningful and usable

Integrity can be enforced in much the same way as can confidentiality: by rigorous control of who or what can access which resources in what ways

# Availability

- **Availability:** This means that the information is available to authorized users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels.
- Availability applies both to data and to services (that is, to information and to information processing), and it is similarly complex. As with the notion of confidentiality, different people expect availability to mean different things.

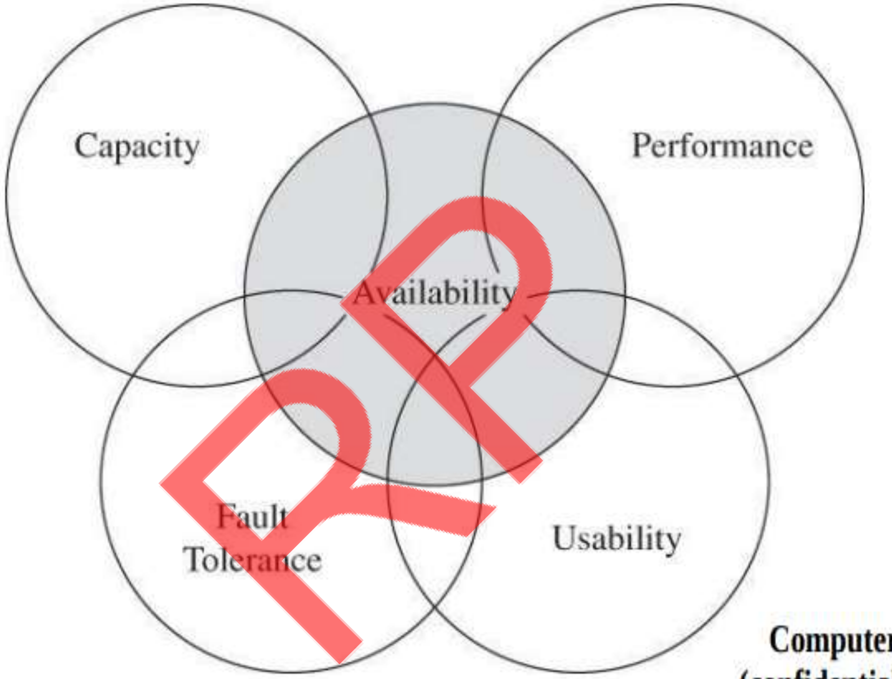
For example, an object or service is thought to be available if the following are true:

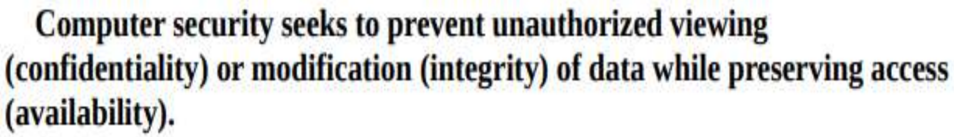
- • It is present in a usable form.
- • It has enough capacity to meet the service’s needs.
- • It is making clear progress, and, if in wait mode, it has a bounded waiting time.
- • The service is completed in an acceptable period of time.

# Following are some criteria to define availability

- • There is a timely response to our request.
- • Resources are allocated fairly so that some requesters are not favored over others.
- • Concurrency is controlled; that is, simultaneous access, deadlock management, and exclusive access are supported as required.
- • The service or system involved follows a philosophy of fault tolerance, whereby hardware or software faults lead to graceful cessation of service or to work-arounds rather than to crashes and abrupt loss of information.
- The service or system can be used easily and in the way it was intended to be used.

- In Figure  we depict some of the properties with which availability overlaps. Indeed, the security community is just beginning to understand what availability implies and how to ensure it.



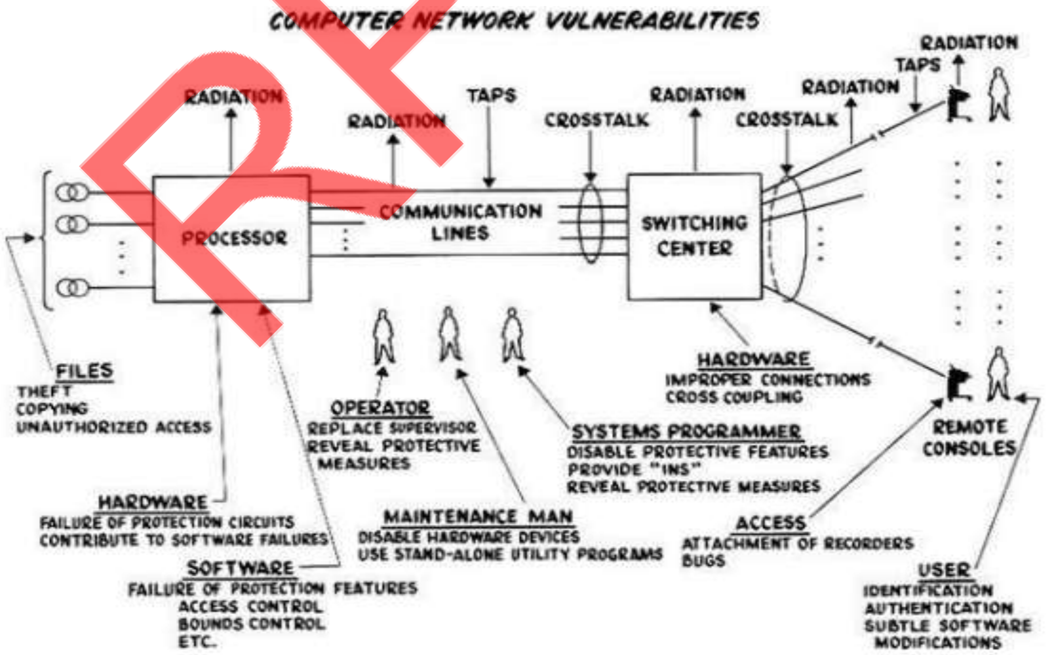

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability).

Availability and Related Aspects

A person or system can do three basic things with a data item: view it, modify it, or use it. Thus, viewing (confidentiality), modifying (integrity), and using (availability) are the basic modes of access that computer security seeks to preserve.

# Types of Threats

- For some ideas of harm, look at Figure , taken from Willis Ware's report [WAR70].
- Although it was written when computers were so big, so expensive, and so difficult to operate that only large organizations like universities, major corporations, or government departments would have one, Ware's discussion is still instructive today.
- Ware was concerned primarily with the protection of classified data, that is, preserving confidentiality. In the figure, he depicts humans such as programmers and maintenance staff gaining access to data, as well as radiation by which data can escape as signals. From the figure you can see some of the many kinds of threats to a computer system.

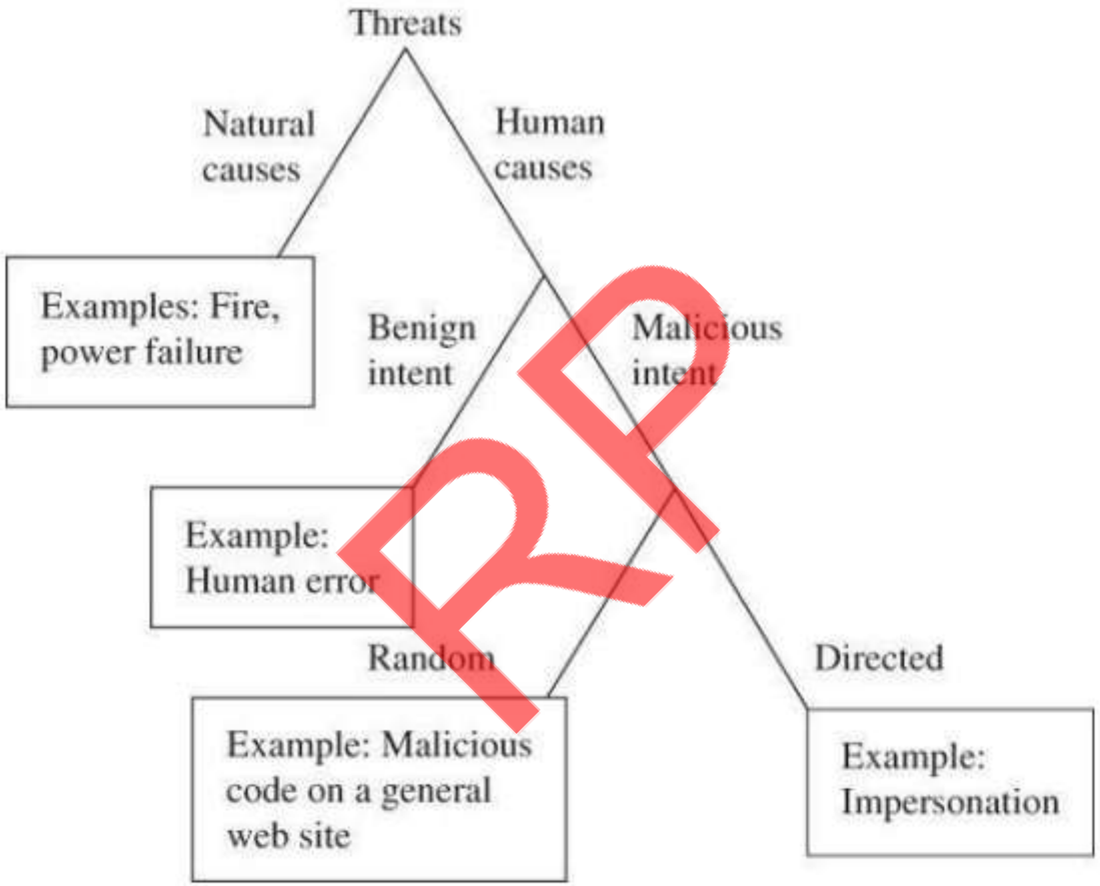


Computer [Network] Vulnerabilities (from [WAR70])

- **Random Attack**. The widespread attack, by a Hacking Event or Computer Virus, directed against the computer systems, software, Data, or telecommunications systems of multiple organizations or persons who are not part of the Covered Party, rather than solely at the Covered Party's computer systems, software, Data, or telecommunications systems. Such attack is intended for the purpose of fraud, nuisance, or malicious tampering or destruction.

- Direct-access attack is an attack where a hacker is able to gain access to a computer and be able to directly download data from it. They will be able to compromise security by modifying that software and adding key loggers, worms, etc. Eavesdropping is listening to a private conversation between hosts and network.

# Different kinds of threats are shown in Figure



Kinds of Threats

# Types of Attackers

- In computer and computer networks, an attacker is the individual or organization who performs the malicious activities to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- As the Internet access becomes more pervasive across the world, and each of us spends more time on the web, there is also an attacker grows as well.
- Attackers use every tools and techniques they would try and attack us to get unauthorized access.

# Reasons behind cyber attacks

- Every business, regardless of its size, is a potential target of cyber attack. That is because every business has key assets criminals may seek to exploit. Sometimes that is money or financial information. At other times, it may be the personal information of staff and customers, or even the business' infrastructure.
- By recognizing the common motives behind cyber attacks, you can build a better understanding of the risks you may face, and find out how best to confront them.

- Why do cyber attacks happen?
- Most often, cyber attacks happen because criminals want your:
- Business' financial details
- customers' financial details (eg credit card data)
- sensitive personal data
- customers' or staff email addresses and login credentials
- customer databases
- clients lists
- IT infrastructure
- IT services (eg the ability to accept online payments)
- Intellectual property (eg trade secrets or product designs)

# Motivations Behind Cyber-Attacks

# Types of cyber threats

- The threats countered by cyber-security are three-fold:
- 1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.
- 2. **Cyber-attack** often involves politically motivated information gathering.
- 3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

- Individuals attack :Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- Organized Crime: Cyber organized criminals have engaged in a variety of cybercrimes, including fraud, hacking, malware creation and distribution, DDoS attacks, blackmail, and intellectual property crime
- **Hacktivists:** Some groups of cyber criminals are driven by a particular political or social agenda. “Hacktivists” tend to be more interested in embarrassing companies or publicizing damning evidence of some sort and are usually not interested in robbing their targets of money or assets.
- **Terrorists:** The threat of terrorism increased significantly in the aftermath of the September 11 attacks. Thankfully, most terror organizations lack the technical savvy and resources to pull off major cyber attacks. In fact, according to The International Cyber Terrorism Regulation Project, terrorist cyber crime tends to involve mostly the publication of propaganda, psychological campaigns (such as beheading videos), intelligence, information sharing and other communication.

Computer as target of attack: Denial-of-service attacks and website defacements are popular activities for any political organization because they attract attention to the cause and bring undesired negative attention to the object of the attack. An example is the massive denial-of-service attack launched against the country.

Computer as method of attack: Launching offensive attacks requires the use of computers. Stuxnet, an example of malicious computer code called a worm, is known to attack automated control systems, specifically a model of control system manufactured by Siemens. Experts say the code is designed to disable machinery used in the control of nuclear reactors in Iran.

Computer as enabler of attack: Websites, web logs, and email lists are effective, fast, and inexpensive ways to allow many people to coordinate.

Computer as enhancer of attack: The Internet has proved to be an invaluable means for terrorists to spread propaganda and recruit agents

- **Insider threats:** Criminal organizations can also target insiders with blackmail. The goal is to obtain corporate secrets, sensitive data, passwords and other types of access to secure networks that could result in the theft of money or information.

- **Cyber attacks** are malicious attacks on computer systems and networks for damaging data or disrupting operations.
- Types of cyberattacks include:

- Malware attacks
- Ransomware
- Phishing
- Man-in-the-middle attacks
- Zero-day attacks
- Denial of Service (DoS) attacks
- SQL injection attack

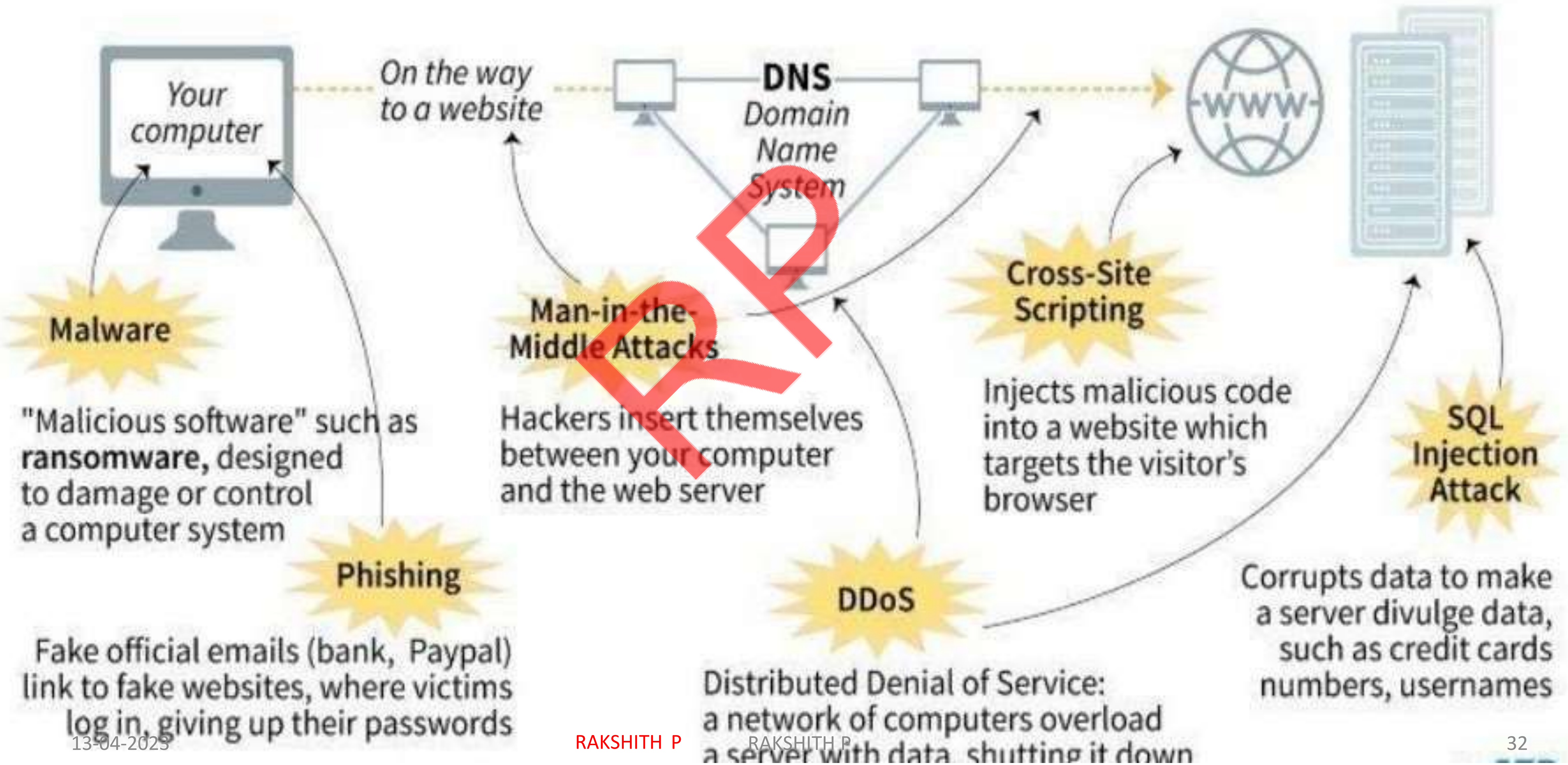
# Malware

- Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer.
- Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.
- There are a number of different types of malware, including:
- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

- **SQL injection**
- An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.
- **Phishing**
- Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.
- **Man-in-the-middle attack**
- A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.
- **Denial-of-service attack**
- A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

# The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*



**Malware**

"Malicious software" such as **ransomware,** designed to damage or control a computer system

**Phishing**

Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

**Man-in-the-Middle Attacks**

Hackers insert themselves between your computer and the web server

**DDoS**

Distributed Denial of Service: a network of computers overload a server with data, shutting it down

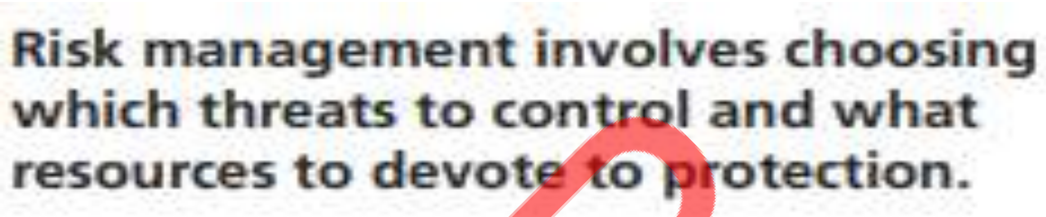
**Cross-Site Scripting**

Injects malicious code into a website which targets the visitor's browser

**SQL Injection Attack**

Corrupts data to make a server divulge data, such as credit cards numbers, usernames

- HARM:The negative consequence of an actualized threat is harm; we protect ourselves against threats in order to reduce or eliminate harm. We have already described many examples of computer harm: a stolen computer, modified or lost file, revealed private letter, or denied access to data. These events cause harm that we want to avoid.
- Choosing the threats we try to mitigate involves a process called risk management, and it includes weighing the seriousness of a threat against our ability to protect.



Risk management involves choosing which threats to control and what resources to devote to protection.

- RISK AND COMMON SENSE: The number and kinds of threats are practically unlimited because devising an attack requires an active imagination, determination, persistence, and time (as well as access and resources). The nature and number of threats in the computer world reflect life in general: The causes of harm are limitless and largely unpredictable.
- Natural disasters like volcanoes and earthquakes happen with little or no warning, as do auto accidents, heart attacks, influenza, and random acts of violence.
- Or we consider alternative courses of action, such as transferring risk by purchasing insurance or even doing nothing if the side effects of the countermeasure could be worse than the possible harm. The risk that remains uncovered by controls is called residual risk.

# METHOD – OPPORTUNITY-MOTIVE

- Method

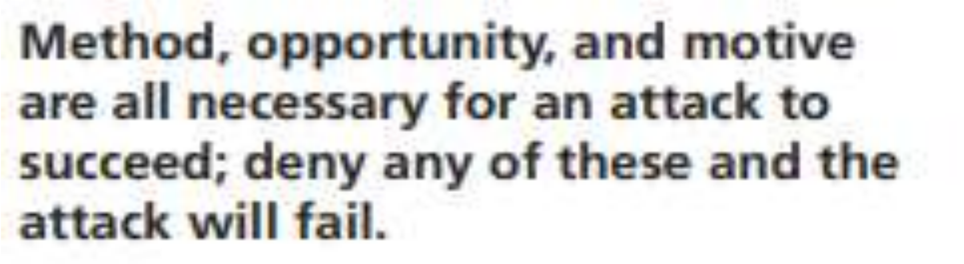
By method we mean the skills, knowledge, tools, and other things with which to perpetrate the attack.

Various attack tools—scripts, model programs, and tools to test for weaknesses—are available from hackers' sites on the Internet, to the degree that many attacks require only the attacker's ability to download and run a program.

Opportunity

Opportunity is the time and access to execute an attack.

Many computer systems present ample opportunity for attack. Systems available to the public are, by definition, accessible; often their owners take special care to make them fully available so that if one hardware component fails, the owner has spares instantly ready to be pressed into service.



Method, opportunity, and motive are all necessary for an attack to succeed; deny any of these and the attack will fail.

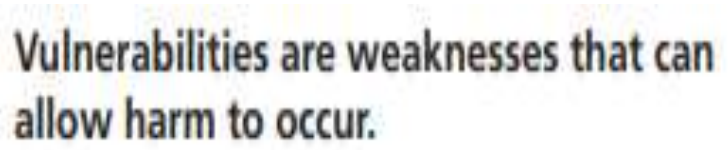
- Motive

Finally, an attacker must have a motive or reason to want to attack.

Motives for computer crime: money, fame, self-esteem, politics, terror. It is often difficult to determine motive for an attack.

Some places are “attractive targets,” meaning they are very appealing to attackers. Popular targets include law enforcement and defense department computers, perhaps because they are presumed to be well protected against attack (so they present a challenge and a successful attack shows the attacker’s prowess). Other systems are attacked because they are easy to attack.

# Vulnerabilities

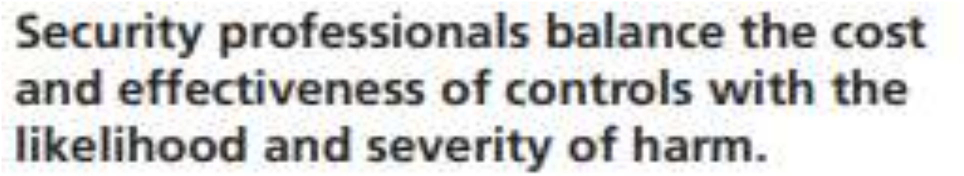


Vulnerabilities are weaknesses that can allow harm to occur.

- A vulnerability is a weakness in a procedure, protocol, hardware, or software within an organization that has the potential to cause damage.
- Computer systems have vulnerabilities, too. In this book we consider many, such as weak authentication, lack of access control, errors in programs, finite or insufficient resources, and inadequate physical protection.
- Paired with a credible attack, each of these vulnerabilities can allow harm to confidentiality, integrity, or availability. Each attack vector seeks to exploit a particular vulnerability

# CONTROLS

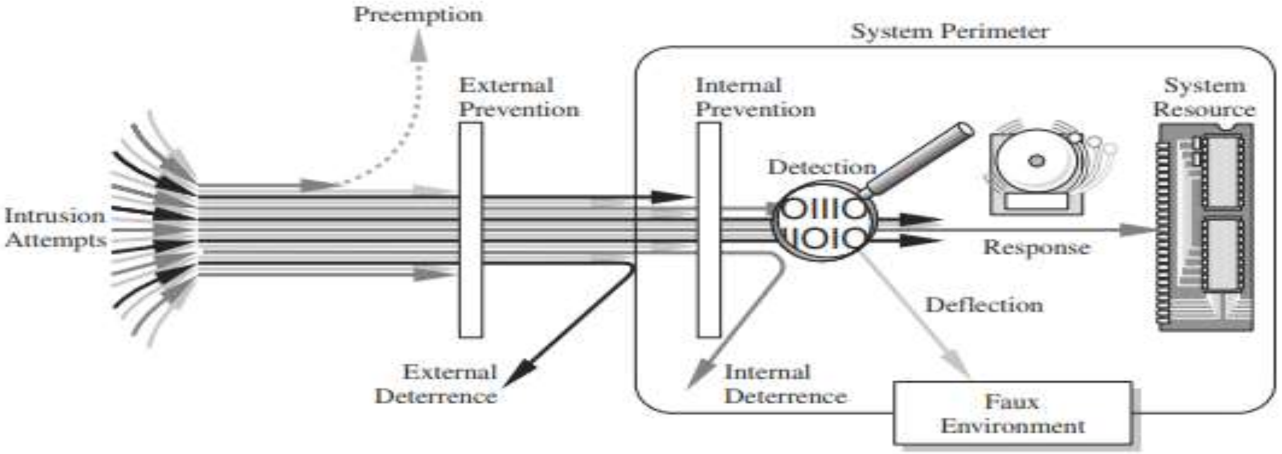
- A control or countermeasure is a means to counter threats. Harm occurs when a threat is realized against a vulnerability.
- To protect against harm, then, we can neutralize the threat, close the vulnerability, or both.
- The possibility for harm to occur is called risk. We can deal with harm in several ways:
- • Prevent it, by blocking the attack or closing the vulnerability
- • Deter it, by making the attack harder but not impossible
- • Deflect it, by making another target more attractive (or this one less so)
- • Mitigate it, by making its impact less severe
- • Detect it, either as it happens or some time after the fact
- • Recover from its effects



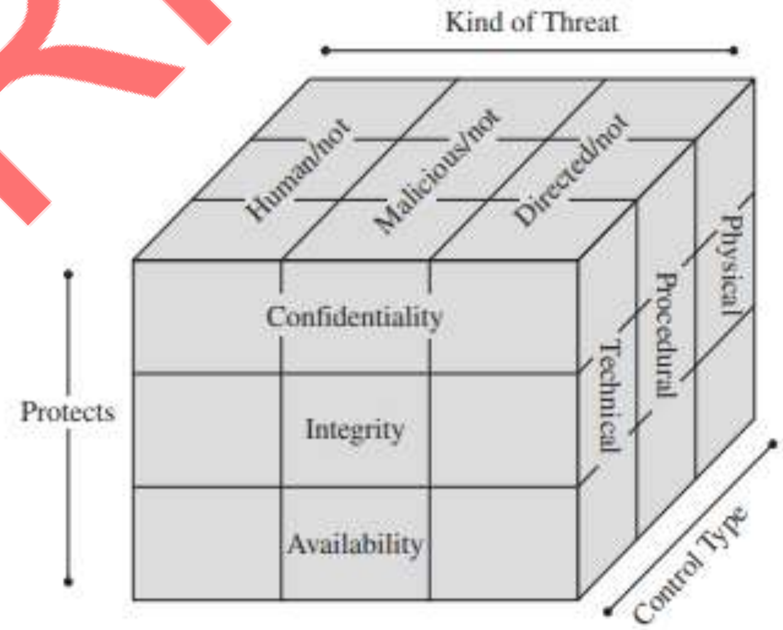
Security professionals balance the cost and effectiveness of controls with the likelihood and severity of harm.

# The following list shows the classes and several examples of each type of control.

- Physical controls stop or block an attack by using something tangible too, such as walls and fences
  - locks
  - (human) guards
  - sprinklers and other fire extinguishers
- Procedural or administrative controls use a command or agreement that
  - requires or advises people how to act; for example,
  - laws, regulations
  - policies, procedures, guidelines
  - copyrights, patents
  - contracts, agreements
- Technical controls counter threats with technology (hardware or software), including
  - passwords
  - program or operating system access controls
  - network protocols
  - firewalls, intrusion detection systems
  - encryption – network traffic flow regulators



- As shown in Figure , you can think in terms of the property to be protected and the kind of threat when you are choosing appropriate types of countermeasures.
- None of these classes is necessarily better than or preferable to the others; they work in different ways with different kinds of results.
- And it can be effective to use overlapping controls or defense in depth: more than one control or more than one class of control to achieve protection

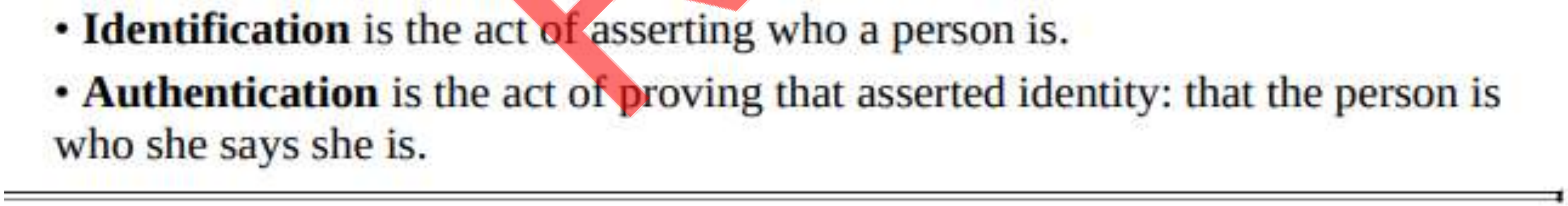


# CONCLUSION

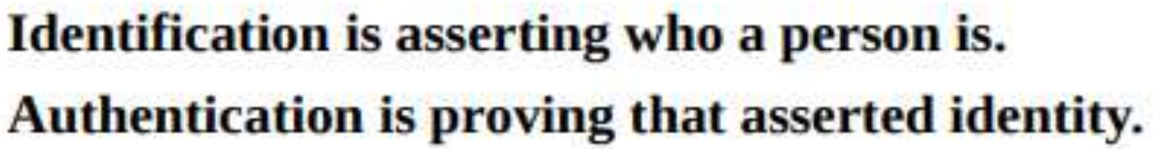
- Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems and their components.
- Three principal parts of a computing system are subject to attacks: hardware, software, and data.
- These three, and the communications among them, are susceptible to computer security vulnerabilities. In turn, those people and systems interested in compromising a system can devise attacks that exploit the vulnerabilities.

# Toolbox: Authentication, Access Control and Cryptography

- Authentication :In authentication, the user or computer has to prove its identity to the server or client. Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.

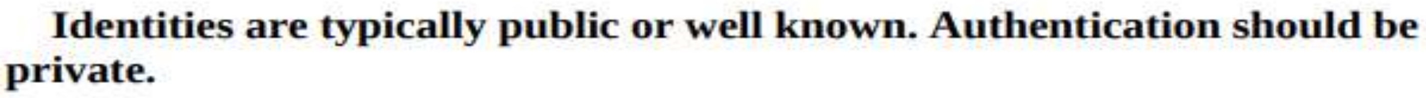


- **Identification** is the act of asserting who a person is.
- **Authentication** is the act of proving that asserted identity: that the person is who she says she is.



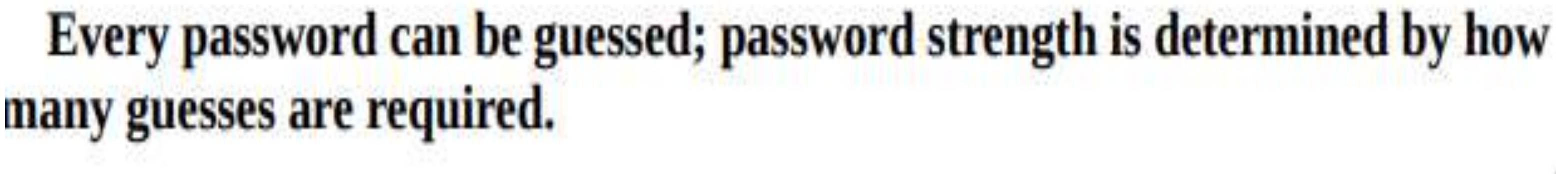
**Identification is asserting who a person is.**

**Authentication is proving that asserted identity.**



**Identities are typically public or well known. Authentication should be private.**

# Password Use



Every password can be guessed; password strength is determined by how many guesses are required.

- The use of passwords is fairly straightforward, as you probably already know from experience.
- A user enters some piece of identification, such as a name or an assigned user ID; this identification can be available to the public or can be easy to guess because it does not provide the real protection.
- Even though passwords are widely used, they suffer from some difficulties of use:
- • Use. Supplying a password for each access to an object can be inconvenient and time consuming.
- • Disclosure. If a user discloses a password to an unauthorized individual, the object becomes immediately accessible. If the user then changes the password to re-protect the object, the user must inform any other legitimate users of the new password because their old password will fail.
- • Revocation. To revoke one user’s access right to an object, someone must change the password, thereby causing the same problems as disclosure.
- • Loss. Depending on how the passwords are implemented, it may be impossible to retrieve a lost or forgotten password. The operators or system administrators can certainly intervene and provide a new password

# DICTIONARY ATTACK

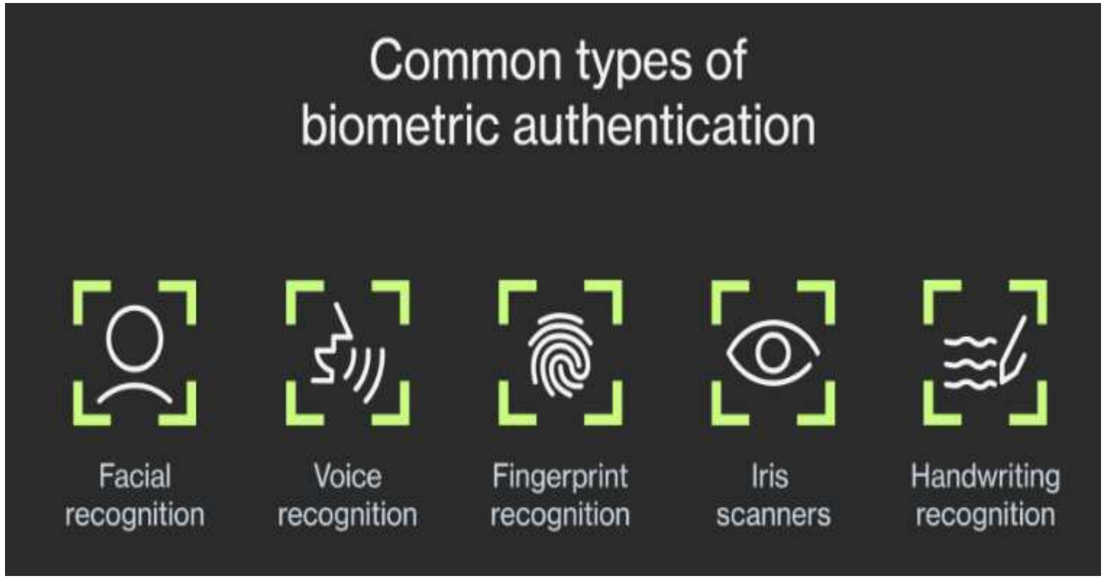
- A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary as a password.
- A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.
- A dictionary attack is a systematic method of guessing a password by trying many common words and their simple variations.
- Attackers use extensive lists of the most commonly used passwords, popular pet names, fictional characters, or literally just words from a dictionary – hence the name of the attack. They also change some letters to numbers or special characters, like “p@ssw0rd”.

# Good Passwords

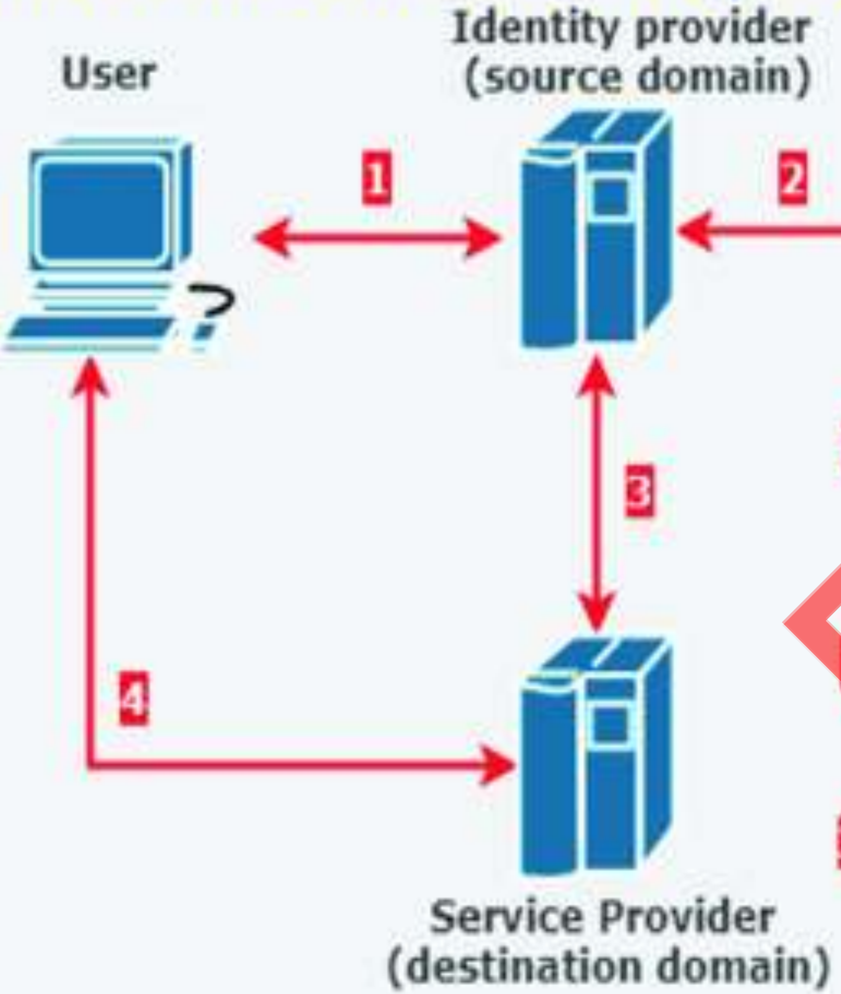
- We can improve their security by a few simple practices:
- • Choose long passwords. The combinatorial explosion of password guessing difficulty begins around length 4 or 5. Choosing longer passwords makes it less likely that a password will be uncovered.
- • Avoid actual names or words. Theoretically, there are 26 ^6 , or about 300 million 6-letter “words” (meaning any combination of letters), but there are only about 150,000 words in a good collegiate dictionary, ignoring length
- • Use a string you can remember. Password choice is a double bind. To remember the password easily, you want one that has special meaning to you.
- • Use variants for multiple passwords. With accounts, websites, and subscriptions, an individual can easily amass 50 or 100 passwords, which is clearly too many to remember.
- • Change the password regularly. Even if you have no reason to suspect that someone has compromised the password, you should change it from time to time.
- Don’t write it down. Note: This time-honored advice is relevant only if physical security is a serious risk. People who have accounts on many machines and servers, and with many applications or sites, may have trouble remembering all the access codes

# Authentication Based on Biometrics:

- • Fingerprint
- • Hand geometry (shape and size of fingers)
- • Retina and iris (parts of the eye)
- • Voice
- • Handwriting, signature, hand motion
- • Typing characteristics
- • Blood vessels in the finger or hand
- • Face
- • Facial features, such as nose shape or eye spacing



# How federated identity works


User
Identity provider (source domain)
Administrator
1
2
3
4
Service Provider (destination domain)

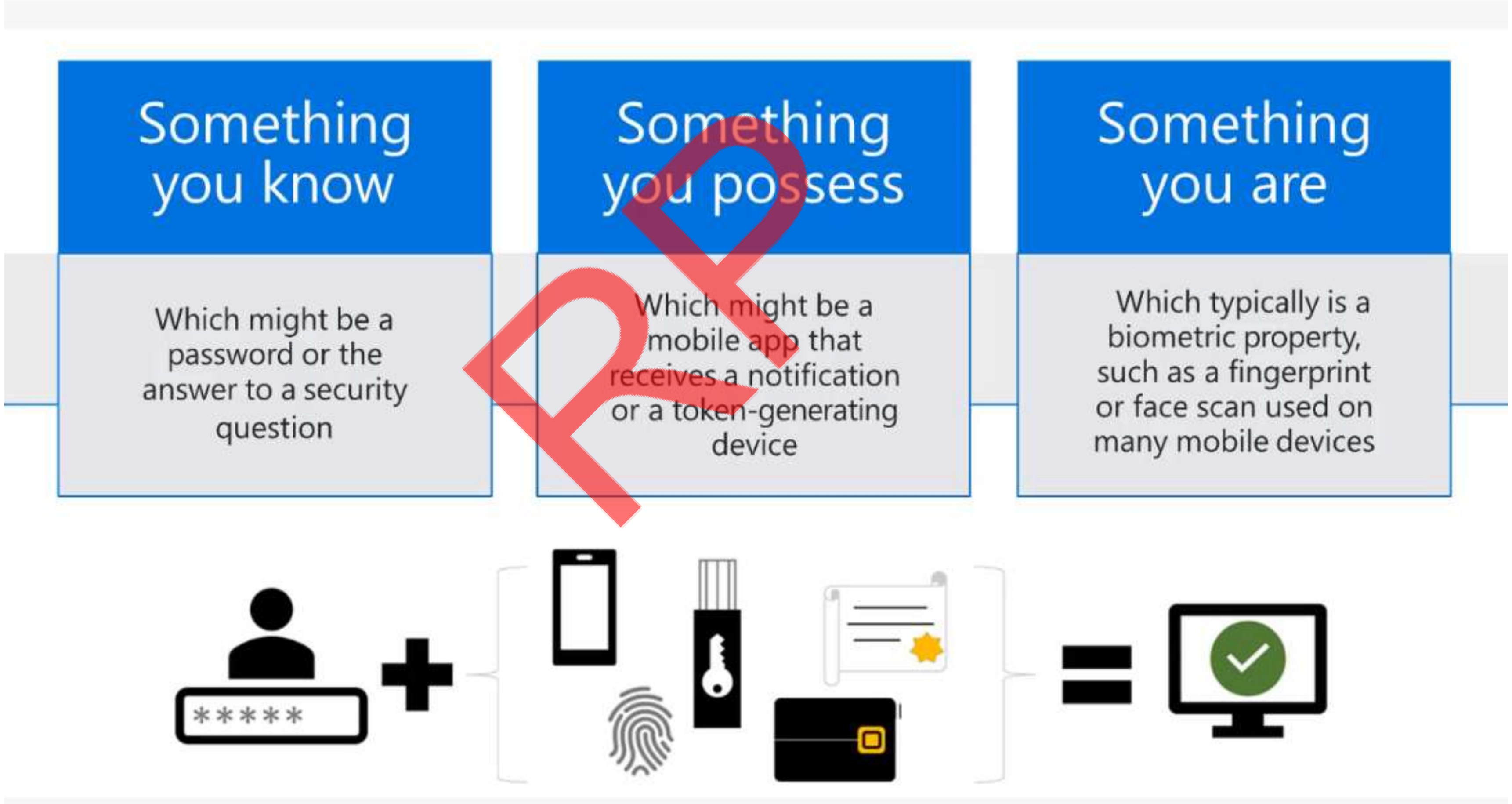
1 User's browser or other application engages in an authentication dialogue with identity provider in the same domain, providing attribute values associated with their identity.

2 Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.

3 A Service provider in a remote domain that a user wants to access obtains identity information, authentication information and associated attributes from the identity provider in the source domain.

4 Service provider opens session with remote users and enforces access control restrictions based on users's identity and attributes.

# Multifactor Authentication



Something you know

Which might be a password or the answer to a security question

Something you possess

Which might be a mobile app that receives a notification or a token-generating device

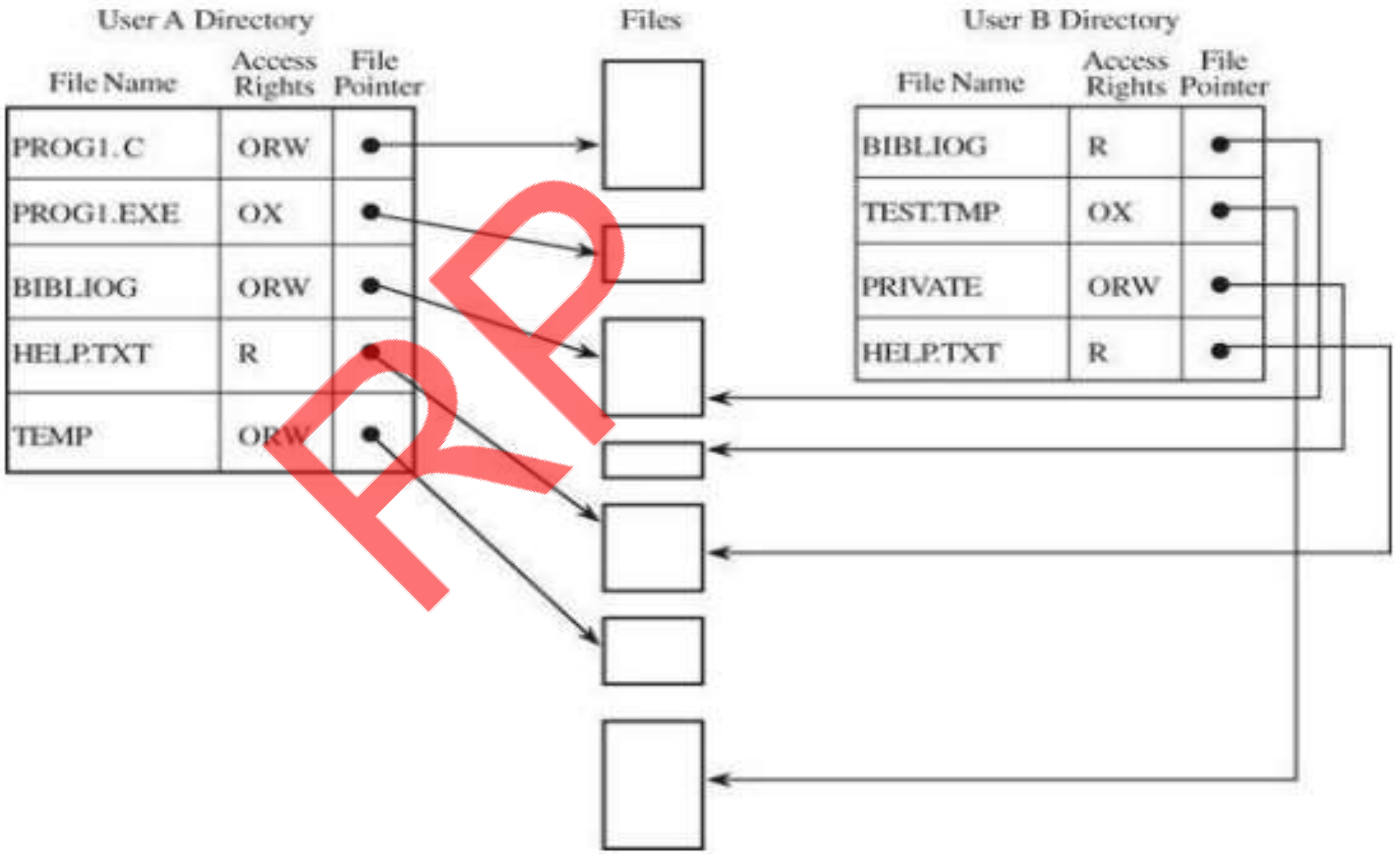
Something you are

Which typically is a biometric property, such as a fingerprint or face scan used on many mobile devices

# Access Control Directory

- One simple way to protect an object is to use a mechanism that works like a file directory. Imagine we are trying to protect files (the set of objects) from users of a computing system (the set of subjects). Every file has a unique owner who possesses “control” access rights (including the rights to declare who has what access) and to revoke access of any person at any time.
- Each user has a file directory, which lists all the files to which that user has access.
- The operating system must maintain all file directories, under commands from the owners of files. The obvious rights to files are the common read, write, and execute that are familiar on many shared systems.

- Furthermore, another right, owner, is possessed by the owner, permitting that user to grant and revoke access rights. Figure shows an example of a file directory.



User A Directory

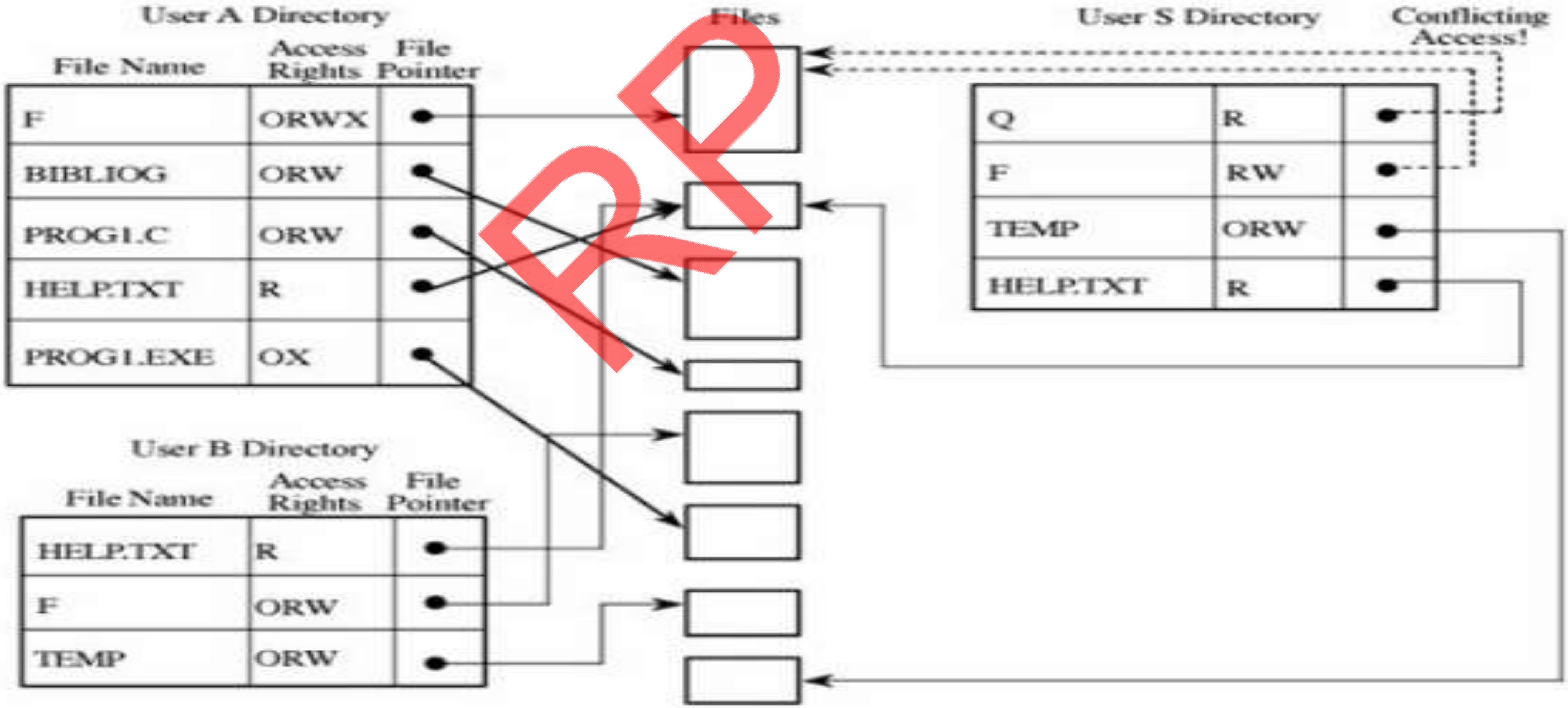
| File Name | Access Rights | File Pointer |
|---|---|---|
| PROG1.C | ORW | ● |
| PROG1.EXE | OX | ● |
| BIBLIOG | ORW | ● |
| HELP.TXT | R | ● |
| TEMP | ORW | ● |

User B Directory

| File Name | Access Rights | File Pointer |
|---|---|---|
| BIBLIOG | R | ● |
| TEST.TMP | OX | ● |
| PRIVATE | ORW | ● |
| HELP.TXT | R | ● |

This approach is easy to implement because it uses one list per user, naming all the objects that user is allowed to access. However, several difficulties can arise. First, the list becomes too large if many shared objects, such as libraries of subprograms or a common table of users, are accessible to all users.

- Owners A and B may have two different files named F, and they may both want to allow access by S. Clearly, the directory for S cannot contain two entries under the same name for different files. Therefore, S has to be able to uniquely identify the F for A (or B). One approach is to include the original owner's designation as if it were part of the file name, with a notation such as A:F (or B:F).
- Suppose, however, that S has trouble remembering file contents from the name F. Another approach is to allow S to name F with any name unique to the directory of S. Then, F from A could be called Q to S. As shown in Figure, S may have forgotten that Q is F from A, and so S requests access again from A for F.



User A Directory

| File Name | Access Rights | File Pointer |
|---|---|---|
| F | ORWX | ● |
| BIBLIOG | ORW | ● |
| PROG1.C | ORW | ● |
| HELP.TXT | R | ● |
| PROG1.EXE | OX | ● |

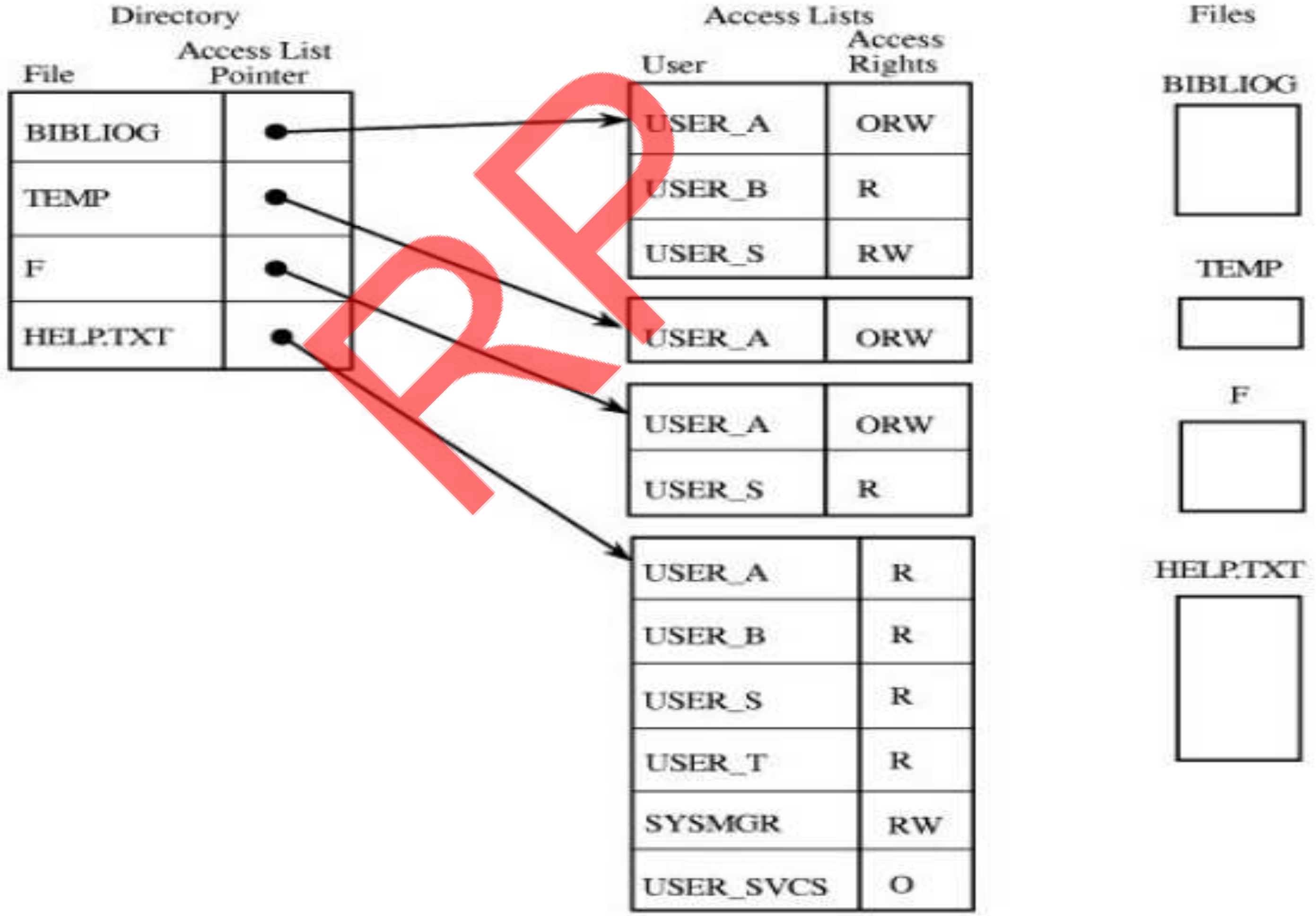
User B Directory

| File Name | Access Rights | File Pointer |
|---|---|---|
| HELP.TXT | R | ● |
| F | ORW | ● |
| TEMP | ORW | ● |

User S Directory

| | | |
|---|---|---|
| Q | R | ● |
| F | RW | ● |
| TEMP | ORW | ● |
| HELP.TXT | R | ● |

- An alternative representation is the access control list. There is one such list for each object, and the list shows all subjects who should  have access to the object and what their access is. This approach differs from the directory list because there is one access control list per object; a directory is created for each subject. Although this difference seems small, there are some significant advantages.
- To see how, consider subjects A and S, both of whom have access to object F. The operating system will maintain just one access list for F, showing the access rights for A and S, as shown in Figure . The access control list can include general default entries for any users.



| File | Access List Pointer |
|---|---|
| BIBLIOG | ● |
| TEMP | ● |
| F | ● |
| HELP.TXT | ● |

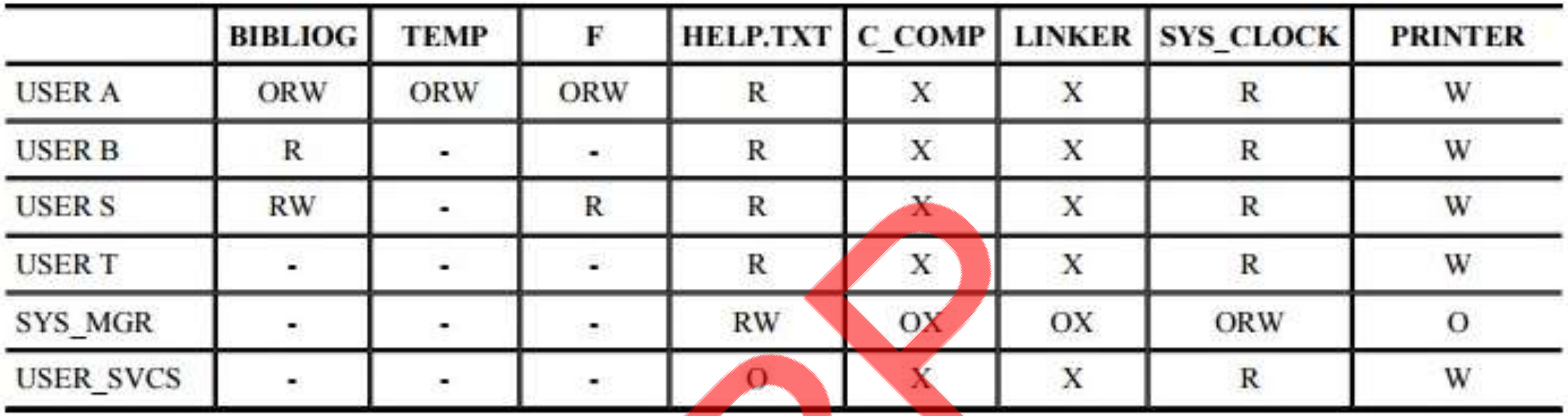
| User | Access Rights |
|---|---|
| USER_A | ORW |
| USER_B | R |
| USER_S | RW |

| User | Access Rights |
|---|---|
| USER_A | ORW |

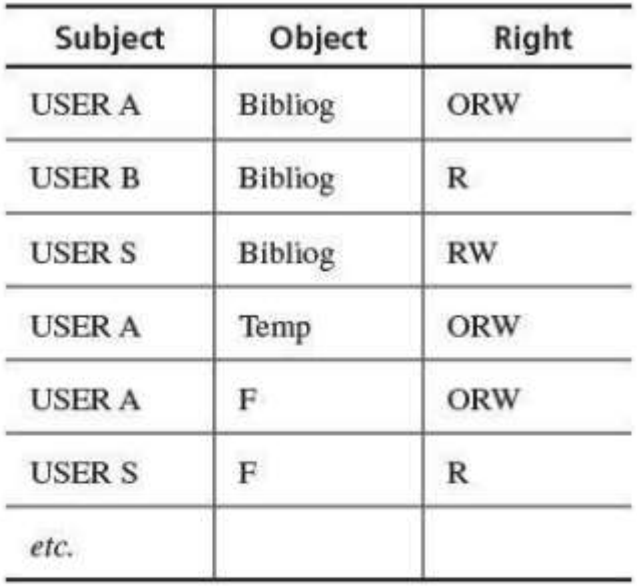
| User | Access Rights |
|---|---|
| USER_A | ORW |
| USER_S | R |

| User | Access Rights |
|---|---|
| USER_A | R |
| USER_B | R |
| USER_S | R |
| USER_T | R |
| SYSMGR | RW |
| USER_SVCS | O |

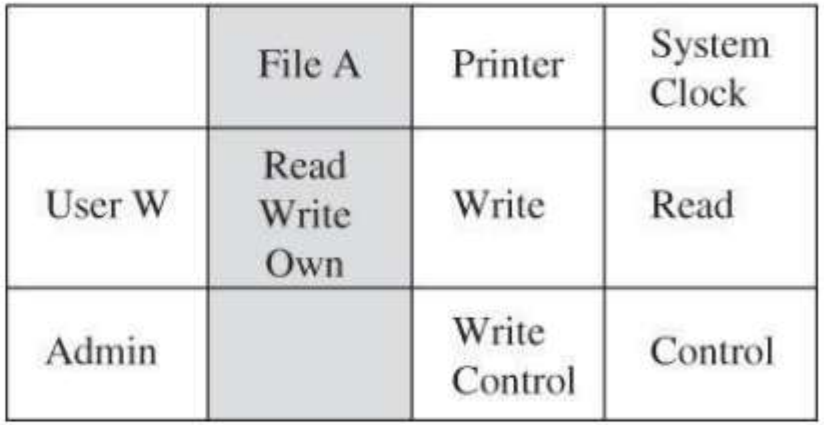
# Access Control Matrix



| | BIBLIOG | TEMP | F | HELP.TXT | C_COMP | LINKER | SYS_CLOCK | PRINTER |
|---|---|---|---|---|---|---|---|---|
| USER A | ORW | ORW | ORW | R | X | X | R | W |
| USER B | R | - | - | R | X | X | R | W |
| USER S | RW | - | R | R | X | X | R | W |
| USER T | - | - | - | R | X | X | R | W |
| SYS_MGR | - | - | - | RW | OX | OX | ORW | O |
| USER_SVCS | - | - | - | O | X | X | R | W |



| Subject | Object | Right |
|---|---|---|
| USER A | Bibliog | ORW |
| USER B | Bibliog | R |
| USER S | Bibliog | RW |
| USER A | Temp | ORW |
| USER A | F | ORW |
| USER S | F | R |
| *etc.* | | |



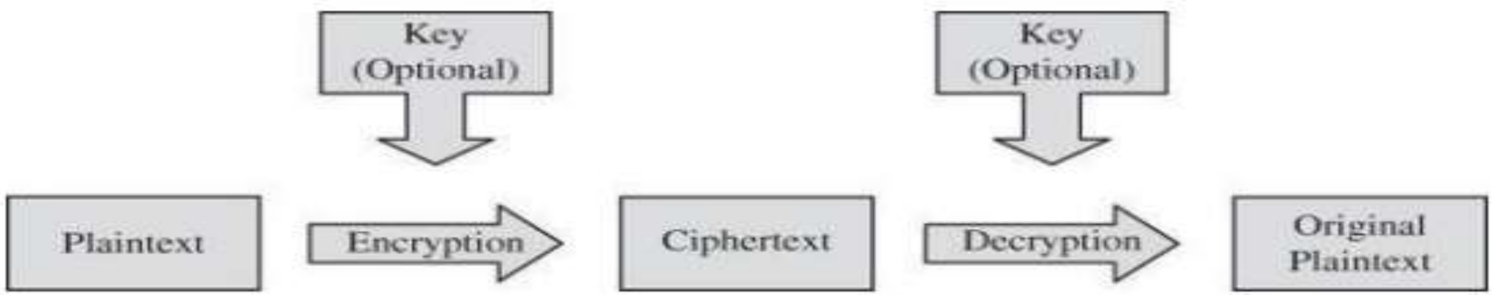
| | File A | Printer | System Clock |
|---|---|---|---|
| User W | Read<br>Write<br>Own | Write | Read |
| Admin | | Write<br>Control | Control |

# Cryptography

- Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.
- In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.
- These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

# Features Of Cryptography are as follows:

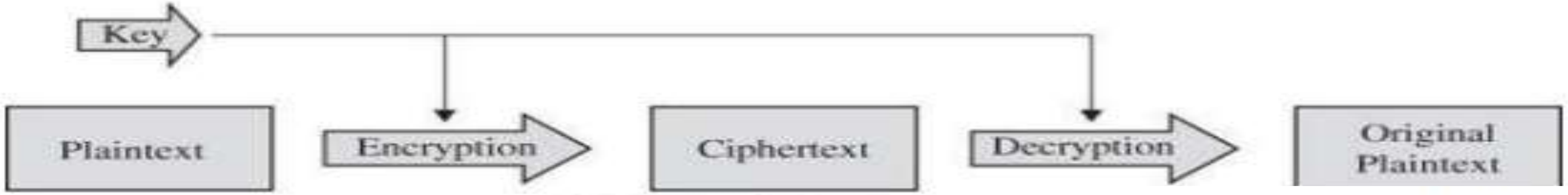
- **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
- **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at later stage.
- **Authentication:** The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.



# Types Of Cryptography: In general there are three types Of cryptography:

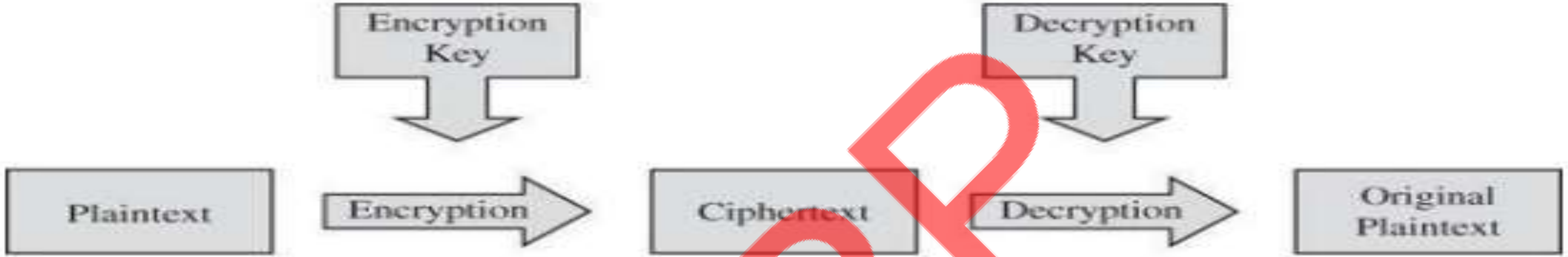
- **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).
- **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
- **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

## Symmetric encryption: one key encrypts and decrypts.



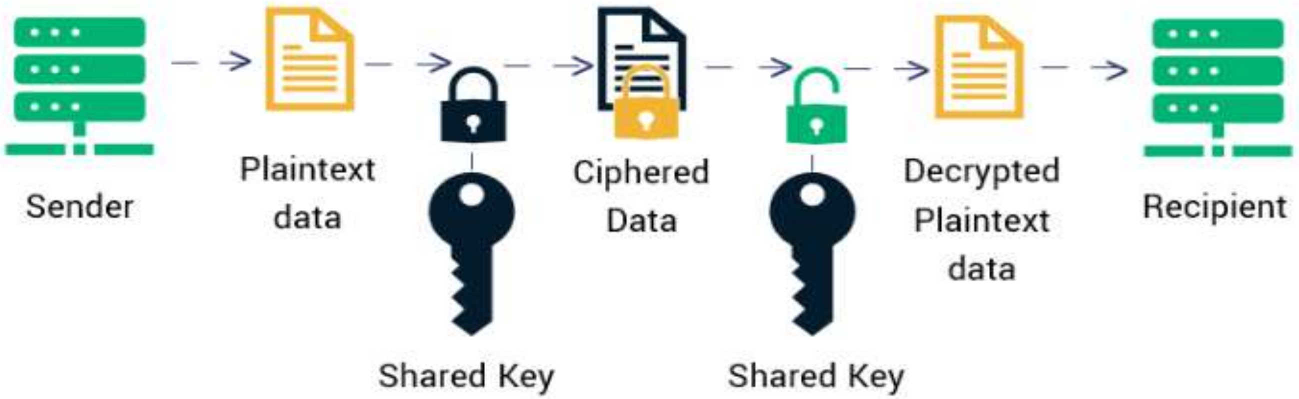
(a) Symmetric Cryptosystem

## Asymmetric encryption: one key encrypts, a different key decrypts.

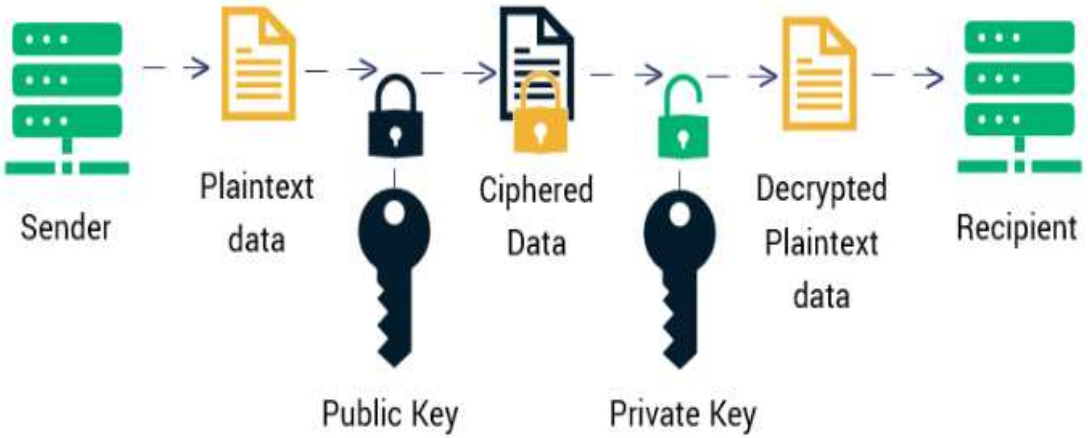


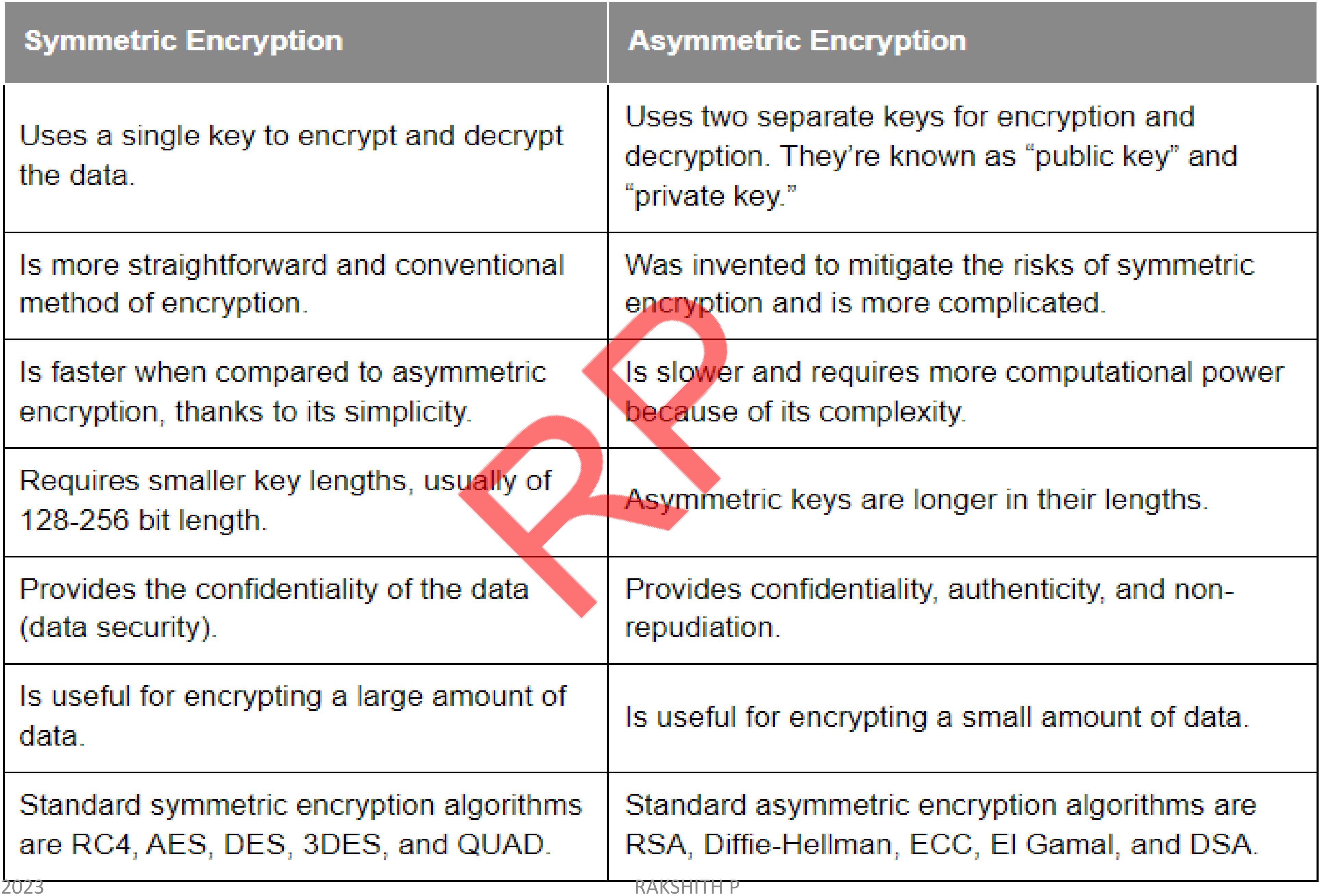
(b) Asymmetric Cryptosystem

### Symmetric Encryption



### Asymmetric Encryption





| Symmetric Encryption | Asymmetric Encryption |
|---|---|
| Uses a single key to encrypt and decrypt the data. | Uses two separate keys for encryption and decryption. They're known as "public key" and "private key." |
| Is more straightforward and conventional method of encryption. | Was invented to mitigate the risks of symmetric encryption and is more complicated. |
| Is faster when compared to asymmetric encryption, thanks to its simplicity. | Is slower and requires more computational power because of its complexity. |
| Requires smaller key lengths, usually of 128-256 bit length. | Asymmetric keys are longer in their lengths. |
| Provides the confidentiality of the data (data security). | Provides confidentiality, authenticity, and non-repudiation. |
| Is useful for encrypting a large amount of data. | Is useful for encrypting a small amount of data. |
| Standard symmetric encryption algorithms are RC4, AES, DES, 3DES, and QUAD. | Standard asymmetric encryption algorithms are RSA, Diffie-Hellman, ECC, El Gamal, and DSA. |

# CRYPTANALYSIS

- Cryptanalysis is the study of cipher text, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.

- Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.