CONTROLLED LINK ESTABLISHMENT ATTACKS ON DISTRIBUTED SENSOR NETWORKS AND COUNTERMEASURES

DISSERTATION

Submitted to the University Graduate School
University of Technology, Sydney

In fulfilment of the requirements for the degree of
Doctor of Philosophy in Engineering and Information Technology

BY

THANH DAI TRAN

B.Eng., Hanoi University of Science and Technology, 2005
M.Eng., Kyung Hee University, 2007

Sydney, December 2010

CERTIFICATE OF AUTHORSHIP/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

……

To the memory of my dearest grandmother and grandfather

Abstract

For over a decade, the boom in research, development, and application of distributed sensor networks (DSNs) has enabled their pervasion in many aspects of human life. In such networks, collaboration among sensor nodes plays a key role in resolving distributed tasks. Typically, traditional cryptographic protections such as encryption and authentication are utilised to secure this collaboration against malicious attacks.

Unfortunately, this secured collaboration is undermined by an attack named Controlled Link Establishment Attack (CLEA). To launch CLEA, the attacker first captures and compromises a limited number of nodes to extract their secret information. Next, the attacker repetitively utilises the compromised nodes and secret information to create overwhelming controlled links with legitimate nodes. These controlled links are then used to subvert network-wide cooperative efforts or gain the control of the network.

This thesis comprises two parts: CLEA investigation and development of new countermeasures against CLEA. The investigation involves (i) identifying and characterising CLEA based on the examination of actual instances (ii) undertaking a literature review of existing key establishment schemes for DSNs and pinpointing their vulnerability to CLEA (iii) performing a comprehensive survey of existing countermeasures applicable to defend against CLEA, and (iv) studying the feasibility of CLEA. The conclusion drawn from this investigation is that although CLEA is a real and serious threat, no sufficiently robust and efficient countermeasures have been found in the literature to defeat the attack.

The development starts with a study of related works that can be used as building blocks for new countermeasures followed by their description. The proposed countermeasures can be classified into either protection-based approach or detection-based approach. Following the first approach, three schemes focusing on protecting key establishment schemes by leveraging a cryptographic one-way hash chain are developed. Following the second approach, three schemes are introduced. The first two schemes are capable

of detecting and stamping out CLEA attempts from the beginning. The final scheme is even more powerful than the previous ones with the ability to identify and revoke the source of the attack.

Finally, thorough evaluations of the proposed schemes in respect of security features and performance overheads are carried out through intensive analyses, simulations, implementation, and extensive comparison with other schemes. The findings from these evaluations indicate that the proposed schemes achieve robust and effective prevention, detection, and revocation capability against CLEA with reasonable overheads. In comparison, the protection-based schemes are more performance efficient but less security effective than the detection-based schemes. They are all suitable for use in the current generation of sensor nodes.

Acknowledgements

A major research project like this is never entirely the work of the author. Over my doctoral candidature, I have been receiving support and encouragement from different people in various ways. My thesis would not have been completed without these support and encouragement.

First and foremost, I wish to express my deepest gratitude towards my supervisor, Dr. Johnson Agbinya, who has been my supervisor since the beginning of my study. Johnson has always been a great mentor and above all good friend, giving me tremendously valuable suggestions, thoughtful guidance, and continuous support. His excellent ideas and feedback from numerous face-to-face discussions and group meetings have assisted me in selecting my thesis topic, formulating research questions, developing new methodology for these questions, publishing my work, and completing this thesis. His research expertise and community network as well as his financing for my publications and conference attendance have been very helpful. His dedication to research and vastness of knowledge have set a standard I long to meet for the years to come. It is my great honour to receive his guidance and direction towards the accomplishment of this dissertation.

My sincere thanks are extended to my co-supervisor, Dr. Adel Ali Al-Jumaily and my previous co-supervisor, A/Prof. Elaine Lawrence, for their advice and support throughout my thesis.

I am indebted to the Faculty of Engineering and Information Technology (FEIT), UTS in general and Prof. Hung Nguyen in particular for having offered me a Faculty of Engineering Postgraduate Research Scholarship. Without this scholarship, my dream of studying in Australia would not have been fulfilled. I would like to extend further my thanks to the Vice Chancellor's Conference Funding and FEIT Travel Funding committees for their generous financial support of my conference trips.

My keen appreciation goes to Ms. Phyllis Agius, Research Administration Officer, for her dedicated assistance. She has always been my first point of contact whenever I had difficulties with paperwork and administrative details.

Moving toward more personal acknowledgments, I owe special gratitude to my closest friend Richard Turnell for his true companionship, unwavering support, and warm encouragement. He has made me feel at home and devoted countless hours to improving my English skills, proofreading my paper drafts, teaching me how to drive cars, and above all helping me absorb and value Australian culture. He has been my point of reference for difficulties I faced in my daily life and acted as my main source of hilarity, vitality, and exhilaration. Without his effort, I would not have concentrated on my study and finished it on time.

My heartfelt gratitude towards my beloved fiancee, Giang, cannot be expressed in words. Her eternal love, understanding, and sharing are always a powerful source of inspiration and energy for my study. She has helped me keep balance in my mind and fetched me happiness in life when I lost track of my research and felt disappointed and stressed. I do not hesitate to say that, with her by my side, I am not alone on this so-called ‘lonely journey’.

Last, but most important, is the dedication of this thesis to my dearest parents and younger sister for their never-ending love, unconditional support, and tireless sacrifices. It is no exaggeration to say that I am very lucky to have such marvellous family members. I hope they will read this work some day and be proud of me.

Table of Contents

List of Figures

List of Tables