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

List of Figures

List of Tables

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