Abstract:
Auto-active verification occupies a niche between fully automatic analysis and interactive proofs: it targets a high degree of automation (usually powered by SMT solvers), while supporting programmer-friendly user interaction through source code annotations. This talk will describe practical auto-active verification techniques in two problem domains: heap-manipulating object-oriented programs and implementations of security protocols.

Invariant-based reasoning about object-oriented programs becomes challenging in the presence of collaborating objects that need to maintain global consistency. This talk will present semantic collaboration: a methodology to specify and reason about class invariants, which models dependencies between collaborating objects by semantic means. The methodology is implemented in an auto-active verifier for the Eiffel programming language, and evaluated on several challenge programs and a realistic data structure library.

The second part of the talk will describe a technique for verifying high-level security properties of cryptographic protocol implementations within an auto-active program verifier for C. The technique is based on stepwise refinement, and has been used to verify parts of Microsoft's Trusted Platform Module.

Bio:
Nadia Polikarpova obtained her PhD at ETH Zurich in April 2014. Her research interests lie in the area of software correctness, at the intersection of formal methods and software engineering. In particular, her research has contributed to auto-active verification, behavioral interface specifications, automated testing, dynamic invariant inference, and user interface for verification.