# *Authentication Logics: New Theory and Implementations*

Lawrence C. Paulson and Roger M Needham, Microsoft Research

Project GR/K77051, funded by the Engineering and Physical Sciences Research Council (EPSRC), was undertaken to provide better tools for verifying security protocols. A new method has been developed in which protocols are modelled inductively [5]. The method has been applied to numerous protocols, such as TLS [6], an Internet protocol descended from SSL 3.0. APM Limited's recursive authentication protocol [2] allows agents to form a chain of arbitrary length. The analysis of this complex protocol, which took only two weeks, identified some flaws. Giampaolo Bella performed an exceptionally detailed formal analysis [1] of Kerberos IV. The Yahalom protocol has an unusually tricky design; by formalizing the relationship between a session key and an encrypted nonce [7], we can show that the compromise of a session key does not lead to cascading losses.

The inductive method uses a simple trace model. A protocol is modelled by an inductive definition consisting of one rule for each step, plus a base case and a rule to model the adversary's actions. The definition is supplied to the proof assistant Isabelle. Theorems are typically proved by induction, which generates a case analysis that considers all possible protocol and adversary actions. Isabelle's rewriting and classical reasoning tools automate much of the work.

Kim Wagner, the first RA, worked on authentication logics. He studied many protocols in order to identify the concepts needed to express their correctness arguments. He devoted much effort to analyzing e-cash protocols and highlighted an obstacle to understanding them. Some of them rely on the virtual impossibility of two unlikely events occurring in conjunction, even though either event could well occur on its own. The probability that two independent events occur together is obtained by multiplying their probabilities; if both are unlikely then their conjunction is highly unlikely. Such probabilistic reasoning remains a challenge for formal methods.

Katherine Eastaughffe, who replaced Wagner, devoted some effort to improving DSTO's XIsabelle, a user interface for Isabelle. Enhancements include a graphical view of proofs as trees, theorem searching facilities, and flexible undoing and re-running of proofs [4]. Her main work [3] was inspired by Ryan and Schneider's attack on an early version of the recursive authentication protocol. Knowledge of one session key could be used to reveal the other keys in that chain: the protocol's implementation of encryption by performing XOR with hash values was wrong. Eastaughffe has modelled XOR in a modification of our theory of messages and proved a crucial secrecy theorem for a modified protocol.

Formal proofs require more effort than does verification using authentication logics or model checking, but they model the protocol at a realistic level of detail. The research has led to several publications. The proof environment is available over the Internet.

## References

[1] G. Bella and L. C. Paulson. Kerberos version IV: Inductive analysis of the secrecy goals. In J.-J. Quisquater, Y. Deswarte, C. Meadows, and D. Gollmann, editors, *Computer Security — ESORICS 98*, LNCS 1485, pages 361–375. Springer, 1998.

[2] J. A. Bull and D. J. Otway. A nested mutual authentication protocol. *Operating Systems Review*, 33(4):42–47, Oct. 1999.

[3] K. Eastaughffe. Algebraic properties of binary xor and the verification of authentication protocols. Technical report, CUCL, 1999. in preparation.

[4] K. A. Eastaughffe. Support for interactive theorem proving: Some design principles and their application. In *UITP'98: User Interfaces for Theorem Provers*, volume 98-08 of *Computing Science Report*, 1998.

[5] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.

[6] L. C. Paulson. Inductive analysis of the Internet protocol TLS. *ACM Transactions on Information and System Security*, 2(3):332–351, Aug. 1999.

[7] L. C. Paulson. Relations between secrets: Two formal analyses of the Yahalom protocol. *Journal of Computer Security*, 9(3):197–216, 2001.