Identity Crisis Management: Usability, Issues and Challenges

Megha Bhatia*

ABSTRACT

An identity crisis is a developmental event that involves a person questioning their sense of self or place in the world. The concept originates in the work of developmental psychologist Erik Erikson, who believed that the formation of identity was one of the most important conflicts that people face. According to Erikson, an identity crisis is a time of intensive analysis and exploration of different ways of looking at oneself. This paper studies the current 'identity crisis and its management' caused by the substantial privacy and usability shortcomings encountered in existing systems for identity management. Some of these issues are well known, while others are much less understood. This paper brings them together in a single, comprehensive study and proposes recommendations to resolve or to mitigate the problems. Some of these problems cannot be solved without substantial research and development effort.An identity crisis is a developmental event that involves a person questioning their sense of self or place in the world. The concept originates in the work of developmental psychologist Erik Erikson, who believed that the formation of identity was one of the most important conflicts that people face. According to Erikson, an identity crisis is a time of intensive analysis and exploration of different ways of looking at oneself. This paper studies the current 'identity crisis and its management' caused by the substantial privacy and usability shortcomings encountered in existing systems for identity management. Some of these issues are well known, while others are much less understood. This paper brings them together in a single, comprehensive study and proposes recommendations to resolve or to mitigate the problems. Some of these problems cannot be solved without substantial research and development effort.

Keywords: *Identity management, privacy, usability, challenges*

INTRODUCTION

Identity is the concept, beliefs, qualities and expressions that differentiate us from the people around us. Identity is something that we develop into; that makes us different than anyone else. The way we define ourselves, through self-identity, is essentially the basis of our self-esteem and self-worth. Our social identity, is constructed through the opinions of others, with groups/labels we are associated into. Our identities are influenced by positive and negative of social identities.

Identity is not only what you want to reveal about yourself, but also what others conclude, believe, and find out about yourself. In fact, most of a person's identity is of this type. Such data may be wrong, become invalid over time, be misrepresented, or be misguiding, etc. In other words, an identity does not necessarily correspond to reality. Moreover, it shows that an identity has many owners: it is not only owned by the entity it describes, but also collected and owned by others. A fine example of this is your health care records that are being collected by GPs, specialists and other health care personnel. Health records are owned by (and the responsibility of) the

* *Associate Professor School of Business Management, IFTM University*

GP. You may have the right to view them, but you don’t necessarily have the right to change them. This has important privacy ramifications.

Instead of an entity having one single identity containing all characteristics taken from all scopes, it is more natural to view an entity as a collection of multiple identities (a set of sets), each with their own scope. Note that this aligns with the idea that privacy ensures that information about a person does not leak from one scope into another.

The fact that identities remain to exist long after the entity ’dies’ can result in a wealth of personal information stored in many places, leading to privacy risks for users that are somehow related to this entity. It may also result in IdPs giving out incorrect claims, damaging their reputation of a trusted partner that needs to be right always. Furthermore, claims (that link some identity information to an identifier) may continue to exist indefinitely, even after the identity information itself is deleted. When the claim of an old identity still exists and a new identity is created with the same identifier, these two may seem to refer to the same entity, while this is not the case.

Managing identities does not only mean handling new and fixed identities within one scope, but also handling the complex situations of changing identities in changing scopes, and managing the different perceptions of identity within the same scope. This is a challenge.

Identity management consists of the processes and all underlying technologies for the creation, management, and usage of digital identities. In practice, it covers the process of establishing the identity of a remote user (or system), managing access to services by that user, and maintaining identity profiles concerning that user. As such, identity management is an essential component for the successful development and growth of the next, so-called “2.0”, user-centric Internet services. Secure, reliable and user-friendly identity management is also considered fundamental in establishing trust, for instance in e-commerce applications.

The aim of the research paper is to address this gap by exploring user perceptions of identity crisis and identity management systems.

LITERATURE REVIEW

Identity encompasses all the essential characteristics that make each human unique but also all the characteristics that enable membership to a particular group or culture as well as established status within the group (Roussos et al. 2003). The identity of a person comprises a large number of personal properties. All subsets of the properties represent partial identities of the person and may relate to roles the person plays. Depending on the context, the person may have multiple different partial identities (Clauss and Koehntopp, 2001).

Roussos et al. (2003) offer three principles of identity: locality, reciprocity and understanding. The Locality Principle argues that identities are situated within particular contexts, roles, relationships and communities. People will have multiple different and overlapping identities in different contexts, and each of these should be respected. A global or universal identifier makes little sense. In human relationships, knowledge of identities is negotiated and both sides in the relationship should know how properties that characterise identity are exchanged and used. Relationships should be symmetrical and reciprocal. Furthermore, identity serves as a basis for understanding in two-way relationships. Mutual knowledge of identities improves the ability to see things from the other point of view and leads to trusting relationships.

Human identity is the individuality and personality of a particular person and may be characterised by a number of properties of that person (Simpson and Weiner 1989). The properties of an individual may be intrinsic (eg. DNA, retina scan, hair colour), descriptive (eg. name, birthplace), demographic (eg. occupation, gender), geographic (eg. address, country, postcode) or psychographic (eg. interests, preferences). The identity of a person denotes that person, reflecting their uniqueness, and provides a means of differentiating them from others. It also provides a means of establishing similarity with others in various roles (eg. customer, employee) and social groups (eg. elderly citizens, family) (Carroll and Murphy 2004).

Key issues with identity management

A critical analysis of literature revealed a number of key issues with identity management. These include control and power, authentication, trust, security, privacy and multiple identities. Each of these is now discussed, linked to relevant literature and provide a basis for data collection in the empirical study.

1. Control and power

The creation and management of information about individuals is central to identity management. Although organizations in the private and public sector should not exchange such information without the user's consent, permission is often given without the user's specific knowledge. For example, the disclaimer that states information will be passed on is often hidden in the fine print. A possible solution is to have interlinked record-keeping (identity management) systems to monitor the exchange of information. A second solution is to use different digital pseudonyms with each organization, enabling users rather than organizations, stay in control of their digital identities. Users can then protect themselves against organizations sharing their digital details. Clarke (2004) claims that the true benefits of federated systems are largely for the provider, in that organizations and governments gain valuable information while the user's privacy is being compromised by the compilation and circulation of detailed user profiles. However, as Hagel and Rayport (2000) point out, it can be argued that the implications of this are that federated systems essentially represent a trade-off, where the user sacrifices privacy and control over personal information for the ease and convenience that one consolidated digital identity brings. They argue that a solution to this is that consumers should capitalise on this situation and demand value in exchange for information.

2. Authentication

Authentication in general is a process by which confidence in some assertion is gained – it need not relate to identity in particular. eBusiness depends on the reliability of a range of assertion type statements, sometimes about identity but often involving value or attributes. Risk assessments would help organizations to clarify what assertions are most in need of authentication. For some transactions there is a need to know the "identity" of the other party – for very few transactions there is a further need to know the "entity" or the real-world thing (Clarke 2004).

3. Trust

The growth of electronic commerce has been hindered by a lack of trust between consumers and service providers (Roussos et al. 2003). A major reason for this is federated identity management systems provide users with limited options to control and personalise their data. Without a sense of control, or the ability to personalise, users become reluctant to reveal details about themselves, instead preferring to provide as little information as possible (Clarke 2004). This is a problem for providers and organizations as detailed information about the user is a valuable asset. A possible means of fostering greater trust would be if providers were to give users an element of control over aspects of their digital identity. This would give users the opportunity to personalise their digital identity and decide what they revealed in relation to the context of the activity.

4. Security

Identity theft occurs when personal information is used by someone else without their knowledge. It usually supports criminal activity, including fraud, deception, or obtaining benefits and services in the person's name. Identity theft is the fastest growing type of electronic crime and it is expected to accelerate (Identity Theft Task Force 2007, Roussos et al. 2003). It is particularly prevalent in the digital domain because all that is needed is one piece of information about a person, for example, a credit card number, to steal their identity. Stronger authentication mechanisms, for example the use of biometrics, can help to reduce the prevalence of identity theft.

5. Privacy

Privacy relates to the claims of individuals that information about themselves should generally not be available to other individuals or organizations, and where data is possessed by another party, the individuals must be able to exercise a substantial degree of control over that data and its use (Koch and Woerndl 2001). Empirical studies show that Internet users are very concerned about their privacy are not inclined to provide personal information when requested – they want more anonymous transactions (Koch and Woerndl 2001). A balance is required between effective governance, legal needs and national security needs on the one hand, and individual dignity and privacy on the other hand (Clarke 2004).

6. Multiple identities

Clarke (2001) argues identity has a multi-faceted quality, therefore, reducing rich and complex user information into a single digital entity results in systems that fail to capture the intricacies of everyday user behaviour. This was supported by Roussos et al (2003). They argue that identities are situated within particular roles, relationships and communities and that people will have multiple, different and overlapping identities in different contexts. Each of these should be respected, thus, a global or universal identifier makes little sense. This means there is a strong need by people to have many identities and avoid their federation. "Silos are good, at least for 7 privacies" (Clarke 2004, p41). Many standards, for example Liberty Alliance and PingId, acknowledge that people need multiple identities but still maintain the idea of an underlying single, federated identity – a global set of attributes from all a person's existing accounts. Multiple identities are assumed to be a problem for individuals and federation will be of benefit. It may help in some circumstances but will certainly improve the social control interests of business and government

IDENTITY CRISIS MANAGEMENT- "WHO AM I TODAY?"

As discussed above, users may have several identities, even within a single scope. This distinction in identities manifests itself when people have several different responsibilities, or, in other words, may have several different "roles". Examples may help to clarify this issue.

When signing a document, a notary can choose to sign this as a notary, or as a private person. The distinction is legally significant. The CFO of a company may use an electronic banking system either to enter a personal or a business transaction. An ICT system administrator may sign in to a system either as "root" (which allows him to run OS-level applications and scripts) or as an ordinary system user (that allows him to only execute end-user applications). We see that users can have different roles that allow them to do different things within a certain service. Furthermore, the impact of user actions depends on their role: a signature of an accountant or a notary represents more legal value.

Current identity management systems do not make it easy for users to manage such different roles (although, to be fair, exceptions exist). Basically, users are forced to maintain and manage several identifiers to separate these roles. But this may lead to confusion. For instance, if a user has previously signed in at its IdP using a particular identity, and the user and the service support single sign-on, the user may automatically be signed in using this same identity when accessing a different service sometime later. This is potentially dangerous: if the CFO signed in as CFO earlier, he may not want to execute a personal transaction while still being signed in as CFO.

Depending on the type of service, actions performed in a certain role may be visible to others that can also access that role, or result in information sent to the organisation that is responsible for that role. For example, all communication of the president of the USA is kept for later reference. The same goes for many transactions performed when doing business. In these situations, privacy sensitive information can become public, such as the purchase of personal books, visiting certain websites, or the rental of a hotel room, when the role that was selected to execute those actions happened to be a business role.

For many current identity management systems these very common usage scenarios pose a problem. There is no way to indicate as which role, or which identity, a user wants to access a particular service, especially if he has accessed that system in both capacities before. One of those identities may be selected automatically (in a single-sign-on context), most likely without the user knowing why, or how to change it.

What is the optimal size of a key chain? – or – How many identities should a user have?

One of the main advantages of identity management for end-users is single-sign on: not having to remember all those user names and passwords, except for the login-token for the IdP. From this perspective, it would be great to have just one IdP: only one user name/password (or another authentication token) and that's it.

Of course, this is not feasible. Not only because users may not trust that one IdP to have access to all their services. Even if users do trust a single IdP for that, using only one IdP means that if that IdP is compromised, all identity data is compromised immediately as well. It is therefore advisable for users to distribute their identity information over multiple IdPs. Furthermore, different RPs will require different IdPs. Financial institutions for example have other requirements and preferences than car rental agencies with respect to an IdP. The first may want to set up their own IdP to be able to control the security of authentication, while the latter is satisfied with using a third-party IdP. Can we then settle for one IdP for personal use, one for work, and one for each financial institution? This seems to be a workable yet quite arbitrary subdivision. The question is: how many identity providers does a user need? What is the best compartmentalisation of the digital identity mess? We need to understand the advantages and risks of using a certain amount and distribution of IdPs and federations, in terms of security, usability, and business.

Therefore, it is recommended to determine which and how many "identities" are optimal, a model that captures these relevant aspects needs to be developed. To our knowledge such a model does not exist yet.

CONCLUSION & RECOMMENDATIONS

Identity management not only comprises identification and authentication, but also access management and user profile management. Stakeholders such as end-users and relying parties require identity management systems to be able to span multiple organisations, to be user-friendly, privacy friendly, and secure. Current systems for identity management are not able to accomplish this.

The issues of identity management systems presented in the paper cause the current identity crisis. In order to resolve the identity crisis, we recommend to follow up on the following main observations made in this paper.

- A proper model for identity underlying identity management should be developed, and IdPs and RPs should make explicit how that model applies to their systems of identity management.

- Building on that model, the trust relationships between the parties using an identity management should be investigated and formalised.

- To prevent phishing attacks, it is very important that users can (and will) authenticate the RP and the IdP. Mutual authentication therefore needs to be incorporated in identity management systems, in such a way that the user is not required to install special software or to use one and the same computer all the time.
- To enhance user privacy, we recommend that users can remain anonymous or use pseudonyms at RPs, and to have IdPs that do not link all user transactions at all RPs together. Although identity management systems already implement at least part of these solutions, not all do so.

- Identity management systems should provide a way for users to see and select their identity with which they "sign in" even if explicitly signing in is not asked for.

- Identity management systems should provide a way to automatically determine the full set of required credentials for a certain service, and the minimal role the user can assume that covers those credentials.

- Finally, we need identity management systems that put the user back into control and that support the user in maintaining a user profile that can be used (in a controlled manner) by business from several organisational domains.

Most of these recommendations are not trivial, and to implement them requires substantial research, development, and standardisation effort. Moreover, to resolve the identity crisis stakeholders need to work together on this. We believe the growing need for a proper, well-founded, identity management solution legitimates the effort.

BIBLIOGRAPHY

- CARROLL, J. and MURPHY, J. (2004) Who am I? I am Me! Identity Management in a Networked World, Proc 4th International We-B Conference, Edith Cowen University, November
- CHAUM, D. (1985) Security Without Identification: Transaction Systems to make Big Brother Obsolete, Communications of the ACM, 28:10 (October), 1030-1044
- GENGLER, B. Standard ID clears a path in password jungle, IT Alive Section, The Australian, August 3rd 2004, p 4
- HAGEL, J. and RAYPORT, J. (2000) The Coming Battle for Customer Information, Harvard Business Review, January-February, pp 53-65
- HEARDT, DICK. Web 2.0 High Order Bit - Identity 2.0. http://identity20.com/media/WEB2_2005 HEMMINGS, T. et al.
- KOCH, M. and WOERNDL, W. (2001) Community Support and Identity Management, Proc. European Conference on Computer Supported cooperative Work, Bonn, Germany (September)
- KRUEGER, R. A. (1988) Focus groups: A practical guide for applied research. Newbury Park, CA: Sage Publications
- LEENES, R., SCHALLABOCK, J. AND HANSEN, M. (2007) PRIME white paper v2, version 1.0 (accessed 5th July 2007) https://www.prime-project.eu/prime_products/whitepaper/
- LIBERTY ALLIANCE PROJECT (2003) Introduction to the Liberty Alliance Identity Architecture, Revision 1.0, March (accessed 5 August 2004) https://www.projectliberty.org/liberty/content/view/full/183/(offset)/15
- NEUMAN, W. L. (2003) Social research methods : qualitative and quantitative approaches. Boston, Allyn and Bacon REID, E. (2004) Cultural Formations in Text-Based Virtual Realities. Cypersociology Magazine. January 28
- ROUSSOS, G., PETERSON, D. and PATEL, U. (2003) Mobile Identity Management: An Enacted View, International Journal of Electronic Commerce, 8:1, pp 81-100 SATCHELL, C., SHANKS, G.,
- HOWARD, H., MURPHY, J. (2006) Knowing Me, Knowing You: End User Perceptions of Identity Management Systems, Proc. European Conference on Information Systems, Gothenburg, June
- SIMPSON, J.A. and WEINER, E.S.C. (1998) The Oxford English Dictionary, Clarendon Press, Oxford.
- STRAUSS,L., and CORBIN, J. (1997). Grounded Theory in Practice. Sage. TURKLE, S. (1995). Life on the screen: Identity in the age of the Internet. New York: Simon & Schuster.