SIGACT News Logic Column 20

Riccardo Pucella
Northeastern University
Boston, MA 02115 USA
riccardo@ccs.neu.edu

A short column this time around. Simon Kramer sent me a synopsis of his Ph.D. thesis, defended earlier this year at l'École Polytechnique Fédérale de Lausanne. He introduces a new logic for reasoning about cryptographic protocol called CPL (Cryptographic Protocol Logic). The result is an intriguing blend of modal logic and process algebra, reminiscent of spatial logics for process calculi, but extended with knowledge, belief, and provability operators. Congratulations, Simon.

On a different note, and in a shameless bit of self-promotion, allow me to announce my joining the blogosphere:

`https://wiki.ccs.neu.edu/display/~riccardo/Close+Encounters+of+the+Logical+Kind`

The blog, *Close Encounters of the Logical Kind*, focuses on logic-related curios, especially as applied to Computer Science. Definitely in the spirit of this Column.

Logical Concepts in Cryptography[1]

Simon Kramer
Ecole Polytechnique
Paris, France

Ph.D. Thesis Synopsis

The thesis is about a breadth-first exploration of logical concepts in cryptography and their linguistic abstraction and model-theoretic combination in a comprehensive logical system, called CPL (for *Cryptographic Protocol Logic*). We focus on two fundamental aspects of cryptography. Namely, the security of *communication* (as opposed to security of *storage*) and cryptographic *protocols* (as opposed to cryptographic *operators*). The logical concepts explored are the following. PRIMARY CONCEPTS: the *modal* concepts of belief, knowledge, norms, provability, space, and time.

[1] © Simon Kramer, 2007.

Secondary concepts: belief with error control, individual and propositional knowledge, confidentiality norms, truth-functional and relevant (in particular, intuitionistic) implication, multiple and complex truth values, and program types. The distinguishing feature of CPL is that it unifies and refines a variety of existing approaches. This feature is the result of our *wholistic conception* of property-based (modal logics) and model-based (process algebra) formalisms. We illustrate the expressiveness of CPL on representative *requirements engineering* case studies. Further, we extend (core) CPL (qualitative time) with *rational-valued time*, i.e., time stamps, timed keys, and potentially drifting local clocks, to tCPL (quantitative time). Our extension is conservative and provides further evidence for Lamport's claim that adding real time to an untimed formalism is really simple. Furthermore, we sketch an extension of (core) CPL with a notion of *probabilistic polynomial-time* (PP) computation. We illustrate the expressiveness of this extended logic (ppCPL) on tentative formalisation case studies of fundamental and applied concepts. *Fundamental concepts*: (1) one-way function, (2) hard-core predicate, (3) computational indistinguishability, (4) (n-party) interactive proof, and (5) (n-prover) zero-knowledge. *Applied concepts*: (1) security of encryption schemes, (2) unforgeability of signature schemes, (3) attacks on encryption schemes, (4) attacks on signature schemes, and (5) breaks of signature schemes. In the light of logic, adding PP to a formalism for cryptographic protocols is perhaps also simple and can be achieved with an Ockham's razor extension of an existing core logic, namely CPL.

Moreover, we define: (1) *message meaning*; (2) *message information content*; (3) *protocol meaning*; and, based on all that, (4) *protocol information content.* From the meaning of a cryptographic message, we obtain (1) an equational definition of its *context-sensitivity*, and (2) a *formalisation* of the first of Abadi and Needham's principles for prudent engineering practice for cryptographic protocols. From the meaning of a cryptographic protocol, we obtain natural definitions of the concepts of (1) a protocol *invariant*, (2) protocol *safety*, and (3) protocol *refinement.* Last but not least, we show that *protocol agents* can be conceived as evolving *Scott information systems.*

Keywords applied formal logic, information security.

URL `http://library.epfl.ch/en/theses/?nr=3845`