Module 20
SOA Security Lab

Security Concepts

- trust
- claims
- tokens
- identification
- authentication
- authorization
- confidentiality
- integrity
- non-repudiation
- transport-layer
- message-layer security

Security Threats

- buffer overrun
- information leakage
- XML parser
- malicious intermediary
- denial of service
- insufficient authorization

Industry Standards

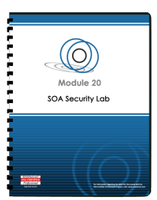
- XML-Encryption
- XML-Signature
- Canonical XML
- Decryption Transform for XML Signature
- Web Services Security
- Security Assertion Markup Language (SAML)
- WS-Trust
- WS-SecureConversation
- WS-Policy
- WS-SecurityPolicy
- WS-PolicyAttachment

Security Mechanisms

- encryption
- hashing
- digital signatures
- identify and access management (IAM)
- public key infrastructure (PKI)
- digital certificates
- certificate authority (CA)
- single sign-on (SSO)
- security token actions
- trust brokering
- security sessions
- security policies

Security Patterns*

- Data Confidentiality (641)
- Data Origin Authentication (649)
- Direct Authentication (656)
- Brokered Authentication (661)
- Exception Shielding (376)
- Message Screening (381)
- Trusted Subsystem (387)
- Service Perimeter Guard (394)



SOA Certified Professional (SOACP) Program
Module 20: SOA Security Lab
Official Mind Map Supplement
www.soaselfstudy.com

* Numbers in parenthesis are page references from “SOA Design Patterns”.

SOASchool.com®
SOA CERTIFIED
Professional

SOASchool.com® SOA Certified Professional (SOACP) Program
www.arcitura.com • www.soaschool.com
Copyright © Arcitura Education Inc.