IJICTR International Journal of Information & Communication Technology Research ITRC

Volume 4- Number 2- March 2012 (61-70)

Research Note

Ontological Modeling of Radio Frequency Identification(RFID)Attacks

Ahmad Salahi
Information Security Department
Research Institute for ICT
Tehran, Iran
salahi@itrc.ac.ir

Mahshid Delavar
Information Security Department
Research Institute for ICT
Tehran, Iran
mdelavar@iust.ac.ir

Received: October 20, 2011- Accepted: January 25, 2012

***Abstract*— Advances in RFID technology has led to increasing usage of these systems in various applications such as supply chain management, object identification and so on. At the same time, security attacks against these systems have also grown. Employing a common vocabulary for the sensors of RFID intrusion detection systems will be useful for collaborating with each other in identifying security incidents. Ontological approach for defining RFID attacks can obtain this common vocabulary that is understandable for both humans and software agents. In this paper, an ontological modeling of RFID attacks is presented.**

Keywords- RFID Attack, Ontology, Modeling, Intrusion Detection System, Security

I. Introduction

Radio Frequency Identification (RFID) is a technology that uses radio frequency for transmitting data. A general RFID system consists of three major components: tag, reader and backend server. A tag is a tiny integrated circuit equipped with antennas that communicate with its reader using radio frequencies. A reader can be considered as a middle man between tags and backend server that read the data encoded in tag and sends the data to backend server depending on application wirelessly or through wire. And a backend server is responsible for running application based on the data it receives from readers. A typical RFID system architecture is depicted in figure 1.

RFID systems are used in various applications such as supply chain management, object identification, home security, healthcare monitoring, and warehouse management.

Although there exists great potential of using RFID systems in wide area of applications, these systems also suffer from some inherent vulnerability. RFID systems are subject to a broad range of malicious attacks, ranging from passive eavesdropping to active interference. Since both RFID tags and readers operate on an inherently unstable and potentially noisy environment, attacks on these systems can target the infrastructure in a decentralized manner. Moreover, advances in RFID technology result in multiplying and shrinking the RFID tags, so the threats they are susceptible to are evolving. In other hand, since tags are small in size, with limited storage memory and processing capacity, the number and length of encryption keys are restricted and implementation of a strong encryption algorithm on the tag is hard to achieve.

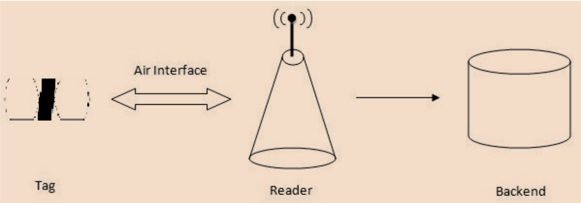

Figure 1. A typical RFID system architecture

Developing an Intrusion Detection System (IDS) for RFID systems can be a good solution to make these systems more secure. An IDS monitors the RFID network for any anomalous activity and thus it can be used in addition to the existing security mechanisms for securing RFID systems. A central component of existing IDSs is the taxonomy employed to characterize and classify the attack or intrusion and a language that describes instances of that taxonomy [1]. Taxonomy based IDSs have some inherent problems. A taxonomy only provide a scheme for classification and it doesn't have the necessary constructs needed to enable a software system to reason over an instance of the taxonomy which is representative of the domain under observation. Also, most attacks and signature languages are special to specific domains, environment and systems; so, they are not extensible and are not communicable between non-homogeneous systems. However, ontologies, unlike taxonomies, have powerful constructs that contain machine interpretable definitions of the concepts within a domain and the relations between them. Therefore, by using ontology, one can provide a software system that is able to share a common understanding of the information at issue and to reason over and analyze this information. Gruber [2] defines an ontology as an explicit specification of conceptualization. This term is borrowed from philosophy and is used to provide a formal specification of the concepts and relationships that can exist between the entities of a domain. Thus, ontologies are designed to enable knowledge sharing and reuse between the entities of a domain.

In this work, we present an ontological modeling of RFID attacks that can be employed for sharing a common understanding of concepts of RFID attacks between non-homogenous IDS sensors. This approach lets IDS sensors agree on what they observe. So, they will present a better logical structure based on description logic in detecting and predicating attacks in RFID network.

Our approach for developing the ontology is shown in Figure 2. Our domain ontologies are RFID and attack domains and the super-domain ontology is RFID attack ontology that is a subset of network attack mid-level ontology. Further description of this hierarchy from upper-level ontologies to domain ontologies can be found in [27].

This paper is organized as follows. Section II discusses related works. Section III describes the proposed ontology for RFID attacks. Section IV presents an evaluation of the ontology, Section V presents how we develop the ontology and eventually in section VI, some concluding remarks are reported.

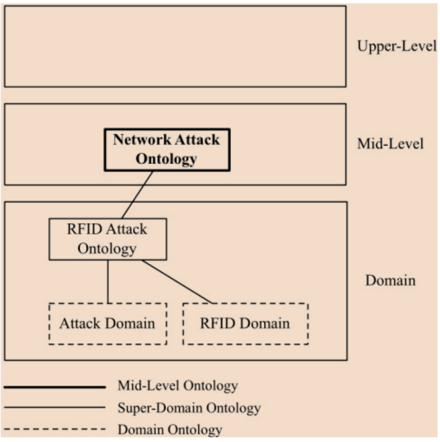

Figure 2. Ontology Layers

II. Related Work

There are many overviews of security issues related to RFID systems in literature. More precisely, [3] and [4] simply listed common attacks in RFID systems. Other papers such as [5;6;7] focused on privacy threats, while yet authors in [8;9;10] proposed a more comprehensive taxonomy. An RFID risk model focusing on network, business process and business intelligence risks was proposed in [8]. The focus of [9] was on the RFID hardware layer and model attack sequences. Mitrokotsa et al. [24] classify attacks based on the layer where each attack is taking place. They discriminate RFID threats in four main layers: physical, network transport, application and strategic layer as well as multilayer attacks which affect more than one layer. In another work, [11] presented a detailed overview of the most important RFID threats by dividing them in three main layers and then considering which of the three security principles (i.e. confidentiality, integrity and availability) is being compromised in each case. We use the introduced concepts of this paper for developing our ontology.

Another group of publications focus on the security and privacy implications in various RFID applications [12,7,13]. Rotter et al. present a comprehensive description of possible security attacks in RFID systems and propose a framework for evaluating and assessing various security and privacy risks [14]. Until now, several countermeasures to RFID threats such as deactivation of tags, on-tag cryptographic solutions such as encryption, authentication and hash codes have been developed. In [3], several RFID authentication protocols against the security threats are studied. A simple tag-reader mutual authentication scheme based on 16 bit random number generator, XOR function and access and kill passwords is proposed by [15]. Although, many security solutions are available, due to small size and constrained resources of tags, they are not capable of executing complex cryptographic solutions like hash functions. Thus, few lightweight authentication protocols that do not require cryptographic hash/keys in the tag have been proposed in [16,17]. However, lightweight security mechanisms (for example, using bitwise keys which proposed by Peris-Lopez et al.) are not fully secure and can easily be broken or compromised [18,1,19]. RFID safeguards that integrate various security mechanisms (auditing, key management, access control and authentication) into a single compact battery device have been proposed. Some of these security concepts such as auditing had not been used in the context of RFID earlier [20]. Although this idea enhances the security features of the system, it suffers from a big problem of single point of failure. In other words, compromising RFID safeguards is sufficient for taking over the entire network. Mirowski et al. proposed an intrusion detection system model for detecting changes in tag ownership [9]. This work is one of the first researches to address the need for intrusion detection systems in RFID. After that, Thamilarasu et al. proposed a generic security framework to detect various RFID attacks. They used the reader-to-reader communication to obtain the audit data needed for detection in such a way that a RFID reader is used as a watchdog to observe and gather information from multiple neighboring readers and tags [20].

In another approach, we review the publications that develop an intrusion detection system based on ontology.

Few literatures can be found about the adoption of the ontology-based approach in developing IDSs. Raskin et al. [21] recommended the use of ontology modeling in the field of information security for providing a common ontology that lets IDS sensors agree on what they observe. Undercoffer et al. [1] proposed a target centric ontology for intrusion detection. Their ontology models properties that are observable and measurable by the target of an attack. Li et al. [22] introduced a hierarchical knowledge model to support alert correlation. This model is formalized in an ontology and a set of rules built on top of it. In RFID domain, Della Vecchia et al. [23] present an ontology-based intrusion detection system that integrates information coming from RFID middleware layer to detect tag cloning.

In [30] the development method for domain ontology from point of view of reveres engineering discussed , taking the relational data model as the object. In [31] A new ontology model called domain ontology graph (DOG) is presented. There are two components in DOG namely , the definition of ontology graph, and ontology learning process.

However, to the best of our knowledge, the RFID security literatures have not yet addressed ontological modeling of RFID attacks.

III. RFID Attack Ontology

For developing our ontology, we define the classes *RFID_*Attack, *Layer*, *Security_Property* and *Potential_Damage.* *Layer* is *Target* to, the relationship between *RFID_Attack* and *Security_Property* is Compromise, The relationship between *RFID_Attack* and *Potential_Damage* is *Resulting in.*

RFID Attacks can be in different forms, so we classify the class *RFID_Attack* into subclasses as follows:

- Cloning
- Spoofing
- Eavesdropping
- Man-in-the-Middle_Attack
- Tag_Disabling
- Tag_Data_Modification.

The class Layer consists of subclasses Edge_ Hardware_Layer, Communication_Layer and Backend_Layer. Subclasses of the class *Security_Prop* are Confidentiality, Integrity and Availability and finally as each of RFID attacks result in a special damage in RFID systems, we define some subclasses for the class *Potential_Damage* includes Extracting information, Elicitation of sensitive information, Access to private information and so on.

Figure 3 presents a high level graphical illustration of the proposed ontology for RFID attacks. In the illustration, a rectangular denotes a subject and object while an arc represents the predicate (relationship).

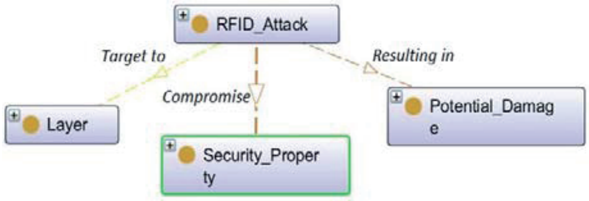

Figure 3. High level illustration of RFID attack ontology

A. Classes

1) RFID_ Attack

One of the classes of our ontology is named RFID_Attack. This class includes different types of attacks that may be happen in RFID networks. The *RFID_ Attack* class is shown in Figure 4. Following, the subclasses of this class is described.

a) Cloning

Tag cloning is one of the most significant threats to the security of RFID systems. Cloning can be achieved by reverse engineering the tags or by building a device that imitates the tag's signal. In this type of attack, attackers aim to catch tag's unique identifier in order to make an exact copy (clone) of the cloned tag, such that the clone can pose as the genuine tag being indistinguishable from the original. Once legitimate tag data are attained, attackers can reproduce their clone tags on a wide scale and gain access to secured facilities, make deceitful purchases, alter or even disrupt supply chains, etc. In case that the RFID tag does not have any security features, cloning can be performed only by copying the tag's

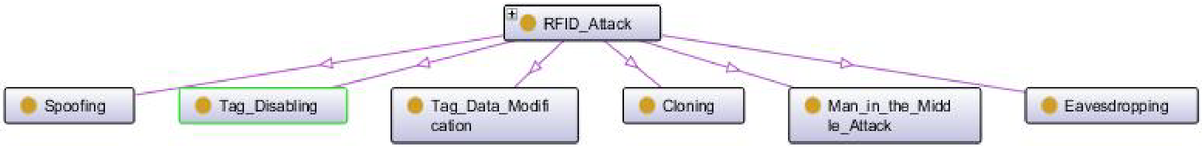

Figure 4. The RFID_ Attack Class with it's subclasses

ID and any associated data to the cloned tag. If tag employs extra security features, then the attacker should perform a more sophisticated attack such that the rogue cloned tag may fool the reader to accept it as a legitimate tag. So, the degree of effort needed to achieve this attack depends on the security features of the RFID tag.

b) Spoofing

Spoofing is a variant of cloning that does not physically replicate an RFID tag [24]. In spoofing attack, adversaries use special devices with increased functionality that can emulate RFID tags given some data content. Thus, the adversary impersonates a valid RFID tag to gain its privileges. For this impersonation, an attacker must have full access to the same communication channels as the original tag and knows everything about the protocols and secrets used in any authentication that is going to take place.

c) Eavesdropping

Because of wireless nature of RFID, eavesdropping is one of the most serious and widely deployed threats. In eavesdropping, an unauthorized party records data communicated between legitimate RFID tags and readers using an antenna. This type of attack is performable in both directions, tag to reader and reader to tag. However, as readers transmit information at much higher power than tags, the former is subject to this type of attacks at much greater distances. The obtained information from recording the communications can be used to perform more sophisticated attacks later. The feasibility of this attack depends on many factors such as the distance of the eavesdropper from the legitimate RFID devices.

d) Man-in-the-Middle (MIM) Attack

An attacker in RFID networks may exploit the vulnerabilities of the wireless channel to perform man-in-the-middle (MIM) attacks. This type of attack targets the communication between RFID tag and reader. The adversary places himself in the communication channel between them. Whenever either tag or reader attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other as if it was never intercepted. This interposition is transparent, leaving the tag and reader unaware of the potential corruption or leakage of their communications.

e) Tag_Disabling

Tag disabling leads to untraceability of tagged objects so that it can be a serious threat to inventory applications, military shipments and so on. Tag disabling can be permanent or temporary. Permanently disabling RFID tags includes all the threats that result in the total destruction or principally degraded operation of a tag be implemented. Physical tag removal or destruction is possible ways to render a tag useless. Also, privacy related countermeasures such as KILL command can be misused and yields the same effect. Even if a RFID tag can counter the threat of permanent disablement, it is still possible to be temporarily disabled. An attacker can use a Faraday cage such as an aluminum foil-lined bag for shielding it from electromagnetic waves (such as those of the checkout reader) so that he can steal any product simply. Passive or active radio interference, also, can temporarily disable the tags.

Malicious readers can render a tag useless through the unauthorized application of delete commands or kill commands, or through physical destruction.

f) Tag_Data_Modification

Critical tag data can be transformed or erased by unauthorized write access to the tag. Tags that have a rewritable memory for updating its contents and notifying updates can be subject to this attack. By acting as an authentic reader, an attacker can modify tag data. The feasibility of this type of attacks greatly depends on the employed READ/WRITE protection and the used RFID standards. The impact of this attack is variant depending on the application and the degree of modification. For example, the manipulation of tags employed in medical applications may have dreadful consequences. Sophisticated attackers may modify critical information without changing the tag's ID or any security related data (such as credentials) such that the reader cannot indicate modifications. Abusing the coding scheme is one of the main approaches for manipulating tag data in RFID communications.

2) *Layer*

Another class of proposed ontology is *Layer* (Figure 5). This class has three subclasses that represent the layers of RFID networks that are targets of RFID attacks. These subclasses will be described in the following subsections.

a) Edge_Hardware_Layer

This layer consists of the RFID tags and readers. These devices usually do not have a very strong physical security, so that, they are exposed to physical attacks such as tampering. In particular, this is true for tags, because their resources are often constrained due to cost and size limitations.

b) Communication_Layer

This layer deals with exchanging information between tag and reader. As sending and receiving data is the main purpose of radio-based technologies such as RFID, the radio link is a dominant point of attack. Such that everyone can listen in and signals are easily modified or jammed.

c) Back-end_Layer

Another layer of RFID systems is the Back-end layer which is responsible for connecting RFID readers to databases and other supporting systems where RF transaction data are stored, analyzed and processed [25]. As this layer consists of elements such as databases, web servers, etc., many attacks on networking applications and systems can be performed through vulnerabilities of this layer.

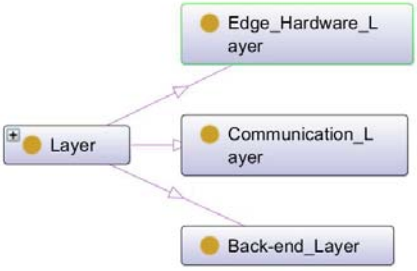

Figure 5. The Layer Class

3) *Security_Property*

We introduce another class named *Security_Property* that includes subclasses of Integrity, Confidentiality and Availability. This class represents the Security_Property that may be compromised by an RFID attack. Figure 6 shows the *Security_Property* class and its subclasses.

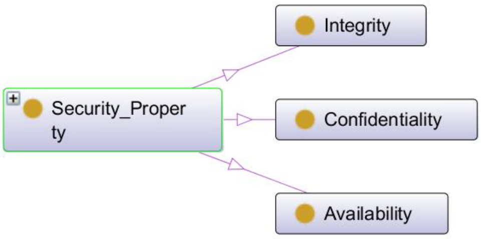

Figure 6. The Security_Property Class

a) Confidentiality

Confidentiality is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes [28, 29].

b) Integrity

To preserve the *integrity* of information means to protect the accuracy and completeness of information and the methods that are used to process and manage it [28, 29].

c) Availability

Availability is a characteristic that applies to assets. An asset is available if it is accessible and usable when needed by an authorized entity. In the context of this definition, assets include things like information, systems, facilities, networks, and computers. All of these assets must be available to authorized entities when they need to access or use them [28, 29].

4) *Potential_Damage*

There are potential damages that are caused by attacks in RFID networks. So, we define the class of *Potential_Damage.* The potential damages of RFID attacks can be as follows:

- Extracting information (such as cryptographic keys)
- Elicitation of sensitive information
- Access to private information
- Altering data stored on tag memory
- Altering back-end data
- Supplanting legitimate tags
- Gaining unauthorized access to services
- Avoid identification
- Untraceability of tagged objects
- Intercept messages
- Breaking the whole system
- Manipulate communication
- Desynchronization
- Interruption of communication
- Interruption of services

B. Predicates

By studying the papers in RFID attack domain such as [10,11] which present a comprehensive classification of attacks, we define predicates *Has*, *Target to*, *Compromise*, *Resulting in* and *Associated with* that show the relation of defined classes. Moreover, inter-relations between taxonomy concepts and their properties in OSVDB, CAPEC, CVE, and CWE taxonomies help us in choosing these relations, too. As said earlier, the relationship *Target to* defines the relation of *RFID_Attack* and *Layer* classes. The relationship between *RFID_Attack* and *Security_Property* defined by *Compromise*. *Resulting in* defines the relationship between *RFID_Attack* and *Potential_Damage* classes. Moreover, the predicates *Has* and *Associated with* define the relationship between subclasses of *Layer class* and their components as shown in Figure 7.

IV. IMPLEMENTATION

To provide a solid structure for further development and potential applications of this ontology, the following technologies and tools have been used for developing RFID attack ontology:

- OWL-DL, with expressivity of SHIOIQ. SHIOIQ includes attributive language, complex concept negation, transitive property, role hierarchy, nominals, inverse property, cardinality restriction, and uses datatypes. It is also capable of using qualified cardinality restrictions.
- SPARQL query language to define closed world assumptions (for consistency checking).
- Pellet Reasoner
- Protégé 4.2 for OWL version 2.

- OntoGraph and OWLViz plug-ins for creating the figures.

The OntoGraph and OWLViz representation of our ontology is shown in Figure 8 and Figure 9, respectively.

V. Evaluation of the Ontology

We applied qualitative and quantitative approaches for evaluating our ontology. In qualitative evaluation, we gave our ontology to three different human experts in RFID attack domain to evaluate the quality of the ontology; and in quantitative evaluation various quantity parameters were extracted.

The evaluation tool that is applied in this paper for quantitative evaluation is OntoQA. OntoQA is a feature-based method for evaluating ontologies. Its main characteristic is that it works on populated ontologies, so it can utilize knowledge represented in the instances to gain a better measure of the quality of the ontology. Also, OntoQA uses much simpler techniques compared to others in that it doesn't need a lot of training as user involvement is minimal.

In OntoQA, metrics are divided into two groups: schema metrics that address the design of the ontology schema and knowledgebase (instance) metrics that address the way instances are organized within the ontology. The first group evaluates ontology design and its potential for rich knowledge representation. The second group evaluates the placement of instance data within the ontology and the effective utilization of the knowledge modeled in the schema [26]. Following a description of both groups of metrics is presented.

➢ Schema metrics

As said, schema metrics address the design of the ontology. Although we cannot clearly know if the ontology design correctly models the domain knowledge, metrics in this category indicate the richness, width, depth, and inheritance of an ontology schema design [27]. Below the most significant metrics in this group are described.

1) Relationship Richness (RR) - This metric shows the diversity of the types of relations in the ontology. An ontology with a diverse set of relationships usually conveys more information than an ontology with only inheritance relationships. The relationship richness is defined as the percentage of the (non-inheritance) relationships between classes compared to all of the possible connections (i.e. inheritance and non-inheritance relationships).
2) Inheritance Richness (IR) – This metric describes the distribution of information across different levels of the ontology's inheritance tree or the fan-out of parent classes. IR is a good index that shows how well knowledge is grouped into different categories and subcategories in the ontology. An ontology with a low IR shows that the ontology covers a specific domain in a detailed manner, while an ontology with a high IR shows that the ontology represents a wide range of general knowledge with a low level of detail. The inheritance richness is defined as the average number of subclasses per class.
3) Attribute Richness (AR) - The number of attributes that are assigned to each class can show both the quality of ontology design and the amount of information related to instance data. In general, it is assumed that the more attributes that are assigned the more knowledge the ontology conveys. The AR is defined as the average number of attributes per class.

➢ Knowledgebase metrics

How the data is placed within an ontology is also a very important measure of ontology quality as it can show the effectiveness of the ontology design and the amount of real-world knowledge represented by the ontology. Knowledgebase metrics include metrics that describe the knowledgebase as a whole, and metrics that describe the way each schema class is being utilized in the KB. These metrics are Class Richness (CR), Class Connectivity (CC), Class Importance (CI), Cohesion (Coh), Relationship Richness (RR).

The quantitative evaluation of our ontology based on schema metrics is presented in Table 1.

Table 1 - Quantitative Metrics for RFID Attack Ontology

Metric	Value
Relationship Richness (RR)	$\frac{23}{55} = 0.41$
Inheritance Richness (IR)	$\frac{32}{45} = 0.71$
Attribute Richness (AR)	$\frac{9}{45} = 0.20$
Axioms (Triples)	142
Concepts	45
Object Properties	14
Data Properties	9

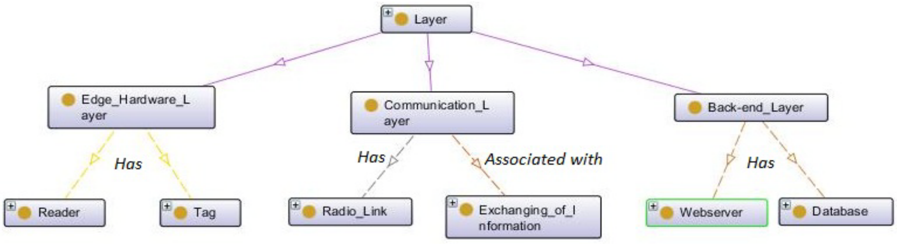

Figure 7. Has and Associated with Predicates

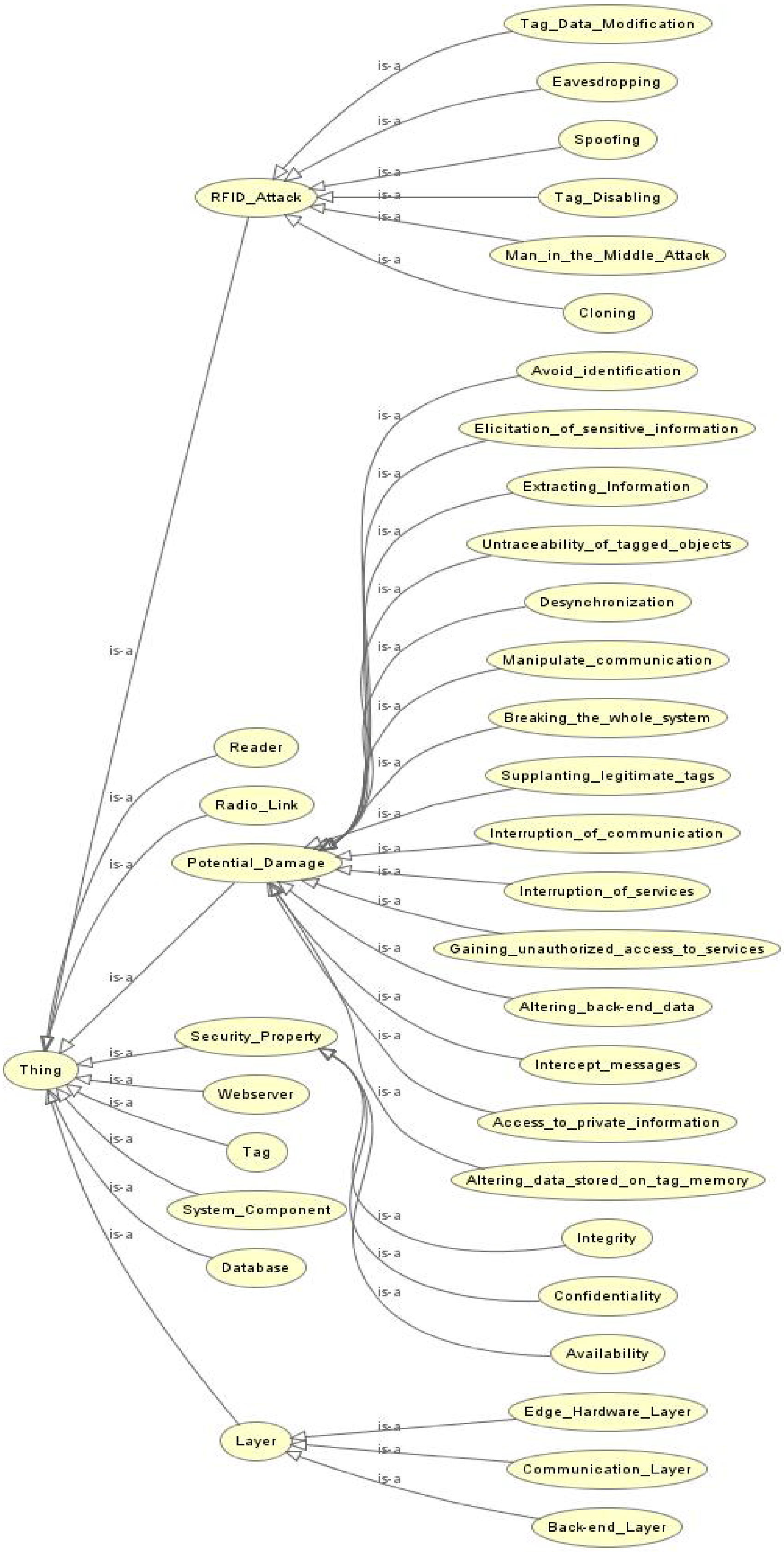

Figure 8. OWLViz representation of RFID Attack Ontology

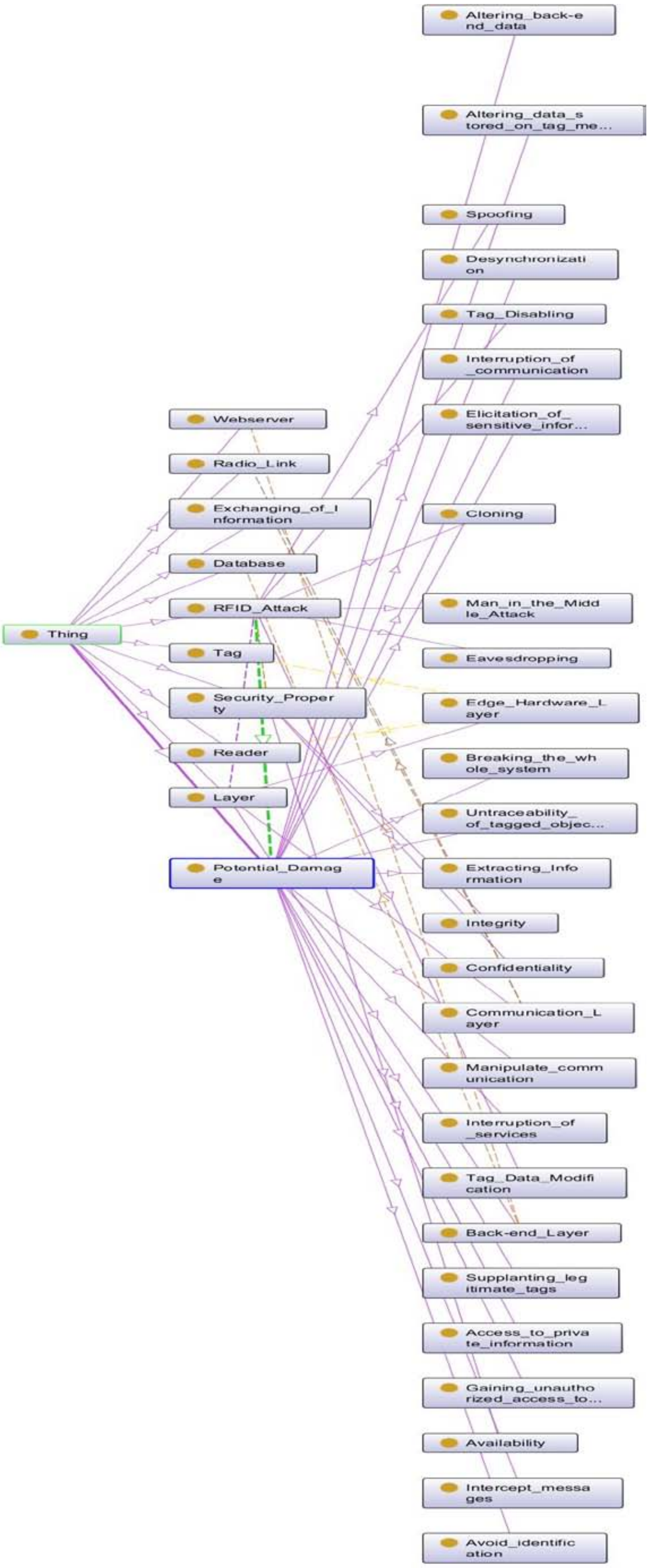

Figure 9. OntoGraph representation of RFID Attack Ontology

In addition to OntoQA metric-based methodology, in order to evaluate consistency and completeness of the ontology, Pellet reasoner has been used. Pellet provides inference capabilities for open world assumption (mostly used for inferring new axioms), and closed world assumption (via Pellet Integrity Constraint Validator for consistency checking). As a result of running Pellet against proposed ontology, no inconsistency has been detected while asserting its axioms. The results of running reasoner over the ontology guarantee well-designed structure, robustness, and consistency of the proposed ontology in this phase of ontology development lifecycle.

VI. CONCLUSION

In this paper, an ontological modeling of RFID attacks is presented. OWL-DL is used for developing the ontology. This ontology can be used for developing an intrusion detection system for RFID networks. Ontological approach help the IDS sensors have a common sense about concepts of an attack, so, communicating between IDS sensors will be much easier than taxonomy based IDSs. Also, by improving the ontology, detection of RFID attacks such as man in the middle attack will be possible.

In general, designed ontology employs description logic, so it can be used as a base schema for attack report aggregation, attack plan recognition, and semantic unification of network interactions.

Moreover, the ontology is evaluated by two approaches: metric-based OntoQA method and reasoner based for consistency checking. And results show the robustness and consistent structure of proposed ontology.

REFRENCES

[1] J. Undercoffer, A. Joshi and J. Pinkston, “Modeling computer attacks: An ontology for intrusion detection,” In Proceeding of the 6th International Symposium on Recent Advances in Intrusion Detection (RAID’03), Pittsburgh, PA. Lecture Notes in Computer Science, vol.2820, pp. 113-135, 2003.

[2] T. F. Gruber, “A Translation Approach to Portable Ontologies,” Knowledge Acquisition, 5(2), pp.199-220, 1993.

[3] A. Juels, “RFID security and privacy: a research survey,” In: IEEE Journal on Selected Areas in Communications, 24(2), pp.381-394, 2006.

[4] P. Peris-Lopez, JC Hernandez-Castro, JM Estevez-Tapiador et al., “RFID systems: a survey on security threats and proposed solutions,” In: Cuenca P, Orozco-Barbosa (eds), PWC 2006, LNCS 4217, pp. 159-170. Springer Verlag Berlin Heidelberg, 2006.

[5] S. Garfinkel, A. Juels, R. Pappu, “RFID privacy: an overview of problems and proposed solutions,” IEEE Security & Privacy 3(3), pp.34-43, 2005.

[6] G. Avoine, P. Oechslin P, “RFID traceability: A multilayer problem,” In: Patrick A, Yung M (eds) Financial cryptography and data security, 9th International conf., FS 2005, LNCS 3570, pp. 125-140. Springer-Verlag Berlin Heidelberg, 2005.

[7] J. Ayoade, “Privacy and RFID systems, roadmap for solving security and privacy concerns,” In RFID systems. Computer Law & Security Report, 23: pp. 555-561, 2007.

[8] T. Karygiannis, T. Phillips, A. Tsibertzopoulos, “RFID Security: A taxonomy of risk,” In Proceedings of the 1st International Conference on Communications and Networking in China (China’Com 2006), pp. 1-8, IEEE Press, 2006.

[9] L. Mirowski, J. Hartnett, R. Williams, “An RFID attacker behavior taxonomy,” In: IEEE Pervasive Computing, pp. 1536-1268. IEEE Computer Society, 2009.

[10] A. Mitrokotsa, MR Rieback, AS Tanenbaum, “Classifying RFID attacks and defenses,” Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer Science & Business Media, LLC 2009, July 2009.

[11] A. Mitrokotsa, M. Beye and P. Peris-Lopez, “Classification of RFID Threats based on Security Principles,” Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, 2011.

[12] M. Mitra, “Privacy for RFID systems to prevent tracking and cloning,” International Journal of Computer Science and Network Security, vol. 8, pp. 1.5, January 2008.

[13] M. Rieback, B. Crispo, and A. Tanenbaum, “The evolution of RFID security,” IEEE Pervasive Computing, vol. 5, pp. 62.69,January.March 2006.

[14] P. Rotter, “A framework for assessing RFID system security and privacy risks,” IEEE Pervasive Computing, vol. 7, no. 2, pp. 70.77, 2008.

[15] D. Konidala, Z. Kim, and K. Kim, “A simple and cost-effective RFID tag-reader mutual authentication scheme,” In Conference on RFID Security, (Malaga, Spain), pp. 141.152, July 2007.

[16] S. Karthikeyan and M. Nesterenko, “RFID security without extensive cryptography,” In *Workshop* on Security of Ad Hoc and Sensor Networks . SASN'05, (Alexandria, Virginia, USA), pp. 63.67, ACM, ACM Press, November 2005.

[17] H.Y. Chien, “SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity,” IEEE Transactions on Dependable and Secure Computing, vol. 4, pp. 337.340, December 2007.

[18] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, “M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags,” In International Conference on Ubiquitous

Intelligence and Computing . UIC06, vol. 4159, pp. 912.923, September 2006.

[19] T. Li and G. Wang, "Security analysis of two ultra-lightweight RFID authentication protocols," In IFIP SEC 2007, 2007.

[20] M. Rieback, B. Crispo, and A. Tanenbaum, "RFID guardian: A battery-powered mobile device for RFID privacy management," In Australasian Conference on Information Security and Privacy, ACISP'05, (Brisbane, Australia), pp. 184.194, July 2005.

[21] G. Thamilarasu and R. Sridhar, "Intrusion detection in RFID systems," *Proceedings of IEEE Military Communications Conference*, pp. 1-7, ISBN 978-4244-2677-5, San Diego, CA, USA, November 17-19, 2008.

[22] V. Raskin; C.F. Hempelmann; K.E. Triezenberg & S. Nirenburg, "Ontology in information security: a useful theoretical foundation and methodological tool," Proceedings of the 2001 workshop on New security paradigms, pp. 53-59, ISBN 1-58113-457-6, Cloudcroft, New Mexico, USA, September 10-13, 2001.

[23] W. Li and S. Tian, "Preprocessor of Intrusion Alerts Correlation Based on Ontology," Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing , Vol. 03, pp. 460-464, ISBN 978-0-7695-3501-2, Kunming, Yunnan, China, January 6-8, 2009.

[24] M. Esposito and G.D. Vecchia, "An ontology-based intrusion detection for RFID system," Technological Developments in Networking, Education and Automation, Vol. 1, pp.467–472, 2010.

[25] A. Mitrokotsa, MR. Rieback, AS. Tanenbaum, "Classifying RFID attacks and defenses," Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer Science & Business Media, July 2009.

[26] T. Karygiannis, B. Eydt, G. Barber G et al, "Guidelines for securing Radio Frequency Identification (RFID) systems," Special Publication 800-98, National Institute of standards and Technology, Technology Administration U.S. Department of Commerce, 2007.

[27] S. Tartir, I. B. Arpinar, and A.P. Sheth. Ontological evaluation and validation. Theory and Applications of Ontology (TAO), Vol.2, Springer-Berlin, 2008.

[28] ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements

[29] ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management

[30] Development Method of Domain Ontology Based on Reverse Engineering Yan, Luo; Changrui, Yu. Service Operations and Logistics, and Informatics, 2007. SOLI 2007. IEEE International Conference on

[31] A New Method for Knowledge and Information Management Domain Ontology Graph Model Liu, J. N. K.; He, Y.-L.; Lim, E. H. Y.; Wang, X.-Z.Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on

Ahmad Salahi was born in Tehran, Iran, on Feb.10.1947. He received his B.Sc. degree in electrical engineering from Tehran University, Iran, his M.Sc. degree from Kansas University U.S.A in 1974 and his Ph.D. degree from Purdue University West Lafayette Indiana, U.S.A in 1979, all in electrical engineering. At present, he is a senior project manager in Network Security Department in Iranin Research Institute for ICT (ex. ITRC). His research interests are network security, switching and routing.

Mahshid Delavar was born in Tehran, Iran, on Oct.15.1983. She received her B.Sc. degree from Amirkabir University of Technology (Tehran Polytechnic) and her M.Sc. degree from Islamic Azad University (South Tehran Branch), all in electrical engineering. At present, she is a Ph.D. candidate in Iran University of Science and Technology. Her research interests are cryptography, network security and hardware implementation of cryptoprocessors.