WS-Security

Unit-V

Introduction

- WS-Security is provided by WS-Security framework

- **Identification**
- provide information about its origin or owner (claims)
- Claims are represented as ID info' stored in the SOAP header (token)

- **Authentication**
- proving an identity – service must provide proof that its claimed identity is true

- **Authorization**
- determines to what extent authentication applies to the requestor

Issue in security implementation

- SOA is propagating the authentication and authorization information for a service requestor across multiple services behind the initial service provider

- No state, requires authentication and authorization for each request

Single sign-on

- Services are autonomous – need mechanism to persist the security context, for a requestor

- Otherwise, requestor need to re-authentication for every subsequent request

- Solution – Single sign-on

- Single sign-on – allows service requestor authenticated once - security context information shared with other services it uses – to avoid re-authentication

Contd…

- 3 primary extensions that support single sign-on concept:

- SAML (Security Assertion Markup Language)
- .NET Passport
- XACML (XML Access Control Markup Language)

- SAML
  - point of contact for a service requestor can also act as an issuing authority
  - Service requestor authorize and authenticate with issuing authority
  - Other services, contact issuing authority for authentication and authorization clearance it originally obtained

Contd...

- Confidentiality:
- protects the privacy of the message contents
- Transport level security – Secure socket layer (SSL) – feature for secure HTTP channel
- Message-level security - guarantees end-to-end message protection
- Provided by encryption and digital signatures
- XML-Encryption - applied to an entire message or specific parts of message

Contd...

- XML-Signature - features allows an XML document to be accompanied with algorithm-driven piece of information represents a digital signature

- Content claims to be unaltered only if signature verification on receiving service succeeds

- WS-Security framework in SOA fulfill fundamental QoS of enterprises:
  - utilize service-oriented solutions for the processing of sensitive and private data
  - restrict service access as required