UNIVERSITI PUTRA MALAYSIA

AN INTRUSION TOLERANT SYSTEM ARCHITECTURE FOR SECURE AND SELF-HEALING SMART GRID CONTROL CENTERS

MARYAM TANHA

FK 2013 44

AN INTRUSION TOLERANT SYSTEM ARCHITECTURE FOR SECURE AND SELF-HEALING SMART GRID CONTROL CENTERS

By

MARYAM TANHA

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

October 2013

DEDICATIONS

This thesis is dedicated to:

My dearest husband, Dawood, for his whole-hearted and substantial support

And

My caring and devoted parents for their unconditional love and support

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science.

AN INTRUSION TOLERANT SYSTEM ARCHITECTURE FOR SECURE AND SELF-HEALING SMART GRID CONTROL CENTERS

BY

MARYAM TANHA

October 2013

Chair: Fazirulhisyam Hashim, PhD
Faculty: Engineering

The ever-increasing, novel and sophisticated cyber threats underscore the need for more robust and resilient security approaches. The situation would be further aggravated due to the dependence of many critical infrastructures on information and communication technology. Critical infrastructures require automatic response and self-healing capabilities to handle multifarious malicious attacks while remaining survivable and secure. The cyber security is of great importance for critical infrastructures due to far-reaching societal and economic impacts caused by failure or malfunction of their key components (in particular, control centers) resulting from malicious attacks on the communication infrastructure. Unfortunately, conventional security mechanisms, namely prevention and detection systems have limitations to suffice for the crucial operation of critical infrastructures such as smart grid. For this reason, a new security paradigm referred to as intrusion tolerance needs to be incorporated into critical infrastructures. The intrusion tolerance is envisaged to complement the existing security solutions, as well as to provide availability (as the top security priority) and self-healing capabilities for control centers of critical infrastructures. However, intrusion tolerance techniques are associated with substantial cost. This dissertation proposes an intrusion tolerant system architecture which incorporates distinctive features, namely hybrid and hierarchical rejuvenation mechanism as well as dynamic redundancy level. The aforementioned characteristics are formulated in such a way to decrease the incurred intrusion tolerance cost while improving security. The security of the proposed architecture is analytically evaluated, and the acquired results show improvements compared to two established intrusion tolerant system architectures. The incurred cost in terms of overhead is also analyzed, and the outcomes demonstrate the cost-effectiveness of the proposed architecture.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

SATU SENI BINA PENCEROBOHAN TOLERAN SISTEM UNTUK KE SELAMAT DAN PEMULIHAN DIRI PINTAR PUSAT KAWALAN GRID

OLEH

MARYYAM TANHA

Oktober 2013

Pengerusi: Fazirulhisyam Hashim, PhD
Fakulti: Kejuruteraan

Ancaman siber yang semakin meningkat, baru dan canggih menekankan keperluan bagi kaedah keselamatan yang lebih kukuh dan berdaya tahan. Keadaan ini akan menjadi lebih teruk akibat kebergantungan banyak infrastruktur kritikal kepada teknologi maklumat dan komunikasi. Infrastruktur kritikal memerlukan tindak balas automatik dan keupayaan pemulihan diri untuk menangani pelbagai serangan berniat jahat manakala mengekalkah keupayaan hidup dan selamat. Keselamatan siber adalah amat penting untuk infrastruktur kritikal kerana kesan sosial dan ekonomi yang meluas disebabkan oleh kegagalan atau kerosakan komponen utama mereka (khususnya, pusat kawalan) akibat daripada serangan berniat jahat ke atas infrastruktur komunikasi. Malangnya, mekanisme keselamatan konvensional, iaitu sistem pencegahan dan pengesanan mempunyai had untuk mencukupi dalam operasi penting infrastruktur kritikal seperti grid pintar. Berdasarkan sebab ini, satu paradigma keselamatan baru yang merujuk kepada toleransi pencerobohan perlu dimasukkan ke dalam infrastruktur kritikal. Toleransi pencerobohan dijangka akan melengkapkan penyelesaian keselamatan yang sedia ada, serta menyediakan ketersediaan (sebagai keutamaan keselamatan tertinggi) dan keupayaan pemulihan diri untuk pusat kawalan infrastruktur kritikal. Walaubagaimanapun, teknik toleransi pencerobohan dikaitkan dengan kos yang besar. Disertasi ini mencadangkan satu seni bina sistem toleran pencerobohan yang menggabungkan pelbagai ciri yang tersendiri, iaitu mekanisme rejuvenasi hibrid dan hierarki serta tahap lebihan dinamik. Ciri yang disebutkan di atas dirumuskan dengan cara sedemikian untuk mengurangkan kos pencerobohan toleransi tertanggung disamping meningkatkan keselamatan. Keselamatan bagi seni bina yang dicadangkan dinilai secara analitikal, dan keputusan yang diperolehi menunjukkan peningkatan apabila dibandingkan dengan dua seni bina sistem toleran pencerobohan yang sedia ada. Kos yang ditanggung dari segi overhed juga

dianalisis, dan hasil menunjukkan keberkesanan seni bina yang dicadangkan.

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor, Dr. Fazirulhisyam Hashim for his generous support and great encouragement to conduct this research as well as his valuable comments to enhance the quality of the dissertation.

Also, I am very grateful to the members of my supervisory committee, Associate Professor Dr. Shamala K. Subramaniam and Dr. Khairulmizam b.Samsudin for their help and support to achieve my research dissertation.

I certify that a Thesis Examination Committee has met on 4 October 2013 to conduct the final examination of Maryam Tanha on her thesis entitled "AN INTRUSION-TOLERANT SYSTEM ARCHITECTURE FOR SECURE AND SELF-HEALING SMART GRID CONTROL CENTERS" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Alyani binti Ismail, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abd. Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mohd Zainal Abidin bin Ab. Kadir, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Tiong Sieh Kiong, PhD
Associate Professor Ir.
Universiti Tenaga Nasional Malaysia
(External Examiner)

NORITAH OMAR, PhD
Associate Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 19 December 2013

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Fazirulhisyam Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairperson)

Shamala K. Subramaniam, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Khairulmizam b.Samsudin, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institution.

MARYAM TANHA
Date: 4 October 2013

TABLE OF CONTENTS