Anupam Datta
Research Scientist
Team for Research in Ubiquitous Secure Technology (TRUST), SCS
4 September 2007

Research Topic
Computer Security

Research Problem
What does it mean for a network to be secure?

Problem Statement
Given a body of research in the area of Computer Security, construct a definition of secure that can be used to measure the quality of different proofs and protocols.

Problem Description
Define the theoretic basis for security practice. This includes defining what secure means in the context of network communication. Given a definition determine if a system is secure. Proofs and protocols are used to verify the security of machines accessing the network. Different proofs and protocols are better than others under certain conditions and assumptions.

Computer Science Perspective
This is an important issue in computer science as people rely more and more on electronic, networked communication and less on face-face communication. This research is central to maintaining secure computer networks widely used in banking, defense, and many other applications.

Disciplines Actively Involved
Mathematics

Other Discipline Involved
Cryptography is widely used in this research. Cryptography is an application of abstract algebra (mathematics) that studies message secrecy. Issues in complexity theory and information theory are also used in this research.

Actively Involved Discipline is defined as a discipline associated with an investigator working on the research problem.

References

- A. Barth, A. Datta, J. C. Mitchell, S. Sundaram, Privacy and Utility in Business Processes, to appear in *Proceedings of 20th IEEE Computer Security Foundations Symposium*, July 2007. [Paper]

- A. Barth, A. Datta, J. C. Mitchell, H. Nissenbaum, Privacy and Contextual Integrity: Framework and Applications, in *Proceedings of 27th IEEE Symposium on Security and Privacy* , pp. 184-198, May 2006. [Paper]
- A. Roy, A. Datta, A. Derek, J. C. Mitchell, Inductive Proofs of Computational Secrecy, to appear in *Proceedings of 12th European Symposium On Research In Computer Security* , September 2007.
- A. Datta, A. Derek, J. C. Mitchell, A. Roy, Protocol Composition Logic (PCL), to appear in *Electronic Notes in Theoretical Computer Science (Gordon D. Plotkin Festschrift),* 2007. [Paper]
- A. Roy, A. Datta, A. Derek, J. C. Mitchell, Inductive Trace Properties for Computational Security, to appear in *Proceedings of ACM SIGPLAN and IFIP WG 1.7 7th Workshop on Issues in the Theory of Security,* March 2007. (Invited to *Special Issue of Journal of Computer Security*). [Paper]
- A. Datta, R. Küsters, J. C. Mitchell, A. Ramanathan, On the Relationships between Notions of Simulation-based Security, in *Proceedings of Theory of Cryptography Conference, Lecture Notes in Computer Science, Vol. 3378,* pp. 476-494, February 2005. [Paper]

By imccullo
Updated imccullo