12th International Conference - IcETRAN 2025
Čačak, Serbia, June 9-12, 2025

Computing and Information Engineering Section (RTI)
INVITED LECTURE:

"New Approaches to Data Protection in the Cloud"

Pavle Vuletić and Žarko Stanisavljević
University of Belgrade, School of Electrical Engineering
Belgrade, Serbia
pavle.vuletic@etf.bg.ac.rs, zarko@etf.bg.ac.rs

Abstract: Two recent server processor capabilities, AMD SEV SNP and Intel TDX, enable isolating and encrypting the whole memory of a virtual machine running on a server in so-called trusted execution environments or enclaves. The data of the virtual machines are encrypted and decrypted using well-known symmetric cryptographic algorithms on the fly (before being written to the system memory and upon reading from it) using a hardware-based encryption engine, which resides on the CPU, and using cryptographic keys, which cannot be exported from it. This approach, which fully isolates virtual machine memory even from the malicious hypervisor, led to the rise of confidential computing techniques that protect data when processed on untrusted computing resources (e.g., cloud). Similar approaches are introduced to other processor architectures like Arm, RISC-V, and the most recent GPUs. Before confidential computing technologies, applications that needed data-in-use protection on untrusted hardware, like outsourced or secure multiparty computation, used purely cryptographic techniques, which negatively impacted processing performance by several orders of magnitude. Processing data in trusted enclaves protected by confidential computing technologies promises to protect data-in-use while imposing a negligible performance penalty, providing a promising technology for data privacy during processing on untrusted resources, which cloud servers are. In this paper, we provide an overview of current confidential computing concepts and mechanisms for ensuring trust in remote computations, provide insight into the performance of these technologies in machine learning use cases, and give an overview of the recently discovered threats.

Short biography:

PAVLE VULETIĆ obtained his BSc, MSc, and PhD in Computer Systems and Network Architecture from the University of Belgrade, School of Electrical Engineering (ETF). He has worked in all positions from network engineer to the deputy director of AMRES, a national research and education network where he participated in the establishment of the first national CSIRT team. He is currently an associate professor at the ETF teaching Data Security, Computer Systems and Network Security, Advanced Computer Networks, and SDN courses, leads the Laboratory for Information Security, and is the leader of the CoCos.ai project at the ETF. His research interests span from data protection and privacy, network and systems security, network and system performance evaluation to programmable networks, and network and systems management.

ŽARKO STANISAVLJEVIĆ received his BSc, MSc, and PhD degrees in Computer Engineering from the School of Electrical Engineering, University of Belgrade, Belgrade, Serbia, in 2007, 2008, and 2015, respectively. He is currently an Associate Professor with the Department of Computer Engineering and Information Theory and the Deputy Head of the Laboratory for Information Security at the School of Electrical Engineering, University of Belgrade, teaching several courses on computer security and computer architecture and organization. His research interests include data protection and privacy, network and system security, secure software development, computer architecture and organization, and eLearning tools.