From "security for privacy" to "privacy for security"

Riccardo Bonazzi*, Boris Fritscher*, Zhan Liu* and Yves Pigneur*
*Faculty of Business and Economics
University of Lausanne, 1015 Lausanne Switzerland
Email: zhan.liu@unil.ch

***Abstract*—This article envisions the use of context-awareness to improve single sign-on solutions (SSO) for mobile users. The attribute-based SSO is expected to increase users' perceived ease of use of the system and service providers' authentication security of the application. From these two features we derive two value propositions for a new business model for mobile platforms. The business model can be considered as an instantiation of the privacy-friendly business model pattern presented in our previous work, reinforcing our claim that privacy-friendly value propositions are possible and can be used to obtain a competitive advantage.**

***Index Terms*—Current awareness systems, Authentication, Machine learning, Business.**

I. Problem Identification

This paper assesses ways for context-aware mobile applications to authenticate a mobile user using Personal Identifiable Information (PII). According to previous literature, information security is required to protect PII and ensure users' privacy; yet such security implies a trade-off between the system developers' effort to implement privacy-enabling technologies and the cognitive effort required by the user to use such technologies. Consider a mobile user trying to access a set of web services, as shown in the top part of figure 1. The user has to pass a set of access controls for authentication, identification, authorization, and accountability. This security procedure increases the user's perceived performance of the protection application, but it negatively affects the ease of use of the system. Previous studies [1] have shown how low perception of ease of use can lead to lack of user compliance with security policies. A single sign-on (SSO) solution can increase the ease of use, as shown in the middle part of figure 1. Solutions like Firefox's built-in password manager increase ease of use but reduce the amount of effort attacker must put forth to access the user accounts since there is only the master password to break.

In order to offer stronger authentication SSO usually requires a shift from an access control list system (e.g., passwords) to a capability-based system (e.g., biometric controls or multi-factor authentication). However this approach lack of flexibility, since users biometry cannot be changed over time. We believe that context awareness can help us to achieve the proper trade-off between dynamic authentication and ease of use, as shown in the bottom part of figure 1. Since the early 1990s, context-aware mobile computing has received interest from scholars [2] [3].

For the purposes of this paper, we refer to context as *any information that can be used to characterize the situation of [...] a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and application themselves* [2]. Based on this definition, there are four types of primary context: *location*, *identity*, *activity*, and *time*. These types characterize a situation by answering where, who, what, and when, respectively. We are looking for a system that can transparently authenticate the user and dynamically adapt to the user's behavior. Therefore, our research question is: **How can context-awareness be used to improve authentication security and ease of use, while designing SSO applications for mobile devices?**

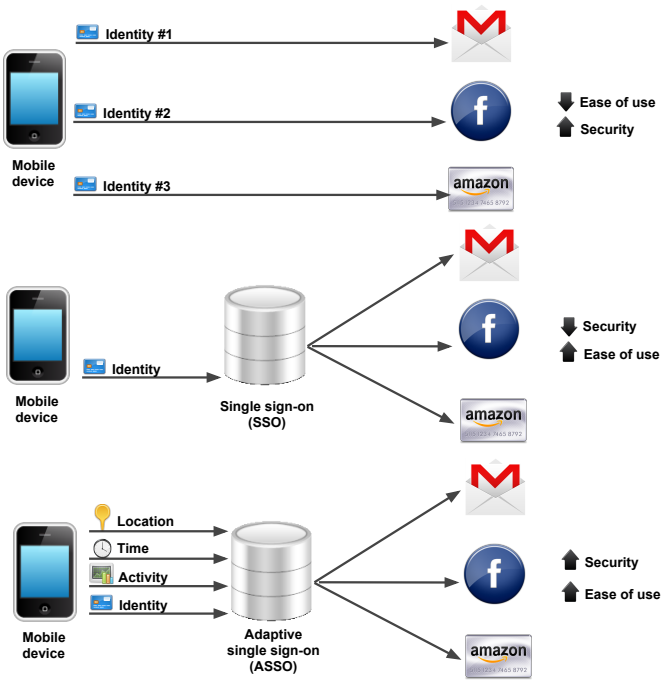

Fig. 1. Adaptative Single Sign-On (ASSO) for security and ease of use

In the rest of the paper we adopt the methodology proposed by Peffers et al. [4]. The next section presents an illustrative scenario to introduce the solution we aim to achieve. The third section lists the objectives of our research, and the fourth section illustrates a set of business model considerations concerning the application of our solution. The last section concludes by listing the contributions of this paper and the research directions it opens.

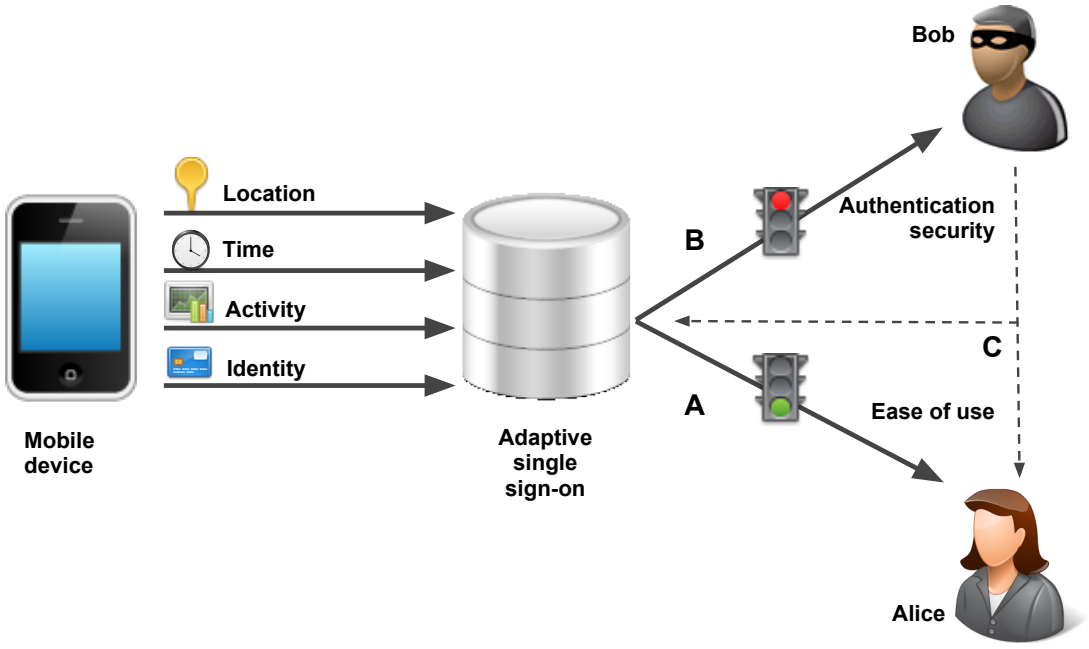

Fig. 2. Process of ASSO solution for a context-aware mobile device

II. A Simple Illustrative Scenario

Figure 2 represents a simple scenario presenting the adaptive single sign-on solution.

A. Alice accesses her Internet accounts

The end user, Alice, has a mobile device with a paid application called *Privacy Manager*. This application uses adaptative authentication to combine real-time transaction data with Alice's behavioral profile. Real-time transaction data used to identify Alice include her current location, speed (activity), and time. Once the data analysis application returns a positive authentication result, Alice can check her e-mail and bank accounts online through the protected channel. Thanks to *Privacy Manager* she can access her email and bank accounts without having to enter any passwords, as long as data analysis returns a positive result.

B. Bob cannot access Alice's accounts

Assume that a thief (Bob) plans to steal Alice's mobile device to access Alice's bank account. Once Bob steals the device, the real-time transaction data does not match the data stored in Alice's profile. Suppose Bob knows this authentication method, and he tries to to follow Alice before stealing the phone: Bob would note her location at any given time and collect personal information about Alice in order to copy her behavior. However the *Privacy Manager* applies state-of-the-art obfuscation techniques to not disclose any information about the activity and the identity of Alice, leaving Bob with only half of the information required.

C. Alice goes on holiday

When Alice goes to another city to see a friend, *Privacy Manager* detects that the behavior disclosed does not match Alice's older profiles. Neverless Alice possesses a trusted mean of identification (e.g. a password) to provide user's identification. After identification, *Privacy Manager* creates a new profile and stores data to include Alice's behavior on this day. When Alice comes to this city again to see her friend, her behavior data will be matched with this profile.

III. Objectives of the Solution

From a cognitive point of view, usability issues arise when users cannot properly manage the information required to sign in to different web services using a large set of different pseudonyms and passwords. The possibility of capturing the change in the identity of the real user (the features of his or her everyday life behavior) has been considered only as a threat to his or her privacy. We propose to shift from a discretionary access control approach to an attribute-based approach, where the attributes are features of the user's environment and his or her behavior in that context.

This approach provides a high level of control over access to the services while maintaining its high level of usability for mobile users, under the assumption that each user has a unique pattern of behavior. In previous studies, context-aware technology has evoked concerns about privacy. Location-based applications track users automatically on an ongoing basis, generating an enormous amount of potentially sensitive information so the identity of the owner of the mobile device can be implicitly obtained from the analysis of its location [5] [6]. However, we see great potential in this potential threat,

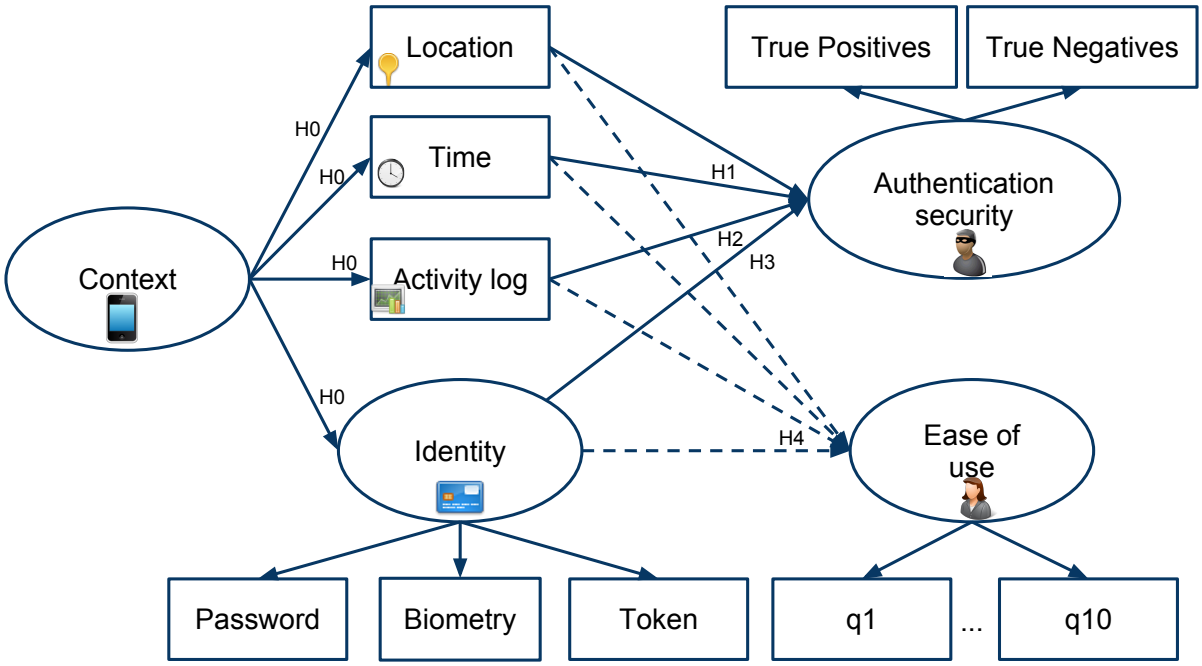

Fig. 3. Theoretical Model

and we formulate our starting assumption in the form of a null hypothesis: **context is a unique user identifier (H0)**.

Context-based authentication is currently used for credit card fraud detection relying primarily on artificial intelligence techniques using unsupervised learning methods [7]. Machine learning usually refers to evolved behaviors based on empirical data, such as that from sensor data or databases associated with artificial intelligence. The information is acquired during authentication through a learning process to authenticate the mobile user. The asserted advantages of machine learning are accuracy comparable to that achieved by human experts and considerable savings in terms of expert labor power, since no intervention from either knowledge engineers or domain experts is needed for the construction of the classifier or for its porting to a different set of categories [8]. User data clustering can be performed on two levels: on one hand, the best matches and the corresponding data points can be automatically or manually grouped into several clusters so outliers can be easily detected, and the alert will be activated once the number of outliers exceeds the predefined threshold. On the other hand, new trends can be found when regions on the map representing a cluster are identified and used for classification of new data. To test our hypotheses we propose a system that collects a set of mobile sensor data and compares them to a known set of user's profile. Moreover we suggest using an escalating procedure to minimize the computational effort of the system for most authentication cases. Therefore a limited amount of phone sensor data are collected by the context-awareness component, and through the machine leaning the mobile phone can determine whether it is dealing with an authorized user or not. If the result is positive, the user is authorized to access the services (e.g., Amazon, Gmail, Facebook); otherwise, additional contextual information (escalating from time and location up to activity and, eventually, identity) about the user is collected and analyzed before access to any service is granted. Figure 3 presents the structural model. A rectangular element is associated with a variable that can be directly measured, whereas an oval represents a latent concept that has to be measured indirectly by summing the variables to which it is associated.

We define authentication security as the number of true positives and true negatives obtained by the system. In other words, we aim to minimize the number of occurrences in which the user is not allowed to access the system (false negative) or an unauthorized person is allowed to access the system (false positive). We have already stated that location data can be used to infer much about a person, even without the user's name attached to the data [9]. In our case, let us suppose that the user goes to work every day and comes back following the same routine. In this case, the system would assess the user's location at a certain frequency against the expected pattern (home-work-home). Thus, we derive our first hypothesis: **the conjoint effect of time and location increases authentication security (H1).**

There may be cases when the home-work-home pattern lacks sufficient variance to discriminate the user from other people. For example, someone physically close to the user could take the phone while it is unattended and access a

number of services. Since the phone does not change location, the unauthorized access would be possible, even if for a limited amount of time. To address this problem, the system detects when the variance among the collected data is too small, and in that case collects the user's activities (e.g., web pages visited) against known activity patterns. Previous research has shown that such activity patterns are also discriminant [10]. Thus, we derive our second hypothesis: **the conjoint effect of time, location, and activity increases authentication security (H2).**

Many users do not often follow repetitive patterns. For this reason, the fourth contextual dimension (i.e., identity) is used when sensor data do not fall into any known pattern. To update the behavioral patterns we grant access rights to the user after proper identification (e.g., by means of a password, biometric control, or near-field communication card). This kind of identification has already been used by a large set of services. Banks call credit card users after an unexpected buying pattern, and Facebook asks for the answer to a secret question when the user tries to access it from a foreign country. Thus, our third hypothesis arises: **the conjoint effect of time, location, activity, and identity increases authentication security (H3).**

A final consideration concerns how we handle ease of use, which we measure using Venkatesh's [11] survey items (indicated in figure 3 as q1-q10). We believe that our escalating approach, combined with the machine learning techniques for classification and the eventual use of available solutions for identification would reduce the number of human-computer interactions required for authentication, increasing the user's perceived ease of use. This idea is in line with similar research currently undertaken by banks to obtain mobile-payment devices that do not use passwords [12]. Thus, we derive the last hypothesis: **the conjoint effect of time, location, activity, and identity increases ease of use (H4).**

IV. The Business Model

This section extends the business model pattern to a third party in charge of managing the privacy of mobile users, third-party and mobile services providers [13]. For the sake of coherence with the approach previously used we apply the business model ontology (BMO) of Ostewalder and Pigneur [14]. This approach allows us to represent a business model, whose value propositions are derived from the two performance criteria of our theoretical model (i.e. ease of use and authentication security). The following paragraphs use the nine business model elements defined by BMO to assess the strategic contribution of our adaptive single sign on (ASSO) application for context-aware mobile device.

Value proposition: it is at the center of the business model. It describes which customer problems are solved and why the offer is more valuable than similar products or services from competitors. The privacy-friendly business model pattern presented in [13] had four value propositions. One value proposition (personalized) that concerned the privacy risk-neutral customer segment is out of scope since it concerns distributive justice. Another (matchmaking) that concerned the typical added value of a third party is not changed. The two remaining value propositions (privacy risk mitigation and customer data analysis) do not change, but their corresponding customer segment is inverted. Therefore, customer data analysis for ease of use is associated with the mobile user instead of with the service provider. Our context-aware ASSO solution increases the level of usability without sacrificing its protection level. At the same time, the mobile device authenticates the mobile user through an accurate learning process that has no other costs. Risk mitigation by means of security authentication is now associated with service providers instead of mobile customers

Customer segments: In the BMO customers are analyzed and separated into groups to help identify their needs, desires, and ambitions (singles, families). In our new pattern, we pass from four to two distinct customer segments: the mobile user seeking ease of use and the service provider seeking authentication security. Since our solution can benefit both mobile users and service provides, our business model patterns is similar to an infomediary between two customer segments.

Customer relationship: it specifies what type of relationship the customer expects and how it is establish and maintained (promotion, support, individual, or mass). Since we do not introduce any significant change for this business model component, the key to attracting users is to promote the importance of privacy protection and to build a strong trust relationship with the customer. We define trust as *a willingness to rely on an exchange partner in whom one has confidence* [15]. A trust relationship may be built on physical, social, economic, or emotional characteristics.

Channel: it illustrates how the customer wants to be reached and by whom the customer is addressed (e.g., the Internet, a store). We do not introduce any significant change to this business model component. Our ASSO application for a context-aware mobile device is based on the mobile phone for an end user. The authentication technology would be provided under the shape of a service providing an application programming interface (API) or an application made with a software development kit (SDK).

Key activities: they are used to transform all resources into the final product or service (development, production, proprietary process). In the new pattern, we maintain the previous key activities (control and build network), and we introduce the important concept of adaptative authentication, which implies unsupervised rule generation. The user can be authenticated by identifying the feature of the user's behavior pattern through machine learning, but if the context-based authentication fails, an adaptive authentication is required.

Key resources: staff, machines, and proprietary knowledge are required to deliver the value proposition. In the new pattern, we maintain the previous key resources (user data, brand, and platform access) and eventually add the algorithm for adaptative authentication.

Key Partners: for resources or activities, most businesses depend on an external partner network (logistics, financial) that which can provide better quality or a lower price on non-

essential components, and we introduce no significant changes for this business model component. In order to guarantee the trust worthiness and security of this solution and to be able to certify that application made for this platform is compliant our solution has to be certified by an external certification provider. To offer additional services, our solution must also be in relationship with a mobile user and a service provider.

Revenue streams: they reflect the value the customers are willing to pay and how they will perform the transaction. In the new pattern, the two revenue streams associated with the two selected customer segments are switched: the end user pays a fee to use the application, and the service provider pays a fee for each secure transaction (or it could by a license to develop a set of ASSO applications).

Cost structure: it is another side of financial information and it should be aligned to the core ideas of the business model. In the new pattern, we maintain the previous key resources (network building, platform management, and development) and eventually add the dynamic authentication algorithm management.

V. Discussions and Conclusions

This paper proposes a new instantiation of the business model pattern presented last year at BMMP 2010 [16] and described in detail in a journal article [13]. Our new model has privacy at the core of its value proposition whereas previous instantiations considered privacy as a complementary service to be aggragated to other value propositions.

Therefore this paper makes three contributions: (1) we present an improved solution for SSO using the mobile user's attributes; (2) we reinforce our previous call for better and more privacy-friendly business models; and (3) we present new ways to use privacy as key component of mobile business models.

In the current stage of project development, we acknowledge a set of limitations. The first one concerns the choice of the approach to represent the business model. Since we wanted to instantiate an existing business model pattern, we kept the same representation, but we acknowledge the existence of alternative business model frameworks, such as Bouwman et al. [17] and Wegmann [18], that may be more geared to mobile since they can take the mobile or ICT service as a unit of analysis. We also acknowledge that IBM and Vodafone are currently developing a software solution similar to the one proposed here. However, since their solutions are proprietary, we could not include information about their performance.

As future extensions of our solution, we recall the *mobile device vs central server* options presented in the previous work [13] and we intend to explore two *what-if* scenarios, which arise when one of the two agents takes the lead:

(1) *What if the ASSO is owned by services providers in a situation of coopetition?* In this case, the application would mostly reside in central servers of service providers. These providers would use an ASSO API to develop new applications or by defining an ASSO standard. The mobile user would use a client application on the mobile device that would send the context information in order to obtain authentication. This approach would increase the performance of the authentication algorithm, which could take advantage of power the central server and that could decrease its learning time by having a larger pool of users' data. Moreover the update of client's application would be easier to perform and user's data could reside on the server to not leave anything on the mobile in case of stealth.

(2) *What if a device-centric authentication is preferred to the ASSO platform?* In this case, the ASSO would mostly reside on the user's mobile device. The authenticating algorithm would be stored within a mobile application that would establish a secure connection with the service provider after user's authentication. This approach would address privacy concerns, which might arise against the centralized solution, since in this case the user's data are not stored in the server. Additionally this approach is expected to drain less battery power, since the increased computational effort would be compensated by the reduction of client-server data exchanges required in the first scenario. In a possible extension of this scenario users could authenticate each other without the need for a third party. This solution would spread the user's data among peers, in order to reduce the success chances of malicious attacks [19].

Acknowledgment

The work presented in this paper was supported by the Swiss National Science Foundation (NSF) under grant number 205121-120534.

References

[1] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the 28th international conference on Human factors in computing systems*, New York, NY, USA, 2010, pp. 383–392.

[2] H. de Vos, T. Haaker, M. Teerling, and M. Kleijnen, "Consumer value of context aware and location based mobile services," in *Bled 2008 Proceedings*, Austria, Jun. 2008, pp. 50–62.

[3] B. Schilit, N. Adams, R. Want *et al.*, "Context-aware computing applications," in *First workshop of Mobile Computing Systems and Applications*, Santa Cruz, California, USA, 1994, pp. 85–90.

[4] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.

[5] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, 2003.

[6] J. Freudiger, M. Manshaei, J. P. Hubaux, and D. C. Parkes, "On Non-Cooperative location privacy: A Game-Theoretic analysis," in *Proceedings of the 16th ACM conference on Computer and communications security*, New York, NY, USA, 2009.

[7] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235–249, 2002.

[8] F. Sebastiani, "Machine learning in automated text categorization," *ACM computing surveys (CSUR)*, vol. 34, no. 1, pp. 1–47, 2002.

[9] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[10] A. L. Barabasi, "Authors@Google: albert laszlo barabasi," Sep. 2010. [Online]. Available: http://www.youtube.com/watch?v=7YFNf1ix_yY

[11] V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research*, vol. 11, no. 4, pp. 342–365, 2000.

[12] J. Sterngold, "Say goodbye to all those passwords," *BusinessWeek: Online Magazine*, Jan. 2011.

[13] Z. Liu, R. Bonazzi, B. Fritscher, and Y. Pigneur, "Privacy-friendly business models for Location-Based mobile services," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 6, no. 2, Aug. 2011.

[14] A. Osterwalder and Y. Pigneur, *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. New York, NY, USA: Wiley, 2009.

[15] C. Moorman, G. Zaltman, and R. Deshpande, "Relationships between providers and users of market research: the dynamics of trust within and between organizations," *Journal of marketing research*, vol. 29, no. 3, pp. 314–328, 1992.

[16] R. Bonazzi, B. Fritscher, and Y. Pigneur, "Business model considerations for privacy protection in a mobile location based context," in *Proceedings of the First Business Models for Mobile Platforms (BMMP) workshop*, Berlin, Oct. 2010.

[17] H. Bouwman, M. Zhengjia, P. v. d. Duin, and S. Limonard, "A business model for IPTV service: a dynamic framework," *info*, vol. 10, no. 3, pp. 22–38, 2008.

[18] A. Wegmann, "On the systemic enterprise architecture methodology (SEAM," in *Proceedings of the International Conference on Enterprise Information Systems (ICEIS) 2003*, 2003.

[19] V. Pathak and L. Iftode, "Byzantine fault tolerant public key authentication in peer-to-peer systems," *Computer Networks*, vol. 50, no. 4, pp. 579–596, 2006.