Hindawi
Security and Communication Networks
Volume 2018, Article ID 6545314, 2 pages
https://doi.org/10.1155/2018/6545314

Editorial

Security Measurements of Cyber Networks

Zheng Yan,[1,2] **Yuqing Zhang**,[3] **Kim-Kwang Raymond Choo**,[4] **and Yang Xiang**[5]

[1]*The State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China*
[2]*The Department of Communications and Networking, Aalto University, Espoo, Finland*
[3]*School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing, China*
[4]*Department of Information Systems and Cyber Security, University of Texas at San Antonio, TX 78249, USA*
[5]*School of Software and Electrical Engineering, Swinburne University of Technology, Hawthorn, Australia*

Correspondence should be addressed to Zheng Yan; zheng.yan@aalto.fi

Received 7 May 2018; Accepted 7 May 2018; Published 10 October 2018

Cyber networks facilitate and expedite the development of information systems, communication technologies, and digital economies. However, as the cyber networks become large, heterogeneous, and pluralistic, evaluating the security of cyber networks becomes increasingly challenging. Successful attacks and intrusions against cyber networks can result in significant impacts, ranging from personal risk to national-level security. Thus, there is an increasing need to understand and measure network security by considering a range of requirements and standards, and in the context of different network scenarios. Although many prior studies have focused on network intrusion detection, malware detection, and security threat defense, a generally accepted security measurement framework is still lacking. Such a framework is urgently required for quick identification of security holes, assessment of potential threats, and implementation of efficient countermeasures.

Security measurement theories and methods concern several pertinent questions in terms of security-related data collection, composition, analytics, and processing. This is especially crucial for detecting security threats and measuring cyber network security in a quantified, precise, and efficient manner. (i) How can we adaptively collect related data for security measurement for large-scale heterogeneous networks in a generic and pervasive way? (ii) How can we compose and fuse collected big data without incurring expensive data storage and transmission costs, as well as ensuring efficient data processing to facilitate precise security threat detection and judgment? (iii) How can we protect valuable data, preserve data privacy, and effectively control access to key data, as well as manage its storage? (iv) How can we aggregate and mine security-related data to measure the security of the whole network in a quantifiable manner and with high trustworthiness? These open and interesting issues are now attracting attention from both the research community and the practitioner community.

This special issue brings together recent advances on security-related data processing and analytics, detection of malware, virus and network intrusion, and network system protection, in the context of network security assessment and measurement. We selected 11 research papers from more than 30 submissions after rigorous peer-reviews. Next, we categorize these 11 accepted papers into three categories and briefly discuss each paper.

1. Intrusion Detection and Network Security Measurement

In the survey entitled "Data Fusion for Network Intrusion Detection: A Review", G. Li et al. conducted a comprehensive review on massively high dimensional data fusion techniques for network intrusion detection in order to accurately detect complex or synthetic network attacks.

Based on attack prediction, L. Yin et al. proposed a method of security measurement in their paper entitled "Security Measurement for Unknown Threats Based on Attack Preferences". They computed optimal attack timing

from the perspective of attackers. They used a long-term game to estimate the risk of being found in terms of choosing optimal timing according to risk and profit. On the basis of game theoretical analysis, the likelihood of being attacked for each node is estimated as a security metric result.

Z. Liu et al. attempted to build a malicious domains detection model oriented to imbalanced data. They proposed an imbalanced malicious domain detection method based on passive DNS traffic analysis in the paper entitled "An Imbalanced Malicious Domains Detection Method Based on Passive DNS Traffic Analysis". It can deal with not only between-class imbalance problem but also within-class imbalance problem.

In the paper entitled "Uncovering Tor: An Examination of the Network Structure", B. Monk et al. used social network analysis to examine hyperlink connections and the structure of website communities they form on Tor and how characteristics of these communities could have implications for criminal activity on Tor as understood through the lens of social disorganization theory.

In the paper entitled "An Approach for Internal Network Security Metric Based on Attack Probability", C. Shan et al. proposed an internal network security metric based on attack probability. It simplifies network attack graph for a large-scale network and assists network security detection.

2. Software Fault Location and Maintenance

In the paper entitled "Security Feature Measurement for Frequent Dynamic Execution Paths in Software System", Q. Wang et al. proposed a security feature measurement algorithm of frequent dynamic execution paths in software to provide a basis for improving the security and reliability of software. By using a complex network model and a sequence model and combining them with the invocation and dependency relationships between function nodes, the authors can analyze fault cumulative effect and spread effect. The function node security features of the software complex network are also defined and measured. In addition, frequent software execution paths are mined and weighted in order to obtain security metrics of the frequent paths.

For understanding software design patterns and controlling their development and maintenance process, H. He et al. proposed an approach to define node importance for mining influential software nodes based on invoking dependency relationships among the nodes in the paper entitled "Analysis on Influential Functions in the Weighted Software Network". The authors constructed a weighted software network to represent software execution dependency structure and proposed an algorithm to evaluate node importance to further obtain the most influential nodes in the software network based on it.

In the paper entitled "OFFDTAN: A New Approach of Offline Dynamic Taint Analysis for Binaries", X. Wang et al. proposed an approach to offline dynamic taint analysis for binaries through four stages: dynamic information acquisition, vulnerability modeling, offline analysis, and backtrace analysis.

3. Network Security Countermeasures

In the paper entitled "A Dynamic Hidden Forwarding Path Planning Method Based on Improved Q-Learning in SDN Environments", Y. Chen et al. proposed an improved Q-learning algorithm to automatically plan an optimal attack path. They adopted Software-Defined Network (SDN) to adjust routing paths and dynamically create hidden forwarding paths to filter vicious attack requests.

F. Shan et al. proposed a hybrid access control model (HAC) that leverages attributes and relationships to control access to resources in the paper entitled "HAC: Hybrid Access Control for Online Social Networks". They designed a new policy specification language to express both the relationships and attributes of users and proposed a path checking algorithm to figure out if a path between two users can satisfy with a hybrid policy.

H. Wang et al. studied graphical password (GPW) used in information communications in the paper entitled "A New Type of Graphical Passwords Based on Odd-Elegant Labelled Graphs". The authors designed new Topsnut-GPWs by means of a graph labelling, called odd-elegant labelling. The new Topsnut-GPWs are constructed using Topsnut-GPWs (a type of GPWs) with smaller vertex numbers and more robust to deciphering attacks, compared with traditional Topsnut-GPWs.

4. Summary

Editing this special issue has been an invaluable experience for us. We hope this special issue will provide a useful reference to its readers and contribute to advances in network security, as well as stimulate additional innovation.

Acknowledgments

This work is sponsored by the National Key Research and Development Program of China (Grant 2016YFB0800700), the NSFC (Grants 61672410 and U1536202), the Project Supported by Natural Science Basic Research Plan in Shaanxi Province of China (Program no. 2016ZDJC-06), and the 111 project (Grants B08038 and B16037). We would like to express our appreciation to all authors for their contributions and the reviewers for their valuable review comments. We also sincerely thank the Editorial Board of ***Security and Communication Networks*** for approving this special issue and their continuous support on its final publication.

Zheng Yan
Yuqing Zhang
Kim-Kwang Raymond Choo
Yang Xiang