ThoughtWorks®

SPOOFED IDENTITY

How hard is it for an attacker to pretend to be someone with authority to use the system?

Can someone spoof an identity and then abuse its authority? Spoofing identity allows attackers to do things they are not supposed to do.

An example of identity spoofing is an attacker illegally accessing and then using another user's authentication information, such as username and password.

KEY CONCEPTS:

- Identity
- Authentication

Examples of Weak Authentication

- Lack of any form of authentication
- Dependency on browser-based implementation
- Failure of user interface to obscure entry of credentials
- Failure to prevent users creating weak credentials
- Failure to prevent caching of credentials on a shared computer
- Authentication mechanism subject to brute force attack
- Can authenticate with credentials harvested from other breaches
- Failure to allow use of password manager and strong credentials
- Reliance on a single factor for authentication
- Weakness in process to reset credentials
- Guessable values such as IMEI number used in authentication

Examples of Weak Processes

- Lack of identity or entitlement checks in setting up a new account
- Use of shared accounts and credentials
- Weakness in offline process to reset credentials
- Failure to revoke access when someone leaves

Other Examples

- Authentication, authorisation or session management has been coded from scratch
- Failure of session to timeout after a reasonable duration of time
- Failure to configure authorisation, i.e. based roles and least privilege
- Failure to re authenticate session when taking destructive actions, such as delete account

And what else?

ThoughtWorks®

thoughtworks.com