EAI Endorsed Transactions
on Security and Safety

Research Article EAI.EU

Editorial

David Mohaisen[1], Sencun Zhu[2]

[1]University of Central Florida, Orlando, FL 32816, USA
[2]The Pennsylvania State University, University Park, PA 16802, USA

Received on 16 May 2020; accepted on 18 May 2020; published on 18 May 2020

doi:10.4108/eai.18-5-2020.164587

The Internet of Things (IoT) has delivered many systems that facilitate the interaction between users and their environments, allowing for data transfer and processing with ease, and enabling many interesting and crucial applications by utilizing a unique convergence of machine learning, sensing, control, and automation. Applications of IoT include medical devices, smart home devices and automation, wearable and immersive experience systems (e.g., virtual and augmented reality), and industrial systems, among many others. The increasing number of IoT devices deployed today is paralleled with an increased number of security and privacy concerns. In this issue, we present four papers that attempt to address various aspects of the security and privacy of IoT systems, namely: 1) flexible access control of medical IoT, 2) an attack and a defense on smart speakers, 3) a privacy-preserving annotation mechanism for images generated by smartphone devices, and 4) a one-time passkey design and implementation on Arduino using ambient noise.

The first paper in this issue is titled “Controlled BTG: Toward Flexible Emergency Override in Interoperable Medical Systems”, and is written by Qais Tasali (Kansas State University), Christine Sublett (Sublett Consulting), and Eugene Y. Vasserman (Kansas State University). In this work, the authors address the challenge of crafting least-privilege authorization policies which preserve patient safety and confidentiality even during emergency situations through Controlled BTG. BTG, which stands for “Break the Glass” is an analogy to breaking a physical barrier to access a protected emergency resource such as a fire extinguisher or “crash cart”. In healthcare, BTG is used to override access controls and allow for unrestricted access to resources, e.g. Electronic Health Records. After a “BTG event” completes, the actions of all concerned parties are audited to validate the reasons and legitimacy for the override. Medical BTG has largely been treated as an all-or-nothing scenario: either a means to obtain unrestricted access is provided, or BTG is not supported. In the work, the authors show how to handle BTG natively within the attribute-based access control model, maintaining full compatibility with existing access control frameworks, putting BTG in the policy domain rather than requiring framework modifications. Their approach also makes BTG more flexible, allowing for fine-grained facility-specific policies, and automates auditing in many situations, while maintaining the principle of least-privilege. The authors present a sample BTG policy and verify its correctness while allowing for an expanded access during BTG events.

The second work in this issue is titled “Manipulating Users’ Trust on Amazon Echo: Compromising Smart Home from Outside”, and is written by Yuxuan Chen (Florida Institute of Technology), Xuejing Yuan (University of Chinese Academy of Sciences), Aohui Wang (University of Chinese Academy of Sciences), Kai Chen (University of Chinese Academy of Sciences), Shengzhi Zhang (Boston University), and Heqing Huang (Bytedance AI lab). In this paper, the authors explore the security of smart speakers by exploring compromising smart home from outside. Motivated by the fact that voice control systems have become very popular and allow people to communicate with their devices more conveniently, the security of those systems is significant, especially when using IFTTT (if-this-then-that) service, which allows for those systems, to improve skills significant. The key contribution of the work is MUTAE (Manipulating Users’ Trust on Amazon Echo), an attack to remotely compromise Amazon Echo’s voice control interface. The authors conducted a security analysis and performed a taxonomy based on different consequences considering the level of trust that users have placed on Echo. Finally, they also proposed mitigation techniques that protect Echo from MUTAE attack.

The third paper of this issue is titled “Development of a Multifactor-Security-Protocol System Using Ambient Noise Synthesis”, and is written by Agbotiname Lucky Imoize, Boluwatife Samuel Ben-Adeola, and John Adetunji Adebisi, all of whom are from the University of Lagos. The escalating cases of security threats on the global scene, especially in the cyberspace, demands urgent need to deploy sophisticated measures to mitigate these calamitous threats. To this end, various lock mechanisms have been developed and deployed to prevent access to control systems from potential intruders. In this paper, the authors provide a solution to this pervasive problem, addressing concerns on the physical and virtual components of an access control system. For their solution, a locally generated One-Time-Passkeys (OTPs) was created, leveraging ambient noise as an entropy input. Then, the system was deployed on an Arduino microcontroller embedded in a safe-cabinet secured with a 12V solenoid lock. The design was implemented and tested against standard metrics. Results achieved include algorithmic optimizations of existing local OTP protocol implementations, and the realization of a safe lock module, which interfaces with a mobile application developed on Android over a secured Bluetooth connection.

The fourth paper in this issue is titled "CPAR: Cloud-Assisted Privacy-preserving Image Annotation with Randomized k-d Forest", and is written by Yifan Tian (Agari Data, Inc.), Jiawei Yuan (University of Massachusetts Dartmouth), and Yantian Hou (Boise State University). In this paper, the authors propose a cloud-assisted privacy-preserving image annotation with randomized k-d forest technique, named CPAR. With CPAR, users are able to automatically assign keywords to their images by leveraging the power of cloud with privacy protected. CPAR proposes a novel privacy-preserving randomized k-d forest structure, which is shown to significantly improve the annotation performance of images compared with existing research. Thorough analysis is carried out by the authors to demonstrate the security of CPAR, over the well-known IAPR TC-12 dataset, showing the efficiency and effectiveness of CPAR.

We hope that you will enjoy those four papers, as we did, and we look forward to your contribution in line with this theme of contributions.