Copyright ⓒ2017 KSII

Indicator-based Behavior Ontology for Detecting Insider Threats in Network Systems

Janghyuk Kauh[1], Wongi Lim[1], Koohyung Kwon[1], Jong-Eon Lee[2], Jung-Jae Kim[3], Minwoo Ryu[4] and Si-Ho Cha[5]

[1] The 2nd Institute 3rd Directorate, Agency for Defense Development (ADD), Seoul, 05661, Republic of Korea
[e-mail: jhkauh@add.re.kr]
[2] Tactical Communication Team, Hanwha Systems, Gyeonggi-do, 13494, Republic of Korea
[e-mail: jong-eon.lee@hanwha.com]
[3] Dept. of Computer Science, Kwangwoon University, Seoul, 01897, Republic of Korea
[e-mail: kjj6929@kw.ac.kr]
[4] Korea Telecom R&D Center, Korea Telecom (KT), Seoul, 06763, Republic of Korea
[e-mail: mw.ryu@kt.com]
[5] Dept. of Multimedia Science, Chungwoon University, Incheon, 22199, Republic of Korea
[e-mail: shcha@chungwoon.ac.kr]
*Corresponding authors: Minwoo Ryu and Si-Ho Cha

Received February 2, 2017; revised May 23, 2017; accepted July 8, 2017; published October 31, 2017

Abstract

Malicious insider threats have increased recently, and methods of the threats are diversifying every day. These insider threats are becoming a significant problem in corporations and governments today. From a technology standpoint, detecting potential insider threats is difficult in early stage because it is unpredictable. In order to prevent insider threats in early stage, it is necessary to collect all of insiders' data which flow in network systems, and then analyze whether the data are potential threat or not. However, analyzing all of data makes us spend too much time and cost. In addition, we need a large repository in order to collect and manage these data. To resolve this problem, we develop an indicator-based behavior ontology (IB2O) that allows us to understand and interpret insiders' data packets, and then to detect potential threats in early stage in network systems including social networks and company networks. To show feasibility of the behavior ontology, we developed a prototype platform called Insider Threat Detecting Extractor (ITDE) for detecting potential insider threats in early stage based on the behavior ontology. Finally, we showed how the behavior ontology would help detect potential inside threats in network system. We expect that the behavior ontology will be able to contribute to detecting malicious insider threats in early stage.

Keywords: Semantics, insider threat, behavior indicator, ontology, network system, security

1. Introduction

Recently, malicious insider threat is getting increasingly diversified everyday [1][2][3]. The insider threats are becoming significant and real problem in corporations and governments today. According to the US State of Cybercrime Survey, 46% of cybercrime on organization are perpetrated by insiders and all these cybercrimes result in heavy damaging costs. In addition, intrusions are handled without legal action or law enforcement by insiders [4].

From a technology standpoint, detecting potential insider threats is difficult in early stage because the insider threats are unpredictable as well as diverse. According to the Cyber Security Intelligence Index, 55% of cyber-attacks were carried out by insiders, in which 31.5% were malicious insiders and 23.5% were inadvertent actors , and also these attacks took place in anywhere and anyplace [5]. With growing insider threats there is a high risk of proprietary information and data leakage from corporations and the insider threats could also lead to national and economic security threat [6].

In order to prevent insider threats, one approach is to collect all of data which flow in network and then analyze whether the data could be a potential insider threat. Unfortunately, to do this, corporations and governments not only need to spend more time, but also would need to invest lot of capital. Another approach is to forecast potential insider threats through interpretation of data used by insiders on networks, based on well-known semantic technologies [7]. The semantic technologies allow to better understand and interpret the meaning of data according to a model, and also can discover new relationships via inference. For example, if insider tries to move proprietary information or data via internet, we can detect the threats by interpreting the meaning of network packets based on semantic technologies. Accordingly, if semantic technologies are used to detect potential insider threats, it can support to directly detect insiders' malicious threats which are using network including remote controlling of own employees' computers in early stage.

In order to apply the semantic technologies for detecting potential insider threats, we have to resolve three main problems: (1) well-defined ontology model for interpreting meaning of network packets; (2) comprehensive semantic representation regarding potential insider threats; (3) flexibility in changing ontology model according to potential insider threats behavior and corporations requirement.

To resolve these problems, in this paper, we propose an indicator-based behavior ontology (IB2O). IB2O is applied formal modeling to the explicit representation of potential behaviors for insider threats. To do this, we define potential insider threats behavior as indicator and then analyze network packets which have relations these behaviors. In addition, the proposed ontology developed to flexibly change to aggregate new behaviors or removal of existing behaviors in relevance to potential insider threats and corporation's requirement.

Finally, to show the feasibility of the proposed ontology, we develop a prototype platform called insider threat detecting extractor (ITDE). The ITDE provides dynamical creation of ontology in order to interpret the meaning of network packets used by insiders' threat according to user definition or corporation's requirement. It also enables to detect potential insider threats based on the defined ontology.

The rest of this paper is organized as follows. The existing related work in this research field is introduced in Section 2. The detail description of the IB2O is presented in Section 3.

The ITDE architecture and development are introduced in Section 4. Section 5 presents a performance evaluation of the behavior ontology by ITDE. Finally, we conclude our remarks in Section 6.

2. Related Work

Insider threat research has highlighted from early workship, named the insider workship in August 2000. In there, a number of proposals addressed research challenges in order to detect insider threats [8][9]. In particular, they discussed strategies to resolve the insider threat problems.

Nowadays, the insider threat research is becoming more intelligent, for example, Costa, *et al*. proposed ontology for sharing insider threat indicator without compromising organization-sensitive data, to bridge the gap between natural language descriptions of malicious insiders, malicious insider activity, and machine-generated data [10]. Accordingly, the ontology supports create, share, and analyze indicators of insider threat. Heerden *et al*. proposed a methodology using network attack ontology to classify computer based attacks [11]. In this article, they defined taxonomy and ontology to classify a large range of computer network attacks. Additionally, they listed up 10 scenarios regarding diverse network attacks from viewpoints of the attacker and the target. Accordingly, the methodology allows detecting and classifying insider threats using computer network attacks predefined in the scenarios.

Aleman-Meza *et al*. proposed system that takes an ontological approach in order to resolve the legitimate document accessing problem of insider threat [12]. In this article, they utilized the notion of semantic associations and their discovered a collection of heterogeneous the documents. Hence, the system allows supervisors to inspect each document and then to know why the insiders need access to these documents. Frank et al. proposed predictive modeling framework, called CHAMPION to prevent data leakage by insider [13]. The proposed framework could integrate a diverse set of data sources from the cyber domain, and then inferred psychological and motivational factors of malicious insider threats using ontological model. The framework also provides automated support for detecting high priority insider threats. The proposed framework is also able to automatically predict data leakage by insiders through inferred results based on ontological model.

Raskin *et al*. proposed a computational system to detect data leakage using ontological semantic technology (OST) based on understanding of human-level natural language [14]. In this articles, the authors advanced version of existing ontological semantics [15]. The authors also defined person of interest (POI) based on casual and unsolicited verbal output, social engineering including blogs, Facebook, and Twitter, and oral speech. Accordingly, the proposed system enables to extract hidden semantic information from POI and then to protect against insider threat via POI and OST. Symonenko *et al*. proposed a system which allows to detect levels of insider threat risk [16]. This research is part of ARDA's Information Assurance for the Intelligence Community Program [17]. Hence, they used intelligence community's malicious insider threat scenario developed by Subject Matter Experts (SMEs) for modeling and testing. The authors also proven insiders' text-based communications based on natural language processing (NLP) and machine learning. Subsequently, the proposed system allows to analyze insiders threat as well as determine risk level.

Recently, many researchers have been studying to detect insider threats as well as cyber-attacks [18][19][20]. However, in order to detect insider threats which are getting increasingly diversified, we not only have to define a model for understanding and interpreting

data used on networks such as social engineering and local domains but also to flexibly change relationship between entities defined in the model. This paper is motivated from all the above-mentioned research points.

3. Indicator-based Behavior Ontology

In this section, we describe the indicator-based behavior ontology (IB2O). To this end, we classify insider threat behavior for data leakage in higher level, and then investigate relationship between the behavior and network packets with protocols used in data leakage on the Internet as well as local domain. For classification, we divide employees' behaviors which could be becoming insider threat into 5 behaviors, and then we extend activities based on anomalous activity [21]. Finally, we defined warning sign such as evasiveness, suspiciousness, and anomalies regarding each activity. **Table 1** shown classification of insider threat behaviors.

Table 1. Classification of insider threat behaviors in higher level

Behaviors	Activities	Warning sign
Print	Print bursts	Evasiveness
	Suspicious printing timing	Evasiveness
	Remote printing	Evasiveness
	Print blacklisted documents	Suspiciousness
	Large document printing	Anomalies
	Print jobs outlier	Anomalies
Search	Excessive query	Evasiveness
	Suspicious query timing	Evasiveness
	Blacklisted query term	Suspiciousness
	Direct access to database	Suspiciousness
	Odd topic query	Suspiciousness
	High distinct query count	Anomalies
	High query results pages	Anomalies
Access	Excessive access to same IP address	Evasiveness
	Suspicious access timing	Evasiveness
	Access to blacklisted IP address	Suspiciousness
	Try to access using admin account	Suspiciousness
	Access jobs outlier	Anomalies
Download	Download bursts	Evasiveness
	Non-work time downloading	Evasiveness
	Download from remote servers	Suspiciousness
	Download non-accessible files	Suspiciousness
	Large files downloading	Anomalies
	Downloading escalation	Anomalies
Browse	Excessive browsing to same server	Evasiveness
	Suspicious browse timing	Evasiveness
	Browse sensitive terms	Suspiciousness
	Browse anomalous number of document	Suspiciousness
	Browse jobs outlier	Anomalies
	High distinct browse count	Anomalies

The classified behaviors are commonly enacted by employees. However, these behavior patterns can also be found in malicious insiders. To distinguished malicious activities and common activities, we extend and define activities that could be an insiders threat. In addition, these activities are used to investigate relevant network packets and protocols. **Table 2** show type of relevant network packets and protocols according to defined activities.

Table 2. Type of relevant network packets and protocols used in insider treat

Type of protocol	Relevant network packets
HTTP	HTTP header
	Target URL
	Send / Receive data
FTP	Sent / downloaded files
	Sent / downloaded type of file
	Used commands
	Used Messages
SMB	Sent / downloaded files
	Sent / downloaded type of file
	Sharing files
	Sharing type of file
	Sent file for printing
	Sent type of file for printing
SMTP / POP3	Email address (To, From, CC, BCC)
	Email body message
	Email subject
	Attached files in email
	Attached type of file in email

In the **Table 2**, each protocol and relevant network packet have very close relationship with activities defined in **Table 1**. Therefore, we analyze correlation between the activities and relevant network packets with protocols in order to design the proposed IB2O.

For the design of IB2O, we reference fundamental structure from DARPA agent markup language for services (DAML-S) [22]. The IB2O is summarized in **Fig. 1**, is composed of five models including InsiderThreat, Resource, Description, Method, and Grounding. The InsiderThreat model is a support model for IB2O. Accordingly, potential insider behaviors are defined as individual of the model. For this, we use indicators defined in **Table 1**.

3.1 Resource Model

The Resource model describes generic information about proprietary information or data in organizations. In order words, basic information such as owners, accessing levels, and information types are represented in the Resource model. To represent the information, the Resource model is composed of six classes including Resource, ResourceDescription, Type, Owner, AccessInterface, and InterfaceType as shown **Fig. 2**.

The Resource class represents a specific resource and is a supper class of the Resource model. The ResourceDescription class represents detailed description of a resource such as accessing level for authority, short description for explaining the resource, and public or private accessing scope of the resource. For this, the ResourceDesription has data properties

including hasDescription, hasAccessLeve, and isPublic. The Type class represents information regarding resoure types, and extinction of resources. To represent information, this class has data properties such as hasType, and hasExtenstion. The AccessInterface class describes accessing point to access resources, these accessing points are allocated by the organizations. In the class, each accessing point is represented as URI using data properties, named hasAccessPoint. The InterfaceType class describes interface kind when insider access to resource using the accessing point. In order to extend interface type, HyperText Transfer Protocol (HTTP), File Transfer Protoco (FTP), Server Message Block (SMB), Simple Mail Transfer Protocol (SMTP), and Post Office Protocol (POP3) are defined as sub classes of the InterfaceType class.

Consequentially, the Resource class has relationships with ResourceDescription class, Type class, Owner class, and AccessInterface class using object properties including hasResourceDescription, hasResourceType, hasOwner, and hasAccessInteface. Accordingly, the Resource Model is used as standard information regarding resource when data leakage is occurred by insider.

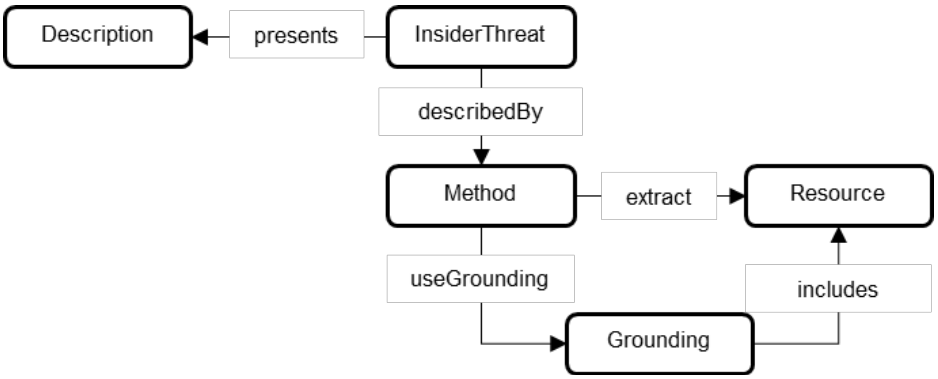


Fig. 1. IB2O model for insider threat

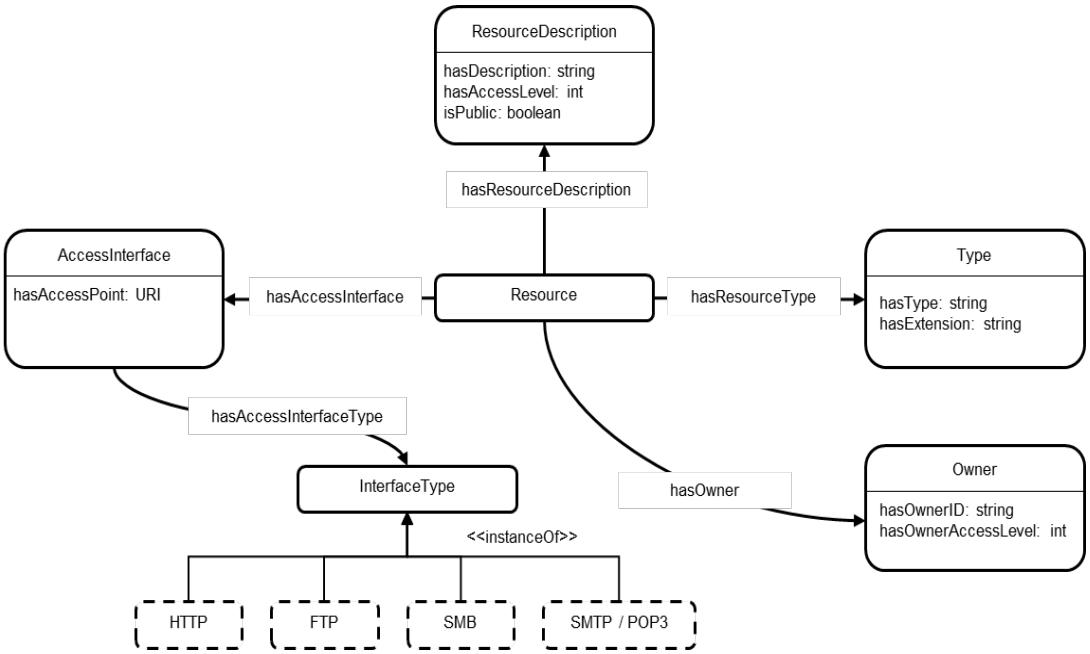


Fig. 2. Resource Model

3.2 Description Model

The Description model represents short description of insider threat behavior. In particular, in this model, each description will explain detailed information regarding indicators defined in **Table 1** with warning signs.

3.3 Method Model

The Method Model represent detail approaches regarding insider threats. Accordingly, potential insider threats are represented in this model. For that, the Method model is composed of four classes including Method, MethodDescription, Device, TimeRange, and also, this model has relationship with the Grounding model via object property, named useGrounding as shown **Fig. 3**.

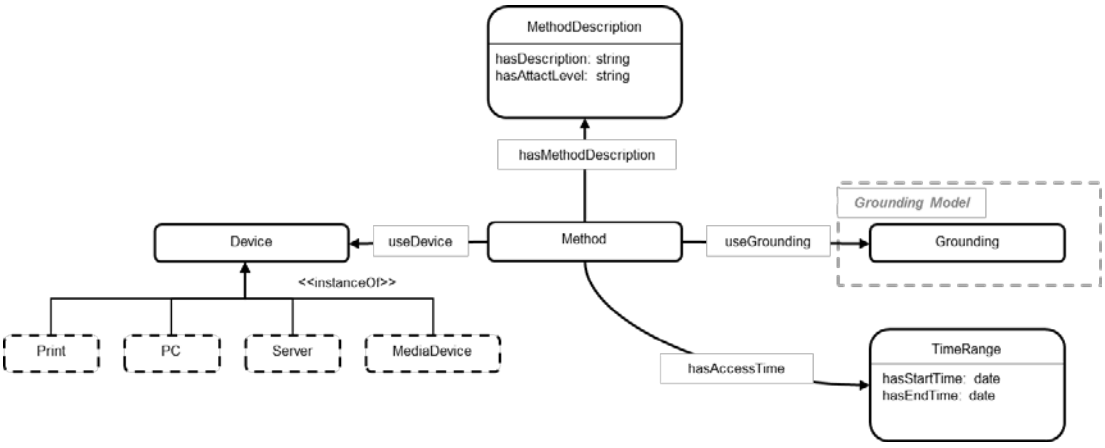


Fig. 3. Method Model

The Method class describes approaches regarding potential insider threats, and is supper class of the Method model. The MethodDescription class represents detailed information of the approaches such as short description of the approaches, and attack levels. To define attack level, we reference attack steps of a project, named Corporate Insider Threat Detection: Cyber Security Inside and Out [23]. In this project, they defined 77 attack steps regarding insider threat, in particular, they described data leakage attacks by insiders. The Device class represents device types used for insider threat. In order to expend device types, each device type is defined as sub class of the Device class. The TimeRange class describes a time information such as insider threat starting time, and finishing time. The Grounding class defined in the Grounding model is used to define accessing method on network. The details will be explained in section 3.3.

The Method model has no internal relationship between the Method class and other class including MethodDescription class, Device class, TimeRange class using object properties such as hasResurceDescription, useDevice, and hasAccessTime, but external relationship with the Grounding model through useGrounding. Accordingly, the model allow to define detailed method about insider threats.

3.3 Grounding Model

The Grounding model describes accessing interfaces on network to define network-based insider threat. As shown **Fig. 4**, the Grounding model is composed of five classes including Grounding, Protocol, Destination, StartingPoint, and Resource.

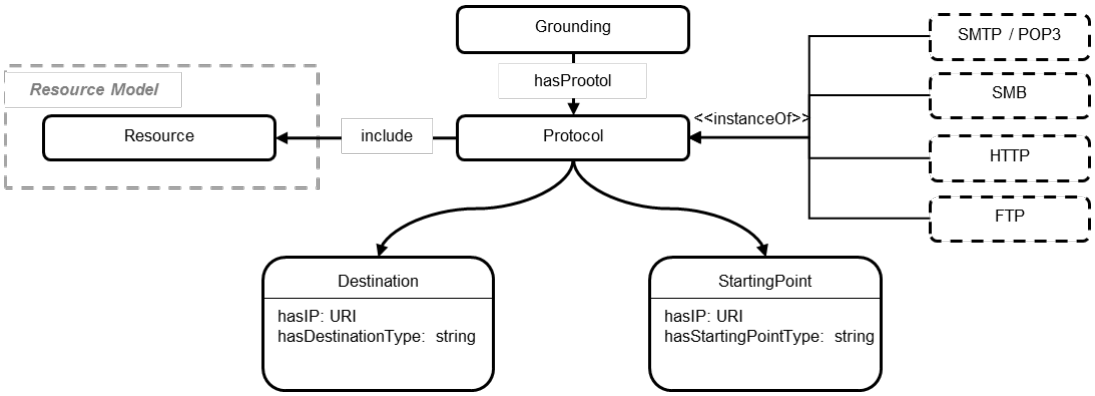


Fig. 4. Grounding Model

The Grounding class represents accessing method on network and is a supper class of the Grounding model. The Protocol class describes protocol type of network packets. Hence, common protocols such as STMP, SMB, HTTP, and FTP are defined as sub class of the Protocol class. The Destination class describes final destination of network packets. In here, destination IP and type are defined in data properties. The StartingPoint class describes start location of network packets. Same as Destination class, start IP and type are defined in data properties. In the Grounding model, individuals of the Destination class, and StratingPoint class are dynamically created in real time based on network packet. Accordingly, this model will use as trigger to discover insider threats.

4. Insider Threat Detecting Extractor

In this section, we describe implementation of prototype platform, named insider threat detecting extractor (ITDE). The ITDE allows to detect insider threat via understanding and interpreting network packet based on IB2O in real time. **Fig. 5** shows the overview of the ITDE.

First of all, managers in organizations such as companies or governments input information in order to predefine IB2O according to the policies of the organizations using ITDE user interface. At this time, the user interface will send this information inputted by manager to ITDE function modules, and then, this information will be defined as an individual of IB2O, as shown **Fig. 5-①**. Now, the IB2O is ready to detect insider treats through understanding and interpreting network packet. After creation of IB2O according to policy of organizations , the ITDE tries to collect network packet used by insider, as shown **Fig. 5-②**. In here, unlike predefined information, the network packet on network are created as individuals of the Grounding model in real time through semantic annotation, as shown **Fig. 5-③**. Hence, this created individuals are used to detect insider threat through comparing with predefined model such as the Resource, Description, and Method. In other words, ITDE detect insider threat by comparing annotated network packets with predefined individuals of Resource model, and

Method model as shown **Fig. 5-④**. Finally, the results of analyzing network packets will be reported to manager through ITDE user interface, as shown **Fig. 5-⑤**.

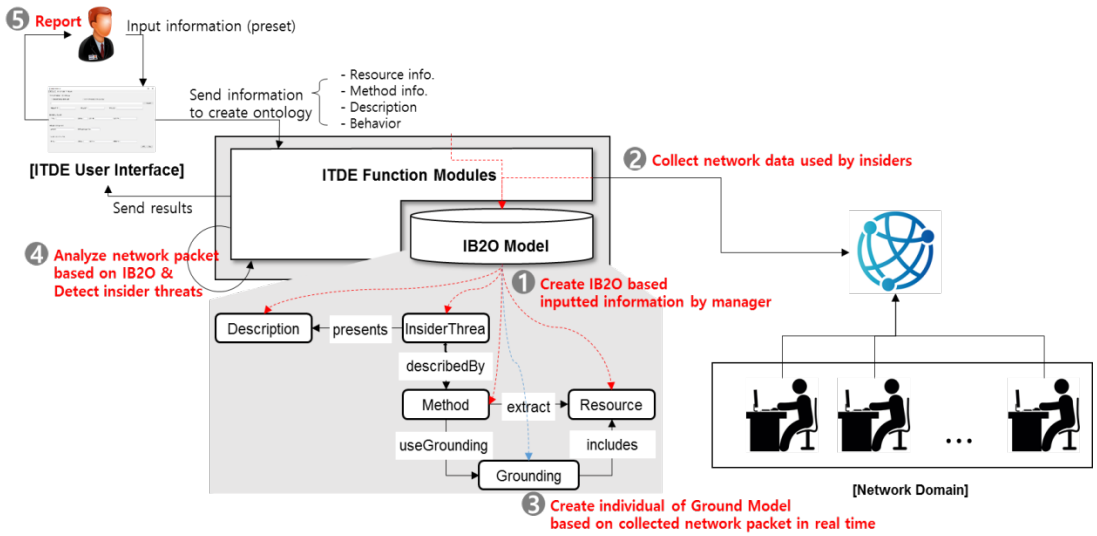


Fig. 5. The overview of insider threat detecting extractor (ITDE)

4.1 Architecture of ITDE

In this section, we describe architecture of ITDE. As shown **Fig. 6**, the ITDE consists of two software packages including user interface and function modules.

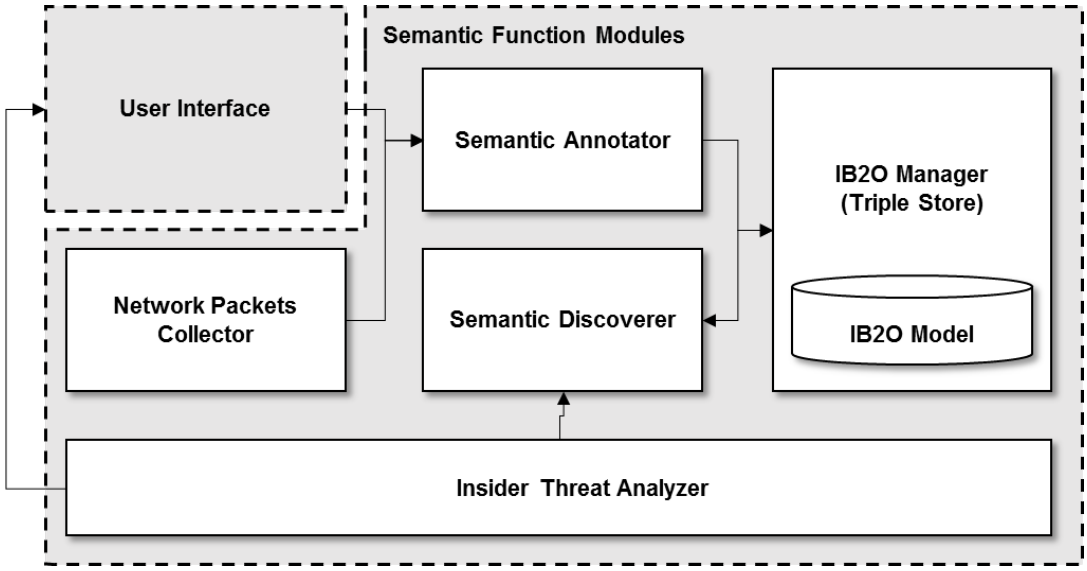
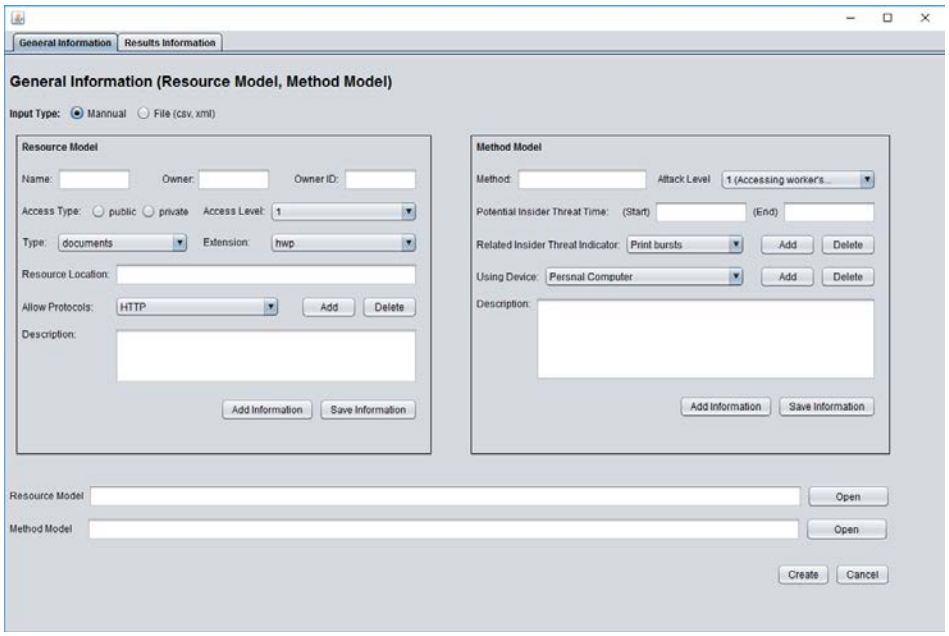


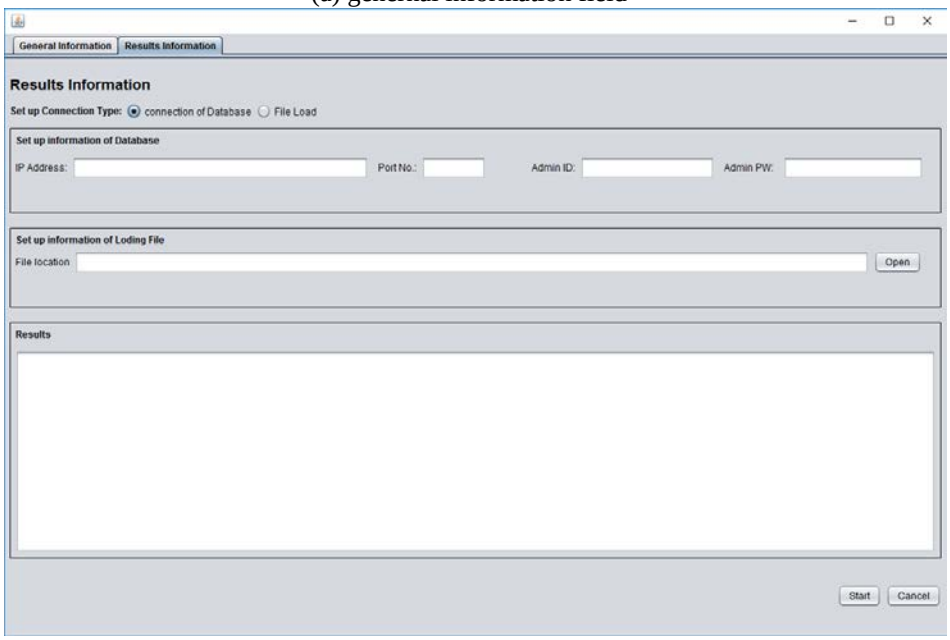
Fig. 6. System architecture of ITDE

4.1.1 User Interface

The user interface of ITDE (ITDE UI) enables to input information by manager, and also report detecting results to manager. In addition, the ITDE UI provides human readable information about the detected results. To this end, the ITDE UI consists of two fields as follow: (1) general information for creating IB2O; and (2) result information for collecting network packets and reporting results to manager. **Fig. 7** shows snapshots of ITDE UI.



(a) genernal information field



(b) results information field

Fig. 7. Snapshots of ITDE UI

As shown **Fig. 7-(a)**, the general information field allows selection of input types which is to manually input all of sub fields in Resource Model panel, and Method Model panel, or to upload files such as csv and xml. Subsequently, the information that will be in the general information field are created as individuals of the Resource Model, Description Model, and Method Model in the IB2O.

Fig. 7-(b) shows detailed results information field. In this field, ITDE UI requires connection types including database and file. Commonly, network packets used by insider are stored in local database or log files. Thus, we consider a way to collect network packets. Here, if user select connection type as database, user should fill information for accessing database such as IP address, port number, admin ID, and admin password.

Finally, the Results panel in the results information field shows human-readable results analyzed by semantic function modules. The information inputted by user using the ITDE UI are sent to semantic function modules in order to create the IB2O, and also semantic-based analyze network packet.

4.1.2 Semantic Function Modules

The Semantic Function Modules consist of five components such as Network Packets Collector, Semantic Annotator, Semantic Discoverer, Insider Threat Analyzer, and IB2O Manager. The Network Packets Collector gathers real time network packets used by insider on network from database or log files defined by user using ITDE UI. Then, the Network Packets Collector classifies the network packets by detailed information such as protocol, source IP address, destination IP address, and content type including extension. Finally, The Network Packets Collector send the detailed information according to predefined XML format to the Semantic Annotator.

The Semantic Annotator annotates information received from the Network Packets Collector and ITDE UI to translate as RDF triples (e.g., Turtle, RDF/XML, and JSON-LD) [24]. For this, the Semantic Annotator performs two semantic annotation: (1) initial semantic annotation; and (2) real time annotation. The initial semantic annotation enbles to represent information inputted in general information field of ITDE UI as RDF triples to create IB2O model according to explicit each model. It also provides to add additional information into the existed IB2O. Accordingly, the Semantic Annotator tries to discover existed IB2O in order to distinguish duplicated individuals before the creating IB2O. At this time, the duplicated individuals are ignored when the Semantic Annotator sends annotated initial information to the IB2O Manager to create IB2O.

The real time annotation also annotates detailed information received from the Network Packets Collector. However, unlike the initial annotation, the real time annotation creates individual without discovery from the existing IB2O in order to distinguish duplicated individuals. This is because, the real time annotation allows to represent real time network packet as individuals in order to apply annotation to all network packet, to analyzing process in the Insider Threat Analyzer via comparing between annotated network packets and creating individuals of Resource model, and Method model.

The Semantic Discoverer performs discovery of individuals from the IB2O Model according to requestion of the Semantic Annotator and Insider Threat Analyzer based on reasoning algorithm. In here, we use reasoner [25] provided by Apache foundation. The discovered results are sent to Semantic Annotator and Insider Threat Analyzer according to request owners, respectively.

The IB2O Manager performs to handle and create individual of IB2O model according to request the Semantic Annotator, and Semantic Discoverer. To manage the individuals, we use

Jena TDB [26] which is a RDF store and made by Apache foundation.

The Insider Threat Analyzer performs detecting detailed insider. To detect detailed insider threats, the Insider Threat Analyzer stats semantic-based analyzation regarding annotated real time network packets from the IB2O Manager. At this time, the Insider Threat Analyzer compares analyzed network packets with resource information including accessing level, owner, allowed protocols, and public or private from the Resource model. In here, if the analyzed results dose not match with the resource information, it will discover detailed insider threat method from the Method model based on protocol, used devices, and accessing time. Finally, detected insider threat methods are sent to the User Interface.

4.1.2 Implementation

In this section, we describe implementation of IB2O schema and ITDE. To create IB2O schema, we use protégé 5.0 [27] which is well-known ontology editing tool. **Fig. 8** shows Hierarchy of IB2O schema. In Fig 8, each model of IB2O is create in single ontology model due to represent relationships between them.

The ITDE is developed using Java, the Jena library on the we application server (WAS), *i.e.*, Tomcat 8.0. In the ITDE, In the ITDE, we developed a RESTful interfaces in order to connect with the ITDE UI. We also developed the Semantic Annotator, Semantic Discoverer, and Insider Threat Analyzer using the Jena library and SWRL [28]. In addition, we developed the IB2O Manager using the Jena TDB to manage semantic triples which are created in each model of IB2O. Thus, semantic queries for discovery of semantic triples are allowed in the ITDE based on SPARQL. Finally, the ITDE UI is developed using the Java Swing.

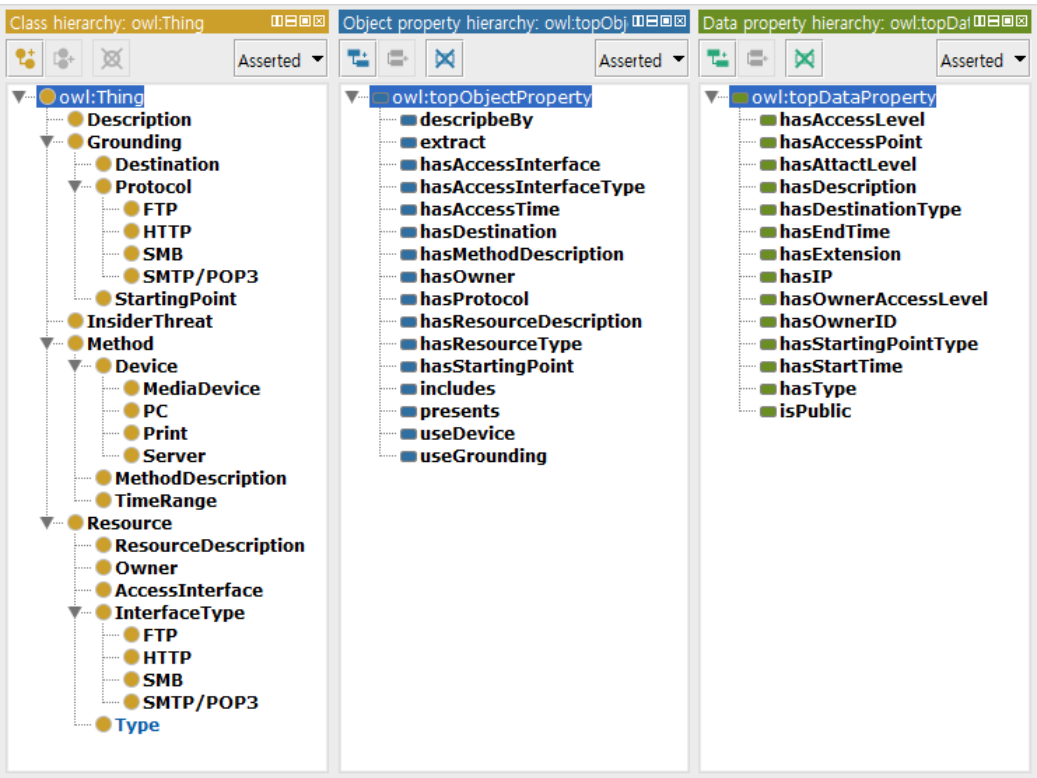


Fig. 8. Class hierarchy, Object Property, and Data Properties of IB2O schema

5. Performance Evaluation

In this section, we describe the feasibility of proposed IB2O by two evaluation processes (1) evaluating IB2O created by ITDE UI and (2) evaluating detection of malicious insider threat behaviors regarding network packet collect from network system. In (1), we use protégé to evaluate the individuals of IB2O focused on relationships between the individuals and annotation according to the general information inputted by the ITDE UI and schema of IB2O. To evaluate (2), we use CERT data [29] generated by their simulation instead of collecting network packet in real time.

5.1.1 Evaluation of IB2O

As mentioned above, to create individuals of IB2O, we input general information including potential insider threat behaviors, proprietary information, method about the behaviors, and description for human understanding using ITDE UI. In particular, we use activities shown in **Table 1** in order to define potential insider threat behaviors. **Fig. 9** shows snapshot of the inputted general information using ITDE UI.

To create individuals of IB2O, we input 30 activities to define potential insider threat behaviors, and we create 20 resources which have difference owners, location and types. In particular, all of resource dose not allow to access from other user using protocols including HTTP and FTP.

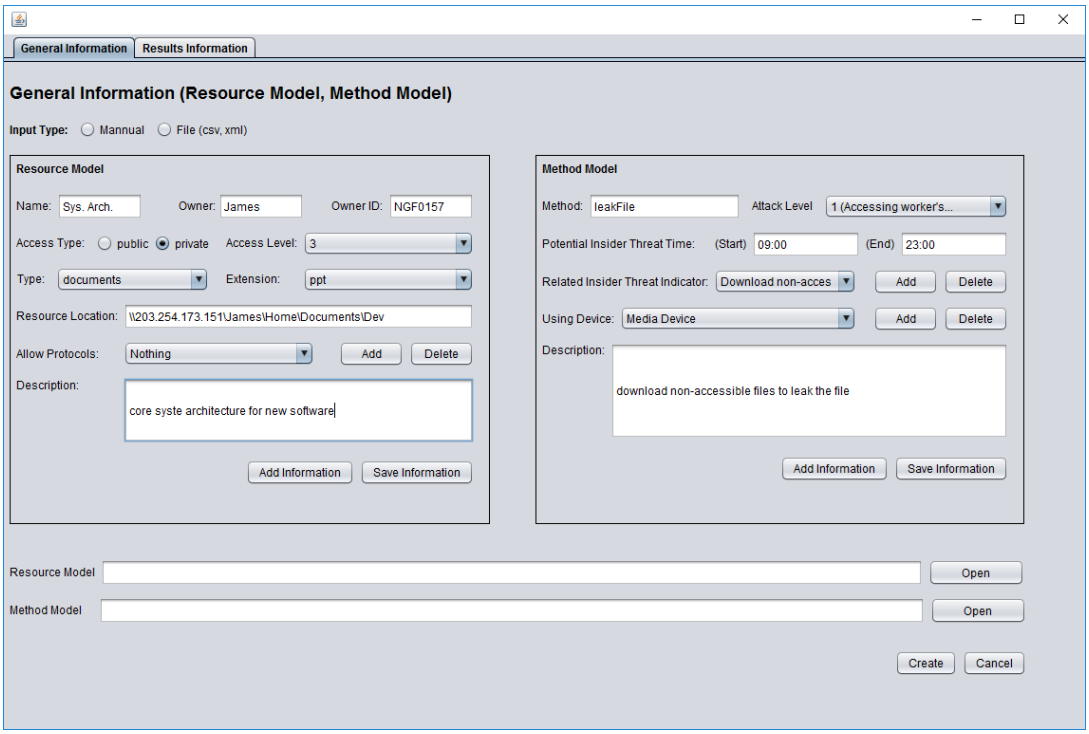


Fig. 9. A Snapshot of the inputted general information using ITDE UI

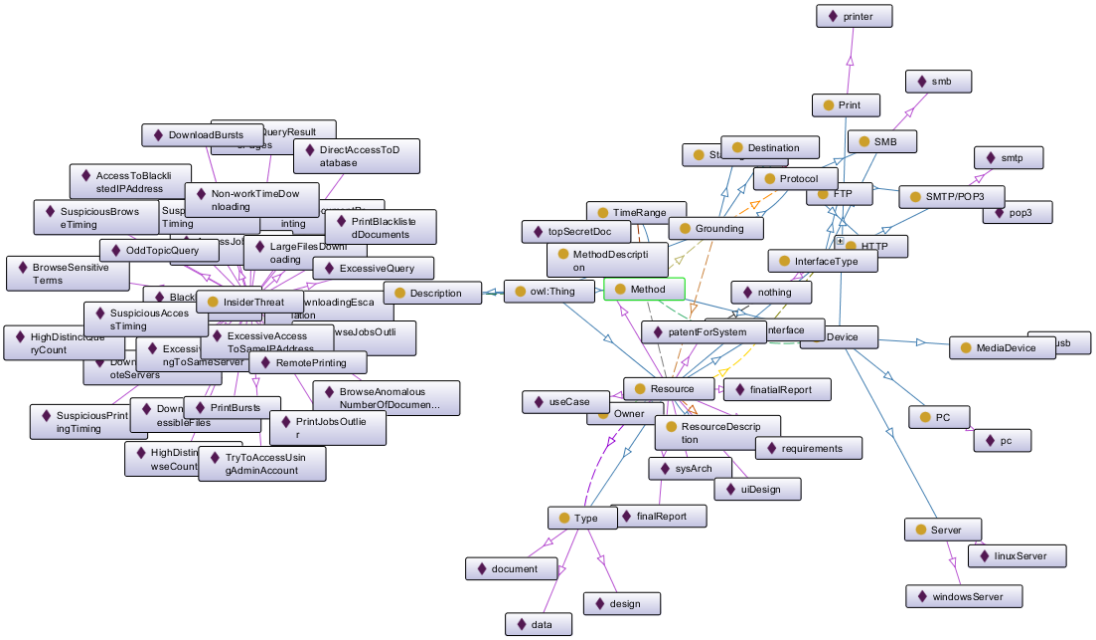


Fig. 10. The result of individuals of IB2O including relationships between them

Finally, we create methods with its short description regarding the 30 activities. **Fig. 10** shows individual of IB2O created by ITDE UI including relationships between the them. In **Fig. 10**, purple diamante and yellow circle denote individuals and denote classes, respectively. And arrow denote relationships between individuals. From the results, we validated the IB2O created by ITDE UI regarding schema and relationships.

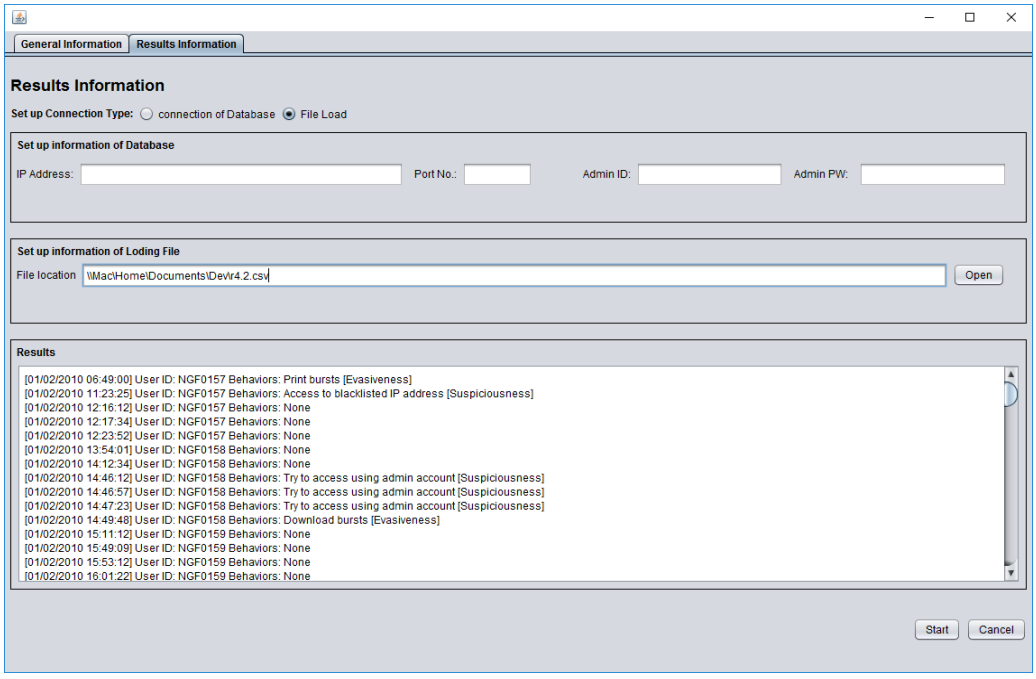


Fig. 11. A snapshot of showing results

5.1.2 Evaluation of detection of malicious insider threat behaviors

In this section, we describe evaluation of detecting insider threat behaviors based on the IB2O created in section 5.1.1. To evaluate this process, we use CERT data generated by Insider Threat Tool developed by CERT division. We use 13,992,172 data. In order to efficiently evaluate the performance of detection, we divide all number of data (i.e., 13,992,172) into each day (i.e.,141,294). We extract session data (i.e., 29,719) from the each day data, and acquire the results of predicted condition regarding the session data. As shown in **Table 3**, the calucuate recall based on detecting result of the session data is 93% (9,143 / (9,143 + 19,220) = 0.931). **Fig. 11** shows snapshot of showing result regarding 1 day.

Table 3. The results of predicted condition regarding session data

	29,719	**Predicted Condition**		
		Positive	Negative	Session Data
Actual Condition	Positive	1,263	93	1,356
	Negative	9,143	19,220	28,363
	Session Data	10,406	19,313	29,719

6. Conclusions

In this paper, we have presented an indicator-based ontology (IB2O) to detect malicious insider threat behaviors using real time network packets. We designed and developed an ontology model in order to understand and interpret the meaning of network packets. To this end, we designed and developed five-sub ontology including InsiderThreat model, Resource model, Description model, Method model, and Grounding model. In order to create the ontology flexibly, we also developed an interface called ITDE UI. The UI could more help to the IB2O according to the requirements or policy of companies or organizations. With the proposed method, we have tried to touch three main challenging problems to apply the semantic technologies to detecting potential insider threats: well-defined ontology model for interpreting the meaning of network packets, comprehensive semantic representation regarding potential insider threats, and flexibly changing of ontology model. To show the practical feasibility of proposed ontology, we developed ITDE which can collect network packets from network systems, and also detecting insider threat behaviors based on the IB2O regarding the collected network packets. With the ITDE, we perform evaluation using CERT data. Through the evaluation, we have shown that the IB2O can detect insider threat behaviors using network packets with this we can conclude with confidence that the IB2O can eventually contribute to detecting insider threat behaviors in network systems.

References

[1] Kroll and Economist Intelligence Unit, “Annual Global Fraud Report. 2015/2016,” 2016.
[2] PricewaterhouseCoopers LLP, “Cybercrime: Protecting against the growing threat - Events and Trends,” 2012.
[3] Spitzner, L., “Honeypots: Catching the insider threat,” in *Proc. of 19th Annual IEEE Computer Security Applications Conference, 2003*, pp. 170-179, 2003. Article (CrossRef Link)
[4] CERT Insider Threat Center, “2014 U.S. State of Cybercrime Survey,” 2014, Available online: http://resources.sei.cmu.edu/asset_files/Presentation/2014_017_001_298322.pdf (accessed on 21 November 2016).

[5] IBM, "IBM 2015 Cyber Security Intelligence Index," 2015, Available online: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&htmlfid=SEJ03278USEN&attachment=SEJ03278USEN.PDF&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US (accessed on 21 November 2016)
[6] Robert N. Rose, "The Future Of Insider Threats," 2016, Available online: http://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/2/#3240ea4e3381 (accessed on 21 November 2016)
[7] Berners-Lee, T., Hendler, J., Lasslia, O., "The semantic web," *Scientific American*, pp. 28-37, 2001. Article (CrossRef Link)
[8] R. Anderson, T. Bozek, T. Longstaff, W. Meitzler, M. Skroch, K. Van Wyk, "Research on Mitigating the Insider Treat to Information Systems," in *Proc. of the Insider Workshop*, August 2000.
[9] F. L. Greitzer, A. P. Moore, D. M. Cappelli, D. H. Andrews, L. A. Carroll, and T. D. Hull, "Combating the Insider Cyber Threat," *IEEE Security & Privacy*, pp. 61–64, 2007. Article (CrossRef Link)
[10] Costa, D. L., Collins, M. L., Perl, S. J., Albrethsen, M. J., Silowash, G. J., Spooner, D. L., "An Ontology for Insider Threat Indicators," in *Proc. of 10th International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS)*, 2015.
[11] van Heerden, R. P., Irwin, B., Burke, I., "Classifying network attack scenarios using an Ontology," in *Proc. of of the 7th International Conference on Information-Warfare & Security (ICIW 2012)*, pp. 311-324, January 2012.
[12] Aleman-Meza, B., Burns, P., Eavenson, M., Palaniswami, D., Sheth, A. P., "An Ontological Approach to the Document Access Problem of Insider Threat," in *Proc. of IEEE Intl. In Conference on Intelligence and Security Informatics (ISI-2005)*, 2005. Article (CrossRef Link)
[13] Greitzer, F. L., Hohimer, R. E., "Modeling human behavior to anticipate insider attacks," *Journal of Strategic Security*, vol. 4, no. 2, pp. 25-48, 2001. Article (CrossRef Link)
[14] Raskin, V., Taylor, J. M., Hempelmann, C. F., "Ontological semantic technology for detecting insider threat and social engineering," in *Proc. of the 2010 workshop on New security paradigms ACM*, pp. 115-128, September 2010. Article (CrossRef Link)
[15] Nirenburg, S., Raskin, V., "Ontological Semantics," *MIT Press*, 2004
[16] Symonenko, S., Liddy, E. D., Yilmazel, O., Del Zoppo, R., Brown, E., Downey, M., "Semantic analysis for monitoring insider threats," in *Proc. of International Conference on Intelligence and Security Informatics*, Springer Berlin Heidelberg, pp. 492-500, June 2004. Article (CrossRef Link)
[17] Advanced Research and Development Activity (ARDA), Available online: http://www.ic-arda.org/ (accessed on 21 November 2016)
[18] Karande, M. H. A., Kulkarni, M. P. A., Gupta, S. S., Gupta, D., "Security against Web Application Attacks Using Ontology Based Intrusion Detection System," *in Proc. of 2015 International Conference on Communication Networks (ICCN)*, Gwalior, India, November 2015. Article (CrossRef Link)
[19] Wang, H., Wang, S., "Cyber warfare: steganography vs. steganalysis," *Communications of the ACM*, vol 47, no. 10, pp. 76-82, 2004. Article (CrossRef Link)
[20] Obrst, L., Chase, P., Markeloff, R., "Developing an Ontology of the Cyber Security Domain," in *Proc. of CEUE Workshop on STIDS*, pp. 49-56, October 2012.
[21] Stephens, G. D., Maloof, M. A., "U.S. Patent No. 8,707,431," *Washington, DC: U.S. Patent and Trademark Office*, 2014
[22] Coalition, D. S., "DAML-S: Semantic markup for Web services," in *Proc. of the International Semantic Web Workshop (SWWS-01)*, 2001.
[23] I. Agrafiotis, J. R. C. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, "Insider Threat Attack steps," Corporate Insider Threat Detection (CITD), Available online: https://www.cs.ox.ac.uk/files/7011/Attack%20steps.pdf (accessed on 21 November 2016).
[24] Klyne, G., & Carroll, J. J., "Resource description framework (RDF): Concepts and abstract syntax," W3C Recommendation, 2006.

[25] Apache Jena, "Reasoners and rule engines: Jena inference support." Available online: https://jena.apache.org/documentation/inference/ (accessed on 21 November 2016).
[26] Apache Jena, "TDB Architecture," Available online: https://jena.apache.org/documentation/tdb/architecture.html (accessed on 21 November 2016).
[27] Protégé 5.0, Available online: http://protege.stanford.edu (accessed on 21 November 2016)
[28] Horrocks, I., Patel-Schneider, P.F., Boley, H., Tabet, S., Grosof, B., Dean, M., "SWRL: A semantic web rule language combining OWL and RuleML." Available online: http://www.w3.org/Submission/2004/SUBM-SWRL-20040521/ (accessed on 21 November 2016).
[29] CERT, http://www.cert.org/insider-threat/tools/index.cfm (accessed on 21 November 2016)

Janghyuk Kauh received his B.S. and M.S. degrees from Kwangwoon University, Seoul, Korea in 1996 and 1998, respectively. Currently, he is working for Ph. D. degree on Computer Science in Kwangwoon University. He is working for Agency for Defense Development (ADD), Seoul, Korea, from 1998 to now. His research interests are in computer security, insider threat, machine learning techniques applied to the military network.

Wongi Lim received the B.S. degree from Konkuk University, Seoul, Korea, in 1994 and the M.S. degree in Department of Computer Science and Engineering from Konkuk University, Seoul, Korea, in 1996. Currently, he is working for Agency for Defense Development, Seoul, Korea from 1996 to now. His research interests include tactical data link network and protocol, information security for insider threat.

Koohyung Kwon received the B.S. and M.S. degrees from Korea University, Seoul, Korea in 2001 and 2003, respectively. He is working for the Agency for Defense Development of Korea. His current research interests include cyber security for insider threat, cyber command and control.

Jong-Eon Lee received his B.S., M.S., and Ph.D. degrees in Computer Science from Kwangwoon University, Seoul, South Korea, in 2001, 2003, and 2007, respectively. Since 2008, he has been working for Hanwha Systems R&D Center as a Chief Engineer. His research interests include Tactical Communication Networks, Wireless Sensor Networks, Wireless Mesh Networks, Advanced Network Management Technology, and Big Data Processing Technology.

Jung-Jae Kim received his B.S. and M.S. degrees in Computer Science from Kwangwoon University, Seoul, Korea in 2013 and 2015, respectively. He is currently working on Ph.D. course at the Department of Computer Science, Kwangwoon University, Seoul, Korea. His research interests include Intelligent Network System, Machine Learning and Deep Learning.

Minwoo Ryu received his B.S. degree in Internet Information Processing from Yeoju Institute of Technology, Korea in 2007, and his M.S. and Ph.D. degrees in Computer Science from Kwangwoon University, Seoul, Korea in 2009 and 2012, respectively. From 2011 to 2016, he worked as a research scientist at Korea Electronics Technology Institute (KETI), Korea. He is now a research scientist in the KT R&D center, Korea Telecom (KT), Korea. His research interests include Internet of Things, Semantics, Cognitive Computing, Intelligence Service and Vehicular Ad Hoc Networks.

Si-Ho Cha is a professor in the Department of Multimedia Science, Chungwoon University, Incheon, South Korea. He received his Ph.D. degree in Computer Science from Kwangwoon University, Seoul, South Korea in 2004. From 1997 to 2000, he worked as a senior researcher at Daewoo Telecom R&D Center, Korea. His research interests include network management, wireless sensor networks, vehicular ad hoc networks, semantic web, and web of things.