Security for OWL-S

DAML PI Meeting

Captiva Island, FL

10/03

Presented by Grit Denker

SRI International

Security for OWL-S

1. **Annotation and matchmaking of security aspects of web services**
   - Grit Denker (SRI), Tim Finin (UMBC), Lalana Kagal (UMBC), Massimo Paolucci (CMU), Katia Sycara (CMU)

2. **Design and annotation of security services**
   - Grit Denker, Andrew Ton, Son Nguyen (SRI)

Annotation and Matchmaking

Ontologies

- **Simple Credential**
  - Certificate/X509Certificate/XMLX509Certificate, Login, Cookie, Key/Pkey/SKey, BioMetric, etc.
- **Composed Credentials**
  - IDCard/DriversLicense, SmartCard, etc.
- **SecurityMechanism – classes and properties**
  - Syntax: ASCII, OWL, etc.
  - KeyFormat: X509, RSA, etc.
  - Protocol (incl. KeyProtocol/KeyDistributionProtocol, DataTransferProtocol, etc): X-KISS, X-KRSS, etc.
  - SecurityNotation: Authentication, Confidentiality, etc.
  - Signature/Encryption: S/MIME, XML-DSIG, Open-PGP, etc.
  - ObjectProperties (relSecurityNotation, reqCredential, syntax, etc.) with appropriate range classes
- see www.csl.sri.com/~denker/owl-sec/

Annotation and Matchmaking II

Definition of "security classes/characteristics"

- **Approach**
  - **Basis: security ontologies**
  - **Definition of restriction classes - restricting range/value of properties**
- **Examples:**
  - **AuthorizationSubClass**
    - Restriction on property "relSecurityNotation" to "Authorization"
  - **X509SubClass**
    - Restriction on property "reqCredential" to "X509Certificate"
  - **SSH**
    - Intersection of "KeyProtocol"and "AuthorizationSubClass"
  - **XKMS**
    - Intersection of "KeyProtocol", "AuthenticationSubClass", and "X509SubClass"

Annotation and Matchmaking III

- **Security extensions for web service profile**
  - SecurityMechanism
    - subClassOf profile:Parameter
  - ObjectProperties: securityCapability/securityRequirement
    - subPropertyOf profile:parameter
    - range: SecurityMechanism
  - Used to describe *requirements* and *capabilities* of the web service (such as which protocol is used, which credentials can be offered, etc.)
  - Similar for "Agent"
- **Matchmaking of web service and agent security**
  - Prototypical Implementation uses JTP
  - Integrated with CMU Matchmaker

Security Services

- Definition, annotation, and deployment of security services
  - Idea: Compose security services with other services
  - Examples:
    - Encryption/Decryption of file/text
    - SOAP message signature/encryption
    - XML Signer/Verifier (entire file, element, content of one element)
    - X509Certificate generation
- OWL-S annotation
  - profile/process/grounding/wsdl
  - see www.csl.sri.com/~denker/owl-sec/SecurityServices
  - annotation could be used as reference spec

Security Services II

- **Implementation/deployment**
  - **IBM WSTK3.1 and Apache Tomcat 4.1**
  - **Sun Jdk-1.3 (incl. open-source packages for enc/dec)**
- **see Demo (not yet online, but soon)**