I2-D8

Semantic Web Policies: where are we and what is still missing – ESWC'06 Tutorial

Project number:	IST-2004-506779
Project title:	Reasoning on the Web with Rules and Semantics
Project acronym:	REWERSE
Document type:	D (deliverable)
Nature of document	O (other)
Dissemination level:	PU (public)
Document number:	IST506779/Naples/I2-D8/D/PU/b0.0
Responsible editor(s):	P. A. Bonatti
Contributing participants:	Hannover, Naples
Contributing workpackages:	I2
Contractual date of delivery:	30 June 2006
Actual date of delivery:	31 August 2006

Abstract

The term *policy* encompasses different notions like, among others, security policies, trust management policies, business rules and quality of service specifications. Researchers have mainly focuses in one or more contexts separately but not on a broader view. In addition, in web applications, policies are pervasive and they play crucial roles in enhancing security, privacy, but also service usability. Interoperability and self-describing semantics become key requirements and there is where Semantic Web comes into play.

This tutorial aims at providing an overall view of state of the art (requirements for a policy framework, existing policy frameworks/languages, policy negotiation, context awareness, etc.) as well as open research issues in the area (understanding of policies in their broad sense, integration of trust management, increasement of system cooperation, user-awareness, etc.) required to develop a successful Semantic Policy Framework.

Keyword List

Policies, Security, Trust, Privacy, Negotiation

Semantic Web Policies: where are we and what is still missing – ESWC'06 Tutorial

P. A. Bonatti[1] **and D. Olmedilla**[2]

[1] Università di Napoli Federico II
Email: bonatti@na.infn.it

[2] L3S Research Center and Hanover University
Email: olmedilla@l3s.de

14 September 2006

Abstract
The term *policy* encompasses different notions like, among others, security policies, trust management policies, business rules and quality of service specifications. Researchers have mainly focuses in one or more contexts separately but not on a broader view. In addition, in web applications, policies are pervasive and they play crucial roles in enhancing security, privacy, but also service usability. Interoperability and self-describing semantics become key requirements and there is where Semantic Web comes into play.

This tutorial aims at providing an overall view of state of the art (requirements for a policy framework, existing policy frameworks/languages, policy negotiation, context awareness, etc.) as well as open research issues in the area (understanding of policies in their broad sense, integration of trust management, increasement of system cooperation, user-awareness, etc.) required to develop a successful Semantic Policy Framework.

Keyword List
Policies, Security, Trust, Privacy, Negotiation

Contents

1 Tutorial Description

There has been extensive research in the area, including the Semantic Web community, but there exist yet some issues that prevent policy frameworks from its adoption by users and real world applications. This tutorial aims at providing an overall view of state of the art (requirements for a policy framework, existing policy frameworks/languages, policy negotiation, context awareness, etc.) as well as open research issues in the area (understanding of policies in their broad sense, integration of trust management, increasement of system cooperation, user-awareness, etc.) required to develop a successful Semantic Policy Framework.

The tutorial will focus on the following three main blocks:

- **Block 1:** *Policies: What, Why, What for and How*
  This block of the tutorial will provide the basis to understand the rest of the tutorial, trying to give a general overview of the motivation and need of policy research. It will focus on providing a clear view of *what* a policy is, the different notions of policies that are included within the single term "policy" (e.g., security policies, trust management policies, business rules, etc.) and *why* they are important. In addition, it will enumerate the set of requirements that policies must fulfill and *what* they are useful *for*, as well as sketch some ideas of the different possibilities of *how* those requirements can be fulfilled.

- **Block 2:** *Policy Languages/Frameworks*
  This block aims at providing an exhaustive description of the policy languages and frameworks that have been specified to date, what are the contexts where they are applied, the main rationals behind their specification, some examples and their limitations. A not yet complete list of the languages/frameworks that we plan to include is REI/REIN [131, 130, 207], Kaos [210, 211, 207], EPAL [86, 20, 21], XACML [172], PSPL [44], RT [156, 152, 153], SD3 [208], PeerTrust [95, 169, 202], Cassandra [25, 26], Protune [51, 52] and PeerAccess [246].

- **Block 3:** *Open Research Issues*
  This block will try to highlight and orientate new researchers into those issues which have not yet been focus of attention or which still remain unsolved. Special interest will be given to those that represent crucial problems in order to have a semantic policy framework to be adopted in real world applications. There will be discussed issues like different notions covered by policies, explanations and user awareness, legacy systems and numerical trust management integration, management of disclosed information, etc.

The tutorial will be presented to the audience in a lecture mode. However, in order to maximize the profit of the tutorial, we plan to performed it as interactive as possible in a way in which the audience is able to participate actively. The presenters will use a set of slides to be displayed with a proyector (and which will be distributed to the audience) as well as extra slides to be shown in case any participant requires a more detailed view in a specific area. No specific technical requirements are needed apart of a proyector and a whiteboard for annotations and further explanations.

2 Relevance of the tutorial to ESWC 2006

Policy specification and enforcement is not a new research topic. Interoperabiliy, user awareness, explanations, etc. are just some examples of the relevance to Semantic Web research. Recently, policies have been given a higher relevance in the context of the (Semantic) Web and therefore it is required to have a clear understanding of the new challenges and what is already covered by state of the art. The relevance of a tutorial on policies to the European Semantic Web Conference is clear: providing new researchers in the area (new Ph.D. students or researchers moving in from different areas) with an overview of existing state of the art and open lines of research in order to maximize their future research contributions in the field.

3 Outline of the tutorial content and schedule

The tutorial will be scheduled as follows:

Timing	**Block N**	**Brief Description**
0:00 — 0:30	1	*Policies: What, Why, What for and How* What is a policy and examples, why policies are needed and requirements: Well-defined semantics,, Expressivity, Delegation of authority, Negotiations, Stateful vs Stateless protocols, Credential-based Monotonicity, Light & Strong evidence management, Policy protection, External functions integration, etc.
0:30 — 2:00	2	*Policy Languages/Frameworks* Rei/Rein, Kaos, EPAL, XACML, PSPL, RT, SD3, PeerTrust, Cassandra, Protune, PeerAccess, etc.
2:00 — 3:00	3	*Open Research Issues* Notion of policy covered, Explanations, User awareness, Legacy systems integration, Numerical Trust management Integration, Management of disclosed information, Others.

4 Information on presenters

Piero A. Bonatti is a professor at the University of Naples "Federico II" and coordinator of the working group on Policy specification, composition and conformance of the Network of Excellence REWERSE (EU FP6). His main research interests include Computer Security and Knowledge Representation and Reasoning. He published over sixty papers on these topics. He has over 10 years of experience in teaching. Currently he is a member of the Steering Commettee of the PhD school in Computational Sciences and Informatics of the University of Naples "Federico II". Further experiences in organizing and teaching PhD-level tutorials include: (i) Co-organization of the 1998 International Summer School on Logic Programming Perspectives in hot research areas, Acquafredda di Maratea (Basilicata, Italy) September 7-12, 1998 `http://www.di.unito.it/~bonatti/SCUOLA_GULP`; (ii) the tutorial "Nonmonotonic logics and their application to security", University of Dortmund, Computer Science Department, 26/8-1/9/2001; (iii) the tutorial "Nonmonotonic Logics: History, foundations, challenges" held at the 2005 ICCL Summer School on Logic-based Knowledge Representation, Technische

Universitat Dresden, 2nd - 17th July 2005 http://www.computational-logic.org/content/events/iccl-ss-2005/.
Daniel Olmedilla is a PhD student at the University of Hannover's Computer Science Department and a research scientist at the L3S Research Center. He is a member of the PeerTrust project[1] and the research Network of Excellence REWERSE[2] which deal with trust, security and privacy in distributed environments like the Web, P2P and Grid. He has published several policy related publications like [202, 51, 170, 95, 49, 169]. In addition, he is/has has been a reviewer/PC member of several conferences, journals and workshops including ISWC, Journal of Web Semantics, IEEE TCLT's Journal of Educational Technology & Society, IEEE ISCAS, IEEE ISPA and RuleML. He has organized several workshops including "Trust, Security, and Reputation on the SW" at ISWC'04 and the forthcoming "Trust Models for the Web" at WWW'06. Daniel Olmedilla has taught "Software Engineering" and "Oberstufenlabor" (slightly theory and mainly project oriented courses) at the Faculty of Information Systems, University of Hannover as well as supervised several Bachelor and Master thesis students.

5 Online material

- **Tutorial page**:
  http://www.l3s.de/~olmedilla/events/2006/ESWC06/ESWC06_Tutorial.html
- **Tutorial page on the ESWC'06 site**:
  http://www.eswc2006.org/tutorials.html#tutorial3
- **Slides**:
  http://www.l3s.de/~olmedilla/presentations/2006/20060611_ESWC_Tutorial_Policies.pdf

[1] http://www.l3s.de/peertrust/
[2] http://www.rewerse.net/i2/

References

[1] *Liberty Alliance Project. http://www.projectliberty.org/about/whitepapers.php.*

[2] PeerTrust Project. http://sourceforge.net/projects/peertrust/.

[3] *Web Services Trust Language (WS-Trust) Specification. http://www-106.ibm.com/developerworks/library/specification/ws-trust/.*

[4] Smartcard Security: Essential and Assurable!, 1998.

[5] *Proceedings of the Network and Distributed System Security Symposium, NDSS 2001, San Diego, California, USA*. The Internet Society, 2001.

[6] http://www.ics.mq.edu.au/ rolfs/controlled-natural-languages (controlled natural language homepage), 2004.

[7] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *HICSS 2000*, 2000.

[8] K. Aberer. P-grid: A self-organizing access structure for p2p information systems. In *Ninth International Conference on Cooperative Information Systems (CooIS 01)*, 2001.

[9] K. Aberer and Z. Despotovic. Managing trust in a peer-2-peer information system. In *CIKM 2001*, pages 310–317, 2001.

[10] K. Aberer and Z. Despotovic. On reputation in game theory - application to online settings, 2004. Working paper.

[11] N.R. Adam and J.C. Wortman. Security-Control Methods for Statistical Databases: A Comparative Study. *ACM Computing Surveys*, 21(4), 1989.

[12] E. Adar and B.A. Huberman. Free riding on gnutella. Technical report, Xerox, PARC, 2000.

[13] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In *28th International Conference on Very Large Data Bases*, Hong Kong, August 2002.

[14] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Implementing P3P Using Database Technology. In *19th International Conference on Data Engineering*, Bangalore, March 2003.

[15] A.Herzberg, Y. Mass, J. Mihaeli, D. Naor, and Y. Ravid. Access control meets public key infrastructure, or: Assigning roles to strangers. In *IEEE Symposium on Security and Privacy*, pages 2–14, 2000.

[16] Grigoris Antoniou, Michael J. Maher, and David Billington. Defeasible logic versus logic programming without negation as failure. *Journal of Logic Programming*, 42(1):47–57, 2000.

[17] K. R. Apt, D. S. Warren, and M. Truszczynski, editors. *The Logic Programming Paradigm: A 25-Year Perspective*. Springer-Verlag, 1999.

[18] A.Skarmeta, G. Perez, O. Reverte, and G. Millan. PKI Sevices for IPv6. *IEEE Internet Computing*, 7(3), May 2003.

[19] R. Atkinson. Security Architecture for the Internet Protocol. In *http://www.ietf.org/rfc/rfc2401.txt*, November 1998.

[20] Michael Backes, Markus Dürmuth, and Günter Karjoth. Unification in privacy policy evaluation - translating EPAL into prolog. In *POLICY*, pages 185–188, 2004.

[21] Michael Backes, Birgit Pfitzmann, and Matthias Schunter. A toolkit for managing enterprise privacy policies. In *Proceedings of the Eight ESORICS*, volume 2808 of *Lecture Notes in Computer Science*, pages 162–180. Springer-Verlag, Berlin Germany, October 2003.

[22] D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H.-C. Wong. Secret Handshakes from Pairing-Based Key Agreements. In *IEEE Symposium on Security and Privacy*, Oakland, May 2003.

[23] D. Bank and M. Prudence. A High-Performance Network Architecture for a PA-RISC Workstation. *IEEE Journal on Selected Areas in Communications*, 2(2):191–202, February 1993.

[24] Jim Basney, Wolfgang Nejdl, Daniel Olmedilla, Von Welch, and Marianne Winslett. Negotiating trust on the grid. In *2nd WWW Workshop on Semantics in P2P and Grid Computing*, New York, USA, May 2004.

[25] M. Y. Becker and P. Sewell. Cassandra: distributed access control policies with tunable expressiveness. In *5th IEEE International Workshop on Policies for Distributed Systems and Networks*, Yorktown Heights, June 2004.

[26] M. Y. Becker and P. Sewell. Cassandra: flexible trust management, applied to electronic health records. In *17th IEEE Computer Security Foundations Workshop*, Pacific Grove, CA, June 2004.

[27] D.E. Bell and L.J. LaPadula. Secure Computer Systems: Mathematical Foundations and Model. Technical Report M74-244, Mitre Corporation, Belford, MA, 1975.

[28] C.J. Bennett. *Regulating Privacy: Data Protection and Public Policies in Europe and the United States*. Cornell University Press, 1992.

[29] E. Bertino, S. Castano, and E. Ferrari. On Specifying Security Policies for Web Documents with an XML-based Language. In *Sixth ACM SACMAT*, Chantilly, VA, May 2001.

[30] Elisa Bertino, Sushil Jojodia, and Pierangela Samarati. Supporting multiple access control policies in database systems. In *IEEE Symposium on Security and Privacy*, pages 94–109, Oakland, CA, 1996. IEEE Computer Society Press.

[31] Thomas Beth, Malte Borcherding, and Birgit Klein. Valuation of trust in open networks. In *Proceedings of the Third European Symposium on Research in Computer Security*, pages 3–18. Springer-Verlag, 1994.

[32] Jaijit Bhattacharya and S. K. Gupta. EPAL based privacy enforcement using ECA rules. In *ICISS*, pages 120–133, 2005.

[33] E. Bina, V. Jones, R. McCool, and M. Winslett. Secure Access to Data Over the Internet. In *Conference on Parallel and Distributed Information Systems*, September 1994.

[34] J. Biskup and P.A. Bonatti. Lying versus refusal for known potential secrets. *Data & Knowledge Engineering*, 38(2), 2001.

[35] J. Biskup and P.A. Bonatti. Controlled Query Evaluation for Known Policies by Combining Lying and Refusal. In *International Symposium on Foundations of Information and Knowledge Systems*, Salzau Castle, Germany, February 2002.

[36] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The KeyNote Trust Management System Version 2. In *Internet Draft RFC 2704*, September 1999.

[37] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis. The KeyNote Trust-Management System Version 2, 1999. RFC 2704.

[38] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. The role of trust management in distributed systems security. *Lecture Notes in Computer Science*, 1603:185–210, 1999.

[39] M. Blaze, J. Feigenbaum, and J.Lacy. Decentralized trust management. In *IEEE Conference on Security and Privacy*, 1996.

[40] M. Blaze, J. Feigenbaum, and A. D. Keromytis. KeyNote: Trust Management for Public-Key Infrastructures. In *Security Protocols Workshop*, Cambridge, UK, 1998.

[41] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 1996.

[42] M. Blaze, J. Feigenbaum, and M. Strauss. Compliance Checking in the PolicyMaker Trust Management System. In *Financial Cryptography*, British West Indies, February 1998.

[43] G. Bleumer. Biometric yet Privacy Protecting Person Authentication. In *International Workshop on Information Hidding*, volume 1525 of *Lecture Notes in Computer Science*. Springer, 1998.

[44] P. Bonatti and P. Samarati. Regulating Service Access and Information Release on the Web. In *Conference on Computer and Communications Security (CCS'00)*, Athens, November 2000.

[45] P. Bonatti, S. Vimercati, and P. Samarati. A Modular Approach to Composing Access Control Policies. In *ACM Conference on Computer and Communication Security*, Athens, Greece, November 2000.

[46] P. A. Bonatti, N. Shahmehri, C. Duma, D. Olmedilla, W. Nejdl, M. Baldoni, C. Baroglio, A. Martelli, V. Patti, P. Coraggio, G. Antoniou, J. Peer, and N. E. Fuchs. Rule-based policy specification: State of the art and future work. Technical report, Working Group I2, EU NoE REWERSE, aug 2004. `http://rewerse.net/deliverables/i2-d1.pdf`.

[47] P.A. Bonatti, D. Olmedilla, and J. Peer. Advanced policy queries. Technical Report I2-D4, Working Group I2, EU NoE REWERSE, Aug 2005. http://www.rewerse.net.

[48] P.A. Bonatti and P. Samarati. A uniform framework for regulating service access and information release on the web. *Journal of Computer Security*, 10(3):241–272, 2002. Short version in the Proc. of the Conference on Computer and Communications Security (CCS'00), Athens, 2000.

[49] Piero A. Bonatti, Grigoris Antoniou, Matteo Baldoni, Cristina Baroglio, Claudiu Duma, Norbert E. Fuchs, Alberto Martelli, Wolfgang Nejdl, Daniel Olmedilla, Viviana Patti, Joachim Peer, and Nahid Shahmehri. The rewerse view on policies. In *Semantic Web Policy Workshop in conjunction with 4th International Semantic Web Conference*, Galway, Ireland, November 2005.

[50] Piero A. Bonatti, Claudiu Duma, Daniel Olmedilla, and Nahid Shahmehri. An integration of reputation-based and policy-based trust management. In *Semantic Web Policy Workshop in conjunction with 4th International Semantic Web Conference*, Galway, Ireland, nov 2005.

[51] Piero A. Bonatti and Daniel Olmedilla. Driving and monitoring provisional trust negotiation with metapolicies. In *6th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2005)*, pages 14–23, Stockholm, Sweden, June 2005. IEEE Computer Society.

[52] Piero A. Bonatti and Daniel Olmedilla. Policy language specification. Technical report, Working Group I2, EU NoE REWERSE, February 2005. `http://rewerse.net/deliverables/m12/i2-d2.pdf`.

[53] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H.F. Nielsen, S. Thatte, and D. Winer. *Simple Object Access Protocol (SOAP) 1.1.* World Wide Web Consortium, May 2000.

[54] Marc Branchaud. A Survey of Public Key Infrastructures. Master's thesis, Department of Computer Science, McGill University, Montreal, March 1997.

[55] S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* The MIT Press, 2000.

[56] C. Breed. Pki: The myth, the magic and the reality. *Information Security*, June 1999.

[57] John S. Breese, David Heckerman, and Carl Kadile. Empirical analysis of predictive algorithms for collaborative filltering. In *14th Conference on Uncertanaity in Artificial Intelligence (UAI-98)*, pages 43–52, July 1998.

[58] Bruce Christianson and William S. Harbison. Why Isn't Trust Transitive? In T. Mark and A. Lomas, editor, *Security Protocols, International Workshop 1996*, LNCS 1189, pages 171–176, Cambridge, United Kingdom, April 10-12 1996. Springer.

[59] Chiranjeeb Buragohain, Divy Agrawal, and Subhash Suri. A game-theoretic framework for incentives in p2p systems. In *IEEE P2P 2003, Linköping, Sweden*, 2003.

[60] J. Camenisch and E.V. Herreweghen. Design and Implementation of the *Idemix* Anonymous Credential System. In *ACM Conference on Computer and Communication Security*, Washington D.C., November 2002.

[61] J. Camenisch and A. Lysyanskaya. Efficient Non-Transferable Anonymous Multi-Show Credential System with Optional Anonymity Revocation. In *EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*. Springer, 2001.

[62] Germano Caronni. Walking the web of trust. In *WETICE*, 2000.

[63] S. Castano, M.G. Fugini, G. Martella, and P. Samarati. *Database Security*. Addison-Wesley & ACM Press, 1995.

[64] C. Castelfranchi and R. Falcone. Principles of trust for mas: Cognitive anatomy, social impoartance, and quantification. pages 72–79, 1998.

[65] D.W. Chadwick, A. Otenko, and E. Ball. Role-Based Access Control With X.509 Attribute Certificates. *IEEE Internet Computing*, 7(2), March 2003.

[66] L. Chang and I.S. Moskowitz. An Integrated Framework for Database Privacy Protection. In *14th IFIP WG11.3 Working Conference on Data and Application Security*, Amsterdam, August 2000.

[67] D. Chaum. Security without Identification: Transactions Systems to Make Big Brother Obsolete. *Communications of the ACM*, 24(2), 1985.

[68] D. Chaum and J.H. Evertse. A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations. In *CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*. Springer, 1987.

[69] Ying Chen. *Automatic Parallel I/O Performance Optimization in Panda*. PhD thesis, Dept. of Computer Science, University of Illinois, February 1998.

[70] F. Chin and G. Ozsoyoglu. Auditing and Inference Control in Statistical Databases. *IEEE Transactions on Software Engineering*, 8(6), 1982.

[71] Yang-Hua Chu, Joan Feigenbaum, Brian LaMacchia, Paul Resnick, and Martin Strauss. REFEREE: Trust management for Web applications. *World Wide Web Journal*, 2:127–139, 1997.

[72] Dwaine Clarke, Jean-Emile Elien, Carl Ellison, Matt Fredette, Alexander Morcos, and Ronald L. Rivest. Certificate chain discovery in spki/sdsi. *Journal of Computer Security*, 9(4):285–322, 2001.

[73] F. Cornelli, E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Choosing Reputable Servents in a P2P Network. In *WWW2002*, 2002.

[74] Paulo P. da Silva, Deborah L. McGuinness, and Richard Fikes. A proof markup language for semantic web services. Technical Report KSL Tech Report KSL-04-01, January, 2004.

[75] I.B. Damgård. Payment Systems and Credential Mechanism with Provable Security Against Abuse by Individuals. In *CRYPTO'88*, volume 403 of *Lecture Notes in Computer Science*. Springer, 1990.

[76] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation-based approach for choosing reliable resources in peer-to-peer networks. In *ACM Conference on Computer and Communications Security*, pages 202–216, 2002.

[77] E. Damiani, S. Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A Reputation-based Approach for Choosing Reliable Resources in Peer-to-Peer Networks. In *ACM Conference on Computer and Communication Security*, Washington, DC, November 2002.

[78] D. Damianou, N. Dulay, E. Lupu, and M. Sloman. The Ponder Policy Specification Language. In *2nd International Workshop on Policies for Distributed Systems and Networks*, Bristol, UK, January 2001.

[79] D. Dean and A. Stubblefield. Using Client Puzzles to Protect TLS. In *Annual USENIX Security Symposium*, Washington, D.C., August 2001.

[80] T. Dierks and C. Allen. The TLS Protocol Version 1.0. In *http://www.ietf.org/rfc/rfc2246.txt*, January 1999.

[81] Roger Dingledine, Michael J. Freedman, and David Molnar. The free haven project: Distributed anonymous storage service. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*. Springer-Verlag, LNCS 2009, 2000.

[82] Stuart Roger Dingledine, Nick Mathewson, and Paul Syverson. Reputation in P2P Anonymity Systems. In *Workshop on economics of P2P systems*, 2003. URL: http://freehaven.net/papers.html.

[83] I. Dinur and K. Nissim. Revealing Information While Preserving Privacy. In *ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems*, San Diego, CA, June 2003.

[84] L.V. Doorn, M. Abadi, M. Burrows, and E. Wobber. Secure Network Objects. In J. Vitek and C.D. Jensen, editors, *Secure Internet Programming, Security Issues for Mobile and Distributed Objects*, pages 395–412. Springer, 1999.

[85] C. Dwork, J.B. Lotspiech, and M. Naor. Digital Signets: Self-Enforcing Protecction of Digital Information. In *Symposium on the Theory of Computing*, Philadelphia, PA, May 1996.

[86] Enterprise privacy authorization language (epal 1.2). `http://www.w3.org/Submission/EPAL/`.

[87] W. Eayr, F. Kastner, G. Pernul, S. Preishuber, and A.M. Tjoa. Authorization and access control in iro-db.

[88] S. Farrell. TLS Extension for Attribute Certificate Based Authorization. In *http://www.ietf.org/proceedings/99jul/I-D/draft-ietf-tls-attr-cert-01.txt*, August 1998.

[89] R. Fikes, D. McGuinness, J. Rice, G. Frank, Y. Sun, and Z. Qing. Distributed repositories of highly expressive reusable knowledge, 1999.

[90] W. Ford. PKI Grows up. *Information Security*, November 1999.

[91] I.T. Foster and A. Iamnitchi. On death, taxes, and the convergence of peer-to-peer and grid computing. In *IPTPS 2003*, pages 118–128, 2003.

[92] A. Frier, P. Karlton, and P. Kocher. *The SSL 3.0 Protocol*. Netscape Communications Corp., November 1996.

[93] D.L. Gamberoni. In-Person Proofing at Post Offices (IPP) Program. In *http://www.ribbs.usps.gov/files/fedreg/usps2003/03-15211.PDF*, June 2003.

[94] Diego Gambetta. Can we trust trust? In Diego Gambeta, editor, *Trust: Making and Breaking Cooperative Relations*, 1990.

[95] Rita Gavriloaie, Wolfgang Nejdl, Daniel Olmedilla, Kent E. Seamons, and Marianne Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. In *1st European Semantic Web Symposium (ESWS 2004)*, volume 3053 of *Lecture Notes in Computer Science*, pages 342–356, Heraklion, Crete, Greece, May 2004. Springer.

[96] M. Gelfond and V. Lifschitz. Logic programs with classical negation. In *Proc. of Int. Conf. on Logic Programming*. MIT Press, 1990.

[97] M. Gelfond and V. Lifschitz. Classical negation in logic programs and disjunctive databases. *New Generation Computing*, 9:365–385, 1991.

[98] Jennifer Golbeck, Bijan Parsia, and James Hendler. Trust networks on the semantic web. In *Cooperative Intelligent Agents*, Helsinki, Finland, August 2003.

[99] O. Goldreich and Y. Oren. Definitions and Properties of Zero-Knowledge Proof Systems. *Journal of Cryptology*, 6(3-4), 1983.

[100] O. Goldreich, B. Pfitzman, and R. Rivest. Self-Delegation with Controlled Propagation — or — What If You Lose Your Laptop. In *CRYPTO'98*, volume 1642 of *Lecture Notes in Computer Science*. Springer, 1998.

[101] L. Gong. A Secure Identity-Based Capability System. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 1989.

[102] T. Grandison and M. Sloman. A survey of trust in internet applications. *IEEE Communications Surveys and Tutorials*, 3(4), 2000.

[103] Tyrone Grandison. *Trust Management for Internet Applications*. PhD thesis, Imperial College London, 2003.

[104] J. Griffith and C. O' Riordan. Collaborative filtering. Technical Report NUIG-IT-160900, National University of Ireland, Galway, September 2000.

[105] Benjamin Grosof. Representing e-business rules for the semantic web: Situated courteous logic programs in RuleML. In *Proceedings of the Workshop on Information Technologies and Systems (WITS)*, New Orleans, LA, USA, December 2001.

[106] Benjamin Grosof and Terrence Poon. SweetDeal: Representing agent contracts with exceptions using XML rules, ontologies, and process descriptions. In *Proceedings of the 12th World Wide Web Conference*, Budapest, Hungary, May 2003.

[107] B.N. Grosof. Prioritized conflict handling for logic programs. In *Proc. International Symposium on Logic Programming (ILPS-97)*, 1997.

[108] C.A. Gunder and T. Jim. Generalized Certificate Revocation. In *Symposium on Principles of Programming Languages*, Boston, MA, January 2000.

[109] A. Herzberg and Y. Mass. Relying Party Credentials Framework. In *The Cryptographer's Track at RSA Conference*, San Francisco, CA, April 2001.

[110] A. Herzberg, J. Mihaeli, Y. Mass, D. Naor, and Y. Ravid. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2000.

[111] A. Hess, J. Jacobson, H. Mills, R. Wamsley, K. Seamons, and B. Smith. Advanced Client/Server Authentication in TLS. In *NDSS*, San Diego, CA, February 2002.

[112] A. Hess and K. E. Seamons. An Access Control Model for Dynamic Client Content. In *8th ACM Symposium on Access Control Models and Technologies*, Como, Italy, June 2003.

[113] High Performance Fortran Forum. *High Performance Fortran Language Specification*, November 1994.

[114] J. Holt, R. Bradshaw, K. E. Seamons, and H. Orman. Hidden Credentials. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 2003.

[115] Ian Horrocks and Peter Patel-Schneider. A proposal for an owl rules language. http://www.cs.man.ac.uk/ horrocks/DAML/Rules/, October 2003.

[116] http://www.cio-dpi.gc.ca/pki-icp/. *Government of Canada Public Key Infrastructure.*

[117] http://www.ietf.org/html.charters/spki-charter.html. *Simple Public Key Infrastructure (SPKI).*

[118] International Telecommunication Union. *Rec. X.509 - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework*, August 1997.

[119] N. Islam, R. Anand, T. Jaeger, and J. R. Rao. A Flexible Security System for Using Internet Content. *IEEE Software*, 14(5), September 1997.

[120] C. Sierra J. Sabater. Social ReGreT, a reputation model based on social relations. *SIGecom Exchanges*, 3.1:44–56, 2002.

[121] R.D. Jarvis. Selective Disclosure of Credential Content during Trust Negotiation. Master's thesis, Dept. of Computer Science, Brigham Young University, April 2003.

[122] T. Jim. SD3: A Trust Management System With Certified Evaluation. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2001.

[123] W. Johnson, S. Mudumbai, and M. Thompson. Authorization and Attribute Certificates for Widely Distributed Access Control. In *IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, 1998.

[124] A. Josang, E. Gray, and M. Kinateder. Analysing topologies of transitive trust. In *Workshop of Formal Aspects of Security and Trust*, 2003.

[125] Audun Josang. The right type of trust for distributed systems. In *ACM New Security Paradigm Workshop*, pages 119–131, 1996.

[126] Audun Josang. An algebra for assesing trust in certifiction chains. In *Network and Distributed Systems Security Symposium 1999*, 1999.

[127] Audun Josang and Tyrone Grandison. Conditional inference in subjective logic. In *6th International Conference on Information Fusion*, 2003.

[128] M. Jovanovic. Modeling large-scale peer-to-peer networks and a case study of gnutella. Master's thesis, University of Cinicnnati, 2001.

[129] A. Juels and J. Brainard. Client Puzzle: A Cryptographic Defense Against Connection Depletion Attacks. In *Network and Distributed System Security Symposium*, San Diego, CA, February 1999.

[130] Lalana Kagal. Rei: A policy language for the me-centric project. Technical Report HPL-2002-270, Hewlett Packard Laboratories, October 04 2002.

[131] Lalana Kagal, Timothy Finin, and Anupam Joshi. A policy language for a pervasive computing environment. In *4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2003)*, Lake Como, Italy, June 2003.

[132] Lalana Kagal, Massimo Paoucci, Naveen Srinivasan, Grit Denker, Tim Finin, and Katia Sycara. Authorization and privacy for semantic web services. In *AAAI 2004 Spring Symposium on Semantic Web Services*, Stanford University, March 2004.

[133] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina. Eigenrep: Reputation management in p2p networks. pages 640–651, 2003.

[134] G. Karjoth, M. Schunter, and M. Waidner. Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. In *2nd Workshop on Privacy Enhancing Technologies*, San Francisco, CA, April 2002.

[135] G.C. Kessler. Romaing PKIs: Harbinger of Virtual VPNs? *Information Security*, February 2000.

[136] R. Khare and A. Rifkin. Weaving a Web of Trust. *World Wide Web Journal, special issue on security*, 2(3), 1997.

[137] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *http://www.cryptography.com/resources/whitepapers/TimingAttacks.pdf*, December 1995.

[138] P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*. Springer, 1999.

[139] P.C. Kocher. On Certificate Revocation and Validation. In *International Conference on Financial Cryptography*, Anguilla, British West Indies, February 1998.

[140] Vladimir Kolovski, Yarden Katz, James Hendler, Daniel Weitzner, and Tim Berners-Lee. Towards a policy-aware web. In *Semantic Web Policy Workshop in conjunction with 4th International Semantic Web Conference*, Galway, Ireland, nov 2005.

[141] H. Krawczyk and T. Rabin. Chameleon hashing and signatures.

[142] B.W. Lampson. Protection. In *5th Princeton Symposium on Information Science and Systems*, Princeton, New Jersey, March 1971.

[143] C. Landwehr. Formal Models of Computer Security. *ACM Computing Surveys*, 13(3), 1981.

[144] Jonghyun Lee. Web-based Data Migration for High-performance Scientific Codes. Master's thesis, Dept. of Computer Science, University of Illinois, August 1999.

[145] S. Lee, R. Sherwood, and B. Bhattacharjee. Cooperative Peer Groups in NICE. In *IEEE Infocom*, San Francisco, CA, April 2003.

[146] Seungjoon Lee, Rob Sherwood, and Bobby Bhattacharjee. Cooperative peer groups in nice. In *IEEE Infocomm'03*, 2003.

[147] J. Leyden. Office Workers Give Away Passwords for a Cheap Pen. In *http://www.theregister.co.uk/content/55/30324.html*, April 2003.

[148] N. Li, W. Du, and D. Boneh. Oblivious Signature-Based Envelope. In *ACM Symposium on Principles of Distributed Computing*, Boston, July 2003.

[149] N. Li, B. Grosof, and J. Feigenbaum. A Practically Implementable and Tractable Delegation Logic. In *IEEE Symposium on Security and Privacy*, Berkeley, California, May 2000.

[150] N. Li, B. N. Grosof, and J. Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. *ACM Trans. Inf. Syst. Secur.*, 6(1):128–171, 2003.

[151] N. Li, B.N. Grosof, and J. Feigenbaum. Delegation Logic: A Logic-based Approach to Distributed Authorization. *ACM Transactions on Information and System Security (TISSEC)*, 6(1), February 2003.

[152] N. Li and J.C. Mitchell. RT: A Role-based Trust-management Framework. In *DARPA Information Survivability Conference and Exposition (DISCEX)*, Washington, D.C., April 2003.

[153] N. Li, J.C. Mitchell, and W. Winsborough. Design of a Role-based Trust-management Framework. In *IEEE Symposium on Security and Privacy*, Berkeley, California, May 2002.

[154] N. Li, W. Winsborough, and J.C. Mitchell. Distributed Credential Chain Discovery in Trust Management (Extended Abstract). In *ACM Conference on Computer and Communications Security*, Philadelphia, Pennsylvania, November 2001.

[155] N. Li, W. Winsborough, and J.C. Mitchell. Beyond Proof-of-compliance: Safety and Availability Analysis in Trust Management. In *IEEE Symposium on Security and Privacy*, Berkeley, California, May 2003.

[156] N. Li, W. Winsborough, and J.C. Mitchell. Distributed Credential Chain Discovery in Trust Management. *Journal of Computer Security*, 11(1), February 2003.

[157] Ninghui Li and John C. Mitchell. Datalog with Constraints: A Foundation for Trust-management Languages. In *Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages (PADL 2003)*, pages 58–73, January 2003.

[158] John W. Lloyd. *Foundations of Logic Programming*. Springer, 2nd edition edition, 1987.

[159] A. Lysyanskaya, R. Rivest, A. Sahai, and S. Wolf. Pseudonym Systems. In *Selected Areas in Cryptography, 1999*, volume 1758 of *Lecture Notes in Computer Science*. Springer, 2000.

[160] MANBIZ IPP LLC. *Frequent Asked Questions*.

[161] S. Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, University of Stirling, 1994.

[162] S. Marti and H. Garcia-Molina. Identity crisis: Anonymity vs. reputation in P2P systems. In *Peer-to-Peer Computing 2003*, pages 134–141, 2003.

[163] P. McDaniel and A. Rubin. A Response to "Can We Eliminate Certificate Revocation Lists?". In *International Conference on Financial Cryptography*, Anguilla, British West Indies, February 2000.

[164] Deborah L. McGuinness and Paulo Pinheiro da Silva. Explaining answers from the semantic web: The inference web approach. *Journal of Web Semantics*, 1(4):397–413, 2004.

[165] Deborah L. McGuinness and Paulo Pinheiro da Silva. Trusting answers from web applications. In *New Directions in Question Answering*, pages 275–286, 2004.

[166] M. Mont, S. Pearson, and P. Bramhall. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services, 2003.

[167] S.M. More and R. Impagliazzo. Anonymous Credentials with Biometrically-Enforced Non-Transferability. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 2003.

[168] L. Mui. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD thesis, Massachusetts Institute of Technology, 2003.

[169] Wolfgang Nejdl, Daniel Olmedilla, and Marianne Winslett. Peertrust: Automated trust negotiation for peers on the semantic web. In *VLDB Workshop on Secure Data Management (SDM)*, volume 3178 of *Lecture Notes in Computer Science*, pages 118–132, Toronto, Canada, August 2004. Springer.

[170] Wolfgang Nejdl, Daniel Olmedilla, Marianne Winslett, and Charles C. Zhang. Ontology-based policy specification and management. In *2nd European Semantic Web Conference (ESWC)*, volume 3532 of *Lecture Notes in Computer Science*, pages 290–302, Heraklion, Crete, Greece, May 2005. Springer.

[171] Matthias Nickles and Gerhard Weiss. Agent-based social assessment of shared resources. In *Second International Workshop on Agents and Peer-to-Peer Computing(AP2PC 2003)*, 2003.

[172] Oasis extensible access control markup language (xacml). `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml`.

[173] Daniel Olmedilla, Rubén Lara, Axel Polleres, and Holger Lausen. Trust negotiation for semantic web services. In *1st International Workshop on Semantic Web Services and Web Process Composition (SWSWPC)*, volume 3387 of *Lecture Notes in Computer Science*, pages 81–95, San Diego, CA, USA, July 2004. Springer.

[174] L. Page, S. Brin, R. Motwani, and T. Winograd. The pagerank citation ranking: Bringing order to the web. Technical report, Stanford University, 1998.

[175] C. Papadimitriou and K. Steiglitz. *Combinatorial Optimization: Algorithms and Complexity*. Prentice-Hall Inc., 1982.

[176] D. Pearce and G. Wagner. Reasoning with negative information I – strong negation in logic programs. In M. Kusch L. Haaparanta and I. Niiniluoto, editors, *Language, Knowledge and Intentionality*. Acta Philosophica Fennica 49, 1990.

[177] P. Persiano and I. Visconti. User privacy issues regarding certificates and the tls protocol. In *Conference on Computer and Communications Security*, Athens, November 2000.

[178] Asad Amir Pirzada and Chris McDonald. Establishing trust in pure ad-hoc networks. In *Proceedings of the 27th conference on Australasian computer science*, pages 47–54. Australian Computer Society, Inc., 2004.

[179] Ian Pratt-Hartmann. Fragments of language. *Journal of Logic, Language and Information*, (13):207–223, 2004.

[180] E. Rescorla. HTTP Over TLS. In *http://www.ietf.org/proceedings/99jul/I-D/draft-ietf-tls-https-02.txt*, September 1998.

[181] E. Rescorla. *SSL and TLS, Designing and Building Secure Systems*. Addison-Wesley, 2001.

[182] Paul Resnick and James Miller. PICS: Internet access controls without censorship. *Communications of the ACM*, 39(10):87–93, October 1996.

[183] Paul Resnick and Richard Zeckhauser. Trust among strangers in internet transactions: Empirical analysis of ebays reputation system. 2000.

[184] Paul Resnick, Richard Zeckhauser, Eric Friedman, and Ko Kuwabara. Reputation systems. In *Communication of the ACM*, volume 43, pages 45–48. December 2000.

[185] C. Ribeiro and P. Guedes. Spl: An access control language for security policies with complex constraints, 1999.

[186] M. Richardson, R. Agrawal, and P. Domingos. Trust management for the semantic web. In *Second International Semantic Web Conference*, September 2003.

[187] R.L. Rivest. Can We Eliminate Certificate Revocation Lists? In *International Conference on Financial Cryptography*, Anguilla, British West Indies, February 1998.

[188] Donna Romano. *The nature of trust: clarification of its defining characteristics*. PhD thesis, Louisiana State University, 2002.

[189] Arnon Rosenthal and Marianne Winslett. Security of shared data in large systems: State of the art and research directions. In *Proceedings of the ACM SIGMOD International Conference on Management of Data, Paris, France, June 13-18, 2004*, pages 962–964. ACM, 2004.

[190] M. Rotenberg. Fair Information Practices and the Architecture of Privacy. *Stanford Technology Law Review*, 1, 2001.

[191] A. Rubin and D. Greer. A Survey of the World Wide Web Security. *IEEE Computer*, 31(9), 1998.

[192] K. Sagonas, T. Swift, and D. Warren. Xsb as an efficient deductive database engine. In *Proceedings of the 1994 ACM SIGMOD International Conference on Management of Data*, pages 442–453, Minneapolis, MN, May 1994. ACM Press.

[193] B. Schneier. *Applied Cryptography, second edition*. John Wiley and Sons. Inc., 1996.

[194] B. Schneier. *Secrets & Lies*. Wiley Computer Publishing, 2000.

[195] K. Seamons, M. Winslett, and T. Yu. Limiting the Disclosure of Access Control Policies during Automated Trust Negotiation. In *Network and Distributed System Security Symposium*, San Diego, CA, February 2001.

[196] K. Seamons, M. Winslett, T. Yu, B. Smith, E. Child, J. Jacobsen, H. Mills, and L. Yu. Requirements for Policy Languages for Trust Negotiation. In *3rd International Workshop on Policies for Distributed Systems and Networks*, Monterey, CA, June 2002.

[197] K. Seamons, M. Winslett, T. Yu, L. Yu, and R. Jarvis. Protecting Privacy during On-line Trust Negotiation. In *2nd Workshop on Privacy Enhancing Technologies*, San Francisco, CA, April 2002.

[198] Kent E. Seamons, Marianne Winslett, and Ting Yu. Limiting the disclosure of access control policies during automated trust negotiation. In *NDSS* [5].

[199] R. Shinghal. *Formal Concepts in Artificial Intelligence*. Chapman & Hall Computing, 1992.

[200] J. Sinclair, J. Tang, and P. Varman. Placement-related problems in shared disk I/O. In R. Jain, J. Werth, and J.C. Browne, editors, *Input/Output in Parallel and Distributed Computer Systems*, volume 362 of *The Kluwer International Series in Engineering and Computer Science*, chapter 12, pages 271–289. Kluwer Academic Publishers, 1996.

[201] A. Singh and L. Liu. TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems. In *Peer-to-Peer Computing 2003*, pages 142–149, 2003.

[202] Steffen Staab, Bharat K. Bhargava, Leszek Lilien, Arnon Rosenthal, Marianne Winslett, Morris Sloman, Tharam S. Dillon, Elizabeth Chang, Farookh Khadeer Hussain, Wolfgang Nejdl, Daniel Olmedilla, and Vipul Kashyap. The pudding of trust. *IEEE Intelligent Systems*, 19(5):74–88, 2004.

[203] V. S. Subrahmanian, Piero A. Bonatti, Jürgen Dix, Thomas Eiter, Sarit Kraus, Fatma Ozcan, and Robert Ross. *Heterogenous Active Agents*. MIT Press, 2000.

[204] V.S. Subrahmanian, S. Adali, A. Brink, R. Emery, J.J. Lu, A. Rajput, T.J. Rogers, R. Ross, and C. Ward. Hermes: Heterogeneous reasoning and mediator system. http://www.cs.umd.edu/projects/publications/ abstracts/hermes. html.

[205] William Swartout, Cecile Paris, and Johanna Moore. Explanations in knowledge systems: Design for explainable expert systems. *IEEE Expert: Intelligent Systems and Their Applications*, 6(3):58–64, 1991.

[206] Michael C. Tanner and Anne M. Keuneke. Explanations in knowledge systems: The roles of the task structure and domain functional models. *IEEE Expert: Intelligent Systems and Their Applications*, 6(3):50–57, 1991.

[207] Gianluca Tonti, Jeffrey M. Bradshaw, Renia Jeffers, Rebecca Montanari, Niranjan Suri, and Andrzej Uszok. Semantic web languages for policy representation and reasoning: A comparison of KAoS, rei, and ponder. In *International Semantic Web Conference*, pages 419–437, 2003.

[208] Jim Trevor and Dan Suciu. Dynamically distributed query evaluation. In *Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, Santa Barbara, CA, USA, May 2001.

[209] Andrew Twigg and Nathan Dimmock. Attack resistance of computational models. In *Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pages 275–280. IEEE, June 2003.

[210] Andrzej Uszok, Jeffrey M. Bradshaw, Renia Jeffers, Niranjan Suri, Patrick J. Hayes, Maggie R. Breedy, Larry Bunch, Matt Johnson, Shriniwas Kulkarni, and James Lott. KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. In *POLICY*, page 93, 2003.

[211] Andrzej Uszok, Jeffrey M. Bradshaw, Matt Johnson, Renia Jeffers, Austin Tate, Jeff Dalton, and Stuart Aitken. KAoS policy management for semantic web services. *IEEE Intelligent Systems*, 19(4):32–41, 2004.

[212] W3C, http://www.w3.org/TR/WD-P3P/Overview.html. *Platform for Privacy Preferences (P3P) Specification*.

[213] G. Wagner. A database needs two kinds of negation. In B. Thalheim and H.-D. Gerhardt, editors, *Proc. of the 3rd. Symp. on Mathematical Fundamentals of Database and Knowledge Base Systems*, volume 495 of *Lecture Notes in Computer Science*, pages 357–371. Springer-Verlag, 1991.

[214] X. Wang and M.K. Reiter. Defending Against Denial-of-Service Attacks with Puzzle Auctions. In *IEEE Symposium on Security and Privacy*, Berkeley, CA, May 2003.

[215] Y. Wang and J. Vassileva. Bayesian network-based trust model. 2003.

[216] Y. Wang and J. Vassileva. Trust and reputation model in peer-to-peer networks. In *Peer-to-Peer Computing 2003*, pages 150–157, 2003.

[217] Yao Wang and Julita Vassileva. Bayesian network trust model in peer-to-peer networks. In *Second International Workshop on Agents and Peer-to-Peer Computing (AP2PC 2003)*, 2003.

[218] Gerhard Weikum, Arnd Christian König, and Stefan Deßloch, editors. *Proceedings of the ACM SIGMOD International Conference on Management of Data, Paris, France, June 13-18, 2004*. ACM, 2004.

[219] D.J. Weitzner, J. Hendler, T. Berners-Lee, and D. Connolly. Creating a policy aware Web: Discretionary, rule-based access for the World Wide Web. In *Web and information security*. Idea Group Inc., to appear.

[220] M. R. Wick. Second generation expert system explanation. In J.-M. David, J.-P. Krivine, and R. Simmons, editors, *Second Generation Expert Systems*, pages 614–640. Springer Verlag, 1993.

[221] D. Wijesekera and S. Jajodia. Policy Algebras for Access Control - The Propositional Case. In *ACM Conference on Computer and Communication Security*, Philadelphia, PA, November 2001.

[222] D. Wijesekera and S. Jajodia. Policy Algebras for Access Control - The Predicate Case. In *ACM Conference on Computer and Communication Security*, Washington, DC, November 2002.

[223] W. Winsborough and N. Li. Protecting Sensitive Attributes in Automated Trust Negotiation. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, November 2002.

[224] W. Winsborough and N. Li. Towards Practical Automated Trust Negotiation. In *3rd International Workshop on Policies for Distributed Systems and Networks*, Monterey, California, June 2002.

[225] W. Winsborough, K. Seamons, and V. Jones. Negotiating Disclosure of Sensitive Credentials. In *Second Conference on Security in Communication Networks*, Amalfi, Italy, September 1999.

[226] W. Winsborough, K. Seamons, and V. Jones. Automated Trust Negotiation. In *DARPA Information Survivability Conference and Exposition*, Hilton Head Island, SC, January 2000.

[227] W. Winsborough, K. Seamons, and V. Jones. Automated Trust Negotiation. *submitted for journal publication, currently available at http://www.csc.ncsu.edu/faculty/vej/atn.ps*, April 2000.

[228] William H. Winsborough, Kent E. Seamons, and Vicki E. Jones. Automated trust negotiation. DARPA Information Survivability Conference and Exposition, IEEE Press, Jan 2000.

[229] M. Winslett, T. Yu, K.E. Seamons, A. Hess, J. Jarvis, B. Smith, and L. Yu. Negotiating Trust on the Web. *IEEE Internet Computing, special issue on trust management*, 6(6), November 2002.

[230] Marianne Winslett, Ting Yu, Kent E. Seamons, Adam Hess, Jared Jacobson, Ryan Jarvis, Bryan Smith, and Lina Yu. Negotiating trust on the web. *IEEE Internet Computing*, 6(6):30–37, 2002.

[231] W. Winslett, N. Ching, V. Jones, and I. Slepchin. Using Digital Credentials on the World-Wide Web. *Journal of Computer Security*, pages 255–267, 1997.

[232] M. Witteman. Advances in Smartcard Security. *Information Security Bulletin*, July 2002.

[233] Thomas Y. C. Woo and Simon S. Lam. Authorizations in distributed systems: A new approach. *Journal of Computer Security*, 2(2-3):107–136, 1993.

[234] L. Xiong and L. Liu. A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities. In *IEEE Conference on E-Commerce (CEC'03)*, 2003.

[235] L. Xiong and L. Liu. PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843–857, July 2004.

[236] B. Yu and M. P. Singh. An evidential model of distributed reputation management. In *AAMAS 2002*, pages 294–301, 2002.

[237] B. Yu and M. P. Singh. Detecting deception in reputation management. In *AAMAS 2003*, pages 73–80, 2003.

[238] Bin Yu and Munindar P. Singh. A social mechanism of reputation management in electronic communities. In *Proceedings of the 4th International Workshop on Cooperative Information Agents IV, The Future of Information Agents in Cyberspace*. Springer-Verlag, 2000.

[239] T. Yu, X. Ma, and M. Winslett. PRUNES: An Efficient and Complete Strategy for Automated Trust Negotiation over the Internet. In *ACM Conference on Computer and Communication Security*, Athens, Greece, November 2000.

[240] T. Yu and M. Winslett. A Unified Scheme for Resource Protection in Automated Trust Negotiation. In *IEEE Symposium on Security and Privacy*, Oakland, CA, May 2003.

[241] T. Yu and M. Winslett. Policy Migration for Sensitive Credentials in Trust Negotiation. In *ACM Workshop on Privacy in the Electronic Society*, Washington, DC, October 2003.

[242] T. Yu, M. Winslett, and K. Seamons. Interoperable Strategies in Automated Trust Negotiation. In *ACM Conference on Computer and Communication Security*, Philadelphia, PA, November 2001.

[243] T. Yu, M. Winslett, and K. Seamons. Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies in Automated Trust Negotiation. *ACM Transactions on Information and System Security*, 6(1), February 2003.

[244] Ting Yu. *Dynamic Trust Establishment in Open Systems*. PhD thesis, Department of Computer Science, University of Illinois, August 2003.

[245] Ting Yu, Marianne Winslett, and Kent E. Seamons. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. *ACM Trans. Inf. Syst. Secur.*, 6(1):1–42, 2003.

[246] C. Zhang, P.A. Bonatti, and M. Winslett. Peeraccess: A logic for distributed authorization. In *12th ACM Conference on Computer and Communication Security (CCS 2005)*, Alexandria, VA, USA, 2005. ACM.

[247] H. Zima, P. Brezany, B. Chapman, P. Mehrotra, and A. Schwald. Vienna Fortran - a language specification. Technical Report ICASE Interim Report 21, MS 132c, ICASE, 1992.

[248] P. Zimmerman. *PGP User's Guide*. MIT Press, 1994.

ESWC 2006
Budva, Montenegro

Semantic Web Policies:
Where are we and What is still Missing?

Piero A. Bonatti, Naples University
Daniel Olmedilla, L3S Research Center & Hanover University

June 11th, 2006

Outline

- **Introduction**
- Where are we?
- Deployed Application Scenarios
- What is still missing?
- Conclusions

Outline

- **Introduction**
  - **Warming up**
  - **Some history (from security/trust to knowledge/reasoning)**
  - **Requirements (expressiveness, user awareness/control)**
  - **Main challenges**
- Where are we?
- Deployed Application Scenarios
- What is still missing?
- Conclusions

Introduction
Why this tutorial?

- Many research papers on policies (also in SW)
- Many approaches (languages and frameworks)
- Little work on comparison, literature review
- Reinventing the wheel
- Can be made more general → greater impact
- Where is the user?

Introduction
About this tutorial (I)

This tutorial is intended to provide

- a basic understanding of requirements of current distributed systems
- a motivation for the use of policies
- a historical review of the field
- an analysis of state of the art

And the most important

- **why should the SW community care**
- open problems and future lines of research

Introduction
About this tutorial (II)

Policies specify the behavior of a system and may be applied to many different areas: security, conversations, business rules, quality of service, etc.

The most common application scenario is security. It covers most of the requirements from other areas.

Although many of our examples and material focus on security, it should be clear all the time that its application is not restricted only to security.

Introduction
About this tutorial (& III)

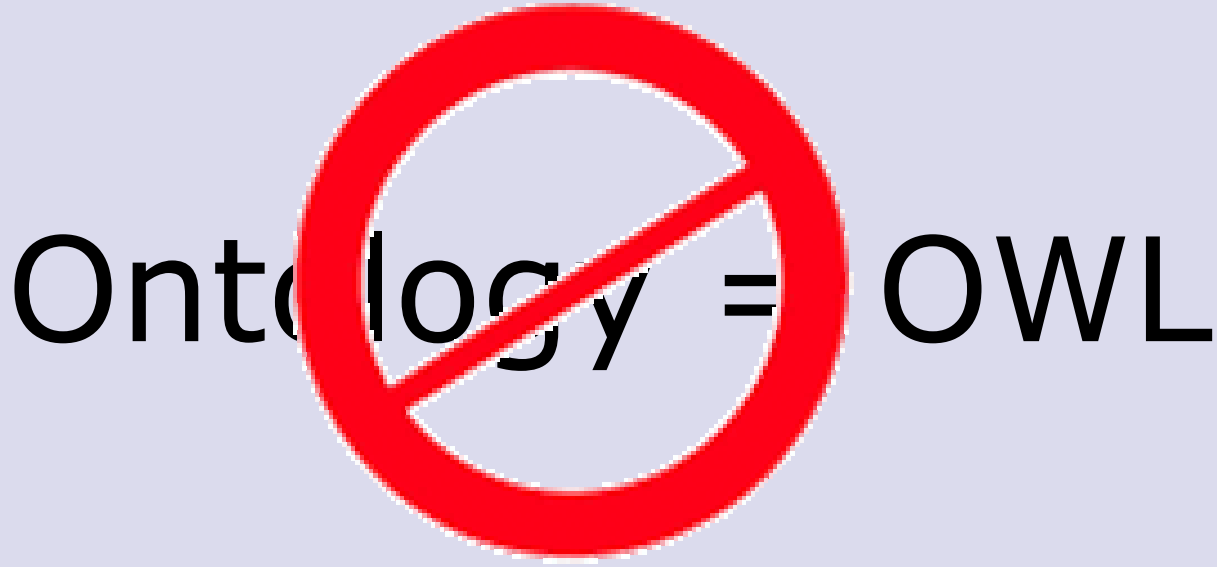
Slides are wordy so they can be easily understood offline after the tutorial

More definitions and references are available in notes and hidden slides

Tutorial is available from:

http://www.l3s.de/~olmedilla/events/2006/ESWC06/ESWC06_Tutorial.html

WARNING
Or clarification ☺



Introduction

Warming Up: Problems (I)

Institutions and companies need to control the way they

- Make business
- Take decisions
- Offer their assets
- Etc …

Generally, they need to control how decisions and actions are taken

Policies Are Everywhere

- B2B contracts
  - e.g. quantity flexible contracts, late delivery penalties, etc.
- Negotiation
  - e.g. rules associated with auction mechanisms
- Security
  - e.g. access control policies
- Privacy
  - Information Collection Policies (aka " P3P Privacy Policies")
  - Obfuscation Policies
- Workflow management
  - What to do under different sets of conditions
- Context aware computing
  - What service to invoke to access a particular contextual attribute
  - Context-sensitive preferences

[by *Norman Sadeh*, Semantic Web Policy Workshop panel, ISWC 2005]

Introduction

Warming Up: Problems (II)

In the Analog Era, everything is in paper via regulations and written policies/statements but

- They are ambiguous
- Someone has to read them and remember them
- They often change
- Etc…

Introduction
Warming Up: Problems (& III)

In the Digital Era, systems guide many of the decisions and actions to be taken but

- Policies are typically hard-coded
- Policies still change really often
  - Costly process
- Difficult to write policies in a machine-understandable way
  - E.g., try to write a regulation or law in a non-ambiguous way
- Etc …

Introduction
Warming Up: Challenges

Provide a framework where

- Behavior is flexible
  - Can be changed/updated
    - without re-coding, re-compiling, re-installing, etc…
    - In a costless manner
- Can be managed by administrators/users without needing to be computer experts
- Can be understood by normal users
- Covers as many different policies as possible

From security & trust to knowledge and reasoning

From security to KR&R

The security community has already

- Stressed the importance of declarative policy languages
  - To avoid ambiguous or ill-defined policies
  - To separate policies and mechanisms
  - To enable automated policy validation
- Proposed logic-based policy languages
  - To improve readability and maintenance
  - High-level formulation, more natural for untrained user
  - To express / integrate different policies (flexibility)

[*Bonatti, Samarati.* Logics for Authorizations and Security. Logics for emerging applications of Databases, 2003]

From security to KR&R

Languages and standards are starting to be influenced

- Java 2
  - Permissions have a method *implies*
- XACML
  - Built around "*rules*"
- *P3P is a rudimentary ontology*
  - *Data classes*
  - *Purpose of use*
  - *Recipients (immediate and indirect)*
- *Syntax has a logical flavour*
- *Semantics is procedural and/or informal*

From security to KR&R

Varieties of proposed policy formalisms

- Logic programs
  - With stratified negation as failure
    - Efficient (PTIME)
    - Unambiguous (one canonical model)
  - To make decisions in the absence of explicit information
    - *Open and closed policies*
  - *To support general rules with exceptions*
    - *Hierarchies of subjects, objects, and actions*
  - *With periodic temporal expressions*
  - *With event-condition-action rules*

[*Bonatti, Samarati.* Logics for Authorizations and Security. Logics for emerging applications of Databases, 2003]

From security to KR&R

Varieties of policy formalisms II

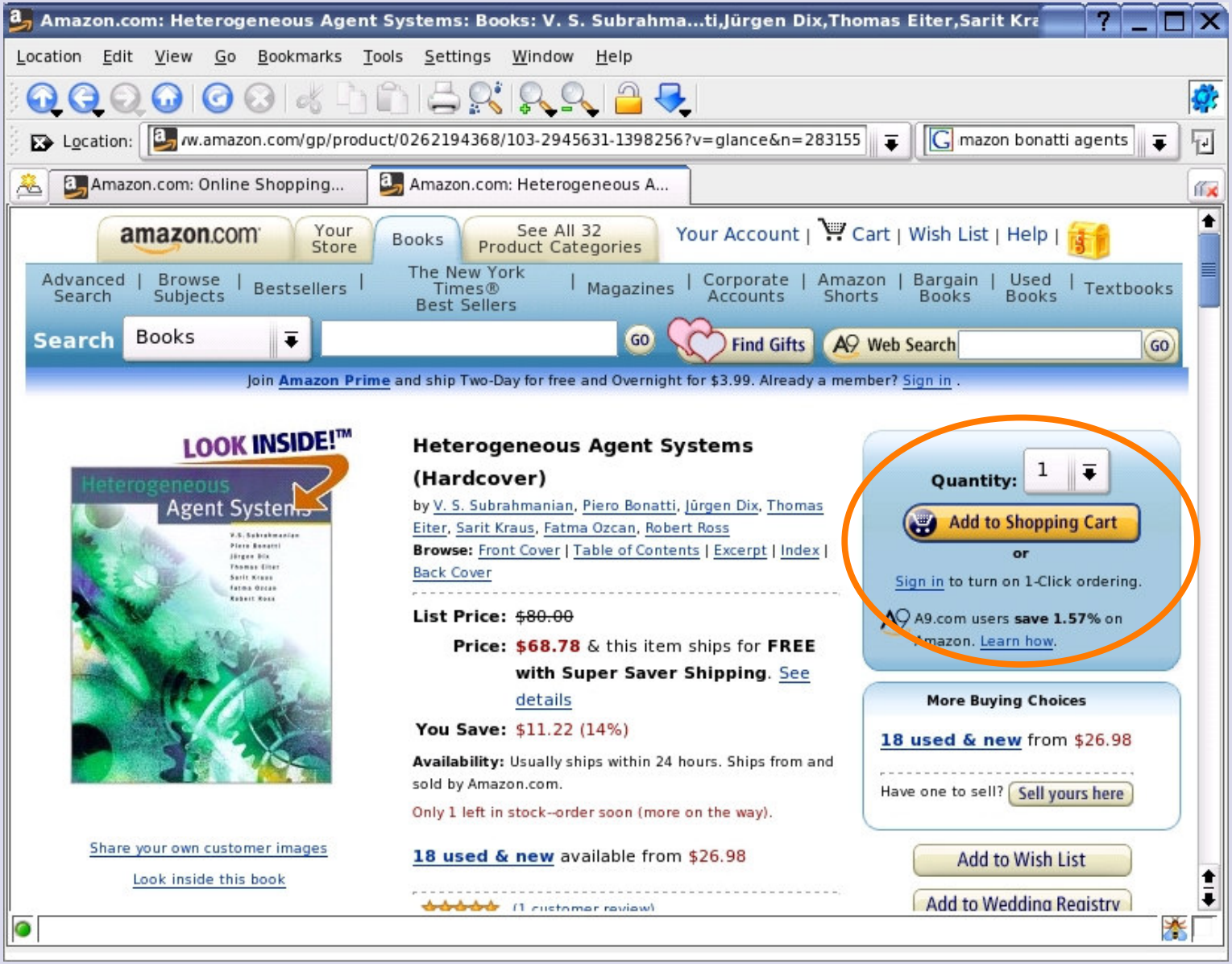
- Deontic logics
  - *Permissions, denials and obligations*
  - *Sometimes in a logic programming fragment*
  - *Is classical deontic semantics adequate?*
    - *Start from policies, not from logic*
- *Description logics*
  - *Plus rules?*
  - *Plus nonmonotonic inference?*
  - *Technical difficulties*

[REWERSE Report I2-D1. http://rewerse.net/deliverables/i2-d1.pdf, 2004 **]**

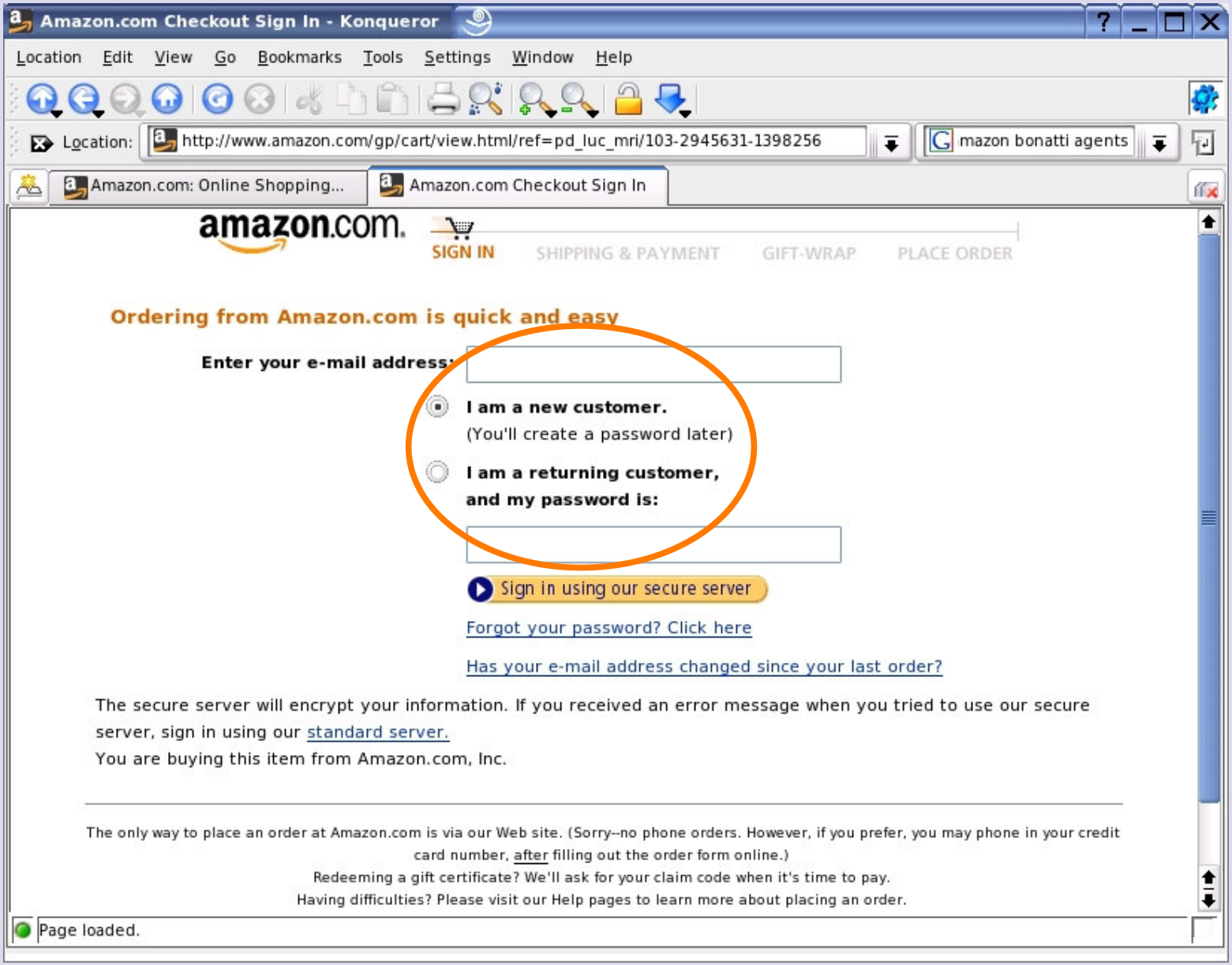
From trust management to SW

- *Computer security for open systems*
  - *Occasional users, unknown to the system*
    - *Traditional authentication is impossible or undesirable*
    - *Property-based access control*
    - *Digital credentials*
- *Privacy issues*
  - *Unknown servers*
    - *Limit disclosure of sensitive information*
    - *Raise the level of trust in the server*
- *Together security and privacy lead to negotiations*

Authentication in open systems



Authentication in open systems



Authentication in open systems

Other password-based systems

- MyProxy
- Kerberos
- Some CAS-based servers

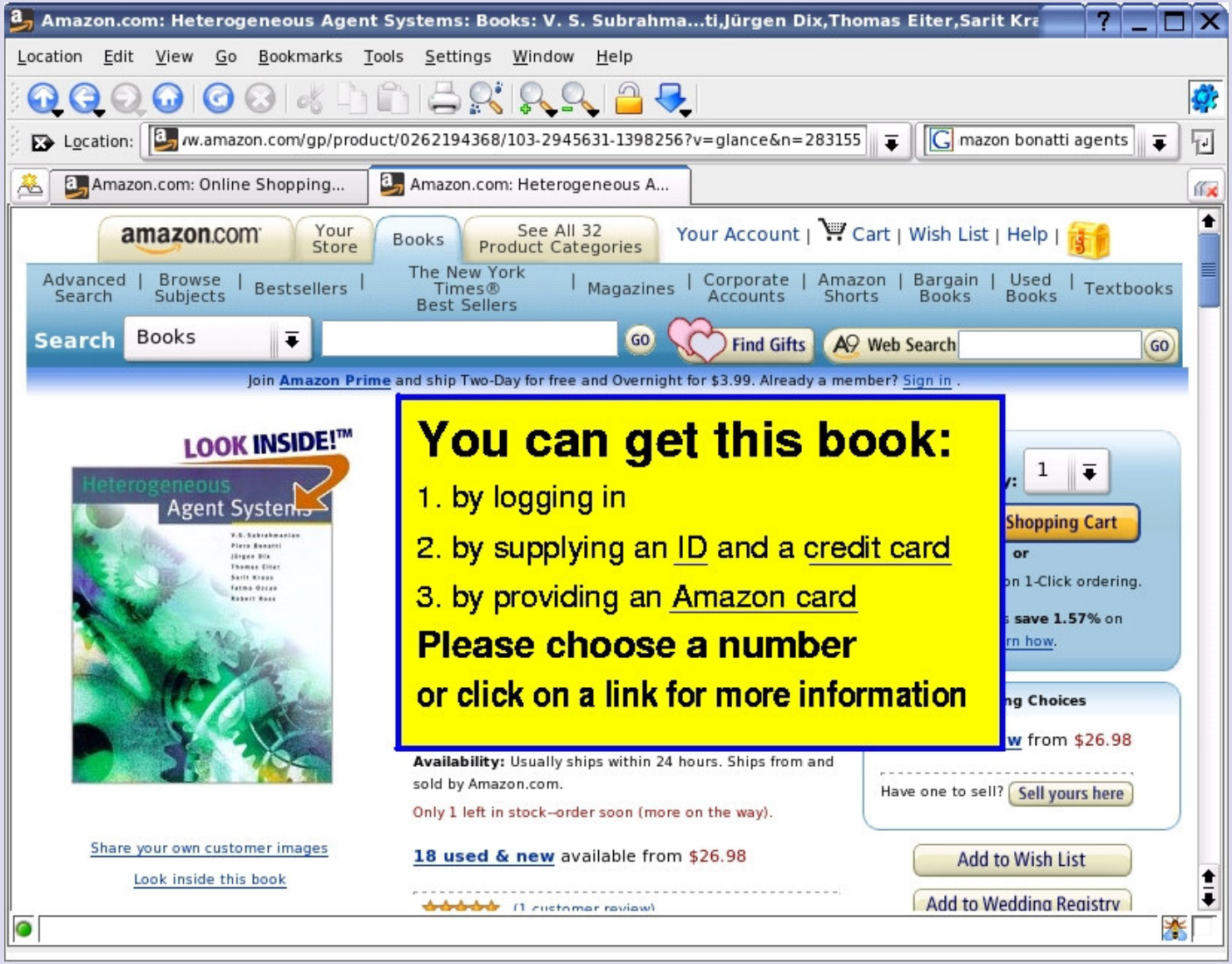
Authentication in open systems
scalability and usability issues

In the absence of more flexible methods

- Web services have to keep accounts for all customers
  - Possibly >1 for some customers
  - Some accounts are used very few times
- Users have to create accounts all the time
  - *Many* passwords vs reuse (highly vulnerable)
  - Needs automated password management
- Articulated business policies are discouraged
  - Because they would require continuous user intervention

Authentication in open systems

scalability and usability issues



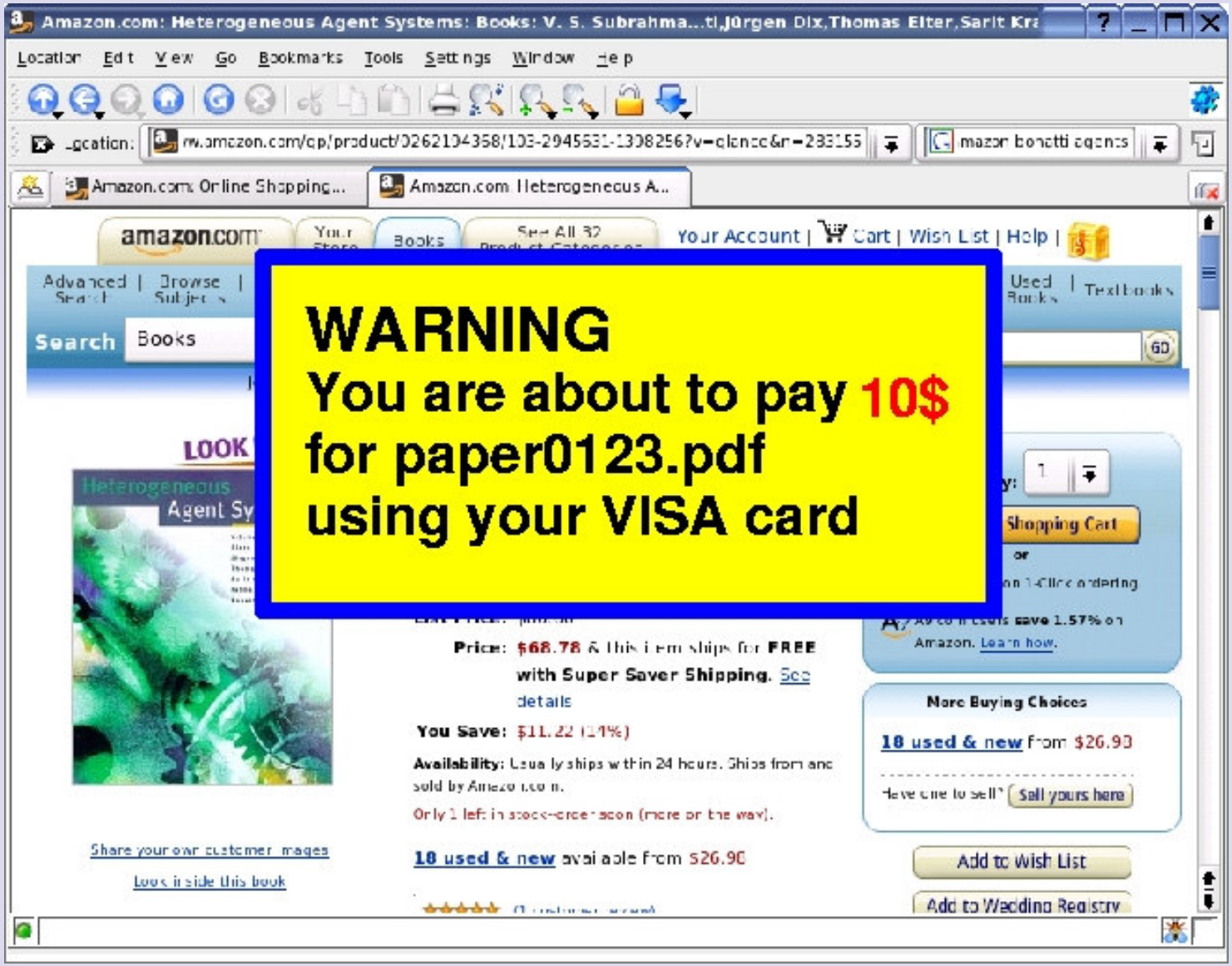
Authentication in open systems
scalability and usability issues

What one would really want:

- Suppose the *Amazon card* gives you free access to some products
- If you have it, you want to use it automatically
  - Click on the purchase button and that's it
- If you don't, you may want to see something like the next figure

Authentication in open systems

scalability and usability issues



Authentication in open systems
scalability and usability issues

Similar desiderata for ubiquitous/pervasive computing scenarios

- E.g. travellers connect to airport lounge services using
  - Frequent flier cards
  - Pre-paid cards
  - Credit cards
  - Employee credentials (government, airlines, ...)
  - ...
- In a transparent way
  - Well, as far as possible

Beyond authentication
property-based access control

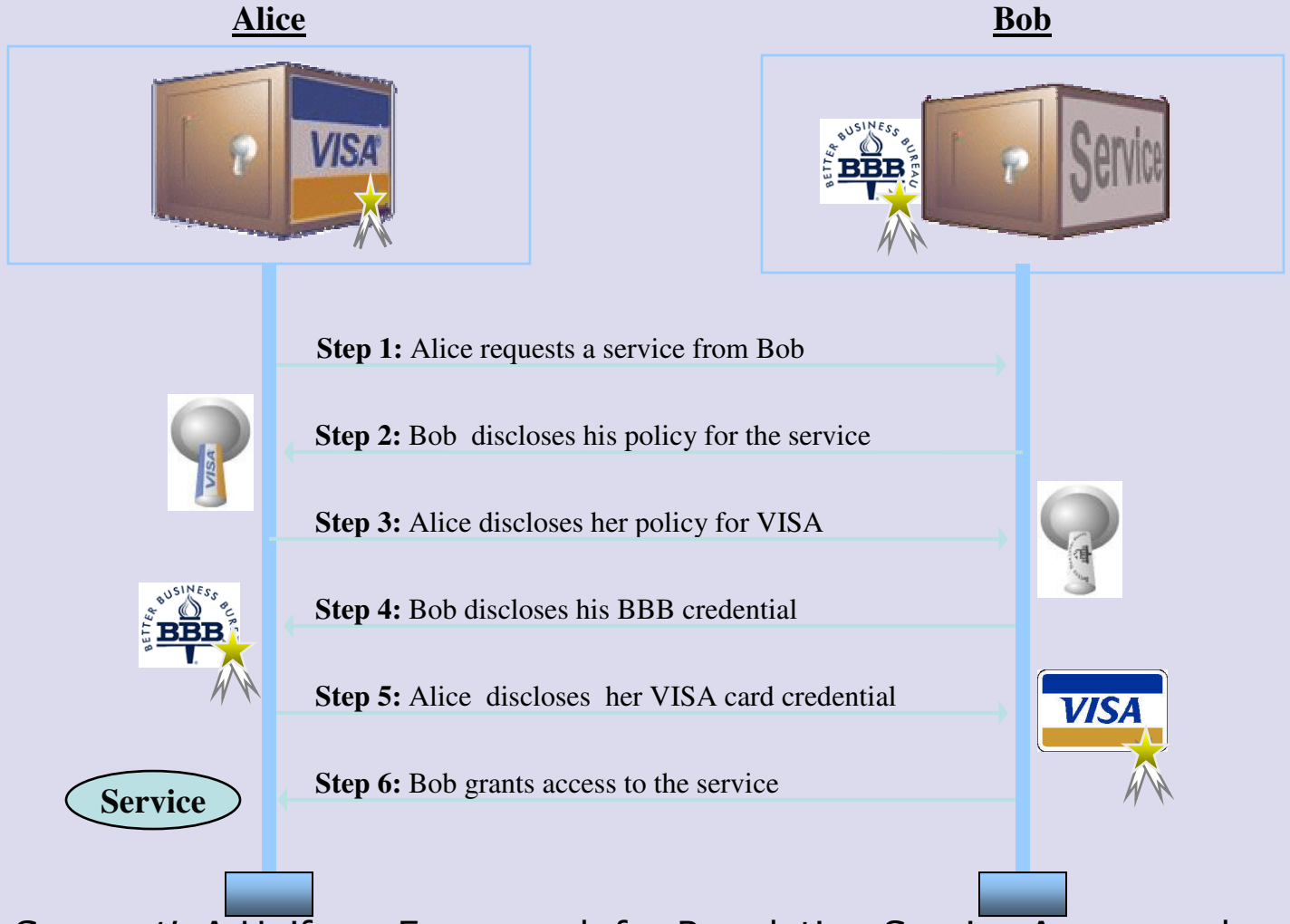
- The amazon card does not necessarily disclose the owner's identity
- Digital credentials can represent also
  - Membership to an association
  - Subscriptions
  - Eligibility to particular services
  - Citizenship, age, and other personal properties
  - Credit cards and other money-related "objects"
  - ...
- Flexible and scalable
  - Domain specific certification authorities
- Privacy preserving
  - Release only what is needed (*need-to-know principle*)

Privacy issues

- Credentials may be sensitive
  - Credit card numbers, SSN, ...
- Servers cannot be trusted, in general
  - New services, unknown responsibles, ...
- Credential release may be subject to server certifications
- Seal programs (self regulation): agree to
  - Follow precise practices for protecting information
  - Be subject to audit procedures
  - TRUSTe, BBBOnLine, WebTrust
- Seal program membership can be certified with electronic credentials

Negotiations

symmetric framework: credential are resources



[*Bonatti, Samarati.* A Uniform Framework for Regulating Service Access and Information Release on the Web. CCS 2000 and J. of Comp. Security 2002]

Expressiveness issues
how to formulate requests

One by one?

- Slow
  - More messages (as opposed to one global request)
- Bad w.r.t. privacy
  - Unnecessary disclosures
  - After submitting *n* credentials you realize you miss the next
- Example
  - After submitting your *id you realize your credit card is not accepted by the server*

Expressiveness issues
how to formulate requests

All alternatives at once?

- Less messages (good!)
- Combinatorial explosion:
  - *one id and one credit card* →
    - ***Passport + VISA***
    - ***Passport + Mastercard***
    - ***…***
    - ***Student card + VISA***
    - ***Student card + Mastercard***
    - ***…***
    - ***SSN + VISA***
    - ***SSN + Mastercard***
    - ***…***

Expressiveness issues
how to formulate requests

Send the policy!

- As a compact representation of all alternatives
  - To download paper XY.pdf do one of the following:
    1) Submit an Amazon card
    2) Submit a valid *id and an accepted credit card*
- *The client can*
  - *Verify that the whole condition can be satisfied*
  - *Choose the best option*
  - *Minimizing the sensitivity of disclosed information*

Expressiveness issues
how to formulate the policy

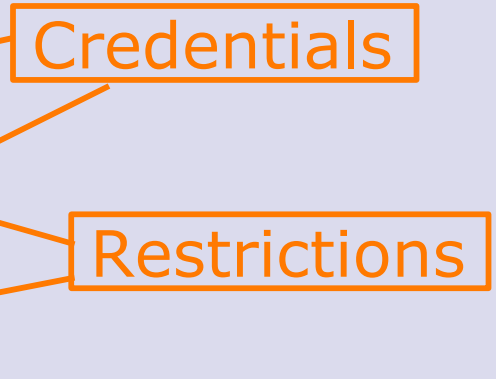
- Boolean combinations of credentials
- Restrictions on their attributes
- Possibly **recursive** conditions
  - Credential chains (~ transitive closure)
- **A rule-based example:**

allow(download(paper1.pdf)) ←
id(Document),
Document.name : User,
credit_card(Card),
Card.name : User.

Expressiveness issues
how to formulate the policy

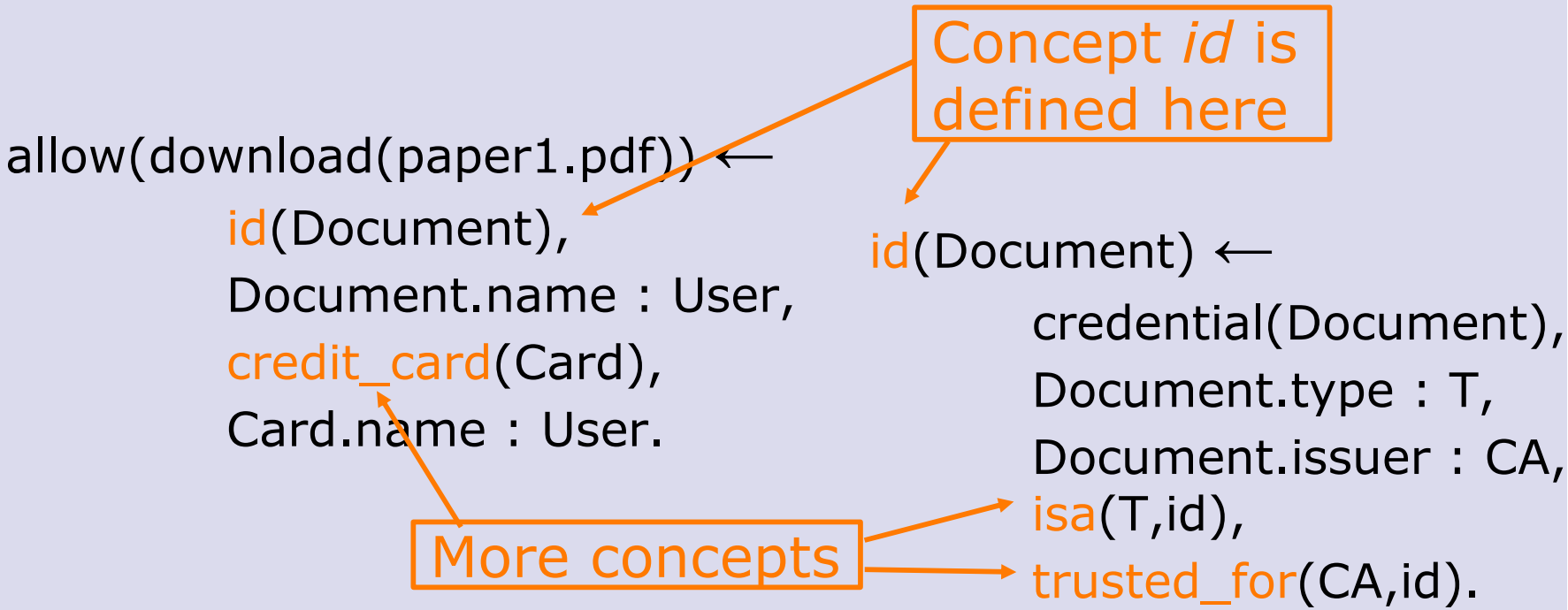
- Boolean combinations of credentials
- Restrictions on their attributes
- Possibly **recursive** conditions
  - Credential chains (~ transitive closure)
- **A rule-based example:**

```
allow(download(paper1.pdf)) ←
        id(Document),
        Document.name : User,
        credit_card(Card),
        Card.name : User.
```



Expressiveness issues
how to formulate the policy

- Policies frequently contain concept definitions



Therefore policies are

- Knowledge bases
- Containing simple ontologies
  - Often ***rule-based***
- Shared among peers (during negotiations)
- Enabling interoperability of heterogeneous peers
  - w.r.t. access control and information release
- Policies comprise both
  - Semantic **markup for decision making** and
  - The **ontology** for expressing the markup

Relevance to SW community

Regardless of whether

- Policies protect semantic data
- Policies refer to OWL ontologies

Minimal prerequisites for application: common understanding of

- Logic semantics
- Credential format (X.509 standard)
- No further semantic infrastructure needed
- Lightweight reasoning if Rule-based

Very close to short-term applications

Expressiveness requirements

A broader notion of Policy

The term *policy covers:*

- Security/Privacy policies, Trust management
- Business rules
- Quality of Service directives
- *Service-level agreements*
  - *and more...*

They all make decisions based on similar pieces of information (evidence)

- user age,
- nationality,
- customer profile,
- identity,
- reputation...

Examples of policies
across business rules and quality of service

- Give customers younger than 26 a 20% discount on international tickets
- Up to 15% of network bandwidth can reserved by paying with an accepted credit card
- Customers can rent a car if they are 18 or older, and exhibit a driving license and a valid credit card

Context-Sensitive Privacy & Security Policies

Pervasive Computing

- *"My colleagues can only see the building I am in and only when they are on company premises"*

Enterprise Collaboration

- *"Only disclose inventory levels to customers with past due shipments"*

DoD Scenarios (e.g. coalition forces)

- *"Only disclose ship departure time after the ship has left"*
- *"Only disclose information specific to the context of ongoing joint operations"*

Homeland Security & Privacy (e.g. video surveillance)

- *"Only allow for facial recognition when a crime scene is suspected"*

[by *Norman Sadeh*, Semantic Web Policy Workshop panel, ISWC 2005]

Policies are not (only) passive objects

Policies may specify

- Event logging
  - *Failed transactions must be logged*
  - *Log downloads of new articles for one week*
- Communications and notifications
  - *Notify the administrator about repeated login failures*
- Workflow triggering
  - such as (partly) manual registration procedures

i.e. Policies may specify actions

- To be interleaved with the decision process

Strong, Soft, and Lightweight Evidence

How can individuals *prove their eligibility?*

- *Strong evidence*
  - *e.g.* ***digital credentials*** ***(id, credit cards, subscriptions)***
- *Soft evidence*
  - *e.g.* ***numerical reputation measures***
  - ***PGP, eBay, …***
- *Lightweight evidence*
  - *e.g.* ***"accept buttons"*** ***(copyright/license agreements)***

They should be integrated for balancing:

- ***trust level***
- ***risk level***
- ***computational costs***
- ***usability (fetching credentials, personal assistants)***

E.g. micropayments vs. buying plane tickets

Exploiting "external" systems
or: policies are not islands

Decisions need data, information, and knowledge

- *Each organization has its own*
  - *Already available through **legacy software and data***
  - *A realistic solution must interoperate with them*
  - *Possible approaches: see **logic-based mediators***
- ***Third parties***
  - *Credit card sites for validity checking*
  - *Credential repositories*
- *Variety of web resources*

User awareness and control

Widespread security

Most security/privacy violations caused by

- Lack of awareness
  - Users ignore security threats and vulnerabilities
  - Users ignore the policies applied by the systems they use
- Lack of control
  - Users don't know how to personalize their policies
- A social problem
  - Everybody's machine is on the internet
  - Millions of computers can be exploited for attacks
  - *By taking advantage of the users' lack of technical competence*

Widespread security

A recent experiment:

- Several computers connected to the network
  - Different platforms and configurations
- With default policies: intrusion in **<5 min.**
  - **Bias towards functionality**
- **With personalized policies: safe for 2 weeks**
  - **Till the end of the experiment**

[Avantgarde. http://www.avantgarde.com/xxxxttln.pdf]

Widespread security

One size does not fit all

- **Strong security policies may cause denial of service**
  - **e.g. try to forbid script execution**
  - **which is one of the most exploited vulnerabilities**

Common users are not able to personalize their policies

- **Formulated obscurely**
  - **Are *cookies good or bad?***
- **Partly cast into program code**

Cooperative policy enforcement
for occasional users

Crucial for the success of a web service

- Never say (only) "*no*"!
- Encourage first-time users
- Who don't know how to use your service

You can't open this door, but you can ask Alice for permission

- Explain policy decisions
  - Especially failures
  - Advanced queries: Why not
- Guide users in acquiring missing permissions
  - Activate registration workflows
  - Point to credential repositories
  - Advanced queries: How-to, What-if

More uses of explanations
for policy validation

Post mortem analysis

- How could X get Y?
  - Advanced queries: Why

Static analysis

- Which kind of users can access resource X?
- Which are the permissions of a user with properties XYZ?
  - Advanced queries: How-to, What-if

Denial of service analysis

- Why didn't X get Y?
  - Advanced queries: Why-not

Policies as KBs

One knowledge many uses, e.g.

- Access control
- Communicating requirements
- Explanations
- Validation
- Service selection
  - Use policies as semantic markup
  - Expressing non-functional properties

Different reasoning tasks

- Deduction
- Abduction
- Proof manipulations ...


REWERSE©
reasoning on the web
Main Challenges
REWERSE©
WG I2 - policy language

Many Policies, One Framework

It is appealing to integrate all policies in one framework

- One common infrastructure
  - for **interoperability** and **decision making**
- Where policies can be harmonized & coordinated

Technical challenge

- **Harmonize/integrate requirements**
  - procedural (ECA) vs. declarative semantics
  - different derivation strategies
  - too complex for one representation language?

Strong, Soft, and Lightweight Evidence

Challenges

- Proper language (discrete + numerical), but
- *Reputation models still in early stage*
  - *new models keep being introduced*
  - *vulnerabilities (e.g., to coalitions)*
  - ***parametric frameworks?*** *(current choice of REWERSE)*
    - *separate reputation module*
    - *integrated via generic constructs (cf. rule-based mediators)*

Interoperability on a larger scale

Challenges

- *Different levels of interoperability*
  - *heterogeneous legacy software and third parties*
  - *more general credential formats*
  - *lightweight evidence can be based on any web contents*
  - *how to explain such requirements in a machine-understandable way?*
  - ***a standard semantic web issue – ontologies***
  - ***still lightweight?...***

Expressive languages, ontology infrastructure

E.g. point to a picture on the conference page to prove you attended ESWC'06
[J. Hendler]

User awareness and control
general challenges

- Explain policies and system decisions
  - Make rules & reasoning intelligible to the common user
  - A classical AI problem – perfectly in line with SW
- *Encourage people to personalize their policies*
  - Make it easy for users to write their own rules
- Use natural language?
  - "*Academic users can download the files in folder historical_data whenever their creation date precedes 1942*"
  - Suitably restricted to avoid ambiguities
  - Fortunately, users spontaneously formulate *rules*

Explanation mechanism
specific challenges

Finding the right tradeoff between

- Quality (2nd generation explanation facilities)
  - Remove irrelevant information
  - User-friendly denotation of internal objects
  - User-oriented description of reasoning
- Framework instantiation effort
  - The framework needs to be adapted to each application domain
  - Expensive in 2nd generation EF (ad hoc KB and engine)
  - Reduce the need for specialized staff

More challenges
and more detailed

- Need technical notions
- Some will be tackled in the rest of the tutorial
- From a slightly different perspective, sometimes

Outline

- Introduction
- **Where are we?**
  - **Requirements for**
    - **Policy Languages**
    - **Policy Frameworks**
  - **Policy Language & Framework State of the Art**
- Deployed Application Scenarios
- What is still missing?
- Conclusions

Requirements for Policy Languages

Requirements for Policy Languages
Overview

- Well-defined semantics
- Declarative
- Monotonicity
- Type of Evaluation
- Use of Variables
- Operations/Combinations
- Management of Attribute Credentials
- Delegation of Authority
- After-Disclosure Control
- External functions / Execution of Actions
- Ontology support
- Rule Support
- Protection of policies
- Extensibility
- Lightweight vs. Strong Evidence
- Usability

Requirements for Policy Languages
Well-Defined Semantics

- **"No surprises"**
- If any party concludes that a policy is satisfied, any other party should conclude the same
- Meaning of policies are independent of the particular implementation
- No space for ambiguity

Requirements for Policy Languages
Declarative

- Closer to the way humans think
- Definition of the what, not the how
  - People do not write algorithms, they write norms

Requirements for Policy Languages
Monotonicity

- Disclosure of additional credentials and policies or execution of actions only results in additional privileges
  - E.g. "grant access if requester is not a student" is invalid
- Only applies to the communication between the client and server
  - Given a VISA, the server may check with a VISA server for the absence of its revocation
- Context (e.g., time, location) is outside of this monotonicity requirement
  - A request made at 16:59 may be successful and the same one be rejected at 17:01

[*Seamons, Winslett, Yu, Smith, Child, Jacobson, Mills, Yu.* Requirements for policy languages for trust negotiation. IEEE POLICY 2002]

Requirements for Policy Languages
Type of Evaluation

- Centralized
  - All information exists locally
  - E.g. Database with permissions or Access Control Lists
- Distributed Policies, Centralized Evaluation
  - Policies are distributed
  - Policies are fetched and brought to a central point
  - Reasoning is performed centralized
- Distributed Evaluation
  - Policies are distributed
  - Reasoning is distributed

Requirements for Policy Languages
Use of Variables

- Required to
  - Extend semantics ("uncle" or "sameAge" examples)
  - Join different rules
  - Generalize predicates

Example

- A valid client is such that it has a subscription and such subscription includes the requested object

  validClient(Client,Resource) ←
  hasSubscription(Client,Subscription),
  includes(Subscription,Resource)

- Previous co-authors of a resource's creator are granted access

  access(Document, Requester) ←
  isAuthor(Document.Author, AnyResource),
  isAuthor(Requester, AnyResource).

Requirements for Policy Languages
Operations / Combinations

- Operations
  - Nested policies need to be combined
  - Disjunction, conjunction, negation, xor, etc.

Example

- Access granted to

  employees

  OR

  students AND student is European citizen

  OR

  clients AND client is not blacklisted

[*Bonatti, De Capitani Di Vimercati, Samarati*. An Algebra for Composing Access Control Policies, ACM Transactions on Information and System Security, 5(1):1-35, 2002]

Requirements for Policy Languages
Management of Attribute Credentials

- Disclosed credentials need to be accessed
- Their properties may be the base for a decision

Example:

- Grant access if the credential is
  issued by "University of Hannover"
  AND
  has type "student credential"

Requirements for Policy Languages
Delegation of Authority

- Decisions are not always local
  - Policies used during evaluation may be distributed
  - Fetching and centralized evaluation may not be possible due to privacy concerns
- Required to delegate decisions to other (possibly external) entities

Example:

- Access is granted if my partner company says so
- A credit card is accepted if VISA says it is valid

Requirements for Policy Languages
After-Disclosure Control

- Parties disclose information only if the requester party is entitled to receive it
- However, once information is disclosed, control over it is lost
- So far, only voluntary is possible, not enforceable
- Needed to control information after its disclosure
  - The information I disclose to you cannot be disclosed to 3rd parties
  - You can give my e-mail only to your friends (one step forward) but no more

Requirements for Policy Languages
External functions / Execution of Actions

- Unfeasible to have a single system with all institution information (e.g. legacy systems)
  - Duplication is undesirable
- Policies may involve the execution of actions outside the policy framework
  - Log each new request
  - If the negotiation succeeds, send a notification e-mail
- It should be possible to specify properties for the action, e.g., the actor that must execute the action
  - E.g. Credential fetching

Requirements for Policy Languages
Ontology Support

- Different entities may have different definitions
- Interoperability
  - Needed to "explain" what a concept means#
  - Sometimes difficult only with rules
  - Other paradigms may need to be integrated
- Definition of concepts using Ontologies
  - E.g. type of credentials
    - Disclose a credential of type credit card. Credit cards are VISA, Master Card and AmEx

Requirements for Policy Languages
Rule Support

- People tend to write policies as rules
  - Declarative
  - Event Condition Action Rules
  - Rules are intuitive and natural way of thinking
- Policies are used as examples in the W3C Rule Interchange Format (RIF) working group

Requirements for Policy Languages
Protection of Policies

- Policies may be sensitive
  - Access allowed only to Sun or Microsoft employees
  - Medical record can be retrieved by the patient or his psychiatrist
  - Police file accessible only by his parole officer
  - My pictures only available to my friends
- In this case, policies are hidden till later stages where more information is available
- Process is not a 1-step communication anymore
- Now it is a negotiation

Requirements for Policy Languages
Extensibility

- Requirements evolve other time
- The language should be able to adapt to new requirements

- Extensible to new
  - Operators
  - Constructors
  - Definitions
  - Concepts

Requirements for Policy Languages
Lightweight vs. Strong Evidence

Policies may need to distinguish on whether information provided as been signed or not

- Lightweight
  - Forms (e.g. user and password, license acceptance)
- Strong / Signed
  - Credentials

Example

- Log in with a user/password
- Access granted if credit card is provided

Requirements for Policy Languages
Strong Evidence: Standard Certificates

- Possibility for additional information via extensions
- Type of extensions
  - Critical
    - Credential should be discarded if the extension is not understood
  - Non-Critical

Requirements for Policy Languages
Usability: Example Policy in Cassandra

loc@iss.canActivateRole(adm,NHS-Caldicott-guardian-cert(org,cg,start,end))
←
loc@iss.hasActivatedRole(adm, RA-admin()),
loc@iss.hasActivatedRole(x, NHS-health-org-cert(org, start01, end01)),
%start in [start01, end01], end in [start01, end01], start < end,
loc='RA-East', iss='RA-East'%

loc@iss.canDeactivate(adm,x,NHS-Caldicott-guardian-cert(org,cg,start,end))
←
loc@iss.hasActivatedRole(adm, RA-admin()),
%loc='RA-East', iss='RA-East'%

loc@iss.other-NHS-health-org-regs(count<y>, x, org, start, end)
←
loc@iss.hasActivatedRole(y, NHS-health-org-cert(org, start01, end01)),
%start in [start01, end01], end in [start01, end01], start<end,
x != y or start != start01 or end != end01,
loc='RA-East', iss='RA-East'%

Requirements for Policy Frameworks
Usability

"Too often, only the PhD student that designed a policy language or framework can use it effectively"

[by *Kent E. Seamons*, Semantic Web Policy Workshop panel, ISWC 2005]

Requirements for Policy Frameworks

Requirements for Policy Frameworks
Overview

- Conflict resolution / combination of policies
- Accountability / Proofs
- Implementation
- Tools / applications
- Support Explanations

Requirements for Policy Frameworks
Conflict Resolution

- Is this expressiveness needed?
  - Depending on scenarios it may not
  - Guarantee must exist that every conflict will be detected
- Given a request, different policies may apply
- Results of conflict evaluation may be conflicting
- Resolution mechanism should be provided

Example:

- A policy grants access and another denies it
- Obligation to do something but prohibited to do it

Requirements for Policy Frameworks
Accountability/Proofs

- Access control decisions may be performed in different entities than the ones holding the resources
- It should be possible to proof the result of an access control decision (e.g., negotiation) to third parties

- Proof-carrying code + credentials allow that

Requirements for Policy Frameworks
Implementation

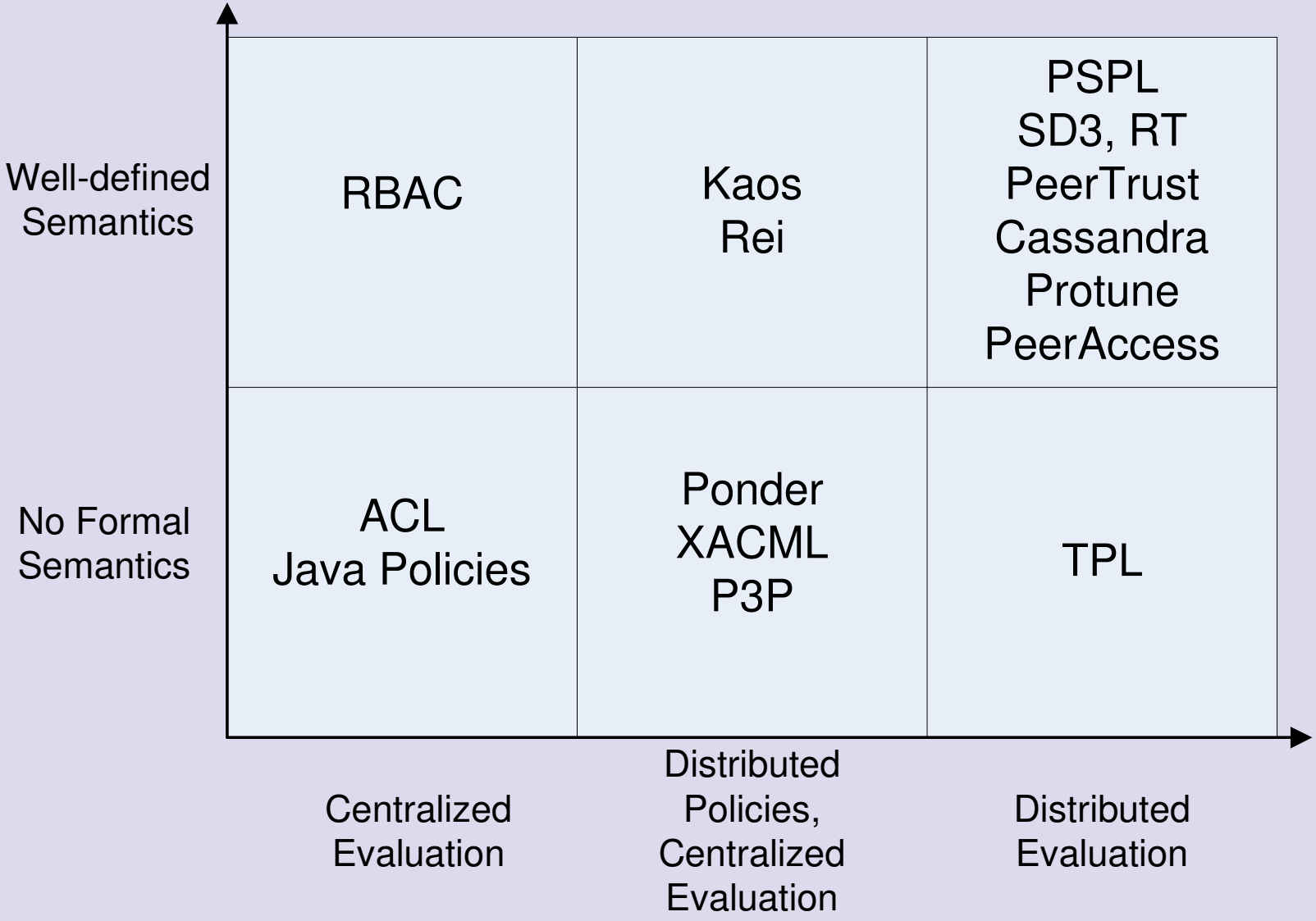
- Obvious, isn't it?
- Unfortunately, for many policy languages there is no implementation, it is only a prototype and/or is not available for general use
- If no well-defined semantics, implementations may differ
  - Space for ambiguities

Requirements for Policy Frameworks
Tools / Applications

- Templates / Profiles
- Editors
- Validation / Verification
- Explanations
- …

Policy Language/Framework State of the Art

Where are we?
Classification



XACML
Overview (I)

- <Rule>, <Policy> and <PolicySet>
  - <Rule>
    - boolean expression
    - Applicable according to <Target> & <Condition>. <Effect> only Permit or Deny
    - not accessible by PDP
  - <Policy>
    - set of <Rule> and procedure for its combination
    - Basic unit used by the PDP
    - May have obligations attached
  - <PolicySet>
    - Set of <Policy> or <PolicySet> and procedure for its combination
    - Combine separate policies into a single combined policy
- Combining algorithms
  - Deny-overrides (conjunction), Permit-overrides (disjunction), First-applicable, Only-one-applicable
  - Extensible
- Multiple subjects in different capacities (attrib. subject-category)

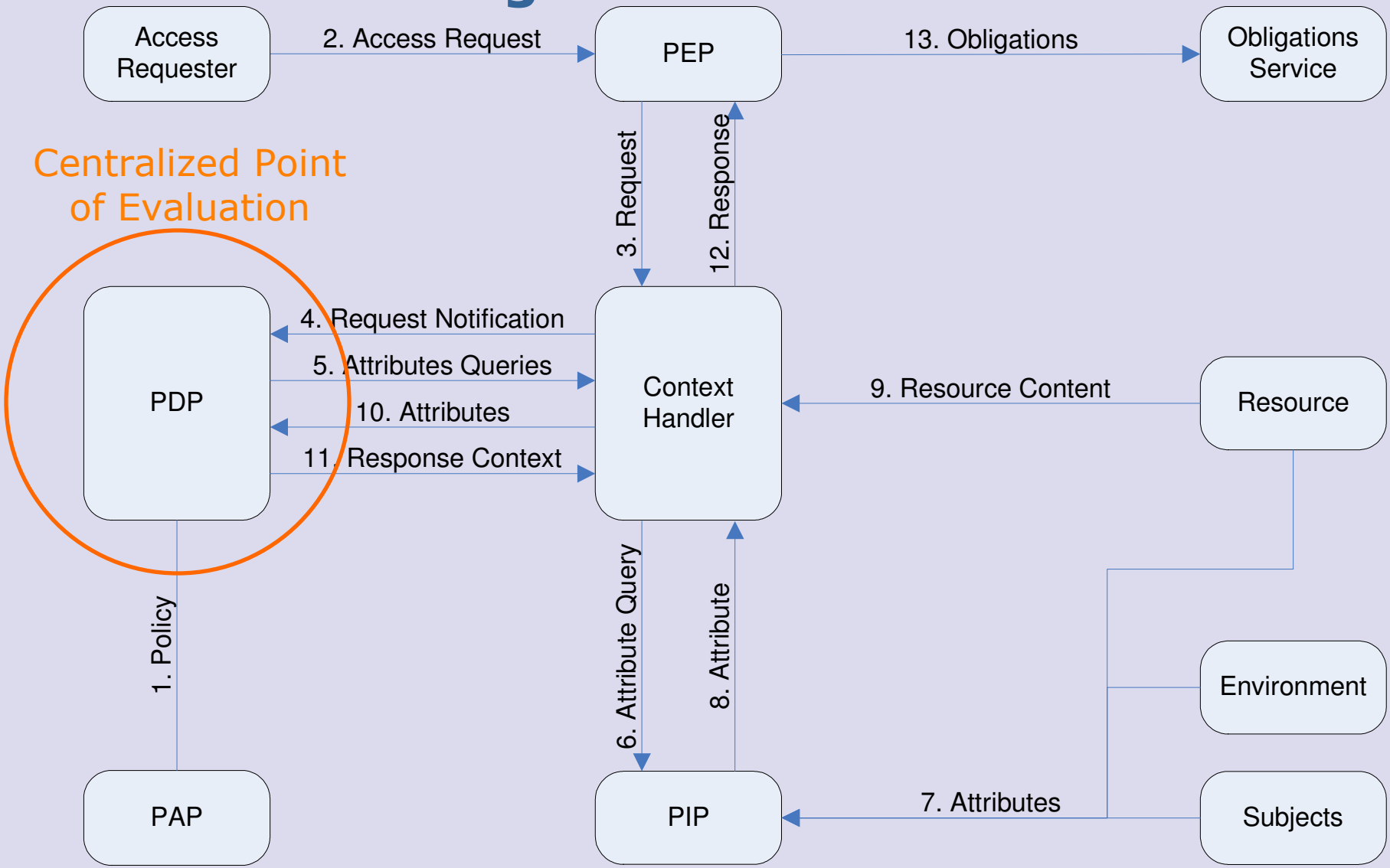
XACML
Overview (& II)

- Attributes of the subject & object
  - <SubjectAttributeDesignator> or <AttributeSelector> (in the context)
  - <ResourceAttributeDesignator> or <AttributeSelector> (in the context)
- Multi-valued attributes
- Content of an information resource (only if document is in XML)
  - <AttributeSelector> (in the context)
- Mathematical operators on attributes (<Apply FunctionId="">)
  - Arithmetic, set operators, boolean, equality and comparison
  - Extensible
- Abstract the location and retrieval of policies but handle distributed sets of policies
  - Check with <Target> if the policy is applicable or not
  - However, they must be retrieved to a central place for evaluation
- Rapidly identify applicable policies (using <Target>)
- Set of actions to be executed
  - In conjunction with policy evaluation <Obligations>

[OASIS eXtensible Access Control Markup Language (XACML) 2.0
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml]

XACML

Data Flow Diagram



XACML
Example

```
<Policy xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
        http://docs.oasis-open.org/xacml/access_control-xacml-2.0-policy-schema-os.xsd"
    PolicyId="urn:oasis:names:tc:example:SimplePolicy1"
    RuleCombiningAlgId="identifier:rule-combining-algorithm:deny-overrides">
    <Description>Medi Corp access control policy</Description>

<Target/>
<Rule RuleId= "urn:oasis:names:tc:xacml:2.0:example:SimpleRule1" Effect="Permit">
    <Description>Any subject with an e-mail name in the med.example.com domain can
    perform any action on any resource.</Description>
    <Target><Subjects><Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-
    match">
                <AttributeValue
    DataType="http://www.w3.org/2001/XMLSchema#string">
                med.example.com
                </AttributeValue>
        <SubjectAttributeDesignator
    AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
        DataType="urn:oasis:names:tc:xacml:1.0:data-type:rfc822Name"/>
        </SubjectMatch>
    </Subject></Subjects></Target>
</Rule>
</Policy>
```

XACML
Analysis of the Language (I)

- Well defined semantics
  - Procedural semantics, in Haskell (functional programming language)
- Declarative
  - No
- Monotonicity (respect to policies, credentials and actions)
  - There is no negation. Combination with "first-applicable" makes it too procedural
- Type of Evaluation
  - Distributed Policies, centralized evaluation
- Use of Variables
  - Implicit for Subject, Action, Resource, Environment and their attributes
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Conjunction, disjunction, first-applicable, only-one-applicable
  - Extra operators may be defined
- Management of Attribute Credentials
  - Yes, if passed in the context
- Delegation of Authority
  - No

XACML
Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - Obligations. Only deferred ones
- Ontology support
  - No
- Rule Support
  - Rules without variables. Nested rules allowed bound by Subject, Action, Resource & Environment attributes only.
  - Not possible to chain rules
- Protection of policies
  - No. Retrieval of applicable policies and centralized point of evaluation
- Extensibility
  - Yes. New algorithms for combination and operators
- Lightweight vs. Strong Evidence
  - Not explicitly
- Usability
  - Difficult with XML syntax. Relatively good for simple policies (if using tools) but difficult if they become complex

XACML
Analysis of the Framework

- Conflict resolution / combination of policies
  - Deny overrides, Permit overrides, first-applicable, only-one-applicable
- Accountability / Proof carrying code
  - No
- Implementation
  - Yes
- Tools / applications
  - Parthenon XACML Evaluation Engine, Sun's XACML Open Source, XACML.NET, UMU XACML editor, AXESCON XACML 2.0 Engine
- Support Explanations
  - No

P3P
Overview (I)

- **Platform for Privacy Preferences**
- Standard XML-format with common vocabulary
  - It is a schema, not a language
- Policies are fetched from the Website being accessed
- Support automatic analysis of privacy statements
  - According to user preferences (e.g., using APPEL)
- It does not enforce compliance

P3P
Syntax (I)

<Policy>

- Includes
  - one or more statements
  - Name and URI to the natural language policy

<Entity>

- Describes the legal entity stating the privacy practices

<Access>

- Indicates whether gathered data can be accessed after it has been collected

<Disputes>

- Describe the dispute resolution procedure in case of possible conflicts over the policy
- Enterprise is still liable according to normal law procedures

[Platform for Privacy Preferences (P3P) 1.0 http://www.w3.org/P3P]

P3P

Syntax (& II)

<Statement>

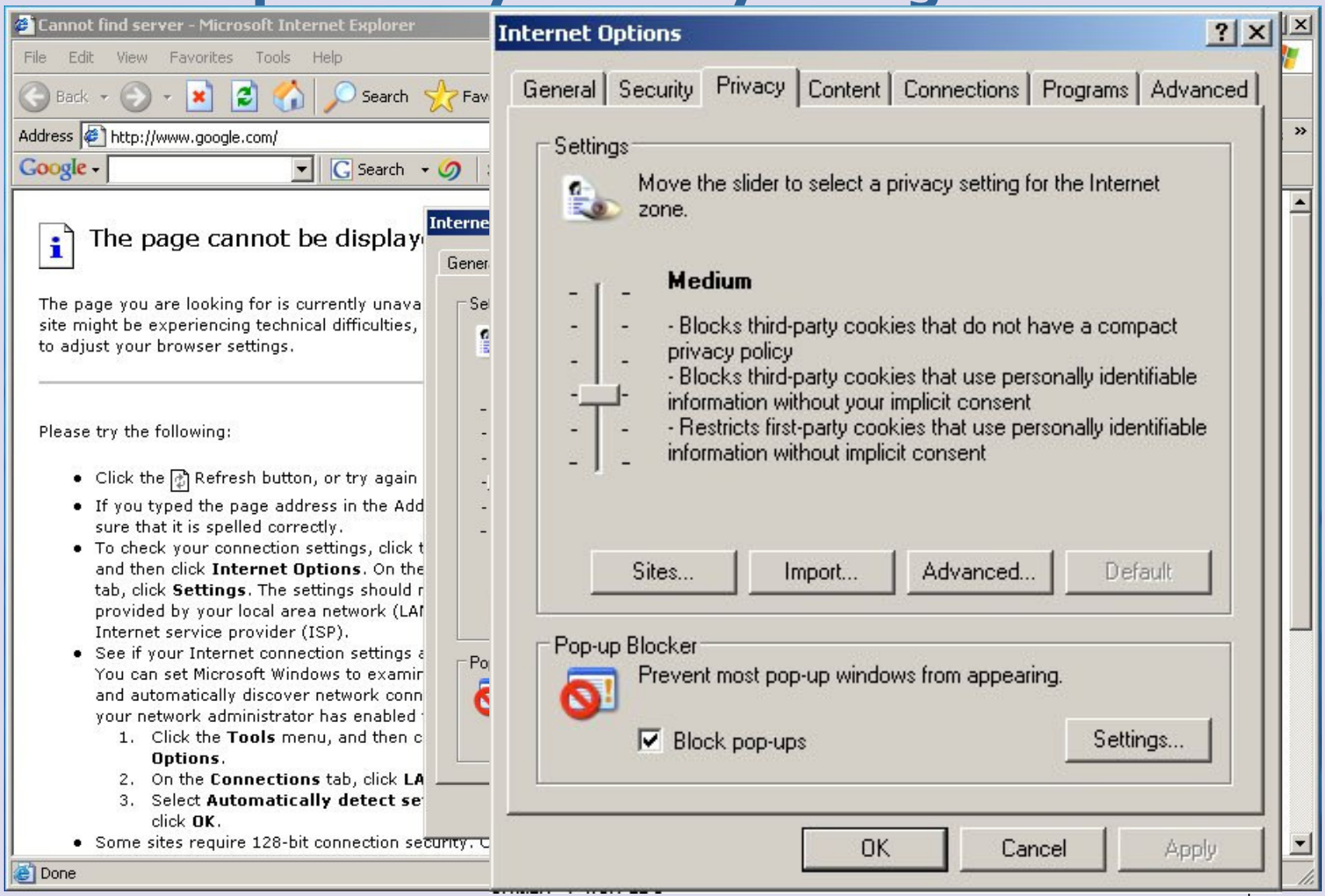
- Describe data practices applied to data collected
- <Non-Identifiable>
  - No data collected or properly anonymized
- <Purpose>
  - Purpose of the collection of data
  - E.g., <current/>,<develop/>,<telemarketing/>, etc.
- <Recipient>
  - Which entities may access the data
  - E.g., <ours>, <public>, etc.
- <Retention>
  - How long is the data going to be stored
- <Data-group>
  - Type of data the site collects
  - E.g., #user.home-info.city, #user.login.id, #user.gender, etc.
  - <Category>
    - Classification of data elements to ease user preferences
    - E.g., <financial/>, <navigation/>, <state/>, etc.

P3P
Example

```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
    <POLICY name="forBrowsers"
        discuri="http://www.catalog.example.com/PrivacyPracticeBrowsing.html" xml:lang="en">
    <ENTITY><DATA-GROUP>
        <DATA ref="#business.name">CatalogExample</DATA>
        <DATA ref="#business.contact-info.postal.street">4000 Lincoln Ave.</DATA>
        <DATA ref="#business.contact-info.postal.city">Birmingham</DATA>
        <DATA ref="#business.contact-info.postal.postalcode">48009</DATA>
        <DATA ref="#business.contact-info.postal.country">USA</DATA>
        <DATA ref="#business.contact-info.online.email">catalog@example.com</DATA>
    </DATA-GROUP></ENTITY>
    <ACCESS><nonident/></ACCESS>
    <DISPUTES-GROUP>
        <DISPUTES resolution-type="independent" service="http://www.PrivacySeal.example.org"
                short-description="PrivacySeal.example.org">
        <REMEDIES><correct/></REMEDIES>
        </DISPUTES></DISPUTES-GROUP>
    <STATEMENT>
        <PURPOSE><admin/><develop/></PURPOSE>
        <RECIPIENT><ours/></RECIPIENT>
        <RETENTION><stated-purpose/></RETENTION>
        <DATA-GROUP>
                <DATA ref="#dynamic.clickstream"/>
                <DATA ref="#dynamic.http"/>
        </DATA-GROUP>
    </STATEMENT>
</POLICY></POLICIES>
```

P3P

You are probably already using it



P3P
Analysis of the Language (I)

- Well defined semantics
  - No. Policies may even be ambiguous
  - From the spec: "In cases where the P3P vocabulary is not precise enough, sites should use the vocabulary terms that most closely match their practices and provide further explanations"
- Declarative
  - It does not apply
- Monotonicity (respect to policies, credentials and actions)
  - It does not apply
- Type of Evaluation
  - Centralized. Fetching of the applicable policy and matching against preferences
- Use of Variables
  - It does not apply
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - No. Only one policy applies for each URI
- Management of Attribute Credentials
  - No
- Delegation of Authority
  - No

P3P
Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - No
- Ontology support
  - No. Common vocabulary
- Rule Support
  - No
- Protection of policies
  - No. Policies are public
- Extensibility
  - Yes. Extension to the syntax via <Extension>
- Lightweight vs. Strong Evidence
  - It does not apply
- Usability
  - Simple schema with predefined vocabulary

P3P
Analysis of the Framework

- Conflict resolution / combination of policies
  - No
- Accountability / Proof carrying code
  - No
- Implementation
  - Yes. Integrated in Internet Explorer
- Tools / applications
  - No
- Support Explanations
  - No

Kaos
Overview

- Framework for specification, management, conflict resolution and enforcement of policies
- Uses OWL ontologies
- Policies may be
  - Positive authorization: permits execution of an action
  - Negative authorization: forbids execution of an action
  - Positive obligation: require execution of an action
  - Negative obligation: waive from execution of an action
- Policies are represented as instances of the appropriate type of policy

[*Uszok, Bradshaw, Jeffers, Suri, Hayes, Breedy, Bunch, Johnson, Kulkarni, Lott.* KAoS policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. In POLICY, page 93, 2003.]

Kaos

Example

```
<owl:Class rdf:ID="RetrieveFileAction">
    <owl:intersectionOf>
        <owl:Class rdf:about="#AccessAction"/>
        <owl:Class><owl:Restriction>
                <owl:onProperty rdf:resource="#performedBy"/>
                <owl:someValuesFrom>
                        <owl:Class>
                        <owl:oneOf rdf:parseType="Collection">
                        <owl:Thing rdf:about="#EmployeeInstitutionXYZ"/>
                        </owl:oneOf>
                        </owl:Class>
                </owl:someValuesFrom>
        </owl:Restriction></owl:Class>
    </owl:intersectionOf>
</owl:Class>

<policy:PosAuthorizationPolicy rdf:ID="PolicyRetrieveFileAction">
    <policy:controls rdf:resource="#RetrieveFileAction"/>
    <policy:hasPriority>1</policy:hasPriority>
</policy:PosAuthorizationPolicy>
```

Kaos
Reasoning

Uses DL subsumption mechanisms to reason over policies

- Check for applicable policy
  - All policies whose controlled actions can be performed by a class or instance of an actor
  - Check if an action instance is an instance of some action class controlled by existing policies
- Detect policy conflicts
  - Check if 2 subclasses of an action controlled by two selected policies are disjoint
  - Check if the subclass of an action controlled by a policy with lower priority is a subclass of the action controlled by the policy with higher priority

Kaos
Policy Conflicts

- Types
  - Positive vs. negative authorization
  - Positive vs. negative obligation
  - Positive obligation vs. negative authorization
- Static Conflict Resolution Algorithm
  - Policy Harmonization
  - Automatic
  - At design time
  - According to policy precedence conditions

KAOS
Analysis of the Language (I)

- Well defined semantics
  - Yes. Based on DL
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - It does not have negation
- Type of Evaluation
  - Policies are delivered to agents and evaluation is centralized.
- Use of Variables
  - No
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - No
- Management of Attribute Credentials
  - No
- Delegation of Authority
  - No

KAOS
Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - No
- Ontology support
  - Yes. OWL ontologies
- Rule Support
  - No
- Protection of policies
  - No
- Extensibility
  - Yes. Via ontologies
- Lightweight vs. Strong Evidence
  - No
- Usability
  - Logic language (DL). Administration tools exist

KAOS
Analysis of the Framework

- Conflict resolution / combination of policies
  - Yes. Automatic algorithm at design time
- Accountability / Proof carrying code
  - No
- Implementation
  - Yes
- Tools / applications
  - Administration tool (KPAT)
  - Enforcers to ensure compliance with policies
- Support Explanations
  - No

REI 2.0
Overview (I)

- Policies as norms of behavior
- Expressed in OWL-Lite
- Includes logic-like variables

- A policy is a list of rules and a context used to define the policy domain

- <policy:context>
  - Conditions over attributes of entities
- <policy:grants>
  - Associate deontic object with a policy

[*Lalana Kagal.* A Policy-Based Approach to Governing Autonomous Behaviour in Distributed Environments. Ph.D. Thesis. 2004]

REI 2.0
Overview (& II)

- Expresses policies according to deontic concepts
  - Permission
  - Prohibition
  - Obligation
  - Dispensation
- Uses speech acts to decentralized control
  - Delegation & revocation of permissions
  - Request & cancellation of actions

REI 2.0
Metapolicies

Defaults
- Behavior
  - Permitted by default, prohibited by default, explicit statement required
- MetaDefault: which metapolicy is invoked first
  - Check modality first or check priority first

Conflict Resolution
- Conflict of Modality
  - Right and prohibition
  - Obligation and dispensation
- Conflict of Obligation and Prohibition
- Priorities
  - A1 is given higher priority than B1 where A1 can be rule or policy
  - E.g., school policy overrides department policy)
- Precedence
  - Positive: permission and obligation override the others
  - Negative: prohibition and dispensation override the others

REI 2.0
Example

```
<policy:Policy rdf:ID="CSDeptPolicy">
    <policy:context rdf:resource="#IsMemberOfCS"/>
    <policy:grants rdf:resource="#Granting_StudentLaserPrinting"/>
    <policy:defaultBehavior rdf:resource="ExplicitPermExplicitProh"/>
    <policy:defaultModality rdf:resource="PositiveModalityPrecedence"/>
    <policy:metaDefault rdf:resource="CheckModalityPrecFirst"/>
</policy:Policy>
<constraint:SimpleConstraint rdf:ID="IsMemberOfCS">
    <constraint:subject rdf:resource="#PersonVar"/>
    <constraint:predicate rdf:resource="&univ;affiliation"/>
    <constraint:object rdf:resource="&univ;CSDept"/>
</constraint:SimpleConstraint>
<policy:Granting rdf:ID="Granting_StudentLaserPrinting">
    <policy:to rdf:resource="#PersonVar"/>
    <policy:deontic rdf:resource="#Perm_StudentPrinting"/>
    <policy:requirement rdf:resource="#IsLaserPrinterAndPhStudent"/>
</policy:Granting>
<deontic:Permission rdf:ID="Perm_StudentPrinting">
    <deontic:actor rdf:resource="#PersonVar"/>
    <deontic:action rdf:resource="#ObjVar"/>
    <deontic:constraint rdf:resource="#IsStudentAndBWPrinter"/>
</deontic:Permission>
```

REI 2.0
Analysis of the Language (I)

- Well defined semantics
  - Yes?
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - Yes. It does not model credentials or action execution
- Type of Evaluation
  - Fetching of relevant policies and centralized evaluation
- Use of Variables
  - Yes
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Conjunction, disjunction, negation as failure
- Management of Attribute Credentials
  - No
- Delegation of Authority
  - No

REI 2.0
Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - No
- Ontology support
  - Yes. OWL ontologies
- Rule Support
  - No
- Protection of policies
  - No
- Extensibility
  - Yes. Via ontologies
- Lightweight vs. Strong Evidence
  - No
- Usability
  - ?

REI 2.0
Analysis of the Framework

- Conflict resolution / combination of policies
  - Yes. Based on priorities and metapolicies
- Accountability / Proof carrying code
  - No
- Implementation
  - Yes. Using Flora and F-OWL
- Tools / applications
  - Specification editor is on-going
  - What-if analysis
- Support Explanations
  - No

RT
Overview

- Set of role based trust management languages
  - RT_0, RT_1, RT_2, RT^T, RT^D
- Combines RBAC, trust management and delegation logic

[*Li, Mitchell, Winsborough.* Design of a role-based trust-management framework. IEEE Symposium on Security and Privacy, 2002.]

RT

RT_1 credentials

- Simple member
  - $A.R \leftarrow D$
  - isMember (D, A.R)
- Simple containment
  - $A.R \leftarrow B.R_1$
  - isMember (?z, A.R) ← isMember (?z, $B.R_1$)
- Linking containment
  - $A.R \leftarrow A.R_1.R_2$
  - isMember (?z, A.R) ← isMember (?x, $B.R_1$), isMember (?z, $?x.R_2$)
- Intersection containment
  - $A.R \leftarrow B_1.R_1 \cap \ldots \cap B_k.R_k$
  - isMember (?z, A.R) ←
    isMember (?z, $B_1.R_1$), …, isMember (?z, $B_k.R_k$)

RT
Example

EPub. discount ← EPub. preferred ∩ EPub. student

EPub. preferred ← EOrg. preferred

EOrg. preferred ← IEEE. member

EPub. student ← EPub. university. stuID

EPub. university ← ABU. accredited

ABU. accredited ← StateU

StateU. stuID ← Alice

IEEE. member ← Alice

RT

Analysis of the Language (I)

- Well defined semantics
  - Yes
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - There is no negation
- Type of Evaluation
  - Distributed Policies, Centralized Evaluation
- Use of Variables
  - Implicit variables
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Intersection, union, product containment, exclusive product containment
  - Extensible
- Management of Attribute Credentials
  - Yes
- Delegation of Authority
  - Yes

RT

Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - No
- Ontology support
  - No
- Rule Support
  - Rules with implicit variables
- Protection of policies
  - No
- Extensibility
  - Yes
- Lightweight vs. Strong Evidence
  - No
- Usability
  - Logic language

RT

Analysis of the Framework

- Conflict resolution / combination of policies
  - Does not apply
- Accountability / Proof carrying code
  - No
- Implementation
  - Yes
- Tools / applications
  - Not known
- Support Explanations
  - No

PeerTrust
Overview (I)

- Based on guarded distributed logic programs
- Distributed evaluation of policies

Definite Horn Clauses of the form

$$lit_0 \leftarrow lit_1, \ldots, lit_n$$

References to other peers

- lit_i @ Issuer
- lit_i $ Requester

Signed Rules

- student(alice) @ uiuc signedBy [uiuc]

Guards: specify a partial evaluation order for the literals

- request(Course, Session) $ Requester ←
  drivingLicense(Requester) @ caState @ Requester
  | getCourse(Course, Session).

[Gavriloaie, Nejdl, Olmedilla, Seamons, Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. European Semantic Web Symposium (ESWS 2004)]

PeerTrust
Overview (& II)

- Distributed policy evaluation
  - Delegation of authority provokes evaluation on different peers
  - E.g., ask my partner if requester is a valid client
- Policy protection
  - Policies protected by policies
  - Sensitive policies are disclosed after required level of trust is established
  - Negotiations
- Signing statements
  - Explicitly represented in the policies
  - Modelling of strong evidence vs. no evidence
- Distributed proofs
  - Constructed during policy evaluation

PeerTrust
Example

validClient (User) ←
    validClient(User) **@ 'Partner Company A'**.

freeEnroll(Course, Requester) **$ Requester** ←
    policeOfficer(Requester) @ 'California State Police' @ Requester,
    rdfType(Course, 'http://.../elena#Course'),
    dcLanguage(Course, 'es'),
    creditUnits(Course, X),
    X <= 1.

policeOfficer('Alice Smith') @ 'California State Police' $ Requester ←
    member(Requester) **@ 'Better Business Bureau' @ Requester**
    | **signedBy** ['California State Police'].

PeerTrust
Analysis of the Language (I)

- Well defined semantics
  - Yes
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - There is no negation
- Type of Evaluation
  - Distributed
- Use of Variables
  - Yes
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Conjunction, Disjunction
- Management of Attribute Credentials
  - Yes
- Delegation of Authority
  - Yes

PeerTrust
Analysis of the Language (& II)

- After-Disclosure Control
  - Yes, restrictive via contexts
- External functions / execution of actions
  - No
- Ontology support
  - Import mechanism for RDF data
- Rule Support
  - Yes
- Protection of policies
  - Yes
- Extensibility
  - Yes, via libraries
- Lightweight vs. Strong Evidence
  - Yes. An extension defines '@' as lightweight evidence and '@@' as strong evidence. Also, signed rules exist
- Usability
  - Logic language

PeerTrust
Analysis of the Framework

- Conflict resolution / combination of policies
  - Does not apply
- Accountability / Proof carrying code
  - Yes
- Implementation
  - Yes. Deployable in a jar file (e.g., in an applet)
- Tools / applications
  - Protégé and RCP Editors, Integration into Web servers and Grid environments
- Support Explanations
  - No

Protune

Specification

PRovisional TrUst NEgotiation framework

- Supports general provisional-style actions
- An extendible declarative metalanguage for driving decisions
- A parameterized negotiation procedure, that gives a semantics to the metalanguage
  - Policy Filtering
- Integrity constraints for negotiation monitoring and disclosure control.
- General, ontology-based techniques for importing and exporting metapolicies and for smoothly integrating language extensions.

[*Bonatti, Olmedilla.* Driving and monitoring provisional trust negotiation with metapolicies. IEEE POLICY 2005]

Protune

Specification

Based on normal logic program $A \leftarrow L_1,\ldots,L_n$

Categories of predicates are

- Decision Predicates:
  - Allow(): queried by the negotiation for access control decisions
  - Sign(): used to issue statements signed by the principal owning the policy
- Abbreviation/Abstraction Predicates
- Constraint Predicates: comprise usual equality and disequality predicates
- State Predicates: decisions according the state
  - State Query Predicates: read the state without modifying it
  - Provisional Predicates: may be made true by means of associated actions that may modify the current state
    - E.g. credential(C,K), declaration(), logged(X,logfile_name)

[*Bonatti, Olmedilla.* Driving and Monitoring Provisional Trust Negotiation with Metapolicies. IEEE Policies for Distributed Systems and Networks (POLICY 2005)]

Protune

Metapolicies

Attribute	Domain	Range
action	provisional predicates	commands
actor	provisional predicates	self, peer
aggregation_method	cost and sensitivity attributes	max, min, sum, adopt(Predicate)
cost	provisional predicates	number
evaluation	state predicates	immediate, delayed, concurrent
expected_outcome	provisional predicates	success, failure, undefined, unknown
explanation	literals and rules	string expression
ontology	abbreviation predicates, credentials, declarations, actions	URI
predicate	literals	predicate names
selection_method	negotiator	certain_first, order(attribute_list), adopt(Predicate)
sensitivity	predicates, literals, rules	public, private, not_applicable
type	predicates, literals	abbreviation, constraint, decision, state_predicate, provisional, state_query

Protune

Examples of metapolicies

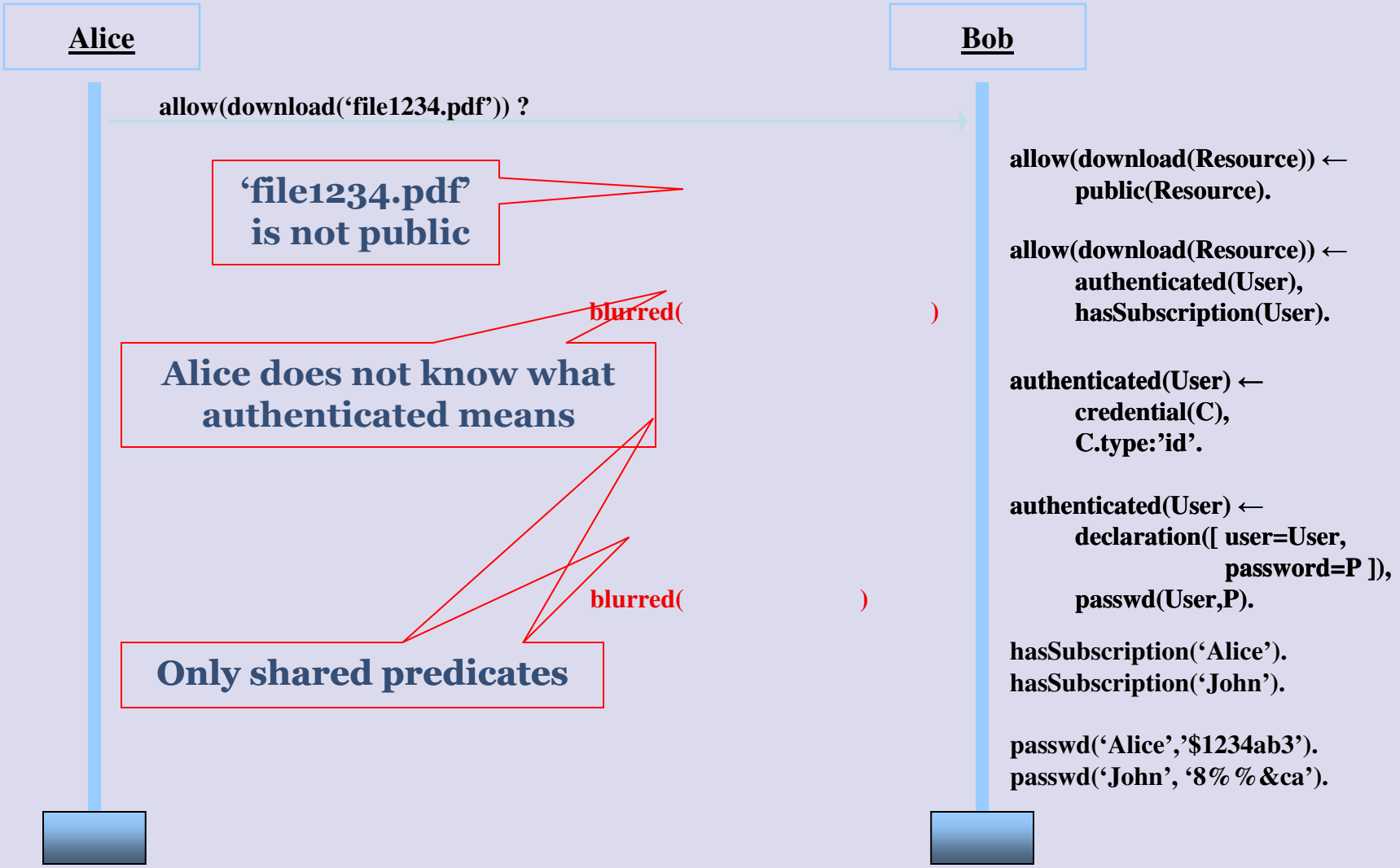
table(Key,Data).evaluation:immediate ← ground(Key).

logged(Msg,File).action:'echo'+Msg+'>'+File.

credential(_).ontology:URI.

abbrev(_).explanation:"this condition checks…"

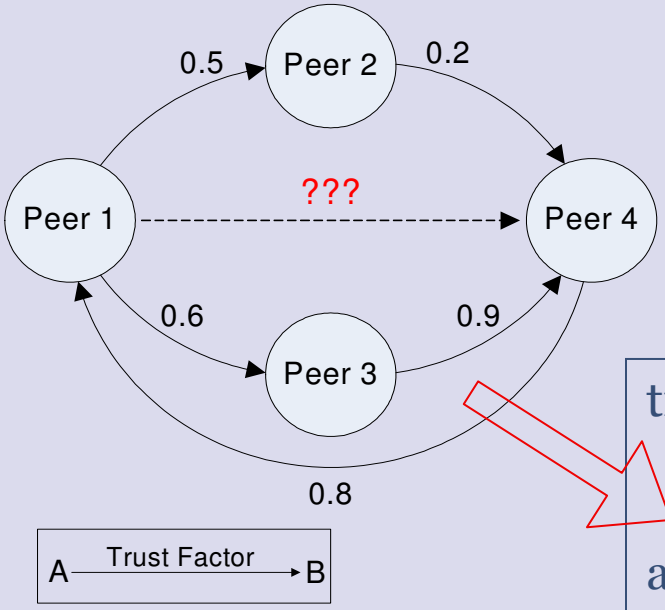
Protune
Policy Filtering Example



Deployed Application Scenarios

Combination of Policies and Trust/Reputation Algs.

Reputation-based



Policy-based

```
accessGranted(Res) ←
        credential(X,VISA),
        X.type : credit card,
        X.owner : B.

trust(A,B, download(file), 80–100) ←
        credential(X, VISA),
        X.type : credit card, X.owner : B .
allow(visaCard) ←
        credential(member(Requester),bbb),
        trust(self, Requester, buying, X), X > 0.8.
in(trust(X,Y ,A, L), reputation pckg : eval trust()))
```

[*Staab et al.,* The Pudding of Trust. IEEE Intelligent Systems Journal, Vol. 19(5), Sep./Oct. 2004]

[*Bonatti, Duma, Olmedilla, Shahmehri.* An Integration of Reputation-based and Policy-based Trust Management. Submitted for Publication]

Protune
Analysis of the Language (I)

- Well defined semantics
  - Yes
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - Yes
- Type of Evaluation
  - Distributed
- Use of Variables
  - Yes
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Conjunction, Disjunction, Negation
  - Extensible
- Management of Attribute Credentials
  - Yes
- Delegation of Authority
  - Yes

Protune

Analysis of the Language (& II)

- After-Disclosure Control
  - No
- External functions / execution of actions
  - Yes
- Ontology support
  - Yes
- Rule Support
  - Yes
- Protection of policies
  - Yes
- Extensibility
  - Yes
- Lightweight vs. Strong Evidence
  - Yes, explicit
- Usability
  - Logic language

Protune
Analysis of the Framework

- Conflict resolution / combination of policies
  - Does not apply
- Accountability / Proof carrying code
  - No
- Implementation
  - Ongoing
- Tools / applications
  - RCP Editor
  - Compatible with PeerTrust framework: integration into Web servers and Grid environments
- Support Explanations
  - Yes. Implemented

PeerAccess
Overview

Model and reason about distributed authorization in distributed systems

- Distributed reason on peers
- Control over disclosed information
- Hints specifying search space for answers

Composed of

- A modal language: base language
  - Specifies basic access control policies and related rules
- A modal meta-language
  - Determine the dynamic behavior of the system

[*Winslett, Zhang, Bonatti.* Peeraccess: a logic for distributed authorization. CCS 2005]

PeerAccess
Overview

Base policies

- A signs L ← …
  - L is directly signed by A
  - A has digitally signed L and it was received by P
- A lsigns L ← …
  - L is logically signed by A
  - P has nonrepudiable evidence that A would sign L if shown such evidence

Release policies (sticky policies)

- A signs srelease (L,S,R) ← …
  - A allows dissemination of L from S to R if L is true at S
  - Signer of a particular piece of information retains control over its future dissemination

PeerAccess
Example

Bob:

Bob lsigns auth(shaketable,X) ←
    CAS signs auth(shaketable,X)
Bob lsigns srelease(Bob signs auth(X,Y), Bob, Y)
Bob lsigns srelease(Bob signs auth(X,Y), Y, X)
Bob lsigns srelease(Bob signs auth(X,Y), Z, W) ←
    Z != Bob,
    Y lsigns condRelease(Bob signs auth(X,Y), Z, W)

Alice:

Bob signs auth(shaketable,Alice)
Bob signs srelease(Bob signs auth(X,Y),Y,X)

PeerAccess
Analysis of the Language (I)

- Well defined semantics
  - Yes
- Declarative
  - Yes
- Monotonicity (respect to policies, credentials and actions)
  - There is no negation
- Type of Evaluation
  - Distributed
- Use of Variables
  - Yes
- Operations/Combinations (conjunction, disjunction, negation, xor, etc.)
  - Conjunction, Disjunction
- Management of Attribute Credentials
  - Yes
- Delegation of Authority
  - Yes

PeerAccess
Analysis of the Language (& II)

- After-Disclosure Control
  - Yes, in cooperative environments
- External functions / execution of actions
  - No
- Ontology support
  - No
- Rule Support
  - Yes
- Protection of policies
  - Yes, through disclosure policies
- Extensibility
  - Yes, via libraries
- Lightweight vs. Strong Evidence
  - Yes.
- Usability
  - Logic language

PeerAccess
Analysis of the Framework

- Conflict resolution / combination of policies
  - Does not apply
- Accountability / Proof carrying code
  - Yes
- Implementation
  - No
- Tools / applications
  - Not known
- Support Explanations
  - No

Other Policy Languages
Not covered in the tutorial

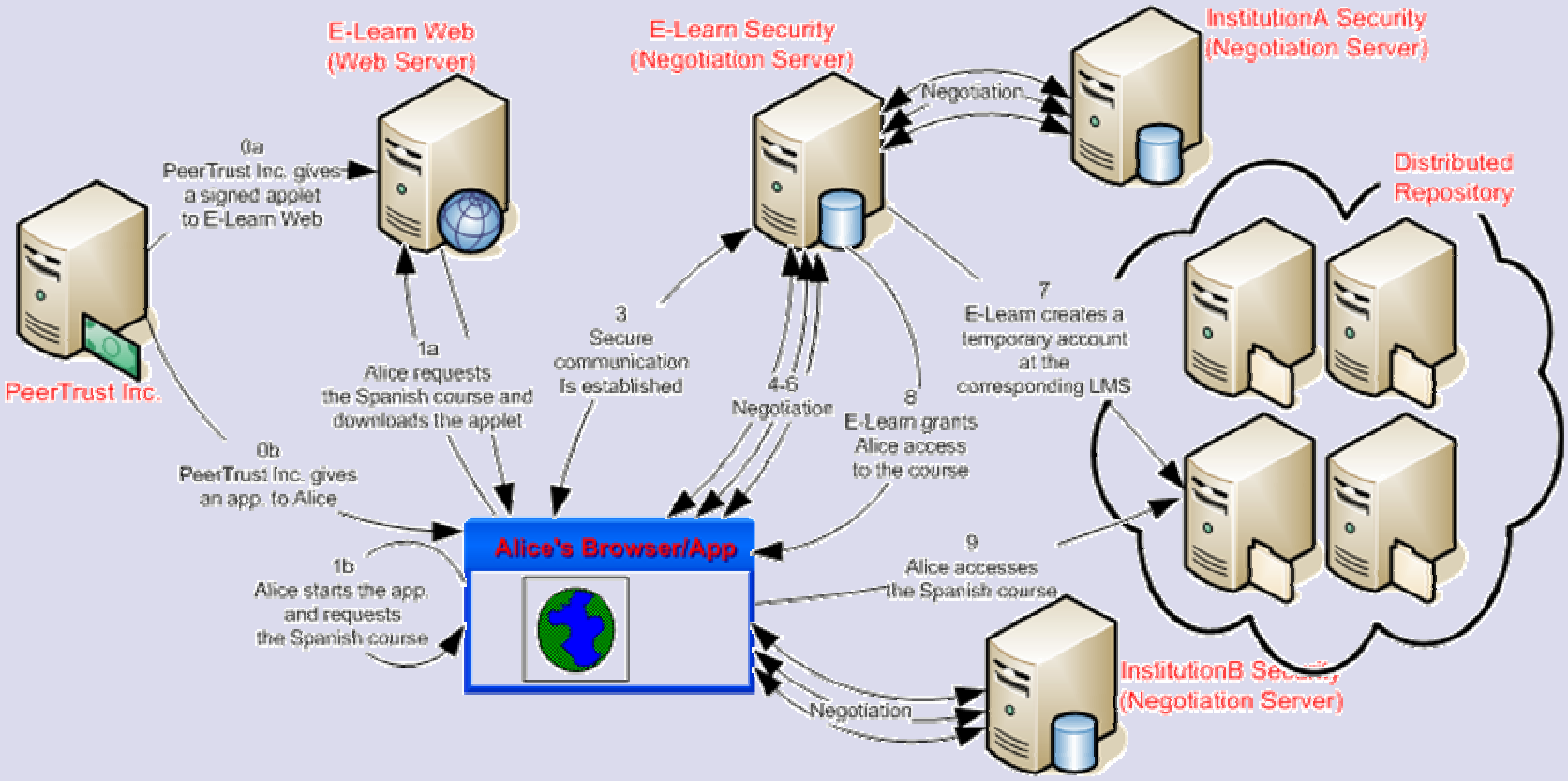
- PolicyMaker
- REFEREE
- Keynote
- Policy Description Language (PDL)
- Ponder
- Delegation Logic
- SD3
- TPL
- Cassandra
- WS-Policy
- E-P3P

Outline

- Introduction
- Where are we?
- **Deployed Application Scenarios**
  - **Application Scenarios**
    - **World Wide Web**
    - **E-Mail**
    - **Semantic Web Services**
    - **Grid**
  - **Other Implemented Features**
    - **Distributed Loop Detection**
    - **Explanations**
- What is still missing?
- Conclusions


REWERSE©
reasoning on the web
Application Scenarios
REWERSE©
WG I2 - policy language

Deployed Application Scenarios
Negotiating on the Web



[*Gavriloaie, Nejdl, Olmedilla, Seamons, Winslett.* No Registration Needed: How to Use Declarative Policies and Negotiation to Access Sensitive Resources on the Semantic Web. 1st European Semantic Web Symposium]

Deployed Application Scenarios
P3P and Policy Enforcement with REI

Improvement of user side support

- More effective preference language: REI
  - More expressive than P3P
  - Well defined semantics
  - Also enables web privacy enforcement mechanisms
- Extensible trust model
  - Based on social recommendations
  - In addition to certificate only based trust

[*Kolari, Ding, Shashidhara, Joshi, Finin, Kagal.* Enhancing Web Privacy Protection through Declarative Policies]

Deployed Application Scenarios
Policy protecting e-mail

- Scalable, attribute-based access control policy
- E-mail messages as access requests from senders
  - Requesting write access to a mailbox
- Integration into SMTP protocol
- Relays on some sort of sender's authentication

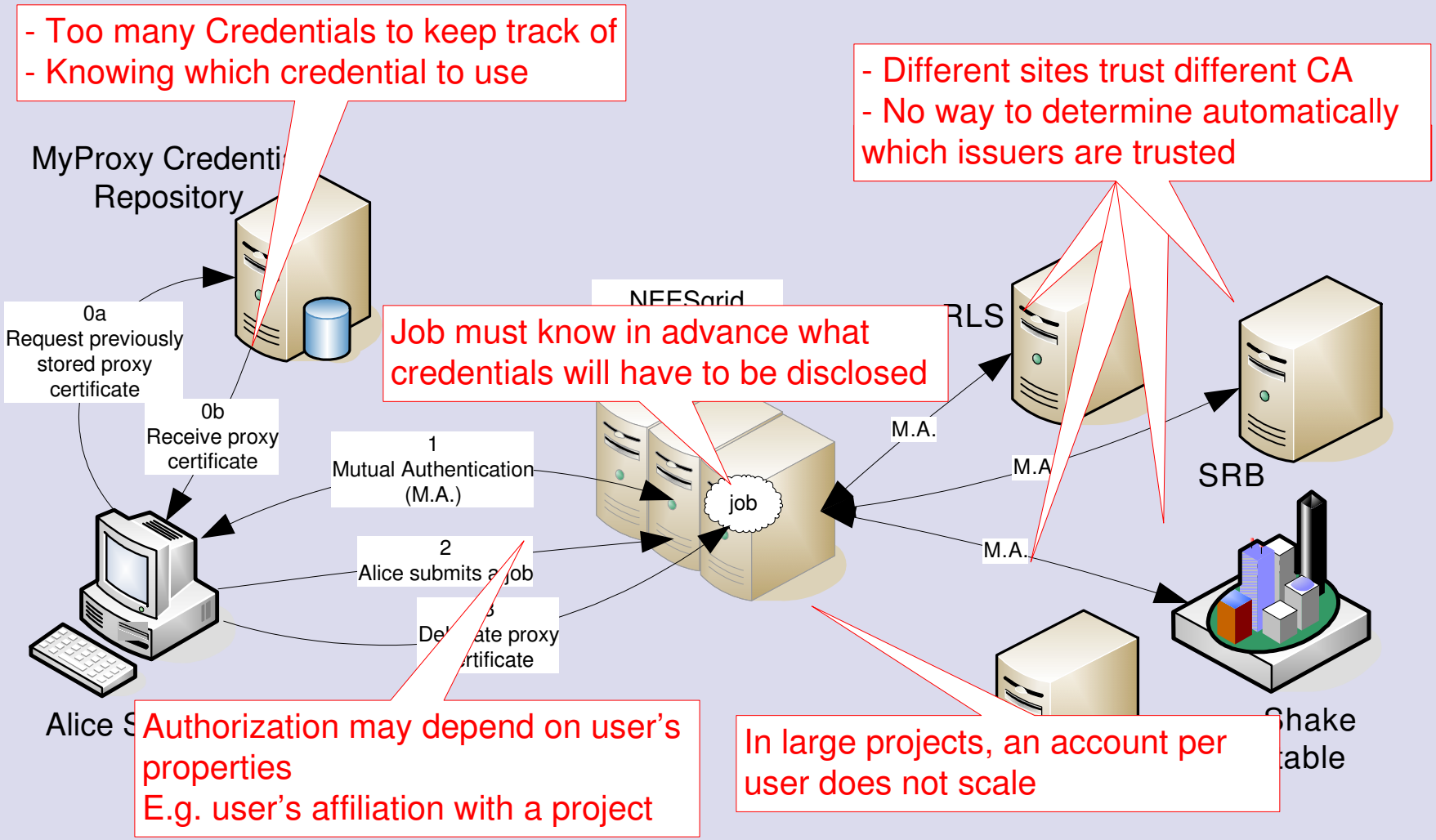
[*Kaushik, Ammann, Wijesekera, Winsborough, Ritchey.* A Policy Driven Approach to Email Services]

Deployed Application Scenarios
Policy Matchmaking for Semantic Web Services

- Proposed ontologies to model high-level security requirements and capabilities
- Policies are symmetric
  - They may constrain both client and service
- Extends OWL-S with REI policies
- Matching of client request with appropriate services
  - Using a Matchmaker, a capability-based matching engine
  - Verify compatibility of requester's policies and the provider's

[*Kagal, Finin, Paolucci, Srinivasan, Sycara, Denker.* Authorization and Privacy for Semantic Web Services. IEEE Intelligent Systems, 19(4):50–56, 2004.]

Deployed Application Scenarios
Automatic Credential Fetching on Grids (I)



[*Basney, Nejdl, Olmedilla, Welch, Winslett.* Negotiating trust on the grid. Workshop on Semantics in P2P and Grid Computing, 2004.]

Deployed Application Scenarios
Automatic Credential Fetching on Grids (II)

Both client and servers are semantically annotated with policies

Annotations

- specify constraints and capabilities
  - access control requirements
    - which certificates must be presented to gain access to it
    - who is responsible for obtaining and presenting these certificates
- are used during a negotiation
  - to reason about and to communicate the need to see certain credentials from the other party
  - to determine whether requested credentials can be obtained and revealed.

User involvement is drastically reduced in favor of automated interactions.

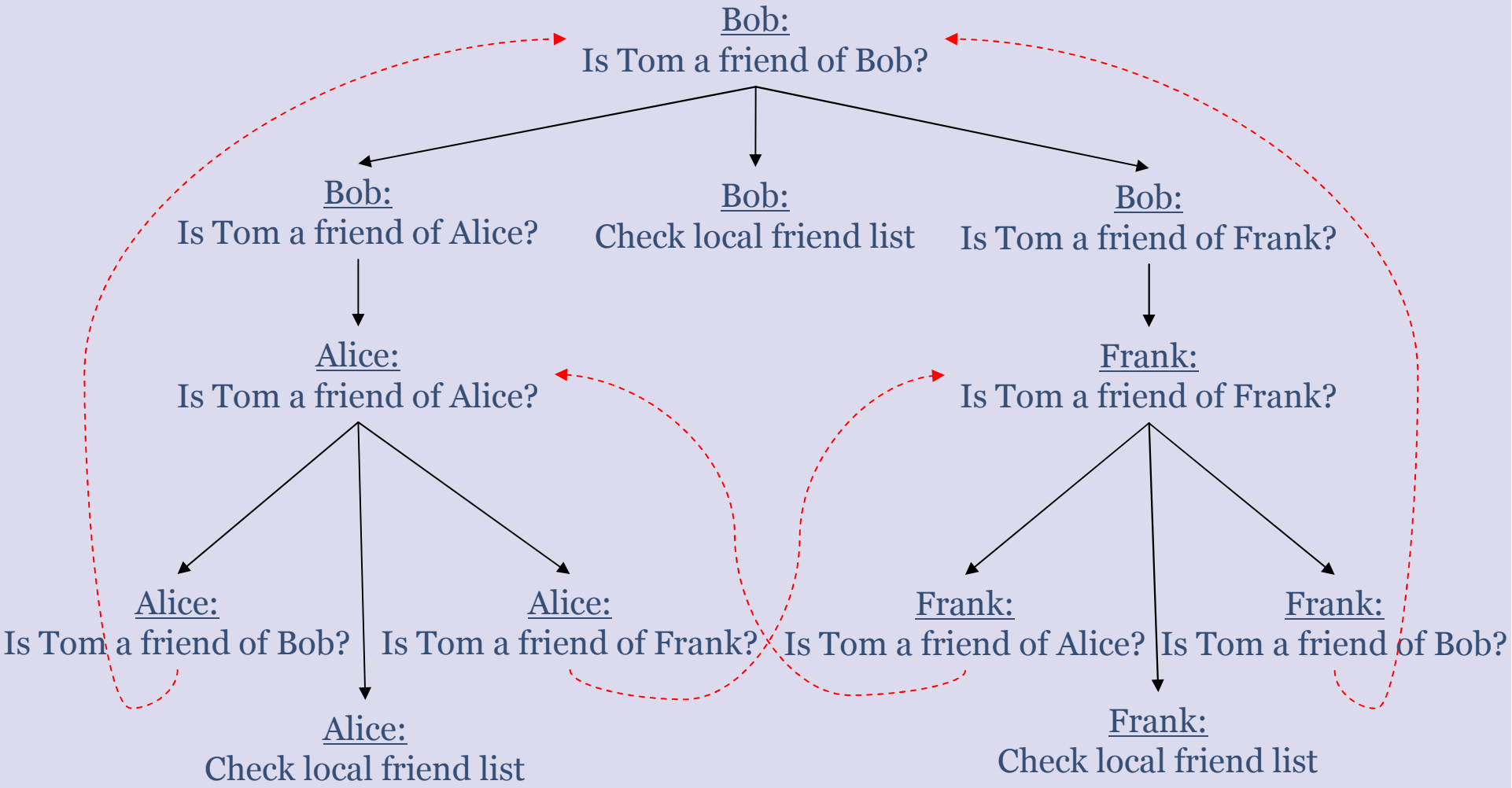
[*Constandache, Olmedilla, Siebenlist, Nejdl.* Policy-driven negotiation for authorization in the semantic grid. 2005.]

Deployed Application Scenarios
Automatic Credential Fetching on Grids (& III)

- Distributed authorization mechanisms
  - Driven by policies, not hardcoded
- Bilateral policy specification
- Access is negotiated
- Dynamic credential fetching
  - Now possible to use discovery and scheduling services to locate the best available resources
  - Otherwise, impossible to predict before hand what exact service instances would be used and which certificates required
- Capability based authorization architecture
  - Instead of identity based
- No previous trust relationships required
- Monitoring and explanation of authorization decision

Other Implemented Features

Deployed Application Scenarios
Loop Detection: Online Sharing Pictures



Deployed Application Scenarios
Loop Detection: CIA Agents

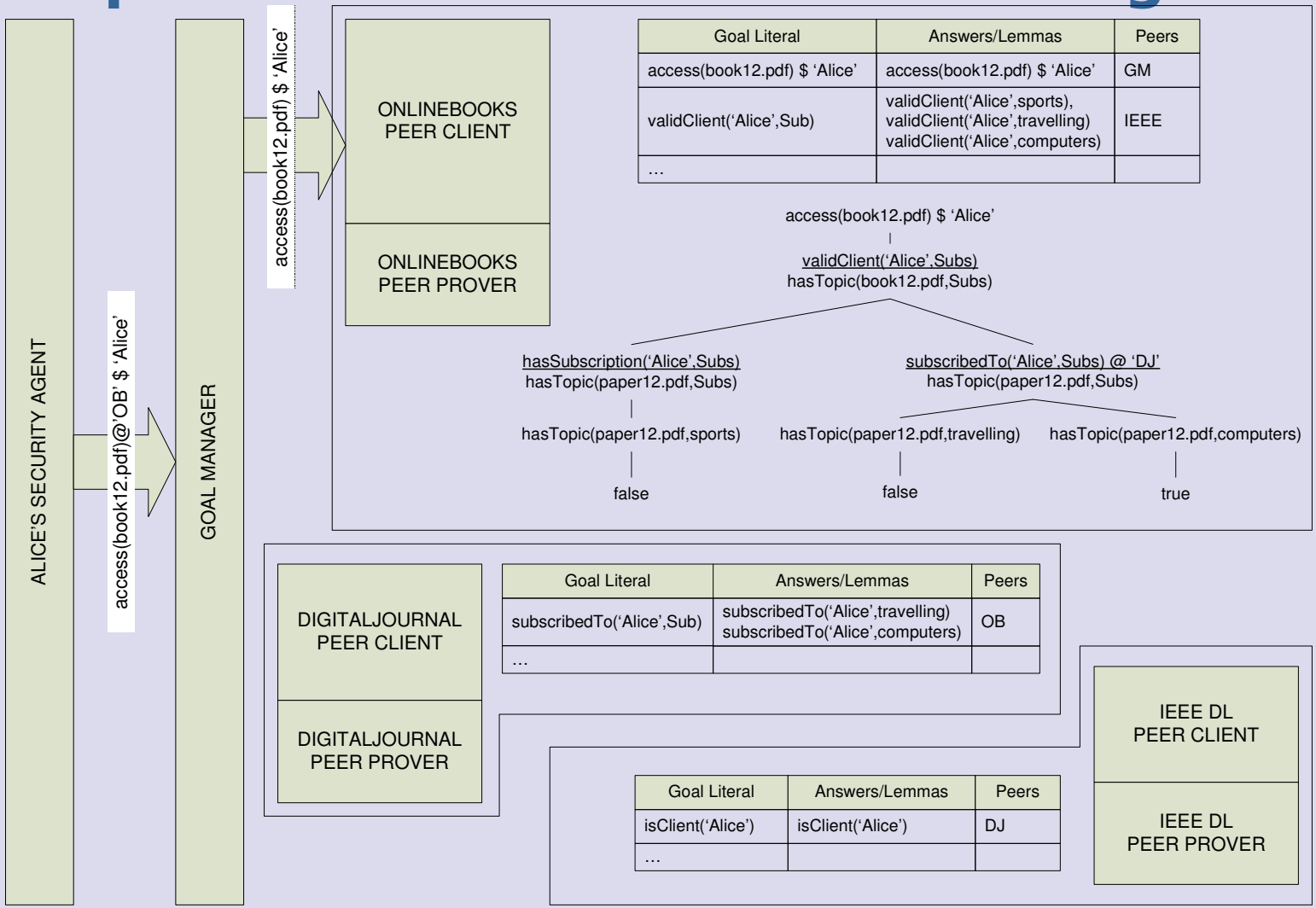
I show you my CIA badge
If you show me yours first

I show you my CIA badge
If you show me yours first

[Li, Du,Boneh*Winsborough, Seamons, Jones.* Oblivious Signature-Based Envelope DARPA *ACM Symposium on Principles of Distributed Computing, 2003]*

Deployed Application Scenarios

Loop Detection: Distributed Tabling



[*Alves, Damásio, Olmedilla, Nejdl*. A distributed tabling algorithm for rule based policy systems. IEEE POLICY, 2006 *]*

Deployed Application Scenarios
Inference Web Answer Explanation

Provides generic explanation tools for (Semantic) Web based systems

- Infrastructure for presenting and managing explanations
  - Knowledge provenance
  - how answer were derived or retrieved
- IWBase
  - Web-registry with information sources, reasoners, languages, rewrite rules
- Proof Markup Language (PML)
  - Encoding of portable proofs
- IW Browser
  - Tool supporting navigation and presentation of proofs and their explanations
- No support for explaining infinitely failed derivations

[*McGuinness, da Silva.* Explaining answers from the semantic web: The inference web approach. Journal of Web Semantics, 2004]

Deployed application scenarios
Protune's explanations: Requirements - solutions

- Easy instantiation in any given application domain
  - One extra step: create literal verbalization rules
- Performance
  - Constructed at client side
- Explanation method
  - Focus on the aspects that are relevant to the user
  - Optional detailed view
  - Queries: **why/why-not, how-to, what-if**
- Presentation strategies
  - Simultaneous local + global information ***new!***
  - Explanations are (potentially cyclic) hypertexts
- Explaining infinite failure
  - Tabled explanation structures ***new!***

[*Bonatti, Olmedilla, Peer.* Advanced Policy Queries. REWERSE report I2-D4 and ECAI'06]

Why-Not Queries
Pruning strategies

new!

I CAN'T PROVE THAT
it is allowed to download paper14.pdf
BECAUSE

Rule [r3] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]

AND

Rule [r4] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]
MOREOVER
THERE IS NO User SUCH THAT
User has paid for paper14.pdf [details]

FILTERED POLICY
[r3]: allow(download(Resource)) ←
authenticated(User),
blurred(hasSubscription(User)).

[r4]: allow(download(Resource) ←
authenticated(User),
paid(User,Resource).

METAPOLICY
allow(download(Resource)).explanation:
[it,is,allowed,to,download,Resource].

public(Resource).explanation:
[Resource,is,public].

authenticated(User).explanation:
[User,is,authenticated].

hasSubscription(User).explanation:
[User,has,subscription].

paid(User,Resource).explanation:
[User,has,paid,for,Resource].

Why-Not Queries

Pruning strategies

new!

"authenticated" depends on a credential.
"hasSubscription" depends on "authenticated"

I CAN'T PROVE THAT
it is allowed to download paper14.pdf
BECAUSE

Rule [r3] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]

Pruning: User is not authenticated so it makes no sense to inspect her subscriptions

AND

Rule [r4] is not applicable:
THERE IS NO User SUCH THAT
User is authenticated [details]
MOREOVER
THERE IS NO User SUCH THAT
User has paid for paper14.pdf [details]

FILTERED POLICY
[r3]: allow(download(Resource)) ←
authenticated(User),
blurred(hasSubscription(User)).

[r4]: allow(download(Resource) ←
authenticated(User),
paid(User,Resource).

METAPOLICY
allow(download(Resource)).explanation:
[it,is,allowed,to,download,Resource].

public(Resource).explanation:
[Resource,is,public].

authenticated(User).explanation:
[User,is,authenticated].

hasSubscription(User).explanation:
[User,has,subscription].

paid(User,Resource).explanation:
[User,has,paid,for,Resource].

Clusters
replace key attributes *new!*

I CAN'T FIND ANY User SUCH THAT
    User is authenticated
BECAUSE

    c012 is a credential with
        type 'id',name 'John' and issuer 'L3S'
    BUT
    IT IS NOT THE CASE THAT
        'L3S' is trusted for 'id' [details]

AND

    Rule [r7] is not applicable:
    THERE ARE NO User AND P SUCH THAT
        username = User and password = P

POLICY
[r6]: authenticated(User) ←
credential(Credential),
Credential.type:'id',
Credential.name:User,
Credential.issuer:CA,
blurred(trusted_for(CA,'id')).

[r7]: authenticated(User) ←
declaration([user=User,
password=P]),
blurred(passwd(User,P)).

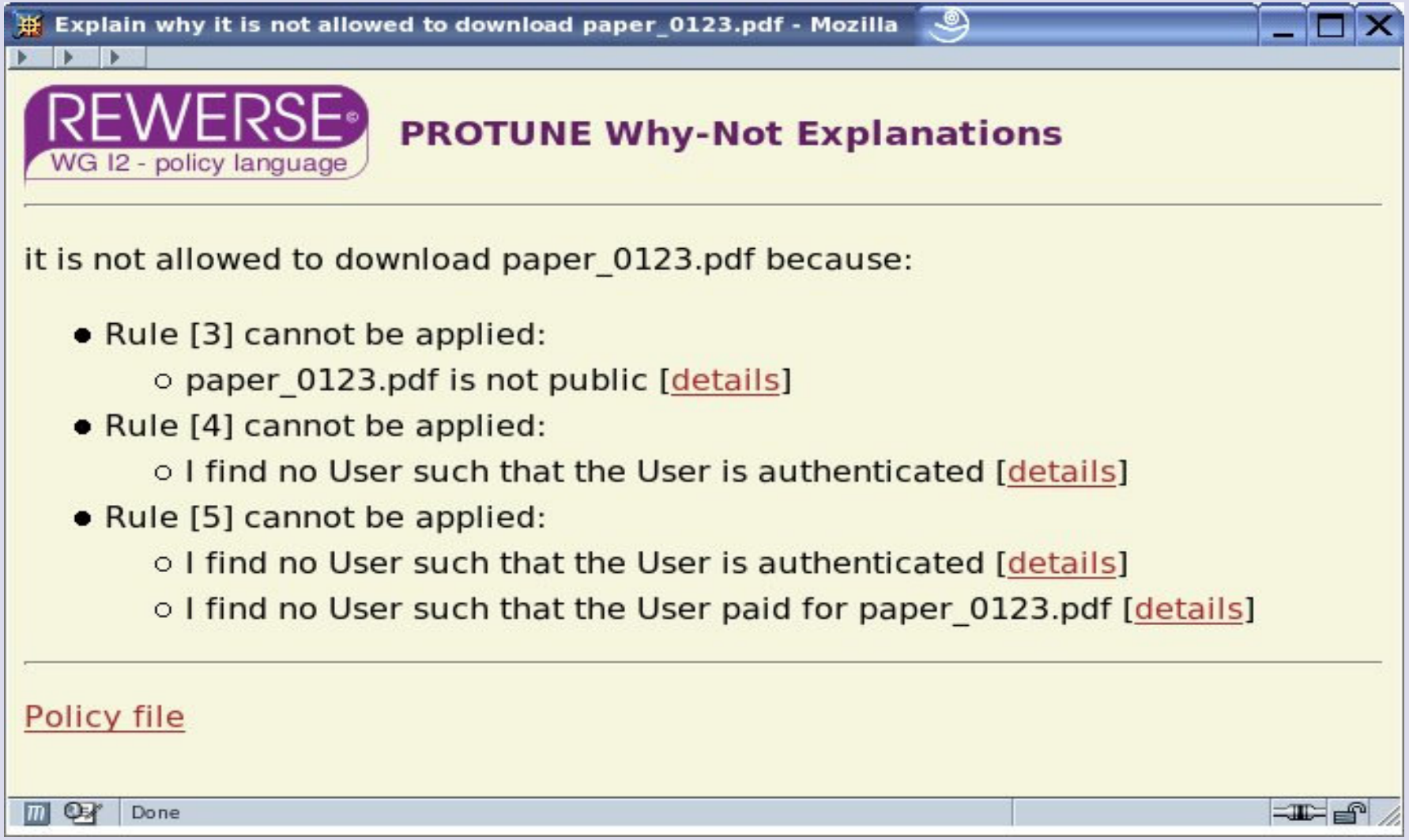
METAPOLICY
authenticated(User).explanation:
[User,is,authenticated].

trusted_for(CA,Type).explanation:
[CA,is,trusted,for,Type].

passwd(User,P).explanation:
[P,is,the,correct,password,for,User].

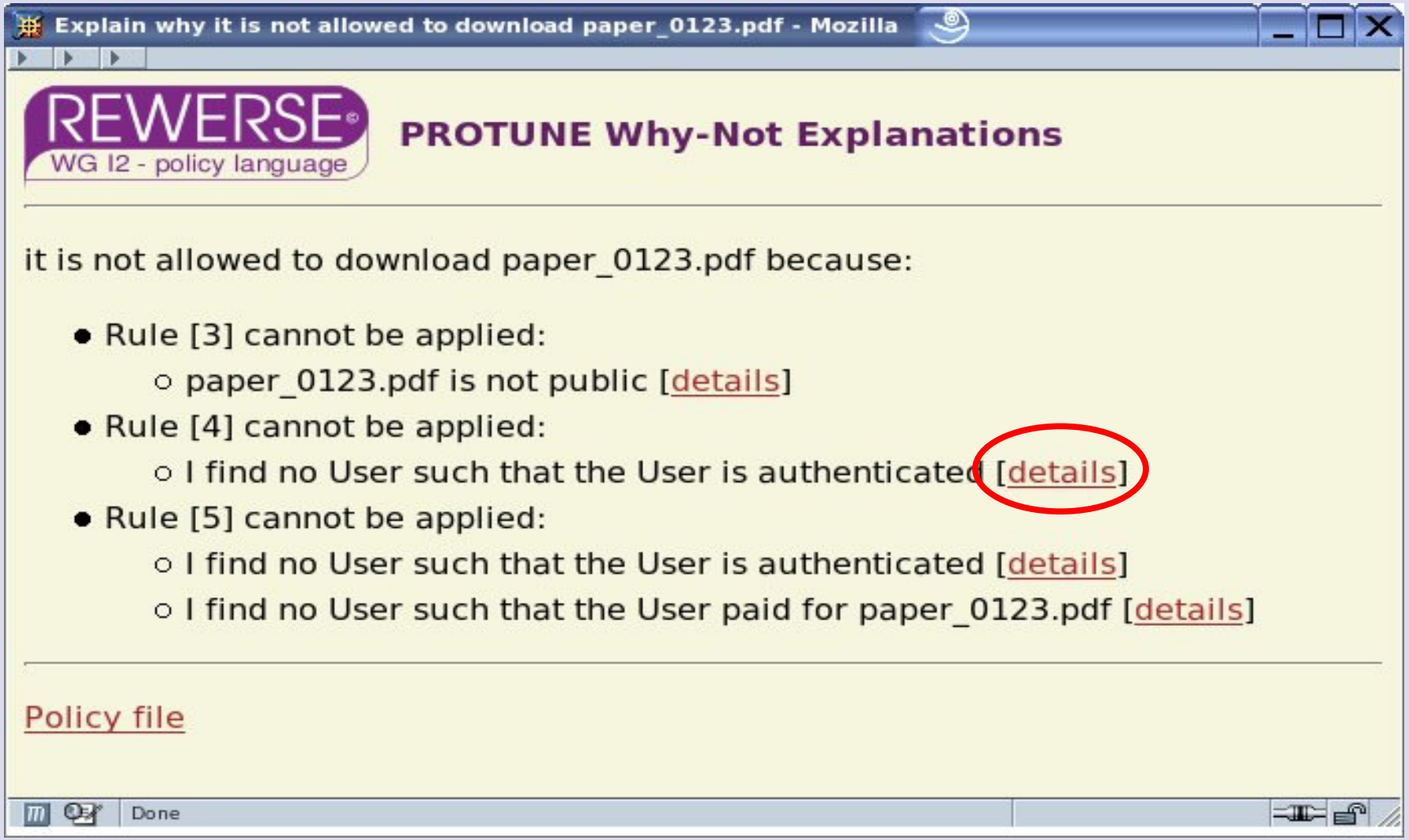
Why-not demo

Sample screenshot



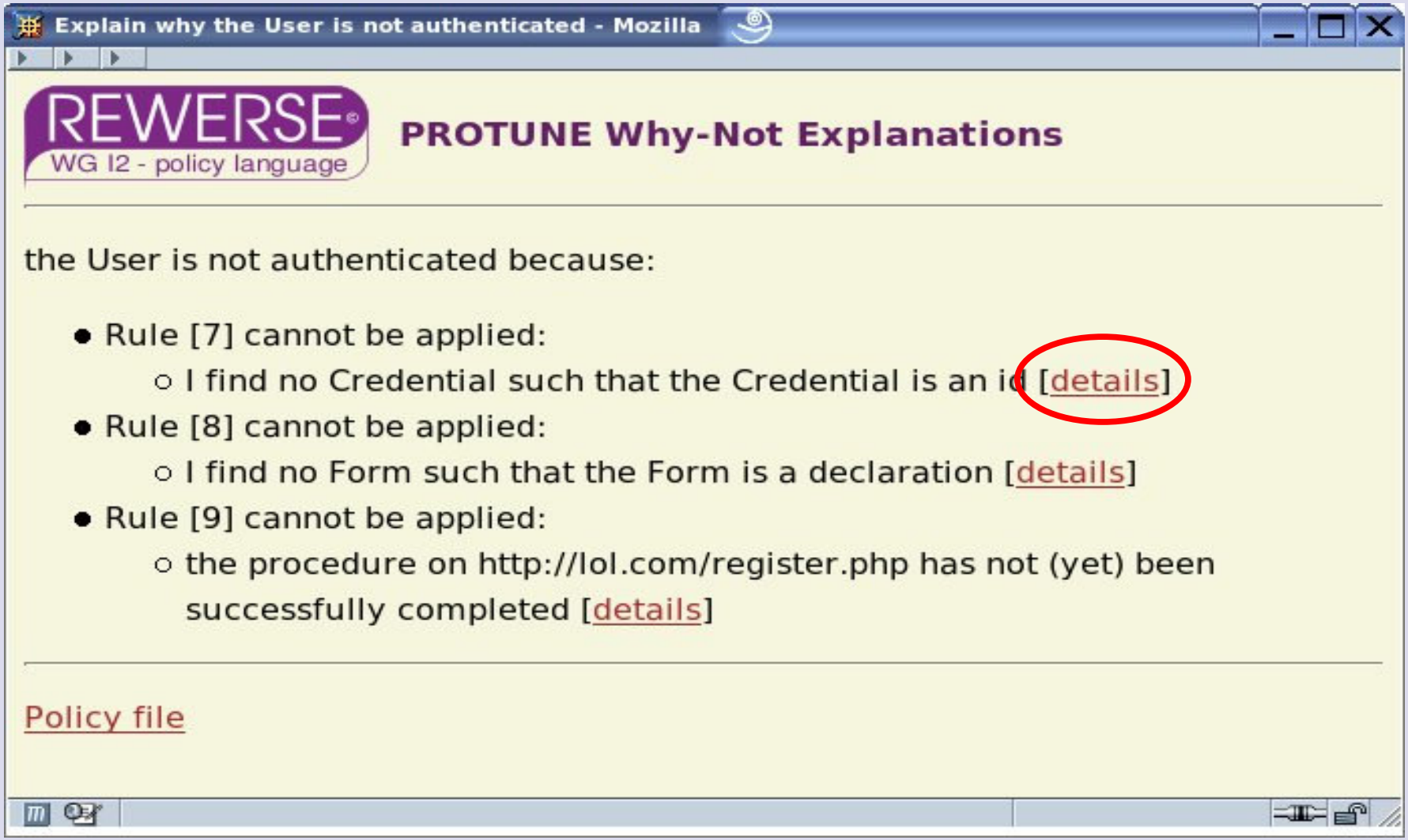
Why-not demo

Sample screenshot



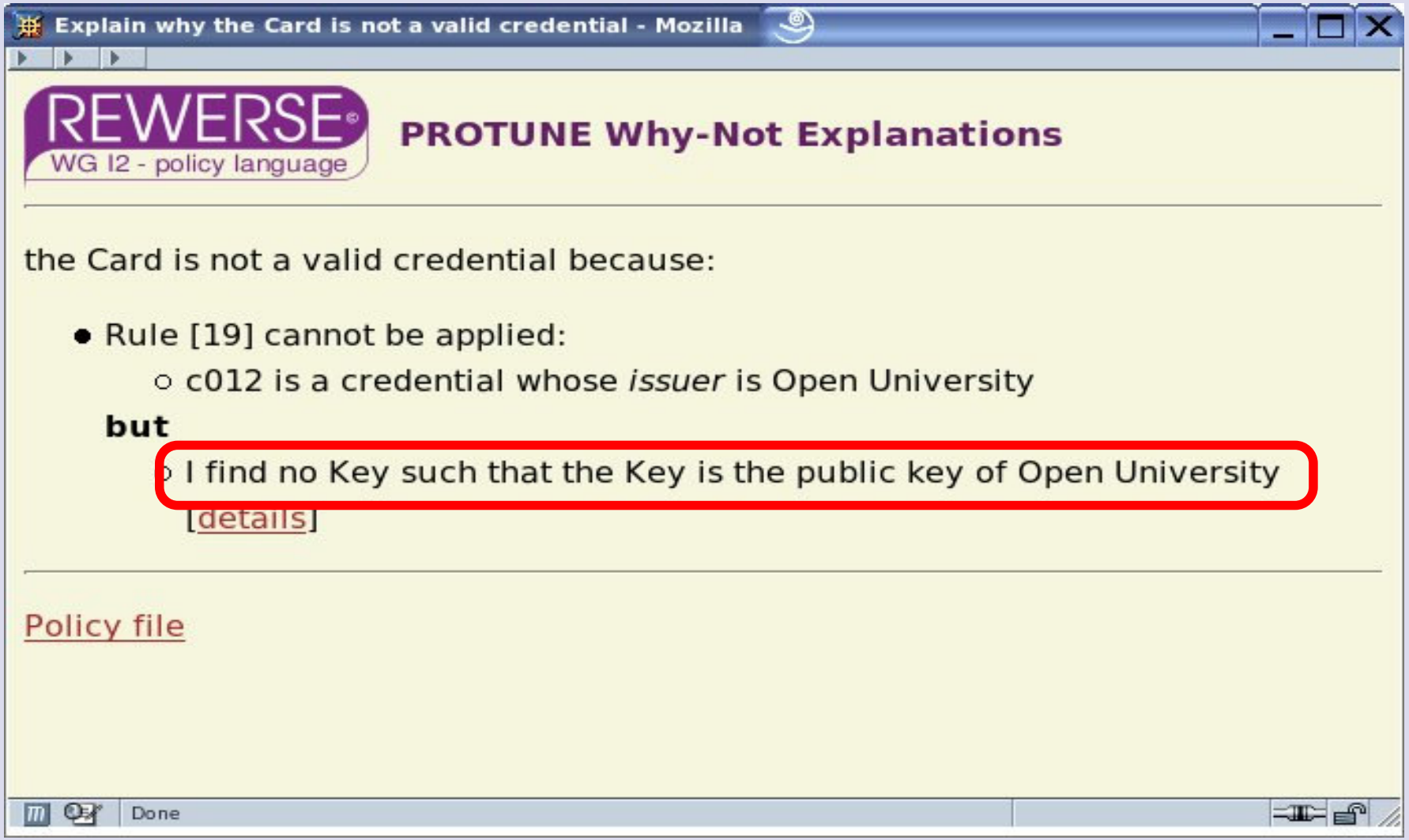
Why-not demo

Sample screenshot



Why-not demo

After one more step...



Outline

- Introduction
- Where are we?
- Deployed Application Scenarios
- **What is still missing?**
  - **Independently of the SW**
  - **Open problems for SW researchers**
- Conclusions

Widely recognized problems
A summary

- Integrating different rule types
  - for supporting multiple policy types
- Integrating strong, soft, lightweight evidence
  - therefore discrete + numeric trust models
- User awareness & control
  - high-quality explanations
  - controlled NL policies

Some problems we couldn't deal with
not SW-specific

- Negation as failure and strong negation
- Mapping high-level policies onto low-level mechanisms
  - abstractions and approximations
- Validation & verification
- Policy composition
  - modules
- Hints for credential discovery

What's new in SW scenarios?

- Security/Privacy/Trust community addressed
  - Open systems
  - Heterogeneous software interoperability
  - Deployment on the web
- No new requirements regarding
  - Public/private nature of policies
  - Stateful/stateless nature of negotiations
  - Unilateral/bilateral forms of negotiations

Policies are still sensitive

☐ not necessarily public

Business policies

- May reveal dishomogeneous treatment of different users
  - Which may irritate some customers
- May reveal strategic agreements with other companies

Private information

- Example: protecting family pictures
  - *Only my friends can download these pictures*
  - *Some people may realize they are not friends by reading the policy*

The Web supports transactions
☐ negotiations can be stateful

Even if HTTP is stateless

- Many major web sites support transactions
  - Despite heavy traffic load
  - **No convinging scalability issues**
- Stateful protocols can be simulated
- Drawback of stateless approaches
  - Burden and responsibility on the programmer
  - Vulnerabilities (e.g. *cookies)*

Servers may release credentials

☐ negotiations may be bilateral

Consider certifications and seal programs

- Publishing these credentials is good advertisement
  - Attracting potential customers
  - Making the service more competitive
- Not necessarily affecting negotiation length
  - Certifications are public
  - May be released all at once
  - On a public repository or on-demand if credentials are too many
  - The server may issue one hint to point to a repository

Within the realm of SW and KR&R
and not in the focus of the trust community

- Ontology-based interoperability
  - including Pervasive lightweight evidence
- Regard policies as KBs
  - One knowledge – many uses
- Focus on intelligent interfaces
  - Explanations
  - Controlled NL front-ends
- Reasoning about policies
  - Select services based on their policies
  - Policy verification and validation
- Intelligent negotiation
  - e.g. Credential selection (cf. ASP tutorial)

Within the realm of SW and KR&R
and not really tackled by security people

- Record linkage
  - Join data sources to infer sensitive information
- Inference problem
  - Possibly using common knowledge and user knowledge
  - Theoretical models exist (e.g. [Biskup et al.]), but
- Currently not checked by real systems
  - No machine-understandable model of available knowledge is implemented
- Ontologies and semantic markup
  - Enable automated inference-based attacks, but also
  - Enable automated inference checking
  - Using the same techniques (like password crackers)

[*Biskup, Bonatti.* DKE 01, FoIKS 02, ESORICS 02, IJIS 04, AMAI 04, FoIKS 2006]

Inference of sensitive information
in the semantic web

Lots of information is implicit in published information

- Salaries can be inferred from roles
  - Salaries can be approximated from house value
- Phone number and zip codes are related
- …

Common knowledge can be encoded

- In a machine understandable way
- Inference can be automated
  - Not tackled by current access control systems

Inference of sensitive information
in the semantic web

Protecting semantic data

- Naturally subject to inference
- Opportunity for high-level specifications
  - Protect *concepts (e.g. "my identity")*
  - *Use semantic techniques to identify data that encode sensitive concepts*
  - Easier for untrained users
- It requires extensive and reliable tagging
  - Security people would not be convinced today

Record linkage

Medical Data released as Anonymous

SSN	Name	Ethn	DOB	Sex	ZIP	Problem
…	…	…	…	…	…	…
…	…	White	09.15.61	F	94142	Obesity
…	…	…	…	…	…	…

Voter List

Name	Address	City	ZIP	DOB	Sex	Party	…
…	…	…	…	…	…	…	…
Sue Carlson	900 Market St.	San Fran.	94142	09.16.61	F	Democrat	…
…	…	…	…	…	…	…	…

Record linkage
in the semantic web

Knowledge and reasoning facilitate

- Finding "linkable" data sources
- Joining heterogeneous data
  - Different attribute names
  - Different formats
- Using implicit information (inference)

Outline

- Introduction
- Where are we?
- Deployed Application Scenarios
- What is still missing?
- **Conclusions**

Conclusions

Policies are semantic markup

- Describing behavior (vs. content)
  - An instance of SW ideas
  - With widespread potential impact
  - In a short term
  - ...and in the long term (visionary perspectives)
- A case for rule-based ontologies
  - Novel interplay between the two towers

Conclusions

Plenty of possible SW contributions to security, privacy and trust & beyond

- Powerful KR&R infrastructure
  - Lightweight but expressive languages, and
  - Fast engines
- Knowledge-based policy handling
  - Enforcement, validation, explanations
- First concrete approaches to
  - Inference attacks
  - Preventing record linkage

Conclusions

Avoid pitfalls

- Wrong assumptions
  - Incompatible with realistic scenarios
  - ...recall conflicts...
- Re-inventing the wheel
  - There are already lots of high-quality works
  - Intersection between security/trust and KR&R communities
  - There are enough (really) new problems to be tackled!


REWERSE©
reasoning on the web
Questions?
REWERSE©
WG I2 - policy language

References
Full List

- More exhaustive list can be found at

  http://www.L3S.de/~olmedilla/policy/policyPapers.html

References
Conferences (I)

1. Miguel Alves, Carlos Viegas Damásio, Daniel Olmedilla, and Wolfgang Nejdl. A distributed tabling algorithm for rule based policy systems. POLICY 2006.
2. Piero A. Bonatti, Claudiu Duma, Norbert Fuchs, Wolfgang Nejdl, Daniel Olmedilla, Joachim Peer, and Nahid Shahmehri. Semantic web policies - a discussion of requirements and research issues. ESWC 2006.
3. Piero Bonatti, Daniel Olmedilla, and Joachim Peer. Advanced policy explanations. ECAI 2006.
4. Marianne Winslett, Charles C. Zhang, and Piero A. Bonatti. Peeraccess: a logic for distributed authorization. CCS 2005.
5. Piero A. Bonatti and Daniel Olmedilla. Driving and monitoring provisional trust negotiation with metapolicies. POLICY 2005.
6. Pranam Kolari, Li Ding, Shashidhara Ganjugunte, Anupam Joshi, Timothy W. Finin, and Lalana Kagal. Enhancing web privacy protection through declarative policies. POLICY 2005

References
Conferences (II)

7. Pranam Kolari, Li Ding, Shashidhara Ganjugunte, Anupam Joshi, Timothy W. Finin, and Lalana Kagal. Enhancing web privacy protection through declarative policies. POLICY 2005
8. Wolfgang Nejdl, Daniel Olmedilla, Marianne Winslett, and Charles C. Zhang. Ontology-based policy specification and management. ESWC 2005.
9. Daniel Olmedilla, Omer F. Rana, Brian Matthews, and Wolfgang Nejdl. Security and trust issues in semantic grids. In Semantic Grid: The Convergence of Technologies, volume 05271 of Dagstuhl Seminar Proceedings. 2005.
10. Moritz Y. Becker and Peter Sewell. Cassandra: Distributed access control policies with tunable expressiveness. POLICY 2004.
11. Saket Kaushik, Paul Ammann, Duminda Wijesekera, William H. Winsborough, and Ronald W. Ritchey. A policy driven approach to email services. POLICY 2004.
12. Rita Gavriloaie, Wolfgang Nejdl, Daniel Olmedilla, Kent E. Seamons, and Marianne Winslett. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the semantic web. ESWS 2004
13. Andrzej Uszok, Jeffrey M. Bradshaw, and Renia Jeffers. Kaos: A policy and domain services framework for grid computing and semantic web services. iTrust 2004.

References
Conferences (III)

14. Gianluca Tonti, Jeffrey M. Bradshaw, Renia Jeffers, Rebecca Montanari, Niranjan Suri, and Andrzej Uszok. Semantic web languages for policy representation and reasoning: A comparison of kaos, rei, and ponder. ISWC 2003.
15. Lalana Kagal, Timothy W. Finin, and Anupam Joshi. A policy based approach to security for the semantic web. ISWC 2003.
16. Andrzej Uszok, Jeffrey M. Bradshaw, Renia Jeffers, Niranjan Suri, Patrick J. Hayes, Maggie R. Breedy, Larry Bunch, Matt Johnson, Shriniwas Kulkarni, and James Lott. Kaos policy and domain services: Toward a description-logic approach to policy representation, deconfliction, and enforcement. In 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), pages 93-, Lake Como, Italy, June 2003. IEEE Computer Society.
17. Lalana Kagal, Timothy W. Finin, and Anupam Joshi. A policy language for a pervasive computing environment. In 4th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), pages 63-, Lake Como, Italy, June 2003. IEEE Computer Society.

References
Conferences (IV)

18. Matt Blaze, John Ioannidis, and Angelos D. Keromytis. Experience with the keynote trust management system: Applications and future directions. In Trust Management, First International Conference, iTrust, volume 2692 of Lecture Notes in Computer Science, pages 284-300, Heraklion, Crete, Greece, May 2003. Springer.
19. Kent E. Seamons, Marianne Winslett, Ting Yu, Bryan Smith, Evan Child, Jared Jacobson, Hyrum Mills, and Lina Yu. Requirements for policy languages for trust negotiation. In 3rd International Workshop on Policies for Distributed Systems and Networks (POLICY), pages 68-79, Monterey, CA, USA, June 2002. IEEE Computer Society.
20. Piero A. Bonatti, Sabrina De Capitani di Vimercati, and Pierangela Samarati. An algebra for composing access control policies. ACM Trans. Inf. Syst. Secur., 5(1):1-35, 2002.
21. Ninghui Li, John C. Mitchell, and William H. Winsborough. Design of a role-based trust-management framework. In IEEE Symposium on Security and Privacy, pages 114-130, 2002.
22. Trevor Jim and Dan Suciu. Dynamically distributed query evaluation. In 20th ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, Santa Barbara, California, USA, May 2001. ACM.

References
Conferences (& V)

23. Trevor Jim. Sd3: A trust management system with certified evaluation. In IEEE Symposium on Security and Privacy, pages 106-115, 2001.
24. Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. The role of trust management in distributed systems security. In Secure Internet Programming, Security Issues for Mobile and Distributed Objects, volume 1603 of Lecture Notes in Computer Science, pages 185-210. Springer, 1999.
25. Matt Blaze, Joan Feigenbaum, and Martin Strauss. Compliance checking in the policymaker trust management system. In Financial Cryptography, Second International Conference, volume 1465 of Lecture Notes in Computer Science, pages 254-274, Anguilla, British West Indies, February 1998. Springer.
26. Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized trust management. In IEEE Symposium on Security and Privacy, pages 164-173, Oakland, CA, USA, May 1996. IEEE Computer Society.

References
Journals

27. Steffen Staab et al. The pudding of trust. IEEE Intelligent Systems, 2004.
28. Joachim Biskup and Piero A. Bonatti. Controlled query evaluation for known policies by combining lying and refusal. Ann. Math. Artif. Intell., 2004.
29. Andrzej Uszok, Jeffrey M. Bradshaw, Matt Johnson, Renia Jeffers, Austin Tate, Jeff Dalton, and J. Stuart Aitken. Kaos policy management for semantic web services. IEEE Intelligent Systems,, 2004.
30. Lalana Kagal, Massimo Paolucci, Naveen Srinivasan, Grit Denker, Timothy W. Finin, and Katia P. Sycara. Authorization and privacy for semantic web services. IEEE Intelligent Systems, 2004.
31. Ninghui Li, Benjamin N. Grosof, and Joan Feigenbaum. Delegation logic: A logic-based approach to distributed authorization. ACM Trans. Inf. Syst. Secur., 2003.
32. Ninghui Li, William H. Winsborough, and John C. Mitchell. Distributed credential chain discovery in trust management. Journal of Computer Security, 2003.
33. Yang-Hua Chu, Joan Feigenbaum, Brian A. LaMacchia, Paul Resnick, and Martin Strauss. Referee: Trust management for web applications. Computer Networks, 1997.

References
Books

34. Grigoris Antoniou, Matteo Baldoni, Piero A. Bonatti, Wolfgang Nejdl, and Daniel Olmedilla. Rule-based policy specification. In Ting Yu and Sushil Jajodia, editors, Decentralized Data Management Security. Springer, 2006.
35. John W. Lloyd. Foundations of Logic Programming, 2nd Edition. Springer, 1987.

References
Other

36. Ionut Constandache, Daniel Olmedilla, and Wolfgang Nejdl. Policy based dynamic negotiation for grid services authorization. Semantic Web Policy Workshop at ISWC 2005.
37. Moritz Y. Becker and Peter Sewell. Cassandra: Flexible trust management, applied to electronic health records. IEEE Computer Security Foundations Workshop 2004.
38. Jim Basney, Wolfgang Nejdl, Daniel Olmedilla, Von Welch, and Marianne Winslett. Negotiating trust on the grid. Workshop on Semantics in P2P and Grid Computing at WWW 2004.
39. Matt Blaze, Joan Feigenbaum, and Angelos D. Keromytis. Keynote: Trust management for public-key infrastructures (position paper). In Security Protocols International Workshop, 1998.