

# University of Wollongong - Research Online

## Thesis Collection

Title: Network attacks and securing streaming content

Author: Liang Lu

Year: 2010

Repository DOI:

### Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

**Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.**

Research Online is the open access repository for the University of Wollongong. For further information contact the UOW Library: [research-pubs@uow.edu.au](mailto:research-pubs@uow.edu.au)

2010

## Network attacks and securing streaming content

Liang Lu  
*University of Wollongong*

Follow this and additional works at: <https://ro.uow.edu.au/theses>

### University of Wollongong

#### Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following: This work is copyright. Apart from any use permitted under the Copyright Act 1968, no part of this work may be reproduced by any process, nor may any other exclusive right be exercised, without the permission of the author. Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material.

Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

Unless otherwise indicated, the views expressed in this thesis are those of the author and do not necessarily represent the views of the University of Wollongong.

---

### Recommended Citation

Lu, Liang, Network attacks and securing streaming content, Doctor of Philosophy thesis, School of Computer Science and Software Engineering - Faculty of Informatics, University of Wollongong, 2010.  
<https://ro.uow.edu.au/theses/3158>

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: [research-pubs@uow.edu.au](mailto:research-pubs@uow.edu.au)

## **NOTE**

This online version of the thesis may have different page formatting and pagination from the paper copy held in the University of Wollongong Library.

## **UNIVERSITY OF WOLLONGONG**

### **COPYRIGHT WARNING**

You may print or download ONE copy of this document for the purpose of your own research or study. The University does not authorise you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site. You are reminded of the following:

Copyright owners are entitled to take legal action against persons who infringe their copyright. A reproduction of material that is protected by copyright may be a copyright infringement. A court may impose penalties and award damages in relation to offences and infringements relating to copyright material. Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.



# 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

© Copyright 2010

by

Liang Lu

All Rights Reserved

*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

---

|  |            |
|--|------------|
| <b>Abstract</b>  | <b>v</b>   |
| <b>Acknowledgement</b>   | <b>vi</b>  |
| <b>Publications</b>  | <b>vii</b> |
| <b>1 Introduction</b>  | <b>1</b>   |
| 1.1 Network Attack and Firewalls . . . . .                                       | 1          |
| 1.2 The Challenge . . . . .  | 2          |
| 1.2.1 Conventional Firewalls . . . . .   | 2          |
| 1.2.2 Modeling Multi-Stage Attacks . . . . .                                     | 4          |
| 1.3 Our Contribution and Thesis Organisation . . . . .                           | 5          |
| <b>2 Preliminaries</b>   | <b>7</b>   |
| 2.1 Streaming Protocols . . . . .  | 8          |
| 2.1.1 Real-Time Streaming Protocol . . . . .                                     | 8          |
| 2.1.2 Session Initiation Protocol . . . . .                                      | 9          |
| 2.1.3 H.323 . . . . .  | 11         |
| 2.1.4 Real Time Transport Protocol . . . . .                                     | 13         |
| 2.2 Other Literature . . . . .   | 15         |
| 2.3 Conclusion . . . . .   | 17         |
| <b>3 Preventing Malicious Streaming Traffic Into A Secured Network</b>           | <b>18</b>  |
| 3.1 Introduction . . . . .   | 18         |
| 3.2 Preliminaries . . . . .  | 19         |
| 3.2.1 Streaming Content Overview . . . . .                                       | 19         |
| 3.2.2 Incapacity of Conventional Firewalls to Handle Streaming Content . . . . . | 20         |

|          |   |           |
|----------|---|-----------|
| 3.3      | Injection of Malicious Traffic . . . . .  | 21        |
| 3.4      | Streaming Content Modelling and the Inspection Scheme . . . . .                       | 23        |
| 3.4.1    | Arrival Process Modelling of Streaming Content . . . . .                              | 23        |
| 3.4.2    | Application of The Central Limit Theorem . . . . .                                    | 25        |
| 3.4.3    | Inspection Scheme . . . . .   | 26        |
| 3.5      | Experiments and Results . . . . .   | 28        |
| 3.5.1    | Experimental Setup . . . . .  | 28        |
| 3.5.2    | Result on Packet Injection . . . . .  | 29        |
| 3.5.3    | Effectiveness of The Inspection Scheme . . . . .                                      | 31        |
| 3.6      | Conclusion . . . . .  | 34        |
| <b>4</b> | <b>Preventing Streaming Traffic From Flowing Out Of A Secured Network</b>             | <b>37</b> |
| 4.1      | Introduction . . . . .  | 37        |
| 4.1.1    | Skype Overview . . . . .  | 39        |
| 4.1.2    | Related work . . . . .  | 40        |
| 4.2      | Payload Based Detection . . . . .   | 41        |
| 4.2.1    | Notations and Preliminaries . . . . .   | 42        |
| 4.2.2    | Simple Signatures . . . . .   | 42        |
| 4.2.3    | Composite Signatures . . . . .  | 43        |
| 4.3      | Characterisation of Skype Traffic . . . . .   | 44        |
| 4.3.1    | Realtime Characteristics . . . . .  | 45        |
| 4.3.2    | Connection patterns . . . . .   | 49        |
| 4.4      | Non-payload Based Detection Technique . . . . .                                       | 51        |
| 4.4.1    | Conventional client-server applications and other peer-to-peer applications . . . . . | 52        |
| 4.4.2    | Realtime applications . . . . .   | 52        |
| 4.4.3    | Final Algorithm . . . . .   | 53        |
| 4.4.4    | Discussions . . . . .   | 54        |
| 4.5      | Implementation and Experiments . . . . .  | 56        |
| 4.5.1    | False-Positive Evaluation . . . . .   | 56        |
| 4.5.2    | False-Negative Evaluation . . . . .   | 57        |
| 4.6      | Conclusion and Further Work . . . . .   | 62        |
| 4.6.1    | A Related Problem . . . . .   | 63        |

|          |  |           |
|----------|--|-----------|
| <b>5</b> | <b>Comparing Firewall Rules</b>  | <b>64</b> |
| 5.1      | Introduction . . . . .   | 64        |
| 5.2      | Related Work . . . . .   | 66        |
| 5.3      | Formally Representing Firewall Rules and Rule Tables . . . . .                               | 68        |
| 5.3.1    | Firewall Rules . . . . .   | 69        |
| 5.3.2    | Firewall Rule Table . . . . .  | 70        |
| 5.3.3    | An Example . . . . .   | 70        |
| 5.4      | Preliminaries . . . . .  | 71        |
| 5.4.1    | An Example . . . . .   | 74        |
| 5.5      | Comparing Firewall Rule Tables . . . . .   | 75        |
| 5.5.1    | Algorithms to Compare Firewall Rule Tables . . . . .   | 78        |
| 5.6      | Implementation and a Complete Example . . . . .  | 79        |
| 5.6.1    | An implementation . . . . .  | 79        |
| 5.6.2    | A Complete Example . . . . .   | 80        |
| 5.7      | Conclusions and Further Work . . . . .   | 82        |
| 5.7.1    | Deficiency of Firewall Techniques and Further Work . . . . .                                 | 84        |
| <b>6</b> | <b>Using Attack Graphs to Analyse Network Security</b>                                       | <b>87</b> |
| 6.1      | Introduction . . . . .   | 87        |
| 6.1.1    | Related Work . . . . .   | 88        |
| 6.1.2    | Our Contribution . . . . .   | 90        |
| 6.2      | Modeling Adversary and Intrusion Detection Capability in Ranking<br>Attack Models . . . . .  | 93        |
| 6.2.1    | Background and Preliminaries . . . . .   | 93        |
| 6.2.2    | Modelling Adversary and Intrusion Detection Capability in<br>Ranking Attack Models . . . . . | 96        |
| 6.2.3    | Web Graph Adjustment . . . . .   | 97        |
| 6.2.4    | Transition Matrix Construction . . . . .   | 99        |
| 6.2.5    | Ranking Attack Models . . . . .  | 100       |
| 6.3      | Implementation and Experiments . . . . .   | 102       |
| 6.3.1    | Implementation . . . . .   | 102       |
| 6.3.2    | The Network Model for Experiments . . . . .  | 104       |
| 6.3.3    | Experimental Results Analysis and Evaluation . . . . .                                       | 118       |
| 6.4      | Ranking Attack Graphs with Graph Neural Network . . . . .                                    | 123       |
| 6.4.1    | Preliminaries . . . . .  | 123       |

|          |   |            |
|----------|---|------------|
| 6.4.2    | Ranking Attack Graph using GNNs . . . . . | 128        |
| 6.4.3    | Experiments and Results . . . . .         | 129        |
| 6.5      | Conclusion . . . . .                      | 135        |
| <b>7</b> | <b>Concluding Remarks</b>                 | <b>140</b> |
| 7.1      | Thesis Contribution . . . . .             | 140        |
| 7.2      | Limitations . . . . .                     | 142        |
| 7.3      | Open Problems . . . . .                   | 142        |
|          | <b>Bibliography</b>                       | <b>144</b> |

# List of Tables

---

|     |   |     |
|-----|---|-----|
| 3.1 | Experimental result under confidence level $\alpha = 0.98$ . . . . .  | 31  |
| 3.2 | Experimental results with confidence level $\alpha = 0.98$ for fast injection .   | 33  |
| 3.3 | Experimental results with confidence level $\alpha = 0.98$ for medium speed<br>injection. Interestingly, this is the case when crafted traffic is injected<br>at a similar rate to that of legal traffic. . . . . | 33  |
| 3.4 | Experimental results with confidence level $\alpha = 0.98$ for slow injection   | 34  |
| 4.1 | Simple Signatures . . . . .   | 43  |
| 4.2 | Composite Signatures . . . . .  | 44  |
| 4.3 | characteristics matrix . . . . .  | 54  |
| 4.4 | OC-48 Traffic Traces . . . . .  | 56  |
| 5.1 | Firewall rule table using both negative and positive rules . . . . .  | 71  |
| 5.2 | Firewall rule table using positive rules only . . . . .   | 71  |
| 5.3 | An example of rule table . . . . .  | 75  |
| 5.4 | Dividing $R_5$ into sub-rules . . . . .   | 75  |
| 5.5 | Another example of rule table . . . . .   | 76  |
| 5.6 | The security policy . . . . .   | 86  |
| 5.7 | The rule table by the chief administrator . . . . .   | 86  |
| 5.8 | The rule table by the assistant administrator . . . . .   | 86  |
| 6.1 | Web Model Notations . . . . .   | 94  |
| 6.2 | Atomic Attacks Modelled in the Sample Network . . . . .   | 138 |
| 6.3 | Connectivity . . . . .  | 139 |
| 6.4 | Trust Relation . . . . .  | 139 |
| 6.5 | Position Pair Coupling Error . . . . .  | 139 |



# List of Figures

---

|      |   |    |
|------|---|----|
| 1.1  | Illustration of that how a firewall works . . . . .   | 2  |
| 2.1  | Typical Protocol Stack of Streaming Applications . . . . .                                      | 15 |
| 3.1  | Experimental Setup . . . . .  | 30 |
| 3.2  | Variation of Packet Arrival Rates: Legal Traffic . . . . .                                      | 32 |
| 3.3  | Variation of Packet Arrival Rates: Legal and Injected Traffic . . . . .                         | 35 |
| 4.1  | An example of composite signature . . . . .   | 44 |
| 4.2  | Packet Size Distribution Diagram . . . . .  | 46 |
| 4.3  | Packet Size Cumulative Density Function . . . . .   | 47 |
| 4.4  | Packet Inter-Arrival Time Cumulative Density Function . . . . .                                 | 48 |
| 4.5  | Packet Inter-Arrival Time Cumulative Density Function Captured at<br>Residential ADSL . . . . . | 49 |
| 4.6  | Bandwidth Burstiness of the start-up 30 seconds . . . . .                                       | 50 |
| 4.7  | Bandwidth Burstiness of 30 minutes . . . . .  | 50 |
| 4.8  | Bandwidth Burstiness Captured Behind Shared ADSL . . . . .                                      | 51 |
| 4.9  | Experimental Setup . . . . .  | 58 |
| 4.10 | Experimental Results Day 1 . . . . .  | 59 |
| 4.11 | Experimental Results Day 2 . . . . .  | 59 |
| 4.12 | Experimental Results Day 3 . . . . .  | 60 |
| 4.13 | Experimental Results Day 4 . . . . .  | 60 |
| 4.14 | Experimental Results Day 5 . . . . .  | 61 |
| 4.15 | Experimental Results Day 6 . . . . .  | 61 |
| 4.16 | Experimental Results Day 7 . . . . .  | 62 |

|      |   |     |
|------|---|-----|
| 5.1  | The Venn Diagram illustrating $R'$ , $R''$ , and $R'''$ . $R'''$ is the set of packet “only” matched by $R$ . Here it is assumed that $R$ has overlap with earlier rules; $R'$ , $R''$ , and $R'''$ may be empty otherwise. . . . . | 73  |
| 5.2  | The Prototype . . . . .   | 80  |
| 5.3  | An example of network setup . . . . .   | 81  |
| 5.4  | Rule table compare result . . . . .   | 82  |
| 5.5  | Rule table compare result . . . . .   | 83  |
| 6.1  | An example of web graph . . . . .   | 95  |
| 6.2  | Transitions in attack models . . . . .  | 99  |
| 6.3  | Toolkit Architecture . . . . .  | 103 |
| 6.4  | Network . . . . .   | 105 |
| 6.5  | Comparison of Ranked Attack Models. (a) The complete ranked attack model (b) Attack Model after fixing up the SSH vulnerability (c) Attack Model after fixing FTP vulnerability . . . . .   | 120 |
| 6.6  | Rank varies with attack probabilities . . . . .   | 121 |
| 6.7  | Rank varies with decaying rate . . . . .  | 121 |
| 6.8  | Rank varies with decaying rate and attack probabilities . . . . .   | 122 |
| 6.9  | An example of a multi-layered perceptron neural network, where $F_1$ , and $F_2$ form the input layer, $F_3$ and $F_4$ form the hidden layer, while $F_5$ forms the output layer. . . . .   | 124 |
| 6.10 | The dependence of state $s_1$ on neighborhood information . . . . .   | 126 |
| 6.11 | The encoding network . . . . .  | 127 |
| 6.12 | Effect of number of training epochs . . . . .   | 132 |
| 6.13 | Relative Position Diagram when trained on real-world attack graphs .  | 134 |
| 6.14 | Effect of number of attack graphs used in the training data set . . . .   | 135 |
| 6.15 | Relative Position Diagram when training on pseudo attack graphs . .   | 136 |