Security Analysis of Network Protocols

John Mitchell
Stanford University, USA

This series of lectures will provide an introduction to network protocols that have security requirements. We will cover a variety of contemporary security protocols and give students information needed to carry out case studies using automated tools and formal techniques. The first lectures will survey protocols and their properties, including secrecy, authentication, key establishment, and fairness. The second part will cover standard formal models and tools used in security protocol analysis, and describe their advantages and limitations. In addition to fully automated finite-state model checking techniques, we will also study other approaches, such as constraint solving, process algebras, and a protocol logic that has been used to develop proofs for a number of large, widely used network protocols. While prior knowledge of networking and cryptography may be helpful, a short overview of needed cryptography will be included. This is a fun topic, since practical protocols tend to have subtle flaws that can be discovered by systematic means.

Students interested in looking at material prior to the Summer School can start with paper [2] below. The CS259 course web site (reference [5]) has sample lectures and student projects that represent the kind of topics and case studies that we will discuss.

References

1. J.C. Mitchell, M. Mitchell, and U.Stern. *Automated Analysis of Cryptographic Protocols Using Murphi*, IEEE Symp. Security and Privacy, Oakland, pp. 141-153, 1997.
2. J.C. Mitchell, V.Shmatikov, and U. Stern. *Finite-State Analysis of SSL 3.0*, Seventh USENIX Security Symposium, San Antonio, pp. 201-216, 1998.
`(http://theory.stanford.edu/people/jcm/papers/ssl-usenix.ps)`
3. A. Datta, A. Derek, J. C. Mitchell, A. Roy. *Protocol Composition Logic (PCL)*, Electronic Notes in Theoretical Computer Science (Gordon D. Plotkin Festschrift), to appear 2007.
`(http://www.stanford.edu/ danupam/ddmr-pcl06.pdf)`
4. A. Datta, A. Derek, J.C. Mitchell, V. Shmatikov, and M. Turuani. *Probabilistic polynomial-time semantics for a protocol security logic*, 32nd International Colloquium on Automata, Languages and Programming (ICALP '05), 2005.
5. Related material may be found at: `http://www.stanford.edu/class/cs259/`