

FAST-CSP

Finding A Solution To - Cloud Security Problems




Magnus Westerlund, Bob Duncan, Andreas Aßmuth, and Sebastian Fischer

Cloud Computing 2022 – Barcelona, Spain






April 24, 2021 to April 28, 2022




Dr. Magnus Westerlund

 Arcada University of Applied Sciences
 Finland
 magnus.westerlund@arcada.fi




Dr. Bob Duncan

 University of Aberdeen
 Scotland, UK
 bobduncan@abdn.ac.uk

Prof. Dr. Andreas Aßmuth

 OTH Amberg-Weiden
 Germany
 a.assmuth@oth-aw.de

Sebastian Fischer, PhD Candidate

 OTH Regensburg
 Germany
 sebastian.fischer@othr.de

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.

- Introduction
Chairs
- An Automotive Penetration Testing Framework for IT-Security Education
Stefan Schönhärl, Philipp Fuxen, Julian Graf, Jonas Schmidt, Rudolf Hackenberg and Jürgen Mottok
- Design and Implementation of an Intelligent and Model-based Intrusion Detection System for IoT Networks
Peter Vogl, Sergei Weber, Julian Graf, Katrin Neubauer and Rudolf Hackenberg
- A Security-, Privacy- and Usability- Scoring System for IoT Devices
Sebastian Fischer

- The Covid-19 Pandemic And Its Influence On Cloud Cyber Security
Andreas Aßmuth
- Cost-Effective Permanent Audit Trails for Securing SME Systems when Adopting Mobile Technologies
Robert Duncan and Magnus Westerlund
- Open Discussion and Closing Remarks
Chairs (Moderators)