Goods Movement Security: *An Information Technology Problem*

Jens Pohl, Ph.D., Executive Director
Collaborative Agent Design Research Center (CADRC)
California Polytechnic State University, San Luis Obispo, California, USA

Abstract

This paper discusses the security problems associated with the movement of goods across international in-land borders and at ocean ports. The author proposes an information technology solution approach that is based on the *profiling* of international shipments. The collection of data describing the end-to-end movement of a shipment from the initial acquisition transactions, throughout the various transshipment stages, to the final delivery, allows intelligent software to assist customs and homeland security officials to determine the risks associated with the shipment long before it reaches the inspection point. The technical basis and architecture of the SecureOrigins™ software system is described. Designed for the border traffic between the United States and Mexico, this system is an ontology-based application that incorporates collaborative software agents with reasoning capabilities.

Keywords

Agents, artificial intelligence, computer software, containers, goods movement, international borders, ontologies, ports, profiling, SecureOrigins, security, shipments.

The Goods Movement Security Problem

Since September 11, 2001 the United States (US) has been faced with a serious goods movement security dilemma: how to prevent the smuggling of nuclear, biological and chemical weapons into the US without seriously impacting the flow of shipments across its borders and through its ports? Realistically, every container entering the US must be viewed as a potential weapon of mass destruction, every conveyance carrying the container as a delivery device, and every port of entry and inland destination as a potential target. With individual ships capable of carrying up to 6,000 containers each, more than six million container shipments entered the US in 2001. At an approximate value of (US)$60,000 per container, this constitutes an annual trade volume of around (US)$360 billion.

Physical intrusive inspection of more than a very small percentage (i.e., less than 3%) of container shipments at the port of entry would have serious national economic implications and is therefore not practical. From a business perspective, speed and cost are the critical criteria for the selection of transportation routes and shippers. While logistic costs in the US have declined from 20% to about 15% of the Gross Domestic Product over the past two decades, the inventory (i.e., goods in storage) cost still amounts to some $400 billion. The potentially serious impact of increasing the rate of full physical inspection at the point of entry is easily demonstrated by the following example. Manual intrusive inspection of a 3,000 container ship (assuming an optimistic inspection period of only 60 minutes per container) would add at least two man-years of labor to the unloading operation. Yet, an additional 1% burden on logistic costs (i.e., increased inventory due to slower processing) would cost the US economy around (US)$25 billion (or the equivalent of 15,000 lost jobs) annually.

A similar security problem exists at the US-Canada and US-Mexico borders. For example, El Paso (TX) and Juarez (Mexico) are twin border communities located in close proximity to each other on either side of the US-Mexico border. Over the years five major industrial parks have formed within 10 miles of the Mexican side of the border, driven to a large extent by US commercial interests. Many US companies have found it profitable to locate manufacturing and assembly plants in Mexico and take advantage of significantly lower labor costs. This cross-border commercial relationship generates a great deal of goods shipment traffic across the border.

On any given day approximately 3,000 trucks transport goods and parts to and from the Juarez industrial parks across the US-Mexico border. These trucks together with other vehicular traffic pass through three congested Border Check Points. Waiting times for trucks can exceed three hours, leading to loss of time, increased shipping costs, environmental pollution, and frustration. However, even more importantly the current shipment control processes do not assure a reasonable level of security. There is an urgent need for a greatly improved border control process to provide an adequate level of security with a minimum impact on the flow of cross-border vehicular traffic. Typically, the principal elements of such a solution should include the following:

1. Electronic capture of reliable and complete shipment documentation at the point of departure through: agreements with shippers, goods owners and local Mexican authorities; sealing of shipments with approved mechanisms and

devices; wireless electronic data entry devices; barcodes and smart tags (i.e., radio frequency identification devices or RF-Tags); web-cameras; and data integration within a shared database facility.

2. Tracking of shipments utilizing wireless Global Positioning System (GPS) devices, automatic electronic sensing gates, and web-camera surveillance facilities.
3. Near real-time processing of shipment information by computer software to identify anomalies and select higher risk shipments for full inspection at the point of entry. In addition, selection of random shipments for full inspection at the point of entry as a basis for the dynamic modification of agent rules as results warrant.
4. Automatic identification of shipments and drivers at the point of entry through bar codes, smart tags, web-cameras, and other non-invasive technology applications.
5. Thorough inspection of selected shipments, in designated areas, utilizing physical inspection technologies.
6. Continuous shipment information tracking to the completion of each shipment transaction.
7. Automatic maintenance of historical records of shipments to serve as a basis for analysis, trend identification, and 'what if' explorations.

Over the past several years goods movement security at US ocean ports and international borders has increasingly focused on two strategies as a countermeasure. The US Customs Service has been exploring ways of extending its Trusted Shipper program. This program is essentially based on the concept that systematic security measures executed by a compliant and reliable shipper at the point of departure will not require inspection at the point of entry. Under this first strategy the Customs Service defines a set of requirements that a *trusted shipper* must adhere to, and then strives to the best of its ability to verify that the shipper is and continues to be compliant with these requirements. The second strategy relies on advances in non-intrusive inspection technologies (Mallon 2001). Such technologies include neutron and gamma ray scanning, motion detection, as well as radiological and chemical sniffing devices. Typically, this kind of inspection can be performed in seconds while the container is in motion between gates, or in one or two minutes in a special drive-through en route test station (Fig.1). While this second strategy is certainly attractive and promising it is as yet expensive, the necessary devices are not available in the required quantities, and the technology lacks proven reliability.

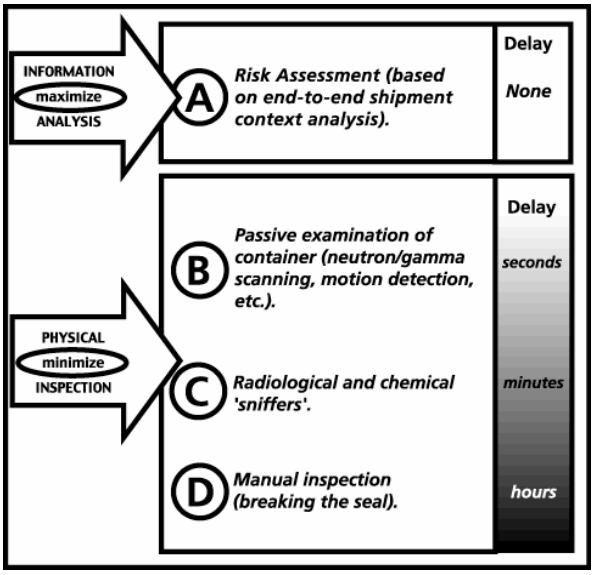

Fig.1: Inspection delay levels

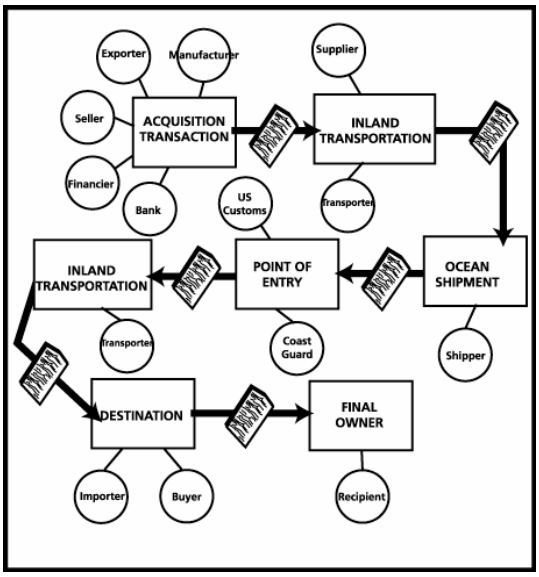

Fig.2: End-to-end shipment process

Clearly, any control action at the point of entry, such as inspection, has only a small probability of preventing a determined terrorist or contraband act. Accordingly, it is now well recognized that the interdiction of terrorist activities in the realm of goods movement into and out of the US cannot start at the border, but must commence with the shippers and their customers and the collection of the data representing the physical and transactional beginning of the goods acquisition chain. In this respect goods movement security is firstly an information technology problem and only secondly a physical border and port problem (Quartel 2002). However, current intelligence gathering and data collection processes are seriously encumbered by the overwhelming volume of data involved, the fragmented and disconnected nature of the data sources, the limitations of current automated information extraction and analysis capabilities, and ownership barriers. There is an urgent need to utilize more advanced computer software systems that operate at the *information* rather than data level, with automatic reasoning and analysis capabilities.

Such *information-centric* computer software technology has been developed over the past several years to elevate computer-based data-processing to intelligent information management. In information-centric decision-support systems software modules (referred to as agents) are able to automatically reason within the context of an internal information model (rather than data representation) to collaboratively assist each other and human operators in near real-time monitoring of current events, planning for future events, and the analysis of alternative courses of action (Pohl 2001).

The *Profiling* Solution Approach

The information technology solution approach to goods movement security relies on the concept of *profiling* all international shipments. In other words, it utilizes information technology to capture the end-to-end context of each shipment so that software agents operating in a collaborative mode can automatically perform at least the initial filtering, evaluation and profiling functions. In general terms the necessary context includes the data used by commerce to achieve efficiency, the data obtained through the in-transit monitoring of shipments and the detection of apparent anomalies, the relevant law enforcement data on both sides of the border, and at least some elements of national security intelligence.

The end-to-end supply chain for a complete shipment transaction commences with the initial acquisition of the product to be shipped to the US (Fig.2). For example, the acquisition transaction data that is relevant to the construction of the shipment profile includes not only the purchasing documents, but also the bank statements that describe the financial transactions and even the documents that define the financing agreement itself. Certainly the monitoring and tracking data related to the ocean voyage and the inland transportation on both sides of the border is of high value, particularly if the shipment process is based on trusted source concepts. Finally, data related to the destination and the final owner constitute important contributions to a complete shipment profile. Relevant data collection questions include the following:

- What kind of cargo does this shipment consist of?
- Where did the shipment originate?
- Who purchased these goods?
- Who sent the shipment?
- Where is the shipment going?
- Who are the shippers on both sides of the border?
- What was the planned and actual shipping route?
- How long has the shipment been in transit?
- Who will receive the shipment?
- What is the history of all parties who touched the shipment?

The focus must be on profiling the shipment first, and then the container. Many of the required data elements are already available in existing documents such as: the shipper's Letter of Instructions; the various commercial invoices; the Certificate of Origin; and, the carrier's Bill of Lading. Additional data elements that are needed for building a complete and reliable shipment profile include: financial data such as letters of credit and bank reports; inland transportation records from both sides of the border; and, in-transit monitoring data for identifying transshipment route changes, delays, and other events. In summary, the following guiding principles constitute the overall framework within which the solution approach to goods movement security can be formulated:

1. Move the security process to the source of the shipment and provide incentives for complete and accurate data.
2. Provide physical protection of the in-transit shipment and transportation infrastructure (e.g., sealing standards, tracking, and in-transit visibility).
3. Streamline the point of entry processing, including the provision of express lanes, shipper incentives, and indemnification options.
4. Implement shipment and container profiling through data capture and the application of intelligent information management technology.
5. Automatically select higher risk shipments and containers for the appropriate level of inspection, by taking advantage of collaborative software agents operating in an information-centric decision-support system environment. At the same time select random inspection samples and dynamically modify the profile building rules used by the software agents based on inspection results.
6. Progressively improve the physical inspection hardware devices with the objective of increasing reliability, and decreasing inspection time and cost.

It must be recognized that ports and border checkpoints are part of the last line of defense. In other words, *the decision to inspect or not to inspect a container and the level of inspection should be made well before a shipment reaches the port of entry*. This is possible only if the full context of the shipment is available for consideration.

The Technical Approach

The technical approach utilized by the SecureOrigins system solution incorporates intelligent agent technology to provide a *shadow staff* of digital assistants (i.e., software agents) to responders and coordinators at all nodes within an extended, distributed, intelligent homeland security network. These assistants analyze and categorize incoming signals and data, and then issue warnings and alerts as appropriate. The digital assistants manipulate the incoming data within an internal information-centric representation framework to publish statements of implication, and if so empowered, proceed to develop plans for appropriate action. Digital assistants will receive status reports, track shipments, incorporate suitable and available assets in plans, and provide appropriate updates on location and security risks. Others will track the path of incidence and provide appropriate graphic and textual updates for action. Finally, the assistants will manipulate incoming signals, identify significant events (i.e., changes), and modify proposals to meet the changing situation as it develops.

Existing data-centric systems can become clients of such an agent-based system through the use of translators that map the data model in one system to the information model of the other and allow a two way exchange. Such translators have been successfully demonstrated by military organizations for linking legacy data-centric systems to intelligent command and control systems. The technology is inherently scalable and allows for the creation and interconnection of multiple object serving communication facilities.

Conceptually, an intelligent shipment tracking and control network calls for the seamless merging of an intelligent information management facility with existing data sources. This can be achieved with an *information-centric* architecture that consists essentially of two components (Fig.3): a data-centric Data Capture and Integration Layer that incorporates linkages to existing data sources; and, an Intelligent Information Management Layer that resides on top of the data layer and utilizes software agents with automatic reasoning capabilities, serving as decision-support tools.

The Intelligent Information Management Layer of the SecureOrigins system architecture (Fig.3) utilizes intelligent software agents capable of collaborating with each other and human operators in tactical and logistical command and control environments. Typically such intelligent systems are based on software development frameworks, such as the ICDM (Integrated Cooperative Decision Making) and TIRAC (Toolkit for Information Representation and Agent Collaboration) software development frameworks previously used by the CADRC Center for the development of military and commercial systems, respectively (Pohl et al. 2004).

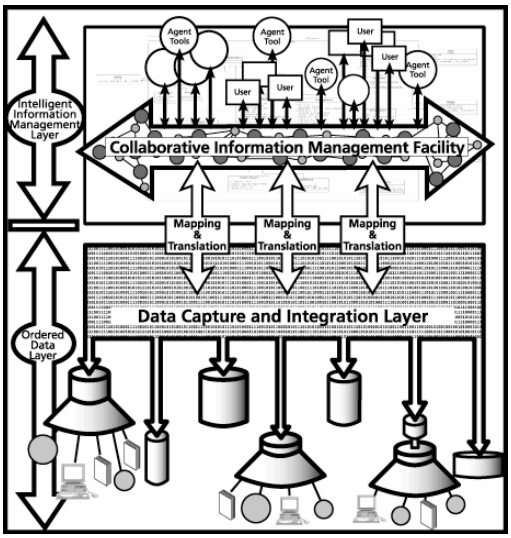

Fig.3: Conceptual system architecture

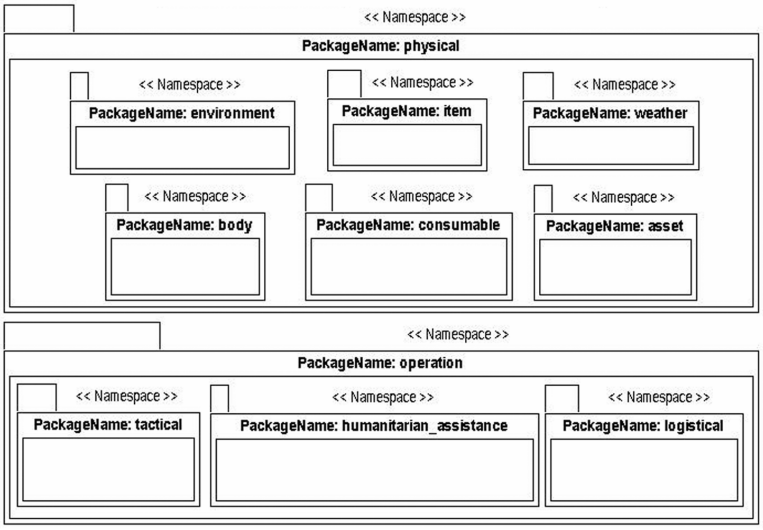

Fig.4: Typical ontology domains

Data Capture and Integration Layer: The bottom layer of the SecureOrigins system takes the form of an operational data store and/or Data Warehouse, implemented within a commercial off-the-shelf relational database management system (RDBMS). This data categorization facility integrates data extracted on a periodic basis from several external sources into a *goods shipment* specific data schema. The design of the data schema is closely modeled on the structure of the ontology of the Intelligent Information Management Layer to minimize the required data-to-information and information-to-data mappings between these two system layers.

In conformity with normal Data Warehouse design practices the SecureOrigins Data Capture and Integration Layer incorporates the following four characteristics:

- It is subject-oriented to the specific business processes and data domains relevant to the shipment of goods across US borders.
- It is integrated so that it can relate data from multiple domains as it serves the data needs of the analysis functions performed by collaborative agents in the Intelligent Information Management Layer.
- It is periodically updated through its linkage to external data sources.
- It is time-based to support the performance of analyses over time, for the discovery of patterns and trends.

A multi-tier architecture is used to logically separate the necessary components of the data layer into levels. The first tier is the RDBMS, which ensures the persistence of the data level and provides the necessary search capabilities. The second tier is the service level, which provides the interface to the data level and at the same time supports the data access requests that pass through the mapping interface from the Intelligent Information Management Layer to the Data Capture and Integration Layer. It is designed to support request, response, subscribe, and publish functionality. The third tier is the control level, which routes information layer and user requests to the service level for the update, storage and retrieval of data. Finally, a view layer representing the fourth tier serves as a user-interface for the Data Capture and Integration Layer.

Information Management Layer: The Intelligent Information Management Layer of the SecureOrigins system is designed as a TIRAC-based decision-support application. The initial development of the TIRAC toolkit was undertaken with the objective of providing a formalized architecture together with a set of development and execution tools that could be utilized to design, develop, and execute agent-based, decision-support applications (Pohl et al. 2004). The core element of this process is the development of an ontological framework to provide a relationship-rich model of the various system and application domains in which the proposed application is required to operate. Based on a three-tier architecture, TIRAC incorporates technologies, such as distributed-object servers and inference engines, to provide a framework for collaborative, agent-based decision-support systems that offer developmental efficiency and architectural extensibility.

The TIRAC software development framework is based on a three-tier architecture that clearly distinguishes among information, logic, and presentation. These tiers are represented by the three major components comprising the TIRAC™ model: the *information tier* consisting of a collection of information management servers (i.e., Information Server, Subscription Server, etc.); the *logic tier* represented currently by an Agent Engine; and, the *presentation tier* or Client User Interface. Each of these components functions in an integrated fashion to form a comprehensive agent-based decision-support execution framework. This framework allows multiple human decision-makers to solve complex problems in a collaborative fashion obtaining decision-support assistance from a collection of heterogeneous on-line agents.

Decision-support applications can be designed and developed through a series of high-level models describing the information structure and analytical logic. High-level classes can be identified through a series of Unified Modeling Language (UML) class diagrams, forming a comprehensive information object model (Fowler and Scott 1997). Such a model describes the application specific design and problem space as a collection of high-level objects complete with attributes and relationships. This is essentially the same high-level description of application information that is required for agent-based, decision-support applications.

The analytical reasoning applied to this information can be described in terms of a methodology suitable for representing object-based logic, such as a series of rules (Hayes-Roth et al. 1983). Each of these rules identifies both a condition and a corresponding action to take upon the satisfaction of that condition. Both the condition and action components of these rules can be described in terms of the information representation (i.e., object model) of an application. In other words, conditions can be represented as a series of constrained references to object attributes strung together with logical and relational operators. At the same time, the corresponding rule action is itself described in terms of a series of basic manipulation functions (i.e., create, modify, delete) executed against the information object model. When the informational state described in the condition section of the rule occurs, the corresponding action component will modify or produce information thus creating an entirely new informational state. This new state may in turn trigger other rules to execute in a similar fashion. Although not all logic can be represented in this manner, experience has shown that this approach can be applied to a significant portion of analytical reasoning found in decision-support applications.

Structure of the SecureOrigins Ontology

The underlying ontology of the Intelligent Information Management Layer in the SecureOrigins application is divided into several somewhat related domains (Fig.4). While some of these domains describe application-specific events and information (e.g., goods movement transactions, shipping routes, and so on) others describe more general, abstract notions (e.g., event, threat, view, agent). The goal in developing such an ontology is to abstract general, cross-domain notions into high-level domain models. As such, these descriptions can be applied across several application sub-domains. More domain-specific, concrete notions can then be described as extensions of these high level models.

Accordingly, the ontology of the Intelligent Information Management Layer has been modeled to include several primary meta-characteristics. Through inheritance, these meta-characteristics are propagated to extended and more specific ontological components. One of these meta-characteristics is the property of being *trackable*. This characteristic has been introduced at the 'physical.Mobile' level. Through inheritance, any entity that is a kind of 'physical.Mobile' automatically receives the property of being *trackable*.

A second meta-characteristic relates to the dispensability of an item. This property is represented at the 'physical.item.Item' level. Similar to the *trackable* characteristic, anything that is a kind of 'physical.item.Item' automatically receives the quality of being dispersible or *suppliable*. In addition, as an extension of 'physical.Mobile' such *suppliable* items are also *trackable*. Together, these two meta-characteristics provide an effective foundation for assigning basic logistical and tactical functionality to the application-specific domains identified within the ontology.

While meta-characteristics are only implicitly represented in an ontology, other additional notions may be represented explicitly in the form of object classes. For example, two such notions in the SecureOrigins ontology are *Container* and *Empowerable*. A *Container* holds (i.e., contains) components. In fact, a *Container* can be thought of as a dynamic set of components. There is no inherent order imposed. However, while the contents of *Containers* may be very different all *Container* objects have a common derivation. An *Empowerable* object is one that can be dynamically embodied, or enhanced with additional information, knowledge, or capabilities. This is intentionally a very open-ended notion allowing for unconstrained exploration into various potential 'powers' that can be imparted to an object.

The SecureOrigins Agents

Rule-based agents residing in the Intelligent Information Management Layer of the SecureOrigins system automatically analyze the particular data pertaining to each truck or convoy in the context of the ontology. Their inferencing capabilities exist at a monitoring and largely reactive level, and at a higher consequential level. Typical lower level inferences include: warning that hazardous material is en route; warning that a truck has not reached a waypoint within a certain time limit; alert that a truck has not reached a waypoint within a more critical time limit; warning that a truck is near a higher risk area; alert that a truck has stopped for more than a certain time near a higher risk area; warning that a replacement driver of low risk is driving a truck; alert that a replacement driver of elevated risk is driving a truck; and, alert that the loaded weight of a truck does not match the final weight at the border check point.

At the higher level more sophisticated agent inferencing capabilities that are currently in various stages of implementation include warnings and alerts that a particular combination of circumstances involving encyclopedic data and truck-based/convoy-based confirmation data entered at waypoints and checkpoints constitutes a higher risk situation. Examples include, a particular driver transporting certain kinds of goods, the avoidance of a particular route under certain weather conditions, and so on.

References

Fowler M. and K. Scott (1997); 'UML Distilled: Applying the Standard Object Modeling Language'; Addison-Wesley, Reading, Massachusetts.

Hayes-Roth F., D. Waterman and D. Lenat (eds.) (1983); 'Building Expert Systems'; Addison-Wesley, Reading, Massachusetts.

Mallon, L. G. (2001); 'Deconstructing the Pre-Technology Driven paradigm for Border Security: A Survey of Port of Entry and Exit Inspection Process and Technology'; Inspection Technology Phase I Report, Center for the Commercial Deployment of Transportation Technologies, California State University Long Beach, California.

Pohl J., K. Pohl, R. Leighton, M. Zang, S. Gollery and M. Porczak (2004); 'The TIRAC Development Toolkit: Purpose and Overview'; Technical Report CDM-17-04, CDM Technologies, Inc., San Luis Obispo, California, USA (August).

Pohl, J. (2001); 'Information-Centric Decision-Support Systems: A Blueprint for Interoperability'; Proceedings of the Workshop on Collaborative Decision-Support Systems, Office of Naval Research (ONR) and Collaborative Agent Design Research Center (CADRC), Cal Poly (San Luis Obispo), Quantico, VA, June 5-7 (pp. 35-49). [Proceedings available from CADRC, Cal Poly (Bdg. 117T), San Luis Obispo, CA 93407; Phone: 805-756-1310]

Quartel, R. (2002); Testimony before the Senate Committee on the Judiciary Subcommittee on Technology, Terrorism and Government Information, on 'Securing Our Ports Against Terror: Technology, Resources and Homeland Defense'; February 26.