

The Future of Incident Response
March 2007

Dr. Thomas A. Longstaff
Deputy Director, CERT
Software Engineering Institute, Carnegie Mellon University

Abstract

From the earliest days of networked computing, we have counted on a collection of computer security experts to watch for anomalous activity, track down the source of the attacks, and bring the network intruders to justice. Cliff Stoll, "The Cuckoo's Egg", documents a good review of how this used to work. Today, attacks are fully automated, vulnerability seeking weapons that hide in our normal activity and attack from our homes and offices around the world. These attacks are beyond the abilities of traditional firewalls or intrusion detection systems to mitigate. Responding to these attacks has completely changed the nature of our reaction from investigating a single attack to a complex distributed analysis process designed to inform our enterprise security staff of immanent threat. In this presentation, I will describe how recent advances in detection and analysis capabilities have enhanced our ability to preempt some attacks and how we can use that information to better protect our systems.