Karlsruhe Institute of Technology

Research Talk Series on Digitalization

Addressing the Dilemma of Insecure Programming Advice with Deep Learning and Behavioral Research

Prof. Jens Grossklags, Ph.D.
Technische Universität München (TUM)

Abstract
Stack Overflow is the most popular discussion platform for software developers. However, recent research identified a large amount of insecure encryption code in production systems that has been inspired by examples given on StackOverflow. By copying and pasting functional code, developers introduced exploitable software vulnerabilities into security-sensitive high-profile applications installed by millions of users every day. Proposed mitigations of this problem suffer from usability flaws and push developers to continue shopping for code examples on Stack Overflow once again. This motivates us to fight the proliferation of insecure code directly at the root before it even reaches the clipboard. By viewing StackOverflow as a market, implementation of cryptography becomes a decision-making problem. In this context, our goal is to simplify the selection of helpful and secure examples. More specifically, we focus on supporting software developers in making better decisions on Stack Overflow by applying nudges, a concept borrowed from behavioral economics and psychology. This approach is motivated by one of our key findings: For 99.4% of insecure code examples on Stack Overflow, similar alternatives are available that serve the same use case and provide strong cryptography. Our system design that modifies Stack Overflow is based on several nudges that are controlled by a deep neural network. It learns a representation for cryptographic API usage pat-terns and classification of their security, achieving average AUC-ROC of 0.99. With a user study, we demonstrate that nudge-based security advice significantly helps tackling the most popular and error-prone cryptographic use cases in Android.

Short CV
Prof. Jens Grossklags, Ph.D., holds the Associate Professorship for Cyber Trust at the Department of Informatics at the Technical University of Munich. He studies security and privacy challenges from the economic and behavioral perspectives with a variety of methodologies. His published research has appeared in high quality publications at technical and social science venues, and has been honored with three best paper awards. Prof. Grossklags received his Ph.D. from the University of California, Berkeley and was a Postdoctoral Research Associate at the Center for Information Technology Policy at Princeton University. He then directed the Security, Privacy and Information Economics Lab, and served as the Haile Family Early Career Professor at the Pennsylvania State University. In addition, Prof. Grossklags has been an invited visiting professor at École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, during the summers of 2011 and 2012, an invited visiting researcher at Copenhagen Business School (CBS) during the summer of 2013, an invited visiting scientist at EURECOM during the summer of 2014, and an invited professor at the IMDEA Software Institute during the summer of 2016.

Date:	May 21st, 2019, 14:00
Location:	KD²Lab
Host(s) of this Talk:	Prof. Dr. Ali Sunyaev (AIFB)

The research talk series on digitalization is co-organized by professors of the three institutes:

aifb IISM INSTITUTE OF INFORMATION SYSTEMS AND MARKETING ksri Karlsruhe Service Research Institute