

Female Scientists Lecture Series

Lecture by Prof. Dr.-Ing. Alexandra Dmitrienko



TECHNISCHE
UNIVERSITÄT
DARMSTADT

"From
Advantages to
Adversaries:
Safeguarding
Security in
Federated
Machine
Learning"



Prof. Dr. Alexandra Dmitrienko
Head of Secure Software
Systems Research Group
Chair of Software Engineering
(Informatik II), Department of
Computer Science. University
of Würzburg

27.10.2023, 11 am

@ TU Darmstadt

Main Building, (S1 03,R.08)



Privacy and Trust
for Mobile Users

DFG Deutsche
Forschungsgemeinschaft




Abstract:

Prof. Dr.-Ing. Alexandra Dmitrienko

Machine Learning (ML) methods have reached a level of maturity where they are being widely deployed across various domains, aiding users in classification and decision-making tasks. In this talk, we will showcase the numerous advantages ML offers for applications. However, we also stress that it is important to address the security and privacy concerns that arise when utilizing ML methods.

One particular focus of our talk will be on Federated Learning (FL), which is a distributed form of ML that enhances privacy of underlying training data during the training process. We will conduct a comprehensive evaluation of the security and privacy risks associated with FL, delving into the specifics of targeted and untargeted poisoning attacks, as well as the countermeasures employed to mitigate these threats. Our discussion will highlight the ongoing challenges in this field, such as the ability to differentiate between poisoned models and benign but uncommon models, particularly those trained on datasets with different data distributions. We will also address the issue of adaptive attackers who, once aware of the detection method, can add an additional training loss to minimize any changes in the detection metric, effectively evading detection. To stimulate further dialogue and exploration, we will highlight potentials for improvements and outline promising directions to foster productive discussions in the research community.





Short Bio:

Alexandra Dmitrienko is an Associate Professor and head of the Secure Software Systems group at the University of Würzburg in Germany. Before taking her current faculty position in 2018, she collected an extensive background in security institutions in Germany and Switzerland, including Ruhr-University Bochum (2008-2011), Fraunhofer Institute for Information Security in Darmstadt (2011-2015), and ETH Zurich (2016-2017). She earned her PhD in Security and Information Technology from TU Darmstadt (2015), where her dissertation focused on the security and privacy of mobile systems and applications, and was recognized with awards from the European Research Consortium in Informatics and Mathematics (ERCIM STM WG 2016 Award) and Intel (Intel Doctoral Student Honor Award, 2013). Over the years, her research interests spanned across various topics such as secure software engineering, systems security and privacy, security and privacy of mobile, cyber-physical, and distributed systems. Today, her recent research also largely focuses on security and privacy aspects of Artificial Intelligence methods.
