

Agency Interoperation for Effective Data Mining in Border Control and Homeland Security Applications¹

Nabil R. Adam, Vijayalakshmi Atluri, Rey Koslowski, Vandana P. Janeja, Janice Warner, Aabhas Paliwal

CIMIC and MSIS Department, Rutgers University

{adam,atluri,vandana,jwarner,aabhas}@cimic.rutgers.edu, rkoslowski@earthlink.net

1. PROJECT SUMMARY

US Customs embarked on a major modernization initiative of its Information Technology systems. Drawing in data from Customs trade systems, targeting inspectors review manifest information as well as strategic and tactical intelligence to determine which shipments and containers are “high-risk.” This entails a considerable level of communication and data sharing between various government agencies. Our NSF funded project, funded through the digital government program, aims at providing decision makers with the ability to extract and fuse information from multiple, heterogeneous sources in response to a query while operating under a decentralized security administration. Based on the idea of “Smart Borders”, the system will utilize data available from different agencies, ports and customs divisions to supplement the profiling by targeting towards anomalies, and detect various flags raised by non-conforming shipments or abnormal behavior of inbound cargos and raise a combination of alerts. This project proposes generalizable development work, which devises solutions to accomplish secure interoperation among different government agencies. The output of this project would ideally enhance the security aspect of the Automated Commercial Environment (ACE) system by incorporating the concept of semantic interoperability, anomaly detection and subsequent spatial and geographical visualization of information that can help Customs inspectors make better decisions. This project is a collaboration between the industry, government and the academia, providing the opportunity to directly influence the practical needs of the government agency, in this case the US Customs.

2. RESEARCH ACTIVITIES

The impact of this project is in many dimensions. (1) It devises solutions to accomplish secure interoperation among different government agencies. (2) It advances fundamental research in Data interoperability, data mining, decentralized security administration, and the diplomacy and politics. (3) As a result of the partnership SAP, the supplier of software to the Customs Modernization Program and contractor to IBM, which is the prime contractor for eCustoms Partnership (eCP) implementing Customs Modernization, it provides the opportunity to directly influence the practical needs of US Customs. (4) The research and development work in this project is generalizable and therefore can serve as a reference model to be adopted by related homeland security agencies.

Our work in the area of *coalition based access control model* (CBAC)[1], comprised of three layers: coalition, role and user-object. Our model enables translation of coalition level policies to implementation level access control in a manner similar to that of

the layers of the TCP/IP protocol. We presented a *coalition policy translation protocol* that allows the implementation level access control details to be piggy-backed as the access control policy percolates to the coalition level, and similarly, as the coalition level policy trickles down to the implementation level. Under our approach, a user’s request to access an object belonging to another coalition entity is automatically translated by employing an approach that considers attributes associated with user credentials and objects. CBAC assumes that every pair of coalition entities have agreed on high level coalition policies in advance. To rectify this, we have proposed a *dynamic coalition-based access control* (DCBAC) model in [9]. To cater to true ad-hoc dynamic coalitions, we employ a *coalition service registry* (CSR) where coalition entities publicize their coalition level access policies. Any coalition entity wishing to access a specific resource of another coalition entity can obtain a *ticket* by submitting its entity credentials, which are subsequently evaluated by the CSR. Access is based on the credentials possessed by coalitions as well as subjects. Translation is performed in our DCBAC through a *mapper layer* that accurately computes the credentials required by a user to access a resource. We have also demonstrate how the access policies, at the coalition level and resource level, can be specified in XML and be evaluated. In [2], we extended the notion of delegation to allow for *conditional delegation*, where the delegation conditions can be based on time, workload and task attributes. When workflow systems entertain conditional delegation, different types of constraints come into play, which include authorization constraints, role activation constraints and workflow dependency requirements. We address the problem of assigning users to tasks in a consistent manner such that none of the constraints are violated.

Our work in the area of collusion set detection[6] poses the general problem of Collusion Set Detection (CSD): identifying sets of behavior that together satisfy some notion of “interesting behavior”. We focused on an interesting subset of the problem (called CSD’), by restricting our attention only to outliers. We proposed a novel technique using semantics to identify collusive behavior among outliers. Thus, in essence, we identified an important general problem and propose a solution to an important subset of the problem. Our work on interrelationship identification [4] focuses on identification of interrelationships across domains or groups based on the semantics driven by individuals rather than the domain semantics as in[6]. Our work on alert management system [5] proposed to generate meaningful alerts from alarms received from different sensors. The alert generation module of our system (i) flags and eliminates potential false positives by characterizing the region into uniformly behaving neighborhoods, (ii) generates aggregated alerts from the alarms by employing density based clustering techniques and identifying the overlap among clusters, and (iii) identifies the dynamic flow of the alerts

by integrating scientific models that characterize the behavior of sensor parameters. Once the alerts are generated our customized dissemination module disperses the alerts on the need-to-know basis to the individuals and agencies involved. This module adheres to the National Incident Management System (NIMS) and the National Response plan (NRP) protocols. To implement these protocols, we utilize the Common Alerting Protocol (CAP), which is an XML nonproprietary data interchange format. Finally, our GIS module displays the alerts through a user-friendly interface. Our work on Linear semantic scan statistics[3], identifies anomalous windows along a linear trajectory that reflects unusual rate of occurrence of a specific event of interest. Such examples include: determination of places with high number of occurrences of road accidents along a highway, leaks in natural gas transmission pipelines, pedestrian fatalities on roads, etc. We proposed a Linear Semantic Scan Statistic (LS3) approach to identify such anomalous windows along a linear trajectory.

Our work in web services [8] combines an approach for composing Web Services on the semantic web, using OWL-S for explicitly describing the semantics to Web Services. We proposed an OWL-S based approach for the automatic composition of Semantic Web Services and present a technique to generate composite services from high-level declarative descriptions. We discussed its implementation for the shipment monitoring application, an open, multimodal end-to-end tracking and tracing system in the Border Control domain based on Semantic Web. Our work in the area of diplomacy and politics has focused on International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics[7]. Several presentations have been drawn on this, at Columbia Law School, the Centre for History and Economics, Kings College, Cambridge University and the Global Equity Initiative of Harvard University, Stockholm, Ontario Business Climate Deputies' Committee (BCDC), Ministry of Economic Development and Trade, Toronto. A briefing on U.S. Homeland Security and Border Control Information Technology was made for US Dept. of State International Bureau of Educational and Cultural Affairs Visitors Program at Woodrow Wilson International Center for Scholars, Washington DC. Rey Koslowski attended the 2004 US Customs and Border Protection Trade Symposium. Spoke with Rod McDonald, Customs and Border Protection Acting Assistant Commissioner, Office of Information and Technology, regarding contributing Rutgers "thought leaders" to CBP projects and expanding cooperation with Rutgers to include internship opportunities for Rutgers students. Koslowski also met the Secretary General of the World Customs Organization, Michel Danet and agreed that Rutgers University would join a network of universities conducting research on security and world trade that the WCO is currently planning to establish. Koslowski will work with the WCO on building this university network while he conducts policy research at the WCO headquarters in Fall 2005.

3. PROJECT PARTICIPANTS

The collaborating researchers include CIMIC, Rutgers Univ.: Nabil R. Adam and Vijay Atluri, Dept. of Political Science, Rutgers Univ.: Rey Koslowski, Univ. of Illinois at Chicago: Robert Grossman, National Center for Data Mining, David Hanley (Technical staff), Columbia Univ.: Vasileios Hatzivassiloglou and Kathleen R. McKeown, Dept. of Computer Science. Industry partners include Christof Bornhoevd, Tao Lin-SAP Corporate Research Labs, Domain experts include Dr.

Stephen E. Flynn-Council on Foreign Relations, C.J. Chang-Foreign Operations Division-U.S. Department of Homeland Security, Luis R. Cortes-Chief of Intelligence, Office of National Risk Assessment (ONRA), Transportation Security Administration (TSA), James R. Sutton-Managing Associate of McManis Associates, Inc. and former Senior Intelligence Research Specialist for the U.S. Department of Justice on the Foreign Terrorist Tracking Task Force. Student participants include Rutgers Univ.: Vandana Janeja, Janice Warner, Columbia Univ.: Melania Degeratu and, Univ. of Illinois at Chicago: Chetan Gupta, Jorge Levera.

4. SUCCESS AND IMPACT OF THE PROJECT

As a result of this project, several other collaborations have been generated between Rutgers and SAP. These include the RFID, data interoperability and privacy project, with SAP. Nabil Adam gave a talk at the SAP Research Center in Karlsruhe, Germany, in November 2004. This project has resulted in two on-going Ph.D. dissertations. The research publications generated as direct results of the first and second year of funding of this project are available: <http://cimic.rutgers.edu/~vandana/BorderControlPublications.htm>.

REFERENCES

- [1] V. Atluri and J. Warner, "[Automatic Enforcement of Access Control Policies Among Dynamic Coalitions](#)", International Conference on Distributed Computing & Internet Technology, Bhubaneswar, India, Dec 2004 (Acceptance ratio: 51/211).
- [2] V. Atluri and J. Warner, "Supporting Conditional Delegation in Secure Workflow Management Systems", ACM Symposium on Access Control Models and Technologies, June 2005, Stockholm, Sweden (Acceptance ratio: 19/90).
- [3] V.P. Janeja and V. Atluri, "LS3: A Linear Semantic Scan Statistic Technique for Detecting Anomalous Windows," ACM Symposium on Applied Computing, March, 2005
- [4] V.P. Janeja and V. Atluri, "Semantic based augmentative discovery of interrelationships," Ongoing towards DAWAK 05
- [5] V. Janeja, V. Atluri, A. Goma, N. Adam, C. Bornhoevd and T. Lin., "DM-AMS: Employing Data Mining Techniques Alert Management", NSF National Conference on Digital Government, 2005. Atlanta, Georgia (Acceptance ratio: 15/38)
- [6] V. Janeja, V. Atluri, J.S.Vaidya, N. Adam, "Collusion Set Detection through Outlier Discovery", IEEE Intelligence and Security Informatics, 2005. Atlanta, Georgia
- [7] R. Koslowski, "International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics," Intl. Studies Assoc., Montreal, Mar. 17-20, 2004
- [8] A.V Paliwal, N. Adam, C. Bornhvd, J.Schaper, Semantic Discovery and Composition of Web Services for RFID Applications in Border Control Semantic Web Services: Preparing to Meet the World of Business Applications a workshop at The Third International Semantic Web Conference Nov, 2004
- [9] J. Warner, V. Atluri and R. Mulkamala, "A Credential-based Approach for Facilitating Automatic Resource Sharing among Ad-hoc Dynamic Coalitions", IFIP WG 11.3 conference on Data and Application Security, August 2005, submitted February 2005.

¹ Supported by the National Science Foundation under grant IIS-0306838.