Karlsruher Institut für Technologie

Institut für Angewandte Informatik
und Formale Beschreibungsverfahren

Kolloquium Angewandte Informatik

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

Prof. Jens Grossklags, Ph.D., Technical University of Munich

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 Stack Overflow. 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 Stack Overflow 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.

Termin: **Dienstag, 21. Mai 2019, 14:00 Uhr**
Ort: **KD²Lab**, Fritz-Erler-Straße 1-3, 76133 Karlsruhe
(Hinweise für Besucher: https://www.kd2lab.kit.edu/59.php)

Veranstalter: Institut AIFB, Forschungsgruppe Critical Information Infrastructures

Zu diesem Vortrag lädt das Institut für Angewandte Informatik und Formale Beschreibungsverfahren alle Interessierten herzlich ein.

A. Oberweis, H. Sack, A. Sunyaev (Org.), Y. Sure-Vetter, M. Volkamer, J. M. Zöllner

Besucheranschrift:
KIT-Campus Süd
Institut AIFB – Geb. 05.20
Kaiserstr. 89
76133 Karlsruhe

Postanschrift:
KIT-Campus Süd
Institut AIFB – Geb. 05.20
76128 Karlsruhe