2010

Network attacks and securing streaming content

Liang Lu
University of Wollongong

Network Attacks and Securing Streaming Content

A thesis submitted in fulfillment of the
requirements for the award of the degree

Doctor of Philosophy

from

UNIVERSITY OF WOLLONGONG

by

Liang Lu

School of Computer Science and Software Engineering
July 2010

Dedicated to
My mother and my father

Declaration

This is to certify that the work reported in this thesis was done by the author, unless specified otherwise, and that no part of it has been submitted in a thesis to any other university or similar institution.

Liang Lu
July 22, 2010

Abstract

Despite many years of effort by the industry as well as the research community, attacks on computer systems via access networks are still a severe threat. In the battle against network attacks, firewalls and Intrusion Detection Systems (IDSs) have played one of the most important roles. However, conventional firewalls and IDSs have technical limitations and as such have difficulties dealing with emerging network applications, a notable example of which being streaming content. Besides, configuring firewall rule tables for large networks with complex security requirements is a difficult and error prone task.

In this thesis, we study the behavior of streaming content applications and look into techniques for enhancing firewalls/IDSs capabilities to cater for this new network application requirement. To assist system administrators to correctly implement organisational policies, we also develop a method of representing a firewall rule table that allows comparison of two tables, and provide an algorithm that determines if two tables are equivalent.

Even enhanced with techniques we provided, conventional firewalls/IDSs themselves still have difficulties dealing with complicated network threats and challenges. A notable example is multi-stage attacks where each stage itself does not violate security policy and is not detected by firewalls/IDSs.

A new mechanism, namely attack graphs, has emerged to model and defend against multi-stage attacks. However like any other new technologies, attack graphs have technical limitations such as sizing or scaling issues. In this thesis, we present our contribution to the area of ranking attack graphs. Our contribution lies in two major areas: accurate ranking of attack graphs, and efficient ranking by an artificial intelligence approach.

Acknowledgement

My experience as a graduate student in the University of Wollongong has been wonderful. I am grateful to my principal supervisor Prof. Rei Safavi-Naini for this opportunity. Rei has been an excellent supervisor who has offered me directions and yet enough freedom for me to explore different areas. I would like to express my gratitude to my co-supervisor Prof. Willy Susilo and Dr. Jeffrey Horton for their guidance. Willy and Jeffrey have always been nice to me.

My sincere thanks to Dr. Markus Hargenbuckner and his artificial intelligence research group for all their support and advice. Their help has been invaluable for my research work on combining techniques in the network security field and artificial intelligence field. Special thanks to S. L. Yong with his valuable comments on much of my work. All the discussions are very helpful in the development of this thesis.

I am fortunate to be here with a team of interesting people. Discussions are always stimulating and rewarding. I have enjoyed discussions with Angela Piper, Noi Rungrat, Xinyi Huang, Mohammad Reza Reyhanitabar, Man Ho Au, Shams Ud Din Qazi, Siamak Fayyaz Shahandashti, etc. The list goes on and on.

I would like to acknowledge the support that I have received from all the academic and general staff in the School of CS & SE from the University of Wollongong, Australia.

Finally, my love and gratitude to my parents and families for their enduring love and support. A special thanks to my beloved girl friend Yi Gao, nicknamed colored-piggy.

Publications

The following papers have been published or presented, and contain materials based on the content of this thesis.

1. Liang Lu, Rei Safavi-Naini, Markus Hagenbuchner, Willy Susilo, Jeffrey Horton, Sweah Liang Yong, Ah Chung Tsoi. Ranking Attack Graphs with Graph Neural Networks. The 5th Information Security Practice and Experience Conference (ISPEC 2009), Lecture Notes in Computer Science 5451, pp. 345 - 359, 2009.

2. Liang Lu, Jeffrey Horton, Rei Safavi-Naini and Willy Susilo. Transport Layer Identification of Skype Traffic. The International Conference on Information Networking (ICOIN 2007), Lecture Notes in Computer Science 5200, Springer-Verlag, pp. 465 - 281, 2008.

3. Liang Lu, Jeffrey Horton, Rei Safavi-Naini and Willy Susilo. An Adversary Aware and Intrusion Detection Aware Attack Model Ranking Scheme. The 5th International Conference on Applied Cryptography and Network Security (ACNS'07), Lecture Notes in Computer Science 4521, Springer-Verlag, pp. 65-86, 2007

4. Liang Lu, Rei Safavi-Naini, Jeff Horton and Willy Susilo. Comparing and Debugging Firewall Rule Tables. IET Information Security, Vol. 1 No. 4, pp. 143 - 151, 2007.

5. Liang Lu, Rei Safavi-Naini, Jeffrey Horton and Willy Susilo. On Securing RTP-Based Streaming Content With Firewalls. The 4th International Conference on Cryptology and Network Security (CANS2005), Lecture Notes in Computer Science 3810, Springer-Verlag, pp. 304 - 319, 2005.

6. Liang Lu, Rei Safavi-Naini and Willy Susilo. Design of Policy Tables For Implementation of Hybrid Distributed Firewalls. Australian Telecommunication Networks and Applications Conference (ATNAC) 2004, pp. 68 - 73, 2004.

Contents

List of Tables

List of Figures