Verified Secure Implementations for the HTTPS Ecosystem

Invited Talk

Cédric Fournet
Microsoft Research
fournet@microsoft.com

ABSTRACT

The HTTPS ecosystem, including the SSL/TLS protocol, the X.509 public-key infrastructure, and their cryptographic libraries, is the standardized foundation of Internet Security. Despite 20 years of progress and extensions, however, its practical security remains controversial, as witnessed by recent efforts to improve its design and implementations, as well as recent disclosures of attacks against its deployments.

The Everest project is a collaboration between Microsoft Research, INRIA, and the community at large that aims at modelling, programming, and verifying the main HTTPS components with strong machine-checked security guarantees, down to core system and cryptographic assumptions. Although HTTPS involves a relatively small amount of code, it requires efficient low-level programming and intricate proofs of functional correctness and security. To this end, we are also improving our verifications tools (F*, Dafny, Lean, Z3) and developing new ones.

In my talk, I will present our project, review our experience with miTLS, a verified reference implementation of TLS coded in F*, and describe current work towards verified, secure, efficient HTTPS.

See also `https://project-everest.github.io`, `https://mitls.org`, and `https://fstarlang.org`.

PLAS'16 October 24-24 2016, Vienna, Austria

ACM ISBN 978-1-4503-4574-3/16/10.

DOI: http://dx.doi.org/10.1145/2993600.2996279