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

Revision #1
Created 2025-11-29 01:39:47 UTC by David Rizzo
Updated 2025-11-29 01:45:06 UTC by David Rizzo