PROJECT SUMMARY:
Center for Internet Epidemiology and Defenses

Since 2001, large-scale Internet epidemics — “worm” and “virus” outbreaks — have profoundly demonstrated the threat posed by self-propagating programs. The combination of widespread software homogeneity and the Internet’s unrestricted communication model creates an ideal climate for infectious pathogens, and, worse, each new generation of outbreaks demonstrates increasing speed, virulence, and sophistication. Indeed, a recent Computing Research Association panel framed eliminating epidemic-style attacks from the Internet within 10 years as a Grand Challenge problem.

The Center for Internet Epidemiology and Defenses is dedicated to answering this challenge. The Center aims to address twin fundamental needs: to better understand the behavior and limitations of Internet epidemics, and to develop systems that can automatically defend against new outbreaks in real-time.

Understanding the scope and emergent behavior of Internet-scale worms seen in the wild constitutes an emerging new science termed Internet epidemiology. In this context, the Center pursues: (i) understanding how in reality worms propagate on an Internet scale and how these dynamics interact with the distribution of vulnerabilities, network resources and network topology; (ii) devising a global-scale early warning system to detect incipient network epidemics – both to aid in future defense systems and to dynamically activate heavy-weight monitoring infrastructures for analyzing fine-grained interactions; and (iii) large-scale forensics such as “Patient 0” analysis and attribution. Key tools in this pursuit are the Center’s construction and operation of a distributed network telescope of unprecedented scale that in turn feeds a honeyfarm collection of vulnerable “honeypot” servers whose infection serves to indicate the presence of an Internet-scale worm.

Detecting worms is only half the story. The Center also aims to develop mechanisms to derive signatures of a worm’s activity — based either on analysis of honeyfarm behavior, or traffic dynamics seen locally within an enterprise — and disseminate these globally to worm suppression devices.

Finally, it is crucial to keep in mind that the problem of Internet epidemics is of major practical import as well as pure intellectual challenge. It is vital that the research not exist in a vacuum. It instead must embrace the need to address potentially thorny, but highly relevant, “real-world” issues of informing the development of: first, legal frameworks in terms of the appropriate use of the technologies and their application in terms of providing forensic evidence, while also integrating the need to address privacy concerns; and, second, the potential synergies with enabling the development of economic actuarial models for quantifying exposure to aggregate risk and liability from Internet epidemics. Such quantitative models are critical for supporting the emerging cyber-insurance industry and consequently for providing economic incentives for corporate investment in deploying new defense technologies.

Intellectual merit: Modern network-borne epidemics are entities of such scale that their study in fact constitutes a new empirical science, one requiring a fusion of innovative distributed sensing techniques, detailed behavior analysis, new theoretical frameworks, ambitious reactive real-time systems, and critical legal and economic considerations. The issues that arise are fundamentally both hard and unique in scope: we must defend not a single resource against a class of attacks, but the global population of resources against classes of attacks that will by sheer force of scale cast such a wide net that they automatically spread to where defenses are weakest.

Broader impact: Simply put, the Center’s efforts are germane to the effective future functioning of the global Internet, affecting 100s of millions of computers throughout the world. The Center does not aim to address this problem merely in the abstract, but to grapple with the pragmatics of developing technologies and policies with direct applicability to the operational network. In addition, the Center aims to construct a solid foundation for the future of this burgeoning field via education across the spectrum from undergraduates exploring their interests, to graduates specializing in network security, to practitioners already immersed in the realities of incessant Internet attacks.