SOA & Web Service Security

COMP620

Acknowledgements

Some material in these slides was taken from:

- Slides by Mark Zalar
- Slides by Bhavani Thuraisingham
- Wikipedia

SOA Idea

- Many different services can be provided by different systems
- Access to these services is via web messages
- Client programs affect various services by invoking the service on remote systems

Service Oriented Architectures (SOA)

- A service-oriented architecture is essentially a collection of services.
- These services communicate with each other.
- The communication can involve either simple data passing or it could involve two or more services coordinating some activity.
- Service-oriented architectures are not a new thing. DCOM or Object Request Brokers (ORBs) based on the CORBA has been used for some time.
- A service is a function that is well-defined, self-contained, and does not depend on the context or state of other services

What is SOA?

- Service-Oriented Architecture
  - An architecture that relies on loosely-coupled software agents to perform specified tasks
  - Software agents can be independent of one another
    - Interaction requires no knowledge of a software agent's underlying details

Loose-coupling

- An approach/design goal where interaction between services is developed with minimal assumptions between the services
- A change in one service should not force a change in another service that interacts with it
- Interface is independent of implementation

Service Agents

- A unit of work performed by a service provider for a service consumer
- Service providers and service consumers are both software agents

SOA Web Services

- A software system designed to support interoperable machine to machine interaction over a network (W3C definition)
- A web service is SOA if:
  - Interfaces are based on Internet protocols
  - Messages are XML

architectural principles

- **Service encapsulation** – The service must be performed by a remote server
- **Service loose coupling** – Services maintain a relationship that minimizes dependencies and only requires that they maintain an awareness of each other.
- **Service contract** – Services adhere to a communications agreement, as defined collectively by one or more service-description documents.
- **Service abstraction** – Beyond descriptions in the service contract, services hide logic from the outside world.
- **Service reusability** – Logic is divided into services with the intention of promoting reuse.
- **Service autonomy** – Services have control over the logic they encapsulate.
- **Service discoverability** – Services are designed to be outwardly descriptive so that they can be found and accessed via available discovery mechanisms

XML Messaging

- XML
  - Extensible Markup Language
  - General-purpose
  - Open, free standard
  - Used to share data between systems
  - Human readable
  - Can represent general data structures
    - Trees, lists, etc.
  - Hierarchical structure

XML Messaging

- XML Example

```
<?xml version="1.0" encoding="UTF-8"?>
<recipe name="bread" prep_time="5 mins" cook_time="3 hours">
    <title>Basic bread</title>
    <ingredient amount="3" unit="cups">Flour</ingredient>
    <ingredient amount="0.25" unit="ounce">Yeast</ingredient>
    <ingredient amount="1.5" unit="cups" state="warm">Water</ingredient>
    <ingredient amount="1" unit="teaspoon">Salt</ingredient>
    <instructions>
        <step>Mix all ingredients together, and knead thoroughly.</step>
        <step>Cover with a cloth, and leave for one hour in warm room.</step>
        <step>Knead again, place in a tin, and then bake in the oven.</step>
    </instructions>
</recipe>
```

Example from Wikipedia

SOAP

- Simple Object Access Protocol
- Used to exchange XML messages over a network (using HTTP or other service transport protocol)
- Most common messaging pattern is RPC
  - Client sends request, server immediately responds
- Allows easy interaction between very different systems

SOAP

- All the messages are sent using SOAP. (SOAP at one time stood for Simple Object Access Protocol)
- SOAP essentially provides the envelope for sending the Web Services messages.
- SOAP generally uses HTTP , but other means of connection may be used.
- HTTP is the familiar connection we all use for the Internet.
- It is the pervasiveness of HTTP connections that will help drive the adoption of Web Services.

SOAP Example

- Client request

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
        <getProductDetails xmlns="http://warehouse.example.com/ws">
        <productID>827635</productID>
        </getProductDetails>
    </soap:Body>
</soap:Envelope>
```

Example from Wikipedia

SOAP Example

- Server response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
    <soap:Body>
        <getProductDetailsResponse xmlns="http://warehouse.example.com/ws">
            <getProductDetailsResult>
                <productName>Toptimate 3-Piece Set</productName>
                <productID>827635</productID>
                <description>3-Piece luggage set. Black Polyester.</description>
                <price currency="NIS">96.50</price>
                <inStock>true</inStock>
            </getProductDetailsResult>
        </getProductDetailsResponse>
    </soap:Body>
</soap:Envelope>
```

Example from Wikipedia

Service Description

- WSDL
  - Web Service Definition Language
  - An XML format for describing web services
  - Describes the public interface to a particular web service
    - Data Types <types>
    - Messages <message>
    - Operations <portType>
    - Communication Protocols <binding>
  - Often used with SOAP and XML
    - WSDL tells a client what functions are available
    - The client uses SOAP to actually call functions

Service Description

- WSDL Example

```
<message name="getTermRequest">
    <part name="term" type="xs:string"/>
</message>

<message name="getTermResponse">
    <part name="value" type="xs:string"/>
</message>

<portType name="glossaryTerms">
    <operation name="getTerm">
        <input message="getTermRequest"/>
        <output message="getTermResponse"/>
    </operation>
</portType>
```

Example from W3Schools

UDDI Service Discovery

- Universal Description Discovery and Integration
- XML-based, platform independent, standardized worldwide business registry
- Businesses can publish service listings and describe how services interact over the Internet
- Focuses on the discovery aspect of SOA
- Three types of information can be registered into a UDDI registry
  - White Pages - business identification information (address, name, contact information)
  - Yellow Pages - characterization/description of service
  - Green Pages - technical information about service
- Used with SOAP messages to access WSDL documents describing services in the directory

Service Discovery

REGISTRY TYPE	DESCRIPTION	EXAMPLE APPLICATION
Corporate/Private	An internal registry, behind a firewall, that is isolated from the public network. Access to both administrative features and registry data is restricted. Data is not shared with other registries.	Enterprise Web Service Registry
Affiliated	A registry deployed within a controlled environment, but with limited access by authorized clients. Administrative features may be delegated to trusted parties. Data may be shared with other registries in a controlled manner.	Trading Partner Network
Public	From an end-user's perspective, a public registry appears to be a service in a cloud. Although administrative functions may be secured, access to the registry data itself is essentially open and public. Data may be shared or transferred among other registries, and content may or may not be moderated.	UDDI Business Registry (UBR)

Table from uddi.org

UDDI

- The UDDI registry is intended to eventually serve as a means of "discovering" Web Services described using WSDL .
- The idea is that the UDDI registry can be searched in various ways to obtain contact information and the Web Services available for various organizations.
- UDDI registry is a way to keep up-to-date on the Web Services your organization currently uses

Is SOA Unique?

- Some merge SOA and Web Services together as one feature
- Others claim they are distinctly different
- SOA and Web 2.0 are similar
  - Web 2.0 has been called global SOA

Attack Surface

- Generally you want to minimize the number of points that a hacker can attack
- SOA creates many opportunities for attack