Logical Verification of Security Protocols

M. Carmen Fernández Gago, Michael Fisher, Clare Dixon and Wiebe van der Hoek
Department of Computer Science,
University of Liverpool,
Peach Street, L69 7ZF, United Kingdom
Email: {M.C.Gago,M.Fisher,C.Dixon,wiebe}@csc.liv.ac.uk

1 Introduction

Since the amount of information transferred electronically increases and therefore the sensitivity of the data, there is clearly a need to provide mechanisms that ensure the *security* of the information transferred. This need for security has led to the development of *cryptographic protocols* to verify the authentication of the individuals and messages concerned. A cryptographic protocol is a precisely defined sequence of communication and computation steps that use cryptographic mechanisms such as message encryption and decryption. But even when strong encryption algorithms are used, information is not safe and flaws have been found in protocols considered to be secure. Given the importance of the area, it is vital that techniques are developed which provide fast and automatic analysis of such protocols. *Formal methods* play a key role in analysing security protocols.

One of the first attempts for a method to verify cryptographic protocols was BAN logic [2]. In this paper Burrows, Abadi and Needham introduce a logic to model and to analyse the protocols. The idea is to reason about the beliefs of the agents and how the beliefs evolve during the protocol. Some other techniques are based on model checking [7, 8] or theorem-proving [10].

2 Logics to Reason about Protocols

When using a logical approach, the protocol is replaced by logical formulae (this is called the *idealisation* of the protocol) and then is analysed with a set of inference rules. As we mentioned before the first attempt to model cryptographic protocols was BAN logic. The lack of an automatic tool for this logic has led to some extensions [1, 6]. The majority of these logics have in common that their underlying basis can be seen as a multi-modal logic (typically knowledge, an S5 modal logic, and belief, a KD45 modal logic). However some of the protocols to be verified require more dynamic notations. This has led to the addition of temporal aspects to the logics [12].

A temporal logic of knowledge and belief [3, 9] is a temporal logic enriched with modal connectives for representing the *knowledge* or *belief* of a group of processes. When reasoning about security protocols, it may be necessary to guarantee that a subject will eventually have knowledge or belief during the protocol. For this reason it is useful to combine the logic for knowledge and/or belief with temporal logic [5]. Our intention is to tackle the problem using an authentication logic based on the use of *knowledge* and *belief* combined with time and defining a proof method for the logic based upon resolution [4], which allows us to verify the security protocols. For example, the following is a well known security protocol between two principals A and B from [11].

$$\begin{array}{lcl} A & \rightarrow & B : \{x\}_B \\ B & \rightarrow & A : \{x\}_A \end{array}$$

The first message is that agent A sends to agent B its secret x encrypted with B's public key; A receives later the same message x supposedly from agent B.
The protocol could be specified using a multi-modal logic of knowledge ($S5_n$) fused with a propositional, discrete, temporal logic (PTL). We use special predicates to identify the sending and receipt of messages like *send(A,Msg,Key)* and *rcv(A,Msg,Key)* that are satisfied if agent A sends or receives message Msg encrypted by Key, respectively.

References

[1] M. Abadi and M. Tuttle. A semantics for a logic of authentication. In *Proceedings of the 10th Annual ACM Symposium on Priciples of Distributed Computing*, pages 201–216, 1991.

[2] M. Burrows, M. Abadi, and R. Needham. A Logic for Authentication. In *Proceedings of the Royal Society of London*, volume 426, pages 233–271, 1989.

[3] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning About Knowledge.* MITpress, 1995.

[4] M. Fisher, C. Dixon, and M. Peim. Clausal Temporal Resolution. In *Transactions on Computational Logic 2(1)*, January 2001.

[5] J. Glasgow, G. MacEwen, and P.Panangaden. A Logic to Reason About Security. *ACM Transactions on Computer Systems*, 10(3):226–264, aug 1992.

[6] L. Gong, R. Needham, and R. Yahalom. Reasoning about belief in cryptographic protocols. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pages 234–248. IEEE Computer Society Press, 1990.

[7] G. Lowe. Breaking and Fixing the Needham-Schroeder Public-key Protocol Using csp and fdr. In T. Margaria and B. Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems: Second International Workshop, TACAS '96*, pages 147–166. LNCS, Spinger, 1996.

[8] C. Meadows. The NRL Protocol Analyser: An Overview. *Journal of Logic Programming*, 26(2):113–131, 1996.

[9] J. J. C. Meyer and W. van der Hoek. *Epistemic Logic for Computer Science and Artificial Intelligence*, volume 41 of *Cambridge Tracts in Theoretical Computer Science.* 1995.

[10] Lawrence C. Paulson. The Inductive Approach to Verifying Cryptographic Protocols. *Journal of Computer Security*, 6:85–128, 1998.

[11] R. Ramanujam and S.P. Suresh. Information based reasoning about security protocols. In Jean Goubault-Larrecq, editor, *Electronic Notes in Theoretical Computer Science*, volume 55. Elsevier Science Publishers, 2001.

[12] P. Syverson. Adding Time to a Logic of Authentication. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 97–101. ACM Press, 1993.