Semantics and Security: Applying OWL and RDF to Defense and Security Challenges

Steve **Hamby**

Semantics and Security: Applying RDF and OWL to Defense and Security Challenges

This presentation will address the recent interest in semantic web standards and discuss how these standards impact the defense, security and intelligence communities within the Federal Government. A variety of relevant standards will be discussed with a special focus on the Web Ontology Language (OWL) and Resource Description Framework (RDF). These standards enable the processing of the content and context of information rather than just the information itself. OWL, unlike HTML, is a language for applications rather than for humans, but when information shared through OWL is “translated” for human consumption, the depth and context of information is much deeper than with typical integration standards. This presentation will discuss several implementations of OWL and RDF within the specified communities and provide reasons why the approach was adopted. The case studies will include intelligence aggregation and processing, flight variance notifications, virtual knowledge repositories for structured and unstructured data, cargo inspection notifications, and others.

Table of Contents

1. Understanding the Standards and Terminology

This presentation will deal primarily with the Web Ontology Language (OWL) and Resource Description Framework (RDF). Both are standards defined by the World Wide Web Consortium (W3C) and are focused on describing context of data as opposed to the content. OWL explicitly and formally describes the meaning of terminology used in documents by defining vocabulary to describe properties and classes as well as relations between classes (e.g. disjointness), cardinality (e.g. "exactly one"), equality, richer typing of properties, characteristics of properties (e.g. symmetry), and enumerated classes. RDF is a datamodel for objects / resource and the relations between them that can be represented in XML syntax. Ontology is an explicit specification of concepts and relationships within a domain of knowledge. For purposes of this presentation, data is defined as observable bits and bytes, information is defined as related data, knowledge is defined as information in context of a particular domain, and understanding is defined as the ability for the receiver of knowledge to make a decision based on that knowledge. An example of these definitions can be demonstrated with a simple analogy with playing cards. The five cards you have in your hand are data. The fact that you have Ace, King, Queen, Jack and Ten of Spades is information. Knowledge is based on this information and the rules that in “crazy eights”, this hand is merely okay, but in “poker”, this is the best hand possible without wild cards. Understanding is the person holding the cards and playing poker should bet, since they will win.

2. Issues in Defense and Security

There exists several initiatives in the defense and security agencies to share data and information, and overall, the various agencies do a good job here. However, there are only a few initiatives that share knowledge and understanding. The use of RDF and OWL can assist these agencies with sharing knowledge and understanding. RDF and OWL can provide the context about data and information to create the knowledge. Defense and security related agencies have knowledge management solutions that are supply oriented. Restated, these systems are oriented to the person possessing knowledge to enable them to easily contribute into a knowledge base so that others can query that knowledge. However, the defense and security agencies need to “create” knowledge on demand. There may be pieces of information that assembled together, make the needed knowledge for an end user. RDF and OWL provide the markup necessary to relate these pieces into knowledge he end user needs.

3. How Defense and Security Agencies are Using Semantic Technologies … and Why

3.1. Notice to Airmen

A notice to an airman is a time and safety critical message that contains announcements about airspace or runway changes, such as closed or restricted, or issues about equipment or fuel to name a few. There are approximately 25,000 notices active at any given time. Airmen have to read these, determine the facts about them, and then determine if their flight is affected by the notice. If so, they have to make changes the necessary changes to their flight plan. By defining this knowledge domain as OWL ontology, they are able to automatically resolve any portion of the flight plan that is affected by an active notice. The system has processed over 3 million notices since going production in 2002. This system has improved the Air Mobility Command’s asset management and flight planning systems by automating the analysis portion of these notices and delivering the airmen the knowledge they need to make informed decisions.

3.2. Structured Professional Forums

A Structured Professional Forum (SPF) is simply a group or network of people that share a concern, a problem, or a passion about an object, and who deepen their knowledge of this object by interacting on an ongoing basis. The defense and security communities have adopted these to enrich knowledge available to systems. The SPF’s use ontology, and OWL and RDF specifically, to link these loosely coupled networks. This enables networked virtual communities and teams that manage their own knowledge better. More importantly, these networks weave together across domains to enable a network centric command integrating information and human capital across a network that delivers a competitive edge over security risks.

3.3. Intelligence Analysis

For many years, intelligence analysis operated from a collect, improve, analyze, share paradigm. During recent years, this paradigm has shifted to a collect, share, improve, analyze paradigm to increase the usefulness of intelligence gathered. The amount of intelligence gathered by our defense and security agencies is higher than ever before and growing rapidly. It is impossible to manually process the large amounts of data. OWL and RDF provide standard tools for defining metadata about intelligence information and relating this information to multiple domains. This makes it ideal for the problems in this space. One particular agency receives thousands of messages per day in raw text format. They use extraction engines to extract the relevant information and mark this metadata in an XML format. They use RDF metadata to relate this XML metadata to an OWL ontology that represents their domain of knowledge. This allows analysts to demand the information they require and for the reasoning / inference engines that act on the OWL and RDF markup to determine the appropriate knowledge that needs to be returned and return it in the user’s terminology.

3.4. Risk and Threat Analysis

U.S. Customs and Border Protection experiences risks on a daily basis. These range from terrorists crossing the border to plants and animals carrying diseases. To combat this, CBP created ontology for risks and import-export entities. This system automatically maps the relationships of risks that exist to cargo that an import-export entity may have that could be affected. Furthermore, because this knowledge is defined in a loosely coupled standard way, it is available for other users in other domains.

3.5. Virtual Knowledge Repository

A virtual knowledge repository aggregates data stored in backend systems using ontology with easily changed integration and aggregation rules. Physical models are mapped to information models expressed in OWL using RDF expressions. When a user queries the information model, the information aligned to that ontology with the various mapped data sources is returned to the user. This is an example of Enterprise Information Integration. It provides several agencies a low-risk, inexpensive solution for integrating their backend data using a powerful and flexible approach.

Biography

Steve **Hamby**
Software AG, Inc. [http://www.softwareag.com/]
11190 Sunrise Valley Drive
Reston
Virginia
20191
United States of America
steve.hamby@softwareagusa.com

Steve Hamby is an Architect for Software AG, Inc. He has 17 years' experience in the IT industry with the last 6 focused on XML applications. He is a frequent speaker at various conferences and a published author on XML technologies. He holds MBA and BS degrees.