Modelling Security Relevant Context An approach towards Adaptive Security in Volatile Mobile Web Environments

Kristian Fischer
Cologne University of Applied Sciences
Steinmüllerallee 1,
51643 Gummersbach, Germany
++49 2261 8196 6297
kristian.fischer@fh-koeln.de

Stefan Karsch
Cologne University of Applied Sciences
Steinmüllerallee 1,
51643 Gummersbach, Germany
++49 2261 8196 6472
stefan.karsch@fh-koeln.de

ABSTRACT

Coming along with the spread of location-independent wireless networks and attractive mobile devices like “smartphones” or “pads”, activities in the Web increasingly take place in volatile mobile environments, even if sensitive information objects are involved. In this paper a approach is proposed to apply security measures to such objects in a context sensitive, flexible way. It is based on semantic models of the user’s context and his or her security concepts.

Categories and Subject Descriptors

K.4.4 [**Computers and Society**]: Electronic Commerce –*Security,* I.2.4 [**Artificial Intelligence**]: Knowledge Representation Formalisms and Methods.

General Terms

Human Factors, Security

Keywords

security, context, modelling, mobility, web interaction

1. INTRODUCTION

As a result of the growing interconnection of humans, services and information, the web seizes human activities. Private mobile web usage is already accepted and operational in many application areas like social networking. Currently an emerging demand for web utilization with serious business applications in mobile scenarios is looming. Latest technical developments enable the reliability and usability of mobile web based interaction. Examples for these developments are broadband location-independent wireless networks and more universally usable mobile systems. Major characteristics of these systems are the stronger computing power of “Pads” and improved usability by bigger displays compared to classic PDAs or smartphones. Additionally these systems are equipped with operation environments that meet the requirements of classic operating systems more closely. These developments lead to more data being processed, stored and transported in mobile IT-scenarios, but more importantly, also the quality of data changes. The authors are convinced that the qualitative way of mobile web usage soon will be similar to stationary web usage.

2. SECURITY AND MOBILITY

Whereas in private mobile web scenarios typically privacy can become a concern, in business scenarios major financial or image damage can occur as an overall result of security breaches. For the latter scenarios in terms of IT-security the protection of security relevant objects has to meet much higher requirements in the future.

In comparison to non-mobile scenarios, protection becomes a more complex task. In classic IT-security, IT-Scenarios are analyzed with regard to the objects worth protecting, their protection goals (e.g. confidentiality or integrity) and the scenario-specific physical, organizational and technical threats possibly directed against them. Protective measures try to reduce the probability of damage and/or the amount of a possible damage.

Threats in mobile IT-scenarios constantly change with the volatile circumstances in which systems and data are utilized. There are two ways to meet these varying requirements: Protection measures can be chosen adequate for the highest threat level an object may be exposed to in all possible scenarios (we call this the maximum approach for protection in mobile scenarios). The other way is to flexibly adopt protection measures to the changing threats objects are exposed to (we call it adaptive security for mobile scenarios).

The maximum approach implicates some major disadvantages. Often security measures reduce functionality as well as usability of IT-Systems and applications. Excessive deployment of security measures often reduces user acceptance of systems and applications. Subsequently even eligible users often circumvent security measures. As a result adaptive security for mobile scenarios is superior with respect to usability and functionality as well as to security itself.

3. CONTEXT AND SECURITY

The circumstances under which systems and applications are utilized can be described in a more general way as context [3]. In our approach the notion of context provides a means to denote all information that influences the interaction of the user with the system in a volatile mobile web environment including the information that allows to assess potential threats and to select adequate security measures.

WebSci ’11, June 14-17, 2011, Koblenz, Germany.

Adoption of protection measures to changing context is evident. Recently several approaches to model security relevant information based on the notion of context have been proposed ([1], [7] and [8]). In the area of security management the so called PDCA-circle [6] is used as a general method to adopt security concepts to a changing technical, physical or organizational context. However this approach is intended for adoption to slow changes in large enterprises. Adoption of systems and applications to volatile security threats requires automatic or at least semi-automatic selection and enforcement of security measures. In result this requires an analysis of possible usage context with regard to possible threats and a pre-selection of possible measures to be implemented based on context information.

We are aiming at a systematic approach of modeling security relevant context based on concepts adopted from the „Semantic Web“. Representation of context in a semantic model has already been proposed by Xu [16] for the purpose of alert analysis. We propose a more general model, where current context information from sensors of mobile devices is combined with context information retrieved from the Web. The knowledge required to assess this information shall be represented in ontologies containing personal information, company specific information, and general information.

4. CONTEXT MODELS AND THE WEB

During mobile usage context information can be obtained from different sources: Todays Smartphones provide a wealth of sensor data, the activities of the user during application usage can be sensed, captured and represented in data formats like the Contextualized Attention Metadata (CAM) [17], and location dependant information like weather forecasts or threats resulting from future events might be obtained from Web sources.

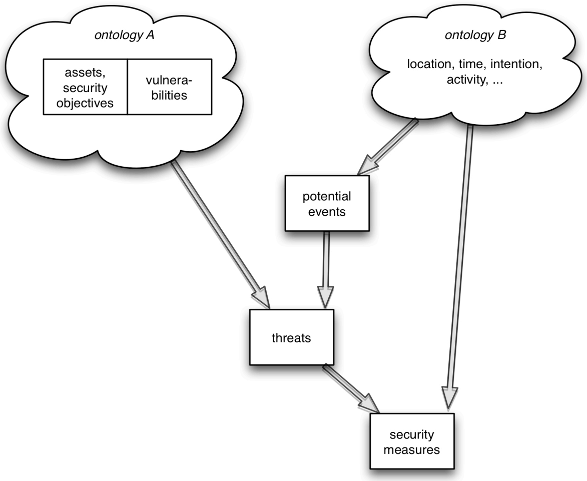

Figure 1. Deriving security measures from context information

In order to derive adequate protection measures from such information the raw context information must be interpreted based on knowledge about the user regarding locations (e.g. at home, in the company, with the customer), his intentions (e.g. travelling, in a meeting, busy with personal affairs) and his security assets and objectives (e.g. confidentiality of messages).

Figure 1 describes the process of dynamically deriving security measures in mobile environments. Our approach is, to represent this knowledge about the user in ontologies and employ the concepts of the Semantic Web in order to cope with its dynamic and distributed nature. The domains that need to be modelled in ontologies are mainly:

- A context ontology comprising concepts for location, intention, time, activity
- A security ontology comprising concepts for assets, objectives, concepts, threats, metrics and measures

The ontologies involved in the evaluation of the security relevant context will be contributed from different sources:

- Some ontologies will be person specific; e.g. the concept of “being at home”, or “being with friends” will to a certain extent be individual for each person.
- Some ontologies will depend on the company the person is working for; e.g. the concepts for “being in office “, “meeting with colleagues”, or “visiting a customer” will be specific for the respective company.
- Other ontologies may come from external organizations, e.g. the police for security relevant information in public spaces, the public transportation for information regarding their locations.

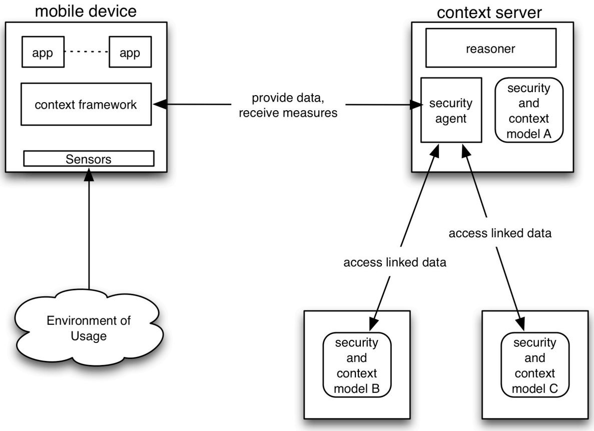

Figure 2. Framework for security relevant context

Figure 2 shows a potential architecture for a framework for security relevant context for volatile web environments. The mobile device runs a framework layer serving all applications (“Apps”), which are designed to use security services. The applications provide data about the user’s activities to the framework and receive potential security measures from the framework.

The framework collects the raw data coming from the sensors through the respective operating systems interfaces and the user activity metadata from the applications. It provides this data to a remote context server, which determines potential measures based on the security and context model. The server provides information on security measures to the context framework of the mobile device when required. The framework then “asks” the applications to execute the measures as far as application specific data objects or the user interaction are concerned, or it executes the measures based on operating system services, when general objects like files are to be protected.

The context server comprises a security agent that integrates models and assertions concerning security and context from different sources. The company, the user works for, may for example administer local data, in figure 2 denoted as "security and context model A". Such data could comprise knowledge about organization- and task- specific threats; it may also integrate the person-specific knowledge.

Remote data, in figure 2 denoted as "security and context model B" and "security and context model C" provides security relevant knowledge from external organizations like business partners or public services. The access is architected according to concepts of Linked Data [18].

A first prototype for the context framework has been developed at the author's institution for Apple's iOS ([19]) and for Google's Android] ([20]).

5. CONCLUSION

We propose a architecture to dynamically derive security measures from context information in volatile mobile web environments. The deduction of the measures is based on knowledge modeled in ontologies and on context information provided by a central context server via a context framework running on the mobile device. A proof of concept implementation for the context server and the framework is already available. The adoption to changing security context and the corresponding design of adequate security ontologies is subject to current research in the author's institution.

6. REFERENCES

[1] An, Bae, Kim, Seo: "Context-aware Dynamic Security Configuration for Mobile Communication Device", *Proceedings of the 3rd international conference on New technologies, mobility and security*, 2009

[2] Bandinelli, Paganelli, Vannuccini, Giuli: "A Context-Aware Security Framework for Next Generation Mobile Networks", Security and Privacy in Mobile Information and Communication Systems, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Volume 17. Springer Berlin Heidelberg 2009, S.134 – 147

[3] Dey, Abowd: "Towards a Better Understanding of Context and Context-Awareness", *Proceedings of the 1st international symposium on Handheld and Ubiquitous Computing*, 1999

[4] Donner: "Toward a Security Ontology", *IEEE Security and Privacy*, Volume 1 Issue 3, 2003, S. 6-7

[5] Ekelhart, Fenz, Klemen, Weippl: "Security Ontologies: Improving Quantitative Risk Analysis", *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007

[6] ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management systems - Requirements*, 2005

[7] Johnson, Agrawala, Billioniere: "A Framework for Shrink-Wrapping Security Services", *Proceedings of the 2010 IEEE International Conference on Services Computing*, 2010, S. 639-640

[8] Johnson: "Towards Shrink-Wrapped Security: A Taxonomy of Security-Relevant Context", *IEEE International Conference on Pervasive Computing and Communications*, 2009

[9] Kagal, Paolucci, Srinivasan, Denker, Finin, Sycara: "Authorization and Privacy for Semantic Web Services", *AAAI Spring Symposium, Workshop on Semantic Web Services*, Stanford, California, 2004, S. 52-58

[10] Kim, Luo, Kang: "Security Ontology for Annotating Ressources" On the Move to Meaningful Internet Systems 2005: CoopIS, DOA, and ODBASE, *Lecture Notes in Computer Science*, Springer Berlin Heidelberg 2005, S. 1483-1499

[11] Lacoste, Privat, Ramparany, "Evaluating Confidence in Context for Context-Aware Security", *Proceedings of the 2007 European conference on Ambient intelligence* Springer-Verlag Berlin, Heidelberg 2007, S. 211-229

[12]]Mostéfaoui, Brézillon: "A Generic Framework for Context-Based Distributed Authorizations", *Proceedings of the 4th International and Interdisciplinary Conference on Modeling and Using Context*, Springer Verlag, Stanford, California, 2003, S. 204-217

[13]]Mostéfaoui, Brézillon: "Modeling Context-Based Security Policies with Contextual Graphs", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, 2004

[14] Simmonds, Sandilands, van Ekert: "An Ontology for Network Security Attacks", *Proceedings of the 2nd Asian Applied Computing Conference*, 2004

[15] Sinha, Bailey, Jahanian: "One Size Does Not Fit All: 10 Years of Applying Context-Aware Security", IEEE *Conference on Technologies for Homeland Security*, 2009, S. 14-21

[16] Xu, Xiao, Wu: "Application of Security Ontology to Context-Aware Alert Analysis", *Eigth IEEE/ACIS International Conference on Computer and Information Science*, 2009, S. 171-176 Abc

[17] Ochoa, Duval. 2006. "Use of contextualized attention metadata for ranking and recommending learning objects" *Proceedings of the 1st international workshop on Contextualized attention metadata: collecting, managing and exploiting of rich usage information (CAMA '06)*. ACM, New York, NY, USA, 9-16.

[18] Parundekar, Knoblock, Ambite. 2010, "Linking and building ontologies of linked data", *Proceedings of the 9th international semantic web conference on the semantic web - Volume Part I (ISWC'10)*, Peter F. Patel-Schneider, Pan, Hitzler, Mika, Zhang (Eds.), Vol. Part I. Springer-Verlag, Berlin, Heidelberg, 598-614

[19] Müller, „Modellierung und Repräsentation des Kontextes von mobilen Nutzungsszenarien - ein Rahmenwerk für mobile kontextsensitive Applikationen", *Master Thesis Fachhochschule Köln*, 2010, http://d-nb.info/1001076869

[20] Krumnow," Mehrprozessbetrieb für mobile kontextsensitive Anwendungen - Konzeption und prototypische Implementierung auf Basis eines bestehenden Rahmenwerks", *Bachelor Thesis Fachhochschule Köln*, 2011, http://d-nb.info/1007874481