A Preliminary Cyber Ontology for Insider Threats in the Financial Sector

Gökhan Kul
Department of Computer Science and Engineering
The State University of New York at Buffalo
Buffalo, New York 14260
gokhanku@buffalo.edu

Shambhu Upadhyaya
Department of Computer Science and Engineering
The State University of New York at Buffalo
Buffalo, New York 14260
shambhu@buffalo.edu

ABSTRACT

Insider attack has become a major threat in financial sector and is a very serious and pervasive security problem. Currently, there is no insider threat ontology in this domain and such an ontology is critical to developing countermeasures against insider attacks. In this paper, we create an ontology focusing on insider attacks in the banking domain targeting database systems. We define the taxonomy used in this ontology and identify the relationships between the ontology classes. The resulting structure is a domain ontology mapped onto the Suggested Upper Merged Ontology (SUMO), Friend of a Friend(FOAF) and Finance ontologies to make our work integrable to the systems that use these ontologies and to create a broad knowledge base. The attack types we formulate in the ontology are masquerade, privilege elevation, privilege abuse and collusion attacks. Our model could be used to systematically evaluate any insider threat detection schemes in a realistic way and discover attacks that share similarities with previously identified attacks.

Categories and Subject Descriptors

H.2.0 [**General**]: [Security, integrity, and protection]; D.3.1 [**Formal Definitions and Theory**]: [Semantics]; D.2.11 [**Software Architectures**]: [Domain-specific architectures]

General Terms

Insider attacks

Keywords

Cyber ontology; financial sector; relational database systems; taxonomy

1. INTRODUCTION

Insider attacks are becoming an extremely serious security problem for financial institutions due to the threat they pose to the monetary assets and the sensitive customer data they handle. The threat that leads to insider attack is called an insider threat and the RAND report [1] addresses insider threats as "malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems."

Due to the nature of the banking domain, even entry level employees can access very sensitive information. An attack that is conducted by an employee can go unnoticed for a very long time [2]. There may be multiple insider attacks consequently within an organization with either the same or different intentions. According to the 2014 U.S. State of Cybercrime Survey [3], 37% of organizations have experienced an insider incident, and in 76% of incidents confidential records were compromised or stolen. It is expressed in this report that 28% of electronic crime events are known or suspected to have been caused by insiders and in 46% of electronic crimes, insider attacks were more costly or damaging to their organization. The report also shows that 75% of cases were handled internally without legal action or law enforcement, mostly because of lack of evidence or not enough information to prosecute. Only 10% of cases were handled internally with legal action and 12% of the cases were handled externally with notification of law enforcement while only 3% of cases were handled externally by filing a civil action. This raises the questions on the reliability of security systems toward identifying insider threats.

We focus on insider attacks on relational database management systems for a variety of reasons. First, keeping the focus on a specific but important domain allows us to contain the scope of the model to a more manageable level. Second, even though there are other data preservation techniques and systems, relational databases are heavily used in backend servers to store financial data, which consists of a lot of sensitive information. This makes relational databases a primary target for criminal activity. The aim of this effort is to develop an ontology of this area, expressed in the Web Ontology Language (OWL) that ensures integration with other knowledge domains and enables data integration across different data sources. Semantic web applications are becoming more popular by the day and ontology is the most important enabling technology of these applications. Basically, it describes terms and different relationship types between terms. In this paper, we create a taxonomy of insider threats and identify the relationships between the entities we define in the taxonomy. These entities and relationships are used to create an insider threats ontology which is then mapped

MIST'15, October 12, 2015, Denver, Colorado, USA.

DOI: http://dx.doi.org/10.1145/2808783.2808793.

onto upper ontologies and domain ontologies that are commonly used in financial systems. The contribution of this work is both creating a framework of a cyber ontology for insider threats in the financial sector focusing on relational database management systems, and integrating this ontology with commonly used ontologies SUMO [4], FOAF [5] and Finance [6] to make it applicable and integrable to the systems that use these ontologies.

Section 2 creates a taxonomy on insider threats. Section 3 discusses the advantages and contributions of our research, and finally Section 4 presents the future work.

2. TAXONOMY AND ONTOLOGY

Taxonomy and ontology are two common terminologies that are being used in information management and there are cases that people treat them as synonyms.

The term "taxonomy" could refer to a hierarchical classification or categorization system, or to an organization of concepts of knowledge, as well as a knowledge organization system designated to include term lists and clasifications [7]. Except for some rare cases, defining the relationships between entities is not a concern when defining taxonomies, other than a hierarchical relationship between entities.

The term "ontology" other than its philosophical meaning, is a formal framework to represent knowledge in computer and information science. Ontologies define classes, properties of these classes and relationships between these classes within their domain. Using the relationships, we can extract other information from these information entities and use them to identify other previously unidentified relationships between them. The authors of [8] classify taxonomies as linguistic/terminological ontologies. However, taxonomies can also be used to define ontologies when the relationships between the classes are defined and a formal structure of an ontology can be constructed with them. How to develop an ontology is summarized in [9] as (1) defining classes in the ontology, (2) arranging the classes in a taxonomic hierarchy, (3) defining slots and describing allowed values for these slots, namely, creating properties of the classes and (3) filling in the values for slots for instances.

This section identifies the methodology employed in the taxonomy and ontology development process and explains the details of the construction of ontology classes.

2.1 Methodology

The ontology development process we employed in this work is a top-down analysis which requires understanding the semantics of the end-users who will actually use the resulting ontology. It starts with creating a list of terms which will be used to construct the taxonomy of the structure. The taxonomy needs to include the terms that define the classes in the domain and to be limited with what the resulting ontology will cover, what will it be used for, and what types of questions the ontology will answer to. Following the creation of the taxonomy, and the hierarchy within the taxonomy, the properties of the classes should be defined along with the relationships between classes.

Validation of the ontology structure is performed through competency questions. These questions assure the targeted value of the structure is achieved. They serve as procedures that indicate when the ontology development is sufficiently complete. The competency questions aim to ensure that the results are accurate, sufficient, and have the right level of granularity which is identified by the subject matter expert. They also ensure that the scope of the ontology is still within the limits.

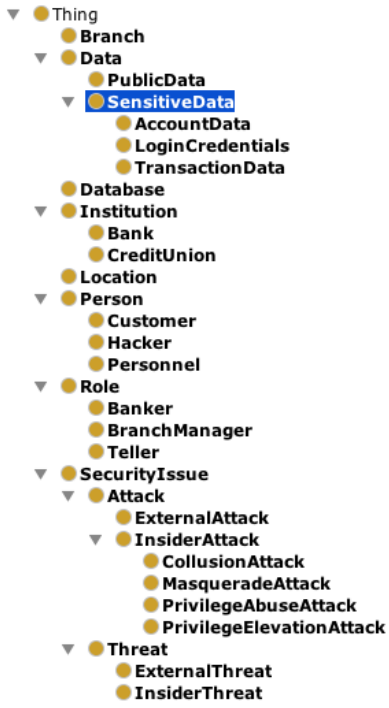

Figure 1: Ontology classes from initial terminology

It is essential to integrate the ontology created with other ontologies, as it will integrate the domain with the rest of the world. Considering that ontologies are a web of knowledge, integrating the ontology with other ontologies will create a bigger knowledge base and extend the opportunities of integrating this ontology with the existing systems. However, to increase data and information quality within a domain, we need to create an ontology that can represent that domain successfully, and creating an ontology requires expert knowledge within that specific domain as well as the skills required to create it. To create an ontology, ontology developers and domain experts need to work together. Ontologies that are created by people who lack either expert knowledge or ontology development skills may result in serious problems and wrong results. However, not all research projects have enough resources to hire people who have these skills. Also, even if the resources are sufficient, project teams may not think it is necessary.

2.2 Our Ontology

The efforts we have put into creating a taxonomy on finance domain has resulted with the taxonomy shown in Figure 1. As a result of the top-down analysis we performed with the domain experts of our collaborator banking institution, we have identified the taxonomy classes based on basic scenarios given in [10]. The validation of these classes is performed through mapping between classes and instances gathered from the mentioned scenarios.

There are several types of ontologies that we can base the rules of our ontology framework. Upper level ontologies describe concepts that are the same across all knowledge

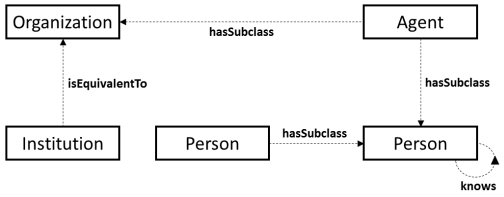

Figure 2: Integration of FOAF ontology classes

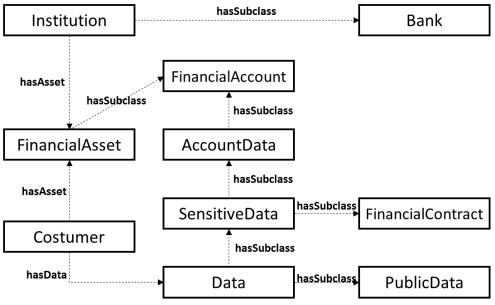

Figure 3: Integration of SUMO ontology classes

domains which provides a high level of semantic interoperability. On the other hand, domain ontologies describe concepts in a specific field or in a part of the world. This specific field or part of the world represents the domain that the ontology describes. Since the concepts belong to the domain, they may or may not be compatible with a concept that has the same name in a different domain ontology. The ontologies that describe concepts that can be both mentioned in domain and upper level ontologies are "hybrid ontologies." Especially by working on integration of different systems together, the hybrid approach makes it easier to work with multiple ontologies. Some concepts can be defined universally but some concepts are described according to the domain related limitations.

Our goal is to provide a web of knowledge by integrating commonly used upper ontologies into our ontology. To achieve this task, we created a domain ontology on insider attacks focusing on financial sector, and then we identified some ontologies that are commonly used by academia and industry that may possibly have similar classes that we identified in our ontology.

Friend of a Friend (FOAF) ontology [5] describes people, their activities and relationships between each other and other objects. It allows groups of people to create social networks, which we are using to describe the relationships between customers, bank personnel and roles and hiearchy within the organizations. The common terms that we imported from this ontology are "Organization" and "Person" classes as can be seen in Figure 2. After importing these classes, we have expanded these terms with the domain specific subclasses, to define the banking environment.

The Suggested Upper Merged Ontology (SUMO) [4], has a broad range of domain areas included in it. However, it only provides a structure and a set of general concepts upon which domain ontologies could be constructed. Financial concepts are among these concepts, too. The common terms that we imported from this ontology are "FinancialAccount", "FinancialContract", "financial asset" and all of their

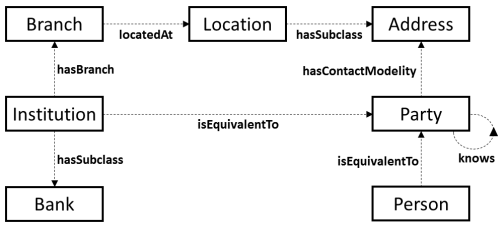

Figure 4: Integration of Finance ontology classes

subclasses. The relationships that these terms have with the other classes in our ontology can be seen in Figure 3.

Finance ontology [6] is an ontology on financial instruments, involved parties, processes and procedures in securities handling. We are using this ontology to define the financial instruments and involved parties within organizations, so that the main concern of our ontology stays as insider attacks instead of expanding into defining banking domain itself. The common terms that we imported from this ontology are "Address", "Party" and all of the subclasses of "Party" as can be seen in Figure 4.

Therefore, we integrated our ontology with FOAF to base our Person and Organization structure on universally defined terms and we expanded these terms. On the other hand, we imported classes from SUMO and Finance ontology to use the classes that are already defined in financial domain, so that we didn't need to define new classes in the finance domain. The graph of the resulting ontology is shown in Figure 5.

3. DISCUSSION

We have presented a preliminary cyber ontology focusing on insider attacks in banking domain targeting database systems. As indicated before, the prior efforts in insider threats branches to two different directions. These branches are the psychological aspects and physical aspects of insider threats. Our work takes the initiative to start efforts on building a cyber ontology for insider threats in the financial sector, as it is critical to developing countermeasures against insider attacks in this domain. The contributions of our work is, creating a cyber ontology framework for insider threats in the financial sector focusing on relational database management systems and ensuring the integration with other knowledge domains to enable data integration. The preliminary cyber ontology we created is mapped onto FOAF and SUMO ontologies, which are universally defined, and the terms in them mean the same across all knowledge domains. In this sense, our ontology provides a high level of semantic interoperability. When fully developed, we believe that this integration with other domains and semantic structures approach can prove effective to addressing more factors about insider threats as it could be used by researchers to test and evaluate their detection and mitigation schemes, as well as identifying similar attacks by using previously identified attacks.

The literature survey we have performed shows us that this ontology fills the gap in ontological structuring of insider threat research in financial sector. The ontologies developed on insider threat research generally focus on defining insider threat and incidents [11]. The work in [11] leads us to ex-

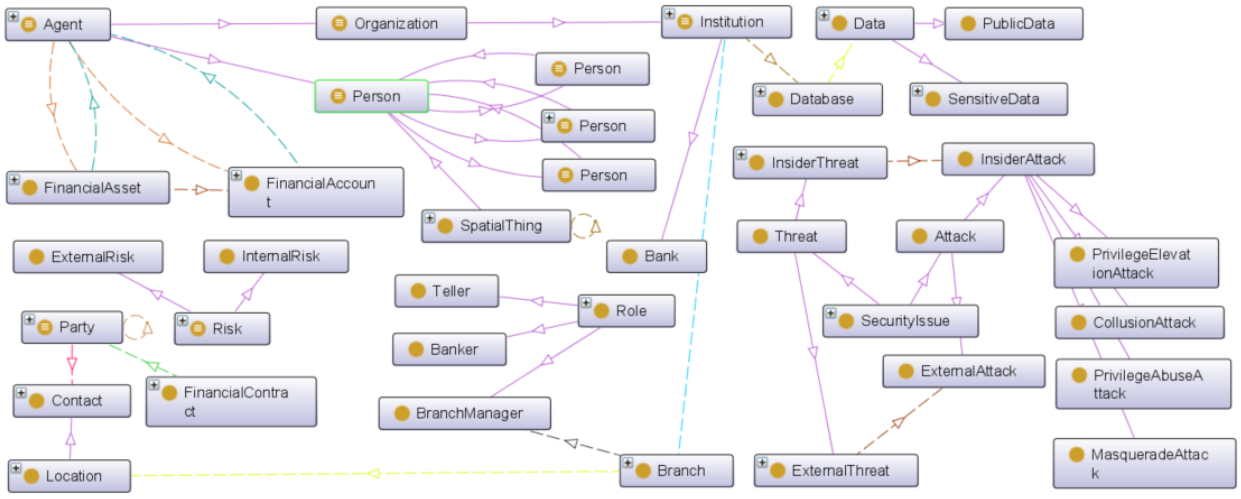

Figure 5: Main components of the ontology

periment on specific domains and use the domain specific knowledge to create a semantic structure. This structure defines the insider threat in financial sector more conclusively. We have collaborated with financial sector experts but we know that there is still a lot to do to expand the capability of our ontology, since we still cannot gather real data from banking databases.

4. FUTURE WORK

The major threat of insider attacks drives both academia and industry to find better solutions. As we continue our research on insider threats, we will need to extend the ontology that we developed and create a knowledge base. We should create our knowledge base from real working systems to be able to validate the ontology that we constructed. We are working on building collaborations with financial institutions to gather the data required to validate the current structure. After the validation phase, we are looking forward to iteratively building on the ontology to improve both scope and capability. The validation phase will be performed with competency questions to test if the ontology contains enough information to answer the questions, if the answers it provides have a sufficient level of detail, or if they represent the domain well enough.

5. ACKNOWLEDGMENTS

This material is based in part upon work supported by the National Science Foundation under award number CNS - 1409551. Usual disclaimers apply. We would like to thank Thomas Mitchell, and Patrick Coonan for their review of related articles and their help in editing.

6. REFERENCES

[1] Robert H. Anderson and Richard Brackney. Understanding the insider threat: Proceedings of a March 2004 workshop. Santa Monica, CA, USA, 2004. RAND Corporation. Also available in print form.

[2] The insider threat: An introduction to detecting and deterring an insider spy. `http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat`. Accessed: 2015-06-15.

[3] CERT Insider Threat Center. 2014 U.S. state of cybercrime survey. July 2014.

[4] Adam Pease, Ian Niles, and John Li. The suggested upper merged ontology: A large ontology for the semantic web and its applications. In *In Working Notes of the AAAI-2002 Workshop on Ontologies and the Semantic Web*, 2002.

[5] Jennifer Golbeck and Matthew Rothstein. Linking social networks on the web with FOAF: A semantic web case study. In *AAAI*, volume 8, 2008.

[6] Eddy Vanderlinden. Finance ontology documentation. `http://fadyart.com/ontologies/documentation/finance/index.html`. Accessed: 2015-06-15.

[7] Heather Hedden. *The Accidental Taxonomist*. Information Today, Inc., Medford, New Jersey, 2010. ISBN: 978-1-57387-397-0.

[8] Gilles Falquet, Claudine Métral, Jacques Teller, and Christopher Tweed. *Ontologues in Urban Development Projects*. Advanced Information and Knowledge Processing 1. Springer-Verlag London Limited, 2011.

[9] Natalya F. Noy and Deborah L. McGuinness. Ontology development 101: A guide to creating your first ontology. `http://protege.stanford.edu/publications/ontology_development/ontology101.pdf`. Accessed: 2015-06-15.

[10] Gokhan Kul and Shambhu Upadhyaya. Creating a preliminary cyber ontology for insider threats in the financial sector. Technical Report 2015-03, The State University of New York at Buffalo, 07 2015.

[11] Daniel Costa, Matthew Collins, Samuel Perl, Michael Albrethsen, George Silowash, and Derrick Spooner. An ontology for insider threat indicators: Development and application. In *Proceedings of the Ninth Conference on Semantic Technology for Intelligence, Defense, and Security*, STIDS 2014, pages 48–53. CEUR Workshop Proceedings, 2014.