E-Profile-based Security for Critical Transactions in Web Applications

Jean Stephan\textsuperscript{1}, Nagi Wakim\textsuperscript{2}, Youakim Badr\textsuperscript{3}

\textsuperscript{1}Holy Spirit University of Kaslik, Faculty of Sciences and Computer Engineering, Lebanon
\textsuperscript{2}National Institute of Applied Sciences (INSA-Lyon), France
{\{nagiwakim, jeanstephan\}@usek.edu.lb
youakim.badr@insa-lyon.fr

Abstract

The recent financial crisis has prompted governments to become more pro-active in order to increase confidence and reestablish trust in the overall economic system. Accordingly, confidential information, such as secret bank accounts and personal information are nowadays being exposed and shared between institutions in order to minimize potential risks. However, exercising control and maintaining transparency should not be at the expense of an individual’s privacy, which is defined as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” Information privacy can be thought of as “the ability of the individual to personally control information about one’s self” [1].

1. Introduction

The goal of this paper is to propose a security framework which depends on the collaboration of e-commerce stakeholders in order to build an infrastructure that provides confidence and security while respecting the privacy of individuals at the same time.

The main thrust of our model is assessing the profile of a user and determining the confidence level which can be entrusted in the user. The overall framework of our model consists of two main components: User profile development and confidence determination and decision making.

2. User profile development

The main goal of this step is to develop a user profile online (e-profile) which reflects the user’s credentials and reputation based on available data and information about the user. The user profile, a centralized service, includes two types of data/information: declarative and deduced. The declarative data is a set of known facts generally provided by the user primarily at the initial stage, i.e., when the user is first “introduced” to the system.

This information may include items such as the user’s biographical data, usernames and passwords, or background information, etc. This part of the profile should be mostly static and, hence, is rarely changed. On the other hand, the deduced part is primarily information that is derived, synthesized, or generated from other information and from the user’s experience and behavior in cyberspace. Examples may include visited websites, saved cookies, past e-commerce transactions or credit rating, etc. Therefore, a profile rating, $R$, is a function of multiple variables:

\[ R = f (S_1, S_2, S_3, S_4, P, F, G) \]

Where:

- $S_1$ denotes a quantified representation of the Social Status (relevant social and professional attributes, such as education level, professional rank, age, etc.)
- $S_2$ denotes a measure of the user’s Surfing Habit of websites of the same category as the currently visited website.
- $S_3$ denotes Security Constraints set by each ecommerce website to tighten or loosen their private selection measures.
S4 denotes Social References; this is another way to acquire confidence in web users, it is a commonly used process to allow people introducing themselves into new communities, for example, to get hired or to be accepted as a supplier, etc. This additional recognition is given by others who will be held accountable for any misleading information. Each social reference is subject to a confidence examination process based on the profile’s attributes and thus a social profile can be modified if one of its variables is changed overtime (see profile maturity below).

P denotes the relevance of the user’s background and identity to the domain area or specialization of the visited website, where the transaction T is taken place. Therefore, there is a different value of P for each website the user visits. For example, if a computer science professor visits the acm.org website, the value of this P should be very high due to the strong relationship between the user’s profession and the website’s domain.

F denotes a measure of the user’s experience with the website. This includes Frequency of accessing the website, date and duration of each visit, and website surfing information (e.g., number of pages visited, actions submitted, inquiries made, etc.).

G denotes the age of the user’s profile.

3. Confidence determination and decision making process

The purpose of this step is to determine the confidence coefficient in the user by assessing the current situation based on the rating of the user’s profile and to decide as to whether or not to adjust the security level of the sought transaction. The input to the confidence coefficient (C) functions include the user’s rating (R), the transaction type (T) and the risk factor (K) associated with this type of transaction as specified by the vendor. In essence, each type of transaction would have a different risk factor. Therefore,

\[ C = f(T, R, K) \]

Depending on the outcome of C, the vendor may decide to allow or decline the transaction.

In summary, the process flow of our distributed model will be as follows:

Profile Builder → Rating Agent → Confidence Determiner → Vendor Decision

Where the “Profile Builder”, a centralized service, may reside at one location, the “Rating Agent” and the “Confidence Determiner” at another location and the “Vendor Decision” would be at whole different location. Furthermore, the implementation of this model calls for each of R and C to be computed through a mathematical model with the possibility of feedback of the computation outcomes into the profile in order to contribute to the evolution of the profile and, hence, to enhance its trustworthiness.

3. Conclusion

Kenichi Ohmae [2] considers the internet as an invisible continent that has no conventional government leading to a major gap in regulations, trust and privacy; nevertheless, our suggested framework promotes awareness and preserves privacy by centralizing the access to user profiles and acquiring a rating through a profile assessment service. Furthermore, Identity Management is no longer based on static data. Instead, the user’s profile is a dynamic entity which evolves with time and matures based on the user’s behavior, experience, and/or interventions. Similarly, e-commerce websites will be able to set their own security rules to manage critical transactions and clarify their filtering schema. In this way, the collaboration of different stakeholders will provide a rich added value towards a more trustworthy Internet-based economy.

4. References

[1] Maria van Heerden, JS Consultants, South Africa
The Economic and Social Impacts of E-Commerce,
Sam Lubbe, Cape Technikon, South Africa, Johanna
ISBN 1-59140-043-0.