A Safe Information Sharing Framework for E-Government Communication

Fillia Makedon
Dartmouth College, Computer Science, Hanover, NH, USA, fillia.makedon@dartmouth.edu
Calliope Sudborough
International Relations, Boston University, Boston, MA, USA, kalioppi@bu.edu
Beth Baiter
Weatherhead Center for International Affairs, Harvard Univ., Cambridge, MA, USA
Grammati Pantziou
TEI, Computer Science, Athens, Greece, pantziou@teiath.gr
Marialena Conalis-Kontos
Whitehead Institute, Harvard University, Boston, MA, USA, mconalis@wcfia.harvard.edu

Abstract: E-government principles are based on the assumption that different government agencies are willing to cooperate and share findings through a network infrastructure. When government agencies refuse to cooperate and share information due to conflicts, then novel mediation mechanisms are needed. We introduce a negotiation-based sharing system called **SCENS: Secure Content Exchange Negotiation System** currently being developed at Dartmouth College with the assistance of many interdisciplinary experts. SCENS is a multi-layer scaleable system that ensure safety of transactions through various security mechanisms. It is based on a metadata description of heterogeneous information and applies to many different domains. Through negotiation, government users would reach agreement on the conditions of sharing, especially when the information is sensitive and distributed.

Keywords: negotiation, sharing, metadata, security, e-government

Introduction

E-*democracy* is dependent on electronic communication infrastructures commonly called e-government. An e-government is not necessarily democratic in nature, unless it has encoded democratic laws that apply to all citizens and address their rights and needs. A democratic e-government system facilitates the citizens' lives, offers round the clock services, transparency, accountability, access to accurate information, legal support, history of past decisions and other services such as e-voting and national discussions.

E-government principles are based on the assumption that different government agencies are willing to cooperate and share findings and analyses of these findings through a network infrastructure. Such a system makes sense only if its benefits outnumber any problems that might be arise due to its technology such as, unsafe communications, difficulty of use, undetectable errors, out of date information, misinformation, huge costs of maintenance, steep learning curves, and other. Its aims should be to assist governance by bringing innovation, self-correcting mechanisms, improved internal processes and rise in productivity, new opportunities and most importantly, better services for the citizen as well as the government.

Current European Commission efforts to absorb different government systems fit these aims and depend on **a common data sharing standard**. However, when government agencies refuse to cooperate and share information due to conflicts among ministries, rivalry or other reasons, then novel mediation mechanisms are needed to enable information sharing and this sharing must become a duty, not an option for any government. Through negotiation, there would come agreement on the conditions of sharing, especially when the information is sensitive and distributed. In addition, negotiation would force large amounts of heterogeneous

information (e.g., text documents, email logs, video tapes, weather data, other sensor data) to become interoperable through a mechanism of common representation for the purpose of negotiation.

Currently, too little information is shared among European government agencies, especially in the security arena. Social, cultural, ownership and administrative bottlenecks, keep data holders from sharing their division's data and informational assets. Fear of revealing sources and losing autonomy thus result in costly and redundant efforts that lower productivity, achieve limited data-reuse and integration. Therefore, if e-government is to succeed a negotiation-based information sharing system is needed that includes effective and rewards and ensures due credit. In this paper we introduce a negotiation-based sharing system called SCENS: Secure Content Exchange Negotiation System being developed at Dartmouth College with the assistance of interdisciplinary experts.

Sharing Information

"**Sharing information**" means different things to different government sectors at different times. It may be collecting and sharing intelligence between two security divisions, or sharing original e-crime data, observations on these data, surveillance notes, scientific facts, commercial transaction data, and other. As there are no standard methods for e-government information sharing, the modes of sharing are currently not uniformly monitored, authenticated and recorded. Information differs in the level of detail, the quantity or type of data exchanged. Furthermore, the sharing is not always guaranteed to be safe from risks that may include, unauthorized access, malicious alteration, destruction of information or misinformation, computer intrusions, copyright infringement, privacy violations, human rights violations and other. A safe information sharing framework in an e-government system requires more than applying encryption algorithms to the data and must be designed to be flexible and evolving just as cyber-security threats evolve.

Negotiation-based sharing is dependent on a common way to represent diverse information. However, integration of heterogeneous information residing in different ministries is not an easy problem. It arises due to different ways of collection and independent (yet often parallel) missions. Thus, massive amounts of valuable scientific, demographic, environmental and other types of data repositories that are part of an agency's informational assets often remain unused after their initial gathering, or "project-locked", i.e., bound to a given project, although they may be of use to other projects within a division or across divisions. In our system we use metadata (data about data) to unify different types of information. This facilitates searching and tracking of how information is used, especially in decision-making.

In a climate of international governance and globalization, tracking the usage of information and accounting for what information contributed to government decision-making are indeed important safety measures. In fact, once can say that an e-government system that lacks information sharing capabilities is really not a safe e-government system and thus not a democratic system at all, as it cannot guarantee that the right decisions were taken to ensure the democratic process. Thus, transparency of information is not an option of a democratic government anymore but a necessary public service to the citizen because it is a mechanism to account for the quality and correctness of information that went into a certain decision.

If one asks a government official about information sharing, he will speak from a divisional viewpoint and tell you that, yes, there is already a lot of sharing involving his division and that more sharing might even be unsafe. In his world, information is attached to a project, a

certain time and certain persons. It does not transcend to become part of **e-government knowledge** and future investment. Should the project change or the official be relocated, the new person would have to reconstruct who shared what with whom and why, possibly making erroneous decisions. This means that a non-sharing e-government system is a security risk. Building e-government knowledge also helps being prepared to handle new situations that should not have to rely on the skills and memory of a particular individual or division but use repositories of knowledge to retrieve related information, along with supporting tools of analysis.

The SCENS framework

An **e-government negotiation system** is inherently international due to its digital nature. It helps establish the conditions of sharing original as well meta-information among different divisions or even countries. We are currently developing such a negotiation system called **SCENS: Secure Content Exchange Negotiation System.**

SCENS has a flexible 3-layer service structure that provides different levels of negotiation services for different type of users:

- Layer 1 behaves as a traditional web-based negotiation support system for human beings. It also provides some **negotiation agents**, which are actually user customizable utility functions. Users can customize the negotiation agents provided by Layer 1 through multiple parameters, such as the weights assigned to different negotiation conditions. However, the agents provided by Layer 1 are not fully customizable; if the negotiation strategy is very complex, Layer 2 must be used.

- Layer 2 supports complete **negotiation strategy customization by users**. In Layer 2, users can have their own negotiation agents to implement any negotiation strategies. The negotiation agents, which are treated as web service consumers and run on the client side, conduct negotiation with other negotiation agents or human beings through web services.

- Layer 3 provides an open and **automated negotiation environment**. DAML+OIL (Dean et al., 2001), a language for creating ontologies and marking up information, is used in Layer 3 to define a negotiation ontology, which allows agents to acquire knowledge about how to conduct negotiations. This knowledge includes negotiation protocols, negotiation proposals and conditions, *etc*. Agents communicating with Layer 3 can be used in any negotiation activities given the proper negotiation ontology. In Layer 2, in contrast, the knowledge about negotiation rules is actually hard-coded into the agents.

SCENS ensures **safe sharing** as it (a) authenticates the user and protects the privacy of data, users and transactions with encryption technology, (b) negotiates the sharing based on a metadata description of the information; using metadata to describe the original information is a form of security that also keeps the information provider in control of his data; (c) allows the actual exchange of the real data to occur only after prior agreement on the conditions has been reached, (d) tracks usage of shared information and collects feedback that becomes part of the security infrastructure of the system, (e) makes non-interoperable data interoperable with a uniformly secure metadata extraction system, (f) provides high-level government security by facilitating government sectors to cooperate and prepare for incidents or events that threaten security due to lack of communication.

Components of the system include, **authentication and authorization security components**

for access control, an intelligent **data collection component** that semi-automates the extraction of metadata and provides a workflow management interface for improved government worker productivity, components for **searching and querying** informational assets via metadata, a **negotiation mechanism** for recording and tracking the exchange of raw (private or sensitive) data, an **incident reporting component** for monitoring risks and security violations, an automated **data broker component**, a **consultation and training component**, user-interaction components that include a discussion forum and a user-interface visualization system.

Technical Details: Our implementation of the negotiation system SCENS, employs RDF schemas to allow negotiation agents or human users to use it with a predefined negotiation ontology. Layers 2 and 3 provide web services. To help define and extend negotiation ontologies, we are developing a **Negotiation OntOlogy Description LanguagE** (NOODLE). Shibboleth is used to provide **authorization and authentication services** to SCENS users. Shibboleth provides an open source implementation to support inter-institutional sharing of web resources subject to access controls, and one of its key concepts, the federated administration, is exactly the same as the distributed deployment pattern of SCENS. The SCENS web-based interface is based on JavaServer Pages (JSP) (Sun, 2003a) and Java Servlets (Sun, 2003b). For the web services we use Java Web Services Developer Pack (Java WSDP) (Sun, 2003c), which is an integrated toolset released by Sun company to build, test and deploy XML applications, Web services, and Web applications. The system is compatible across platforms.

Background

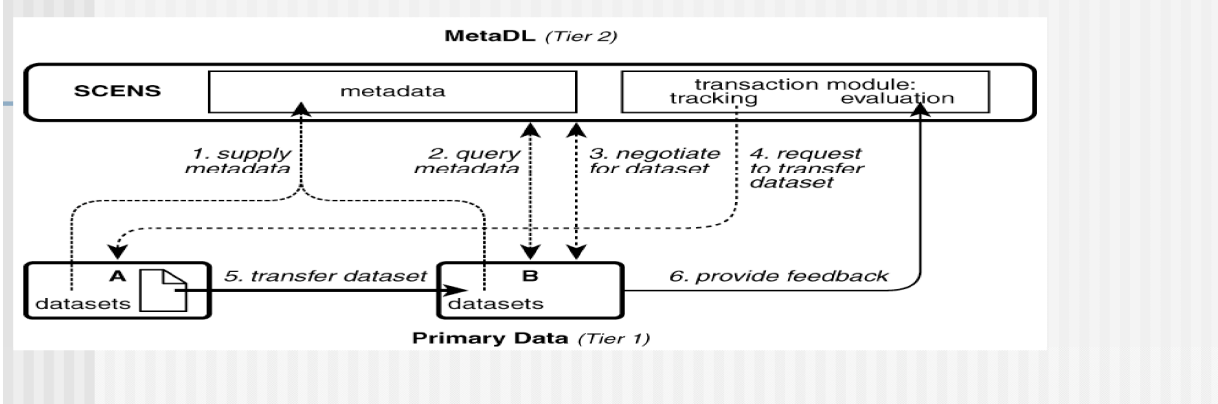
Several web-based negotiation support systems are in use. WebNS (Ding, 2000) is a prototype web-based system designed to facilitate remote negotiations on the Internet. SmartSettle (ICAN, 2003) attempts to find quantitative and qualitative preferences for all parties, and uses a central server to arrive at agreements without exposing confidential data. INSPIRE (Kersten, Noronha, 1997) and INSS (Kersten, Noronha 1998) are web-based systems containing facilities for specification and assessment of preferences, a messaging system, a scoring function to aid in the construction of offers, graphical displays of the negotiation progress, and a facility for constructing compromises. Most existing negotiation systems do not focus on security and privacy concerns, which make them inappropriate in a security-sensitive environment. Since they are designed primarily for use in online markets, they also lack efficient support for representing the exchange of complex information.

SCENS supports negotiation of information that is in the form of metadata. Original data is transformed into a common metadata format, quantified, evaluated and negotiated in that format. We use a 2-layer framework designed at Dartmouth that is called MetaDL to enable this process. MetaDL is the theoretical framework upon which our metadata-based data sharing system, SCENS, is built. A MetaDL is a digital library (DL) containing only metadata from other DLs (Lee et al., 2003). It supports two endeavors: searching for data via metadata, and sharing these data through negotiation [84]. Autonomous DLs or data repositories, each with an interface allowing it to specify access conditions, are referred to as “Tier 1 systems” in this context. Tier 2 systems contain data about Tier 1 DLs, *i.e.*, metadata, and support browsing and searching for data in Tier 1 DLs. Tier 1 DL systems by definition contain actual data, while MetaDL systems by definition contain only metadata, so the two tiers are non-overlapping.

Using MetaDL's, the SCENS system supports “**mediated sharing**”, which occurs when a

trusted third party assists in one party's request for data from another party. Mediated data sharing assumes a common data representation (metadata) for the data to be shared. Shareable data can be complex, may be collected under different assumptions and formats, and can be massive. Mediated sharing allows users to assess the importance of data for their purposes (*e.g.* based on different criteria like quality, creation date, source, size, *etc.*) and makes data amenable to rights management and financial sustainability models as in e-commerce [85].

In a MetaDL (see figure below), any existing data (government) system can become a Tier 1 system by providing metadata to a Tier 2 system. Thus, each government division can remain autonomous and simply submit descriptions of its informational holdings in metadata format, using software provided. This architecture allows for flexibility in organization and configuration. As an example, a group of Tier 1 providers (*e.g.*, European hospitals in the same city) could create their own Tier 2 system (with information for their Tier 1 DLs). For a user to gain an overview of what information is out there, he must search Tier 2 systems. The two-tier architecture permits better scalability, easier adoption of the system and easier combination of (meta)data from different providers while preserving ownership and access rights.



Negotiation incentives

Information sharing in e-government assumes being able to monitor, manage, evaluate resources used and identify needs. It thus helps **resource managment** of staff, computers, consultants, special services, training, digital data (e.g., video footage, photographs, email logs, phone records, flight maps, transportation schedules, structural infrastructure maps, and airport x-rays or video surveillance feeds).

Negotiation-based sharing through SCENS means convincing government users to use the system. We achieve this with incentives. One type of incentives is providing a system that makes their job easier by solving technical problems: ensuring the security of transactions, encoding usage conditions, alerting to privacy violations, ensurig the proper representation or modeling the information and evaluation of the quality of the information (e.g., how it was collected and its relative significance).

Other incentives that SCENS provides to e-government users (Makedon et al., 2003a, Makedon et al., 2003b, Ye et al., 2002a, Ye et al., 2002b, Ye et al., 2002c, Ye et al., 2003, Makedon et al., 2003c) include:

- A point system that quantifies informational contributions and demand for each sector, thus ensuring proper credit; Transparency to divisional efforts and accomplishments for administrators for better resource management;

- Autonomy of operation so that the different divisions who collect and own the information can maintain the format and autonomy of their data and protect their sources according to divisional restrictions;

- Workflow management features, automated data collection, security checks, inconsistency alerts, and other features;

- Interoperability for heterogeneous documents (ranging from hard copy textual documents to large spatiotemporal data) with appropriate security protection for each type of document, usage criteria and security access criteria;

- Searchability of information through a system for indexing;

- Analysis and data mining support tools to help make fast decisions, analyze new/existing information, corroborate sources and findings.

- Placing the government-user at the center and empowering him, whether he is a data provider or data subscriber;

- Standardizing and semi-automating the processes of data/ information collection; facilitating regular updating of information;

- Training modules that allow new personnel to learn easily;

- Incorporation of laws, local, national and international regulations that include built-in checks and balances with alerts in case of privacy or other violation;

- Extraction of valuable demographic information from monitoring the transactions of negotiation and information sharing requests;

- Enrichment of the e-government knowledge through collection of feedback from the users of the shared information and incorporation of this feedback back into the system for future users.

- Citizen «overview windows» to enable glimpses of how different government sectors connect and interelate;

- Provide a better overview of the collected information (who has what and how) and spell out what is necessary further work;

- (h) Security measures for safe sharing.

Crisis preparation and data sharing

Information sharing is most important when a crisis arises. A crisis can mean different things, ranging from an environmental disaster, denial of service attacks on commercial computers, a virus epidemic, anthrax threats, loss of electrical power or any loss that deprives citizens from normal life. Emergency preparedness characterizes a good e-government system.

Suppose an earthquake devastated a village in Western Greece in the month of August. The government acts immediately to help and send what it can. Alternatively, it can also use information from past cases to make its efforts more focused and intelligent. Without a

negotiation-based sharing system, gaining access to such information in the middle of August would require getting hold of the representative who is currently absent and is the only one to authorize release of information. Even rudimentary information on how much aid was given to past earthquakes may require access to information residing in several ministries thus needing permission from several people also vacationing in August. For non-classified data, such as the geography and topology of the earthquake region, one can only make sense if the data are correlated with weather information by experts who are also on vacation. Knowing who or where expertise resides internationally can also help if available.

This simplistic example is meant to illustrate how important it is for e-government to have planned for an information sharing framework that can protect, prevent or counteract crises. Good technology can indeed transform the relation between the government and the citizen with abilities not only to respond to crises, but also provide education about what to do in case of crisis and record results.

In non-crisis situations, negotiation-based sharing also helps as it reduces costs of duplication, chronic overspending and improves decision making through traceable facts, that counterbalance the notion that governments take decisions only based on political reasons, media attention or due to public reaction. Understanding the pattern of a short-term or long term crisis is expensive and longitudinal data collection and information sharing among multiple sources. It is dependent upon having all the facts possible, facts that may be difficult to obtain without negotiation, as they may reside in different national governments who do not agree to share.

International threats and negotiation-based sharing scenarios

"**European security**" means, in great part, efficient communication via up-to-date information sharing. However, any form of information sharing must not cause new threats but be used to counter threats. Prevalent international security threats that European governments worry and need to share information about are: incidents of illegal immigrants, industrial fraud that impacts jobs and economic stability, database tampering, organized crime, terrorism and drug trafficking. Such sharing must come along with supporting analysis tools that make it possible to correlate different studies on a large scale. International relations can be aided through an automated negotiation in handling of international crises.

The impact of global economy, the Internet, the rise of international crime and the ongoing threat of terrorism are some of the reasons that countries are now more interdependent on each other's gathered information. Policy decisions often become "**distributed decisions**" since, to take decision X requires another agency or country to take decision Y. This interdependency has caused government operations and decision-making to not only become more complex but also more fragile to external and internal threats.

Recent events have shown that governments need to share intelligence information, such as cargo and port shipments (Business Wire, 2003), customs information or ways to cut off terrorists from their sources of funding in European banks (Dettmer, 2002). On the other hand, information sharing across countries (UK Home Office, 2003) has a price, the attack on the civil liberties of its citizens (Gold, 2001).

Technology has made businesses very vulnerable to cyber-crime and international security threats. A secure information sharing in place is needed to enable businesses to share alerts

and advice and businesses must take an active role in the design of such a system. Sharing is also needed in cases of environmental disasters, such as the spreading patterns of a virus epidemic. Negotiation is needed not only to agree on the conditions of the sharing but also to help make different sources agree on common formats of sharing and how the information will be presented.

Below we list **scenarios** where negotiation enables safe sharing:
1. **Protection from terrorists**: Suppose that MI5 has interrogated a suspected terrorist, but the agents involved have concluded the identification by a tipster is wrong. The details of the interrogation, and the agents' conclusions, need to be passed to the European organization responsible for security, e.g., Interpol, along with details of other interviews in cases involving other terrorists, to show that the MI5 is taking action on the information that Interpol has provided. The MI5 agents want to restrict access to the interrogation and information about the person incorrectly identified as a terrorist. They are willing to allow Interpol personnel have unfettered access to some other data, but want part of it restricted and available only to (say) the Director of Interpol. SCENS provides an automated means for negotiating these restrictions before the transfer of data involving the misidentified suspect.

2. **Commercial sharing:** Let's say that companies Abel, Baker, and Charlie manufacture widgets, which are vital to a large segment of the public. Abel's computers are attacked, and Abel obtains excellent logs of the intrusions. The intrusions targeted plans for the widget. Abel wants to report this to the other widget manufacturers, but does not want to reveal sensitive information. Abel needs to negotiate the terms under which it will reveal data to Baker and Charlie, for example, what aspect of widget manufacture seemed to be the target of interest, relevant traces of the attack, and the ways in which the system was compromised. But since Baker's and Charlie's manufacturing branch may be able to deduce from the traces details of Abel's manufacture process, Abel and its competitors must agree on special protections (for example, only the security personnel at Baker and Charlie can examine the traces). So the negotiation must include elements of originator-controlled access control, and other access control mechanisms, as requirements. SCENS can provide an automated framework in which these negotiations can be handled. Furthermore, as these exchanges may be important to the European antiterrorist organizations, a mechanism that enables companies to advertise the composition of their computer intrusion data (using metadata) may also allow these organizations to consider if this information is related to European security.

3. **Sharing computer network vulnerability data**: Suppose two research groups, or companies, want to exchange vulnerability data with one another. This may be important information for a European security organization or it may not be. Saving energy and cost in determining whether such data is security-sensitive is possible with the system we propose because it is built upon a data sharing framework that exchanges not the actual data but key properties (metadata) that reflect the level of security importance. For the actual data exchange, each company owner may want to ensure first that the other will provide an adequate level of protection for their newly obtained data. This can be accomplished through negotiation on the terms of the exchange, including restrictions on access and use. SCENS can be used twice: once before any exchange is desired, to set the broad parameters for such an exchange; then again before actual data is exchanged or passed on, to modify the previous, umbrella agreement as required for that particular dataset.

4. **Countering international crime:** Suppose two European security agencies A and B want to share video data collected from two related surveillance cases. A has video data that covers

twice as many locations as B and wants to ensure that, should these datasets be "fused" into one new entity, then due credit is given to the effort of A. By having A and B entering the SCENS negotiation mode in order to exchange their video data, there is automatic record kept of who produced/accessed what and under which conditions of usage. Using metadata indexing, A's and B's data, and any new set of video produced from A's and B's holdings, can be tracked to its sources, assessed according to different parameters (e.g., age, resolution, uniqueness, amount of analysis associated with it, and other parameters), and reused in new efforts. Furthermore, each transaction generates valuable demographic information that indicates, for example, that there was need to fuse particular kinds of data in order to accomplish particular tasks.

Technical Challenges

The user of SCENS searches for information using a one-stop interface that describes diverse data in a uniform way. Once he finds the information needed, then he enters **negotiation mode** through which there is automatic recording of his request, the response, the conditions negotiated and the outcome. One challenge here is the creation of metadata from the original data, manually or automatically. For metadata to be effective, it depends on the context that it was collected under or is to be used and the two are not always the same. Therefore, data described through incomplete or inappropriate metadata may not be located in a search. Automating the generation of metadata through effective data collection interfaces must motivate users to use the system.

Making raw data interoperable by translating them into metadata requires the use of ontological frameworks that encode knowledge of the domain the data comes from, allowing automatic indexing and analysis of certain features of interest. Reuse and integration of existing data should guarantee recognition of the various collection and processing efforts that generated them, both to encourage ongoing efforts and to provide that capability of tracing information flow.

Information that comes in multiple data streams (such as immigration patterns over time) from different sites pose a challenge in finding good distance measures for doing **similarity search** such as «find me an immigration pattern like this one». Furthermore, query tools have to allow for data records missing some of the specified fields, *e.g.* because a field is not available due to security or privacy concerns. This can be viewed as extensions to general similarity searches in multi-attribute sequences (Kahveci et al., 2002, Vlachos et al., 2002, Wang et al., 2000, Lee et al., 2003, Goldin, Kanellakis, 1995).

As mentioned earlier, SCENS, is a trusted third party system for managing information requests, negotiation histories, exchanges and usage. SCENS identifies exceptional events, such as the need to collect additional information or the violations of usage conditions that occur outside the system. The challenge here is incorporating strategies into the system that properly represent the laws and restrictions of a given government system.

At Dartmouth we are currently creating a prototype SCENS for two types of data: (a) A **software vulnerabilities database** to create a prototype negotiation-based sharing system. This includes the precise conditions required for an attacker to exploit the vulnerability of a software system as well as information about discovery, systems affected, and other data. (b) A neuro-informatic database that contains rich information, ranging from structural and functional brain data and spatiotemporal data tracking tumors, lesions, or other brain changes.

Closing remarks

Negotiation-based sharing is a key aspect of any e-government system that wants to ensure democratic principles. Challenges in creating computational infrastructures for such sharing are both technical and non-technical, the latter being the harder to solve and needing novel incentive schemes. Assessing the quality of e-government information is dependent on building trust on the safety and goodness of a negotiation-based sharing system. Encoding European laws is a challenge with all the different nations involved. A negotiation system that includes the usage requirements of the data being shared is essential. As e-government involves large-scale information sharing, it must do so in a scalable way and the SCENS metadata-based description of information makes sense. It offeres economy of effort that helps reach accurate decisions within the e-government paradigm.

References

Bishop M., "Templates and DTD for Vulnerabilities," http://nob.cs.ucdavis.edu/doves

Business Wire, (2003) "Carriersnet Proposes Anti-Terrorist International Cargo System To EU", March 24, 2003, http://www.findarticles.com/cf_0/m0EIN/2003_March_24/99103298/p1/article.jhtml?term=%2Bterrorism+%2BEU

Dettmer J., (2002) "Hiding holes in financial war on terrorism", Insight on the News. March 25, 2002 http://www.findarticles.com/cf_0/m1571/11_18/84184999/print.jhtml

Ding H., (2000) "WebNS Web-based Negotiation System," http://ecomlab.mcmaster.ca/webns/

Donnelly C., (2003) NATO Speeches, NATO HQ, 5 June 2003, Video Interview http://www.nato.int/docu/speech/2003/s030605b.htm ; Updated: 05-Jun-2003.

Gold S., (2001) "Echelon Spying Network Exists, EU Committee Says", Newsbytes News Network, http://www.findarticles.com/cf_0/m0NEW/2001_Sept_5/77848781/p1/article.jhtml?term=%2Bterrorism+%2BEU

Goldin D. Q., and Kanellakis P. C., (1995) "On Similarity Queries for Time-Series Data: Constraint Specification and Implementation," presented at The 1st International Conference on Principles and Practice of Constraint Programming, Cassis, France, 1995.

Goodwin B., (2003) "EC forms a single cyber security agency for Europe". Computer Weekly, Feb 13, 2003

ICAN Systems Inc., (2003) "SmartSettle," http://www.oneaccordinc.com/

Joint US/EU ad hoc Agent Markup Language Committee (Dean M., chair), (2001) "DAML+OIL language specification," http://www.daml.org/2001/03/daml+oil-index, 2001.

Kahveci T., Singh A., and Gurel A., (2002) "Similarity searching for multi-attribute sequences," presented at Scientific and Statistical Database Management, 2002. Proceedings. 14th International Conference on, 2002.

Kersten G. E. and Noronha S. J., (1997) "Supporting International Negotiation with a WWW-based System," Interneg, Research Report INR05/97, 1997.

Kersten G. E. and Noronha S. J., (1998) "Negotiation Support Systems and Negotiating Agents," Interneg, Research Report INR02/98, 1998.

Lee S.-L., Chun S.-J., Kim D.-H., Lee J.-H., and Chung C.-W., (2003) "Similarity search for multidimensional data sequences," presented at Data Engineering, 2000. Proceedings. 16th International Conference on, 2000.

Makedon F., Ford J. C., Shen L., Steinberg T., Saykin A. J., Wishart H. A., and Kapadakis S., (2002) "MetaDL: A Digital Library of Metadata for Sensitive or Complex Research Data," presented at European Conference on Digital Libraries (ECDL2002), Rome, Italy, 2002.

Makedon F., Kapadakis S., Steinberg T., Ye S., and Shen L., (2003b) "Data Brokers: Building Collections Through Automated Negotiation," Dartmouth College Computer Science Department, Hanover, NH, Technical Report DEVLAB-SCENS-03-02, March 2003.

Makedon F., Ye S., and Zhao Y., (2003a) "On the Design and Implementation of a Web-based Negotiation System," presented at 9th Panhellenic Conference in Informatics (PCI2003), Thessaloniki, Greece, 2003.

Makedon F., Ye S., Steinberg T., Zhao Y., Xiao Z., and Sudborough B., (2003c) "A Security Incident Sharing and Classification System for Building Trust in Cross Media Enterprises," presented at International Conference on Cross-Media Service Delivery (CMSD-2003), Greece, 2003.
Sun Microsystems, (2003a) "JavaServer Pages Specification," http://java.sun.com/products/jsp/download.html#specs.
Sun Microsystems, (2003b) "Java Servlet Specification," http://java.sun.com/products/servlet/download.html#specs.
Sun Microsystems, (2003c) "Java Web Services Developer Pack," http://java.sun.com/webservices/webservicespack.html.
United Kingdom Home Office, (2003) www.homeoffice.gov.uk/terrorism
Vlachos M., Kollios G., and Gunopulos D., (2002) "Discovering similar multidimensional trajectories VO," presented at Data Engineering, 2002. Proceedings. 18th International Conference on, 2002.
Wang C., and Sean Wang X., (2000) "Supporting content-based searches on time series via approximation," presented at Scientific and Statistical Database Management, 2000. Proceedings. 12th International Conference on, 2000.
Ye S., Bishop M., Makedon F., Steinberg T., Ford J. C., Shen L., and Wang Y., (2002b) "Security Concerns in Negotiation Systems," Dartmouth College Computer Science Department, Hanover, NH, Technical Report DEVLAB-SCENS-02-02, November 2002.
Ye S., Makedon F., Ford J. C., Shen L., Steinberg T., and Wang Y., (2002c) "An open negotiation system with a web service based implementation," Dartmouth College Computer Science Department, Hanover, NH, Technical Report DEVLAB-SCENS-02-03, December 2002.
Ye S., Makedon F., Ford J. C., Shen L., Steinberg T., Wang Y., and Kapadakis S., (2002a) "A Negotiation Framework for Secure Data Sharing," Dartmouth College Computer Science Department, Hanover, NH, Technical Report DEVLAB-SCENS-02-01, October 2002.
Ye S., Makedon F., Steinberg T., Shen L., Ford J., Wang Y., Zhao Y., and Kapidakis S., (2003) "SCENS: A system for the mediated sharing of sensitive data," presented at Third ACM/IEEE Joint Conference on Digital Libraries, Houston, TX, 2003.