OWL ONTOLOGY REPRESENTATION UNDER A SECURE MOBILE CONTEXT

Silvia Trif [1]
Madalina Zurini [2]

Abstract

This paper aims to assess ontology representations under a secure mobile applications context. Mobile applications security aspects are defined, identifying the vulnerabilities and threats. Mobile devices limits are presented. Modalities of assuring security process are presented. Cryptographic algorithms are presented. The ontology term is described in the context of evolution that time generated upon it. The main standard language, OWL, is applied for creating an ontology that describes the mobile applications' security aspects. The need of ontology in security of mobile applications is highlighted at the conclusions' level of the paper.

Keywords: mobile applications security, ontology, vulnerabilities, threats, OWL representation.

Introduction

Mobile devices have become necessary for everyone, they are indispensable for everyday use. For this reason, mobile devices market is in a fully extension, and not only, like this, there are diversified the types of mobile applications demand. Because mobile devices are used in every process and task of the day, for example not only for making phone calls, but to read and send mails, to read newsletters on the web, to play games, the need of security for applications is encountered.

Mobile applications, as every software application, must be secured, must have a good quality management, and for assuring these, there are followed internationals quality standards for software product (as ISO 9126 standard and others related standards).

For assuring a good quality management for mobile applications, there are identified mobile applications vulnerabilities and threats, threats determined not only by the software product, but by the mobile devices also.

Mobile devices have some limited characteristics, as follows:

- mobile devices screen dimension and resolution;
- the memory of mobile devices;
- the storage capacity.

Because nowadays, using mobile devices information is transferred throughout the network, the users' changes their profile on the network with others users, and not only for these reasons, the mobile application security should be assured, using authorization, authentication and encryption models.

---

[1] Ph.D. Candidate, Academy of Economic Studies, Bucharest, Romania, silviatrif@gmail.com
[2] Ph.D. Candidate, Academy of Economic Studies, Bucharest, Romania, madalina.zurini@gmail.com

Mobile applications market is developing faster; there are demands not only on Windows Mobile system, but on all mobile devices operating systems (Symbian, Blackberry, IOS and Android); mobile applications supply is also growing, developing.

These mobile applications have an important role in society, because using these, there are developed easier interpersonal relationships, the society members can interact one with each other not taking into account the distance between the users.

Many applications are developed that are used as Facebook, a way of socializing between users.

Designing such mobile applications that are used in everyday activities must meet the quality demands of each step of the life cycle process. Software engineering stands for this systematic approach to the analysis, design, assessment, implementation, test, maintenance and re-engineering software, as defined in [6]. Step by step, knowledge engineering appears as a way of representing the knowledge that is used in a specific process. Because of that, the current paper wishes to present a knowledge perspective upon the security concept in the area of mobile technologies.

Mobile applications' security aspects

Mobile development is a new branch of software applications' development. In the past years, there is encountered a continuous developing process for Windows Mobile operating system, Symbian and Android. In this article is treated the security of mobile applications developed for Windows Mobile Operating System.

There are different types of mobile applications architectures, which are detailed in [1]:

- client-server
- standalone
- network.

All these architectures provide vulnerabilities for mobile applications. For assuring a secure data transfer between mobile devices and mobile devices and servers, there are used standards and protocols. The protocols and standards used are described in [1].

The security aspect is a must that should be took into account, identifying in the first place the risks, the vulnerabilities that can affect the application, the ways of reducing and treating these risks, the ways of dealing with them. The risks are reduced building reliable security and control mechanisms. These aspects are presented in [1].

For building a reliable security system for the application, there must be identified:

- *the objectives of the application*; if the scope of the application is well known, and the department where the application will be build is well known, there can be identified all the possible risks that can appear and the ways in which these risks are treated; there should be identified the goal objective and the applications' specific objectives;

- *the characteristics given by the mobile devices*; there must be taken into account the situation of large databases, which cannot be kept on the phone, because of the memory space, the security protocols used for data transfer, the time needed for these transfers;
- *the security related to the objectives*; there are identified all the applications' vulnerabilities starting with the applications' objectives. The more complex objectives are the more complex the application is.

  Security objectives refer to:
- the *confidentiality*, *integrity* and *availability* aspects must be in a balance, and all these aspects should be treated in approximately the same proportions;
- the *security mechanisms must not interfere with mobile application usability*, and the security mechanisms must be transparent.

Realizing a risk analysis, there are determined the exposure to threats and their impact on the application.

In quality management, there are various types of treating the risks and avoiding their consequences [1]:

- *acceptance*; there are not taken actions to avoid these risks, there are taken as they are, with their consequences;
- *impact mitigation*; there are taken special measures for reducing the consequences of these risks;
- *transfer*; the responsibility of these risks is externalized, external components deal with the producing of the risks.

There are identified the following threats of mobile applications, *threats* treated also in [1], [2] and [3]:

- *authentication*; represents the process of establish that the user is who claims to be, the application send a request to the security component, which will prove the user identity;
- *authorization*; represents the process of determining if a validated entity has rights to access a secure resource;
- *integrity*; represents the process of assuring that the unauthorized entity cannot destroy or change the application data (data integrity process, SQL-injection process);
- *availability*; functionality must be available to the users in spite of Denial of Service attacks;
- *confidentiality*; the information is available only for authorized entities;
- *independence*; represents the business registration system assuring the events reconstruction;
- *non-repudiation*; represents the process of preventing the denial of the role of a participant in a transaction;
- *uniqueness of the record*; an authenticated user can access all the resources permitted, without re-authenticating using sessions;
- *secure management*; represents the process of assuring the control of security mechanisms;
- *session protection*; only the authenticated user have access to its dates, other users cannot take control of the other user authentication and authorization information;

- *integration and analysis of logs*; is the process of querying, analyzing, alarming all application components log events; there are managed all the time the users access in the application;
- *security uniform granularity*; there are identified access controls rules for being used for similar user access and gestures;
- *the network security protocols and standards used*; this threat is encountered at the network type application or client-server applications; the information travel throughout a network and the unauthorized users can try to access it.

Following these identified threats there can be mentioned the following *vulnerabilities* of mobile applications:

- authentication of unauthorized users;
- authorization of unauthorized users at data;
- SQL-injection realized by an unauthorized access, or just changing's of data;
- unavailability of data;
- access to confidential information for unauthorized users;
- vulnerabilities given by the network access throughout the security protocols and standards;
- data transfer using sessions over the network;
- application failure given by mobile devices hardware failure, incompatibility between the application and mobile device characteristics.

The ways of treating these threats and vulnerabilities is to assure secure mechanisms, using encryption mechanism.
There are various cryptographic mechanisms, which are treated in specialist literatures.

In [1], [2], [3], [4] and [5] there are presented and detailed the following security mechanisms:

- *public-key –infrastructure PKI mechanisms*; which use encryptions and digital certificates; this mechanism uses pairs of public/private keys, which are used the encrypt and decrypt the sent message;
- *fingerprint authentication*; a fingerprint scanner is used to scan user finger;
- *password authentication*; a password is used to access information;
- *smartcards uses*; the PKI information is kept on smartcards;
- *biometrics*; there are used users physical characteristics as encrypted information;
- *voiceprint*; the voice sample is compared with the user's voice for authenticating process;
- *video authentication*.

Encryptions mechanisms are developing faster, even as open source components; this is a field where more and more developers get involved.
Regarding mobile applications security aspects, security algorithms have an important role and attention.

Ontology evolution

Ontology has become an important aspect in nowadays because of the growth of information circulated over the Internet. A standard for representation of information is needed so that the effort made in a certain domain can be used be another analyze for obtaining the maximum benefit from the total directions involved in each domain that is represented. Let us define the K function, called knowledge function, where K(y) measures the impact, seen as a benefit, of the y information represented in the frame of ontology. The objective of the K function is the following:

$$\begin{cases} \max\limits_{R_i} K\left(\sum\limits_{i=1}^{n} R_i\right) \\ K\left(\sum\limits_{i=1}^{n} R_i\right) > \sum\limits_{i=1}^{n} K(R_i) \end{cases}$$

where:

- R_i is the *i* representation from the total of $i = \overline{1,n}$ number of representations of the total representations of information used in a certain domain;
- $K\left(\sum\limits_{i=1}^{n} R_i\right)$ is the knowledge benefit of integrating the whole ontology defined in a certain domain;
- $\sum\limits_{i=1}^{n} K(R_i)$ is the sum of the knowledge benefit generated by each ontology;
- $K\left(\sum\limits_{i=1}^{n} R_i\right) > \sum\limits_{i=1}^{n} K(R_i)$ the value function of the total ontology integration is greater than the sum of the values generated by all the representations one by one.

Ontology was first a philosophy discipline that was handing with the nature and organization of reality. The term of ontology comes, or is a subset, from information retrieval, that is the representation, storage and organization of information. Both two directions from which ontology in engineering was born have the same roots, and primal objective, that is to model a input data, nature, reality, a certain domain, and to extract the major information that can characterize that input data.
In figure 1, the main directions given by the term of ontology engineering: basic topics, design, applications, development and knowledge sharing and reuse.

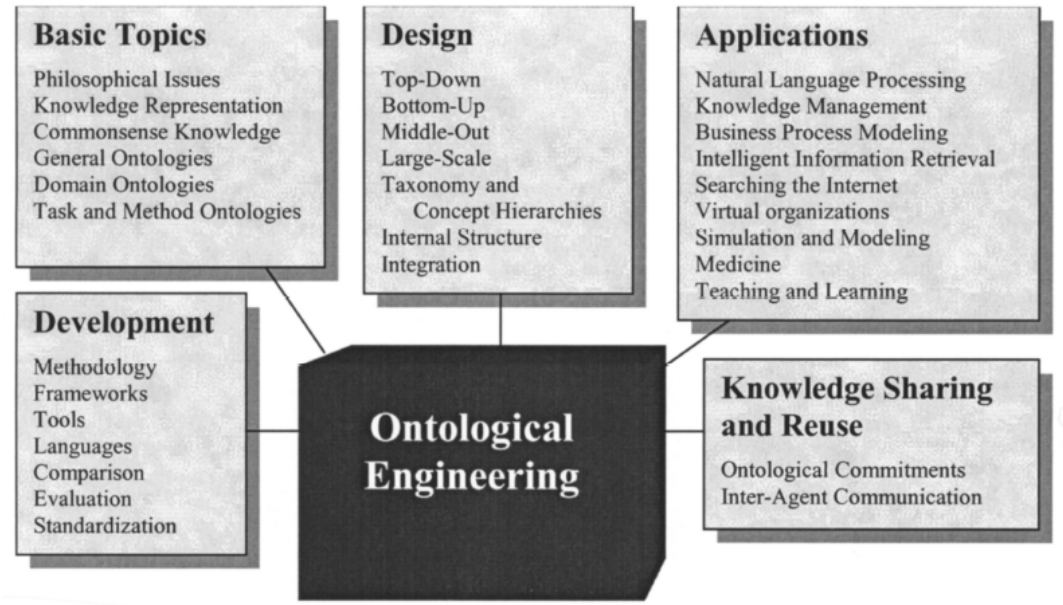

Fig. 1 Main concepts used in ontological engineering, [8]

From the perspective of ontology taxonomy, in [9], 2 directions are formed:

- type of information;
- internal structure.

Guarino also used this level of classification of ontologies, when he designed figure 2, as a representation of the relations between top-level ontology, the most general ontology because they express very basic knowledge, domain ontology, are related to top-level ontology, but define a particular domain, task ontology, a top-level ontology for tasks and activities, and application ontology are used to fulfill the need for ontology for a specific application.

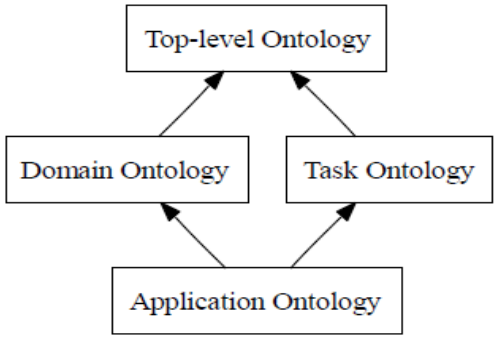

Fig. 2 Guarino ontology classification

The other dimension used for ontology classification is by the richness of the internal structure. For that, in [10], the level of complexity and powerful refer to a line drawn in figure 3. Also regarding the complexity of an ontology, in [11], the distinguish of lightweight ontology and heavyweight was made, when the lightweight uses concepts,

taxonomies of concepts, relationships, properties, and the heavy weighted one including also axioms and constraints, beside the one mentioned for the light weighed one.

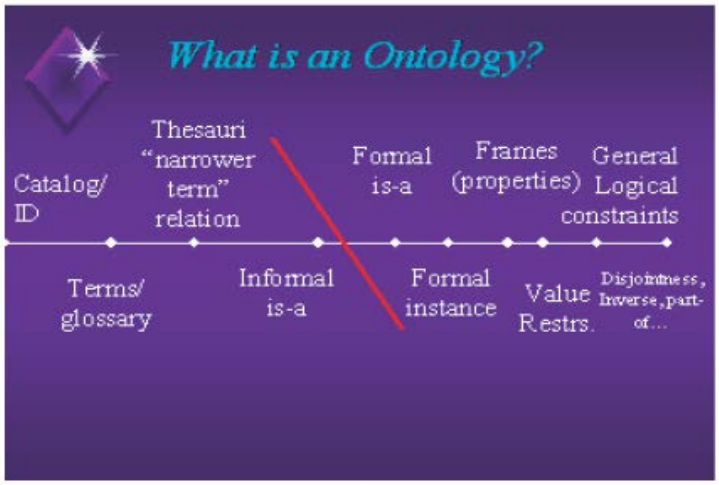

Fig. 3 Ontology level of complexity, [10]

In [7], the concept on ontology is seen from the view of the necessities listed below:

- sharing a common understanding of the structure of information;
- enabling the reuse of domain knowledge;
- making the domain assumptions explicit;
- separating domain knowledge from operational knowledge;
- analyzing the domain knowledge.

The primal concept around which an ontology is designed is the class that describe the concepts of a certain domain. A class is consisted of a set of attributes and properties. Figure 4 is a design of the main components of a class.

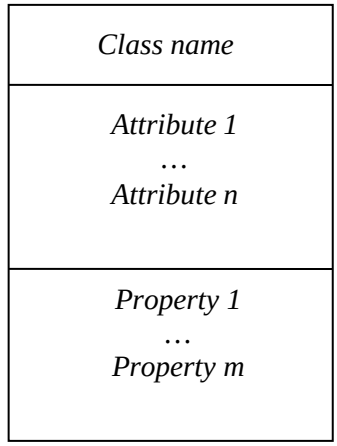

Fig. 4 Main components of a class

When implementing an ontology, a set of actions must be accomplished:

- delimiting the classes from the domain;
- hierarchy of the above mentioned classes;
- developing attributes and properties for each class;
- setting the values for the attributes and properties.

By understanding the main goal of an ontology, that is to represent as accurate as possible a certain domain, we can argue that it can be applied also in the field of security, more precise the security of mobile applications. The next step is to use the above mentioned components from which an ontology is created and to customize them for our dimension.

Security ontology's representation model

The language used for representing the ontology for the security of mobile applications is OWL, Web Ontology Language, which has 3 sublanguages:

- OWL Lite supports classification hierarchy and simple constrains;
- OWL DL is a correspondence to description logics and contains all OWL language concepts, except for a class to be an instance of another class;
- OWL Full is the complete format of OWL language.

Following, the features used in OWL are described. First of all, as mentioned in chapter 3, the class is the main component of an ontology, defined as a group that belongs together because they share some properties. It can be of two types: a thing class, that is a class of all individuals and is the superclass of all OWL classes designed, and a nothing class, a class that has no instances and is a subclass of all OWL classes.

Properties are used to state relationships and are of two types: ObjectProperty and DatatypeProperty. A domain is called a global restriction, while a range is a list of limited values that a property can have as its value. The instances of a class are called individuals.

The characteristics of a property are: ObjectProperty , DatatypeProperty, inverseOf, TransitiveProperty, SymmetricProperty, FunctionalProperty, InverseFunctionalProperty. Inverse of is the state of the property of being the inverse property of another one. Transitive property is described as if (x,y) is an instance of P and (y,z) is an instance of P, then (x,z) is also an instance of P. Symmetric property is represented by if (x,y) is an instance of P, then (y,x) is also an instance of P. The fact that the maximum cardinality is 1 and the minimum is 0 is related to the functional property. Inverse functional property is the state of a property to be inversed, to have more than one value.

In figure 5, an ontology regarding security domain was conducted. The main classes where added, along with the relations among them.

The process starts from a threat, which is a potential danger to the assets, and which affects the security attributes. A thread is exploited by vulnerability. The other section is represented of the control side that is implemented by the assets owned by the organization. There are different standard controls that a control can correspond.

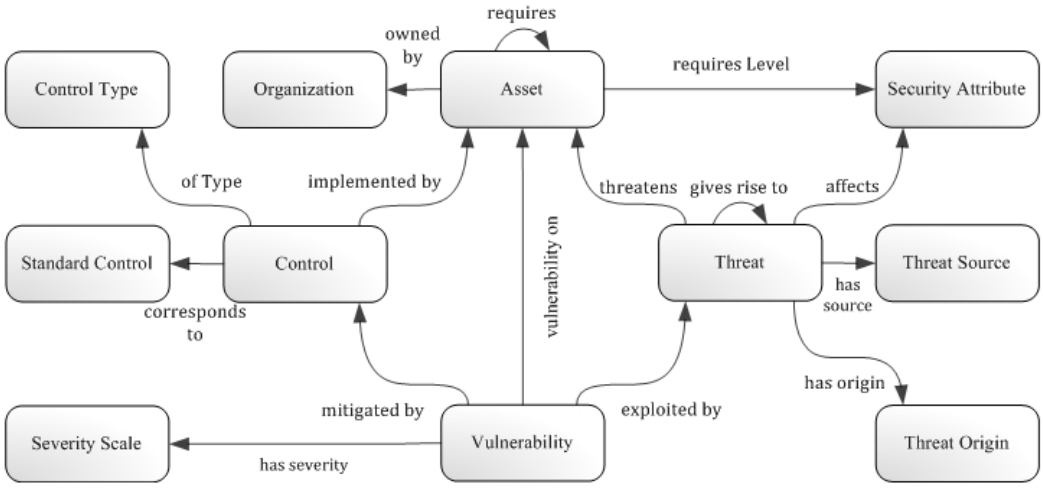

Fig. 5 Security ontology, [13]

Relating the previous ontology, a sub domain of security is mobile applications' security, with its particularities. The limitations made by the diminished dimensions, memory and processor capacity transform the level on security into a more restrictive one.

Conclusions

Mobile applications security aspect has an important role in developing new and more complexes software products, because there are identified various types of vulnerabilities and threats, which must be prevented and treated.

Network mobile applications have the greater number of vulnerabilities, there can be vulnerabilities given by the database, which is stored on a server, the interaction between mobile device and server, the application is running on the device, and the vulnerability is given by the fact that unauthorized users can try to authenticate and to pretend to be another persons.

Security mechanisms must be implemented for protecting data from attacks. For implementing these mechanisms, there are used cryptographic algorithms, like PKI mechanism, fingerprint, password authentication, smartcards and biometrics mechanisms. By assuring a security mechanism, mobile applications are more reliable and secure.

Ontology shouldn't be seen as an external, collateral part of the developing software process, but as an intensive perspective that is needed for a better understanding since the beginning of the life cycle of a software product. Security in mobile context can be represented and can answer main questions that are put concerning the security process.

In the article it is proven the fact that is an ontology is correctly defined and used, the quality of the final result, the software product, is increasing.

References

[1] A. Visoiu, S. Trif. "Open Source Security Components for Mobile Applications", *Open Source Science Journal*, Vol. 2, pp.155-166, No. 2, 2010, ISSN 2066-740X

[2] I. Ivan, A. Visoiu, S. Trif, B. Vintila, D. Palaghita. **"** The Security of the Mobile Citizen Oriented Applications", *Economy Informatics*, Vol. 10, pp. 22-33, No. 1,

2010, ISSN 1582-7941
[3] H. Dwivedi, C. Clark, D. Thiel. *Mobile Application Security, USA*, McGraw Hill Professional, pp. 79-119, 2010
[4] W. Jansen, R. Daniellou, N. Cilleros. "Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation", [Online], Available at: http://csrc.nist.gov/publications/nistir/NIST-IR-7290-pp-mobileFprint-final.pdf, March,2006 [Nov. 26, 2010]
[5] V. Matyas, Z. Riha. "Biometric authentication – security and usability", [Online], Available at: http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf, 2002 [Nov. 26, 2010]
[6] Software Enginnering, [Online], Available at: http://en.wikipedia.org/ wiki/Software_engineering
[7] N. F. Noy, D. L. McGuinness. "Ontology Development 101: A Guide to Creating Your First Ontology", [Online], Available at: http://protege.stanford.edu/publications/ontology_development/ontology101.pdf
[8] V. Devedzic. "Understanding Ontological Engineering", *Communications of the ACM*, Vol. 45, pp. 136-144, No. 4, 2002, ISSN 0001-0782
[9] H. B. Styltsvig. "Ontology-based Information Retrieval", Dissertation, Faculties of Roskilde University, *Computer Science Section*, Denmark, 2006
[10] O. Lassila, D. McGuiness. "The role of frame-based representation on the semantic web. Technical report', *Knowledge Systems Laboratory*, Standford University, California, 2001
[11] O. Corcho, M. F. Lopez, A. Gomez-Perez. "Methodologies, tools and languages for building ontologies: where is their meeting point?", *Data Knowledge Engineering*, Vol. 46, pp. 41-63, No. 1, 2003, ISSN 0169-023X
[12] REC OWL Features, [Online], Available at: http://www.w3.org/TR/2004/REC-owl-features-20040210/#Class
[13] OWL Security Ontology, [Online], Available at: http://securityontology.securityresearch.at/description/