Toward a Culture of Cyber Security Research

Aaron Burstein

Computer and network security (together, "cyber security") have become matters of major economic, social, and national security importance. Present-day attacks on computer systems and networks do not simply disrupt individuals' access to the Internet, an isolated machine, or even a single enterprise's network. Instead, modern attacks target infrastructure that is integral to many facets daily life. Computer networks have joined agriculture, water, transportation, energy, and other resources as critical resources for the functioning of the national economy. Indeed, computer networks tie many of these pieces of infrastructure together. At the same time that networked computing devices are becoming more pervasive, the pace and sophistication of these attacks are increasing. These problems have spawned vigorous research efforts and generated vast quantities of data, but researchers face a common problem: access to usable data. Specifically, security researchers face considerable legal, institutional, and economic obstacles to acquiring, analyzing, and even discussing security-related data. These obstacles place an undue burden on researchers and threaten to impede valuable scientific research. Although other scientific fields -- medicine and public health, for example -- face a similar set of issues, particularly with respect to individual privacy, they have developed ways to manage them. In these fields, the law facilitates research, or at least provides sufficient room for it to occur. In other words, the law contributes to a culture of research. Security research is different. The principal laws that regulate communications privacy do not have research exceptions, making useful datasets scarce and difficult to exchange among researchers. Collecting data that are not subject to these laws can expose researchers to liability for violating laws ranging from copyright to trademark to computer abuse. Moreover, publishing the findings of security research has been constrained by concerns about facilitating crime or violating copyright law. Legal change alone cannot remove all of the obstacles that security researchers face; but a coherent notion of cyber security and changes to a relatively small number of laws would greatly clarify access-to-data issues and create a more favorable environment for research, without compromising the main purposes that those laws serve. Without these changes, security researchers will continue struggling to keep up with their adversaries.