World Wide Web (2020) 23:951–957
https://doi.org/10.1007/s11280-019-00704-x

Editorial: Special issue on security and privacy in network computing

Hua Wang [1,2] · Yongzhi Wang [3] · Tarek Taleb [4] · Xiaohong Jiang [5]

Published online: 25 July 2019

1 Introduction

Computer networks have revolutionized traditional computing architectures and created a wide range of network computing paradigms, including blockchain [1], distributed computing [11], cloud computing [9], Web services [2], Internet of Things [4, 10], crowdsourcing [9], etc. Such a class of paradigms is able to integrate heterogeneous resources provided from different parties, largely extends the computation capacity and empowers a variety of novel use cases and applications.

However, the diversity of network technologies and the complex protocols used among computing parties might contain security loopholes, which could be abused by benign users or malicious attackers unintentionally or on purpose, thus compromising the integrity, confidentiality and availability of the computation [7]. Security incidents happened in practical systems repeatedly revealed such threats, creating financial loss and social upsets. On the other hand, the diversity and the unique characteristics of network computing paradigms make a silver bullet for the general solution difficult to seek. Therefore, securing network computing is urgent and challenging, calling for non-trivial collective efforts from multiple parties, including

✉ Xiaohong Jiang
jiang@fun.ac.jp

Hua Wang
hua.wang@vu.edu.au

Yongzhi Wang
yzwang@xidian.edu.cn

Tarek Taleb
tarik.taleb@aalto.fi

[1] Nanjing University of Information Science & Technology, Nanjing, China

[2] Institute for Sustainable Industries & Liveable Cities, Victoria University, Footscray, Australia

[3] Xidian University, Xi'an, China

[4] School of Electrical Engineering, Aalto University, Espoo, Finland

[5] Future University Hakodate, Hakodate, Japan

researchers, practitioners, service providers and users, with a common objective to building multi-layered defense line that covers both technical and social aspects [8].

Computer networks, such as the Internet, have been quickly growing. A huge number of users including both human being and industry companies from around the world are accessing these networks for various business and personal events [5]. As a result, computer networks such as the Internet have become a virtual community where companies and individuals communicate with each other by sending and receiving electronic, Voice and image messages. These communications may include personal and business messages, expressing opinions and ideas. In response to this network activity, companies attempt to identify and track individual users for numerous purposes, such as advertising, market research, customizing information, Snooping and eavesdropping, fraud and malicious activities. The attempts are threats to users since users' personal information and their activities can be disclosed without the user's consent or knowledge.

Network privacy involves the right or usage of personal information concerning the storing, purposing, disclosing to third parties, and displaying of the information to someone through networks. Network privacy is a subset of data privacy. Privacy issues have been investigated from the beginnings of large-scale computer sharing [6]. Privacy can entail either personally identifying information or non-private information such as locations have been visited or which website was viewed. Personal information refers to the information that can be used to identify an individual. For example, age and physical address alone could identify who an individual is without explicitly disclosing their name. Network privacy is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences. Network privacy and anonymity are paramount to users, especially as online business application continues to receive attentions. Privacy violations and threat risks are standard considerations for any website under development.

To date, lots of research attention to security and privacy of network computing have been drawn from many players, including device manufacturers, service providers and consumers. This special issue is dedicated to security and privacy issues of network computing, and is intended to gather the latest technology learned, social efforts and contributions from industrial practitioners, academia researchers and governments to advance the state of the art, improve the security and privacy, and develop novel security and privacy architectures, system protocols, software mechanisms, and standards.

2 Submissions

A total of 23 research papers were submitted to the special issue for consideration, 15 submissions from the total 23 papers were nominated from the International Conference on Networking and Network Applications (Nana2018). The submissions are from various countries and areas: India, China, Australia, Japan, Vietnam and Taiwan. Each paper was reviewed by at least three reviewers. Finally, 5 submissions were accepted as full papers after a rigorous review process and a couple of rounds revisions (with an acceptance rate of 21.7% approximately). The selection process also took into account the topics of the submissions, with an intention to cover the scope as much as possible. The research papers cover the areas of network data analysis, artificial intelligence, data mining, big data processing, outsourcing, event detection, encryption algorithms, IOT, Fine-grained Access Control, and hardware environments. In the following, we will highlight the contributions of each paper.

The first paper "MALDC: A Depth Detection Method for Malicious Behavior Based on Behavior Chains" authored by Hao Zhang, Wenjun Zhang, zhihan lv, Arun Kumar Sangaiah, Tao Huang and Naveen Chilamkurti is a behavior based detection method for malicious cybersecurity attack. Current intrusion detection systems are primarily based on single-point monitoring and detection and cannot detect attack modes with a hidden attack frequency. The idea presented in this paper is the incorporation of API call sequence software into the analysis and the construction of behavior chains to express the behavior patterns in software. A novel idea of the idea is the behavior patterns applied into the security design. The paper has definitions of behavioral points and behaviors and proposes a depth-detection method for malware based on behavior chains (MALDC). The method monitors behavior points based on API calls and then uses the calling sequence of those behavior points at runtime to construct a behavior chain. Depth detection methods are developed to detect malicious behavior from the behavior chains. The performance of the proposed method is well evaluated. The authors conducted a large experiment on 54,324 malware and 53,361 benign samples collected from Windows systems and used those samples to train and test the model. As a result, the behavior points extracted based on the above method and the constructed behavior chains are verified and can be used to recognize malicious behavior at a high recognition rate. The method achieved an accuracy of 98.64% with a false positive rate of less than 2% in the best case.

Malicious behavior detection methods have two main directions: static behavior detection and dynamic analysis detection. In the beginning, malware detection efforts employed static analyses, and static behavior detection has been the main technique used in code analysis to acquire information concerning software behavior. The limitation of the static methods are that they are unable to detect files with techniques of packing or reverse decompression. On the other hand, dynamic behavior analysis works while a software is actually running, capturing its behavior for analysis. The approach can effectively address problems that cannot be solved by static detection methods. With dynamic behavior analysis, this paper analyzes an API call sequence and how to perform feature extraction and implement detection methods for malicious behavior.

The main contribution of this paper is a method for constructing behavior chains based on malicious behavior and their use in a detection method. To build a behavior chain in a dynamic environment, a malicious behavior in a running process is analysed. Based on the analysis, the behavior and its features are extracted for a corresponding behavior chain that are used for malicious behavior detection.

The second paper "An Incentive Mechanism with Bid Privacy Protection on Multi-bid Crowdsourced Spectrum Sensing" authored by Xuewen Dong, Guangxia Li, Tao Zhang, Di Lu, Yulong Shen and Jianfeng Ma, that is about privacy preserving in crowdsourced environment. Crowdsourced spectrum sensing (CSS) has been recognised as an excellent technique to increase spectrum utilization and enhance spectrum service. To improve the participation of mobile users, some auction-based mechanisms have been proposed for crowdsourced spectrum sensing system. However, both multi-bid crowdsourced spectrum sensing and the bid privacy of participants in it have never been taken into consideration in those mechanisms. This paper has designed a mechanism to protect the bid privacy in spectrum-sensing participants selecting process in multi-bid CSS system. With different objectives of administrators, two methods are analysed to minimize social costs and maximize average costs of winners. The developed two methods can simultaneously achieve differential bid privacy and truthfulness through theoretical analysis and simulations.

In crowdsourced spectrum sensing field, incentive mechanisms aim to keep the participants' accurate locations secret while taking part in the spectrum-sensing tasks. However, none of them consider protecting the bid privacy in a multi-bid scenario, in which a participant (mobile user) may offer several bids for different sensing task sets. This paper proposes two novel spectrum sensing mechanisms with a differential bid privacy-preserving manner that cannot be achieved by traditional auction-based CSS mechanisms. Authors model a multi-bid crowdsourced sensing system with spectrum administration platform and mobile users that can offer multiple bids for crowdsourced sensing tasks. It is assumed that n participants located in a large region and each participant is identified with a unique index in $\mathrm{N} = \{1; \ldots; \mathrm{n}\}$. Both differential bid privacy and truthfulness of the designed mechanisms are analysed and evaluated with a high valued performance.

The major contribution of this paper is to design an incentive mechanism in a multi-bid CSS system, while achieving truthfulness and differential bid privacy. To address the participant selection problem, a CSS system with two different objectives is analysed. One objective is to minimize the social costs while the other one is to maximize the average efficiency of winners.

The third paper discusses WiFi security in wireless network. In our daily file, WiFi is a compulsory facility but it also brings security risks. WiFi security combines physical layer (PHY) layer authentication information and the security mechanism of the PHY layer has become a hot topic in WiFi security research. The PHY layer contains rich information on wireless channels, such as equipment locations and signal quality. The challenges of improving WiFi security have already attract researchers and many advanced skills are applied such as Received Signal Strength (RSS), Channel Impulse Response (CIR), Channel State Information CIS. High performance WiFi verification that supports PHY layer programming has become an indispensable tool for WiFi security research. This paper designs and implements a verification platform named TickSEC that supports the security authentication at PHY layer. It supports real-time acquisition of PHY layer information, and offers the programmability within the PHY layer. Experimental results show that TickSEC can meet the requirements of PHY layer authentication verification.

This paper presents a platform for using PHY layer information to verify security authentication. The results from evaluation show that TickSEC is efficient and effective in extracting PHY layer information. It provides a variety of common PHY layer information under the premise of low resource consumption and low impact on performance. The case study demonstrates TickSEC's value in practical security authentication. To achieve the outcomes, machine learning approaches are applied. More details, please see "A SDR-based Verification Platform for 802.11 PHY Layer Security Authentication" authored by Xiaoguang Li et al.

The contributions of the paper are the design and implementation of the TickSEC platform that supports PHY layer security authentication. Different from commercial network cards, it can obtain PHY layer information in real time while providing programmability, convenient for PHY layer security verification. As a case study, an approach for identifying different WiFi devices using PHY layer information is proposed.

The fourth paper analyses keyword search on encrypted data with enhanced fine-grained access control in cloud service environments. Cloud service is very popular for organisations and individuals since flexibility, cost savings and no limitations of locations. Owners are increasingly inclined to store lots of data in the cloud as the convenience. The data includes files, photos, e-gift cards, travel documents and so on. However, some uploaded data files are sensitive, for example, electrical health data from patients that are vulnerable by attackers who could make profits from these private data. Hence, data privacy-preserving currently becomes a barrier to wide adoption of cloud storage platform. Encryption algorithms are usually an option to solve the problem. However, if data are encrypted and stored in cloud servers, users are difficult to retrieve the files without decryption and download the files. This option will lead a huge waste of resources of computation and bandwidth. To address this problem, the searchable encryption (SE) techniques come into play, which is a promising tool to retrieve encrypted data and gains growing interests both in academia and industrial field. Keyword-based SE is well acknowledged as a major approach.

Public-key encryption with keyword search is regarded as an important approach for the searchable encryption technique. There are still several privacy leakage challenges for the further adoption of these major schemes. One is how to resist the keyword guessing attack which still leaks data user's keywords privacy. Another is how to construct the access control policy to prevent illegal access of outsourced data sharing since illegal access always leak the privacy of user's attribute. Traditional access models, such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role Based Access Control (RBAC), are fundamentally inadequate. The first reason is that privacy policies are concerned with which data object is used for which purpose(s), while traditional access control models focus on which user is performing which action on which data object. Another difficulty is how to make the access control technology in a trustworthy fashion, when the data provider and the requester are unknown to each other [3].

This paper presents a novel secure keyword index to resist the keyword guessing attack from access pattern and search pattern. After that, it proposes an attribute-based encryption scheme which supports an enhanced fine-grained access control search. This allows the authenticated users to access different data although their searching request contains the same queried keywords, and meanwhile unauthenticated users cannot get any attribute privacy information. Security proofs have shown that the construction of keyword index is against keyword guessing attack from the access pattern and search pattern. The paper has theoretical analyses and experimental results to demonstrate the efficiency of the scheme. Details of the research work, please find at "Privacy-Preserving Conjunctive Keyword Search on Encrypted Data with Enhanced Fine-grained Access Control" authored by Qiang Cao et al.

The last paper is about Internet-of-Things (IOT) Hardware security research work. Paper "A PUF-based Unified Identity Verification Framework for Secure IoT Hardware via Device Authentication" authored by Zhao Huang and Quan Wang, presents a novel system-level device identity verification framework to resist the theft attacks which may not compromise the chip-level unique identification mechanisms. The proposed framework is on the basis of physical unclonable function (PUF) designs and utilizes the PUF circuits to generate the unique fingerprint for each IoT hardware device.

With the applications of IOT, millions of smart devices are interconnected and communicated through networks. The security and reliability of data transmission in IoT applications, the underlying hardware of these devices must be safe and trusted. Due to the nature of inherent mobility of current embedded devices, IoT hardware is vulnerable to security threats from multiple malicious participants. Device thefts, such as counterfeit, pirate, clone, over-produce Integrated Circuits (ICs) and Intellectual Property (IP) cores in embedded devices, are growing rapidly in a worrisome trend and are now becoming one of the most challenging security issues. The security vulnerabilities exposed by IoT hardware and therefore to access potentially sensitive or confidential information raise a host of new security and piracy concerns. This situation affects the reliability of IoT hardware, but also causes huge economic losses to both industry and individuals.

To effectively alleviate this threat, silicon PUF has been presented and considered to be a reliable anti-piracy solution to complete the device authentication and key storage. However, current PUF solutions are mostly focused on chip-level verification and cannot provide systematic identification and authentication. This real problem motivated the research work in the paper that proposes a unified identity verification framework which can provide fine-grained protection for embedded devices against theft attacks from the system level.

This framework is established on a series of PUF circuits that have been implanted into each individual chip of the devices. All chips in the devices are stored in the inconsistencies of the system-level fingerprint. The implementation and verification of the proposed scheme have demonstrated on the field programmable gate array (FPGA) platforms. The proposed framework can uniquely and accurately identify thefts to the embedded system hardware at low silicon overhead.

The contribution of the last paper are proposing a PUF-based unified identity verification framework, which can generate unique signatures for embedded device authentication from the system level. With optimization methods, CRO PUFs have been implanted into each individual chip of the devices as a hardware security primitive. The framework can identify any substitution of chips in the embedded devices.

3 List of accepted papers

1. Hao Zhang, Wenjun Zhang, zhihan lv, Arun Kumar Sangaiah, Tao Huang and Naveen Chilamkurti. MALDC: A Depth Detection Method for Malicious Behavior Based on Behavior Chains.
2. Xuewen Dong, Guangxia Li, Tao Zhang, Di Lu, Yulong Shen and Jianfeng Ma. An Incentive Mechanism with Bid Privacy Protection on Multi-bid Crowdsourced Spectrum Sensing.
3. Xiaoguang Li, Jun Liu, Boyan Ding, Zhiwei Li, HaoyangWu, TaoWang. A SDR-based Verification Platform for 802.11 PHY Layer Security Authentication.
4. Qiang Cao, Yanping Li, Zhenqiang Wu, Yinbin Miao, Jianqing Liu. Privacy-Preserving Conjunctive Keyword Search on Encrypted Data with Enhanced Fine-grained Access Control.
5. Zhao Huang and Quan Wang. A PUF-based Unified Identity Verification Framework for Secure IoT Hardware via Device Authentication.

Acknowledgements The guest editors would like to express their thanks to the Editor in Chief Professor Yanchun Zhang for giving them the opportunity to edit this special issue on "Security and Privacy in Network Computing". Also, we gratefully thank the authors for submitting their work as well as the tireless reviewers who have constructively evaluated the papers within the stipulated time. Finally, we sincerely hope the reader will share our view and find this special issue very useful.

References

1. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F.: Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access. **7**, 74361–74382 (2019). https://doi.org/10.1109/ACCESS.2019.2919982
2. Jiang, H., Zhou, R., Zhang, L. et al.: Sentence level topic models for associated topics extraction. World Wide Web. 1–16 (2018). https://doi.org/10.1007/s11280-018-0639-1
3. Li, M., Sun, X., Wang, H., Zhang, Y., Zhang, J.: Privacy-aware access control with trust management in Web service. World Wide Web. **14**(4), 407–430 (2011)
4. Shen, Y., Zhang, T., Wang, Y., Wang, H., Jiang, X.: MicroThings: a generic IoT architecture for flexible data aggregation and scalable service cooperation. IEEE Commun. Mag. **55**(9), 86–93 (2017)
5. Shu, J., Jia, X., YANG, K., Wang, H.: Privacy-preserving task recommendation services for crowdsourcing. IEEE Trans. Serv. Comput. 1 (2018). https://doi.org/10.1109/TSC.2018.2791601
6. Sun, X., Wang, H., Li, J., Pei, J.: Publishing anonymous survey rating data. Data Min. Knowl. Disc. **23**(3), 379–406 (2011)
7. Wang, H., et al.: A flexible payment scheme and its role-based access control. IEEE Trans. Knowl. Data Eng. **17**(3), 425–436 (2005)
8. Wang, H., Jiang, X., Kambourakis, G.: Special issue on security, privacy and trust in network-based big data. Inform. Sci **318**(C), 48–50 (2015)
9. Wang, H., Yi, X., Bertino, E., Sun, L.: Protecting outsourced data in cloud computing through access management. Concurr. Comp.-Pract. E. **28**(3), 600–615 (2016)
10. Wang, H., Zhang, Z., Taleb, T.: Special issue on security and privacy of IoT. World Wide Web. **21**(1), 1–6 (2018)
11. Zhang, J., Tao, X., Wang, H.: Outlier detection from large distributed databases. World Wide Web. **17**(4), 539–568 (2014)

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.