Standard Ontology of Security of Information and Networks

Atilla Elçi
Aksaray University, Turkey

Keynote Talk, SIN’14, Sept. 9-11, 2014 Glasgow
SIN Conferences:

Topics of Interest include:

- Security ontology, models, protocols & policies
- Semantics, metadata and ontology

aspects besides security research areas.
Search for **books** on “**ontology +security**” in title

At Amazon, Springer Link, Google:

- Absolutely no relevant results!
- What get listed are citations to certain talks or passing remarks in edited books.
Search for “ontology” books

Books having «ontology» in title at:

- Amazon
- Springer Link

⇒ Plenty
Search for “security” books

Books having «security» in title at:

- Amazon
- Springer Link

➤ Plenty
Conjecture

- The two fields separately exist at a grand scale but do not intersect!
- Security ontology has not been worked on
- Let alone becoming a mainstream research or professional practice.
The span of the interest: a long list of specialized research topics

- Security standards for information systems
- Security standards for the semantic Web
- Ontology standards for the semantic Web
- Ontology languages standards
- Standards for secure data sharing across organizations
- Dynamic security configuration for the semantic Web
- Secure software engineering
- Engineering secure software systems
- Building secure survivable semantic Web application systems
- Confidentiality, privacy and trust policy enforcement for the semantic Web
- Secure knowledge management: confidentiality, trust and privacy
- Policy languages and specifications for adaptive Web services security framework
- Ontology for building privacy into the semantic Web
- Security in the web services framework
- Enhanced multi-level security and secure sharing model
- ….
Security terminology is often vaguely defined, causing uncertainty and difficulty

(Donner, M. 2003. Toward a Security Ontology [From the Editor], May/Jun, *IEEE Security and Privacy*, 1, 3, 6-7.)

Let us define “information security” as “IT security” and “information assurance” combined.

Covers not only the information side, but also the computer and communication networking with respect to security considerations.
Few studies exist on ontologizing security

- **Peer advice**: Go for advancing “the theory and practice of security, privacy, and trust of Web-based Applications and to provide declarative policy representation languages and ontologies together with algorithms to reason about policies.”


- Misses the standardization requirement
An account of project work on information security ontology

Fairly advanced but topical: «An ontology that describes security technologies as a taxonomy and as countermeasures to protection goals.»

There are currently four security ontologies.

- **Main Security Ontology**
  The main security ontology contains assets, threats, vulnerabilities, countermeasures as well as security goals like confidentiality, integrity etc. and defense strategies such as detection, prevention etc.

- **Security Views Ontology**
  This ontology imports the main security ontology and defines classes that sort countermeasures and threats according to assets, security goals and defense strategies.

- **Source Code Analysis Ontology**
  This ontology imports the main security ontology and extends the countermeasure class *source code analysis* with tools that are used for C source code analysis.

- **Memory Protection Ontology**
  This ontology imports the main security ontology and extends the countermeasure class *memory protection* with a number of memory protection tools and techniques.
Sample: **Main ontology in HTML**

An ontology that describes security technologies as a taxonomy and as countermeasures to protection goals. Typical starting points for browsing should be the classes `Asset`, `Countermeasure`, `Threat`.

**Annotations**

- `dc:creator`: Almut Herzog, almhe@ida.liu.se
- `dc:publisher`: Dept. of Computer and Information Science, Linköpings universitet, Sweden

**Namespaces**

**Default Namespace**

```
http://www.ida.liu.se/~almhe/Security.owl#
```

```
http://protege.stanford.edu/plugins/owl/dc/protege-dc.owl#
```
This paper considered the fact that ontology would certainly contain company knowhow, internal database, and even trade secrets thus it has to be kept private. Yet, in order to utilize ontology it has to be accessed openly. This work proposes to remedy the issue by:

- Securing ontology through creating a secure flavor of OWL, and
- Handling security problems of ontology as embedded into the layers of the semantic web protocol cake (ref. next slide).

This work appears to be the first to talk of «Semantic web security standards»

Singhal and Wijesekera ‘10

- Propose to evolve a scheme in order to model enterprise level security metrics where they suggest a design model of ontology for security metrics and touches on implementation issues.

Surveys of Security Ontologies

- Systematic review and comparison of security ontologies:
  - A ground breaking survey
  - But, the ontologies are bits & pieces.

- Of security requirements: proposes an analysis and a typology, and thus may form a starting point towards any work on standardization:
  - Most requirements engineers lack security knowledge; consequently a gap exists between the fields of security requirement engineering and ontologies.
Forward attempts

- **Blanco et al:**
  - Proposed a basis for generating an *integrated security ontology* following systematic survey of existing proposals.
  - Highly advanced
  - Could be the foundation for standardization
    

- **Dana Petcu:** evolves a taxonomy for SLA-based monitoring of cloud security.
  
Security Standards

- As it is public knowledge, and evident from source searches, there exist numerous security standards, many of which pertain to information security, computer security, network security .... Many of these include metadata sections on information security, but no ontology.

- Take NIST for example; and search “information security” in titles at IHS Standards Expert.
"information security" in titles:

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Status</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>DI-SESS-81343A</td>
<td>Active</td>
<td>2013.01.15</td>
<td>Information Security (INFOSEC) Boundary Configuration Management PI</td>
</tr>
<tr>
<td>DODD 5200.1-R</td>
<td>Cancelled</td>
<td>1997.01.01</td>
<td>INFORMATION SECURITY PROGRAM</td>
</tr>
<tr>
<td>DOE 471.2A</td>
<td>Active</td>
<td>1997.03.27</td>
<td>INFORMATION SECURITY PROGRAM</td>
</tr>
<tr>
<td>ETSI GS ISI 001-1</td>
<td>Active</td>
<td>2013.04.01</td>
<td>Information Security Indicators (ISI); Indicators (INC); Part 1: A full set of guidelines for security posture - V1.1.1; Includes Diskette</td>
</tr>
<tr>
<td>ETSI GS ISI 001-2</td>
<td>Active</td>
<td>2013.04.01</td>
<td>Information Security Indicators (ISI); Indicators (INC); Part 2: Guide to selecting security strategies - V1.1.1</td>
</tr>
<tr>
<td>ETSI GS ISI 002</td>
<td>Active</td>
<td>2013.04.01</td>
<td>Information Security Indicators (ISI); Event Model A security event classification - V1.1.1</td>
</tr>
<tr>
<td>ETSI GS ISI 003</td>
<td>Active</td>
<td>2014.06.01</td>
<td>Information Security Indicators (ISI); Key Performance Security Indicators - V1.1.2</td>
</tr>
</tbody>
</table>
Ontology Standards

- Many ontology standards on various research areas exist as one will discover by searching the term “ontology” in titles at IHS Standards Expert. Research areas vary from geographic information, to IP traffic measurement, to European eConstruction, and so on, but, there is none on “information security ontology”.

- Certainly the World Wide Web Consortium has numerous community standards, called “recommendations”, on ontology languages.
• “ontology” in titles:

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Status</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSA JIS X 7254</td>
<td>Active</td>
<td>2008.11.20 (R 2013)</td>
<td>OWL Web Ontology Language - Semantics and Abstract Syntax</td>
</tr>
<tr>
<td>SN CWA 15142:2004</td>
<td>Withdrawn</td>
<td>2004.12.01</td>
<td>European eConstruction Ontology (EeO)</td>
</tr>
<tr>
<td>AFNOR NF ISO 21127</td>
<td>Active</td>
<td>2007.09.01</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>BSI BS ISO 21127</td>
<td>Active</td>
<td>2006.10.31</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>DS DS/ISO 21127</td>
<td>Active</td>
<td>2009.11.30</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>ISO DIS 21127</td>
<td>Draft</td>
<td>2013.10.09</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>ISO 21127</td>
<td>Active</td>
<td>2006.09.15</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>UNI UNI ISO 21127</td>
<td>Active</td>
<td>2011.05.05</td>
<td>Information and documentation - A reference ontology for the interchange of culture</td>
</tr>
<tr>
<td>AIAA S-133-7</td>
<td>Active</td>
<td>2013.01.01</td>
<td>Space Plug-and-Play Architecture Standard Ontology</td>
</tr>
<tr>
<td>BSI 12/30248557 DC</td>
<td>Draft</td>
<td>2012.02.03</td>
<td>Draft BS EN 62656-3 Standardized product ontology register and transfer by spre</td>
</tr>
</tbody>
</table>
Information Security Ontology Standards

- Hardly any standard exists as one would realize by searching “information security ontology” or “information security” +ontology at IHS Standards Expert.
Search Results for:
Keyword(s): "information security" +ontology
Applied Filters: ✗ Most Recent Revision

No documents were retrieved by this search.

Suggested changes to your search to make the search less specific:

- Check the text search field for incorrect spelling.
- Ensure there is a space between the Organization and base number in the document number field.
- Use the "*" wildcard to represent 0 or more characters.
- Ensure the selected refinements are what you intended. Remove one at a time.
All would agree on the ultimate position International Standards Organization (ISO) plays in standardization. Yet, regarding information security ontology, there is no working committee under ISO, Nor, a work group in IT Security Techniques Technical Committee.
The **Universal Business Language** (UBL-2.1, 4 Nov 2013):

- Long been fostered by OASIS as a **universal standard of business information exchange**,
- Has met official acceptance by global parties and states.
- UBL contains extensive metadata
- But hardly any on information security
- Except consideration of e-signature for use towards authentication purpose.
There is little work being carried out in W3C with respect to standardized security ontology; and, hardly any results exist in information security ontology.

Security at W3C is taken up as Web Security meaning securing Web applications and Web usage.
Security at W3C

Web Security is a collaborative effort across the Web ecosystem; W3C coordinates some of that work in its Security Activity, within the Technology & Society Domain. Among the work we are doing to help secure Web applications and Web usage:

**Web Cryptography Working Group**
Motivated by the emergence of more complex protocols executed between Web applications, the WebCrypto group is defining an API to expose trusted cryptographic

**Web Application Security**
WebAppSec is developing the Content Security Policy and CSP 1.1; Cross-Origin Resource Sharing; UI Security; Subresource Integrity Recommendations. This work

**XML Security**
XMLSec produced three W3C Recommendations: a stable interim set of 1.1 specification. The XML Signature 1.1 and XML Encryption 1.1 specifications clarify and enhance the previous
Auto Alliance could have developed «a peer-reviewed generic automobile ontology which their individual automobile manufacturers, and potentially others, could modify, or import, as needed for their specific needs».  

«Other alliances and associations for other domains could also create "approved" ontologies for their membership.»

«Unfortunately, there doesn't appear to be enough demand from association membership to support this sort of standardized ontology development.»

John Flynn of semanticsimulations.com
Information Security Ontology?

- What?
- Who?
- How?
- Standardization?
To Conclude

- It should be clear that a generic ontology for security of information and networks is needed and that earlier the better.

- Furthermore, there is a dire need for standardization of high-level information security ontology, perhaps an upper ontology for all others to link up to. Thus there should come about a forest of linked ontologies allowing all concerned to link their big data.
Qs? Comments?

» You are welcome.
Addtl Refs

Semantic Web layers

- Different Graphs: check papers & W3C site