IT2605
Applications of Web Services

L05 Web Services Security

Web Services Security

- Before applying security to your Web Services, consider whether it is necessary. E.g.:
  - A Unit Conversion Web Service
  - A Parts Ordering Web Service

- Security in Web Services is concerned with securing two things:
  - Access – Who can access the web service
  - Data – The confidentially and integrity of data

Web Services Security

- Specifically, the following must be addressed:
  - **Confidentiality**
    - Make sure the data being transmitted is NOT readable by unauthorised parties while it travels through the Internet.
  - **Integrity**
    - Allow receivers to check that the data they received was not changed along the way by other parties on the Internet.
  - **Authentication**
    - Which system is trying to use the web service?
  - **Authorisation**
    - Is the identified system authorised to use the web service or specific web service operation?
  - **Non-repudiation**
    - Proves that an action occurred in order to prevent the client from fraudulently denying a transaction.

Security Problems and Threats

The Problems/Threats

- Recall
  - Web Services uses HTTP and the internet to transport messages.
- HTTP and the internet are open and **NOT secure**.
- HTTP messages travel through many servers and any of them can:
  - Read the messages (no **Confidentiality**)
  - Change the messages (no **Integrity**)

The Problems/Threats

- Any one can call the Web Services
  - They can grab the URL and Web Service details from the HTTP messages
  - **Authentication** and **Authorisation** is needed to control access
- HTTP and the Internet are Stateless
  - No built in mechanisms to remember transactions
  - Any party can deny making any transaction (no **Non-repudiation**)

Solutions

HTTP Secure

- Combination of **HTTP** and **Secure Socket Layer (SSL)** or **Transport Layer Security (TLS)**
- Provides **encrypted communication** and **secure identification** of a network web server.
- Requires certification by a Trusted Authority
  - E.g. : Verisign
- Often used for secure payment on the Internet.
- Web sites secured with HTTPS: URL starts with **https**

HTTP Secure

- HTTPS messages are encrypted and ensures:
  - Confidentiality
    - No other party can read the messages
  - Integrity
    - No other party can change the messages

SOAP Messages

- Web Services communicate with SOAP messages.
- SOAP messages are NOT encrypted by default.
- The SOAP standard allows it to be extended to include encryption and certification
  - E.g. : WS-Security protocol published by Oasis
- Handles:
  - Confidentiality
  - Integrity
  - Non-repudiation

Authentication

- Like Web Applications, Web Services access can be controlled via authentication (and authorisation)
  - However, methods differ - Web Services are not meant to provide user-friendly UIs: i.e. Web Service provider will not provide a "Login Web Page"
- Authentication is usually required as part of the Web Service Operation. Either:
  - In the Header of the SOAP message (we will learn this in the practical)
  - As input parameters of the Web Service Operation. E.g. :
    - wsBookCatalog.getBooks(userid, password)
    - wsBookCatalog.getBookDetails(userid , password, bookId)
  - The former is preferred as it keeps the Web Service Operations neater.

Authorisation

- Once consumer is authenticated, Web Service Provider can determine which Web Service Operation the consumer can access. E.g.:
  - External customer can only browse the catalogue and place orders
  - Internal staff can edit the catalogue

Summary

- Web Services Security must address:
  - Confidentiality
  - Integrity
  - Authentication
  - Authorisation
  - Non-repudiation
- HTTP communications are NOT secure
- Web Services can be secured by:
  - HTTPS
  - Extending the SOAP standard
  - Requiring authentication and implementing authorisation

PRACTICAL TIME!