Towards Visual Configuration Support for Interdependent Security Goals

Fatih Karatas, Mohamed Bourimi, and Dogan Kesdogan

Chair for IT Security, Privacy and Trust,
University of Siegen,
57076 Siegen, Germany
{karatas,bourimi}@wiwi.uni-siegen.de, kesdogan@uni-siegen.de

Abstract. This work investigates visual support for easing the configuration of interdependent security goals. The interdependent nature of security goals did not receive sufficient attention in related work yet. A formal approach to adequately model interdependent security goals are *multi-criteria optimization problems* which can be solved either exactly or heuristically. This however depends on the question if the user is able to articulate his/her preferences regarding security goals. Furthermore, heuristic approaches confront users with possibly unlimited alternative configurations where each solution is equally well. In order to support users in the process of articulating preferences and selecting a suiting alternative, we provide visual facilities at the level of the user interface. The need for handling such issues emerged from the analysis of the EU funded di.me project which explicitly requires that such configurations are carried out by lay users. We present an approach tackling these issues by means of visual concepts triggering a service selection in the background which respects the interdependence of security goals. We concretely discuss the application of our approach by addressing a scenario concerned with deployment decisions in the di.me project.

Keywords: Interdependent Security, Decision-support, Preference Articulation, Trade-off Visualization, Security and Usability, User Experience.

1 Introduction

The majority of applications, processing data of users offer security settings for ensuring different levels of protection depending on the user's needs. This is mostly supported for instance by respective wizards in the user interface (UI). Security preferences are seen as quality attributes and the usability of provided wizards strongly affects the user experience (UX). Indeed, usability is a prerequisite for security [1][1] and UX is related to *every aspect of the user's*

[1] The inherent interplay between usability and security with respect to easing security configuration in general was realized as early as 1883 by *Kerckhoffs* who formulated it as his sixth principle for building secure systems [2]. An english translation of the original french article can be found at http://www.petitcolas.net/fabien/kerckhoffs/index.html#english .

A.A. Ozok and P. Zaphiris (Eds.): OCSC/HCII 2013, LNCS 8029, pp. 375–384, 2013.

interaction with a product, service, or company that make up the user's perceptions of the whole[2] [SIC].

Supporting visual configuration of interdependent security goals did not receive sufficient attention in related work yet. Since these kind of security objectives can either strengthen, weaken or implicate each other, respective visual configuration facilities should reflect emerging trade-offs resulting from this interdependence i.e. at the level of the respective application's UI. To our best knowledge, the only application tackling this issue is described in [3] for SSONet system. The solution does however not address any kind of user feedback at the level of the UI. The foundation of our approach is a model to describe interdependent security goals, formulated as *multi-criteria optimization problem*. Problems of this class are characterized by the circumstance, that they can usually only be solved heuristically. Exact solutions can only be obtained (if at all) if users articulate their preferences with respect to the objectives. Otherwise the result is a possible unlimited set of solutions where each solution represents an equally well compromise with respect to the objectives. In order to support users in the process of articulating preferences and selecting a suiting alternative, we provide visual facilities at the level of the UI. To our best knowledge, this kind of facilities were not proposed in the field of interdependent security configuration yet.

The rest of the paper is structured as follows. Section 2 introduces the EU funded di.me project which forms a test bed for the approach presented here. Consequently the requirements analysis in section 3 is based on this project. Section 4 presents our approach for tackling the issues discussed above as well as the implementation in di.me and Section 5 concludes the paper. It should be noted that along the whole paper, we concretely discuss the application of our approach by having in mind a scenario concerned with deployment decisions in the di.me project.

2 Target Community and Use Case

The EU funded project di.me[3] specifies a platform incorporating user-control deeply in design: a private service (PS) and userware offer a central user node in a decentralized network connecting to other user nodes or external services, like social networking platforms, through distinct identities [4,5] (cf. Figure 1). This node integrates all personal data in a personal information sphere, including user interests, contact information, and social network services. Intelligent features further guide user interactions within the digital sphere, illustrated by context-aware access control, trust and privacy advice, or organizing their personal information sphere [6,7].

[2] According to Usability Professionals Association's (UPA) Glossary: `http://www.usabilitybok.org/glossary`

[3] `http://www.wiwi.uni-siegen.de/itsec/projekte/dime/index.html.en`

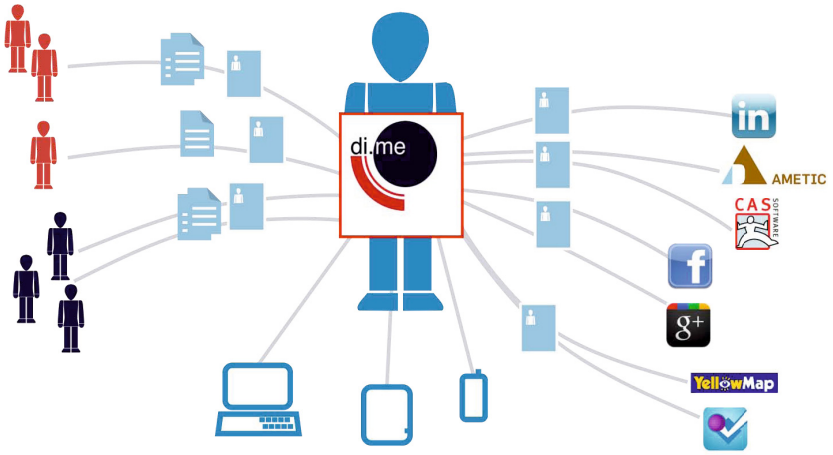


Fig. 1. The big picture of di.me

One of the main objectives of the di.me userware is to be under full control of end users, which implicates enabling them to be able to host the userware on any trusted node they state as secure enough for their usage purposes (e.g. on a desktop PC at home which is accessible via the Internet). With this, the deployment of the PS onto cloud infrastructures was required as cloud computing (CC) as a facility for the deployment of user-controlled servers is a growing trend[4]. Furthermore, various industrial[5] partners explicitly required supporting this feature along with enabling di.me to support multi-user/multi-tenant hosting[6]. In the case of di.mes' industrial partners, the end-user carrying out the deployment task is the administrator at the respective company. Because of this, di.me has to support lay as well as experienced users in performing the CC deployment by considering ease of configuration (incl. consideration of interdependent security goals). For meeting our gathered requirements, we proposed in [8] a solution, which is formed by an "Environment for secure cloud applications by adaptable virtualization and best practice consideration" or ESCAVISION for short. ESCAVISION is the core of our approach and supports lay as well as experienced users in considering security best practices. The requirements gathering, elicitation and negotiation process followed the AFFINE methodology involving all stakeholders (i.e. end-users, experts, developers) and enforcing the earlier

[4] One main cause is the high availability and various cost-reducing factors in comparison to own hosted PSs.

[5] i.e. industrial partner interested in di.me exploitation later.

[6] One of the main objectives of di.me is to evaluate developed concepts with a large set of users. This technical/infrastructural challenge led to the discussion if the userware should not be extended to multi-user/multi-tenant support for trusted communities, e.g. a family or friends servers.

consideration of functional as well as non-functional requirements (i.e. usability and security) in an agile way [9,10]. In the following, we analyze the requirements and present our approach with the deployment support scenario in mind.

3 Preliminaries and Requirements Analysis

As mentioned before, security objectives are interdependent and can either strengthen, weaken or implicate each other [3] (see Figure 2). As an example consider anonymity and accountability. A high level of anonymity makes it hard to account single events to certain users while a high degree of accountability makes it hard for users to upkeep their anonymity. Thus anonymity and accountability are mutually weakening each other. Because of the interdependent nature of security objectives, the problem of determining the security level of applications such as service compositions can be formulated as multi-criteria optimization problem [11,12]. The basic idea is to assess the influence of technical as well as organizational factors such as encryption algorithms and admission control policies on security objectives. These objectives can thus be formulated as interdependent objective functions (for further details, the interested reader is referred to [11]).

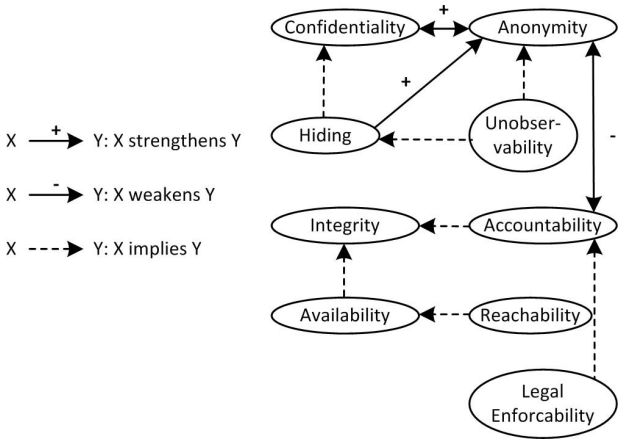


Fig. 2. Correlation of protection goals (from [3])

A challenge remains solving multi-criteria optimization problems. Usually such problems have a set of optimal solutions where each solution represents a compromise with regards to the objective functions. Depending on the question if the decision maker is allowed to articulate her preferences before (*a priori*), during (*interactive*) or after (*a posteriori*) performing the search algorithm, it is possible to employ either exact algorithms or heuristic approaches [13].

In this paper we focus on *a priori* and *a posteriori* approaches as one of the design goals of our prototype (see next section as well as [11]) was to determine near-optimal solutions with minimal user-interaction.

Articulation of preferences *a priori* or *a posteriori* has however also effects on the exploration of the search space. While approaches with *a priori* articulation of preferences allow for finding exact solutions, they restrict the search space. On the contrary, approaches with *a posteriori* articulation of preferences are heuristic but allow for exploring the search space without limitation.

Another issue is the selection of the solution which best fits the decision-makers needs. As stated above, each solution of a multi-criteria optimization problem represents a compromise with regards to the single objective functions. Therefore it is not possible to automatically decide which solution is "the best". Instead, decision-makers need to decide, based upon the trade-offs of each solution which one fits their needs best. This can however become hard in the face of numerous objective functions.

Supporting decision-makers in the process of (a) preference articulation and (b) selecting the solution which best fits their needs thus yields the following requirements:

1. Decision-makers need facilities to articulate preferences *a priori* as well as *a posteriori* (**R1**).
2. Consequences of preference articulation by means of received solutions (exact vs. heuristic) and search space exploration need to be communicated to decision-makers (**R2**).
3. Decision-makers need support to better evaluate the trade-offs of single solutions (**R3**).

4 Approach

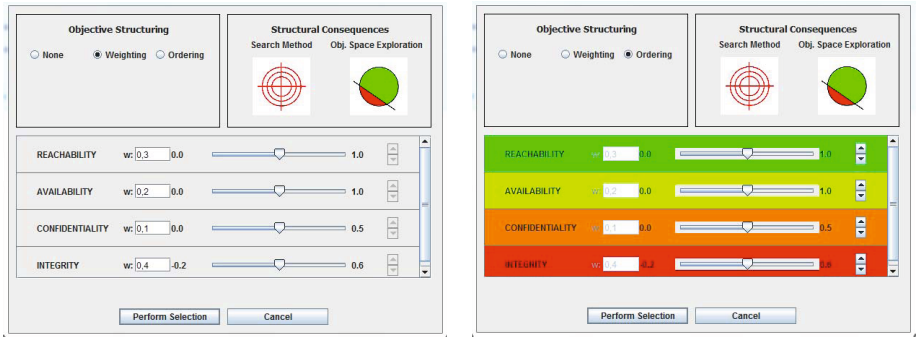
In this section we will present our concepts for tackling the requirements identified above. The concepts are illustrated with a prototypical implementation within the Service Selection Workbench (SSW). The SSW is a tool for determining secure service compositions for given workflows. It was first introduced in [11] which provides more information about the tool. In this paper we will focus on the selection facilities and how decision-makers are supported visually for the di.me deployment scenario introduced in section 2. For di.me we apply workflows with one task to find a suiting deployment option offering security facilities that match user requirements. While from a service composition point of view, di.me is less interesting, the issues described in section 3 still apply. The typical sequence of tasks in service selection is as follows:

1. The user formulates requirements for each protection goal.
2. If desired, the user can express preferences regarding protection goals.
3. A service selection is performed by solving a multi-criteria optimization problem with the user requirements being the constraints. If the user articulated

preferences in step 2, the problem can be solved exactly. Otherwise a predefined number of heuristic solutions (e.g. 10) is determined.
4. The user selects from the determined solutions the one which best fits her preferences.

4.1 Preference Articulation (R1)

We concentrated on two methods for *a priori* preference articulation, namely weighting of objective functions and lexicographic ordering of objectives (see Figure 3). The decision-maker must specify, which kind of *a priori* preference articulation she prefers (if any). Weighting of objective functions is straightforward. Decision-makers can enter a real value $w \in [0, 1]$ for each objective function where the sum of all weightings must be ≤ 1. For ordering functions, decision-makers are provided with buttons next to each objective function. The rule is that the highest function is optimized first. The result set of the first function represents the input for the second and so on. In order to give decision-makers a visual feedback of the relevance of each objective function in the order, objectives are automatically colored according to their rank from green to red.



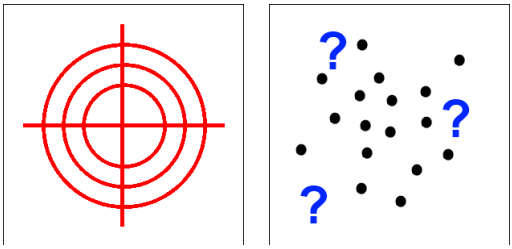
(a) Objective Weighting (b) Lexicographic Ordering

Fig. 3. Different methods for preference articulation

4.2 Communication of Structural Consequences (R2)

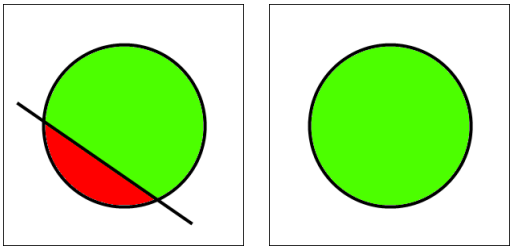
As already mentioned, preference articulation *a priori* leads to exact solutions at the cost of search space restrictions. On the other hand, heuristic approaches allow for searching the search space more thoroughly. In order to visualize these structural consequences to decision-makers, we implemented a view showing icons depending on the problem structure (see the upper right corner in both screenshots in Figure 3).

Currently we take effects on search method (see Figure 4) and search space exploration (see Figure 5) into account as these apply on each optimization problem. Other effects such as primal degeneracy which only apply to certain classes of optimization problems [14], were not included (yet).



(a) Exact (b) Heuristic

Fig. 4. Icons for visualizing search method properties



(a) Restricted (b) Unrestricted

Fig. 5. Icons for visualizing search space exploration

4.3 Trade-Off Visualization (R3)

In order to communicate the trade-offs regarding different protection goals, we employ metaphors for visualization. A sample metaphor which we prototypically implemented is a house on a hill with a sun shining above the scenery. Depicted in Figure 6 is the metaphor representing user-requirements for single protection goals. Depending on the security model employed, the single elements of the metaphor need to be mapped to a protection goal. For the widely used CIA model of security (*Confidentiality*, *Integrity* and *Availability*), a possible mapping is shown in Table 1. As mentioned in section 1, the result of service selection is a set of function values for each alternative. These function values are used to construct a visualization for each composition alternative on the basis of $\delta_k = pf_k - r_k$ where pf_k is the function value of protection goal k for the current alternative and r_k the user requirement for protection goal k. If $\delta_k \neq 0$, the corresponding metaphor element is being altered to reflect this difference. E.g., if integrity is less than required ($\delta_k < 0$), the smile of the sun turns over to a sad face. If it's higher ($\delta_k > 0$), the smile gets even brighter. Figure 7 shows two examples for service composition alternatives with different than required security properties. Alternative 1 offers better confidentiality than required, but less integrity and availability. Alternative 2 offers better integrity and availability than required but less confidentiality.

Table 1. Sample mapping of protection goals to metaphor elements

Protection Goal	Metaphor Element
Confidentiality	*Jalousies in the windows*
Integrity	*Smile of the Sun*
Availability	*Hill steepness*

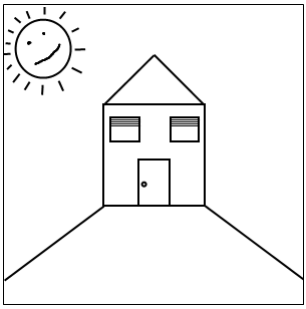
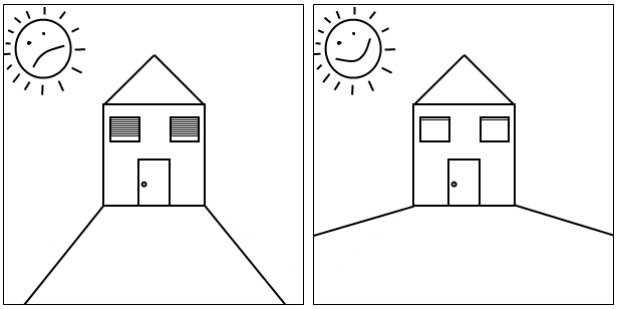


Fig. 6. Metaphor representing user-requirements for protection goals



(a) Alternative 1 (b) Alternative 2

Fig. 7. Alternative service compositions with different security properties

4.4 Deployment Scenario from di.me

The deployment scenario is concerned with creating a di.me PS at the instance of a few mouse-clicks and deploying it on almost any cloud infrastructure. After logging in at the website of di.me, the user can configure her di.me PS by selecting required features from a list. Next, a personalized ISO is created which then can be deployed on cloud infrastructure[7]. Integrating our proposed approach with the current state of the deployment scenario would require the steps in section 4

[7] A demo video for an adapted CRM usage of this scenario is available at: `http://www.uni-siegen.de/fb5/itsec/projekte/dime/dime-cloud-deployment-setup.avi`

to be executed after the ISO creation step. For each selection option, identified by the selection algorithm, a metaphor would be generated in order to visualize the trade-offs of that particular solution. Finally, the solution with the metaphor which attracts the user most, would be selected and deployment of the di.me, PS would be performed.

5 Conclusion and Future Work

In this paper, we investigated visual support for easing the configuration of interdependent security goals. The need for handling such issues emerged from the analysis of the EU funded di.me project with requirements for carrying out such configurations by lay users for supporting a scenario concerned with deployment decisions. Our analysis yielded the following three requirements: (i) Articulation of preferences *a priori* and *a posteriori*, (ii) communication of consequences of preference articulation on obtained solutions in terms of search method properties (exact vs. heuristic) as well as search space exploration (partial vs. unlimited) and (iii) visualization of trade-offs of single solutions with metaphors. For each requirement we presented an approach to tackle the respective issue, namely: (i) *a priori* preference articulation by weighting or lexicographically ordering security objectives, (ii) communicating structural consequences by showing icons in a view and (iii) by presenting the user metaphors (e.g. a scenery with a house on a hill) to visualize trade-offs of single solutions. To our best knowledge, there is no work proposing similar facilities in the field of interdependent security configuration. Future work will focus on continuing the implementation of the proposed approach by following AFFINE and evaluating it with end-users as well as experts. Another direction of future work will be implementing facilities for articulating preferences *a posteriori*.

Acknowledgments. This work has been partially supported by the German Federal Ministry of Education and Science (BMBF) under grant no. 13N10964 in the project ReSCUe IT which is jointly conducted together with the French Agence Nationale de la Recherche (ANR). Parts of this work are also supported by the digital.me EU FP7 project, funded by the EC(FP7/2007-2013) under grant agreement no. 257787. Thanks are mainly due to Sophie Wrobel and Marcel Heupel for their contributions to this work.

References

1. Cranor, L.F., Garfunkel, S.: Security and Usability: Designing Secure Systems That People Can Use. O'Reiley (2005)
2. Kerckhoffs, A.: La cryptographie militaire. Journal des Sciences Militaires IX, 5–38 (1883)
3. Wolf, G., Pfitzmann, A.: Properties of protection goals and their integration into a user interface. Computer Networks 32, 685–699 (2000)

4. Scerri, S., Gimenez, R., Herman, F., Bourimi, M., Thiel, S.: digital.me towards an integrated Personal Information Sphere, (June 2011), http://d-cent.org/fsw2011/wp-content/uploads/fsw2011-digital.me-towards-an-integrated-Personal-Information-Sphere.pdf
5. Thiel, S., et al.: A requirements-driven approach towards decentralized social networks. In: Park, J.J., Leung, V.C.M., Wang, C.-L., Shon, T. (eds.) Future Information Technology, Application, and Service. LNEE, vol. 164, pp. 709–718. Springer, Heidelberg (2012)
6. Heupel, M., Fischer, L., Kesdogan, D., Bourimi, M., Scerri, S., Hermann, F., Gimenez, R.: Context-aware, trust-based access control for the di.me userware. In: 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–6 (May 2012)
7. Bourimi, M., Rivera, I., Scerri, S., Heupel, M., Cortis, K., Thiel, S.: Integrating multi-source user data to enhance privacy in social interaction. In: Proceedings of the 13th International Conference on Interacción Persona-Ordenador, INTERACCION 2012, pp. 51:1–51:7. ACM, New York (2012)
8. Karatas, F., Bourimi, M., Barth, T., Kesdogan, D., Gimenez, R., Schwittek, W., Planagumà, M.: Towards secure and at-runtime tailorable customer-driven public cloud deployment, pp. 124–130 (March 2012)
9. Bourimi, M., Barth, T., Haake, J.M., Ueberschär, B., Kesdogan, D.: AFFINE for enforcing earlier consideration of nFRs and human factors when building socio-technical systems following agile methodologies. In: Forbrig, P., Bernhaupt, R., Forbrig, P., Gulliksen, J., Lárusdóttir, M. (eds.) HCSE 2010. LNCS, vol. 6409, pp. 182–189. Springer, Heidelberg (2010)
10. Bourimi, M., Kesdogan, D.: Experiences by using AFFINE for building collaborative applications for online communities. In: HCI International 2013, Parallel Sessions. HCII 2013 (to appear, 2013)
11. Karatas, F., Kesdogan, D.: A flexible approach for considering interdependent security objectives in service composition. In: Proceedings of the 28th Symposium on Applied Computing (ACM SAC), pp. 1919–1926 (2013)
12. Karatas, F., Heupel, M., Bourimi, M., Kesdogan, D., Wrobel, S.: Considering interdependent protection goals in domain-specific contexts: The di.me case study. To be published in the Proceedings of the 10th International Conference on Information Technology - New Generations (2013)
13. Cohon, J.L., Marks, D.H.: A review and evaluation of multiobjective programing techniques. Water Resources Research 11(2), 208–220 (1975)
14. Dantzig, G.B., Thapa, M.N.: Linear Programming 2: Theory and Extensions. Springer (2003)