EAI Endorsed Transactions
on Security and Safety
Editorial ICST.ORG

Security, Privacy and Trust in Cyber Physical Systems

Dr. H. Janicke[1], Dr. Kevin Jones[2] and Dr. L. Maglaras[1]

[1] De Montfort University

[2] Airbus Group

Received on 30 November 2016, published on 08 November 2016

doi: 10.4108/eai.8-12-2016.151724

Introduction

The first issue of the third volume of the EAI transactions on Security and Safety provides an insight to methods and techniques that improve security, safety and privacy of benchmark systems. Actually, two main classes of research results are considered. The first one is on attack prevention and secure planning while the second one is focused on forensics analysis. In particular, in the area of attack preventions and secure planning the issue presents (i) a new model and an algorithm to estimate and generate a network path identified by flow performance indicators of a heterogeneous communication network, (ii) suitable procedures that e-commerce operators may apply to minimize the risk of criminal activities, and (iii) a novel pseudorandom number generator family, called filtering nonlinear feedback shift register for RFID tags. In the area of forensic research the issue presents new findings on new methods exploiting the metadata of a large corpus.

In article Assessing Security, Capacity and Reachability of a Heterogeneous Industrial Network during Planning Phase by Apala Ray, Johan Akerberg, Mats Bjorkman and Mikael Gidlund authors try to assess the relation of security and network performance for overall plant operation. The article focuses on identifying an optimal flow path between two devices in a multi-hop heterogeneous network. Based on this analysis, authors propose a model along with an algorithm that can estimate and generate a network path identified by flow performance indicators of a heterogeneous communication network. Finally using an example, they evaluate flow performance metric in terms of security, capacity and reachability of the devices in the network.

In article Prevention of crime in B2C E-Commerce: How E-Retailers/Banks protect themselves from Criminal Activities by Najlaa Almajed, Leandros Maglaras, Francois Siewe, Helge Janicke and Pooneh Bagheri Zadeh the issue of what e-commerce websites should do to minimize their customer's risk is investigated. Authors analyze current deficiencies in online shopping and online banking websites, and identify suitable procedures that e-commerce operators may apply in order to minimize the risk of criminal activities.

In article Filtering Nonlinear Feedback Shift Registers using Welch-Gong Transformations for Securing RFID Applications by Kalikinkar Mandal and Guang Gong deals with privacy issues in RFIDs. Authors present a pseudorandom number generator family called filtering nonlinear feedback shift register and show how this could applied on EPCC1Gen2 tags.

Finally in article Identifying Forensically Uninteresting Files in a Large Corpus by Neil Rowe several methods for methods exploiting the metadata of a large corpus are discussed. The work presented in this article provides both new uninteresting hash values and programs for finding more.

The topics treated in the aforementioned articles come to confirm that the area of security and safety is a multi-disciplinary one and combines both analytical methods and computational tools for improving the performance of security mechanisms, advancing trust among different entities, and investigating incidents.

Dr. Helge Janicke Email: heljanic@dmu.ac.uk

Dr.Kevin Jones Email: kevin.jones@airbus.com

Dr. L. Maglaras Email: leandrosmag@gmail.com

Moreover, it has shown that the use of preventions and detections tools in online platforms and production systems can result into the improvement of the overall security level and into a more profitable and reliable functioning of the system. As there is constant growth in the need for reliable systems' operation under challenging conditions and security threats, one should also anticipate further development of the aforementioned security and privacy methods.