TU Clausthal

Abschlussvortrag Masterarbeit Ammar Mansuri

„Building a usable cryptographic API“

Prior research has consistently found that cryptographic APIs lacking usability aspects drastically contributes to their misuse, which ultimately leads to security vulnerabilities in software applications. Cryptographic APIs pose critical challenges for the developers, as they require interaction with complicated low-level details. Furthermore, despite the availability of static analysis tools for detecting cryptographic APIs misuses, they often fall short in detecting all the misuses due to the complex nature of cryptographic APIs. We developed SafEncrypt, a high-level wrapper built on top of the native Java Cryptography Architecture (JCA) in Java. The intention behind SafEncrypt is to remove the complexity from developers end, by abstracting away all the low-levels details and provide assistance to integrate secure and usable cryptographic solutions into their software applications in a seamless manner. We conducted an analysis using Halstead complexity measures to determine the difficulty and efforts required to complete a task using SafEncrypt and JCA. The results revealed that tasks in SafEncrypt is half as difficult compared to those done with JCA. Furthermore, we conducted an analysis of SafEncrypt with real-world developers and found that participants with varying levels of experience, from those with no cryptographic APIs experience to experts, were able to securely complete the defined task using SafEncrypt.

Betreuer der Arbeit:	Prof. Dr. Mohammad Ghafari, Prof. Dr. Benjamin Leiding
Datum:	Montag, 23. Oktober 2023, 10:00 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/rooms/f4c-c6c-k02-cay/join