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 online 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 Suther, 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 DEvelopement 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
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 6-33: 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
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 SplitString() .................................................................................................. 246
Table A2: Function encrypt() ..................................................................................................... 248
Table A3: Function saveKey() .................................................................................................. 250
Table A4: Function encrypting() ................................................................................................. 251
Table A5: MTA Class .................................................................................................................. 252
Table A6: cryptoAgent Class ..................................................................................................... 256
Table A7: SUA Class .................................................................................................................. 259
Table A8: MobileAgent 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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Agent Communication Language</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>IA</td>
<td>Interface Agent</td>
</tr>
<tr>
<td>cA</td>
<td>Crypto Agent</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher-block Chaining Mode</td>
</tr>
<tr>
<td>CDC</td>
<td>Connected Device Configuration</td>
</tr>
<tr>
<td>CLA</td>
<td>Communication Listener Agent</td>
</tr>
<tr>
<td>CLDC</td>
<td>Connected Limited Device Configuration</td>
</tr>
<tr>
<td>com_layer</td>
<td>Layer of Communication</td>
</tr>
<tr>
<td>DA</td>
<td>Decrypt Agent</td>
</tr>
<tr>
<td>DOA</td>
<td>Data Organizer Agent</td>
</tr>
<tr>
<td>FIPA</td>
<td>Foundations of Intelligent Physical Agents</td>
</tr>
<tr>
<td>FIPA-ACL</td>
<td>FIPA-Agent Communication Language</td>
</tr>
<tr>
<td>IPMS</td>
<td>Inter-Platform Mobility Service</td>
</tr>
<tr>
<td>J2ME</td>
<td>Java 2 Platform Micro Edition</td>
</tr>
<tr>
<td>JCA</td>
<td>Java Cryptography Architecture</td>
</tr>
<tr>
<td>JCE</td>
<td>the Java Cryptography Extension</td>
</tr>
<tr>
<td>JDK</td>
<td>Java Development Kit</td>
</tr>
<tr>
<td>K1</td>
<td>Symmetric key 1 (secret)</td>
</tr>
<tr>
<td>K2</td>
<td>Symmetric key 2 (shared)</td>
</tr>
<tr>
<td>KQML</td>
<td>Knowledge Query and Manipulation Language</td>
</tr>
<tr>
<td>L₀</td>
<td>Default Layer</td>
</tr>
<tr>
<td>MA</td>
<td>Mobile Agent</td>
</tr>
<tr>
<td>MAS</td>
<td>Multi Agent Systems</td>
</tr>
<tr>
<td>MAgSeM</td>
<td>Multi-agent Security Model</td>
</tr>
<tr>
<td>MLC</td>
<td>Multilayer Communication Model</td>
</tr>
<tr>
<td>MTA</td>
<td>Multi-tasking Agent</td>
</tr>
<tr>
<td>RA</td>
<td>Receiver Agent</td>
</tr>
<tr>
<td>SC</td>
<td>System Coordinator</td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
</tr>
<tr>
<td>sDA</td>
<td>Specialized DA</td>
</tr>
<tr>
<td>sRA</td>
<td>Specialized RA</td>
</tr>
<tr>
<td>sSUA</td>
<td>Specialized SUA</td>
</tr>
<tr>
<td>SUA</td>
<td>SetUp Agent</td>
</tr>
<tr>
<td>SvA</td>
<td>Server Agent</td>
</tr>
<tr>
<td>SW</td>
<td>Social Worker</td>
</tr>
</tbody>
</table>