FAST-CSP
Finding A Solution To - Cloud Security Problems

Special Track running alongside CLOUD COMPUTING 2022, The Thirteenth International Conference on Cloud Computing, GRIDs, and Virtualization, April 24, 2021 to April 28, 2022 – Barcelona, Spain

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

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

***Abstract*—With the rapid growth of networked devices with cloud environments, there are questions about how secure the data and devices are. To address these security issues, there are many different approaches in current research. In special tack FAST-CSP: Finding A Solution To - Cloud Security Problems, different problems were analyzed and suitable solutions were presented. A penetration testing framework for automobiles, which is intended to support universities in their teaching, makes it possible in the form of hardware to test the many different attacks on vehicles. Other papers concern the world of the Internet of Things and thus all kinds of networked devices. An intrusion detection system that uses static analysis with various artificial intelligence methods to enable better detection and classification of attacks. Furthermore, a scoring system to better define security, privacy and usability requirements. This system can address the security of devices already during development. Moreover, a paper investigated the impact of the Covid-19 Pandemic on Cyber Security, as the changing world of work has also changed the security risks. As last, a security solution for SMEs was presented, which is especially adapted to the requirements of the target group and combines modern research topics.**

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

I. Introduction

Cloud computing has been a great enabler for a great many companies and individuals in the decade or so since it gained traction. The ability to access new systems rapidly without concern for forward planning, accessing corporate budgets and in particular the ability to scale up (or down) on demand has proved particularly attractive. A great many researchers have been actively involved to ensure that systems are developed in a responsible way to ensure the security and privacy of users.

During these years, cloud has evolved at a prodigious rate, to the extent that many would scarcely believe just how much it has evolved in such a short period of time. Of course, evolution does not happen seamlessly, and there have been many growing pains along the way. This is common to all computing systems, whether traditional monolithic systems or cloud systems. Often the speed of change introduces new weaknesses and vulnerabilities. These need to be identified and properly dealt with.

As more and more corporates are turning to cloud, whether for their main business delivery systems, or to accommodate rapid spooling up to handle sudden business increases, it has been seriously adopted in huge numbers. Even governments and not-for-profit organisations are adopting cloud in a big way. Cloud also gives SMEs the ability to carry out their business on a par with large corporates, meaning there is no longer the need for SMEs to believe they cannot compete with the big players on a similar IT level.

However, we need to be cognizant of the fact that not all security and other issues have necessarily been found and properly dealt with. Given the ever more challenging regulatory environment in which all organisations must work within, we need to be ever more vigilant when we consider the impact these unresolved issues might have on compliance.

II. Submissions

Due to the rising digitalization of vehicles, they are increasingly becoming the target of attacks. However, since vehicles are not only about Cyber Security, but also about safety, it is important that a security issue in information technology cannot cause personal injury. This is why Cyber Security is also increasingly coming into focus in the automotive sector. The Papter, “An Automotive Penetration Testing Framework for IT-Security Education” [1], presents a framework that can be used to practice penetration tests in higher education. For this purpose, different layers are defined, which simulate various interfaces of a vehicle, so that attacks on these can be carried

out. The implementation was done in the form of hardware in order to teach knowledge in the field of penetration tests and automotive as realistically and didactically as possible.

Not only vehicles are affected by security risks and attacks, but also all other networked devices. The number of networked devices is continuously increasing. In order to be able to operate potentially insecure devices, intrusion detection systems (IDS) are often used. However, these systems have to adapt dynamically to the increasingly sophisticated malware. Therefore, the paper, "Design and Implementation of an Intelligent and Model-based Intrusion Detection System for IoT Networks" [2], uses a mixture of artificial intelligence (AI) and static analysis for the IDS. The paper describes the multi-layered architecture of the system, in which different AI methods are used. Data collection, processing and the obtained results are analyzed and evaluated. By using different techniques and the interaction of static analysis and AI, a much better detection rate and automated identification of attacks can take place.

As the number of connected devices, the Internet of Things (IoT), increases, so are the risks of the new technology. More and more security issues are emerging as the data and control of the devices are outsourced to the cloud. To help device manufacturers to develop and users to select a secure device, a scoring system for IoT devices was presented [3] that combines the aspects of security, privacy and usability. Depending on the requirements and target group of a device, the requirements for a device in the three aspects can vary.

"The Covid-19 Pandemic And Its Influence On Cloud Cyber Security" [4] shows the changes in cyber security over the course of the pandemic. New security challenges arose due to changes in working conditions. The opportunities for attacks have increased, as more and more work is done remotely. But on the other hand, security mechanisms have also quickly gained acceptance. Major threats existed and continue to exist due to rapidly adapting attacks.

The number of attacks on SMEs is constantly increasing, but SMEs often do not have the budget and exptertise to take sufficient security measures. The paper, "Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies" [5], addresses the problem and presents a suitable solution. The focus is on cost-efficiency. With the help of technologies already known from other domains, security measures are to be transferred to SMEs.

III. Conclusions

The FAST-CSP special track is not limited to cloud applications and shows a wide range of current research topics. The focus is always on Cyber Security. This can be seen in the publications, which are useful for finding security issues as well as for evaluating them. Furthermore, problems and solutions were presented in the current situation and for SMEs. The research shows the global situation through contributions from different countries.

Acknowledgment

We would like to thank the organizers of Cloud Computing 2022 for their tireless efforts and for accepting FAST-CSP as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

References

[1] S. Schönhärl, P. Fuxen, J. Graf, J. Schmidt, R. Hackenberg, and J. Mottok. "An Automotive Penetration Testing Framework for IT-Security Education," in Special Track: Finding A Solution To - Cloud Security Problems (FAST-CSP), along with Cloud Computing 2022. IARIA XPS Press, 2022.

[2] P. Vogl, S. Weber, J. Graf, K. Neubauer, and R. Hackenberg. "Design and Implementation of an Intelligent and Model-based Intrusion Detection System for IoT Networks," in Special Track: Finding A Solution To - Cloud Security Problems (FAST-CSP), along with Cloud Computing 2022. IARIA XPS Press, 2022.

[3] S. Fischer. "A Security-, Privacy- and Usability- Scoring System for IoT Devices," in Special Track: Finding A Solution To - Cloud Security Problems (FAST-CSP), along with Cloud Computing 2022. IARIA XPS Press, 2022.

[4] A. Aßmuth. "The Covid-19 Pandemic And Its Influence On Cloud Cyber Security," in Special Track: Finding A Solution To - Cloud Security Problems (FAST-CSP), along with Cloud Computing 2022. IARIA XPS Press, 2022.

[5] R. Duncan and M. Westerlund. "Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies," in Special Track: Finding A Solution To - Cloud Security Problems (FAST-CSP), along with Cloud Computing 2022. IARIA XPS Press, 2022.