
Our Contribution: The Translation and Verification Process

ProVerif Specifications

ProVerif to JML Specifications

JML Specifications

JML Specifications to Development

Development to Type Checking

Overview

Background: It is vital that computer communication protocols are not only securely designed but also securely programmed. The importance of this problem is exemplified by a recent bug called Heartbleed found in the Transport Layer Security protocol, which is responsible for securing communication between websites and web browsers, that made vulnerable an estimated 24-50% of the 1 million most popular websites [4].

Problem: Verify the implementation (code) of a cryptographic protocol is performing the protocol in accordance with the security properties of the formal specification of that protocol.

Approach: We build upon an existing tool which verifies formal protocol specifications and compile the specifications into implementation language specifications which are then verified by our type checker and an existing implementation language verifier.

Contribution: Existing approaches to this problem fall into two categories. The first category is comprised of solutions that take a protocol specification and translate directly from that specification into a fully implemented program. The second category is comprised of solutions that take a fully implemented program and translate it into a protocol specification which they then attempt to prove is equivalent to the reference protocol specification. Our approach falls into a novel third category of compiling a protocol specification into a set of implementation language specifications. Compared to existing solutions that generate the compiled program from the protocol specification, our tool allows more flexibility in the exact implementation details of the program while avoiding the infeasibility of attempting to translate a program into a protocol specification that is equivalent to the reference.

Our Contribution: Development and Verification

Luke Myers
luke.myers@knights.ucf.edu

Gary T. Leavens
Leavens@ucf.edu

Department of Computer Science

ProVerif

JML Specifications

Development

Overview

References

[4] Zakr Hussain, James Kasten, David Adrian, J. Alex Halderman, Michael Bailey, Frank Li, Nicholas Wroclaw, Anna Asana, Jared Beall, Mathias Payer, and Vern Paxson. The Heartbleed Bug. 2014. ACM.