Specifying and Verifying Timing Aspects of Security Protocols

Musab A. AlTurki[1,2], Tajana Ban Kirigin[3], Max Kanovich[4,5], Vivek Nigam[6,7], Andre Scedrov[8,5], Carolyn Talcott[9]

[1] *King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia*
[2] *Runtime Verification Inc., USA*
[3] *University of Rijeka, Department of Mathematics, Rijeka, Croatia*
[4] *University College London, London, UK*
[5] *National Research University Higher School of Economics, Moscow, Russia*
[6] *Federal University of Paraíba, João Pessoa, Brazil*
[7] *fortiss, Munich, Germany*
[8] *University of Pennsylvania, Philadelphia, PA, USA*
[9] *SRI International, Menlo Park, CA, USA*

Keywords:
Multiset Rewriting, Security Protocols, Dolev-Yao Intruder, Distance-Bounding Protocols, Computational Complexity

Protocol Security Verification is one of the greatest success stories of formal methods. Indeed, a number of attacks on security protocols have been found using formal methods. Tools are used in the automated discovery of new attacks and the shaping of new protocols. However, some aspects relevant to protocol security are not covered by many formal models. Time is one of such important aspects.

We describe the use of Multiset Rewriting for the specification and verification of timing aspects of protocols, such as network delays, processing time, timeouts, timed intruder models and distance bounding properties. We investigate such timed features and specify these timing aspects of security protocols using multiset rewriting with real time. We formalize timed Dolev-Yao intruder theories, as well as network and protocol theories that take into account physical laws related to time.

We also investigate related verification problems, such as the secrecy problem and the false acceptance and the false rejection problems related to Distance-Bounding Protocols. We describe decidable fragments of our framework for the specification and verification of timing properties of security protocols and provide PSPACE complexity results.

Acknowledgments

Part of this work was done during the visits to the University of Pennsylvania by Alturki, Ban Kirigin, Kanovich, Nigam, and Talcott, which were partially supported by ONR grant N00014-15-1-2047 and by the University of Pennsylvania. Ban Kirigin is supported in part by the Croatian Science Foundation under the project UIP-05-2017-9219. Scedrov is partially supported by ONR grants N00014-15-1-2047 and N00014-18-1-2618. The participation of Kanovich and Scedrov in the preparation of this article was partially within the framework of the HSE University Basic Research Program funded by the Russian Academic Excellence Project '5-100'. Talcott is partly supported by ONR grant N00014-15-1-2202 and NRL grant N0017317-1-G002. Nigam is partially supported by NRL grant N0017317-1-G002, and CNPq grant 303909/2018-8.

References

[1] M. A. Alturki, M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Statistical model checking of distance fraud attacks on the Hancke-Kuhn family of protocols. In *Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy*, pages 60–71. ACM, 2018.

[2] M. I. Kanovich, T. Ban Kirigin, V. Nigam, and A. Scedrov. Bounded memory Dolev-Yao adversaries in collaborative systems. *Inf. Comput.*, 238:233–261, 2014.

[3] M. I. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, and C. Talcott. Time, computational complexity, and probability in the analysis of distance-bounding protocols. *Journal of Computer Security*, 25(6):585–630, 2017.

[4] D. Pavlovic and C. Meadows. Bayesian authentication: Quantifying security of the Hancke-Kuhn protocol. *Electronic Notes in Theoretical Computer Science*, 265:97–122, 2010.