Journal of Universal Computer Science, vol. 21, no. 3 (2015), 365-368
submitted: 13/2/15, accepted: 26/2/15, appeared: 1/3/15

Recent Advances in Security and Privacy in Big Data

J.UCS Special Issue

Yong Yu
(University of Electronic Science and Technology of China, Chengdu, China
yyucd2012@gmail.com)

Yi Mu
(University of Wollongong, Wollongong, Australia
ymu@uow.edu.au)

Giuseppe Ateniese
(Sapienza-University of Rome, Rome, Italy
ateniese@di.uniroma1.it)

1 Introduction and Motivation

Big data has become an important topic in science, engineering, medicine, healthcare, finance, business and ultimately society itself. Big data refers to the massive amount of digital information stored or transmitted in computer systems. Approximately, 2.5 quintillion bytes of data are created every day. Almost 90% of data in the world today are created in the last two years alone. Security and privacy issues becomes more critical due to large volumes and variety, due to data hosted in large-scale cloud infrastructures, diversity of data sources and formats, streaming nature of data acquisition and high volume inter-cloud migration. In large-scale cloud infrastructures, a diversity of software platforms provides more opportunities to attackers. Traditional security mechanisms, which are usually invented for securing small-scale data, are inadequate. With a rapid growth of big data applications, it has become critical to introduce new security technology to accommodate the need of big data applications. The objective of this special issue is to capture the latest advances in this research field.

We solicited papers through two ways: conference and open call-for-papers. The conference is the 10th International Conference on Information Security Practice and Experience (ISPEC 2014). We also publicized an open call-for-papers at J.UCS website as well as in major academic announcement mailing lists/websites.

2 Contributions

Specifically, for this special issue 22 submissions were received. Each paper has followed a strict peer-review process: it was reviewed by at least three international experts, and in several cases a second reviewing found for minor or major revisions

was performed. Finally, after that process, eight quality research papers were selected for this special issue. The articles presented in this special issue deal with a variety of important topics within the security and privacy scope. In the following, we offer a brief description of each paper.

2.1 Polymorphic Malicious JavaScript Code Detection for APT Attack Defense

In this paper, authors propose a method that defines the malicious behaviors of malware using conceptual graphs that are able to describe their concepts and the relationships among them and, consequently, infer their malicious behavior patterns. The inferred patterns are then learned by a Support Vector Machine classifier that compares and classifies the behaviors as either normal or malicious. In the experimental results, it exhibits a better detection rate than that of malicious code detection methods that rely solely on the signature-based approach.

2.2 A Resolving Set based Algorithm for Fault Identification in Wireless Mesh Networks

In this paper, authors design a novel malfunctioned router detection algorithm, denoted by A-SRS, on searching resolving set based on private neighbor of dominating set. The A-SRS not only offers a highly efficient solution to position malfunctioned routers against intermitted communication that guarantees the availability of network services, but also pursues the minimum number of detecting routers due to limited resource of wireless mesh routers.

2.3 On the Security of a User Equipment Registration Procedure in Femtocell-Enabled Networks

In this paper, authors note that the user equipment registration procedure, which is defined in the Third Generation Partnership Project standard, in a femtocell-enabled network is vulnerable to denial-of-service attacks. The authors then propose a mechanism to defend against these attacks. For compatibility, the proposed mechanism makes use of the well-defined control message in the 3GPP standard and modifies the user equipment registration procedure as little as possible.

2.4 Restricted Identification Secure in the Extended Canetti-Krawczyk Model

In this paper, authors consider security of an extended version of the ChARI protocol presented at the 11th International Conference on Trust, Security and Privacy in Computing and Communications. Authors preserve the features of ChARI, but provide security proof in the well-studied Canetti-Krawczyk model. The extension has similar computational complexity as the original ChARI protocol in terms of the number of modular exponentiations.

2.5 Searchable Public-Key Encryption with Data Sharing in Dynamic Groups for Mobile Cloud Storage

In this paper, authors propose a searchable public-key encryption scheme for a group of users in mobile cloud storage. In the proposal, a dynamic asymmetric group key agreement protocol is utilized for data sharing among a body of mobile users and the technique of proxy re-signature is employed to update the searchable ciphertexts when the mobile users in the group varies.

2.6 An Improved Cloud Data Sharing Scheme with Hierarchical Attribute Structure

In this paper, authors present a new approach to implement scalable and fine-grained access control systems, which can be applied for big data in untrusted cloud computing environment. The solution is based on symmetric, efficient broadcast encryption and ne-grained attribute-based encryption. In this access control system, users are able to join and revoked with broadcast encryption. An outsourced Hierarchical ABE scheme is proposed to construct the access control system.

2.7 Insecurity of an Efficient Privacy-preserving Public Auditing Scheme for Cloud Data Storage

In this paper, authors demonstrate that a new auditing protocol due to Worku et al. fails to achieve soundness and obtains merely limited privacy. Specifically, authors show even deleting all the files of a data owner, a malicious cloud server is able to generate a response to a challenge without being caught by TPA in their enhanced but unrealistic security model. Worse still, the protocol is insecure even in a correct security model. For privacy, a dishonest verifier can tell which file is stored on the cloud.

2.8 Multi-Authority Attribute-Based Encryption Scheme from Lattices

In this paper, authors present a multi-authority attribute-based encryption scheme from lattices, in which identities of users are authenticated by a central authority, which improves the efficiency of authentication. Furthermore, different attribute private keys are still distributed by different authorities, and the central authority cannot obtain any secret information of other attribute authorities, which resolves key escrow problem to some extent.

3 Reviewers

We would like to express our gratitude to the reviewers involved in this special issue for their valuable comments and detailed feedback. Most of them are program members of ISPEC 2014.

Man Ho Au, Hong Kong Polytechnic University, China
Joonsang Baek, KUSTAR, UAE

Yong Yu
Yi Mu
Giuseppe Ateniese
January 2015
China, Australia, Italy