Time-Bounding Needham-Schroeder Public Key Exchange Protocol

Max Kanovich, Queen Mary, University of London, UK
Tajana Ban Kirigin, University of Rijeka, Croatia
Vivek Nigam, Federal University of Paraíba, João Pessoa, Brazil,
Andre Scedrov, University of Pennsylvania, USA

We consider some properties of timed models for protocol specification and verification and address the non-trivial relation between models with discrete time and models with continuous time. Although discrete time is suitable for some applications such as [7], it is just an abstraction of physical time. In other instances normal physical reality plays an essential role. This is the case with *cyber-physical security protocols* which take into account the physical properties of the environment where its protocol sessions are carried out. For instance, Distance Bounding Protocols such as [1] are cyber-physical security protocols which infer an upper bound on the distance between two agents from the round trip time of messages. The common feature in most cyber-physical security protocols is that they mention cryptographic keys, nonces and time.

We investigate the motivation and the need of using continuous time models in protocol verification instead of the more simple discrete ones and show that in protocol verification these models behave differently.

In our recent work [5, 6] we presented some first steps towards building general timed models for cyber-physical security protocols verification. We proposed a language based on multiset rewriting which extends the security protocols framework [2, 4] with continuous time. We also proposed a novel intruder model based on the Dolev-Yao [3] which takes into account the *physical properties* of the environment that the intruder is in. We then showed that the reachability problem for Bounded Memory Cyber-Physical Security Protocols in presence of a Memory Bounded Intruder is PSPACE-complete [5, 6].

We show that protocol verification models with discrete time behave differently when compared to models with continuous time. In particular, there are protocols for which no attack can be found when using a model with discrete time, but there is an attack when using a model with continuous time (or even dense time). This means that, in general, one has to be careful when using models with discrete time in protocol verification as such models may not able to expose some protocol security flaws that models with continuous time would show.

We illustrate the main subtleties by adding the dimension of time to the original flawed *Needham-Schroeder* public key protocol. We address the basic issues that arise in the formalization of protocols with explicit time, namely the time-sensitive features such as the *network delays* and *participants' processing time* are taken into account. Also, protocol execution depends on the round trip time of messages by means of *measuring the response time*.

The intriguing result is that this *Time-bounding Needham-Schroeder protocol* is *secure* in the discrete time model, while it is *insecure* in the continuous time model. We consider various scenario assumptions and show that the security properties of our Time-bounding Needham-Schroeder protocol depend on whether time is considered discrete or continuous as well as on network delay and internal processing time.

These results hold already with respect to an adversary which is able to intercept and send messages, as well as encrypt and decrypt messages providing he has the corresponding keys. Such an adversary does not need to manipulate various submessages or even create fresh values. Here, as all the participants in the protocol execution, the adversary is subject to non-zero network delays and non-zero processing time.

The actual difference between discrete and continuous time models lays in the fact that inbetween two moments in time, an unbounded number of timed events are possible within continuous time, whereas only a finite number of acts could happen within discrete time model. In other words, discrete time models implicitly impose lower bounds on transmission and processing time. This is not the case in models with continuous time. Indeed, continuous time (or even dense time) allows us to not have such bounds. Nevertheless, lower bounds for delays for both processing time and for traversal time can be introduced in continuous time models. We investigate such scenarios as well, and show that there is a difference between the models even with lower bounds imposed.

In the future work we plan to consider extensions and alternative intruder and protocol models reflecting various technologies and *e.g.* scenarios with agents that are allowed to move. Another assumption of our model is that all agents share a global clock. Although this is reasonable for some applications, such as distance bounding protocols, it is not the case for others such as Network Time Protocols.

Finally, we point out that no rescaling of discrete time units removes the presented difference between the models. Namely, for any discretization of time, such as days, seconds or any other infinitesimal time unit, there is a protocol for which there is an attack with continuous time and no attack is possible in the discrete case. This novel result illustrates the challenges of timed models for cyber-physical security protocol verification.

Acknowledgments: Nigam is supported by the Brazilian Research Agency CNPq. Scedrov is supported in part by the AFOSR MURI "Science of Cyber Security: Modeling, Composition, and Measurement" as AFOSR Grant No. FA9550-11-1-0137. Additional support for Scedrov from NSF Grant CNS-0830949 and from ONR grant N00014-11-1-0555.

During the work on these results Kanovich and Scedrov were visiting the National Research University Higher School of Economics, Moscow. They would like to thank Sergei O. Kuznetsov for providing a very pleasant environment for work.

References

[1] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT*, 1993.

[2] I. Cervesato, N. A. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov. A meta-notation for protocol analysis. In *CSFW*, pages 55–69, 1999.

[3] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[4] N. A. Durgin, P. Lincoln, J. C. Mitchell, and A. Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, 12(2):247–311, 2004.

[5] M. I. Kanovich, T. B. Kirigin, V. Nigam, A. Scedrov, C. L. Talcott, and R. Perovic. A rewriting framework for activities subject to regulations. In *RTA* 2012.

[6] M. Kanovich, T. B. Kirigin, V. Nigam, and A. Scedrov. Towards timed models for cyber-physical security protocols. In *FCS-FCC* 2014.

[7] V. Nigam, T. B. Kirigin, A. Scedrov, C. Talcott, M. Kanovich, and R. Perovic. Towards an automated assistant for clinical investigations. In *IHI* 2012.