Identity and Access Management

IAAA Model

Identification, Authentication, Authorisation, and Accountability (IAAA) are four pillars of information security. Each of these elements plays an essential role in ensuring the confidentiality, integrity, and availability of sensitive information and resources.

1. **Identification** is the process of verifying who the user is. It starts with the user claiming a specific identity. The identity can be represented by a unique identifier such as an email address, a username, or an ID number. Any identifier unique in the respective environment is a valid option; hence, many websites would rely on an email address for identification instead of asking the user to create a unique username.
2. **Authentication** is the process of ensuring that the user is who they claim to be. In other words, this step is about confirming the claimed identity. One way to authenticate would be by providing the correct password. Because of potential password weaknesses, many other methods, such as asking users to type the code sent to their email, are gaining popularity.
3. **Authorisation** determines what the user is allowed to access. In other words, they will be authorised to carry out specific operations based on their account privileges. This process is typically done by assigning roles and permissions based on the user's job function or level of clearance. The risk of unauthorised access or data breaches is reduced by restricting access to only the resources necessary for the user to perform their duties.
4. **Accountability** tracks user activity to ensure they are responsible for their actions. After a user is granted access to a system, it is essential to have mechanisms that hold everyone accountable for their actions. This process is achieved by logging all user activity and storing it in a centralised location. In the event of a security incident, this information can be used to identify the source of the problem and take appropriate action.

You are granted access to read and send an email. What is the name of this process?
Answer: Authorisation

Which process would require you to enter your username?
Answer: Identification

Although you have write access, you should only make changes if necessary for the task. Which process is required to enforce this policy?
Answer: Accountability

Identification

Identification is how a user (or process or system) claims a specific identity. Let's consider a couple of examples from our everyday life.

Identification can also be achieved through a number such as:

- National ID number
- Student ID number
- Passport number
- Mobile phone number

Any number unique to the user might be used for identification. Many websites ask for an email address for registration because a user's email is guaranteed to be unique; this spares the user from trying to find a unique username and remembering it.

Without proper authentication, severe damage can be incurred; consider the case of someone claiming a fake identity when taking a loan from the bank. In the IT world, without authentication, anyone could access your email if they knew your email address. Most systems cannot function properly without proper authentication; systems are not limited to computer systems and include banking systems, hotel reservation systems, and flight systems, among many others.

Which of the following cannot be used for identification?

1. Email address
2. Mobile number with international code
3. Year of birth
4. Passport number

Answer: 3 - Year of Birth

**Which of the following cannot be used for identification?

1. Landline phone number
2. Street number
3. Health insurance card number
4. Student ID number

Answer: 2 - Street Number

Authentication

Authentication is the process of verifying the identity of a user or system.

Authentication and identification are core components of any information system and network. It is essential to understand the difference between authentication and identification.

During identification, the user (or system or process) claims a specific (unique) identity in the respective settings. Authentication is proving the identity of the user (or system or process). This process is usually accomplished through one of the following ways:

1. Something you know
2. Something you have
3. Something you are

Two more methods are used, although to a lesser degree:

- Somewhere you are (logical/physical location)
- Something you do (behaviour)

Something You Know

Something you know refers to something that you know or have memorised. These might include:

- Passwords
- Passphrases
- PIN

Most mobile phones are automatically locked within minutes of inactivity. Depending on the original configuration, the user can unlock them by providing the correct PIN, password, or pattern. Although drawn, a pattern is no different than a PIN, i.e., something memorised.

Something You Have

Something you have refers to an object, usually physical, that you have. It can range from a phone to a security key.

Something You Are

Something you are refers to biometric readers. Examples include fingerprint readers, facial recognition, retina scanners, and voice recognition.

You have most likely experienced authenticating using a fingerprint reader when trying to unlock your phone. Many modern mobile phones allow the user to authenticate using a fingerprint while keeping the password/PIN/pattern as a backup option in case fingerprint authentication fails.

Facial recognition is also becoming popular in modern smartphones. Over the years, biometric readers and scanners are becoming not only more reliable but also more affordable. This technology benefits both companies that require high security and consumers.

Multi-Factor Authentication

Multi-factor authentication (MFA) refers to using two or more of the above mechanisms (something you know/have/are). The purpose is to have additional security in case one authentication mechanism gets compromised.

2FA requires two authentication mechanisms, and it falls under the more general MFA, which requires two or more authentication factors. This requirement can significantly improve security and protect against various attacks, such as those that take advantage of weak passwords.

Answer the following questions using the correct item number from the numbered list below.

1. Something you know
2. Something you have
3. Something you are
4. 2FA

When you want to check your email, you enter your username and password. What kind of authentication is your email provider using?

Answer: 1 - Something you know

Your bank lets you finish most of your banking operations using its app. You can log in to your banking app by providing a username and a password and then entering the code received via SMS. What kind of authentication is the banking app using?

Answer: 4 - 2FA

Your new landline phone system at home allows callers to leave you a message when the call is not picked up. You can call your home number and enter a secret number to listen to recorded messages. What kind of authentication is being used here?

Answer: 1 - Something you know

You have just started working at an advanced research centre. You learned that you need to swipe your card and enter a four-digit PIN whenever you want to use the elevator. Under which group does this authentication fall?

Answer: 4 - 2FA

Authorisation and Access Control

Once authenticated, a user should be granted the proper level of access. Authorisation specifies what the authenticated user should be allowed to access and do. Access control mechanisms would ensure that the proper authorisation is enforced.

Authorisation decides what a user should be able to access, while access control enforces the set policy.

In the following questions, answer with 1 or 2 to indicate:

1. Authorisation
2. Access Control

The new policy states that the secretary should be able to send an email on the manager's behalf. What is this policy dictating?

Answer: 1 - Authorisation

You shared a document with your colleague and gave them view permissions so they could read without making changes. What would ensure that your file won't be

modified?

Answer: 2 - Access Control

The hotel management decided that the cleaning staff needed access to all the hotel rooms to do their work. What phase is this decision part of?

Answer: 1 - Authorisation

Accountability and Logging

Accountability ensures that users are accountable for the actions they perform on a system. In other words, after authenticating their identity and getting authorised to access a system, they can be held responsible for their actions. Accountability is possible if we have **auditing** capabilities, which usually require proper **logging** functionality.

Logging

A critical aspect of accountability is logging. Logging is the process of recording events that occur within a system. This process includes user actions, system events, and errors. By logging user actions, an organisation can maintain a record of who accessed what information and when. This record is vital for regulatory compliance, incident response, and forensic investigations.

With a comprehensive logging system in place, an organisation can trace the actions of any user, identify any anomalies or unauthorised access, and take appropriate action. For example, if an unauthorised user attempts to access sensitive data, the logging system can generate an alert to notify security personnel.

Logging can also help organisations detect and respond to security incidents. By analysing log data, security teams can identify patterns of suspicious activity, such as repeated failed login attempts or unusual access patterns. This information can then be used to investigate and respond to potential security threats.

Because accountability is a crucial component of any secure infrastructure, proper care should be taken to ensure that logging is performed properly and securely. Furthermore, depending on the security requirements, logs should be tamper-proof. The reason is that you don’t want the attacker to delete or alter the logs and hide their actions on the network. This is why it is a good practice to set up a separate logging server with one task: receive and store the logs securely.

Log forwarding is the process of sending log data from one system to another. This process often aggregates log data from multiple sources into a central location for more accessible analysis and management. Log forwarding can also be used to send log data to a cloud-based service for storage and analysis.

There are several benefits to log forwarding. By centralising log data, organisations can more easily analyse and correlate log events from different systems to identify potential security threats.

Logging and SIEM

Security Information and Event Management (SIEM) is a technology that aggregates log data from multiple sources and analyses it for signs of security threats. SIEM solutions can help organisations identify anomalies, detect potential security incidents, and provide alerts to security teams.

Furthermore, the integration of logging and SIEM provides additional benefits such as compliance reporting and forensic investigations.

Identity Management

Identity Management (IdM) includes all the necessary policies and technologies for identification, authentication, and authorisation. IdM aims to ensure that authorised people have access to the assets and resources needed for their work while unauthorised people are denied access. IdM requires that each user or device is assigned a digital identity.

Identity Management (Idm)

IdM is an essential component of cybersecurity that refers to the process of managing and controlling digital identities. It involves the management of user identities, their authentication, authorisation, and access control. The main goal of IdM is to ensure that only authorised individuals have access to specific resources and information. IdM systems are used to manage user identities across an organisation’s network.

IdM systems use a centralised database to store user identities and access rights. They also provide functionalities to manage and monitor user access to resources. IdM systems generally include features such as user provisioning, authentication, and authorisation. User provisioning refers to the process of creating and managing user accounts, while authentication and authorisation refer to verifying the identity of a user and granting access to specific resources.

IdM systems are critical in organisations where there are multiple systems and applications that require access control. They help to simplify the management of user identities, reducing the risk of unauthorised access to resources. In addition, IdM systems provide a single point of reference for user identity management, which makes it easier for organisations to manage user access rights.

Identity and Access Management (IAM)

IAM is a more comprehensive concept than IdM. It encompasses all the processes and technologies to manage and secure digital identities and access rights. IAM systems include a variety of functions, such as user provisioning, access control, identity governance, and compliance management. IAM systems ensure that only authorised users have access to specific resources and data and that their access is monitored and controlled.

IAM systems use various technologies to manage access, including role-based access control, multi-factor authentication, and single sign-on. IAM systems help organisations comply with regulatory requirements such as HIPAA, GDPR, and PCI DSS.

IdM and IAM are essential components of cybersecurity. They ensure that only authorised individuals have access to specific resources and information. IdM systems manage user identities, while IAM systems encompass broader functions to manage and secure digital identities and access rights.

What does IdM stand for?
Answer: Identity Management

What does IAM stand for?
Answer: Identity and Access Management

Attacks Against Authentication

The purpose is to give an idea about the importance of using existing and tested protocols instead of creating a protocol and using it without rigorous peer testing.

The situation on the network is even more challenging to secure. If the user sends their username and password in cleartext, anyone capturing traffic on the network can learn the username and the password. How can we prevent them from learning the login credentials?

The server and the user can agree on a fixed secret key. Instead of sending the password in cleartext, the user encrypts it using the selected secret key. Whenever users want to log in, they send their username and password encrypted using their assigned secret key. Now the attacker should never be able to learn the password, right? Unfortunately, although they won't be able to know the password, they can still authenticate.

Although the attacker does not know the password, they can still authenticate by replaying the same response. This attack is considered a **replay attack** (An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access). Is there anything we can do to fix this?

An encrypted password that is always the same value is easy to circumvent. We need some mechanism to ensure that the response won't be reused repeatedly. One approach would be to use the current time and date as part of the response. In other words, the user would send an encryption of the current time (and date) along with the password. Although this requires both parties to synchronise their clocks, it ensures that the response is only valid for a brief time, usually in milliseconds.

The attacker could authenticate using the user's response when the authentication protocol required a password encrypted with a shared key. What is the name of the attack?
Answer: Replay Attack

Access Control Models

A system controls access to various resources based on the chosen model. Some of the common access control models are:

1. Discretionary Access Control (DAC)
2. Role-Based Access Control (RBAC)
3. Mandatory Access Control (MAC)

Discretionary Access Control

Many have already used Discretionary Access Control (DAC) when sharing files or folders with friends and colleagues. When using DAC, the resource owner will explicitly add users with the proper permissions.

Role-Based Access Control

Role-Based Access Control (RBAC) uses a very intuitive approach. Each user has one or more roles or functional positions; furthermore, they are authorised to access different resources based on their roles.

Mandatory Access Control

An operating system using Mandatory Access Control (MAC) would prioritise security and significantly limit users' abilities. Such systems are used for specific purposes or to handle highly classified data. Consequently, users do not need to carry out tasks beyond the strictly necessary. In other words, users won't be able to install new software or change file permissions.

Answer the following questions using the correct item number from the numbered list below.

1. DAC
2. RBAC
3. MAC

You are sharing a document via a network share and giving edit permission only to the accounting department. What example of access control is this?
Answer: 2 - RBAC

You published a post on a social media platform and made it only visible to three out of your two hundred friends. What kind of access control did you use?
Answer: 1 - DAC

Single Sign-On

Users need to access various sources to carry out their daily work routines. For instance, they would need to access their email, shared files, and printers, among others. Accessing these resources requires the user to have login credentials for successful authentication. The number of different usernames and passwords makes it quite challenging, especially if the users are rightfully not reusing the same password across multiple systems.

Single Sign-On (SSO) tackles this problem. Instead of a user having to remember multiple usernames and passwords, they only need to remember a single set of login credentials. They can authenticate themselves to one system, granting them access to the other systems necessary for their work.

SSO allows organisations to authenticate users once before granting them access to the resources required for their work. We can achieve many advantages from this. We will mention a few.

- One strong password: Expecting a user to remember a single strong password is more acceptable than asking them to remember ten different strong passwords.
- Easier MFA: Adding MFA to every different service is a humongous task to accomplish and maintain. With SSO, MFA needs to be enabled and configured once.
- Simpler Support: Support requests like password reset become more straightforward as they are now confined to a single account.
- Efficiency: A user does not need to log in every time they need to access a new service.

What does SSO stand for?
Answer: Single Sign-On

Does SSO simplify MFA use as it needs to be set up once? (Yea/Nay)
Answer: Yea

Is it true that SSO can be cumbersome as it requires the user to remember and input different passwords for the various services? (Yea/Nay)
Answer: Nay

Does SSO allow users to access various services after signing in once? (Yea/Nay)
Answer: Yea

Does the user need to create and remember a single password when using SSO? (Yea/Nay)
Answer: Yea

Scenarios

It is worth repeating that we need to have proper processes in place to help protect the security of the data, systems, and networks. Expressing this in technical terms, protecting the security of a system, for example, means protecting the confidentiality, integrity, and availability of that system. And part of the proper processes required includes appropriate identification, authentication, authorisation, access control, accountability, and logging, among others. Inadequacy in any one process results in the weakening of the security of the respective systems. Securing one process won’t replace securing the other processes.

Click on View Site **and follow the exercise to get a flag.**

After answering all 10 questions correctly in 45 seconds we receive the flag