Future Generation Computer Systems 55 (2016) 224–226

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Editorial

Trust, Security and Privacy in Emerging Distributed Systems

1. Introduction

The rapid development and increasing complexity of computer systems and communication networks coupled with the proliferation of services and applications in both Internet-based and ad-hoc based environments have brought network and system security issues to the fore. We have been witnessing ever-increasing cyber-attacks on the network and system leading to tarnished confidence and trusts in the use of networked distributed systems. As a result, there is an increasing demand for development of new trust, security and privacy approaches to guarantee the privacy, integrity, and availability of resources in networked distributed systems.

The collections in this special issue present recent advances in trust, security and privacy for emerging parallel and distributed systems. The first set of papers focus on the detection and prevention of malicious activates sub-theme. The second set of papers is on trusted resource sharing. The third set of the papers is on the security of wireless sensor networks. The final set of papers focus on the access control mechanisms sub-theme.

2. Detection of malicious activities

Malicious software (malware) is one of the core arsenal used by the cybercriminals to compromise organisations information system. Much of today's malware use obfuscation techniques to avoid detection by the current generation anti-virus (AV) engines. Huda, et al. [1] proposed a hybrid approach based on support vector machine wrapper and filter based framework for malware detection. Knowledge about the intrinsic characteristics of malicious activities is determined by the API call statistics which is injected as a filter score into the wrapper's backward elimination process in order to find the most significant APIs.

Lately, detection of fraudulent activities in the financial sector has received renewed interest in research. As a result, a flurry of work in the area of clustering based unsupervised anomaly detection in the financial domain. Ahmed et al. [2] present an in-depth survey of various clustering based anomaly detection approaches and compares them from different perspectives. Anomaly detection is used to identify interesting phenomenon, abnormalities and trends such as financial fraud detection, computer network intrusion, human behavioural analysis and forth.

A CAPTCHA is a security solution that prevents malicious codes gaining illicit access to resources by pretending to be human users. Roshanbin and Miller [3] propose a new multi-layered CAPTCHA that offers resistance against pre-processing and various forms of segmentation and recognition attacks. The approach mainly comes from its use of Unicode as an input space, a virtual keyboard as the input device, homoglyphs and correlated usage of color in foreground and background as well as several layers of randomization that aim to minimize the formation of detectable patterns that can be exploited by machines. A user study conducted to measure the usability of the proposed CAPTCHA indicates that its solving accuracy is comparable to major CAPTCHAs in use today and offers insights into factors that affect CAPTCHA usability.

3. Trusted resource and data sharing

The paper by Alamri, et al. [4] highlights the need to enhance authorization security across semantically heterogeneous repositories. This is especially important for a secure and trusted information-sharing environment. To this end, Alamri, et al. [4] proposed the Mediator Authorization-Security framework that is capable of providing secure interoperation among heterogeneous semantic repositories. The evaluation showed that, despite the complexity of the mediator system, it still provides acceptable performance.

BitTorrent is a popular file sharing system in peer-to-peer platform. BitTorrent is based on the principle of fair sharing of resources pledged by the peers. In practice, BitTorrent suffers from the free rider problem in which the selfish peers consume the system resources while contributing nothing. As this problem could potentially lead to the collapse of the peer-to-peer system, the need for a solution to the free rider problem quite obvious. Azzedin and Yahaya [5] propose an approach that is based a game theory to mitigate the free riders issue in a BitTorrent environment. The proposed model enables peers to determine the best strategy to interact with others and the overall objective of our model is to inhibit free riding, increase fairness, and encourage resource contribution.

Recently, the notion of mobile social networks (MSNs) has received serious attention from a wide variety of researchers. One of the tenets of MSNs is enabling mobile users to distribute, discover, access and exchange data among themselves. Trusted data sharing is one of the major challenges facing MSNs environment. Chen et al. [6] describe the implicit social behavioral (ego-i) graph that is formed from users' contacts. These relationships are ranked to form a dynamic contact rank to enable users to evaluate the trust values. Group-based trust values are calculated according to the level of contacts, interaction evolution and users' attributes. The group-based trust is used to derive a cluster trust by the aggregation of inter group-based trust values. The performance of the trust model is carried out through simulations, and the results demonstrate the effectiveness of group-based behavioural relationships in MSNs' information sharing system.

http://dx.doi.org/10.1016/j.future.2015.11.008
0167-739X/

Collaborative filtering methods are commonly used by recommender systems for the purpose of analyzing and predicting user ratings or preferences of newly generated items depending on user historical behaviors. However, privacy issue arises in this process as sensitive user private data are collected by the recommender server. Li et al. [7] propose an efficient privacy-preserving item-based collaborative filtering algorithm. The proposed algorithm can protect user privacy during online recommendation process without compromising recommendation accuracy and efficiency. Empirical analysis of the proposed method demonstrates its superiority to several exiting approaches in recommendation efficiency while achieving similar or even better recommendation accuracy.

4. Securing wireless sensor networks

Benzaid, et al. [8] addressed the problem of message broadcast authentication, which is a fundamental security service in wireless sensor networks (WSNs). Exiting approaches are classified as symmetric-based schemes and public-key based schemes. Although the public-key based schemes obviate the security vulnerability inherent to symmetric-key based schemes, their signature verification is time-consuming. Benzaid, et al. [8] discuss an approach that exploits the sensor nodes cooperation to accelerate the signature verification of vBNN-IBS. Empirical evaluation of the scheme shows that the accelerated vBNN-IBS attains the longest network lifetime compared to the conventional vBNN-IBS.

There has been a host of research works on wireless sensor networks (WSN) for medical applications. Although WSNs for medical applications provide useful and real information about patients' health state, the data collected by medical sensor networks is sensitive data requiring proper safeguarding. Lounis, et al. [9] propose an architecture for collecting large amount of data generated by medical sensor networks and sharing between healthcare professionals in normal and emergency situations. The architecture contains a Ciphertext Policy Attribute-based Encryption to provide confidentiality, integrity and fine-grained access control to the collected medical data.

Rahman, et al. [10] identify privacy leakage channels by means of privacy leakage tree analysis in the distributed video surveillance context and propose the design of a secure privacy vault to conceal privacy-sensitive data obtained from distributed visual sensors. The viability of the proposed approach is demonstrated through security analysis of the proposed solution.

5. Access control mechanism

Access control mechanism are used in a diverse domains to manage privileges over resources. Risk-based access control mechanism are relatively new approaches in the access control technologies. Risk-based access control mechanism integrate risk analysis as part of the inputs when making an authorization decisions.

Nogoorani and Jalili [11] propose the trust-driven risk-aware access control (TIRIAC) framework for Grid computing environment. TIRIAC uses obligations to seamlessly monitor users and mitigate risks. In the TIRIAC framework, trust evaluation and risk management are added to the base Grid access control services. Thereafter, site administrators can explicitly specify users' responsibilities in form of obligations alongside access control rules. In addition, obligation-specific policies can be specified to mitigate risks according to their severity. We study the adoption of our framework by the European Grid Infrastructure (EGI), and demonstrate its superiority in comparison with the related work using multiple criteria. Moreover, we evaluate the performance of the framework and demonstrate its scalability in simulation experiments.

Díaz-López, et al. [12] propose the adoption of dynamic counter-measures for risk-based access control systems. System resource protection based on the risk level and an access control system granting/denying access depending on the fulfilment of a set of security controls applicable in an authorization access request constitute the advantages of the proposed approach. Genetic algorithm based approach is used to define the most appropriate set of counter-measures valid for a specific situation.

In role-based access control (RBAC), a role is a collection of permissions and all users acquire permissions only through the roles. However, it is costly to develop and maintain an RBAC system. With the increasing adoption of RBAC by businesses, the need for building high quality RBAC system is paramount. Ye, et al. [13] propose a role mining approach that is based on answer set programming (ASP) capable of simultaneously filling various constraints. The effectiveness and efficiency of the proposed approach is demonstrated through experimental results.

Wang et al. [14] proposed a secure hybrid-indexed search (SHIS) scheme for high efficiency over keyword searchable ciphertexts. The authors establish static index (SI) and dynamic index (DI) for public-key encryption with keyword search to make search efficient and secure in the state of the art. Using analysis, the SHIS scheme is shown to be significantly more efficient than PEKS.

For this special issue, we been able to select excellent papers providing a range of methods on the theme of the special issue. We thank the authors for contributing to our special issue. We also thank the reviewers for taking their valuable time to review and provide valuable comments to the authors. Last but not least the help of Maliha Omar is highly appreciated.

References

[1] Shamsul Huda, Jemal Abawajy, Mamoun Alazab, Mali Abdollalihian, Rafiqul Islam, John Yearwood, Hybrids of support vector machine wrapper and filter based framework for malware detection, Future Gener. Comput. Syst. 55 (2016) 376–390.
[2] Mohiuddin Ahmed, Abdun Naser Mahmood, Md. Rafiqul Islam, A survey of anomaly detection techniques in financial domain, Future Gener. Comput. Syst. 55 (2016) 278–288.
[3] Narges Roshanbin, James Miller, ADAMAS: Interweaving unicode and color to enhance CAPTCHA security, Future Gener. Comput. Syst. 55 (2016) 289–310.
[4] Abdullah Alamri, Peter Bertok, James A. Thom, Adil Fahad, The mediator authorization-security model for heterogeneous semantic knowledge bases, Future Gener. Comput. Syst. 55 (2016) 227–237.
[5] Farag Azzedin, Mohammed Yahaya, Modeling BitTorrent choking algorithm using game theory, Future Gener. Comput. Syst. 55 (2016) 255–265.
[6] Shuhong Chen, Guojun Wang, Weijia Jia, Cluster-group based trusted computing for mobile social networks using implicit social behavioral graph, Future Gener. Comput. Syst. 55 (2016) 391–400.
[7] Dongsheng Li, Chao Chen, Qin Lv, Li Shang, Yingying Zhao, Tun Lu, Ning Gu, An algorithm for efficient privacy-preserving item-based collaborative filtering, Future Gener. Comput. Syst. 55 (2016) 311–320.
[8] Chafika Benzaid, Karim Lounis, Ameer Al-Nemrat, Nadjib Badache, Mamoun Alazab, Fast authentication in wireless sensor networks, Future Gener. Comput. Syst. 55 (2016) 362–375.
[9] Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah, Yacine Challal, Healing on the cloud: Secure cloud architecture for medical wireless sensor networks, Future Gener. Comput. Syst. 55 (2016) 266–277.
[10] Sk. Md. Mizanur Rahman, M. Anwar Hossain, Mohammad Mehedi Hassan, Atif Alamri, Abdullah Alghamdi, Mukaddim Pathan, Secure privacy vault design for distributed multimedia surveillance system, Future Gener. Comput. Syst. 55 (2016) 344–352.
[11] Sadegh Dorri Nogoorani, Rasool Jalili, TIRIAC: A trust-driven risk-aware access control framework for grid environments, Future Gener. Comput. Syst. 55 (2016) 238–254.
[12] Daniel Díaz-López, Ginés Dólera-Tormo, Félix Gómez-Mármol, Gregorio Martínez-Pérez, Dynamic counter-measures for risk-based access control systems: an evolutive approach, Future Gener. Comput. Syst. 55 (2016) 321–335.
[13] Wei Ye, Ruixuan Li, Xiwu Gu, Yuhua Li, Kunmei Wen, Role mining using answer set programming, Future Gener. Comput. Syst. 55 (2016) 336–343.
[14] Wei Wang, Peng Xu, Hui Li, Laurence Tianruo Yang, Secure hybrid-indexed search for high efficiency over keyword searchable ciphertexts, Future Gener. Comput. Syst. 55 (2016) 353–361.

Jemal Abawajy
Deakin University, Australia
E-mail address: jemal@deakin.edu.au.

Guojun Wang
Central South University, China
E-mail address: csgjwang@mail.csu.edu.cn.

Laurence T. Yang
St. F.X. University, Canada
E-mail address: ltyang@stfx.ca.

Bahman Javadi
University of Western Sydney, Australia
E-mail address: b.javadi@uws.edu.au.