DIGITAL PSEUDONYM IDENTITY FOR E-COMMERCE

Rafael Martínez-Peláez, Francisco J. Rico-Novella, Luis A. Zarza-López
Department of Telematics Engineering, Technical University of Catalonia, C/Jordi Girona 1 i 3, Barcelona, Spain

Keywords: Digital Identity, Identity Risks, Genuine Identity.

Abstract: The identity is a unique and intransitive property which any human being possesses. Due to its characteristics is used in Internet. Unfortunately, when a user discloses his personal information to web site does not know the risks about his identity's privacy. This paper describes the usefulness of user's identity in Internet and the problems related with their usage in web sites. To improve the user's privacy we propose a digital pseudonym identity as an alternative to replace the used of genuine identity in Internet.

1 INTRODUCTION

The real world identity has different perspectives, and all identities make reference to an individual whose characteristics make him/her unique in different fields where he/she is. Commonly, identity is referred to the name of a person, but possibly two or more people may have the same name. In this case, other characteristics can make the difference among them. We defined Genuine Identity (GI) as all the characteristics that can be make unique a person like address, e-mail, DNA, habits, name, social security number, etc.

The adoption of e-commerce and use of different Internet services have created in the customers a necessity of having various digital identities in different web sites. Digital identity is an effort to recreate, to organize and to make up aspects about genuine identity in digital world to be able to be linked in the real world (Casassa et al., 2002).

Virtual sites request customer's information by web form. With this method the customer need to give personal information to each web site in order to have access (Koch and Wörndl, 2001). Additionally, this mechanism converts a user experience into tedious task.

When users use Internet to disclose theirs GI involve risks that demands security requirements. On the one hand, customers want to maintain their GI's privacy and anonymity. On the other hand, companies need to have a mean to identify and link an attacker in both real world and digital world.

In this paper we propose a new Digital Pseudonym Identity (DPI) for exclusive use in Internet. With this new proposal the users could have the option to create digital identities in any web site without using web form and disclose personal information over an open network.

2 APPLICATION OF GENUINE IDENTITY IN E-COMMERCE

The application and administration of GI's information is a key to develop electronic commerce. The importance of management is concluded in validating established profiles, and rights in the relations (Casassa et al., 2002). The information can be used in process related with identity management (Koch and Wörndl, 2001; Berthold and Köhntopp, 2001) or security mechanisms (Clifford, 1995).

2.1 Identity Management

The implementation of identity management makes possible to provide the user with the opportunity to manage their digital identities reusing the information between web sites. Identity management system maintains the privacy not only on his/her digital identity, but genuine identity too. Another advantage is the control over digital identities in terms of authenticity, lifecycle and validity (Berthold and Köhntopp, 2001).

The main use of GI's information is to create accounts (figure 1). In order to create an account is necessary specific user's information (user profile) such as, name, DNI or passport, address, telephone, email, date of birth, nationality, in some cases

Martínez-Peláez R., J. Rico-Novella F. and A. Zarza-López L. (2006).
DIGITAL PSEUDONYM IDENTITY FOR E-COMMERCE.
In *Proceedings of the International Conference on Security and Cryptography*, pages 91-94
DOI: 10.5220/0002103700910094
Copyright © SciTePress

financial information (Koch and Wörndl, 2001). The purpose of creating an account in a web site is to have a digital identity that would make it unique, and to allow receiving rights, privileges and obligations.

Companies have a special interest in knowing its customers with the purpose to offer a best service and to make easier the internal administrative operations (Smith et al., 1999). Other advantages are the opportunity to monitoring the clients' behaviours for three aspects: to make a market research, to identify business opportunities, and preventive security.

2.2 Security Mechanisms

The importance of using the GI in Internet is to give the option of being identified in both real and digital world. Security mechanisms take advantage of digital identity: authentication, authorization, identification and non repudiation (Clifford, 1995).

- Identification is a process whereby a person is recognised. The identification is made through the use of digital identity. The digital identity is created on the customer's GI. Companies base its trust on the user's information. Users can be linked in the real world by his/her digital identity as long as the delivered information be valid and authentic.
- Authentication is a mechanism used to verify if a customer is really a person who says to be (Clifford, 1995). In this case, companies can use the information like secret piece of user's knowledge in order to know who he/she is.
- Authorization defines the privileges given to the customers within the system. The privileges involve limiting actions, granting access to resources, and avoiding changes of identity (Clifford, 1995). As the account was created using the user's GI, his/her digital identity will have the privileges based on the information related with him.
- Non-repudiation is the process to prevent the denial of actions inside and outside the system. In e-commerce, it is common the user denies his/her participation in electronic transactions. Companies require a mechanism to be able to prove the user's participation and can initialize legal actions. For this reason the information about the user must be true.

3 RISK SCENE IN E-COMMERCE

The participants in e-Commerce require a mutual identification. Virtual sites are identified by the use of digital certificate and their reputation, while a client requires giving personal information in order to create an account. When users disclose personal information do not know the risk that this action implies in the real world. The illegality is not in the use of false identity, but the fraud is by doing so (Smith et al., 1999).

a) Identity supplanted: After giving all the detailed information about its GI, a customer trusts in the private policy offered by the web site. Unfortunately a worker could not be honest and could use the information to mask itself under this identity. With detailed information about a person it is easy to make frauds or attacks as much in Internet as in the real world (Arnold, 2000). Another scenario is when an attacker can obtain personal information about any person in the real world and then use it in Internet, without victim's knowledge.
b) Fraudulent transactions: In some cases the goal of stealing a GI is to make fraudulent transactions (Arnold, 2000). An attacker has an opportunity to use a person's identity to open bank accounts, request for credits or play online in a legitimate manner in virtual sites. It is difficult for virtual sites to check authenticity and veracity of information. From a legal point of view, the owner of this information (GI) is guilty (Smith et al., 1999).
c) Publication of identities: web sites are responsible for maintaining information of their customers in privacy. However it is possible to make the customers information public either by an attack or by internal errors, like it occurred in

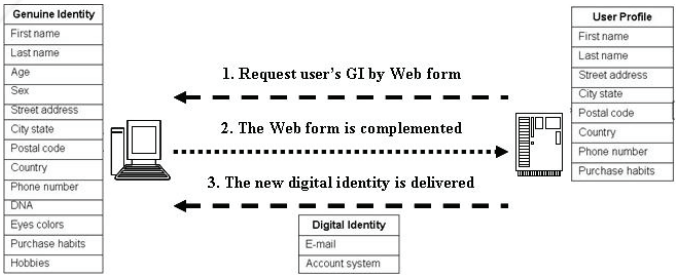

Figure 1: General process to create a digital identity.

October 1999 (Arnold, 2000), when the US Army published a document with the identities of officials in service and retired, producing a series of frauds which affected people who appeared in the document.

d) Identity Theft: Due to the low participation of the customer in the process of creating an account it is possible to produce attacks based on the supplanting of authentication dialogue box or the web form (Tygar et al., 1996). This is achieved due to the high probability that a next event would take place because always is the same dialogue box and web form. For an attacker is easy to imitate it and to be able to obtain information of the customer without his awareness.

4 OUR PROPOSAL

With the goal to offer a solution to the problem of giving information about GI to every web site which required having an access through public network, so the use of new Digital Pseudonym Identity (DPI) is proposed.

4.1 Security Requirements

Privacy and anonymity are requirements desired by users in Internet. Companies require identifying the user in its system.

Users' requirements

- Privacy usually refers to maintaining personal information in secret and autonomy. Customers demand to maintain their personal information privacy in transactions online and while data may be stored.
- Anonymity is the state of being not identifiable within a set of subjects (Pfitzmann and Köhntopp, 2001). Anonymity is a characteristic to avoid a relation between GI and digital identity.

Companies' requirements

- Pseudonym is an identifier of subjects. Whereas be anonym and non-anonym are the extremes with respect to GI public. A pseudonym contains characteristics that can be used to make a relation between GI and digital identity in legal actions (Pfitzmann and Köhntopp, 2001).

4.2 Objectives

Our solution is to allow users to disclose personal information about their genuine identity while reduces risks for their privacy. Our objectives can be summarized as follows:

- To allow users to disclose specific information without giving it directly to the Web site.
- To allow users to create accounts in different web sites with minimal effort.
- To allow users to standardize the company's request of its information.
- Provide a digital identity that can be stored in a flexible and secure mean (smart card).
- To allow companies to store valid and authentic user's information.
- To allow companies to prevent identity theft.
- Provide a mean to improve network security.

4.3 Criteria for Digital Pseudonym Identity

Taking as bases the GI the following properties are necessary:

a) Durability: Due to the risk of security in Internet, the cycle of life proposes is one year.
b) Mobility: Like an identity card (DNI or passport) the digital identity must be transportable.
c) Portability: The data structure of the digital identity must be able to be used by different devices.
d) Revocation: In the cycle of life of the digital identity it must be possible to revoke it.
e) Renovation: When the time of life of the digital identity finishes, the owner must have the opportunity to continue using it.
f) Traceable: In the case of a penal investigation, it would be possible to know and follow an attacker in the real world.
g) Unicity: After a digital identity is created there must not exist another identical digital identity.
h) Untransferable: As the digital identity has privileges and responsibilities in different web sites it can not be transferable to other person.

4.4 Profile Scheme

We want to enable users to create their digital identity in different web sites with minimal effort using his/her DPI. The DPI is pseudonym because the holder can be identified without to reveal his/her GI. On the other hand, his/her DPI is unique and suitable to be used to authenticate the holder.

DPI is created by a user only one a year. The DPI is signed by a TTP (trust third party). With the signature the holder can prove its validity. The web sites can trust on its authenticity and integrity. The holder of the DPI can create an account in different sites without disclosing his/her information by web form. On the other hand, the web sites can have the

option to accept or deny the creation of two or more accounts for the same user (figure 2).

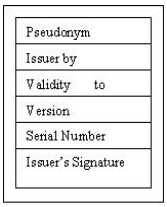

Figure 2: DPI Profile Structure.

4.5 Comparison

In comparison with the traditional mechanism, our proposal guarantees an amount of information necessary to the virtual sites in order to create an account within the system. By this mean the following results can be obtained:

- Companies which search customers' information will be able to trust in its validity and authenticity.
- The distribution of information to malicious web sites does not affect the customer in the real world.
- The customer does not require interacting with any web form.
- Companies can make supervision on the activities and behaviour of the customer without invading his/her identity's privacy.
- The GI theft by Internet is limited.
- Companies can have the opportunity to link an attacker in the real world.
- DPI theft reduces the risk of being used in real world.
- The DPI publication does not affect a customers' privacy in real world.
- Companies will be able to reduce the frauds made by identity supplanted.

5 CONCLUSIONS

In this paper, we presented the use of genuine identity in Internet. The main risks related with the use of genuine identity in Internet and how can affect a customer in the real world have been explained. The proposal of the use of digital pseudonym identity has been proposed for replacing the use and distribution of genuine identity by web forms. Digital pseudonym identity is an effort to motivate the adoption of e-Commerce based in the customer's identity authenticity and validity. Another aim is increasing the security in web sites and reduces problems related with the identity theft.

Future work will be made in the design and develop of data structure in where appears the DPI profile structure information (like in the real world DNI or passport) and can be verifiable its authenticity and validity by any organization or company.

ACKNOWLEDGEMENTS

This work has been partially supported by the Spanish Research Council (CICYT) under the project SECONNET (TSI2005-07293-C02-01).

REFERENCES

Casassa, M., Bramhall, P., Gittler, J., Pato, J., & Rees, O. (2002, June 12). Identity management: A key e-business enabler. Retrieved July 28, 2005, from Hewlett-Packard Laboratories Web Site:
http://www.hpl.hp.com/techreports/2002/

Koch, M., & Wörndl, W. (2001). Community support and identity management. *In Proceedings of the 7th European Conference on Computer Supported Cooperative Work*, 319-338.

Berthold, O., & Köhntopp, M. (2001). Identity management based on P3P. *In Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, 141-160.

Clifford, B. (1995). Security, payment, and privacy for network commerce. *IEEE Journal on Selected Areas in Communications*, 13, 1523-1531.

Smith, A., Pittman, S., & Clarke, R. (1999). Identification, authentication and anonymity in legal context. Retrieved June 7, 2005, from Australian National University, Department of Computer Science Web site:
http://www.anu.edu.au/people/Roger.Clarke/DV

Arnold, T., (2000, June). Internet identity theft -A tragedy for victims-. SIIA. Retrieved from http://ctl.ncsc.dni.us/publicaccess/states/otherresources/articles/whitepaper-internetidtheft-2000.pdf

Tygar, J., & Whitten, A. (1996). WWW Electronic commerce and java trojan horses. *In Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, 243-250.

Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity –A proposal for terminology. *In Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, 1-9.