Digital Identity Modelling and Management

by

Sittampalam Subenthiran

Supervisor
Dr Johnson Agbinya

Thesis submitted to the University of Technology, Sydney
in total fulfilment of the requirement for the degree of
Master of Engineering by Thesis

Faculty of Engineering

University of Technology, Sydney

2005

Certificate of Originality

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Candidate

Production Note:
Signature removed prior to publication.

Acknowledgements

I would like to thank Dr. Kumbesan Sandrasegaran for the encouragement during the early part of my candidature.

I am profoundly grateful to Dr. Johnson Agbinya who helped immensely and guided me with his knowledge and experience throughout the critical point of my research phase to completion. I am also grateful for his continuous patience, support and advise during the course of my studies.

I would like to thank Prof. John Hughes and Prof. Hung Nguyen for helping me by providing vocational scholarship, conference travel funds and valuable guidance.

It is very difficult to acknowledge everyone who has helped me in numerous ways. However, I would like to mention few people who have helped me in many ways: Prof. Peter White, Prof. Subhash Challa, A/Prof. John Leaney, Dr. Tim O'Neil, Dr. Tracy Tung, Prof. Robin Braun, A/Prof. Ananda Sanagavarapu, Rosa Tay, John Mueller, Ramzi Shalak and Simon Trajkovski.

Finally and most importantly, I like to thank my lovely wife Pamini, my two wonderful sons Raahulan and Lavan, and my mother-in-law Mrs. Vadivelu for their patience, understanding and support while I was away doing my research.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

List of Publications

Conference Proceedings

[1] S. Subenthiran, K. Sandrasegaran, and R. Shalak, "Requirements for Identity Management in Next Generation Networks", *Proceedings of IEEE International Conference on Advanced Communications Technology*, vol. 1, Korea, 9-11 February 2004, pp. 138-142

[2] R. Shalak, K. Sandrasegaran, J. Agbinya, and S. Subenthiran, "UMTS core network planning model and comparison of vendor product performance", *Proceedings of IEEE International Conference on Advanced Communications Technology*, vol. 2, Korea, 9-11 February 2004, pp. 685-689

[3] S. Subenthiran and Dr. J. Agbinya "Identity Modelling and Management", *Accepted for publication at the University of Technology Sydney, Faculty of Engineering Research Showcase*, Sydney, 11th May 2005,

Poster Presentations

[1] S. Subenthiran, "Identity Modelling and Management", *Accepted for presentation at the University of Technology Sydney, Faculty of Engineering Research Showcase*, Sydney, 11th May 2005,

Abstract

User identification and authentication is the first and most important aspect of identity management in maintaining security and privacy of users and their assets. Due to the open nature of the Internet, without reliable identification and authentication, subsequent security and privacy protections become worthless. Amid the increase of the number of online services and users, identity fraud is on the increase. It has been widely reported that identity fraud costs the industry many billions of dollars each year around the world.

Perpetrators use false identities to engage in fraudulent activities. False identities can be established in one of two ways: (i) creating fictitious identity by manufacturing, forging or fraudulently obtaining legitimate documentation to satisfy proof of identity (POI) requirements, and (ii) stealing or forging someone else's identity from an actual person (living or dead) such as passwords, security tokens or biometric information.

One of the effective ways to prevent identity fraud is to build defence against the use of false identities. Use of false identities can be prevented by implementing strong authentication, using multi-factor identity proofing (during service enrolment phase) and multifactor identity authentication (during service delivery sessions). To balance convenience and security, the strength of the authentication needs to match the required level of trust. If the implemented strength is lower than the required level of trust, it may introduce risk of fraudulent activities. On the other hand if the implemented strength is higher than the required level of trust, it may introduce inconvenience to the user, preventing the usage.

To solve this issue, we propose CaMa (Credential Attribute Mapping) models to calculate the strength of authentication for multi-factor identity proofing and multi-factor identity authentication scenarios. The strengths are calculated from the desired properties of identities and presented in two ways. (i) a process of summation of the weighting index of the desirable properties, and (ii) application of information theory.

Further, a scheme for constructing digital representations of personal identities from conventional identity documents such as birth certificates, citizenship certificates, passports, driving licences, bank card and photo ID is also proposed. This digital representation of personal identity along with the concept of (i) active credentials, (ii)

trusted identity providers, (iii) secure assertion protocol such as SAML and with the (iv) established policies and procedures, enable a user to assert their identity to a remote online service provider that request the proof of identity (POI) requirements. Thus, it will help freeing users from the limitation of personal presence during service enrolment. For example, in this way, it will be possible to open a bank account in the USA by remotely submitting trusted identity credentials online from Australia.