Compositional System Security with Interface-Confined Adversaries

Deepak Garg
dg@cs.cmu.edu

Jason Franklin
jfrankli@cs.cmu.edu

Dilsun Kaynar
dilsun@cs.cmu.edu

Anupam Datta
danupam@cmu.edu

March 29, 2010

Compositional security is a recognized central scientific challenge for trustworthy computing. Even if each component of a composite system is secure in isolation, the composed system may not achieve the desired end-to-end security property: an adversary may exploit complex interactions between components to compromise security. Such attacks have shown up in the wild in many different settings, including web browsers, network protocols and application and systems software. While there has been progress on understanding secure composition in specific settings, such as information flow control for non-interference-style properties and cryptographic protocols, a systematic understanding of the general problem of secure composition has not emerged yet.

Our work makes a contribution in this space. We present a formal framework for compositional reasoning about secure systems, incorporating two main insights. First, we posit that a general theory of secure composition should enable one to flexibly model and parametrically reason about different classes of adversaries. A key insight that enables us to develop such a theory is to view a trusted system in terms of the interfaces that the various components expose: larger trusted components are built by combining interface calls in known ways; the adversary is confined to the interfaces it has access to, but may combine interface calls without restriction. Such interface-confined adversaries are precisely modeled in our framework and provide a generic way to model different classes of adversaries. Second, we develop compositional reasoning principles for such systems by extending ideas from rely-guarantee reasoning. While rely-guarantee reasoning was developed for proving correctness properties of known concurrent programs, we extend it to soundly reason about system security in the presence of interface-confined adversaries. These principles generalize prior work on compositional logics for network protocol analysis and secure systems analysis.

At a technical level, the paper presents an expressive concurrent programming language with recursive functions and side-effects for modeling system interfaces and interface-confined adversaries. Security properties (specifically, safety properties) are specified in a new logic of programs. Compositional reasoning principles are codified in the proof system for the logic of programs to support modular reasoning about program specifications, trusted programs whose programs are known, and interface-confined adversarial (untrusted) code. Our main technical result is a proof of the soundness of the proof system with respect to the trace semantics of the logic. We also describe how the proof rules support rely-guarantee reasoning in the presence of adversaries and illustrate the methods by applying them to representative examples of web-based systems and network protocols.