Identity & Access Management

IAAA Model

Overview

The IAAA model consists of four essential pillars—Identification, Authentication, Authorization, and Accountability—that work together to protect sensitive information and resources in an organization. Identification establishes who a user claims to be through unique identifiers like usernames or email addresses, while Authentication verifies that claim through methods such as passwords or verification codes. Authorization then determines what resources and operations the authenticated user is permitted to access based on their role and privileges. Together, these three elements form a security foundation that is reinforced by Accountability, which logs and tracks all user activity for incident investigation and responsibility enforcement.

Key Information

- Identification: User claims an identity using unique identifiers (email, username, ID number) to establish who they are in the system
- Authentication: Verification process confirming the user's claimed identity through credentials (passwords, codes, multi-factor methods) to ensure they are who they claim to be
- Authorization: Access control mechanism that grants or restricts user permissions based on assigned roles and job functions, limiting access to only necessary resources
- Accountability: Logging and monitoring system that tracks all user activities in a centralized location, enabling incident investigation and ensuring users are responsible for their actions
- Security Benefit: IAAA implementation prevents unauthorized access, reduces data breach risk, and enables organizations to respond effectively to security incidents through audit trails

---

Task

1. You are granted access to read and send an email. What is the name of this process?
    1. **Authorisation**
2. Which process would require you to enter your username?
    1. **Identification**
3. Although you have write access, you should only make changes if necessary for the task. Which process is required to enforce this policy?
    1. **Accountability**

Conclusion

The IAAA model provides a comprehensive security framework that addresses both access control and audit requirements essential for modern cybersecurity. By systematically implementing identification, authentication, authorization, and accountability mechanisms, organizations can significantly reduce vulnerability to internal and external security threats. Understanding each component's distinct role is fundamental for 4th-year cybersecurity students designing secure systems and developing security policies.

Resources

- **TryHackMe**: Intro to Cryptography

Identity

Overview

Identification is the process by which a user, process, or system claims a specific identity through a unique identifier, without any verification of that claim's truthfulness. Identifiers can take various forms including usernames (such as tanderson, neo, or thomas01), email addresses, national ID numbers, student IDs, passport numbers, or phone numbers—any attribute that is reasonably unique within a given context. The key distinction is that identification is purely a claim of identity, similar to someone at a party stating their name; the system accepts this claim at face value without confirming its authenticity. This process sets the foundation for subsequent security measures like authentication, which verify whether the claimed identity is legitimate.

Key Information

- Claim-Based Process: Identification involves a user stating who they are through a unique identifier without requiring proof or verification of that claim
- Identifier Types: Common identifiers include usernames, email addresses, national ID numbers, student IDs, passport numbers, and mobile phone numbers
- Organizational Variation: Different organizations and platforms use different identifier formats (e.g., tanderson, thomasa, ta001, or neo could all represent the same person)
- Email as Identifier: Many websites use email addresses for identification because they are globally unique and eliminate the burden of users creating and remembering usernames
- Foundation for Security: Identification alone is insufficient for system security; it must be followed by authentication to prevent unauthorized access and fraud (such as someone falsely claiming to be a gym member or loan applicant)

Task

1. Which of the following cannot be used for identification? `Email address` `Mobile number with international code` `Year of birth` `Passport number`
    1. **Year of Birth**
2. Which of the following cannot be used for identification? `Landline phone number` `Street number` `Health insurance card number` `Student ID number`
    1. **Street Number**

Conclusion

Identification serves as the initial step in the IAAA model, establishing a claimed identity within a system, but provides no security guarantee on its own. Without subsequent authentication mechanisms, systems become vulnerable to impersonation and fraud, making proper identification combined with strong authentication critical for protecting sensitive resources and maintaining system integrity. Understanding this distinction is essential for designing secure systems that prevent unauthorized access and protect legitimate users.

Resources

- **TryHackMe**: Intro to Cryptography

Authentication

Overview

Authentication is the process of verifying a user's or system's claimed identity, distinct from identification which is simply claiming that identity. The primary mechanisms for authentication include something you know (passwords, PINs), something you have (security keys, phones), and something you are (biometrics). Multi-factor authentication (MFA) combines two or more of these mechanisms to significantly enhance security against compromised single factors.

Key Information

- Something You Know – Includes passwords, passphrases, and PINs that users memorize; examples include complex strings like "4SNoPawKkdFiCdnm" and numeric codes like "25063"
- Something You Have – Physical objects such as hardware security keys (Yubico, Titan Security Key), SIM cards, or mobile phones used to receive verification codes via SMS or NFC
- Something You Are – Biometric authentication methods including fingerprint readers, facial recognition, retina scanners, and voice recognition that are becoming increasingly affordable and reliable
- Multi-Factor Authentication (MFA) – Combines two or more authentication mechanisms to provide layered security; classic example is an ATM requiring both a debit card (something you have) and a PIN (something you know)
- Real-World Applications – Authentication is essential in everyday scenarios like gym membership verification, mobile phone unlocking, banking systems, and instant messaging app registration

---

Notes

Task

1. .

Conclusion

Understanding the three primary authentication mechanisms and their combinations through MFA is critical for designing secure systems. Organizations and individuals should implement MFA where possible, as it substantially reduces the risk of unauthorized access even if one authentication factor is compromised. The evolving affordability and reliability of biometric technologies make MFA increasingly practical for widespread deployment across both enterprise and consumer applications.

Resources

- **TryHackMe**: Intro to Cryptography