THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

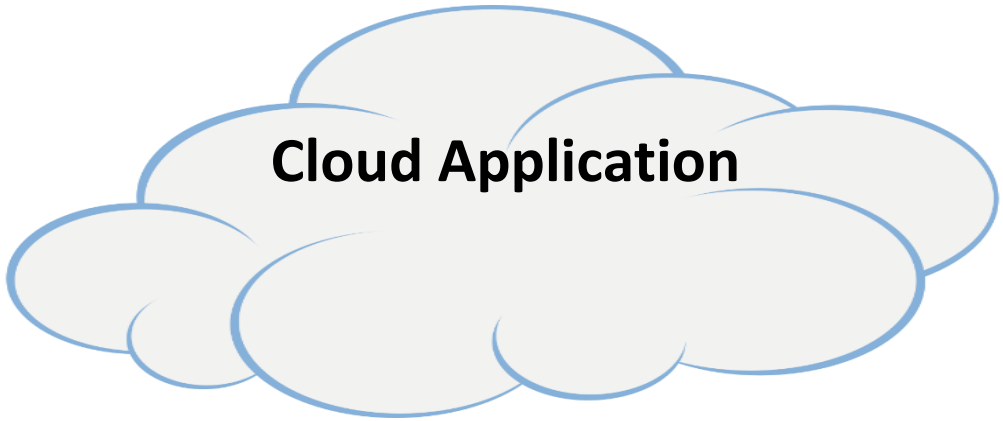
COMPX527 Week 10

Cloud Application Security

Announcements:

- There will be no class on Thursday due to “Kīngitanga Day”.
- Assignment 2 will be published in this week.
- Quiz will open on Thursday.

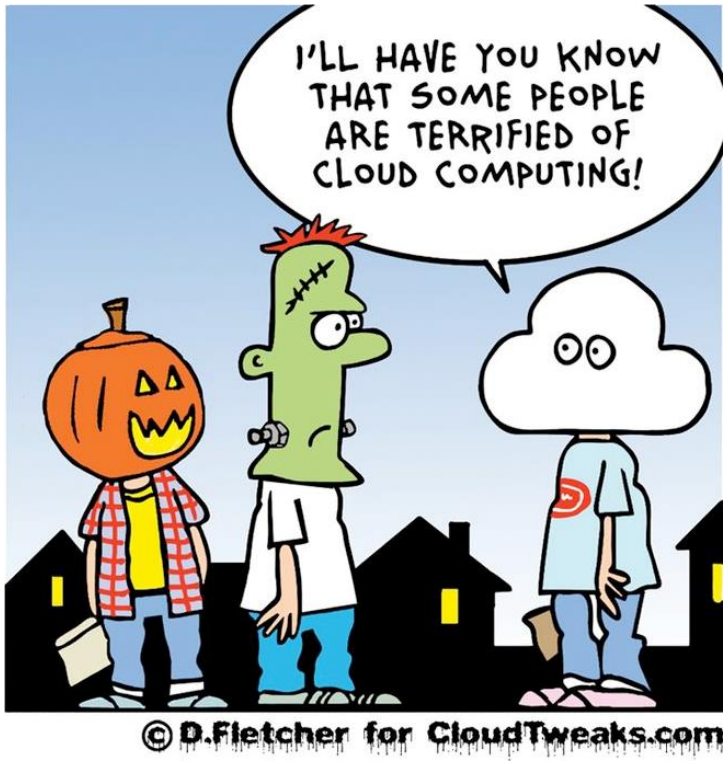
What is a Cloud Application?



- Provides the functionality of a native application
- May have a lightweight client or be completely web based
- May interface with multiple clouds.

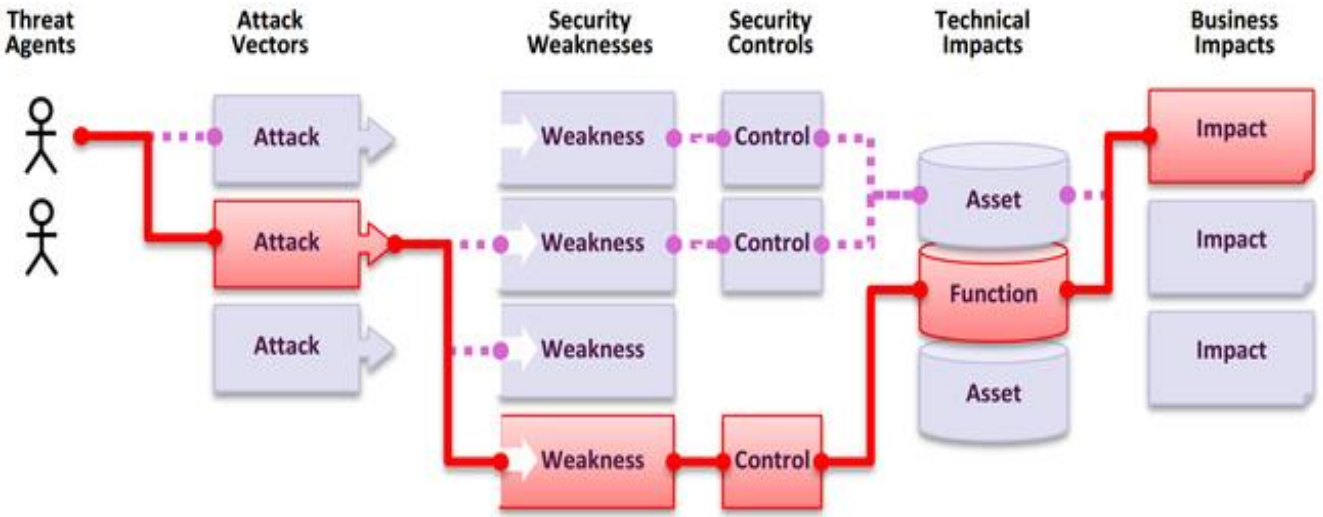
How is securing cloud applications different from securing non-cloud applications?

What might happen to a cloud app?



- Limited visibility
- Attack surfaces are wider/larger → more open to outsider attacks
- Applications (and their data) are not fully managed by the owner
- Different threat model

Web Application Security Risks



Reference: OWASP

Web Application Security Risks

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

OWASP
The Open Web Application Security Project

Reference: OWASP (2021) https://owasp.org/Top10/

Mitigating Security Risks

- Secure coding
  - OWASP has provided secure coding practices.
  - https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/

- Vulnerability Assessment
- Penetration Testing

Vulnerability Assessment

- Vulnerability assessment is a process to identify and prioritize vulnerabilities present in a system.
- Vulnerability scanners are tools that will assess the applications and servers to search for any vulnerabilities and report
- Vulnerability assessment is also one of the initial things that an attacker performs before attacking an application

Continuous Vulnerability Scanning

- Vulnerability Scanners
  - SAST: Static Application Security Testing
    - Detects vulnerabilities in code before compilation
    - SQL injection, cross-site scripting
  - SCA: Software Composition Analysis
    - Analyses code for dependencies.
    - Cross references public knowledge for detecting vulnerabilities
  - DAST: Dynamic Application Security Testing
    - Detects vulnerabilities in running applications by dynamically interacting with them

Penetration Testing

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

- A penetration test (pentest) is performed by someone you've engaged to try to get unauthorized access to your systems and tell you where the vulnerabilities are.
- White box testing
- Black box testing
- Grey box testing

Q&A

THE UNIVERSITY OF WAIKATO
Te Whare Wānanga o Waikato

FaaS and Furious by Forrest Brazeal

A CLOUD GURU