UNIVERSITY OF TECHNOLOGY SYDNEY
Faculty of Engineering and Information Technology

Modeling and Analysis of Advanced Persistent Threats in Cyber Space

by

Xu Wang

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Sydney, Australia

2020

Certificate of Authorship/Originality

I, Xu Wang declare that this thesis, is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney. This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. I certify that the work in this thesis has not been previously submitted for a degree nor has it been submitted as a part of the requirements for other degree except as fully acknowledged within the text. This thesis is the result of a research candidature jointly delivered with Beijing University of Posts and Telecommunications as part of a Collaborative Doctoral Research Degree. This research is supported by the Australian Government Research Training Program.

Production Note:
Signature: Signature removed prior to publication.

Date: 07/01/2020

Dedication

This thesis is dedicated to my parents.

This stands as a testimony for their endless support and love.

To my supervisors, for the academic guidance.

To my friends, for their encouragement.

Acknowledgements

I have to start by thanking my perfect parents Daofeng Wang and Peizhen Zhang. They bring me to this fantastic world, support me to pursue research, allow me to be myself. Many Thanks!

Throughout the doctoral program, I have received a great deal of support and assistance. I would like to express my sincere gratitude to Prof. Y. Jay Guo for his invaluable support and immense knowledge. My deepest thanks also go to Prof. Ren Ping Liu for all the opportunities he offered and his patience and help. I would like to show my very profound gratitude to Dr. Wei Ni in CSIRO. My research would have been impossible without his support and supervision. I would also like to acknowledge Prof. Xinxin Niu and Associate Prof. Kangfeng Zheng in BUPT. I would also like to thank everyone in GBDTC and UTS who helped me so much.

I must express my sincere thanks to my co-author, Xuan Zha, for the company throughout the whole Ph.D. period from China to Australia. A very special gratitude goes out to my mates Bo Song, Guangsheng Yu, Shangjing Lin, Cheng Qin, Li Duan, Shoulu Hou, Ping Yu, Yixun Hu, Yue Shi, Qingyang Liu, Qingyuan Kuang, Heng Liu, Chao Jiang, and Yongjun Song. It is great having the awesome time with you guys. I would like to thank the wonderful colleagues in UDT. I am also grateful to my family and friends who have supported me along the way.

Xu Wang
Sydney, Australia, 2020

List of Publications

Published Journal Papers

J-1. **X. Wang**, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Game Theoretic Suppression of Forged Messages in Online Social Networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019, (Chapter 3).

J-2. **X. Wang**, W. Ni, K. Zheng, R. P. Liu and X. Niu, "Virus Propagation Modeling and Convergence Analysis in Large-scale Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2241-2254, Oct. 2016 (Chapter 4).

J-3. **X. Wang**, B. Song, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Group-based Susceptible-Infectious-Susceptible Model in Large-Scale Directed Networks," *Security and Communication Networks*, vol. 2019, Article ID 1657164, 2019 (Chapter 5).

J-4. **X. Wang**, G. Yu, X. Zha, W. Ni, Y. J. Guo, X. Niu and K. Zheng, "Capacity of Blockchain based Internet-of-Things: Testbed and Analysis," *Elseiver Internet of Things*, vol. 8, 100109, 2019.

J-5. B. Song, **X. Wang**, W. Ni, Y. Song, R. P. Liu, G. Jiang and Y. J. Guo, "Reliability Analysis of Large-Scale Adaptive Weighted Networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 651-665, 2020.

J-6. **X. Wang**, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Survey on Blockchain for Internet of Things," *Computer Communications*, vol. 136, pp. 10-29, 2019.

J-7. X. Zha, W. Ni, **X. Wang**, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "The Impact of Link Duration on the Integrity of Distributed Mobile Networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp.

2240-2255, Sept. 2018.

J-8. X. Zha, **X. Wang**, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Blockchain for IoT: The Tradeoff Between Consistency and Capacity," *Chinese Journal on Internet of Things*, vol.1, no.1, pp.21-33, 2017.

J-9. Y. Hu, K. Zheng, **X. Wang** and Y. Yang. "WORM-HUNTER: A Worm Guard System using Software-defined Networking," *KSII Transactions on Internet and Information Systems*, 11, no. 1, 2017.

J-10. Y. Xu, C. Wu, K. Zheng, **X. Wang**, X. Niu, and T. Lu., "Computing Adaptive Feature Weights with PSO to Improve Android Malware Detection," *Security and Communication Networks*, vol. 2017, Article ID 3284080, 14 pages, 2017.

Published Conference Papers

C-1. **X. Wang**, K. Zheng, X. Niu, B. Wu and C. Wu, "Detection of Command and Control in Advanced Persistent Threat based on Independent Access," *IEEE International Conference on Communications*, 2016, pp. 1-6, (Chapter 6).

C-2. **X. Wang**, Y. Ping, G. Yu, W. Ni, R. P. Liu and Y. J. Guo, "A High-Performance Hybrid Blockchain System for Traceable IoT Applications," *International Conference on Network and System Security*, Springer, Cham, 2019: 721-728.

C-3. **X. Wang**, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Attack and Defence of Ethereum Remote APIs," *IEEE Globecom Workshops*, 2018.

C-4. G. Yu, **X. Wang**, X. Zha, J. A. Zhang and R. P. Liu, "An optimized round-robin scheduling of speakers for peers-to-peers-based byzantine faulty tolerance," *IEEE Globecom Workshops*, 2018.

C-5. X. Zha, **X. Wang**, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Analytic model on data security in VANETs," *International Symposium on Communications and Information Technologies (ISCIT)*, Cairns, QLD, 2017, pp. 1-6.

Patents

P-1. R. P. Liu, **X. Wang**, G. Yu, J. Baird, "A Machine Type Communication System or Device for Recording Supply Chain Information on a Distributed Ledger in a Peer to Peer Network," 2019901683, filed on 17 May 2019..

P-2. **X. Wang**, R. P. Liu, X. Zha, G. Yu, "Secure image capture and storage on blockchain," 2019903089, filed on 23 Aug 2019.

ABSTRACT

Modeling and Analysis of Advanced Persistent Threats in Cyber Space

by

Xu Wang

Advanced Persistent Threat (APT), a professional cyber threat as indicated by its name, has become a type of significant risk in modern society. APT attackers employ various advanced attack technologies to carry out attacks in multiple stages over a long period of time. Due to its complexity, APT research is challenging and incomplete. This thesis proposes a series of models to analyze key processes of APT, i.e., social attack, propagation, and remote control. To be specific, game theoretic models are proposed to describe social network attacks, and epidemic models based on the susceptible-infected-susceptible process are developed to capture the propagation process; machine learning methods are adopted to detect the remote control traffic.

The main contributions of this thesis can be summarized as follows.

- This thesis proposes infinitely repeated games to capture the interactions between a message publisher and the administrator to suppress social attack messages. Critical conditions, under which the publisher can be disincentivized to send any attack messages, are identified. Closed-form expressions are established to give the maximum number of attack messages from an attacker in the absence or presence of misclassification on genuine messages.
- This thesis proposes a new approach to model the propagation of APT across non-trivial networks. A discrete-time absorbing Markov process of epidemic model is first developed based on the adjacency matrix of the network. Asymptotically accurate bounds of the virus extinction rate are derived. We propose

a practical approach for the estimation of the extinction rate in large networks. Our proposal has been proved theoretically and validated via simulations.

- This thesis proposes a group-based propagation model to analyze the propagation process of APT in large-scale networks. The proposed model is efficient and accurate. The network nodes are divided into groups according to their connectivity. A continuous-time Markov susceptible-infectious-susceptible model is developed. The propagation threshold, under which the propagation will eventually stop, is derived based on the spectral radius of the collapsed adjacency matrix. Simulation results validate the model accuracy and the analytical epidemic threshold.

- This thesis proposes a method of traffic feature analysis to detect the remote control traffic of APT. Based on the independent access feature of APT network traffic, concurrent domains in the domain name service are selected to detect APT domains from domain name system records. The proposed traffic features and detection process are then validated using public datasets.

Contents

List of Figures

List of Tables

Abbreviation

AN : Average Number

APT : Advanced Persistent Threat

CIA : Confidentiality, Integrity and Availability

CODD : Concurrent Domains in DNS Records

CPU : Central Processing Unit

DDoS : Distributed Denial of Service

DNS : Domain Name System

HC : Highest Confidence

HTTP : HyperText Transfer Protocol

HTTPS : HyperText Transfer Protocol Secure

IoT : Internet of Things

IP : Internet Protocol

IRC : Internet Relay Chat

LANL : Los Alamos National Laboratory

OSN : Online Social Network

P2P : Peer-to-peer

SI : Susceptible-Infected

SIR : Susceptible-Infected-Recover

SIS : Susceptible-Infected-Susceptible

SLD: Second-Level Domain

TCP : Transmission Control Protocol

TTL : Time to Live

URL : Uniform Resource Locator