

Trusted Agent-Mediated E-Services via Semantic Web Rules Inference

Yuh-Jong Hu

May-25, 2002

jong@cherry.cs.nccu.edu.tw
http://www.cs.nccu.edu.tw/ENT
Emerging Network Technology(ENT) Lab.
Department of Computer Science
National Chengchi University Taipei, Taiwan

Talk Outline

- ✓ Research Background
- ✓ The Semantic Web
- ✓ The Semantic Web Rules
- ✓ Agent-Mediated E-Services
- ✓ Trusted Agent-Mediated E-Services
- ✓ Research Challenges
- ✓ Summary

Research Background

Research Background

- ➡ Achieving the semantic web vision will be one of the emerging research areas for the academic community in the near future.
- ➡ We believe that software agents will be the prime beneficiary for the success of semantic web research.
- ➡ We focus on the agent trust issue for the semantic web research based on ontology (taxonomies + axioms (rules)) and security technologies.
- ➡ Agent-mediated e-services (or e-commerce) is one of the application domains to demonstrate the feasibility of our trust verification methodology.

The Semantic Web

The Semantic Web


- ➡ A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities.
- ➡ The Semantic Web will enable machines to **comprehend** semantic documents and data, not human speech and writings.
- ➡ The explicit representation of the semantics of data, accompanied with domain theories (that is, **ontologies**), will enable a Web that provides a qualitatively new level of service.

*Tim Berners-Lee, James Hendler, and Ora Lassila
Scientific American, May 2001*

Ontology = Taxonomies + Axioms?

- An ontology is a formal, explicit specifications of a shared conceptualization.
- The ontology for the Web has a **taxonomy** and a set of **inference rules**. The taxonomy defines classes of objects and relations among them. Inference rules in ontologies supply further power.
- Some people treat ontology as a subset of logic, some treat logic as a subset of ontological reasoning, and others consider the terms disjoint.
- Is the ontology equation shown to be: **Ontology = Taxonomies + Axioms?**

Ontology Language vs. Rule Language

☞ RDF/RDF(S)  ontology language

☞ OIL  ontology/rule language

☞ DAML + OIL  ontology/rule language

☞ RuleML  rule language

☞ DAML-Rules  rule language

Ontology Languages for the Semantic Web

Taxonomies	XOL	SHOE	OML	RDF(S)	OIL	DAML+OIL
Subclass of	+	+	+	+	+	+
Exhaustive decompositions	-	-	+/-	-	+	+
Disjoint decompositions	-	-	+	-	+	+
Not subclass of	-	-	-	-	+	+
Concepts	XOL	SHOE	OML	RDF(S)	OIL	DAML+OIL
General Issues						
Partitions	-	-	+	-	+	+
Documentation	+	+	+	+	+	+
Attributes						
Instance attributes	+	+	+	+	+	+
Class attributes	+	-	+	-	+	+
Local scope	+	+	+	+	+	+
Global scope	+	-	+	+	+	+
Facets						
Default value	+	-	-	-	-	-
Type constraints	+	+	+	+	+	+
Cardinality constraints	+	-	-	-	+	+
Documentation	+	+	+	+	+	+

Asuncion Gomez-Peres and Oscar Corcho

Ontology Languages for the Semantic Web (conti.)

Instances	XOL	SHOE	OML	RDF(S)	OIL	DAML+OIL
Instances of concepts	+	+	+	+	+	+
Facts	+	+	+	+	+	+
Claims	-	+	-	+/-	+/-	+/-
Axioms	XOL	SHOE	OML	RDF(S)	OIL	DAML+OIL
First-order logic	-	+/-	+	-	+/-	+/-
Second-order logic	-	-	-	-	-	-
Independent axioms	-	-	-	-	-	-
Embedded axioms	-	-	+	-	-	-
Relations and functions	XOL	SHOE	OML	RDF(S)	OIL	DAML+OIL
<i>n</i> -ary relations/functions	+/-	+	+	+/-	+/-	+/-
Type constraints	+	+	+	+	+	+
Integrity constraints	-	-	+	-	-	-
Operational definitions	-	-	-	-	-	-

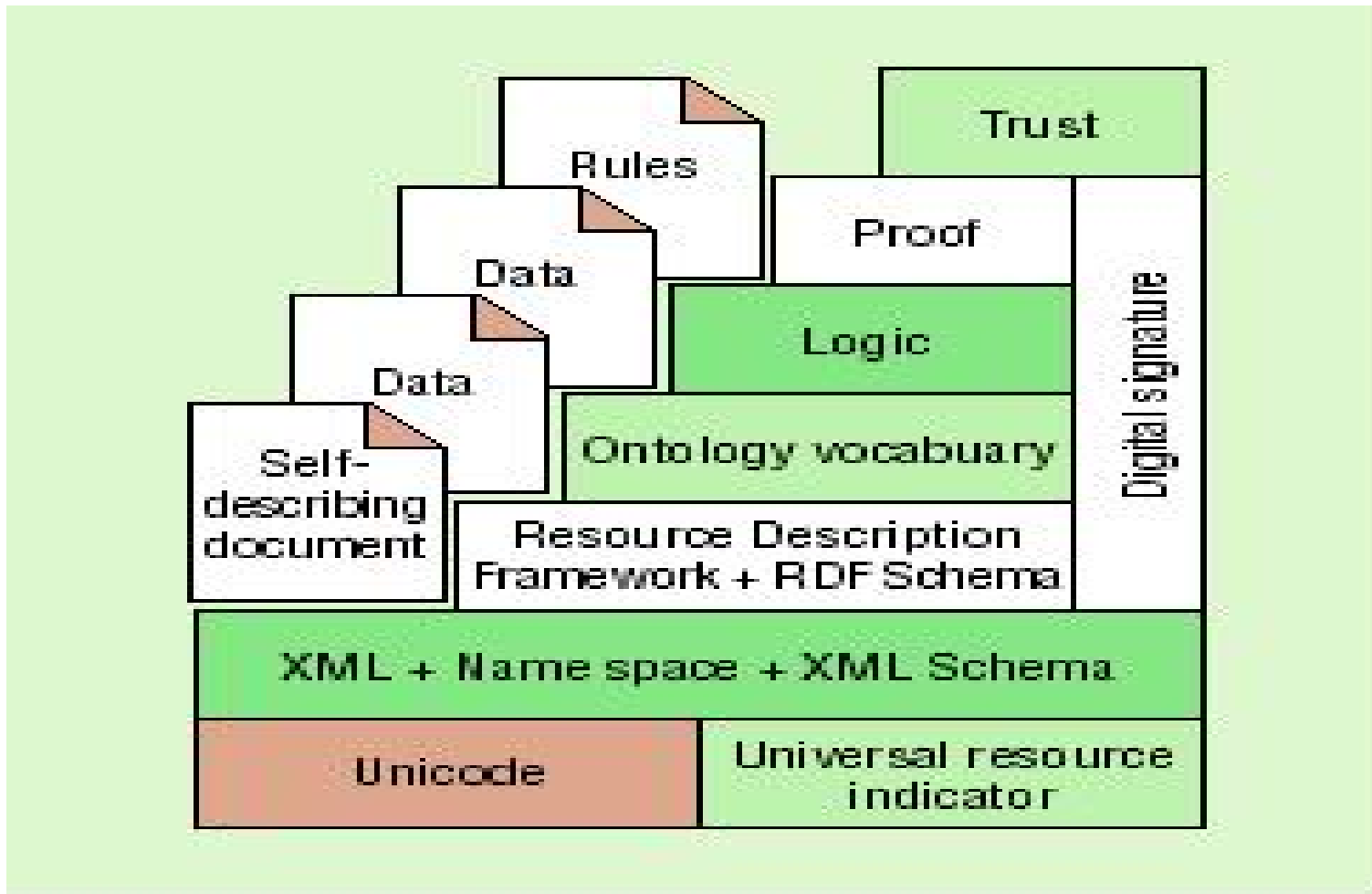
Asuncion Gomez-Peres and Oscar Corcho

Agents and the Semantic Web

The real power of the Semantic Web will be realized when people create many programs that collect Web content from diverse sources, process the information and exchange the results with other programs. The effectiveness of such software agents will increase exponentially as more machine-readable Web content and automated services (including other agents) become available. . . .

Tim Berners-Lee, James Hendler, and Ora Lassila

The “Original Layer Cake” for the Semantic Web



Tim Berners-Lee

Agents and Ontology

- ➡ Ontology specifies the concepts and terms in a well-defined format for agents to refer and communicate.
- ➡ If the ontology specifies that a particular class has a particular property and that the property has some restriction, then each agent can assume that the other has legal values for that property maintaining that restriction.
- ➡ Agents that are not using the same ontology might still be able to communicate. If you can find a common ontology for each agent's ontology to map into.

The Semantic Web Rules

Axioms and Rules for DAML+OIL

Based on our observations, the DAML+OIL only provides axioms and rules for reasoning on the followings:

👉 Ontology **design**

- ✓ Check class consistency and (unexpected) implied relationships
- ✓ Particularly important with large ontologies/multiple authors

👉 Ontology **integration**

- ✓ Assert inter-ontology relationships
- ✓ Reasoner computes integrated class hierarchy/consistency

Axioms and Rules for DAML+OIL (conti.)

👉 Ontology deployment

- ✓ Determine if set of facts are consistent w.r.t. ontology
- ✓ Answer queries w.r.t. ontology, e.g. DQL

Are those axioms and rules enough for us to define our arbitrary trust validation rules once we have built the trust ontologies?

RuleML

- ➡ RuleML is a rule markup language for the Semantic Web.
- ➡ RuleML rulebase exchange will require a taxonomy of the relations defined in the rulebase, where a relation with its arguments becomes a class with its slots.
- ➡ DAML+OIL taxonomies will require a rule system to derive/use certain implicit information that is not captured by the taxonomy alone.

DAML-OIL vs. DAML-Rules

- ➡ DAML+OIL is based on Description Logic (DL) and RuleML is based on logic programs (LP).
- ➡ DAML-Rules is a semantic rule markup language for Web resources and it builds on XML and RDF(S).
- ➡ DAML+OIL is an ontology language and RuleML is a rule markup language.
- ➡ A consistent shared taxonomies with portable and interoperable axioms (rules) are required for agents to achieve *autonomous*, *pro-active*, *reactive*, and *flexible* service characteristics.

Combining Rules with Ontologies for the Semantic Web: DAML+OIL vs. RuleML

Two techniques for combination

- ➡ Meta-ontology: use DAML+OIL at a logical meta-level in order to describe classes of rules and rule sets.
- ➡ KR (Knowledge Representation) fusion: build rules on top of ontologies or build ontologies on top of rules.

Benjamin Grosz

Agent-Mediated E-Services

Web(or E)- Services

“Web Services are a new breed of Web application. They are self-contained, self-describing, modular applications that can be published, located, and invoked across the Web. Web services perform functions, which can be anything from simple requests to complicated business process. . . . Once a Web service is deployed, other applications (and other Web services) can discover and invoke the deployed service.”

IBM web service tutorial

Agent-Mediated E-Services (AMES)

The Semantic Web should enable users (or agents) to locate, select, employ, compose, and monitor Web-based services **automatically**. So the primary motivations for Agent-Mediate E-Services (AMES) are:

- ➡ Automatic Web service discovery
- ➡ Automatic Web service invocation
- ➡ Automatic Web service composition and interoperation

Existing AMES Frameworks

👉 DAML-S + OAA

👉 RETSINA/LARKS

👉 IMPACT

👉 FIPA JAS

Ontologies for DAML-S Framework

DAML-S has the following ontologies but it lacks of trust ontologies to prove the trustworthiness of its AMES framework.

👉 Service ontology

👉 Process ontology

👉 Process control ontology (Not Ready Yet)

Trusted Agent-Mediated E-Services

The Trust on the Semantic Web

- ➡ The Web of trust is based on the **proofs** on the Web but very little has been done on this layer.
- ➡ The proof will be a chain of **assertions** and **reasoning rules** with pointers to all the supporting material on the WWW.
- ➡ A semantic Web will not require proof generation, i.e. find the path that constructs a valid proof, to be useful so **proof validation** will be enough.
- ➡ This proof validation w.r.t. Web of trust is a **decidable** reasoning process.
- ➡ An important facet of agents' functioning will be the exchange of "proofs" written in the Semantic Web's **unifying language**. (the language that expresses logical inferences made using rules and information such as those specified by ontologies).

Trusted Agent-Mediated E-Services

- ➡ The trust issue will be one of the most important issues for the successful deployment of agent-mediated e-services framework.
- ➡ People still do not know what are the specific trust issues need to be considered and resolved.
- ➡ Security mechanisms can solve some of trust problems but not all of them so we need a **total** solution for the agent trust verification on the WWW.
- ➡ We must find out what are the trust verification rules besides the security validation rules.

Why Trust Agent and Delegate our Authority?

- ➡ The reasons for human (or agent) to trust their (peer) agents and delegate its authority to these agents are: efficiency, convenience, domain knowledge, capability, fault tolerance, etc.
- ➡ The most important one for agent's delegation is that agents are cyberspace creatures.
- ➡ If you **fully(partially)** trust your agent, then we assume you might delegate your complete(partial) authority to your agents.

Agent Trust Issues

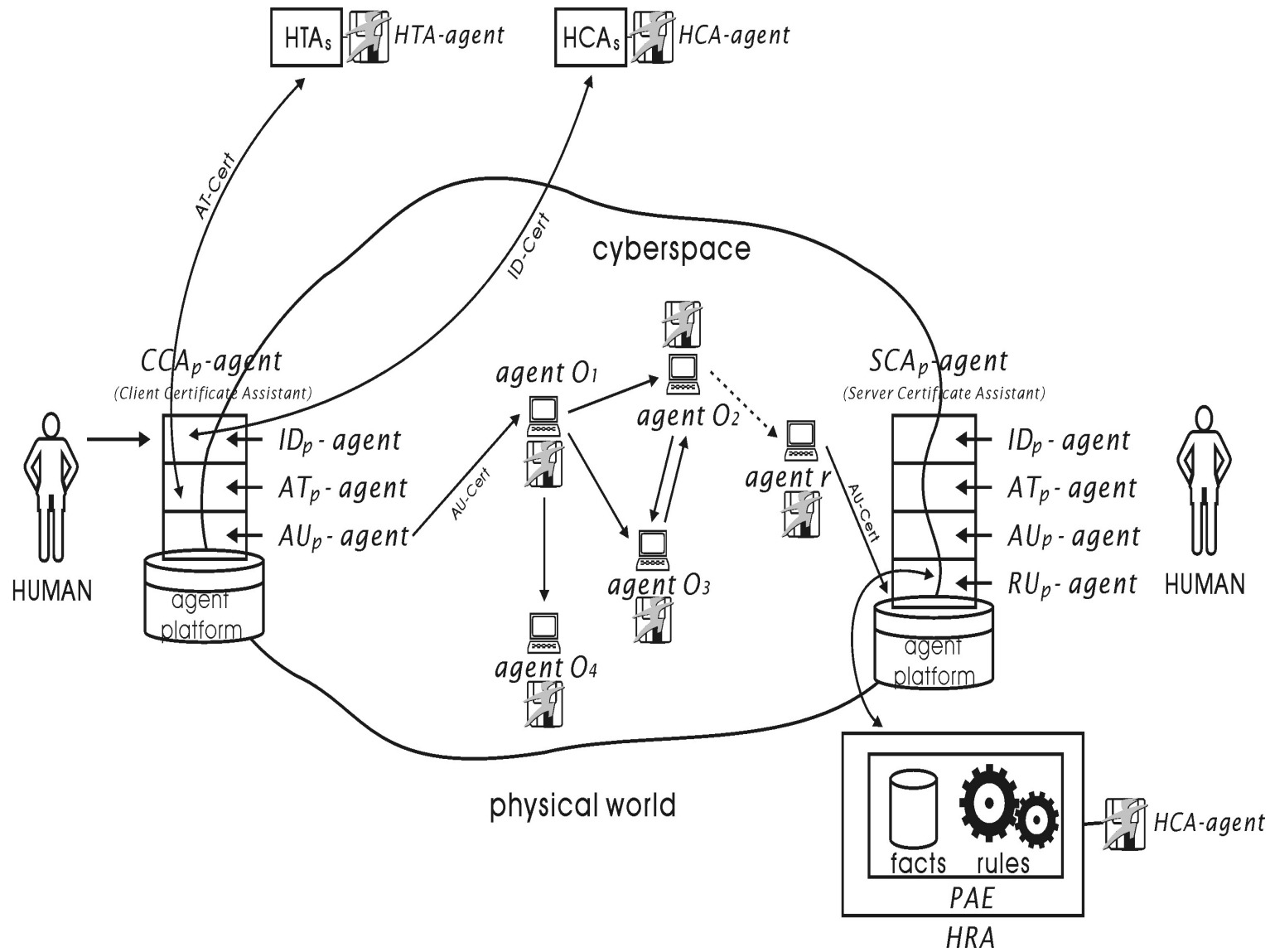
There are at least two facets to deal with agent trust problem:

- ✎ The trust on **agent delegation** must satisfy the “*competence*” (*capability*) and “*disposition*” (*willingness*) criteria.
- ✓ Do you (or your agent) trust your agent (or another agent) so that the important mediation e-services authority can be granted to the delegatee agent?
- ✓ How do you make sure that agent can proceed and finish the task as your intention?
- ✓ Do you have to monitor and control your agent’s operations all the time to guarantee high quality of trust?

Agent Trust Issues (conti.)

- ☞ The trust on **access control** for guardian agent must satisfy the “*authentication*” and “*authorization*” criteria.
- ✓ Once you trust your agents and delegate the access control authority for them to protect your precious resources, what kinds of methodologies are available for your guardian agent to ascertain the access control trust?
- ✓ Achieving agent trust on delegation and access control, we propose that the validation of agent’s authentication and authorization criteria is a fundamental issue.
- ✓ What other issues are needed to consider for agent trust besides authentication and authorization criteria?

Agent-Oriented PKI



Open Group Delegation Scenario

A researcher m_1 is going to apply for financial support from the NSF (National Science Foundation)-Trust to participate in the AMEC 2002 conference. The NSF-Trust requirements for the approval of financial support must have the following digital certificates:

- ✓ an applicant must have a legal citizenship*
- ✓ an applicant must be an faculty member at an MOE(Minister of Education) certified university*
- ✓ an applicant must have full paper(s) accepted by the AMEC 2002 conference*

Access Control Rules for NSF-Trust

Rules

1. NSF-Trust delegates the *issuing* operations for
 $ID_{HCA \mapsto h} - Cert = (?Id_h, ?Pu_h, ?V, Option, ?Sig_{HCA})$ to HCA
If $HCA \in (US - Trust)$.
2. NSF-Trust delegates the *issuing* operations for
 $AT_{HTA \mapsto h} - Cert_1 = (?Id_h, ?IsFacultyOf(?Id_h, ?Id_{HTA}), ?V, Option, ?Sig_{HTA})$
to HTA If HTA *has* $AT_{MOE-Trust \mapsto HTA} - Cert_2$.
3. NSF-Trust delegates the *issuing* operations for
 $AT_{HTA \mapsto h} - Cert_3 = (?Id_h, ?IsFullPaperAcceptedBy(?Id_h, ?Id_{HTA}),$
 $?V, Option, ?Sig_{HTA})$ to HTA
If $HTA \in (ACM - Trust, IEEE - Trust, AMEC - Trust, \dots)$.
4. NSF-Trust delegates the operation for
 $(UseTravelCredit(?Id_h, ?T - Amount) \wedge$
 $UseRegistCredit(?Id_h, ?R - Amount))$ to $Name(?Id_h)$
If $ID_{HCA \mapsto h} - Cert \wedge AT_{HTA \mapsto h} - Cert_1 \wedge AT_{HTA \mapsto h} - Cert_3$.
5. NSF-Trust says $PublicKey(?Pu_h)$ speaks for $Name(?Id_h)$ with
role as $IstheAuthorFor(?Id_h, ?Id_{HTA})$ on the operations for
 $UseTravelCredit(?Id_h, ?T - Amount) \wedge UseRegistCredit(?Id_h, ?R - Amount)$
If $IsPublicKey(?Pu_h, ?Id_h)$.

Access Control Facts for NSF-Trust

Facts

1. $ID_{US-Trust \mapsto m_1} - Cert = (Id_{m_1}, 12345, 2001/01/01 - 2002/12/31, Option, Sig_{US-Trust})$
2. $AT_{NCCU-Trust \mapsto m_1} - Cert_1 = (Id_{m_1}, IsFacultyOf(Id_{m_1}, Id_{NCCU-Trust}), 2001/02/02 - 2004/12/31, Option, Sig_{NCCU-Trust})$
3. $AT_{MOE-Trust \mapsto NCCU-Trust} - Cert_2 = (Id_{NCCU-Trust}, IsCertifiedBy(Id_{NCCU-Trust}, Id_{MOE-Trust}), 2001/02/02 -, Option, Sig_{MOE-Trust})$
4. $AT_{AMEC-Trust \mapsto m_1} - Cert_3 = (Id_{m_1}, IsFullPaperAcceptedBy(Id_{m_1}, Id_{AMEC-Trust}), 2002/02/02 - 2002/02/31, Option, Sig_{AMEC-Trust})$
5. $IsPublicKey(12345, Id_{m_1})$
6. $IsPublicKey(54321, Id_{NSF-Trust})$
7. $IsPublicKey(56789, Id_{NCCU-Trust})$
8. $IsPublicKey(67891, Id_{MOE-Trust})$
9. $IsPublicKey(78912, Id_{AMEC-Trust})$

Research Challenges

On-Going Research Issues

- Design and implement the **trust ontology taxonomies** and **verification rules** for agent-mediated e-services to evaluate agent's authentication, authorization, delegation, and trust, etc criteria.
- Establish the **semantic web rules inference framework** to execute our trust and delegation e-services rules on the Web.
- Use both the trust ontology taxonomy and semantic web rules inference to verify our **trusted agent-mediated e-services model** on the Internet.
- Build a **generic trusted open agent e-services framework** based on FIPA abstract agent architecture to serve a variety of e-service models.

Conclusion

- The **Semantic Web** is one of the important emerging research areas and the results are very promising in the near future.
- The real power of the Semantic Web will be realized when people create a lot of **software agents** to fulfill the agent characteristics for automated e-services.
- The relationships among **Semantic Web, ontology, agent,** and **trust** need to be established.
- The ontology equation: **Ontology = Taxonomies + Axioms (Rules)** needs to be verified.
- One of the challenge issues for the successful deployment of agent-mediated e-services is to resolve the **Web of trust** problem on the Semantic Web.
- The **trusted Semantic Web** has been done very little at this moment but people are very interested in achieving this objective.

References

- ✧ Abadi, M., Burrows, M., and Lampson, B., A Calculus for Access Control in Distributed Systems. *ACM Transactions on Programming Languages and Systems*, 15, 4, (Sep. 1993), 706-734.
- ✧ Ankolekar, A., et al., DAML-S: Semantic Markup For Web Services, *Proceedings of the First Semantic Web Working Symposium, SWWS'01*, Stanford University, California, USA, Jul 30 - August 1, 2001, pp. 411-430.
- ✧ Aura, Tuomas, Distributed Access-Rights Management with Delegation Certificates. *Secure Internet Programming: Security Issues for Mobile and Distributed Objects* LNCS 1603, Springer-Verlag, 1999, 213-238.
- ✧ Boley, H., S. Tabet, and G. Wagner, Design Rational of RuleML: A Markup Language for Semantic Web Rules, *Proceedings of the First Semantic Web Working Symposium, SWWS'01*, Stanford University, California, USA, Jul 30 - August 1, 2001, pp. 381-401.
- ✧ Castelfranchi, Cristiano and Falcone, Rino, Trust and Control: A Dialectic Link, *Applied Artificial Intelligence*, 14:799-823, 2000.
- ✧ Ellison, M. Carl, SPKI/SDSI Certificates, <http://world.std.com/~cme/html/spki.html>.
- ✧ Farrell, S. and R. Housley, An Internet Attribute Certificate Profile for Authorization, draft-ietf-pkix-ac509prof-06.txt, <http://www.ietf.org/internet-drafts>.
- ✧ FIPA Abstract Architecture Specification, Document No. PC00094, 2001, <http://www.fipa.org>.
- ✧ FIPA Nomadic Application Support Specification, Document No. XC00014D, 2001, <http://www.fipa.org>.
- ✧ Ford, Warwick and Baum, S. Michael, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures & Encryption*, Prentice Hall, 1997.

- ✧ Gerck, Ed, *Toward Real-World Models of Trust: Reliance on Received Information*, <http://www.mcg.org.br/trustdef.htm>.
- ✧ Gladney, H., Safe Deals Between Strangers, *IBM Research Technical Report(draft)*, IBM Almaden Research Center, August, 1999.
- ✧ Grosz, N. Benjamin and Labrou, Yannis, An Approach to using XML and a Rule-based Content Language with an Agent Communication Language, *IBM Research Report*, RC 21491(96965) 28 May 1999.
- ✧ He, Qi, Sycara, Katia, and Finin, Tim, Personal Security Agent: KQML-Based PKI. *Proceedings of the Second International Conference on Autonomous Agents*, May 1998.
- ✧ Heckman, C. and O. J. Wobbrock. Put your Best Forward: Anthropomorphic Agents, E-Commerce, Consumers, and the Law, *Proceedings of the Fourth International Conference on Autonomous Agents*, Barcelona, pp. 435-441.
- ✧ Hendler, J., Agents and the Semantic Web, *IEEE Intelligent Systems*, Vol. 16(2), March-April, 2001, pp. 30-37.
- ✧ Herzberg, A., et al., Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers, *2000 IEEE Symposium on Security and Privacy*, 2000, 2-14.
- ✧ Hu, Y. J., Some Thoughts on Agent Trust and Delegation, *Proceedings of the Fifth International Conference on Autonomous Agents*, May 28-June 1, 2001, Montreal, Canada, pp. 489-496.
- ✧ Hu, Y.J., Trusted Agent-Mediated E-Commerce Transaction Services via Digital Certificates Management , *Electronic Commerce Research*, May 2002, <http://www.baltzer.nl/journalhome.htm/1389-5753> .
- ✧ Java Agent Services Specification Version 1.0, <http://www.Java-agent.org>.

- ✧ Jennings, R. N., K. Sycara, and M. Wooldridge, A Roadmap of Agent Research and Development, *Autonomous Agents and Multi-Agent Systems*, 1, pp. 7-38.
- ✧ Kimbrough, O. S. and Moore, A. S., On Automated Message Processing in Electronic Commerce and Work Support Systems: Speech Act Theory and Expressive Felicity, *ACM Tran. on Information Systems*, Vol. 15, No. 4, October 1997, 321-367.
- ✧ Klusch, M. and K. Sycara, Brokering and Matchmaking for Coordination of Agent Societies: A Survey, *Coordination of Internet Agents*, A. Omicini et al. (eds.), Springer, 2001.
- ✧ Lampson, B., Abadi, M., Burrows, M., and Wobber, E. Authentication in Distributed Systems: Theory and Practice. *ACM Trans. Computer Systems*, 10, 4 (Nov. 1992), 265-310.
- ✧ Lee, Ing-Chung and Hu, Y. J., An Agent-Based Secure E-Commerce Environment with Distributed Authentication and Authorization Services, *The 2001 International Conference on Internet Computing(IC-2001) Session on "Agents for E-Business on the Internet"*, Monte Carlo Resort, Las-Vegas, USA, June 25-28, 2001.
- ✧ Li, Ninghui, Grosf, Benjamin, and Feigenbaum, Joan, A Practically Implementable and Tractable Delegation Logic, *IEEE 2000 Symposium on Security and Privacy*, 2000.
- ✧ Li, N., Grosf, N. B., and Feigenbaum. J., A Logic-based Knowledge Representation for Authorization with Delegation, *IBM Research Report*, RC 21492(96966) 28 May 1999.
- ✧ Manchala, W. Daniel, E-Commerce Trust Metrics and Models, *IEEE Internet Computing*, Vol. 4 No. 2, March-April, 2000, pp. 36-44.
- ✧ Martin, L. D., Cheyer, J. A., Moran, B. D., The Open Agent Architecture: A Framework for Building Distributed Software Systems. *Applied Artificial Intelligence*, 13, 1999, 91-128.
- ✧ McIlraith, A. S., T. C. Son, and H. Zeng, Semantic Web Services, *IEEE Intelligent Systems*, Vol. 16(2), March-April, 2001, pp. 46-53.

- ✧ Moukas, A., Guttman, R., Zacharia, G., and Maes, P., Agent-mediated Electronic Commerce: An MIT Media Laboratory Perspective. *International Journal of Electronic Commerce*, Vol. 4 , No. 3, Spring 2000.
- ✧ Nwana, S. H., et al., Agent-Mediated Electronic Commerce: Issues, Challenges and some Viewpoints. *Proceedings of the Second International Conference on Autonomous Agents*, 1998, 189-196.
- ✧ Rivest, Ron and Lampson, Bulter, SDSI- A Simple Distributed Security Architecture, <http://theory.lcs.mit.edu/cis/sdsi.html>.
- ✧ Sowa, f. John, *Knowledge Representation: Logical, Philosophical, and Computational Foundations*, 2000 Brooks/Cole.
- ✧ Subrahmanian, V. S., et al., *Heterogeneous Agent Systems*, MIT Press, 2000.
- ✧ Sycara, K. et al., The RETSINA MAS Infrastructure, *Journal of Autonomous Agent and Multi-Agent System (JAAMAS)*, Kluwer Academic Publishers, 2002.
- ✧ Tim Beners-Lee, James Hendler, and Ora Lassila, The Semantic Web, *Scientific American*, May, 2001
- ✧ UDDI Version 2.0 API Specification, UDDI Open Draft Specification 8 June 2001, <http://www.uddi.org>.
- ✧ Winslett, M., Ching, N., Jones, V., and Slepchin, I. Using Digital Credentials on the World-Wide Web. *Journal of Computer Security*, 1997, <http://drl.cs.uiuc.edu/security/pubs.html>.
- ✧ Wong, H. C., and Sycara, K. Adding Security and Trust to Multi-Agent Systems. *Proceedings of Autonomous Agents '99 (Workshop on Deception, Fraud and Trust in Agent Societies)*. May 1999, Seattle, Washington, pp. 149-161.
- ✧ Wooldridge, M., Semantic Issues in the Verification of Agent Communication Languages, *Autonomous Agents and Multi-Agent Systems*, 3, 9-31(2000).
- ✧ Web Services Description Language(WSDL) 1.1, W3C Note 15, March 2001, <http://www.w3c.org/TR/wsdl>
- ✧ Zacharia, G. and P. Maes. Trust Management Through Reputation Mechanisms. *Applied Artificial Intelligence*, 14, pp. 881-907.