EAI Endorsed Transactions
on Security and Safety
Editorial EAI.EU

Defence Mechanisms for Public Systems

Dr. Sencun Zhu[1], Dr. Kevin Jones[2] and Dr. Leandros A. Maglaras[3]

[1]The Pennsylvania State University
[2]Airbus Group
[3]De Montfort University

Received on 29 December 2017; published on 4 January 2018

doi: 10.4108/eai.4-1-2018.153524

1. Editorial

The third issue of the fourth volume of the EAI transactions on Security and Safety provides an insight to methods and techniques that improve security, resiliency and privacy of modern systems, such as clouds, moving target defense (MTD)-enabled systems and Blockchains. The articles that constitute this issue focus on three main areas. The first one consists of novel methods that can increase detection capabilities of cloud systems; the second one is proposing an MTD evaluation framework; the third is about blockchain technology and its use from lightweight users. In particular, in the area of novel detection methods the issue presents (i) Markov-based models that can be used in order to detect malicious sources engaged in fraudulent use of cloud resources, (ii) cross-layer Bayesian networks for inferring stealthy bridges that exist between enterprise network islands. In the area of MTD-enabled system, the issue presents a generic MTD evaluation framework. Finally regarding blockchain technology the issue presents a novel efficient verification protocol for public blockchain, namely EPBC, which can be used from users with limited resources.

In article Attribution of Economic Denial of Sustainability Attacks in Public Clouds by Mohammad Karami, An Wang and Songqing Chen, authors try to address low-rate and stealth EDoS attacks, which are not so common but are more challenging to detect and mitigate. During a EDOs attack the adversary sends seemingly legitimate requests to a victim service in order to consume cloud resources for which the victim will have to pay for the cost. An effective EDOs attack is stealthy and remains undetected over an extended period of time. For identifying such attacks, the current article presents Markov-based anomaly detection schemes to profile the behavior of legitimate users in terms of their resource consumption and spot malicious entities. By using experimental evaluations for various attack scenarios, authors demonstrate the effectiveness of the proposed methods.

In article Probabilistic Inference of the Stealthy Bridges between Enterprise Networks in Cloud, by Xiaoyan Sun, Jun Dai, Anoop Singhal and Peng Liu, authors use cross-layer Bayesian networks to infer the stealthy bridges that exist between enterprise network islands. In a public cloud, where several tenants “live” in the same space, attackers are able to establish stealthy bridges connecting several enterprise networks. Once the isolation among enterprise networks is penetrated, information confidentiality could be violated and the attacker can traverse from one enterprise network to another. As stated by the authors, stealthy bridges per se may be difficult to detect, but the steps followed from the intruder before and after the construction of stealthy bridges may trigger some abnormal activities. Using this concept, authors built a cloud-level attack graph and construct a cross-layer Bayesian network that is able is able to infer the existence of stealthy bridges. Authors conduct a set of experiments that showcase the efficiency of the proposed method.

In article An Evaluation Framework for Moving Target Defense Based on Analytic Hierarchy Process by Chu Huang, Yi Yang, and Sencun Zhu, authors propose a framework that evaluates security strengths and costs of several MTD-based approaches. The main feature of an MTD based system is that certain system dimensions continuously change over time, in order to increase complexity and cost for attackers to probe the system and launch an attack. Although a variety of moving target defenses exist, a well-accepted methodology to assess the cost-effectiveness of different MTDs is missing and authors fill this gap in this article by proposing a novel evaluation framework. Their proposed framework is based on five general evaluation metrics and it is general enough to be applied in different MTD categories under a variety of attacks. Authors conduct a detailed case study

For a specific MTD category named software diversification in order to validate the effectiveness of the proposed generic evaluation framework.

Finally, in article Efficient Public Blockchain Client for Lightweight Users by Lei Xu, Lin Chen, Zhimin Gao, Shouhuai Xu and Weidong Shi, authors deal with the class of blockchains that are built on the principle of proof-of-work and propose a succinct blockchain verification protocol that allows lightweight users to participate in such applications. A blockchain is a distributed ledger that has been used by Bitcoin and other applications to store their transaction data, where a transaction can be a payment operation, smart contract submission, or smart contract execution result submission. Due to its main characteristics, which are immutability and append-only, its size keeps growing with every transaction, making it difficult for users that have limited computation/storage capacities, such as IoT devices and smartphones to use applications based on blockchains. Trying to cope with this issue, authors propose an efficient verification protocol for public blockchain, namely EPBC, which can be incorporated into existing blockchains as a middle layer service, or can be seamlessly incorporated into new blockchain systems. Authors analyzed the security of EPBC and preliminary experiments showed that it is practical.

Dealing with hot areas of research, such as blockchains and public clouds, and state of the art defense mechanisms like MTD and novel intrusion detection systems, this issue constitutes a very good collection of selected articles. Novel defense mechanisms try to overcome the deficiencies of the systems that they are residing on, and improve the performance of previous solutions that are not capable of dealing with the ever evolving attack environment. These mechanisms can be further improved by incorporating other aspects of user or system behavior in order to be able to detect malicious users, stealthy bridges or other kind of attacks. Trust among different entities is also a crucial part of any defense system along with the ability of the defense mechanisms that are built to adapt to architectural changes, especially for cloud environments that are highly dynamic.