Talks & Abstracts

Eric Bodden, Heinz Nixdorf Institute at Paderborn University and Fraunhofer IEM
Keynote: Managing the Dependency Hell - Challenges and Current Approaches to Software Composition Analysis
Abstract: Most modern software applications comprise more than 90% third-party code, included often as open-source frameworks and libraries. Naturally, these dependencies contain vulnerabilities. Many of these are unknown but as a best effort one should strive to at least remove known vulnerabilities from applications by updating dependencies accordingly. But this is a complex task. For instance, in the Java projects we examined, third-party code is frequently recompiled, repackaged and rebundled, making it hard to even identify which version of which code exactly is part of an application's binary. And even if an app is known to include a vulnerable dependency, how can one determine whether this makes the app itself vulnerable? Last but not least, when recommending dependency updates, how can one assure that this won't break the functionality of the app? I will discuss current research that we conduct jointly with SAP, seeking to address these questions.

Helen Sharp, The Open University
Keynote: Secure code development in practice: the developers' point of view
Abstract: The influence of social and human aspects on all activities related to software development is widely recognised, and understanding software development from the developers' point of view is key to improving both the software development activity and the software that is produced. Developers are at the sharp end of development, and every day make decisions that affect software quality such as its reliability, usability and security. They operate in a dynamic network of technologies, communities, policies, procedures and stakeholders, all of which affect their work, so when seeking to improve the security of code where do you focus? Several issues are pertinent, such as: How do developers perceive security tasks? How does security feature in day-to-day activities? Why do breaches caused by common vulnerabilities still occur? What are the main influences on a developer's secure coding behaviour?
This talk will centre on investigations into questions like these, focusing on the developers' point of view. We worked with practitioners in face-to-face and online settings and developed a view of security in practice that includes a set of security responses that arise out of an interplay between personal factors, task requirements, and the broader organizational environment. Learning to recognise different responses in practice opens the door for individuals, teams and management to understand better how to develop their security culture, and identify any barriers or problems before they materialise.
Building on our studies, we also developed practical materials that help developers connect with subtle, social aspects of security in daily work, and help organisations establish the conditions to enable effective interaction between developers and security specialists. The tutorial workshop that follows this talk will provide attendees the opportunity to explore some of these ideas in their own contexts.

Andreas Zeller, CISPA Helmholtz Center for Information Security
Keynote: Language-Based Fuzzing
Abstract. Common fuzzing techniques work by systematically mutating a set of given inputs, slowly covering more and more of the program code. But if your program has a complex input format, most of these mutations will be *invalid*, resulting in very few inputs reaching code beyond input processing. In this keynote, we will explore techniques to *specify* input languages using grammars, generators, and constraint solvers; and leverage these language specifications to create powerful fuzzers for complex input formats. Includes live coding!
Recommended reads. fuzzingbook.org, notably the chapters "Fuzzing with Grammars", "Fuzzing with Generators", and "Fuzzing with Constraints"

Verena Zimmermann, ETH Zürich
Keynote: Human-Centered Security: Focusing on the human in IT security and privacy research
Abstract: The role of the human for security and privacy is highly relevant, e.g., when it comes to secure authentication, communication, or the detection of phishing e-mails. As such, the human is an important element in today's security-critical systems. Yet, humans have often been considered a weak link as it is finally them who create weak passwords or click on phishing links. Measures to prevent these insecure behaviours include automation, training or the creation of policies. But why do users behave insecurely in the first place? And how can we change that?
This talk first aims to shine light on the psychological aspects of IT security and privacy that help to understand human security behaviour. Second, it will provide examples from different application areas that show how the consideration of human factors can support the design of more usable security and privacy solutions. Third, it will outline a shift in perspective that suggests to go even one step further: Rather than only viewing the human as a weak link to be dealt with, it suggests to view the human as potential solution with regards to security and privacy. The talk will discuss ideas and challenges for enabling the human to be an active contributor to security.