Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols

Max Kanovich[1,5], Tajana Ban Kirigin[2], Vivek Nigam[3], Andre Scedrov[4,5] and Carolyn Talcott[6]

[1]Queen Mary, University of London & University College, UK
[2]University of Rijeka, HR
[3]Federal University of Paraíba, Brazil
[4]University of Pennsylvania, USA
[5]National Research University Higher School of Economics, Russia
[6]SRI International, USA

June 30, 2015

Keywords:

Cyber-Physical Security Protocols, Multiset Rewriting, Computational Complexity

Many security protocols rely on the assumptions on the physical properties in which its protocol sessions will be carried out. For instance, Distance Bounding Protocols take into account the round trip time of messages and the transmission velocity to infer an upper bound of the distance between two agents. We classify such security protocols as Cyber-Physical. Time plays a key role in design and analysis of many of these protocols. This paper investigates the foundational differences and the impacts on the analysis when using models with discrete time and models with dense time. We show that there are attacks that can be found by models using dense time, but not when using discrete time. We illustrate this with a novel attack that can be carried out on most distance bounding protocols. In this attack, one exploits the execution delay of instructions during one clock cycle to convince a verifier that he is in a location different from his actual position. We propose a Multiset Rewriting model with dense time suitable for specifying cyber-physical security protocols. We introduce Circle-Configurations and show that they can be used to symbolically solve the reachability problem for our model. Finally, we show that for the important class of balanced theories the reachability problem is PSPACE-complete.

References

[1] M. Kanovich, T. Ban Kirigin, V. Nigam, A. Scedrov, C. Talcott, *Discrete vs. Dense Times in the Analysis of Cyber-Physical Security Protocols*, 4th Conference on Principles of Security and Trust (POST), London, UK, April 2015. Springer LNCS, Volume 9036, Springer-Verlag, 2015, pp. 259 - 279.