

MAgSeM: A Multi-agent based Security Model for Secure Cyber Services

By

Rossilawati Sulaiman

B Sc. (Computer Science)

M Sc. (Computer Science)

The Faculty of Information Sciences and Engineering
University of Canberra ACT 2601 Australia

PhD Thesis

A Thesis submitted in fulfilment of the requirements of the
Degree of Doctor of Philosophy
(Information Sciences and Engineering)

(August 6, 2010)

Abstract

Ever since people started to become aware of the value of information, they have been conscious about the underlying security issues. Reliance on the Internet as a medium of communication to exchange and share information has become prevalent. Electronic health (or e-health) uses the Internet to enhance healthcare service deliveries. Current practices in e-health involve applications that support online communication such as videoconferencing sessions, electronic mails, web-based applications, and also software applications used with mobile devices. Remote patients and medical staff communicate and exchange messages regarding e-health issues such as patient consultations, diagnosis, and appointment requests. Medical staff can also monitor patients remotely.

However, while the Internet greatly facilitates and enhances these services, significant threats also come in parallel. Network attacks, information privacy/sensitivity breaches, and malicious software, which involve programs that are purposely created to perform illegal operations (such as viruses and worms) on a computer system, are common types of threats to Internet communication. These threats can cause severe damage to computer systems as well as to the information. The information might be stolen or modified or even eavesdropped on and all these may cause undesirable consequences. Therefore, it is imperative that on line communication is secure.

Using these problems as motivation, we proposed a security framework, which caters for the security needs for online communication between two nodes which may have similar or dissimilar communicating environments. We introduce a Multilayer Communication approach (MLC) that improves efficiency, security, and robustness by classifying communication between different categories of users into five different layers based on requirements: Layer 1 to Layer 5, namely Extremely Sensitive, Highly Sensitive, Medium Sensitive, Low Sensitive and No Sensitive Data. This classification is based on the different sensitivity of the information being exchanged during communication. For example, Extremely Sensitive communication involves exchanging extremely sensitive information.

E-health security was the motivating problem. The various categories of users in e-health are identified, so that we can determine the sensitivity level of the information that may be exchanged between the users. Then the *layer of the communication* (Layer 1 to Layer 5) is

determined, to find the most suitable security mechanisms that should be applied to the communication. Data security and/or channel security are provided at each layer depending on the sensitivity of the data. Highest security mechanisms are applied to the extremely sensitive information, while low security mechanisms are applied to the low sensitive information. Cryptography protocols such as encryption/decryption, digital signature, and hash function are used and applied on the data, while secure socket layer (SSL/TLS) is used to secure the communication channel.

A novel multi-agent system architecture is developed to cater for the security processes to secure the communications at the various levels conceptualised at each layer. The agents are skilled with the knowledge to cater for the relevant security processes. Mobile agents are used as supporting tools to carry sensitive data from the Sender's side to the Recipient's side. Cryptographic protocols are used to secure the data as well as the mobile agent code, which provide mechanisms to verify the authenticity, confidentiality and the integrity of data, and decipher the data and code received by the recipient nodes. Here, appropriate MLC is identified and used real time when selecting the security protocols.

Experiments have been conducted on the proof-of-concept and tested using the Jade platform. The performance of each layer in MLC is investigated and we concluded that Layer 1 has the highest overhead compared to the other layers due to the highest security overheads applied in this layer based on the level of security requirements. Results also showed that agents incur a higher cost compared to the traditional method but these costs are largely due to communication requirements. However, the proposed architecture gives a much better control on security to the initiator for the end-to-end channels. The recipient nodes do assume any security control unlike most existing communicating nodes on networks. The proposed novel model contributes significantly to research in security for a class of problems that have distributed IT solutions over data networks. The e-Health problem was the motivating problem for the research. Its characteristic needs were adequately addressed by the model with increased robustness in security and improvement in efficiency.

Keywords: security, mobile agent, multi-agent system, e-health.

Acknowledgements

I would like to take this opportunity to express my sincere gratitude to my supervisors Prof Dr Dharmendra Sharma, Dr Wanli Ma, and Dr Dat Tran for their ongoing support and encouragement, kindness and guidance throughout my four years of research in the university.

Many thanks to all the ISE staff at the University of Canberra, who were involved whether directly or indirectly, and provided essential environment for the completion of this study; especially to Serena Chong, Coral Suthern, Hanh Huynh, Xu Huang, Claire Dunstan, and Jason Weber. My thanks also go to Fariba Shadabi and Girija Chetty for your ongoing encouragement.

Great thanks to other researchers in Room 11B-31, Kavitha Gurusamy, Sisira Adikari, Len Bui, Trung Le, and Dat Huynh; your hard work and support always inspire me to survive through these years. Many thanks for the friendship, and always make me feel at home.

Also, I wish to express my deepest thanks to my husband, Fadzli, who was there for me through thick and thin and continuously encouraged me; and to my lovely little son Amin, for giving me all the smiles and courage that I never thought I have to finish this thesis. Without your support this thesis would not have been possible. Also, my warmest thanks go to my family back home for their ongoing support and prayers.

Last, but not least, it is my pleasure to acknowledge the financial support for this thesis: National University of Malaysia and the Ministry of Higher Education of Malaysia.

Table of Content

Abstract.....	v
Acknowledgements	vii
Table of Content.....	ix
List of Figures.....	xiii
List of Tables.....	xvii
List of Acronyms	xxi
CHAPTER 1 INTRODUCTION.....	1
1.1 Motivations for the Research.....	1
1.2 Research Questions	5
1.3 Proposed Research.....	5
1.4 Contributions	6
1.5 Thesis Organization.....	7
CHAPTER 2 RECENT ADVANCES: SECURITY CONTEXT.....	9
2.1 Introduction	9
2.2 Computer Networks and Security.....	9
2.2.1 Open System Interconnection (OSI) Model.....	10
2.2.2 Network Security Attacks.....	13
2.2.3 Security Architecture and the OSI Model	15
2.3 A Review of Existing Security Systems.....	18
2.3.1 Firewall.....	18
2.3.2 Intrusion Detection Systems.....	21
2.3.3 Cryptography	22
2.3.4 Cryptography Systems.....	26
2.4 Security Applications	33
2.5 Agents and Security.....	37
2.5.1 Agents.....	38
2.5.2 Agent Characteristics.....	38
2.5.3 Multi-agent Systems and characteristics	40
2.5.4 MAS and Security	42
2.6 Gaps in Security: Motivations	54

2.6.1	Different Communication Needs: Current Technologies and Limitations.....	54
2.6.2	Motivations for secure multilayered communication structure.....	63
2.6.3	Multi-agents for secure multilayered communication.....	66
2.7	Summary.....	66
CHAPTER 3 PROPOSED MULTILAYER COMMUNICATION MODEL TO SECURE E-HEALTH COMMUNICATIONS		69
3.1	Introduction	69
3.2	Users and Networks.....	69
3.2.1	Online Communication	69
3.2.2	Motivation for a Secure Communication Environment	72
3.3	The Problem	74
3.3.1	Problem Characteristics.....	74
3.3.2	Analysis	81
3.4	Solution Models.....	97
3.4.1	Design of Solutions	97
3.4.2	Implementation.....	98
3.4.3	Test and evaluation.....	98
3.5	Summary.....	99
CHAPTER 4 MODELLING TRADITIONAL APPROACHES THROUGH MULTI- AGENT SYSTEM.....		101
4.1	Introduction	101
4.2	MAS Characteristics Supporting Traditional System Approach.....	101
4.2.1	Inadequacies of traditional approaches.....	101
4.2.2	MAS for MLC	105
4.3	MAS Suitability for MLC	106
4.3.1	Cooperation and coordination	106
4.3.2	Autonomy and behaviour	113
4.3.3	Extensibility.....	115
4.3.4	Interactive.....	117
4.3.5	Mobile.....	120
4.4	Justification for MAS	125

4.5	Summary.....	127
CHAPTER 5 PROPOSED MULTI-AGENT SECURITY MODEL		129
5.1	Introduction	129
5.2	Identifying Agents Goals against Organizational Structure.....	130
5.2.1	Organizing the Agents.....	132
5.3	MAgSeM Architecture	134
5.3.1	Communication Layers	136
5.3.2	MLC Specification	138
5.3.3	Control over Data by Sender	139
5.3.4	Security Mechanism in MAgSeM.....	141
5.3.5	Advantages of the Control Mechanism	144
5.4	MAgSeM Communication Architecture	145
5.4.1	Certificates and Keys.....	145
5.4.2	Message Format.....	146
5.4.3	Different Agents Actions.....	146
5.5	SUMMARY	151
CHAPTER 6 THE MAgSeM SYSTEM.....		153
6.1	Introduction	153
6.2	Supporting Tools	153
6.2.1	Java Agent DEvelopment Environment (JADE).....	154
6.2.2	Tools for Mobile Devices Development	160
6.2.3	Cryptographic library: Bouncy Castle.....	164
6.3	MAgSeM-based System Implementation.....	164
6.3.1	Agent Interactions: Wired System.....	165
6.3.2	Agent Interactions: Wireless System.....	167
6.3.3	Agent Base Classes Implementation	169
6.4	Socket-based System Implementation.....	193
6.4.1	Client-side Implementation	193
6.4.2	Server-side Implementation.....	195
6.4.3	Communication Link.....	196
6.5	Summary.....	199

CHAPTER 7	RESULT AND ANALYSIS.....	201
7.1	Introduction	201
7.2	Environment Setup	202
7.3	Experiment Setup	203
7.3.1	Wired System Communication.....	203
7.3.2	Wireless System Communication.....	206
7.4	Measurements.....	207
7.4.1	Time Measurement.....	207
7.4.2	Measurement Interval.....	207
7.5	Experimental Results.....	208
7.5.1	Evaluation: Execution Times for Wired Systems	208
7.5.2	Evaluation: Execution Times for Wireless Systems.....	222
7.6	Discussion and Evaluation	234
7.7	Summary.....	237
CHAPTER 8	CONCLUSION AND FUTURE WORK.....	239
8.1	Assessment against Research Questions	245
8.2	Future Work.....	248
Appendix A:	Program Construct for Concepts Developed	251
Appendix B:	Publications.....	303
BIBLIOGRAPHY	305

List of Figures

Figure 2-1: The seven layer of OSI model	10
Figure 2-2: The TCP/IP and OSI layer	12
Figure 2-3: Firewall between two networks	19
Figure 2-4: Demilitarized zone	20
Figure 2-5: IPSec Transport Mode	29
Figure 2-6: IPSec Tunnel Mode	30
Figure 2-7: Agency properties	38
Figure 2-8: Certification and information delivery phase	45
Figure 2-9: Monitoring phase	46
Figure 2-10: Agent platform with SCA	48
Figure 2-11: RETSINA architecture	49
Figure 2-12: Self-protected mobile agent mechanism	50
Figure 2-13: SECMAP architecture	51
Figure 2-14: Example of a company network	58
Figure 2-15: SSH algorithms configuration for Windows Server	60
Figure 2-16: IPSec setting on Window XP Professional	62
Figure 2-17: Examples of multilayered structure	65
Figure 3-1: Different types of communications in a hospital organization	76
Figure 3-2: Data security between two points	86
Figure 4-1: Control Topology	114
Figure 4-2: Example of FIPA-ACL message	119
Figure 4-3: Example of KQML message	120
Figure 5-1: AND/OR graph for the agent's actions	131
Figure 5-2: Organizing the agents in the layered architecture	132
Figure 5-3: Proposed MAgSeM	134
Figure 5-4: An example of MLC specifications	138
Figure 5-5: Maintaining Control over the Data	140
Figure 5-6: Agent Communication in MAgSeM	146
Figure 6-1: Platform and Containers	155

Figure 6-2: JADE-Leap runtime environment.....	158
Figure 6-3: Examples of sending an ACL message	159
Figure 6-4: Examples of receiving an ACL message.....	160
Figure 6-5: J2ME protocol stack	161
Figure 6-6: Jade Environment for Mobile Device.....	163
Figure 6-7: Communication protocols performed on the Wired system.....	165
Figure 6-8: Communication protocols performed on Wireless to Wired systems	168
Figure 6-9: Interface for user authentication	170
Figure 6-10: Interface for message composition	170
Figure 6-11: List of recipients	171
Figure 6-12: Interfaces for the MAgSeM-based Wireless system	171
Figure 6-13: MTA sending a request to every recipient's CLA.....	172
Figure 6-14: Determining com_layer	173
Figure 6-15: Implementation of MLC Specification.....	174
Figure 6-16: cA sends partial results to MTA	175
Figure 6-17: MTA's actions	176
Figure 6-18: Generate symmetric keys for Wired system.....	178
Figure 6-19: Generate a symmetric key for the Wireless system.....	179
Figure 6-20: Obtaining public and private key.....	179
Figure 6-21: Public key extraction	180
Figure 6-22: Key serializations	181
Figure 6-23: Symmetric encryption for the Wired system.....	182
Figure 6-24: Asymmetric encryption for the Wired system.....	182
Figure 6-25: Symmetric encryption for the Wireless system.....	183
Figure 6-26: Asymmetric encryption for the Wireless system.....	184
Figure 6-27: Binary encoding for the Wired system	184
Figure 6-28: Binary decoding for the Wired system	184
Figure 6-29: Binary encoding for the Wireless system	185
Figure 6-30: Binary decoding for the Wireless system	185
Figure 6-31: Generate key pairs	186
Figure 6-32: Signing with a private key	186

Figure 6-33: Verifying signature with a public key	187
Figure 6-34: Generate message digest.....	188
Figure 6-35: Recompute and verify message digest.....	189
Figure 6-36: Symmetric decryption for the Wired system.....	190
Figure 6-37: Symmetric decryption for the Wireless system.....	190
Figure 6-38: Asymmetric decryption for Wired system.....	191
Figure 6-39: Asymmetric decryption for Wireless system.....	191
Figure 6-40: Example of Jade.conf.....	192
Figure 6-41: Creating a client-side socket.....	193
Figure 6-42: Creating a client-side SSL-based socket.....	193
Figure 6-43: Creating a client-side socket.....	194
Figure 6-44: Sending message.....	194
Figure 6-45: Receiving messages.....	195
Figure 6-46: Creating a server-side socket.....	195
Figure 6-47: Creating a server-side SSL-based socket.....	196
Figure 6-48: Implementation for Socket-based system.....	196
Figure 6-49: Communication Flow on the Socket-based system.....	197
Figure 7-1: Environment setup for agent and socket-based communications.....	202
Figure 7-2: Environmental setup for mobile devices	202
Figure 7-3: Measurement of TransacT (MAgSeM-based).....	204
Figure 7-4: Measurement of TransacT (Socket-based)	204
Figure 7-5: Time intervals to complete a communication.....	207
Figure 7-6: Generating Cipherkey and Ciphercode for MAgSeM-based system	210
Figure 7-7: Generating Cipherkey and Ciphercode for Socket-based system.....	210
Figure 7-8: Comparison for T1 for MAgSeM-based system	211
Figure 7-9: Comparison for T1 for Socket-based system	212
Figure 7-10: Comparison for T3 for MAgSeM-based system	213
Figure 7-11: Comparison for T3 for Socket-based system	214
Figure 7-12: Comparison for TT for MAgSeM-based system.....	215
Figure 7-13: Comparison for TT for Socket-based system	216
Figure 7-14: Execution time for TransacT for MAgSeM-based	218

Figure 7-15: Execution time for TransacT for Socket-based	218
Figure 7-16: Generating Cipherkey and Ciphercode for MAgSeM-based.....	223
Figure 7-17: Generating Cipherkey and Ciphercode for Socket-based.....	224
Figure 7-18: Comparison for T1 for MAgSeM-based	224
Figure 7-19: Comparison for T1 for Socket-based.....	225
Figure 7-20: Comparison for T3 for MAgSeM-based	226
Figure 7-21: Comparison for T3 for MAgSeM-based	227
Figure 7-22: Comparison for Transfer Time for MAgSeM-based.....	228
Figure 7-23: Comparison for TT for Socket-based	229
Figure 7-24: Comparison for TransacT for MAgSeM-based.....	231
Figure 7-25: Comparison for TransacT for Socket-based	231

List of Tables

Table 2-1: Summary of the agent' characteristics to handle security processes	53
Table 2-2: Summary of security technologies.....	54
Table 2-3: List of ciphers in SSL v2	61
Table 2-4: List of ciphers in SSL v3 and TLS v1.....	61
Table 3-1: Examples of Online Communication.....	71
Table 3-2: Different Types of Information Exchanged between Users.....	78
Table 3-3: Five layers of communications in MLC	82
Table 3-4: Security levels excerpt from Table 7.4 from ECRYPT (2008).....	92
Table 3-5: The existing key size recommendations	92
Table 3-6: Key size recommendation for each layer in MLC	93
Table 3-7: The security specifications in MLC model.....	94
Table 3-8: Ciphersuites provided by SunX509 provide	95
Table 7-1: Experiment setup for wired system.....	205
Table 7-2: Experiment setup for non-mobile device agent-based system.....	206
Table 7-3: Time measurements for Ciphertext (MAGSeM-based).....	209
Table 7-4: Time measurements for Ciphertext (Socket-based).....	209
Table 7-5: T1 for MAGSeM-based system.....	212
Table 7-6: T1 for Socket-based system	212
Table 7-7: Percentage increased of the MAGSeM-based system for T1	213
Table 7-8: T3 for MAGSeM-based system.....	214
Table 7-9: T3 for Socket-based system	215
Table 7-10: Percentage decreased of the MAGSeM-based system for T3	215
Table 7-11: TT for MAGSeM-based system	217
Table 7-12: TT for Socket-based system.....	217
Table 7-13: Percentage decreased of the MAGSeM-based system for TT	217
Table 7-14: TransacT for MAGSeM-based system	219
Table 7-15: Transact for Socket-based system.....	220
Table 7-16: Percentage decreased of the MAGSeM-based system for TransacT.....	220

Table 7-17: TransacT values in ms for 7 Mb (MAgSeM-based)	220
Table 7-18: TransacT values in ms for 7 Mb (Socket-based)	220
Table 7-19: PSO for 7Mb communications (MAgSeM-based).....	221
Table 7-20: PSO for 7Mb communications (Socket-based).....	221
Table 7-21: Time measurements for Ciphertext (MAgSeM-based).....	222
Table 7-22: Time measurements for Ciphertext (Socket-based).....	223
Table 7-23: T1 for MAgSeM-based system.....	225
Table 7-24: T1 for Socket-based system	225
Table 7-25: Percentage decreased of the MAgSeM-based system for T1	226
Table 7-26: T3 for MAgSeM-based system.....	227
Table 7-27: T3 for Socket-based system	227
Table 7-28: Percentage increased of the MAgSeM-based system for T3	228
Table 7-29: TT for MAgSeM-based system	229
Table 7-30: TT for Socket-based system.....	230
Table 7-31: Percentage increase of the MAgSeM-based system for TT.....	230
Table 7-32: TransacT for MAgSeM-based system	232
Table 7-33: TransacT for Socket-based system	232
Table 7-34: Percentage increased of the MAgSeM-based system for TransacT	232
Table 7-35: TransacT values in ms for 200 Kb (MAgSeM-based).....	233
Table 7-36: TransacT values in ms for 200 Kb (Socket-based).....	233
Table 7-37: PSO for 200 Kb communications (MAgSeM-based)	233
Table 7-38: PSO for 200 Kb communications (Socket-based)	233
Table A1: Function <code>SplitString()</code>	246
Table A2: Function <code>encrypt()</code>	248
Table A3: Function <code>saveKey()</code>	250
Table A4: Function <code>encrypting()</code>	251
Table A5: MTA Class.....	252
Table A6: <code>cryptoAgent</code> Class.....	256
Table A7: SUA Class.....	259
Table A8: <code>MobileAgent</code> Class.....	263

Table A9: DA Class.....	268
Table A10: RA Class.....	272
Table A11: receiveMessage Class.....	275
Table A12: sSUA Class.....	280
Table A13: sDA Class.....	283
Table A14: sRA Class.....	287
Table A15: Code.java.....	294

List of Acronyms

ACL	Agent Communication Language
AES	Advanced Encryption Standard
IA	Interface Agent
cA	Crypto Agent
CBC	Cipher-block Chaining Mode
CDC	Connected Device Configuration
CLA	Communication Listener Agent
CLDC	Connected Limited Device Configuration
com_layer	Layer of Communication
DA	Decrypt Agent
DOA	Data Organizer Agent
FIPA	Foundations of Intelligent Physical Agents
FIPA-ACL	FIPA-Agent Communication Language
IPMS	Inter-Platform Mobility Service
J2ME	Java 2 Platform Micro Edition
JCA	Java Cryptography Architecture
JCE	the Java Cryptography Extension
JDK	Java Development Kit
K1	Symmetric key 1 (secret)
K2	Symmetric key 2 (shared)
KQML	Knowledge Query and Manipulation Language
L ₀	Default Layer
MA	Mobile Agent
MAS	Multi Agent Systems
MAgSeM	Multi-agent Security Model
MLC	Multilayer Communication Model
MTA	Multi-tasking Agent
RA	Receiver Agent

SC	System Coordinator
sDA	Specialized DA
sRA	Specialized RA
sSUA	Specialized SUA
SUA	SetUp Agent
SvA	Server Agent
SW	Social Worker