

Nomination of the paper:

Cracking the Stateful Nut -- Computational Proofs of Stateful Security Protocols using the Squirrel Proof Assistant

By David Baelde, Stephanie Delaune, Adrien Koutsos, and Solène Moreau

Much of the work on formally specifying and verifying security protocols uses the symbolic model. By abstracting from computational complexity and probability, this model facilitates use of formal logic and algebra in automated reasoning, but such results and proofs are not easily connected with the computational model used by cryptographers. To bridge the gap, Bana and Comon-Lundh [CCS'14] introduced Computationally Complete Symbolic Attacker (CCSA) based on first-order logic, that can represent probabilistic Ptime algorithms and attackers. Direct use of the logic is unwieldy and limited to bounded traces. The Squirrel proof assistant is based on an extended logic of unbounded traces over CCSA (dubbed metalogic). This provides a good level of automation for interactive construction of CCSA proofs about trace properties (reachability, including weak secrecy) as well as equivalence/indistinguishability properties (including strong secrecy).

This paper extends the previous work on Squirrel by allowing a notion of states to be modelled. Many protocols are stateful, e.g., using counters and timestamps. The extension is sufficiently powerful to verify a number of RFID protocols, and the paper features a major case study: the protocols of the YubiKey authentication device. These achievements rest on a major theoretical advance, an extension of the logic that supports security arguments mixing reachability and equivalence properties. The theoretical development comprises sophisticated semantic definitions together with proof rules in the form of a sequent calculus.

There are two forms of logical sequents, proving what are called local and global formulas. Local formulas express trace properties of a protocol whereas global formulas can express properties involving multiple protocols.

A key feature of the logic is proof rules for interplay between local and global sequents, which enables proving equivalences on the basis of trace properties and vice versa. For effective automated reasoning the paper introduces bi-terms and bi-formulas which can express properties of pairs of executions, and novel proof rules for reasoning (dubbed bi-deduction) involving bi-formulas.

The main theorems are soundness of all the proof rules, in the sense that anything proved is true with overwhelming probability.

The paper is technically complex but the presentation is effective, based on extensive detailed examples. The significant theoretical contribution is evaluated using an open-source implementation and the applications mentioned earlier.

In light of the significance of the results and the quality of presentation, the work was awarded Distinguished Paper at IEEE CSF 2022, and it is likely to have lasting impact.