Abstract: The insider problem is considered one of the most serious in computer security. But the precise definition of "insider" varies, sometimes wildly, among researchers. The result is that the problem, in its broadest sense, is ill-defined. This talk examines several different aspects of the different definitions and situations broadly classified as "insiders" and develops a definition based on policy models. We then examine the application of process modeling and subsequent analyses to the insider problem. We look at the agents who are carrying out particular tasks, perform different analyses to determine how the process can be compromised, and suggest countermeasures that can be incorporated into the process model to improve its resistance to insider attack.

Biography: Matt Bishop received his Ph.D. in computer science from Purdue University, where he specialized in computer security, in 1984. He is on the faculty at the Department of Computer Science at the University of California at Davis. His main research area is the analysis of vulnerabilities in computer systems, including modeling them, building tools to detect vulnerabilities, and ameliorating or eliminating them. Currently, he is examining data sanitization, modeling election processes, attribution, and the "insider" problem. He is also co-leading a project studying improvements to the teaching of robust (aka "secure") programming. He has been active in the area of UNIX security since 1979, and has presented tutorials at SANS, USENIX, and other conferences. His textbook, Computer Security: Art and Science, was published in December, 2002 by Addison-Wesley Professional. He also teaches software engineering, machine architecture, operating systems, programming, and computer security.