Modularity in Computer Security

By: Anupam Datta
March 30, 2010

Abstract:
Compositional security is a recognized central scientific challenge for trustworthy computing. Contemporary systems are built up from smaller components. However, even if each component is secure in isolation, the composed system may not achieve the desired end-to-end security property: an adversary may exploit complex interactions between components to compromise security. Such attacks have shown up in the wild in many different settings, including web browsers and infrastructure, network protocols and infrastructure, and application and systems software. This talk will report on progress on applying programming language methods to address this problem. Specifically, I will describe Protocol Composition Logic (PCL), a logic for proving security properties of network protocols that use public and symmetric key cryptography. PCL supports compositional reasoning about complex security protocols and has been applied to a number of industry standards including SSL/TLS, IEEE 802.11i and Kerberos V5. I will also report on our recent work that generalizes these ideas to develop a systematic theory of compositional security for system designs that could be applied to other classes of systems, for example, web browser security and trusted computing systems. I will also report on the connections and influence of this work on two other significant approaches to compositional security --- Universal Composability at IBM Research and the F7 project at Microsoft Research.

About the Speaker:
Anupam Datta is a Research Scientist for CyLab. He joined the research faculty at Carnegie Mellon in April 2007. He is affiliated with the Security and the Principles of Programming groups. Dr. Datta's research focuses on foundations of information security and privacy, and draws on methods from a broad range of fields including logic, programming languages, verification, cryptography, and game theory. Specific research topics include cryptographic protocols, privacy, and trustworthy systems. Dr. Datta has a PhD in Computer Science from Stanford University and a BTech from IIT Kharagpur.