Guest editors' introduction

This special issue of the Journal of Computer Security (JCS) is based on some of the selected papers from the 36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec 2022) held in Newark, NJ, USA, from July 18th–July 20th 2022.

Four of the best papers from DBSec 2022 have been included after additional reviews for JCS. These are "Securing Blockchain-based Timed Data Release against Adversarial Attacks" by Jingzhe Wang and Balaji Palanisamy, "The Intrinsic Dimensionality of Network Datasets and its Applications" by Matt Gorbett, Caspian Siebert, Hossein Shirazi and Indrakshi Ray, "Con2Mix: A Semi-Supervised Method for Imbalanced Tabular Security Data" by Xiaodi Li, Latifur Khan, Mahmoud Zamani, Shamila Wickramasuriya, Kevin Hamlen and Bhavani Thuraisingham, and "Robust, Revocable, Forward and Backward Adaptively Secure Attribute-Based Encryption with Outsourced Decryption" by Anis Bkakria.

Wang and Palanisamy in their paper address the challenges faced by blockchain based timed data release in the presence of both malicious and rational adversaries. They present a protocol using reputation-aware peer recruitment and verifiable enforcement. Evaluation has been done with a prototype implementation on the Rinkeby test network and the results look promising.

The paper by Gorbett et al. looks into the problem of analyzing and classifying traffic in IoT, which is one of the primary steps in network management and enforcing security in this domain. An interesting measurement tool named Intrinsic Dimensionality has been introduced and extensive experiments have been carried out with this tool for intrusion detection.

It is well known that datasets for computer security research are not readily available. Even those that exist, suffer from serious data imbalance. Li et al. specifically analyze the data imbalance problem in tabular security data which, unlike image and text, is not amenable to traditional machine learning approaches. They propose and implement Con2Mix – a semi supervised method to bridge the gap along with results from a detailed experimentation.

Attribute-based Encryption (ABE) has developed into an immensely useful approach for access control in cloud computing. Bkakria first identifies some of the shortcomings of traditional ABE in real life cloud based deployment. A novel approach is then proposed that supports outsourced decryption while mitigating the concern of single point of failure. Both theoretical complexity analysis and experimental validation have been done to demonstrate its efficacy.

This special issue of JCS with papers addressing multiple facets of computer security is expected to be of great value to its readership and help to extend the research frontier further.

Shamik Sural and Haibing Lu
(Guest Editors)