Modern society is dependent on software systems of remarkable scope and complexity. Yet methods for assuring the security and correct functionality of these systems have not kept pace. The result is persistent compromises and failures despite best efforts. This minitrack leverages relationships among security, assurance, and testing for cross-pollination of promising methods and technologies.

In the security area, constantly changing and often vulnerable hardware, software, and data provide many interdependent structures that attackers can exploit. Cybersecurity methods must work together for situational awareness, attack prevention and detection, threat attribution, minimization of consequences, and attack recovery. In the assurance area, it is well understood that defective software cannot be secure, and that assurance technologies must play a central role in cybersecurity approaches. In the testing area, dynamic and static analysis technologies must support both cybersecurity objectives and determination of correct functionality. The Minitrack is comprised of six papers addressing these areas, plus an Open Forum on cybersecurity.

The first paper, Effort Estimates on Web Application Vulnerability Discovery by Hannes Holm, Mathias Ekstedt, and Teodor Sommestad, studies the effort required by a penetration tester to find an input validation vulnerability in a web application that has been developed in the presence or absence of four security measures, based on collecting and combining expert judgments.

In the second paper, Security Tagging for a Zero-Kernel Operating System, Jia Song and Jim Alves-Foss observe that security tagging mechanisms that label memory and registers can help protect system and user software from attacks. They evaluate key features of RTEMS (Real-Time Executive for Multiprocessor Systems) and propose a tagging scheme for securing it as a ZKOS (Zero Kernel Operating System).

The third paper, DART3: DHS Assistant for R&D Tracking and Technology Transfer, by Luanne Goldrich, Stephen Hamer, Christina Selby, and Thomas Longstaff, describes DART3, a web-based semantic tool and repository that captures R&D requirements and R&D project descriptions to help facilitate cybersecurity technology sharing.

In the fourth paper, Classifying Information Systems Risks: What have we Learned so Far?, authors Manuel Wiesche, Hristo Keskinov, Michael Schermann, and Helmut Krcmar apply data mining techniques to the largest and oldest public IS risk database. They differentiate between controllable and recurring risks, and note that the growing complexity and interconnection of IS risks requires a holistic approach to solutions.

In the fifth paper, Exploring Hidden Markov Models for Virus Analysis: A Semantic Approach, Thomas Austin, Eric Filiol, Sébastien Josse, and Mark Stamp compare results from HMM analysis of four compilers, hand-written assembly code, a virus construction kit, and a metamorphic virus. They also develop a dueling HMM Strategy, to leverage knowledge about different compilers for more precise virus identification.

The sixth paper, The Specification, Verification, and Implementation of a High-Assurance Data Structure: An ACL2 Approach, by David Hardin, presents a complete specification and formal verification of a data structure using the ACL2 theorem prover. The paper also demonstrates how the high-assurance specification can be implemented in an imperative programming language, and compares the ACL2 verification to model checking and symbolic execution.

This minitrack also includes an Open Forum that will discuss how software, device, host, network, and cloud security technologies must work together to safeguard the Internet of Things. In other words, “Can’t we all just get along?” Over the next few years, network connectivity will explode to encompass devices of all kinds, and cloud computing and machine-to-machine communication will increase dramatically. The Forum will bring together thought leaders to discuss cybersecurity research needs for these emerging areas.