

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

CERTIFICATE OF ORIGINALITY	2
ACKNOWLEDGEMENTS	3
LIST OF FIGURES	9
LIST OF TABLES	10
LIST OF PUBLICATIONS	13
ABSTRACT	14
1. INTRODUCTION	16
1.1 Problem Statement	17
1.2 Aims	17
1.3 Scope	18
1.4 Outcomes	18
1.4.1 Background Theory	19
1.4.2 Digital Representation of Personal Identity	19
1.4.3 Development, Application and Analysis of CaMa Model for Identity-proofing Scenario	19
1.4.4 Development, Application and Analysis of a CaMa Model for Remote Online Identity-authentication Scenario	19
1.4.5 Development, Application and Analysis of a CaMa Model for Multimodal Biometric Authentication	19
1.5 Organisation of Thesis	19
2. DIGITAL IDENTITY	21
2.1 Introduction	21
2.2 Definition of Identity	22
2.3 Digital Identity	24
2.4 Digital Identities on the Internet and its Analysis	25
2.4.1 Explicit Identification	25
2.4.2 Implicit Identification	25
2.5 Desirable Properties of Identities	29
2.5.1 Uniqueness	29
2.5.2 Consistency	29
2.5.3 Persistency	29
2.5.4 Verifiability	30
2.6 Conclusion	30

3. IDENTITY MANAGEMENT	31
3.1 Introduction	31
3.1.1 Federated Network Identity	31
3.2 Identity Management in All IP Networks	32
3.3 Benefits of Identity Management	34
3.4 Identity Management Standards and Solutions	34
3.4.1 Liberty Alliance Project	35
3.4.2 WS-Federation	37
3.4.3 Microsoft Passport	38
3.4.4 Shibboleth	40
3.4.5 Identity Management Components	40
3.4.6 SAML Security	43
3.5 Efforts on Universal Personal Digital Identifiers	44
3.5.1 E-Num	44
3.5.2 Universal Communications Identifier	46
3.5.3 i-Name	46
3.6 Conclusion	47
4. PRIVACY AND DIGITAL IDENTITY	48
4.1 Introduction	48
4.2 What is privacy?	48
4.3 Regulatory Framework	49
4.4 Platform for Privacy Preferences (P3P)	49
4.5 Conclusion	50
5. IDENTITY FRAUD	51
5.1 Introduction	51
5.2 Online Identity Theft	52
5.2.1 Spyware	52
5.2.2 Phishing Attack	53
5.3 Protection against the Use of Fictitious Identities or Altered Own Identity: Identity-Proofing	54
5.3.1 Phase 1: Identity-proofing by Credentialing Authority	55
5.3.2 Phase 2: Creation of Identity Credential	56
5.3.3 Phase 3: Presentation of Identity Credential to Relying Party	56
5.3.4 Phase 4: Acceptance of Credential by Relying Party	57
5.4 Protection against Online Identity Theft	57
5.4.1 Protection against Password Sniffing, Guessing and Cracking	57
5.4.2 Protection against Spyware	58
5.4.3 Protection against Phishing Attack	59
5.5 Conclusion	59

6.	IDENTITY-AUTHENTICATION CREDENTIALS	61
6.1	Introduction	61
6.2	Pseudometrics - Something You Know	62
6.3	Physicalmetrics – Something You Possess	64
6.3.1	Time-based Code Generating Tokens	65
6.3.2	Event-based Code Generating Token	65
6.3.3	Challenge-based Code Generating Token	66
6.3.4	Challenge/Response Based Cryptographic Token	66
6.4	Biometrics – Something You Are	67
6.4.1	Two modes of Biometrics Operation	69
6.4.2	Two types of Identification Applications	70
6.4.3	Desirable Properties of Biometrics	71
6.4.4	Biometric Characteristics	72
6.4.5	Biometric Systems for Cyber-space Applications	72
6.4.6	Biometrics System Errors	75
6.4.7	Limitations of Biometric Systems	77
6.4.8	Multimodal Biometric Systems	78
6.4.9	Social Acceptance and Privacy Issues	79
6.5	Conclusion	79
7.	DIGITAL IDENTITY REPRESENTATION	80
7.1	Introduction	80
7.2	Choosing Identity Credentials	81
7.3	Choosing Attributes	81
7.4	Digital Encoding of the Attribute Values	81
7.4.1	Full Name	82
7.4.2	Residential Address	82
7.4.3	Date of Birth	82
7.4.4	City of Birth	83
7.4.5	Country of Birth	83
7.4.6	Country of Citizenship	83
7.4.7	Race	83
7.4.8	Mother’s and Father’s Names	84
7.4.9	Eye Colour	84
7.4.10	Credentials in Possession	85
7.4.11	Biometric Iris Scan	85
7.4.12	Biometric Fingerprint	86
7.4.13	Height	86
7.4.14	Biometric Signature	86
7.4.15	Photo	86
7.5	Proposed Digital Representation of Personal Identity	87
7.6	Conclusion	87
8.	CREDENTIAL ATTRIBUTE MAPPING (CAMA) FOR MULTIFACTOR IDENTITY-PROOFING	89
8.1	Introduction	89

8.2	Approaches to Calculating strength of Credentials	90
8.3	CaMa 1 – Arbitrary Estimation	90
8.3.1	Assigning Weights to Each Attribute	91
8.3.2	Applying Credential Attribute Mapping (CaMa) to calculate strength of Credentials	92
8.4	CaMa 2 – Applying Desirable Properties of Identities	93
8.4.1	Desirable Properties of Attributes	93
8.4.2	Calculating the weights of the Attributes	95
8.4.3	Applying Credential Attribute Mapping (CaMa) to calculate strength of Credentials	96
8.5	CaMa 3 – Applying Thresholds to Desirable Properties of Identities to weight the attributes	97
8.5.1	Formulation of criteria and threshold for assigning scores	97
8.5.2	The process of assigning the scores	100
8.5.3	Calculating the weights of the Attributes	105
8.5.4	Applying Credential Attribute Mapping (CaMa) to calculate strength of Credentials	106
8.6	Performance Analysis and Comparison of the Credential Strengths	107
8.6.1	Choice of identity attributes	107
8.6.2	Choice of properties of identity attributes	108
8.6.3	Criteria used for scoring against each property	108
8.6.4	Assumptions used for setting threshold for scores	108
8.6.5	Method used to derive the weights of each attribute	108
8.6.6	Method used to calculate strength of each credential	109
8.6.7	Considerations for Further Research	109
8.6.8	Australian Government Banking Identity Point Scoring Scheme	109
8.6.9	Comparing results from the proposed methods and Australian Banking Requirements	110
8.7	Credential Information Content	111
8.7.1	Information Content Based on Attribute Weights Method 1	112
8.7.2	Information Content Based on Attribute Weights Method 2	118
8.7.3	Information Content Based on Attribute Weights Method 3	123
8.7.4	Summary and Analysis of the Results obtained from Information Content	130
8.8	Conclusion	133
9.	CREDENTIAL ATTRIBUTE MAPPING (CAMA) FOR MULTIFACTOR IDENTITY-AUTHENTICATION	134
9.1	Introduction	134
9.2	Applying CaMa for Computing Strength of Identity-Authentication Credentials	134
9.2.1	Security against Brute force Attack	135
9.2.2	Resistant to Copy, Theft and Eavesdrop	136
9.2.3	Able to protect against the ability to use illegitimately acquired credential	136
9.2.4	Ability to replace the credential in the case it is compromised	137
9.2.5	Strength of Credentials	138
9.2.6	Convenience and Cost	138
9.2.7	Analysis of the results	140
9.3	Conclusion	141
10.	CAMA FOR MULTI-MODAL BIOMETRICS	142
10.1	Introduction	142
10.2	Application of CaMa for Calculating Strength of Unimodal Biometric System	143

10.2.1	Criteria and Threshold for the Requirement of Universality	143
10.2.2	Criteria and Threshold for the Requirement of Uniqueness	144
10.2.3	Criteria and Threshold for the Requirement of Permanence	146
10.2.4	Criteria and Threshold for the Requirement of Performance	148
10.2.5	Criteria and Threshold for the Requirement of Circumvention	149
10.3	Strength of Biometric Systems	150
10.4	Performance Analysis and Comparison of the Credential Strengths	151
10.5	Strength of Multimodal Biometrics	152
10.6	Conclusion	153
11.	CONCLUSION	154
11.1	Future work	155
12.	REFERENCE	156

LIST OF FIGURES

Figure 1: Identity Space	21
Figure 2: Concept of Personal Identity.....	23
Figure 3: AIPN Architecture Evolution	33
Figure 4: SAML Architecture	42
Figure 5: ENUM Operation.....	45
Figure 6: Universal Communications Identifier.....	46
Figure 7: Example of a Spoof Email used for Phishing Attack	53
Figure 8: Phases of Identification Process	54
Figure 9: Identity-proofing Process.....	55
Figure 10: Types of Authenticating Credentials	62
Figure 11: RSA Secure ID [®] Token	65
Figure 12: ActiveCard [®] Event-based Code Generator.....	66
Figure 13: ActiveCard [®] Challenge Based Code Generator.....	66
Figure 14: Challenge/Response Based Cryptographic Tokens	67
Figure 15: Biometric Sampling Process.....	68
Figure 16: Taxonomy of Human Races.....	84
Figure 17: CaMa 1 - Process of Calculating Strengths of Credentials.....	90
Figure 18: CaMa 2 - Process of Calculating Strengths of Credentials.....	93
Figure 19: CaMa 3 - Process of Calculating Strengths of Credentials.....	97

LIST OF TABLES

Table 1: Biometric Characterisation	72
Table 2: Components of a residential address	82
Table 3: Human Eye Colour Coding	85
Table 4: Credential types, serial numbers and expiry dates	85
Table 5: Proposed Digital Representation of Personal Identity	87
Table 6: CaMa 1 - Weightings of Identity Attributes by Arbitrary Estimation	91
Table 7: CaMa 1 – Credential Strengths	92
Table 8: CaMa 2 - Weights of Identity Attributes using a Scoring Method	95
Table 9: CaMa 2 – Credential Strengths	96
Table 10: Scoring Based on Uniqueness	98
Table 11: Scoring Based on Consistency	99
Table 12: Scoring Based on Persistency	99
Table 13: Scoring Based on verifiability	100
Table 14: Process of assigning the scores based on uniqueness	101
Table 15: Process of assigning the scores based on consistency	102
Table 16: Process of assigning the scores based on persistency	103
Table 17: Process of assigning the scores based on verifiability	104
Table 18: CaMa 3 - Attribute Weights derived from the desirable Properties of Internet Identities	105
Table 19: CaMa 3 – Credential Strengths	106
Table 20: Credential Strength Calculated by the Three CaMa Schemes	107
Table 21: Australian Banking 100 Point Proof of Identity Requirements	109
Table 22: Scaled Credential Strengths – A Comparison with Australian Banking Requirements	111
Table 23: Information Content Based on Attribute Weights Method 1 - Applying values obtained from CaMa 1	114
Table 24: Information Content Based on Attribute Weights Method 1 - Applying values obtained from CaMa 2	116
Table 25: Information Content Based on Attribute Weights Method 1 - Applying values obtained from CaMa 3	117

Table 26: Information Content Based on Attribute Weights Method 2 - Applying values obtained from CaMa 1	119
Table 27: Information Content Based on Attribute Weights Method 2 - Applying values obtained from CaMa 2	121
Table 28: Information Content Based on Attribute Weights Method 2 - Applying values obtained from CaMa 3	123
Table 29: Information Content Based on Attribute Weights Method 3 - Applying values obtained from CaMa 1	125
Table 30: Information Content Based on Attribute Weights Method 3 - Applying values obtained from CaMa 2	127
Table 31: Information Content Based on Attribute Weights Method 3 - Applying values obtained from CaMa 3	129
Table 32: Summary of the results obtained from Information Content	130
Table 33: Scaled Credential Strengths – A Comparison with Australian Banking Requirements	132
Table 34: Criteria and Threshold for Keyspace Entropy	135
Table 35: Criteria and Threshold for Copy, Theft and Eavesdrop	136
Table 36: Criteria and Threshold for ability to replay illegitimately acquired credential	137
Table 37: Criteria and Threshold for the ability to replace in the case it is compromised	137
Table 38: Identity-authentication Credential Strengths	138
Table 39: Criteria and Threshold for the for the degree of convenience	138
Table 40: Criteria and Threshold for the cost of deployment and use	139
Table 41: Cost and Convenience	140
Table 42: Analysis of Strength of Authentication Credential	140
Table 43: Criteria and Threshold for Universality	143
Table 44: Calculating Scores Based on Universality	144
Table 45: Criteria and Threshold for Uniqueness	145
Table 46: Calculating Scores Based on Uniqueness	146
Table 47: Criteria and Threshold for Permanence	147
Table 48: Calculating Scores Based on Permanence	147
Table 49: Criteria and Threshold for Performance	148
Table 50: Calculating Scores Based on Performance	149

Table 51: Criteria and Threshold for protection against Circumvention	150
Table 52: Calculating Scores Based on Circumvention	150
Table 53: Strength of Biometric Systems	151
Table 54: Strength of Biometric Credentials	151

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.