BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXI No. 3/2009	345 - 351	Seria Tehnică

Protection of Critical Information Infrastructures by Means of Context-aware Services

Marian Costea

Petroleum – Gas University of Ploieşti, 39 Bucureşti Blvd., Ploieşti, ROMÂNIA
e-mail: costeamarian@gmail.com

Abstract

Due to the increasing dependence upon technology of contemporary society, critical information infrastructures and their preservation to their best parameters acquire more and more importance. Expanding an interlacing continuously, these infrastructures crossed national boundaries and aim to spread to a global scale; therefore security risks are the main concern of the entities which manage and exploit them, from international, regional, national organization, providers, to the end-users. Because of the diversity of services and data formats and of the geographical distribution, to ensure inter-operability and data integration – some of them with real time and emergency attributes – is a difficult and costly but nevertheless necessary task. A possible solution to this complex problem is the semantic integration of data and services, by means of semantic-web techniques, into a context-aware model able to analyze dependencies, relationships and to discover causes and predict effects, as well to involved on context-aware services, such as a complex informational security service, which provides information about the type of undesired events, together with the operations needed to counteract them and the order of these operations.

Key words: *Context-Aware Services, Web Services, Semantic WEB, Data Acquiring/Analyzing, OWL, RDF.*

Introduction

Under the current world-wide circumstances, critical infrastructures have become an important research object, especially after the 9/11 events. Countries and international organizations set the trends of development of this domain, elaborated the appropriate legal framework and established specialized agencies. In the international legislation, a definition of critical infrastructures is – "those elements (systems and services) or parts of them which are essential to maintain society functions (health, security, safety, economic and social welfare of population)". A subclass of these is represented by the critical information infrastructures (i.e. telecommunications, computers, software, networks, internet, satellites etc.). Their huge importance is given by the fact that other critical infrastructures such as water or electricity delivery systems, have grown to depend on them [1].

The domain of Critical Information Infrastructures Protection

The dangers to which C.I.I. are exposed to are of various natures: physical dangers, such as malfunction of hardware or services; security dangers, such as misappropriation of equipment or

services, confidentiality dangers – such as the theft of identity, terrorist danger – classic, cyber attacks or combined attacks.

Critical information infrastructures protection is necessary and important because of the impact that malfunction, deterioration or compromise can have upon them. The aim of C.I.I.P. is to remove vulnerabilities and minimize the risks to which C.I.I. are exposed.

Generally, these critical infrastructures have a distributed architecture and consist of several systems, sub-systems, specialized equipment, as well as transport/communications infrastructure. These elements are made up of functional blocks which rely to one another, depending on the role they have to fulfill.

Security measures are implemented at different levels and rely upon a range of devices, from simple services supported by existing equipments to complex specialized systems. Protection is achieved by means of pre-established security policies which specify the manner of authentication, physical or remote access and the way to react to evens.

The main problems that C.I.I. domain has to face today are caused by the fact that, at operator level, protection is limited by their own various networks and equipments, which most of the time use various applications and standards and also by the appearance of new vulnerabilities, caused by new, originally unpredicted, components. Besides, cyber attacks have become more and more complex, aiming not only at individual components, but also at the entire infrastructure.

By using techniques that belong to context-aware systems (architecture, model) and semantic web domain, there can be achieved an ubiquitous and distributed security environment, computer processable, wherein the entities (processing equipment, network devices, storage resources, etc.) are adapted to security necessities, according to the specified rules and constraints imposed by security policies and technical capabilities.

The appropriateness of a context-aware model

Throughout time, “context” was defined by its synonyms such as: “environment”,”situation”. For the first time, the term “context-aware” was used by Schilit & Theimer – 1994 [10], who meant by “context” the location, the identity of the objects and person nearby and the changes upon then. The nest definitions referred to the context by the enumeration of the elements it is made of: who you are; with whom you are; which are your resources [13].

In my view, context is seen as a situation with all its implications: people (identity, role, group), resources (devices, network equipment, services), location (coordinates, security level), the moment in time (working program, unusual situation), the activity, the role in the information infrastructure. When a certain situation is identified, a series of events is triggered, by means of which, in accordance to a set of rules, the system reacts in order to solve the problems and normalize the situation.

Context information is acquired from the existing services in various shapes, from diagnosis and quality data, to data concerning specifications, configurations, current state, data flows, the history of data and activities, access policies and security rules. The gathered data and information are processed and integrated in order to act upon the current state so that the information infrastructures, as a whole, to be able to attenuate risks, eliminate the causes that triggered, the lack of balance and to provide the services in the stated parameters.

The most recent studies in the field of context-awareness and related fields brought up a series of innovations concerning all the components of the general architecture: the development of intelligent sensors; the integration and grouping of these into web sensor-services [7], the endowment of these services with primary processing functions and observation data provision

functions. These services have the abilities of self-description, notification, multicast, streaming and piping and in order to be easily found, they sign up in services registers, which can be interrogated by client applications. Data communication and representation are achieved by means of application-independent languages and protocols, based on XML, which provide easy knowledge retrieval, as they are domain specific and standardized by various entities, such as W3C [14], OpenGIS [9], DMTF [2]. Since data are organized in the shape of knowledge base, the use of techniques belonging to the semantic-web domain (RDF, RDFS, OWL) makes possible operations such as: integration of data belonging to different fields, logical reasoning and inference of high-context information.

Context Modeling and Reasoning Support

Context modeling represents the specification of all the entities and of the relationships amongst them which are necessary to describe the context - i.e. information about people, time, location, computational entities devices, activity etc.

As far as context domain is concerned, reasoning means that from the given context information new facts (information) can be inferred. E.g., if the last magnetic card used to open the door of room X belongs to person P and the presence sensor notifies movement in room X then person P must be in room X.

Since critical information infrastructures are distributed and consist of heterogeneous equipments and systems, belonging to several fields (computer, network equipment, video surveillance systems, authentication systems, presence detection systems, access systems etc.), context modeling has to ensure composition and the collaboration among fields. The most suitable classes of context representation models in my opinion are those based on ontologies.

The term ontology comes from Philosophy and refers to a matter whose object of study is "Being" and "Existence" and their sub-categories: things, properties, processes, facts. In the field of computer science, the things that exist are those which can be represented by data.

Ontologies, in the specialized literature, are explicit formal descriptions of the concepts of a field. Ontology-based context modeling allows semantic description independent of the programming language, the operating system or middleware (services of communication among the application, the computer and the services).

The main advantage of ontologies is the possibility to share communications and knowledge by means a vocabulary common to different applications or agents; besides, they allow logical inferences, offer reasoning support and can be reusable, meaning that general ontologies can be included in domain-specific ontologies.

There are several ontology-defining languages, but I will use for my study the OWL Web Ontology Language, which is a specification of W3C (World Wide Web Consortium) [14] and constitutes a fundamental component of Semantic Web. OWL is relies on XML, XMLS, RDF and RDFS and is divided into 3 sub-languages: Owl-Lite, Owl-DL and OWL-Full [14], of which the most commonly used is Owl-DL (Description Logic). There are also available a series of development tools that support OWL, such as the Protege graphic editor [11], the Jena Application Programming Interface [5] and the FaCT and Racer inference motors.

The most acknowledged ontology-based OWL-relied models in the field of context-aware systems, able to model and represent the context, are SOUPA (Standard Ontology for Ubiquitous and Pervasive Applications) [3] and SOCAM (Service-Oriented Context-Aware Middleware) [12].

SOUPA consists of two sub-sets of ontologies: SOUPA Core – used to define a universal vocabulary for context-aware applications – and SOUPA Extension – derived from SOUPA

Core and used to define an additional vocabulary for particular types of applications. SOUPA Core contains ontologies referring to Persons, Policies and Actions, Agents and BDI, Time, Space (it adopts parts of OpenCyc and OpenGIS), Events, while SOUPA Extension experimentally contains ontologies that refer to Meeting and Schedule, Document and Digital Document, Image Capture (seen as an event), Region Connection Calculus (concerning space relationships) and Location (time/space co-ordinates); it can also include user-defined ontologies.

SOUPA ontological concepts and the relationships among them are presented in Figure 1. For example, an Image is a Digital Document, which is a sub-class of Document. The Document is created by a Person, at a certain moment in Time. As far as our domain is concerned, we can notice that there have already been implemented the entities – such as persons, space, time, events – needed in the modeling of the critical information infrastructures protection domain.

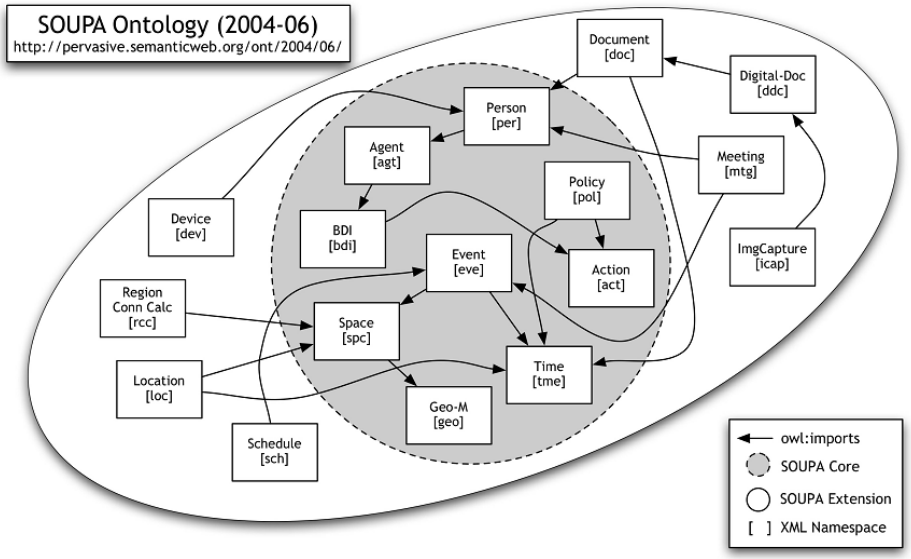

Fig. 1. Graphic representation of SOUPA ontology.

SOCAM model, presented in figure 2, consists of two sets of ontologies: one for the general vocabulary and the other for the vocabulary specific to various applications domains. We can observe that the general vocabulary provides approximately the same description as SOUPA Core, referring to entities such as Person, Space and Activity (in the sense of Event). The specific vocabulary facilitates the connection to the application domain; in our case, there will be necessary to define domain-specific ontologies, such as High Security Area, Data Center Area, Outer Access Area (by means of mobile terminals or remote access etc.).

In conclusion, both these ontology-based models provide the needed description of the meaningful concepts in the field of Critical informatics infrastructures protection – persons, locations, intentions, activities – and ensure the integration of the knowledge acquired from external sources.

For the C.I.I.P. field, the context-aware model will offer support, by conferring access to the knowledge base, not only to management, security and diagnosis services, but also to the end-user, in the sense that it creates an intelligent work space through automatic configuration, resources provision and context-sensitive authentication [6].

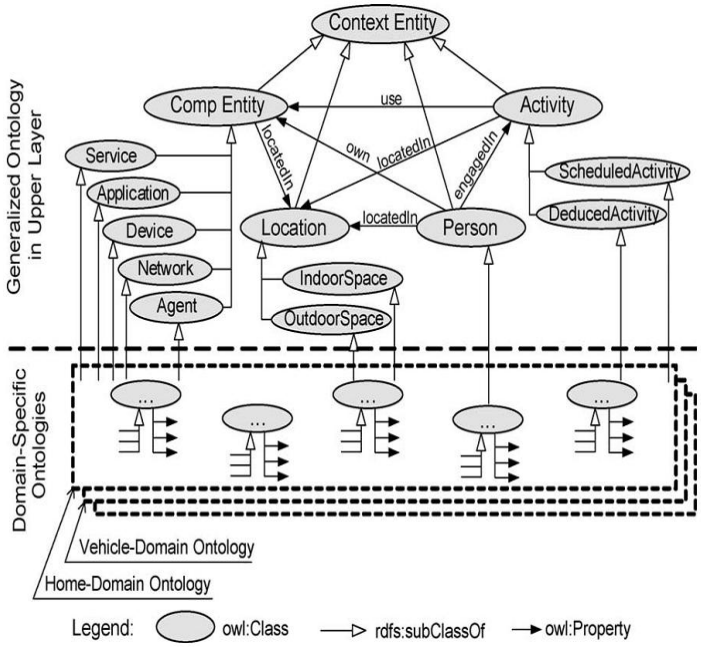

Fig. 2. General model – SOCAM – class hierarchy.

System Architecture

Many of the components of present-day computer systems are endowed with special technical capabilities, which address not only the level of sensitivity, but also the levels of management and security. The great producers of equipment and software solutions such as IBM, Cisco, Nortel, Microsoft, as well as the Open Source Community have been involved in the research of standard XML-based models, languages and protocols, which nowadays are being implemented in the shape of web services (as defined in [7] – "Web services are software applications that can be discovered, described and accessed by using XML and standard WEB protocols within intranet, extranet and internet networks"). Currently, different types of web services [4, 8] are available – Sensor-type, Management-type [2], Security-type – which enhance abstraction but are applicable to particular domains. For example, the Sensor service for hardware equipments provides data concerning disk capacity, memory capacity and bandwidth and, more recently, offers support for the peripheral equipment sensors. The knowledge base that utilizes key elements and semantic web techniques can solve the information management inherent dilemmas encountered by every organization that administrates critical systems and infrastructures. This goal is achieved by integrating the information provided by the web services, abstracting the details into a knowledge base according to a model, providing ontologies able to achieve pattern recognition within a wide range of data and by using retrieval mechanisms for the registry-type information sources.

The general architecture of a context-aware system is made of components for acquiring, interpreting, aggregating, storing and adapting the context data and, optionally, a component that manages the others.

Among the architectures currently known in the field of context-aware systems which implement ontology-based models, I can mention the following:

- SOCAM (Service-Oriented Context-Aware Middleware), which has a 3-layer organization: context sensing, context middleware and context application layer. Its disadvantage is that it requires a centralized interpreter.

- CoBrA (Context Broker Architecture), which is an agent-based architecture, whose main characteristic is the presence of a central agent – Context Broker – that fulfills the roles of Context Database, Context Inference Motor, Context Acquisition and Confidentiality Management.
- Context Toolkit, whose specificity is represented by the widget components used both for the acquisition and for the context service. It is a peer-to-peer architecture and requires a centralized discovery service.

Therefore, I will study a decentralized and distributed multilayer architecture, based on specialized services which accomplish certain tasks and collaborate in order to support the context-aware applications that will ensure the management and security of the critical information infrastructure in an autonomous manner, as well as an ubiquitous work environment for the end users, by the integration of the context services in day-to-day applications.

By multilayer I mean that, from the logical perspective, the architecture will be layer-organized.

From the functional perspective, the architecture will be decentralized, meaning that it can be organized in the shape of groups (domains), possibly redundant.

The architecture will also be distributed, as far as location is concerned, meaning that the components of the system can be spread across departments, buildings, set in different places, in order to ensure minimal damage in case of disaster.

For example, in [6] it is presented a secure distributed proof system for context-sensitive authorization. The system enables multiple hosts to evaluate an authorization query in a peer-to-peer way, while preserving the confidentiality and integrity policies of mutually un-trusted principals running those hosts.

Conclusions

Critical information infrastructures protection is a dynamic and actual field, especially under the current circumstances, in which cyber attacks have reached world-wide proportions, leading, besides the losses caused by systems degradation and malfunction, to continuously increasing costs for the administration, protection and repair.

The field of context-aware systems is facing a continuous development and the results of the specific research are being implemented in successful commercial solutions, in the shape of user-oriented intelligent platforms.

I intend to focus on the study of mechanisms that can provide control-loop for ontology-based context-aware systems, so as to ensure autonomous behavior. For the critical infrastructures, those will allow the implementation of a series of context-aware services that will be able to collaborate in order to ensure configuring capabilities, protection, optimization and automatic repair of the critical infrastructures.

References

1. *** – *Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience*. http://eur-lex.europa.eu/LexUriServ/.
2. Distributed Management Task Force – *Web Services for Management (WS-Management)*. www.dmtf.org, 2006.
3. Chen, H., Perich, F., Finin, T., Joshi, A. – *SOUPA: Standard Ontology for Ubiquitous and Pervasive Applications*. http://ebiquity.umbc.edu/get/a/publication/105.pdf.
4. IBM – *Standards and Web Services*. http://www.ibm.com/developerworks/webservices/standards

5. Jena – *A Semantic Web Framework for Java*. – http://jena.sourceforge.net.
6. Minami, K. – *Secure Context-Sensitive Authorization*. Dartmouth Technical Report TR2006-571.
7. Daconta, M. C., Obrst, L. J., Kevin T. Smith – *The Semantic Web: A Guide to the Future of XML, Web Services, and Knowledge Management*. Wiley, 2005.
8. Microsoft – *Microsoft's Web Services Standards*. http://msdn.microsoft.com/en-us/library/ms951274.aspx
9. Open Geospatial Consortium – *Sensor Web Enablement*. http://www.opengeospatial.org/ projects/groups/sensorweb
10. Schilit, B. N., Theimer, M. M. – *Disseminating active map information to mobile hosts*. IEEE Network 8(5): pp. 22-32. September/October 1994: ftp://ftp.parc.xerox.com/pub/ schilit/AMS.ps.Z, 1994
11. *** – *Protégé*. http://protege.stanford.edu.
12. Gua, T., Punga, H. K., Zhangb, D. Q. – *A service-oriented middleware for building context-aware services*. Journal of Network and Computer Applications 28, 1–18, 2005.
13. Kindberg, T., Barton, J. – *A Web-Based Nomadic Computing System*. HP Laboratories Palo Alto, August 24th, 2000.
14. www.w3c.org.

Protecția infrastructurilor informatice critice utilizând integrarea serviciilor senzitive la context

Rezumat

În contextul dependenţei crescute de tehnologie a societăţii contemporane, infrastructurile informatice critice şi menţinerea acestora în parametri optimi căpătă o importanţă din ce în ce mai mare. În continuă expansiune şi interconectare, aceste infrastructuri au depăşit graniţele naţionale tinzând spre o răspândire globală, riscurile de securitate fiind preocuparea principală a entităţilor care le administrează şi le exploatează, de la organizaţii internaţionale, regionale, naţionale, operatori privaţi, până la utilizatorii finali. Din cauza diversităţii serviciilor şi a formatelor de date, precum şi distribuţiei geografice, asigurarea interoperabilităţii şi integrării datelor, unele cu caracter de timp real şi cu caracter de urgenţă, este o sarcină dificilă şi costisitoare, dar absolut necesară. O posibilă soluţie la această problemă complexă este integrarea semantică a datelor şi serviciilor, folosind tehnici din Semantic WEB, într-un model senzitiv la context care are capacitatea de a analiza dependenţele, descoperi cauzele şi prevedea efectele, precum şi de a furniza celor responsabili servicii senzitive la context, ca de exemplu, un serviciu informaţional complex de securitate, care furnizează, pe lângă informaţii despre tipul evenimentelor nedorite, şi operaţiile necesare pentru contracarare, precum şi ordinea acestora.

This page intentionally left blank