Applying Multi-Level Theory to an Information Security Incident Domain Ontology

Marta Rigaud Faria[1], **Glaucia Botelho de Figueiredo**[2], **Kelli de Faria Cordeiro**[1], **Maria Claudia Cavalcanti**[1], **Maria Luiza Machado Campos**[2]

[1]Seção de Engenharia da Computação - Instituto Militar de Engenharia (IME)

[2]Programa de Pós-Graduação em Informática (PPGI) - Universidade Federal do Rio de Janeiro (UFRJ)

martarigaud@gmail.com, glauciabotelho@ufrj.br, kelli@marinha.mil.br

yoko@ime.eb.br, mluiza@ppgi.ufrj.br

Abstract. *There is a substantial increase in the occurrence of information security incidents. To protect against these incidents, joint approaches, which include sharing incident information, are gaining particular importance. However, organizations do not have a clear distinction between the types of incidents and their specializations, leading to the same occurrence of incident being classified in different ways compromising the decision making process. In this paper it will be elaborated a domain ontology fragment about information security incidents applying Multi Level Theory (MLT) and the Unified Foundational Ontology (UFO) to make these concepts more explicit and, consequently, to facilitate interoperability within the domain.*

1. Introduction

The popularization of the Internet has provided a relevant democratization of access to information as well as a new era of interactions and communication. But parallel to this phenomenon, there is a substantial increase in the occurrence of information security incidents. Such incidents may cause severe damages. Therefore, it is required a constant development of cyber defense strategies to prevent them.

One of the strategies that is being adopted by several organizations is to have a Computer Security Incident Response Team (CSIRT). The CSIRT receives, analyzes, and responds to information security incident notifications. It usually provides services to a well-defined community, serving as a central point for reporting local problems. Thus, all reported incidents to be collected in a single location where informations can be analyzed and correlated across the community. These informations can be used to determine trends and patterns of attackers activity and to recommend appropriate prevention strategies.

Despite having several CSIRTs in operation in Brazil, the lack of a clear conceptualization for this kind of incidents to be used in consensus makes the work difficult. This fact was evidenced in the statistical report published in 2018 by the Governmental Center of Training and Response to Cybernetic Incidents responsible for supporting the organizations and entities of the Federal Public Administration. In this report, 20.566 notifications were received. After a careful screening process, only 9.981 of them were actually considered incidents [1], but the analyzed characteristics and the criteria for evaluating the incidents were not made explicit.

[1]https://www.ctir.gov.br/arquivos/estatisticas/2018/Estatisticas_CTIR_Gov_Ano_2018.pdf

Another relevant factor is related to the statistical reports produced by CSIRTs, which use different forms of incident categorization, making it impossible to correlate information about information security incidents. For example, CSIRT.gov uses eight categories to classify incidents, the Brazilian National Computer Emergency Response Team uses six categories [2], the Bahia Security Incident Response Team uses twelve categories [3] and so on.

In addition, within the organizational context, typically several classification criteria are used to refer to the same incident occurrence. For example, when occurs an attack that caused a site to become unavailable, the technical team could use terms based on the observation of the log register, i.e., they could report the incident as HTTP flooding type, when they identify that the HTTP protocol was used and the number of requests exceeded the site capacity, causing a flood. In contrast, a security manager could register the same incident as denial of service (DoS) type. In this scenario, when the members of the organization need to prepare an inventory and/or carry out comparative analyses over incidents, it can lead to inconsistencies. This is because, the same incident occurrence can be classified as a more specific type (HTTP flooding), as well as a more general type (DoS), depending on the classification criteria used.

All these different ways of representation make the knowledge exchange of information security incidents quite complex. To identify trends, this information should be shared using a common understanding resulting from the comprehensive domain analysis. It is necessary to be aware of the causes of the incident, the participants involved and the damage caused by the incident, to have a solid foundation that supports effective decision making. And, to identify patterns of attacker activity, attack depiction conflicts should be minimized by explaining the relationships that can occur between attack types and their subtypes.

Some ontologies have already been used to represent the information security incident domain, but they do not make a clear distinction between incident types and their proper characterization, which is essential to an area that is continuously evolving and becoming critical to most organizations. In this sense, the Multi-Level Theory (MLT) [Carvalho et al. 2015] may be used as a basis for increasing expressivity, as it defines relationships which occur inter and intra levels of element classification. Recently, some works, [Carvalho and Almeida 2015], have integrated MLT to the Unified Foundational Ontology (UFO), taking advantage of UFO sound system of ontological categories and the multiple levels of classification patterns formally characterized in MLT.

In order to provide a conceptual methodological support for knowledge exchange of information security incident, both in the organizational context and in the community under the responsibility of a CSIRT and between CSIRTs, it was created sCuDO, an information security incident domain ontology supported by Multi-Level Theory. This paper presents sCuDo according to the following structure: in section 2, an overview of information security incident concepts and ontologies is presented; section 3 discusses concepts and advantages of combining of MLT with UFO-A and UFO-B to provide foundations for ontology-based multi-level modeling; section 4 contemplates details of sCuDO; and, finally, section 5 presents concluding remarks and topics for further investigation.

[2]https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html

[3]https://certbahia.pop-ba.rnp.br/pages/stats/

2. Ontology about Information Security Incident

The increase in the number of incidents affecting information security has motivated many studies. Due to the wide scope and complexity of the subject, studies in this area have different approaches. However, some similarities are found related to the practical use of ontologies in conceptual models.

Some domain representation approaches that focus on covering the concepts, such as, [Moreira 2018] represent incident and information asset attacked at the instance level without supporting representation of types and subtypes. Some other approaches such as [Ping et al. 2010] represent concepts such as incident, vulnerability, and, in addition, support the representation of types of malicious tool used to attack and the type of damage caused by the incident, but lacking to capture features associated for each type.

Other ontologies exclusively model classes hierarchy. In [Li and Tian 2010], the authors modeled attack classes to correlate them with the alert of intrusion detection systems (IDS). The ontological model of malware classes designed by [Swimmer 2008] allows the exchange of data between security software prototypes. Another example includes the Distributed Denial of Service (DDoS) attack hierarchy [Ansarinia et al. 2012]. However, they do not make a clear distinction between types and their proper characterization.

All these ontology initiatives emphasize the representation of some elements or classes for a specific environment, i.e., none of them aim at an open and generic approach for interoperability. In addition, it is not sufficient to represent just incident or attack events, but also the context where these events occur, the participants and their respective roles, as well as their impacts.

On the other hand, the categorization scheme itself is important in this domain. This structure gives rise to hierarchies of types in which the more specific types usually form a partition of a more general type distinguishing instances according to a specific classification criteria. For example, a specific occurrence (instance) of an HTTP flooding event may be a specialization of DDoS, which in turn may be a specialization of DoS, and so on. At the end, all these terms, may be used to typify an attack event.

There are already initiatives, such as the ABNT Information Security Norm [ISO/IEC 2013], and the CERT.br reports, which are used as references to describe the occurrences of incidents reported by IDS or log records. However, these terms were not taken into account on the ontology initiatives described earlier. Moreover, there is a lack of expressiveness since they do not elucidate the classification criteria which more general types are specialized into more specific types. When using types such as DoS and Social Engineering, it is not clear why they are specializations of attack. The explicitation of this criteria requires an extra level of abstraction. For instance, in this other level of representation, it is possible to clarify that the classification criteria is the attack method used. However, this is not always clear on the incident reports. Now, suppose a situation where some attacks were reported but were not distinguished with respect to the method used. If the classification criteria was already known, it would be possible to disambiguate such occurrences, by classifying them as DoS or Social Engineering attacks. Furthermore, occurrences could be classified as of the same type if only the common characteristics of them were used as classification criteria.

To fill these gaps, it is important to clarify the semantics, enhancing the expressiveness of concepts in this domain. For this purpose, sCuDO presents an UFO-MLT based perspective of these concepts, making the classification criteria explicit, and defining the relations that may occur between elements of different classification levels.

3. Background

Foundational ontologies are domain independent and philosophically well founded systems of formal categories, which can be used to clearly express real-world conceptualizations. The Unified Foundational Ontology (UFO) was developed by the combination of micro-theories that involve fundamental concepts of modeling, based on formal ontology, cognitive science, linguistics and philosophical logics [Guizzardi et al. 2015].

Over the years, UFO has been applied to the development of core and domain ontologies in different areas [Guizzardi et al. 2015]. The ability to clearly express concepts of the real-world, reducing conceptual ambiguities, leads the scientific community, as well as conceptual modeling professionals, to consider UFO as an important resource to model the domain ontologies.

UFO is divided in three parts dealing with different aspects of reality: UFO-A, UFO-B and UFO-C. UFO-A, which is the core of the ontology, deals with *endurants*, focusing on structural aspects of conceptual modeling. UFO-B fragment focuses on *perdurants*, dealing with events, processes, i.e., temporal aspects, and the possible connections between *endurants* and *perdurants*. UFO-C fragment focuses on *social* and *intentional entities*, built on the previous fragments, aiming to systematize concepts that include agents, intentional states, goals, actions, norms, social commitments/claims, social dependency relations, among others [Guizzardi et al. 2015].

Universals and *individuals* are fundamental and distinct concepts in UFO. *Universals* represent the general aspects that are common to different *individuals*, i.e., *universals* typify *individuals*. Thus, *individuals* instantiate one or more *universals*. *Individuals* represent the entities that exist in the real world and carry an identity of their own. Therefore, these concepts are based on notions such as class and type [Carvalho et al. 2015], similar to the concepts widely disseminated by the Unified Modeling Language (UML) and used by information systems developers. UML uses the *generalizationSet* constructor to provide a way to group generalizations, which may be associated with a classifier, called *powertype*. This means that for every *generalization* in the *generalizationSet*, the specializing classifier is uniquely associated with an instance of the *powertype*, i.e., there is a 1-1 correspondence between instances of the *powertype* and specializations in the *generalizationSet*, so that the *powertype* instances and the corresponding classifiers may be treated as semantically equivalent. These notions lead modelers to classify many objects as *kinds* and *categories* when applying UFO-A. It is common to find plenty of subject domains that require not only the representation of categories of individuals, but also the representation of categories of categories (or types of types) [Carvalho et al. 2015]. This multi-level classification conception has raised a research area entitled multi-level theory (MLT), aiming to address the limitations of the conventional two-level modeling paradigm.

MLT provides ways to define the relations that may occur between the classification levels of an element. The MLT theory also establishes distinction between types

and instances. However, to represent the multiple classifications levels, MLT has to consider types that have other types as instances. In this way, MLT applies the idea of type order. There is no limit established in order type. Whenever a type has individuals as instances, it is called *first-order type* (or shortly *1stOT*); when the instances of a type are *first-order types*, it is called *second-order type* (or shortly *2ndOT*) and so on. Instance of is a primitive relation used to link types whose entities fit in the order type notion [Carvalho et al. 2015].

MLT defines new structural relations for variants of the *powertype* like the categorization relation and its variations to enriches the expressivity of modeling. In this sense, to increase the foundational ontology benefits to domains that require multiple levels of classification, the MLT can be applied to UFO [Carvalho et al. 2015]. Thus, conceptual models built with the UFO-MLT combination take advantage from the system of ontological categories employed by UFO and from the multiple levels of classification patterns formally characterized in MLT [Carvalho et al. 2015].

In order to combine MLT and UFO, in [Carvalho et al. 2015] they had established a hierarchy of conceptual models of UFO-A, with MLT forming the topmost layer. In addition to the UFO-A elements, in this paper, UFO-B elements will be also modeled due to the predominant of events in the domain of information security. Conceptual models constructed with the UFO-MLT combination have to follow the rules of both theories. This combination makes it possible to construct models capable of expressing ontological properties of the types that apply to individuals and represent the types of specific types of a domain.

The concepts in UFO taxonomy of individuals are instances of *1stOT* specializing individual, while the concepts in the taxonomy of universals are instances of *2ndOT* specializing *1stOT*. For each entity in the taxonomy of *individuals*, there is a corresponding entity in the taxonomy of *universals*. Instances of an entity in the taxonomy of *universals* specialize the corresponding entity in the taxonomy of *individuals*. Thus, Endurant Universal *categorizes* Endurant, Event Universal *categorizes* Event, Moment Universal *categorizes* Moment, and so on. Therefore, the *first-order types* of the model must specialize *individuals* and must be instance of some leaf category of UFO *universals* taxonomy. Figure 1 shows the general relations of categorization between *universal* and *individual* of the UFO fragment that are employed in sCuDO.

As a result, the UFO-MLT combination may be used to provide rules and patterns for introducing *second order types* in ontology-based domain models. For instance, the relation between MLT and UFO was able to capture a semantic foundation for the organizational structure domain [Carvalho and Almeida 2015]. This ontology serves as a basis for the development of enterprise specific ontologies. In this background, the *first-order types*, which were defined in the core ontology, act as base types. When the ontology is extended to a specific domain, these types are completely categorized as subkinds, which are *second-order types*.

The application of MLT to UFO had made the modeling more precise, since formally characterizes the nature of classification levels and precisely defines the structural relations that may occur between elements of different classification levels. Therefore, the characteristics of the domain elements modeled with UFO, when typified in multiple

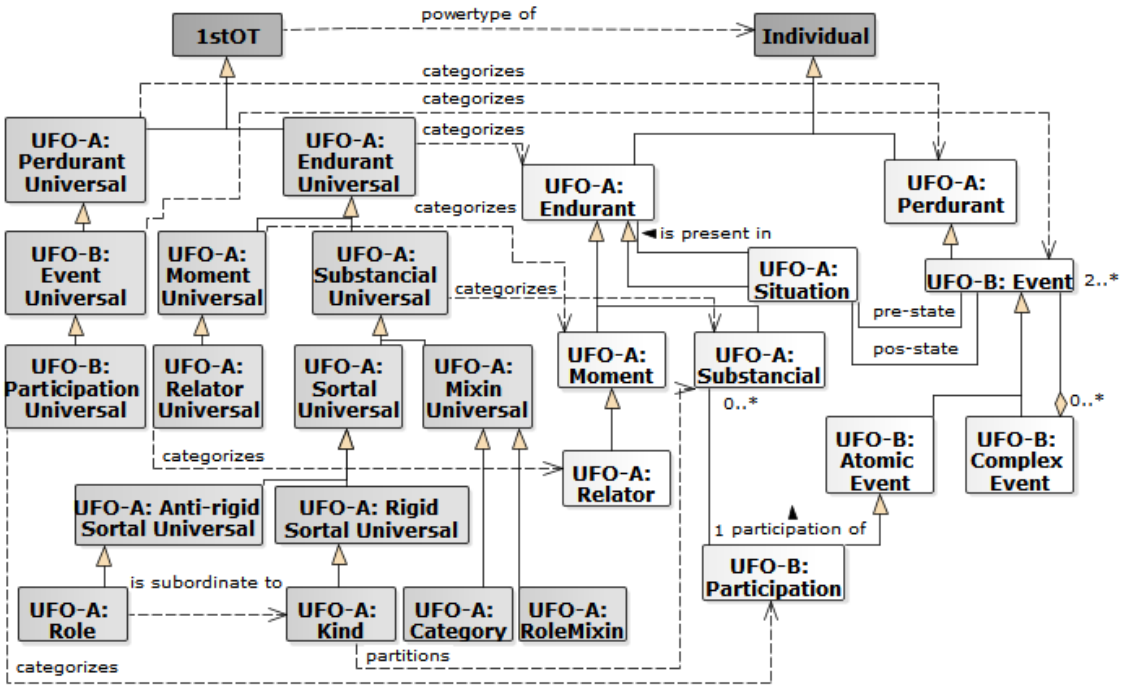

Figure 1. Applying MLT to a UFO fragment. Adapted from [NEMO]

levels, disambiguate the understanding of the domain concepts.

4. sCuDO: Information Security Incident Domain Ontology supported by Multi-Level Theory

To construct sCuDO, a methodology was used, inspired by [Fernndez et al. 1997], composed of the following steps: specification, knowledge acquisition and conceptualization. In the specification step, it was defined that sCuDO is intended to provide conceptual methodological support for the knowledge exchange of information security incident. Its main objective is to communicate the notifications of incidents more clearly so that ambiguities are avoided. In this way, the information can be gathered, analyzed and disseminated by CSIRTs, assisting in the decision making process.

To achieve this, it is necessary to increase knowledge about the domain. At this stage, formal texts on the subject were analyzed, such as the ABNT standard, CSIRTs reports, studies and experiences papers and IDS logs to obtain detailed knowledge about concepts, their properties and their relationships. The sCuDO fragment presented in this paper is based primarily on the taxonomy of information security incident terms proposed in [Howard and Longstaff 1998], on the categorization criteria of [Cheswick and Bellovin 1994] attack and on the attack type hierarchy DoS of [Mirkovic and Reiher 2004].

The conceptualization activity structures the knowledge of the domain in a conceptual model according to the scope defined in the specification using the knowledge acquired in the previous steps. For that, it was made an ontological analysis to elucidate and discover distinctions relevant and relationships bound to domain entities, for the practical purpose of disambiguating terms having different interpretations in different

contexts. Giving a basis for ontology based UFO-MLT as detailed below.

Information security incidents occur in a computational environment and may involve a diversity of elements, such as computers, network equipment, software and data, among others. These information assets are used for various purposes and their operation involve numerous events. In this context, an event is a sequence of directed actions with a specific purpose as a consequence of a change in the state of an information asset. Whenever the actions have the intention of resulting in something that is not allowed to happen, an attack is identified [Howard and Longstaff 1998].

The occurrence of an attack involves the participation of an attacker. An attacker employs a malicious tool, such as a program, to explore an information asset vulnerability and performs an action to obtain an unauthorized result [Howard and Longstaff 1998]. Often, a succession of attacks occur by the action of the same attacker to cause damage. These attacks are part of an incident. In this way, an incident involves a simple attack or a group of attacks that can be distinguished from others considering the attackers, type of attack and damages involved.

Figure 2 shows an incident ontology represented using the UFO-MLT taxonomy. Note that an Incident is an instance of the *UFO-B: Event Universal* consisting of one or more Attacks that were executed by the same Attacker to achieve a certain Damage (*situation*).

As an event, Attack depends on the participation of objects. Person, Information Asset and Tool are objects participants of an Attack. A Person plays the *role* of Attacker and a Tool plays the *role* of Malicious Tool, to execute an Attack. The Attack happens when the Information Asset is in a Vulnerability *situation* and after the Attack it is an Unauthorized Result *situation*. The set of Unauthorized Results of Attacks in an Incident leads to a Damage *situation*.

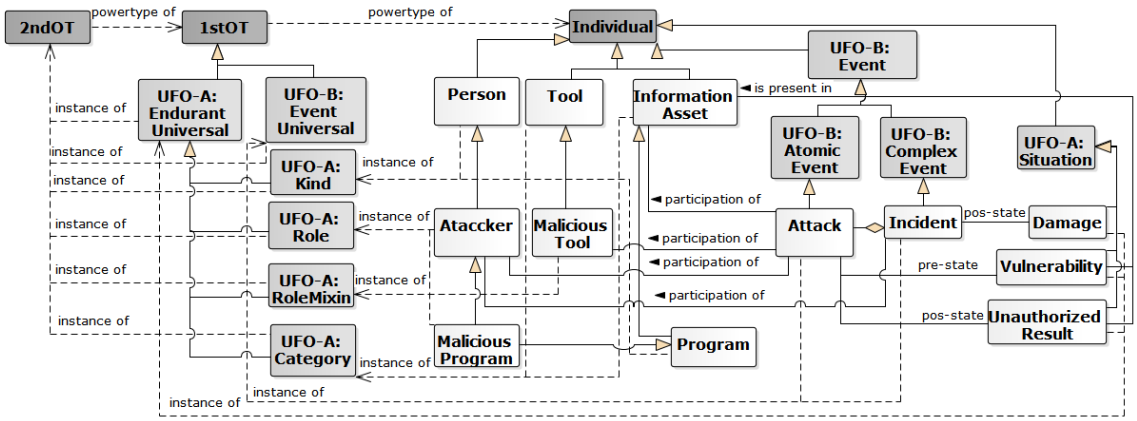

Figure 2. Fragment of the Information Security Incident ontology employing UFO-MLT

Attacks are categorized in several ways, one of which is proposed by [Cheswick and Bellovin 1994], they classify attacks into seven categories: Stealing Passwords, Social Engineering, Bugs and Backdoors, Authentication Failures, Protocol Failures, Information Leakage and Denial of Service (DoS). So that, Attack Type specializes *UFO-B: Event Universal* and *categorizes* Attack which has instances, such as, DoS and

Social Engineering.

Attack Type can be specialized considering different criteria. Due to the limited space, only the specialization of the DoS attack type is detailed in Figure 3. Other Attack Type, such as Social Engineering, could be similarly represented. A DoS Attack makes a system unavailable to its legitimate users. This unavailability can be caused by a single machine or multiple machines. Hence, DoS Attack can specialize in Simple resource, when a single machine is used, or DDoS, when different resources are used [Mirkovic and Reiher 2004].

Descending in the classification hierarchy of the DDoS Attack, it becomes possible to make explicit the rules applied to classify an Attack according to the possibility of characterization. A DDoS Attack is Characterizable when it is possible to identify its occurrence by inspecting the packet headers. Correspondingly, an Attack that can not be identified by inspection of the packet headers is Non-characterizable. In addition, a Characterizable DDoS Attack may be Filterable or Non-filterable. A Filterable DDoS Attack uses malformed packets or packets that are not required for the normal operation of the Information Asset [Mirkovic and Reiher 2004]. Finally, UDP Flooding and Smurf are specializations of Filterable as well as HTTP Flooding, Slow HTTP and Sockstress are specializations of Non-filterable. Figure 3 presents the details of this classification structure.

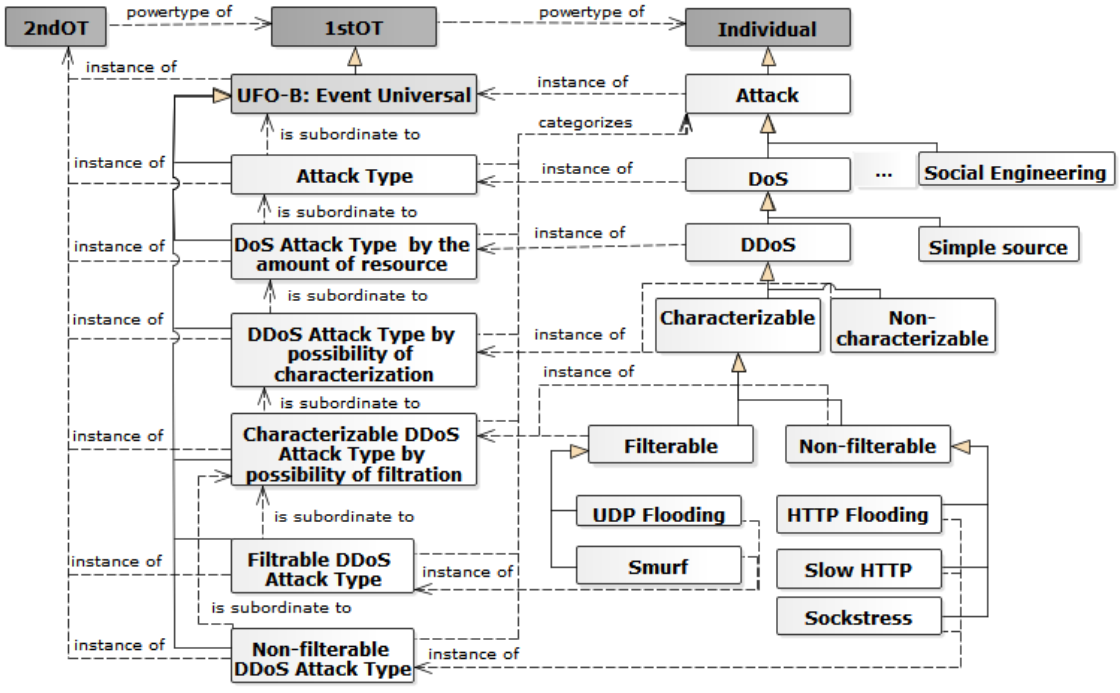

Figure 3. Using MLT-UFO combination to describe the structural relations that exist in attack taxonomy

As shown in Figure 3, the instances of *UFO-B: Event Universal* obey a subordination chain such that every instance of DoS Attack Type by the amount of resources affected proper specializes one instance of Attack Type. Also, every instance of DDoS Attack Type by possibility of characterization proper specializes one instance of DoS Attack Type by the amount of resource. Plus, every instance of DDoS Attack Type by

possibility of filtration proper specializes one instance of DDoS Attack Type by possibility of characterization. Finally, every instance of Non-filterable DDoS Attack Type and Filterable DDoS Attack Type proper specializes one instance of DDoS Attack Type by possibility of filtration. Thus, the specializations of *UFO-B: Event Universal* categorize their corresponding instances.

Types can be seen as entities that capture common characteristics of other entities which are considered their instances. In addition, an instance of a type can specialize an instance of another type. In this context, sCuDo uses the Attack Type to categorize Attack. Therefore, instances of Attack Type (e.g. Social Engineering, DoS) are proper specializations of Attack. The amount of resources used to cause the Attack (DoS Attack Type by amount of resources) *categorizes* Attack and, in addition, its instances (e.g. Simple resource, DDoS) are proper specializations of DoS (e.g. DoS Attack Type by amount of resource is subordinate to Attack Type). Similarly, the possibility to identify an attack occurrence by inspecting the packet header (DDoS Attack Type by possibility of characterization) *categorizes* Attack and its instances are proper specializations of DDoS and so on.

As shown above, the concepts of information security incident were presented through an ontology based on UFO-MLT. sCuDO represents domain concepts, as in [Moreira 2018] and [Ping et al. 2010], but the use of UFO stereotypes as instances of *second order types* has promoted greater semantic expressiveness. For example, the Incident entity, in sCuDO, is an instance of *UFO B: Event Universal*, proper specialization of *UFO-B: Complex Event* and composed of Attack.

The sCuDO type categorization scheme resembles those proposed in [Ping et al. 2010], [Li and Tian 2010] and [Ansarinia et al. 2012] in identifying attack types. However, sCuDo has the differential of elucidating the characteristics of a type and the criterion of specialization. This Attack classification allows to infer that HTTP Flooding proper specializes DDoS by the fact that it proper specializes Non-filterable which, in turn, proper specializes Characterizable and so on. This type of relationship facilitates communication and information exchange.

In this way, sCuDO represents types and subtypes of attack evidencing the criterion of classification, making it possible to correlate occurrences of incidents originating from different sources. For example, supposing there had been two incidents similar to the incident described in Section 1, that is, some attack made some site unavailable. If one of these incidents was logged using the ontology [Li and Tian 2010] the attack would be classified as DDoS type. And, if the second occurrence of incident was reported using the ontology [Ansarinia et al. 2012], the attack would be of the HTTP Flood type (CAPEC-488 [4]). Looking exclusively at the assigned types the two occurrences could be interpreted as of distinct types, however, using sCuDO it would be possible to associate the HTTP Flood type of [Ansarinia et al. 2012] with the HTTP Flooding of sCuDO that is itself specialization of DDoS, making it possible to correlate both occurrences.

4.1. sCuDO scenario application

To demonstrate a practical use of the information security incident ontology with classification criteria, sCuDO was applied to the historical security incident, which took place

[4]https://capec.mitre.org/data/definitions/488.html

in Iran.

During the protests against the Iranian presidential election in 2009, Slowloris was used as a tool to attack sites run by the Iranian government, such as “www.leader.ir”, and “www.president.ir”. Slowloris was developed by Robert ”Rsnake” Hanser using the perl language [Krishna et al. 2018]. It is a denial of service tool which creates a stream of TCP SYN requests to the target victim and keeps them open as long as possible. It does this by continuously sending partial HTTP requests, none of which is completed. The target victim receives the requests, opens connections, and waits for the completion of each request. Ultimately, the targeted victim maximum concurrent connection pool is filled, and additional legitimate connection attempts are denied [Tripathi et al. 2013].

According to sCuDo, the Attack to “www.leader.ir” and Attack to “www.president.ir” compose an instance of Incident. Robert ‘Rsnake’ Hanser is the Person that plays the Attacker *role*. He used the Program called Slowloris that is a *Kind* of Tool to cause Political Damage in protest against the Iranian presidential elections.

The Slowloris Program was used in a Malicious way to Attack those sites. Each Site instance is a *Kind* of Information Asset that is able to accept HTTP requests. These attacks had occurred because the corresponding attacked sites had a configuration Vulnerability. This fact allowed to accept Partial HTTP requests. When the sites were attacked, they become unavailable, which is an Unauthorized Result.

Those attacks utilized several sources, flooding the sites to produce the desired result. According to the hierarchy of categories proposed in Figure 3, “www.leader.ir” Attack and “www.president.ir” Attack are instances of Slow HTTP, and thus, given the specialization relation semantics, it can be inferred that they are also instances of Non-filtrable, Characterizable, DDoS, DoS and Attack. These types, in turn, are instances of *1stOT* Non-filtrable DDoS Attack Type, Characterizable DDoS Attack Type by possibility of filtration, DDoS Attack Type by possibility of characterization, DoS Attack Type, Attack Type and *UFO-B: Event Universal*, respectively. Figure 4 illustrates Attacks to the Iranian government.

Let us consider that those attacks were registered according to the sCuDO ontology, as shown in Figure 4. In this case, it is explicitly represented that those attacks are categorized as Slow HTTP. In addition, suppose another incident had occurred previously in Iran, involving HTTP flooding attacks. Since both incidents were registered according to sCuDO, it becomes possible to identify that there are certain characteristics that are shared by Slow HTTP attacks and HTTP flooding attacks. They resemble the possibility of filtration, the possibility of characterization, the amount of resources and attack type.

Although these incidents were registered by different organizations, at some point in time they may be part of an inventory. Thus, if any of the shared characteristics was used as a criterion to inventory attack occurrences, Slow HTTP and HTTP flooding subtype were recorded on the same type. Assuming that the method used to attack was the characteristic chosen to record the attack occurrences, and that Slow HTTP and HTTP flooding are proper specializations of DoS, and DoS is an instance of Attack Type, then, in this case, instances of Slow HTTP and HTTP flooding should be inventoried as DoS.

Thus, sCuDO defines the relationships that can occur between elements of differ-

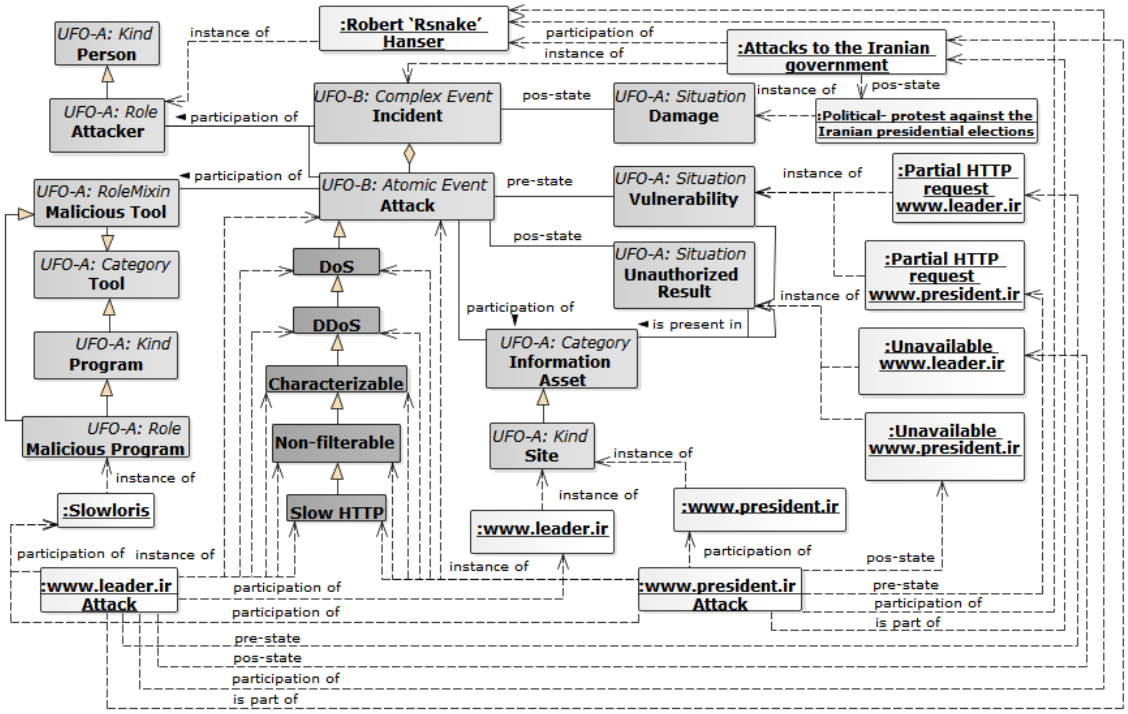

Figure 4. Using sCuDO concepts to describe the Iran Incident

ent classification levels to describe the underlying conceptualization of that domain. The result is a hierarchical modeling approach that can handle a wide variety of attack types and types of attacks would solve the problem of correlating classified instances using different criteria. In addition, sCuDO has the flexibility to be extended with new types or specializations of existing types, to meet the dynamic feature of the domain, which is in constant evolution.

5. Final considerations

This paper presents sCuDO, an information security incident domain ontology built with the combination of UFO and MLT, to support the knowledge exchange of information security incident. The fundamental distinctions provided by UFO have facilitated the representation of the context in which incidents occur, their participants and their roles, as well as their impacts. The use of MLT allowed to address higher-order types and provide a sound basis to formally characterizes the nature of classification levels and to define the structural relations that may occur between elements of different classification levels. The result is a hierarchical modeling approach in which more specific types form a partition of a more general type, making it possible to correlate instances using only their common characteristics as classification criteria.

sCuDO captures, in a concise and elegant manner, the common multi-level properties shared by the instances of DoS attacks and their variations. In the future, the scope of sCuDO will be expanded to encompass other attack categories to be used to facilitate the gathering of information security incident notifications in CSIRTs as well as to correlate information from a CSIRT with information from other CSIRTs. Moreover, other case studies, using real datasets, should be developed in order to validate the ontology.

References

Ansarinia, M., Asghari, S. A., Souzani, A., and Ghaznavi, A. (2012). Ontology-based modeling of ddos attacks for attack plan detection. IST 2012.

Carvalho, V. A. and Almeida, J. P. A. (2015). A semantic foundation for organizational structures: A multi-level approach. In *2015 IEEE 19th International Enterprise Distributed Object Computing Conference*, pages 50–10.

Carvalho, V. A., Almeida, J. P. A., Guizzardi, G., and Fonseca, C. M. (2015). Extending the foundations of ontology-based conceptual modeling with a multi-level theory. In *35th International Conference on Conceptual Modeling*. ER 2015.

Cheswick, W. R. and Bellovin, S. M. (1994). *Firewalls and Internet Security: Repelling the Wily Hacker*, page 7. Addison-Wesley Professional.

Fernndez, M., Gmez-Prez, A., and Juristo, N. (1997). Methontology: from ontological art towards ontological engineering. In *AAAI Technical Report*, pages 33–40.

Guizzardi, G., Wagner, G., Almeida, J. P. A., and Guizzardi, R. S. S. (2015). Towards ontological foundations for conceptual modeling: The unified foundational ontology (ufo) story. In *Applied Ontology (Online), vol. 10*, pages 259–271.

Howard, J. D. and Longstaff, T. A. (1998). A common language for computer security incidents. In *Sandia National Laboratories*.

ISO/IEC, A. N. (2013). *Norma Brasileira de Tecnologia de Informação - Técnicas de Segurança - Código de prática para a gestão da segurança de informação (ABNT NBR ISO IEC 27001:2013)*, volume 1. ABNT.

Krishna, C. R., Dutta, M., and Kumar, R. (2018). *Proceedings of 2nd International Conference on Communication, Computing and Networking (ICCCN 2018)*, page 7.

Li, W. and Tian, S. (2010). An ontology-based intrusion alerts correlation system. In *Expert Systems with Applications 37*, page 7138–7146.

Mirkovic, J. and Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. In *ACM SIGCOMM Computer Communications Review*, pages 39–53. v. 34, n. 2 edition.

Moreira, G. B. (2018). Uma ontologia para tratamento de incidentes de segurança da informação. Master's thesis, Instituto Militar de Engenharia (IME), Rio de Janeiro.

NEMO. Networked ontology specification seon - conceptual model of the mlt subontology. In *http://dev.nemo.inf.ufes.br/seon/UFO.html*. Abril, 2019.

Ping, L., Haifen, Y., and Guoqing, M. (2010). An incident response decision support system based on cbr and ontology. In *2010 International Conference on Computer Application and System Modeling*, page 337–340. ICCASM.

Swimmer, M. (2008). Towards an ontology of malware classes. In *http://www.scribd.com/doc/24058261/Towards-an-Ontology-of-Malware-Classes*. January 27, 2008.

Tripathi, S., Gupta, B., Almomani, A., Mishra, A., and Veluru, S. (2013). Hadoop based defense solution to handle distributed denial of service (ddos) attacks. In *Journal of Information Security vol. 4*, pages 150–164.