

PRESS RELEASE

From the University of Illinois Information Trust
Institute



Information Trust Institute Wins 2 of 3 I3P Fellowships for 2008

The Institute for Information Infrastructure Protection (I3P) has announced the recipients of its 2008 Research Fellowships, and two of the three winners will be hosted by the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign during the term of their fellowships.

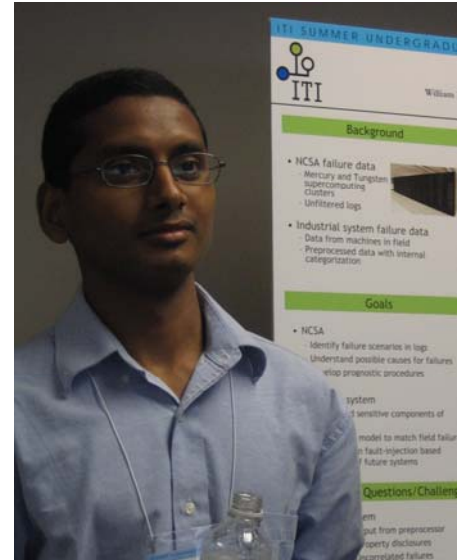
The fellowships, which support postdoctoral work for recently graduated Ph.D. students, are awarded based solely on merit. Eighteen scholars from eleven institutions competed for this year's awards, which are regarded as prestigious in the field of trustworthy computing. The 2008 winners include Shishir Nagaraja, who just completed a Ph.D. at the University of Cambridge in the United Kingdom and will now move to Illinois; Nithin M. Nakka of the University of Illinois; and a scholar from Dartmouth College.

Shishir Nagaraja's area of expertise is security and privacy in decentralized networks. At Illinois, he will work under the guidance of Professor Nikita Borisov of ITI, the Department of Electrical & Computer Engineering, and the Coordinated Science Laboratory (CSL). Together, Nagaraja and Borisov will work to develop defenses against peer-to-peer botnets, which are malicious collections of compromised computers that utilize diverse connectivity among the participating machines. They intend to study possible defense mechanisms that exploit the fundamental limitations of the network structure. The work will support Borisov's overall research program, which focuses on building scalable, secure, and private distributed systems.

In particular, this work will build on and extend Borisov's work on peer-to-peer systems for anonymous communications. Such systems allow people to prevent their online activities from being tracked and to insulate themselves from detailed profiling that is currently carried out by ISPs and service providers. Much of Borisov's existing research has focused on studying how structural properties of peer-to-peer networks affect the privacy and security of anonymous communication.

It was in that context that Borisov and Nagaraja first met, when Borisov presented a seminar about his work at Cambridge in 2006. "He had a great grasp of the relevant research and a good intuition about distributed systems," Borisov recalls. Nagaraja went on to publish a paper that gave Borisov a significant new insight into the problems involved in determining whether unstructured networks provide significantly worse anonymity than structured ones. The two researchers opened a correspondence and discovered a mutual interest in botnet defense. "I'm excited about the opportunity to work with Shishir during his postdoctoral studies in this area," said Borisov.

The other fellowship recipient at Illinois, Nithin M. Nakka, obtained his Ph.D. from Illinois in 2006 under



Dr. Nithin Nakka, one of two University of Illinois recipients of 2008 I3P Fellowships.

the guidance of Ravishankar K. Iyer, who is the Director of CSL, Chief Scientist of ITI, and a professor in the Department of Electrical & Computer Engineering. After graduating, Nakka worked for a time at Motorola, but has since returned to extend his Ph.D. work on the development of a reconfigurable hardware framework called the Reliability and Security Engine (RSE).

The RSE was designed by Nakka, Iyer, and other members of Iyer's team to enable the selection of techniques needed by an application and to demonstrate its capabilities by integrating reliability, security, and recovery modules. The work, which has attracted interest from both industry and academia, is fundamental to the Trusted ILLIAC platform for trustworthy computing. Trusted ILLIAC, which was launched in 2006, is a large cluster computing platform at Illinois that was designed to support on-demand utility computing, also known as "adaptive enterprise computing" or "real-time computing." Such systems are required to meet operational deadlines, and are often associated with mission-critical applications.

Nakka says that his work under the I3P fellowship will extend the concept of the RSE to provide a securely programmable hardware architecture for protection against a broad range of errors and attacks, including insider attacks. "We intend to investigate and implement mechanisms that enforce application-specific reliability properties in an attempt to prevent an application from entering a reliability-critical state resulting in a crash, hang, or incorrect output," he explained. "I'll also be working on formally verifying the guarantees offered by the techniques, by extending my recent work in symbolic program execution."

I3P is a consortium of leading universities, national laboratories, and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States. Their fellowship program, which is funded by the U.S. Department of Homeland Security, is designed to build a nationwide cadre of investigators focused on critical research challenges and to provide expanded research opportunities at I3P member institutions. As the host institution for Nagaraja and Nakka, ITI will receive funding from I3P to cover the salary, fringe benefits, and travel expenses of the fellows.

About the Information Trust Institute (ITI)

The Information Trust Institute is a multidisciplinary cross-campus research unit housed in the College of Engineering at the University of Illinois at Urbana-Champaign. It is an international leader combining research and education with industrial outreach in trustworthy and secure information systems. ITI brings together over 90 faculty, many senior and graduate student researchers, and industry partners to conduct foundational and applied research to enable the creation of critical applications and cyber infrastructures. In doing so, ITI is creating computer systems, software, and networks that society can depend on to be trustworthy, that is, secure, dependable (reliable and available), correct, safe, private, and survivable. Instead of concentrating on narrow and focused technical solutions, ITI aims to create a new paradigm for designing trustworthy systems from the ground up and validating systems that are intended to be trustworthy. www.iti.uiuc.edu

Contact: Molly M. Tracy, Associate Director, Information Trust Institute, 217/333-3437, mollyt@iti.uiuc.edu.

Writer: Jenny Applequist, Information Trust Institute, 217/244-8920, applequi@iti.uiuc.edu.

Released June 19, 2008



University of Illinois at Urbana-Champaign