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 organisation'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 organisations 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 organisation. |

Diagrama

El contenido generado por IA puede ser incorrecto.

The Bell LaPadula Model is popular within organisations such as governmental and military. This is because members of the organisations 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 organisation. 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 summarised 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 confidentiality and data integrity. | Often results in delays within a business. For example, a doctor would not be able to read the notes made by a nurse in a hospital with this model. |

Diagrama

El contenido generado por IA puede ser incorrecto.

The Biba model is used in organisations 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"?

Principio del formulario

Correct AnswerHint

Final del formulario

What is the name of the model that uses the rule "**can** read up, **can't** read down"?

Principio del formulario

Correct AnswerHint

Final del formulario

If you were a military, what security model would you use?

Principio del formulario

Correct AnswerHint

Final del formulario

If you were a software developer, what security model would the company perhaps use?

Principio del formulario

Threat Modelling & Incident Response

Threat modelling is the process of reviewing, improving, and testing the security protocols in place in an organisation'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.

Diagrama

El contenido generado por IA puede ser incorrecto.

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**(**S**poofing identity,**T**ampering with data,**R**epudiation threats,**I**nformation disclosure, **D**enial of Service and**E**levation of privileges) and **PASTA** (**P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis) 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.

Imagen que contiene Forma

El contenido generado por IA puede ser incorrecto.

An incident is responded to by a **C**omputer**S**ecurity**I**ncident **R**esponse **T**eam (**CSIRT**) which is 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"?

Principio del formulario

Submit

Final del formulario

What does the acronym "IR" stand for?

Principio del formulario

Submit

Final del formulario

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

Principio del formulario

Submit

Final del formulario

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

Principio del formulario

Final del formulario