CCSP:RND
Cloud Cyber Security and Privacy: Readiness for the Next Decade

Special Track running alongside CLOUD COMPUTING 2021, The Twelfth International Conference on Cloud Computing, GRIDs, and Virtualization, April 18, 2021 to April 22, 2021 – Porto, Portugal

Magnus Westerlund*, Bob Duncan†, Andreas Aßmuth‡ and Sebastian Fischer§

*Arcada University of Applied Sciences, Finland, Email: magnus.westerlund@arcada.fi
†University of Aberdeen, UK, Email: bobduncan@abdn.ac.uk
‡Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany, Email: a.assmuth@oth-aw.de
§Technical University of Applied Sciences OTH Regensburg, Germany, Email: sebastian.fischer@othr.de

***Abstract*—The field of cybersecurity has both from a research and business aspect grown rapidly over the last decade as a response to the numerous security breaches. The use of cloud and IoT solutions has challenged many of the commonly held practices and demanded that new methods and practices are developed. In particular, a major concern with the use of IoT has been the security of the technology and for cloud computing, in general, there is a lack of control of the underlying infrastructure and services. The use of either technology in safety-critical installations deserves a broad focus on the trustworthiness of such solutions. The special track "Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND)" takes a forward-looking perspective to improve the understanding of security in safety-critical installations. The special track includes five publications on security topics that aim to deepen the understanding of how to improve security and how to retain information for forensic purposes.**

***Index Terms*—Cloud; Cyber Security; Privacy; IoT**

I. Introduction

During the course of the past decade cloud computing has resulted in an almost complete transformation of the IT landscape. The initial reluctance shown by many potential users to utilise public cloud infrastructure due to concerns about security and privacy has given way to greater acceptance following the ability to perform horizontal scaling securely and, in particular, for an economic cost, as compared with self-hosted dedicated hardware. As new software is created, it increasingly is designed as cloud-native solutions that can reap the benefits of the cloud. Monolithic designs are giving way to microservices, serverless, and unikernel designs, whose aim is to improve security, scaling, and cost effectiveness further. The COVID-19 pandemic also forced many people of all ages to use cloud services for video conferences, home schooling, etc., which has led to a significant increase in the number of users of cloud services.

Looking towards the coming decade, the transformation will likely not stop there and the new paradigm is already forming. As the capabilities of cloud continue to evolve and grow, rather more worryingly, so too do the capabilities of attackers. As was already seen in 2020, the increased usage caused by the pandemic made cloud services even more attractive as targets for cyber-attacks. Since new legislation and regulation is continuously being introduced, and some, such as GDPR, have exceptionally high compliance requirements coupled with a high level of punitive fines, it is necessary for companies who use cloud to take a much more serious approach to achieving compliance.

Failure to take appropriate measures to safeguard data held in the cloud will no longer be tolerated by regulators. Equally, failure to report breaches properly and timeously are also starting to be heavily punished by regulatory authorities. Looking at the current level of regulatory fines, it is clear that regulators are getting serious about enforcing better compliance. It is no longer possible for companies to sit back as see what everyone else does, now companies have to demonstrate a proactive approach if there is to be any prospect of a large reduction in the fines levied due to their efforts providing mitigation.

Issues, such as the 'Cloud Forensic Problem' will still impact on cloud systems if cloud users do not take the appropriate steps necessary to secure their own systems properly. Similarly, it is no longer possible for actors such as Cloud Service Providers to sit back and leave all security measures to cloud users as many have done before. Now, all actors are accountable and much more focus on ensuring a proper approach is used for security and privacy is required.

II. Submissions

The paper, "IT Security of Cloud Services and IoT Devices in Healthcare" [1], addresses the challenges of connecting Medical Internet of Things Devices (MIoT) to Cloud services and the Internet in general. Currently, many (older) devices are attached to the Internet, which have never been intended to work within a network. New devices result in the implementation of necessary medically approved hardware, software and attached Cloud services. Both lead to new IT security challenges and demand for new security concepts. The paper identifies such upcoming security challenges. It provides research on existing IT security guidelines targeting network-connected medical IoT devices, their users and the attached Cloud services in homecare and integrated care.

The second paper, entitled "A Secure and Privacy-Friendly Logging Scheme" [2], presents a concept for a new privacy-friendly system, which can be used to securely store user login data. The goal is to create a logging scheme, that enables users to use individual credentials with strong passwords or even multi-factor authentication to log into a computer or machine, and on the other hand, does not allow employers to use this login data for workplace surveillance in order to assess their employees productivity. In case of mistakes, illegal actions, etc., the proposed system allows to track down the responsible person by accessing to encrypted login data. The key required for decryption must be put together of different parts, which are shared among different groups, e.g., one part for the employer, one part for the workers' council representing the employees and one part for law enforcement authorities.

Drones or Unmanned aerial vehicles (UAVs) have become popular in the civilian area because of their great potential for different applications, like delivery of goods, search and rescue missions, wildlife and terrain monitoring. The paper "An Approach for Decentralized Authentication in Networks of UAVs" [3], proposes a decentralized authentication system for networks of drones using a blockchain-based public key infrastructure. In such networks the drones interact with other drones, different kinds of vehicles, infrastructural elements as well as diverse Cloud services. Because secure communication starts with secure authentication, the proposed system is meant to prevent UAVs and Cloud services from compromising each other.

Malware threatens current Internet of Things (IoT) devices and is used for botnets, especially in the smart home environment. In order to be able to assess the security of devices in the home network, IoTAG (IoT Device IdentifiCAtion and RecoGnition) was introduced, which defines an interface with which the IoT devices provide security-relevant information to a central hub. The paper "How to prevent misuse of IoTAG?" [4] is about an extension to IoTAG so that this information cannot be used by an attacker. Already established methods are used for this purpose. Furthermore, the risks are assessed which would be affected by disclosing the information in the network.

Integrating Internet of Things devices in corporate networks has been a great enabler for data collection, which can be used to run systems, processes, and machines more effectively. Unfortunately, security is often not appropriately considered during design and the incorporation of such devices into the corporate network can introduce new attack vectors. Once an attacker gains access, the audit trail is often the single most important target for attackers to allow them to cover their tracks and remain hidden in the system for a long duration. Therefore, precautions must be taken to properly secure this important record in a cryptographically secured immutable database. Without records, we have no means to forensically discover who has perpetrated attacks, nor how they penetrated our systems. The paper "Incorporating Permanent Audit Trails for Corporates" [5] explores a method for securely collecting and storing this information in an immutable database. We approach this using blockchain based smart contracts. The approach has an added advantage by being a distributed approach with no central point of attack.

III. Conclusions

The CCSP:RND special track includes a broad range of topics related to Cloud Cyber Security and Privacy. The different, interesting ideas show a positive development for the future in this thriving research domains. From Healthcare over Smart Home to Drones, every area is represented. The solutions can also be transferred and used in other cloud areas. Scientific exchange advances technologies and research and enables global collaboration, as the contributions are from many countries.

Acknowledgment

We would like to thank the organizers of Cloud Computing 2021 for their tireless efforts and for accepting CCSP:RND as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

References

[1] M. Gleißner, J. Dotzler, J. Hartig, A. Aßmuth, C. Bulitta, and S. Hamm. "IT Security of Cloud Services and IoT Devices in Healthcare," in Special Track: Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND), along with Cloud Computing 2021. IARIA XPS Press, 2021.

[2] A. Aßmuth, R. Duncan, S. Liebl, and M. Söllner. "A Secure and Privacy-Friendly Logging Scheme," in Special Track: Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND), along with Cloud Computing 2021. IARIA XPS Press, 2021.

[3] N. Jäger and A. Aßmuth. "An Approach for Decentralized Authentication in Networks of UAVs," in Special Track: Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND), along with Cloud Computing 2021. IARIA XPS Press, 2021.

[4] B. Weber, L. Hinterberger, S. Fischer, and R. Hackenberg. "How to prevent misuse of IoTAG?," in Special Track: Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND), along with Cloud Computing 2021. IARIA XPS Press, 2021.

[5] R. Duncan, M. Westerlund, and J. Wickström. "Incorporating Permanent Audit Trails for Corporates," in Special Track: Cloud Cyber Security and Privacy: Readiness for the Next Decade (CCSP:RND), along with Cloud Computing 2021. IARIA XPS Press, 2021.