IT & Security

Advances in computer and communications technologies have formed the basis for global economic growth and an increase in our standard of living for more than two decades. We rely on information technology in all aspects of our daily life, and with this reliance comes the need to make information systems more secure, trustworthy, sustainable, and available in the face of both intentional attacks and accidental faults. That's why Carnegie Mellon launched CyLab, a broad new IT security initiative that builds on the university's decades of leadership in the field, leadership cultivated at the institutes detailed on this page, from the Software Engineering Institute's world-renowned CERT/CC computer emergency response team to the Laboratory for Data Privacy's work to keep personal information safe and secure.

CyLab: Carnegie Mellon CyLab is a bold and visionary effort aimed at creating a public-private partnership to develop new technologies for measurable, available, secure, trustworthy and sustainable computing and communications systems and to educate individuals at all levels. CyLab is a university-wide, multidisciplinary initiative involving more than 200 faculty, students and staff, and builds on more than two decades of Carnegie Mellon's leadership in Information Technology. Through its close connection to the CERT/CC, CyLab also works closely with US-CERT, a partnership between the Department of Homeland Security's National Cyber Security Division (NCSD) and the private sector, to protect our national information infrastructure. CyLab is an active participant in the Pittsburgh Regional Cyber Team, in which foundations, universities, businesses, and economic development organizations have conducted a path breaking analysis of the growth and development of the cybersecurity industry in the US. *www.cylab.cmu.edu*

CERT Coordination Center: Established in 1988 as the first computer security incident response team, the CERT/CC is internationally recognized as a trusted reporting center for cyber security incidents and technology vul-

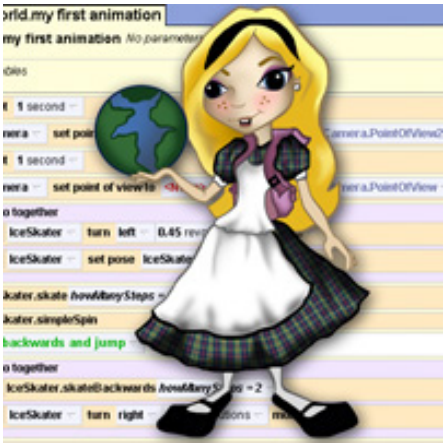
Carnegie Mellon Researchers Awarded NSF Grant to Develop Secure Internet Architecture

Researchers at Carnegie Mellon University will lead a three-year, $7.1 million effort sponsored by the National Science Foundation (NSF) to develop a next-generation network architecture that fixes security and reliability deficiencies now threatening the viability of the Internet. "Obviously, a lot of wisdom is embedded in the current Internet and we'll retain that. But parts of it are clearly broken and can't be fixed with incremental steps," Peter Steenkiste, professor of computer science and electrical and computer engineering. The eXpressive Internet Architecture (XIA) Project, one of four new projects funded through the Future Internet Architecture Program of the NSF's Computer and Information Science and Engineering (CISE) Directorate, will include features that will help users find the content they seek wherever it is most accessible, speeding information retrieval while easing network traffic.

Carnegie Mellon
Office of Government Relations

Pittsburgh office: 412.268.7778
Washington, D.C. office: 202.547.8515
email: governmentrelations@cmu.edu
Web: www.cmu.edu/govrel

Carnegie Mellon, FBI Announce Competition Promoting Internet Safety Awareness



Carnegie Mellon University and the Federal Bureau of Investigation today announced a national competition, in which students will share their knowledge about how to avoid dangers associated with Internet use by creating computer animations that promote safety concepts. The animation competition is the latest component of the FBI's ongoing Safe Online Surfing (SOS) Program developed by the FBI's Cyber Division and Nova Southeastern University. The SOS Program delivers critical Internet safety information to third- through eighth-grade students. More than 70,000 children in 41 states have completed the program, which fosters fun competition between local schools.

nerabilities. The CERT/CC alerts the Internet community to potential threats the security of their systems and provides information about how to avoid, minimize or recover from the damage. *www.cert.org*

The Survivable Enterprise Management Group: This group seeks ways to build security and survivability into systems before they are deployed. The staff defines and transitions organizational and technical security practices and methodologies to help government, nonprofit and private organizations evaluate, improve and maintain the security their systems.

Laboratory for International Data Privacy: The LIDAP is an interdisciplinary research group dedicated to exploring, assessing and creating technology that provides scientific assurances of anonymity in data. Its findings are providing the intellectual basis needed to shape the inform policy dealing with evolving relationship between technology and the legal right to or public expectation of privacy in the collection and sharing of data. *http://privacy.cs.cmu.edu*

Information Networking Institute: INI offers professional graduate degree programs in information networking, information security, and information technology that integrate technologies, economics, and policies of secure communication networks. The INI is also the education partner of Carnegie Mellon CyLab, a university-wide, multidisciplinary research center. As part of its globalization strategy, the INI offers professional degree programs at partner institutions in both Europe and Asia: Athens Information Technology in Athens, Greece, and the Hyogo Institute of Information Education Foundation at Carnegie Mellon CyLab Japan in Kobe, Japan. *www.ini.cmu.edu*

Center for Broadband and Wireless Networking: Founded in 2001, this interdisciplinary center is focused on research and education in advanced networking concepts and systems with an emphasis on industrial relevance. The center's work melds many of Carnegie Mellon's existing strengths including: interdisciplinary research, wired networks, wireless networks, and optical devices and signal processing. *www.ece.cmu.edu/research/areas.html*

Center for the Computational Analysis of Social and Organizational Systems: Using a mix of social and computer sciences, researchers at CASOS are attempting to understand and model the way groups are structured, communicate and interact. Through modeling of two distinct groups: the human group institution or society and the multi-agent artificial computational system, new insights into the fundamental principles of organizing, coordinating and managing multiple information processing agents are gained. The center currently has five research thrusts: organizational design; adaptation and evolution; social and organizational networks; e-commerce and validation and analysis. *www.casos.cs.cmu.edu*

Data Storage Systems Center: Founded in 1990, this NSF Engineering Research Center is considered to be the preeminent university-based research and education program in magnetic and magneto-optic recording technology in the United States. The main research thrusts are storage and computer systems integration, magnetic recording technology, magneto-optic recording technology and the electronic subsystems used in the above technologies. *www.dssc.ece.cmu.edu*

CMU Usable Privacy & Security Laboratory: CUPS was established in 2004 to bring together Carnegie Mellon researchers working on a diverse set of projects related to improving the usability of privacy and security software and systems. The privacy and security research community has become increasingly aware that usability problems severely impact the effectiveness of mechanisms designed to provide security and privacy in software systems. Indeed, one of the four grand research challenges in information security and assurance identified by the Computing Research Association is: "Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future." This is the challenge that CUPS strives to address. CUPS is affiliated with Carnegie Mellon CyLab. *http://cups.cs.cmu.edu*

Entertainment Technology Center: The concept behind the ETC is to have technologists and fine artists work together to produce artifacts that are intended to entertain, inform, inspire or otherwise affect an audience/guest/player/participant. Despite the center's name, a number of its projects have strong connections to national security issues, such as the fire fighting training simulation Hazmat: Hotzone; PeaceMaker, a video game simulation of the Israeli-Palestinian conflict that can be used as a tool to promote peaceful resolutions among Israelis, Palestinians, and young adults worldwide; and MySecureCyberspace for Kids, a collaboration with CyLab that aims to educate children about cyber security and instill in them good cyber citizen habits, so that being safe and secure online becomes as second nature as brushing their teeth or looking both ways before crossing the street. *www.etc.cmu.edu*