INFORMATION DISCLOSURE

Can someone view information they are not supposed to have access to? Information disclosure threats involve the exposure or interception of information to unauthorised individuals.

An example of information disclosure is when a user can read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

KEY CONCEPTS:

- Confidentiality
- Encryption
- Leakage
- Man in the middle

Poor handling of secrets

- Lack of tooling to prevent pushing configuration secrets to source control
- Secrets are stored in plain text in source control
- Possible for malicious process to read plaintext credentials

Encryption of data in transit

- Cleartext transport of credentials or data over WiFi and/or Internet
- Cleartext transport of credentials or data between components within the system
- TLS Cypher configuration is weak
- Configuration of TLS is vulnerable to a 'downgrade' attack
- Lack of measures to prevent domain spoofing, such as Strict Transport Security

Information leakage

- Sensitive information is present in log files
- Leakage of unnecessary system information which can assist an attacker
- Triggering an exception leaks unnecessary information that can assist attacker
- Lack of access control on resources not intended to be discoverable to user
- Possible for another tenant to read deallocated cloud storage

Other examples

- Sensitive data stored in unencrypted storage
- Possible for malicious process to read sensitive information from logs
- Sensitive data is stored in predictable locations in memory
- Lack of anti-caching headers to prevent caching of sensitive HTTP requests or responses
- Lack of rate limiting allows 'scraping' or 'spidering' of valuable data

And what else?

ThoughtWorks®

thoughtworks.com