Web Security

Girindro Pringgo Digdo

Whoami

- Seven years in Information Security
- Lecturer
- Author

Agenda

- Server Security
- Client Security

Server Security

- Server system consist of:
  - Client
  - Server

- Facilities
  - GET Method
  - File
  - Command Execution
  - ?

Issues

- The information changed so that it could be lead the bad mark of company or organization
- The information that should be consumed for a limited (i.e. financial statements, the company's strategy, or client database) was successfully intercepted by your rival
- The information can be tapped (such as sending a credit card number to purchase via www)

Issues

- Your server was attacked so it can not provide services when needed (denial of service attack);
- For a web server that is behind a firewall, a security hole in web server which can be exploited to weaken or even eliminate the function of the firewall.

Web Security

- Access Control
  - Everyone not need the access
  - Limit the domain or IP Address for access
  - Use account pair (user and password)
  - Data encryption so that it could be opened by right person
- Protect the page with password
- Use Secure Socket Layer (SSL) for login or transmission the classified information

Web Security

- Knowing the Server

  Information about server could be used by attacker to attack the system. They search weakness about system and then attack.

- Server Side Scripting Security
  - Use secure coding

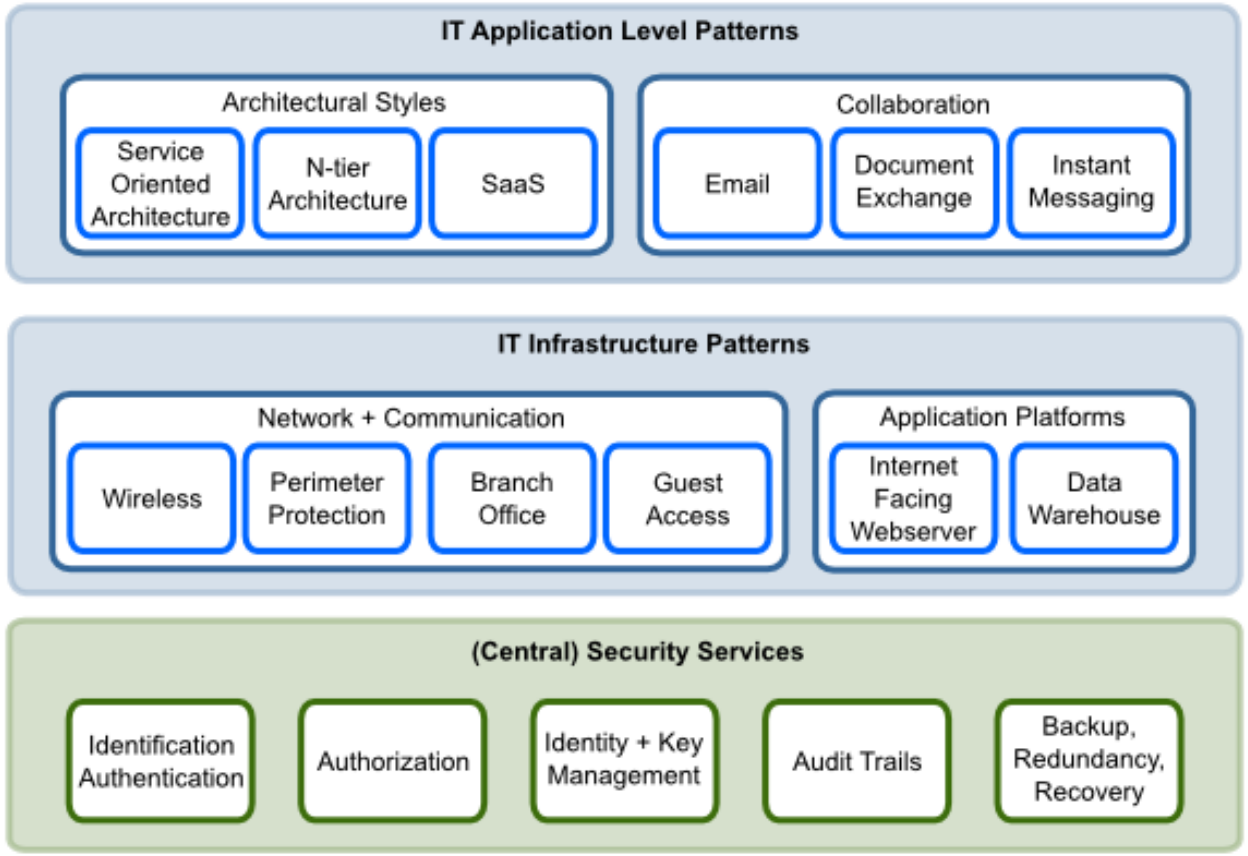
Client Security

- Be careful to click the link. Without awareness, it could be lead you to malicious software
- The page could be execute malicious command.

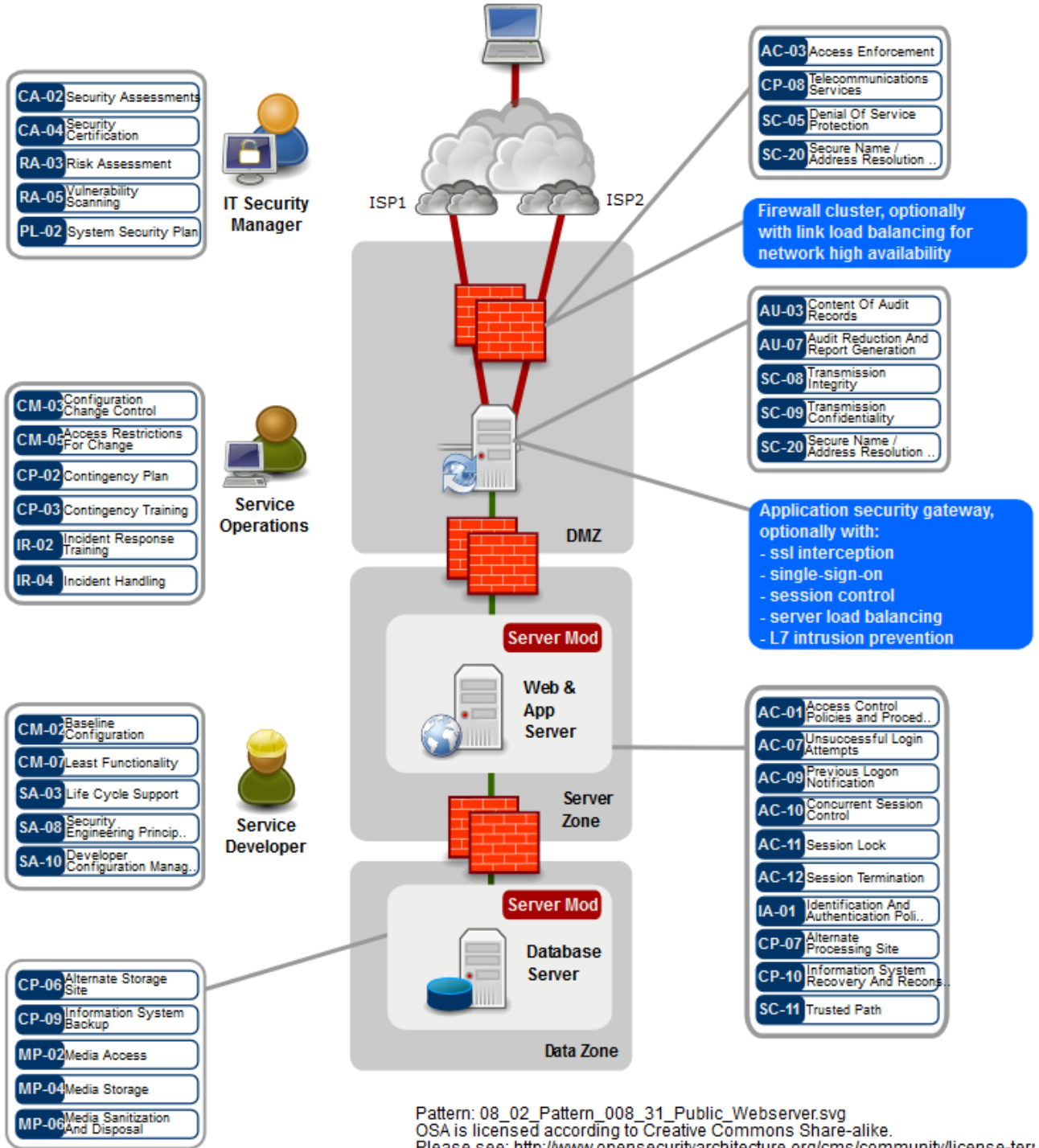
Task

- Make a Security Architecture Pattern
- Explain each component of pattern
- Send to girindigdo@gmail.com
- Due date November 5, 2015; 11.AM

High Level of Security Landscape



Example



Pattern: 08_02_Pattern_008_31_Public_Webserver.svg
OSA is licensed according to Creative Commons Share-alike.
Please see: http://www.opensecurityarchitecture.org/cms/community/license-ter