Principles of Security

Introduction

The following room is going to outline some of the fundamental principles of information security. The frameworks used to protect data and systems to the elements of what exactly makes data secure.

The measures, frameworks and protocols discussed throughout this room all play a small part in "Defence in Depth."

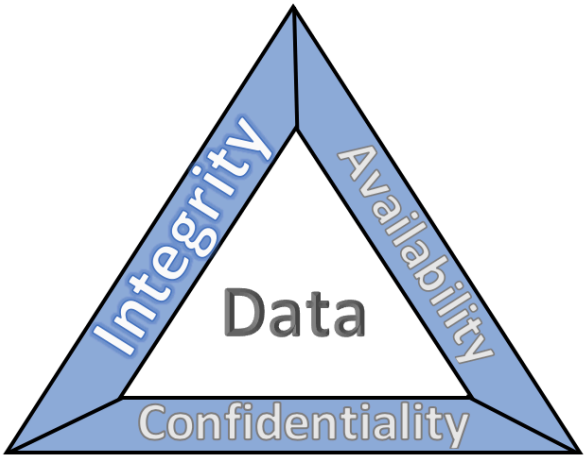
Defence in Depth is the use of multiple varied layers of security to an organization's systems and data in the hopes that multiple layers will provide redundancy in an organization's security perimeter.

The CIA Triad

The CIA triad is an information security model that is used in consideration throughout creating a security policy. This model has an extensive background, ranging from being used in 1998.

This history is because the security of information (information security) does not start and/or end with cybersecurity, but instead, applies to scenarios like filing, record storage, etc.

Consisting of three sections: Confidentiality, Integrity and Availability (CIA), this model has quickly become an industry standard today. This model should help determine the value of data that it applies to, and in turn, the attention it needs from the business.



The CIA triad is unlike a traditional model where you have individual sections; instead, it is a continuous cycle. Whilst the three elements to the CIA triad can arguably overlap, if even just one element is not met, then the other two are rendered useless (similar to the fire triangle). If a security policy does not answer these three sections, it is seldom an effective security policy.

Whilst the three elements to the CIA triad are arguably self-explanatory, let's explore these and contextualise them into cybersecurity.

Confidentiality
This element is the protection of data from unauthorized access and misuse. organizations will always have some form of sensitive data stored on their systems. To provide confidentiality is to protect this data from parties that it is not intended for.

There are many real-world examples for this, for example, employee records and accounting documents will be considered sensitive. Confidentiality will be provided in the sense that only HR administrators will access employee records, where vetting and tight access controls are in place. Accounting records are less valuable (and therefore less sensitive), so not as stringent access controls would be in place for these documents. Or, for example, governments using a sensitivity classification rating system (top-secret, classified, unclassified)

Integrity
The CIA triad element of integrity is the condition where information is kept accurate and consistent unless authorized changes are made. It is possible for the information to change because of careless access and use, errors in the information system, or unauthorized access and use. In the CIA triad, integrity is maintained when the information remains unchanged during storage, transmission, and usage not involving modification to the information. Steps must be taken to ensure data cannot be altered by unauthorised people (for example, in a breach of confidentiality).

Many defences to ensure integrity can be put in place. Access control and rigorous authentication can help prevent authorized users from making unauthorized changes. Hash verifications and digital signatures can help ensure that transactions are authentic and that files have not been modified or corrupted.

Availability
In order for data to be useful, it must be available and accessible by the user.

The main concern in the CIA triad is that the information should be available when authorised users need to access it.

Availability is very often a key benchmark for an organization. For example, having 99.99% uptime on their websites or systems (this is laid out in Service Level Agreements). When a system is unavailable, it often results in damage to an organization's reputation and loss of finances. Availability is achieved through a combination of many elements, including:

- Having reliable and well-tested hardware for their information technology servers (i.e. reputable servers)
- Having redundant technology and services in the case of failure of the primary
- Implementing well-versed security protocols to protect technology and services from attack

****

Answer the questions below:

What element of the CIA triad ensures that data cannot be altered by unauthorized people?
Answer: Integrity

What element of the CIA triad ensures that data is available?
Answer: Availability

What element of the CIA triad ensures that data is only accessed by authorized people?
Answer: Confidentiality

****

Principles of Privileges

It is vital to administrate and correctly define the various levels of access to an information technology system individuals require.

The levels of access given to individuals are determined on two primary factors:

- The individual's role/function within the organization
- The sensitivity of the information being stored on the system

Two key concepts are used to assign and manage the access rights of individuals: Privileged Identity Management (PIM) and Privileged Access Management (or PAM for short).

Initially, these two concepts can seem to overlap; however, they are different from one another. PIM is used to translate a user's role within an organization into an access role on a system. Whereas PAM is the management of the privileges a system's access role has, amongst other things.

What is essential when discussing privilege and access controls is the principle of least privilege. Simply, users should be given the minimum amount of privileges, and only those that are absolutely necessary for them to perform their duties. Other people should be able to trust what people write to.

As we previously mentioned, PAM incorporates more than assigning access. It also encompasses enforcing security policies such as password management, auditing policies and reducing the attack surface a system faces.

****

Answer the questions below:

What does the acronym "PIM" stand for?
Answer: Privileged identity management

What does the acronym "PAM" stand for?
Answer: Privileged Access Management

If you wanted to manage the privileges a system access role had, what methodology would you use?
Answer: PAM

If you wanted to create a system role that is based on a user's role/responsibilities with an organization, what methodology is this?
Answer: PIM

****

Security Models Continued

Before discussing security models further, let's recall the three elements of the CIA triad: Confidentiality, Integrity and Availability. We've previously outlined what these elements are and their importance. However, there is a formal way of achieving this.

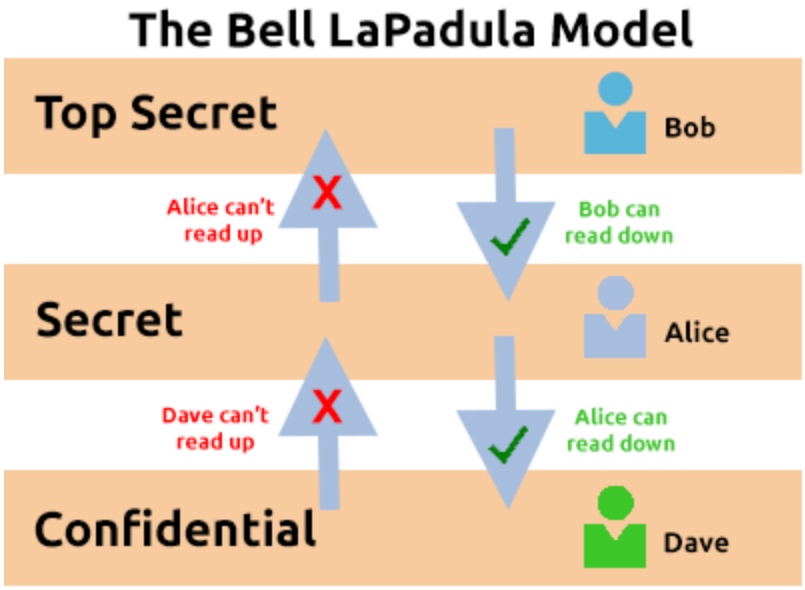
According to a security model, any system or piece of technology storing information is called an information system, which is how we will reference systems and devices in this task.

Let's explore some popular and effective security models used to achieve the three elements of the CIA triad.

The Bell-La Padula Model
The Bell-La Padula Model is used to achieve confidentiality. This model has a few assumptions, such as an organization's hierarchical structure it is used in, where everyone's responsibilities/roles are well-defined.

The model works by granting access to pieces of data (called objects) on a strictly need to know basis. This model uses the rule "no write down, no read up".

Advantages	**Disadvantages**
Policies in this model can be replicated to real-life organizations hierarchies (and vice versa)	Even though a user may not have access to an object, they will know about its existence -- so it's not confidential in that aspect.
Simple to implement and understand, and has been proven to be successful.	The model relies on a large amount of trust within the organization.



The Bell LaPadula Model is popular within organizations such as governmental and military. This is because members of the organizations are presumed to have already gone through a process called vetting. Vetting is a screening process where applicant's backgrounds are examined to establish the risk they pose to the organization. Therefore, applicants who are successfully vetted are assumed to be trustworthy - which is where this model fits in.

Biba Model

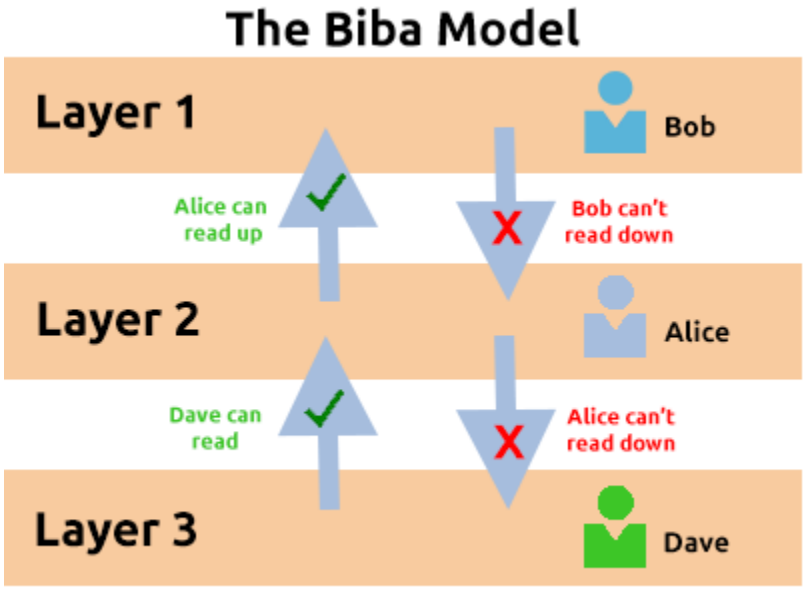
The Biba model is arguably the equivalent of the Bell-La Padula model but for the integrity of the CIA triad.

This model applies the rule to objects (data) and subjects (users) that can be summarized as "no write up, no read down". This rule means that subjects can create or write content to objects at or below their level but can only read the contents of objects above the subject's level.

Let's compare some advantages and disadvantages of this model in the table below:

Advantages	**Disadvantages**
This model is simple to implement.	There will be many levels of access and objects. Things can be easily overlooked when applying security controls.
Resolves the limitations of the Bell-La Padula model by addressing both	Often results in delays within a business. For example, a doctor would not be able

confidentiality and data integrity.	to read the notes made by a nurse in a hospital with this model.



The Biba model is used in organizations or situations where integrity is more important than confidentiality. For example, in software development, developers may only have access to the code that is necessary for their job. They may not need access to critical pieces of information such as databases, etc.

****

Answer the questions below:

What is the name of the model that uses the rule "can't read up, can read down"?
Answer: The Bell-LaPadula Model

What is the name of the model that uses the rule "can read up, can't read down"?
Answer: The Biba Model

If you were a military, what security model would you use?
Answer: The Bell-LaPadula Model

If you were a software developer, what security model would the company perhaps use?
Answer: The Biba Model

****

Threat Modelling and Incident Response

Threat modelling is the process of reviewing, improving, and testing the security protocols in place in an organization's information technology infrastructure and services.

A critical stage of the threat modelling process is identifying likely threats that an application or system may face, the vulnerabilities a system or application may be vulnerable to

The threat modelling process is very similar to a risk assessment made in workplaces for employees and customers. The principles all return to:

- Preparation
- Identification
- Mitigations
- Review

It is, however, a complex process that needs constant review and discussion with a dedicated team. An effective threat model includes:

- Threat intelligence
- Asset identification
- Mitigation capabilities
- Risk assessment

To help with this, there are frameworks such as STRIDE (Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of Service and Elevation of privileges) and PASTA (Process for Attack Simulation and Threat Analysis) infosec never tasted so good!. Let's detail STRIDE below. STRIDE, authored by two Microsoft security researchers in 1999 is still very relevant today. STRIDE includes six main principles, which I have detailed in the table below:

Principle	**Description**
Spoofing	This principle requires you to authenticate requests and users accessing a system. Spoofing involves a malicious party falsely identifying itself as another. Access keys (such as API keys) or signatures via encryption helps remediate this threat.
Tampering	By providing anti-tampering measures to a system or

	application, you help provide integrity to the data. Data that is accessed must be kept integral and accurate. For example, shops use seals on food products.
Repudiation	This principle dictates the use of services such as logging of activity for a system or application to track.
Information Disclosure	Applications or services that handle information of multiple users need to be appropriately configured to only show information relevant to the owner.
Denial of Service	Applications and services use up system resources, these two things should have measures in place so that abuse of the application/service won't result in bringing the whole system down.
Elevation of Privilege	This is the worst-case scenario for an application or service. It means that a user was able to escalate their authorization to that of a higher level i.e. an administrator. This scenario often leads to further exploitation or information disclosure.

A breach of security is known as an incident. And despite all rigorous threat models and secure system designs, incidents do happen. Actions taken to resolve and remediate the threat are known as Incident Response (IR) and are a whole career path in cybersecurity.

Incidents are classified using a rating of urgency and impact. Urgency will be determined by the type of attack faced, where the impact will be determined by the affected system and what impact that has on business operations.

Urgency \ Impact	High	Medium	Low
High	1	2	3
Medium	2	3	4
Low	3	4	5

An incident is responded to by a Computer Security Incident Response Team (CSIRT) which is a prearranged group of employees with technical knowledge about the systems and/or current incident. To successfully solve an incident, these steps are often referred to as the six phases of Incident Response that takes place, listed in the table below:

Action	**Description**

Preparation	Do we have the resources and plans in place to deal with the security incident?
Identification	Has the threat and the threat actor been correctly identified in order for us to respond to?
Containment	Can the threat/security incident be contained to prevent other systems or users from being impacted?
Eradication	Remove the active threat.
Recovery	Perform a full review of the impacted systems to return to business as usual operations.
Lessons Learned	What can be learnt from the incident? I.e. if it was due to a phishing email, employees should be trained better to detect phishing emails.

****

Answer the questions below:

What model outlines "Spoofing"?
Answer: STRIDE

What does the acronym "IR" stand for?
Answer: Incident Response

You are tasked with adding some measures to an application to improve the integrity of data, what STRIDE principle is this?
Answer: Tampering

An attacker has penetrated your organization's security and stolen data. It is your task to return the organization to business as usual. What incident response stage is this?
Answer: Recovery

****