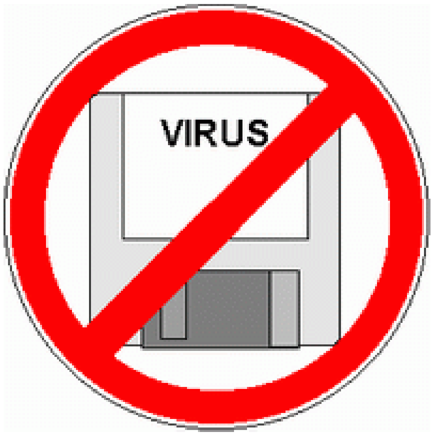
# California Scientists Wage Joint War on Internet Plagues

September 21 2004



Computer scientists at the University of California, San Diego and the International Computer Science Institute, affiliated with UC Berkeley, have joined forces to launch **a full-scale assault on viruses, worms and other plagues afflicting the** Internet. With $6.2 million in funding over five years from the National Science Foundation (NSF) through its new Cyber Trust program, the scientists will develop technologies to detect, analyze and defend against large-scale Internet attacks.

The Center for Internet Epidemiology and Defenses (CIED) will be co-located in San Diego and Berkeley, CA. It will tackle what has been called a grand challenge problem for computer security researchers: defending against epidemic-style attacks. "The very openness and efficiency that drove the Internet's success also make it an ideal breeding ground for infectious network agents," said Stefan Savage, the center's Project Director and a professor in the Computer Science and Engineering department of UCSD's Jacobs School of Engineering. "Infection is spread via contact and the Internet allows a host infected in one place to rapidly contact any other system on the planet. A new worm can become a massive outbreak in minutes -- or even seconds. In fact, the speed of some Internet pathogens is so great that only fully automated defenses can even hope to keep up. Building such defenses is our ultimate goal."

According to fellow principal investigator Vern Paxson of ICSI, at the core of any effective defense will be a better understanding of the fundamental capabilities, characteristics and limitations of epidemic attacks. "It is easy to build a defense against one particular known virus or worm; this is what we do now," said the senior researcher, who will lead CIED activities at ICSI's Center for Internet Research (ICIR), "But to stop whole classes of these pathogens requires far more insight into what it means to be an epidemic and how infectious behavior stands apart from legitimate use."

CIED is one of two Cyber Trust Centers created today in the inaugural round of funding from the $30 million program created last December by the NSF. They were chosen from among 25 full proposals submitted by leading U.S. research institutions. The second is the Security Through Interaction Modeling (STIM) Center, based at Carnegie Mellon University. STIM will focus on deeper understanding of the Internet's 'ecology' in order to build better security defenses. "The Cyber Trust program promotes research into more dependable, accountable and secure computer and network systems," said Carl Landwehr, NSF program director for Cyber Trust. "These activities are looking not only for new ways to cope with imperfections in today's systems, but also for the knowledge and techniques to build better systems in the future."

In addition to the NSF's funding, CIED will also receive support from Microsoft, Intel and Hewlett-Packard, as well as from UCSD's Center for Networked Systems, a recently-created $10 million research center funded by AT&T, Alcatel, Hewlett-Packard and QUALCOMM. Co-principal investigators on the project include ICSI researcher Nicholas Weaver, and professors Geoffrey M. Voelker and George Varghese from UCSD's Computer Science and Engineering department. The center will also fund research activities at the San Diego Supercomputer Center (SDSC) and the Cooperative Association for Internet Data Analysis (CAIDA), and will collaborate with the California Institute for Telecommunications and Information Technology [Cal-(IT)2].

CIED's research efforts revolve around measuring and analyzing live Internet epidemics and then using the insights gained to develop ever more robust defense mechanisms. To gain visibility into pathogens propagating across the global Internet, CIED members say a top priority for the center's first year will be the construction of large-scale monitoring instruments - 'network telescopes' and 'network honeyfarms' - to provide early warning of incipient outbreaks, to measure the dynamics of epidemics as they spread, and to collect forensic data about the modes and methods of attackers.

To provide statistically meaningful data on short time-scales, CIED plans to push this distributed monitoring effort to unprecedented scales by monitoring attacks across millions of potential Internet systems at once. From this data, center researchers plan to craft practical solutions to counteract new outbreaks on the Internet before they reach pandemic levels. Among these initial defenses, the center will develop algorithms for automatically deriving signatures of new worms and viruses, as well as mechanisms to detect and suppress infectious communication behaviors. Researchers will also address real-world legal issues -- including privacy, insurance exposure to large-scale Internet outbreaks, and the treatment of forensic evidence -- that arise from CIED's plan for distributed data collection, filtering, analysis, suppression and prototype defense mechanisms.

In addition to its core research mission, CIED will initiate significant efforts in education and workforce development and will coordinate with ongoing outreach activities on both campuses. The center's researchers will incorporate their results into undergraduate and graduate courses and curricula, and will present their research annually at a center-organized outreach workshop.

Source: University of California - San Diego

Citation: California Scientists Wage Joint War on Internet Plagues (2004, September 21) retrieved 15 August 2024 from https://phys.org/news/2004-09-california-scientists-wage-joint-war.html