Multi-university collaboration to re-engineer internet

September 20 2010

Dr. Antonio Nicolosi, Assistant Professor of Computer Science at Stevens Institute of Technology is part of the interdisciplinary Nebula Project, a multi-university collaboration led by the University of Pennsylvania, which has recently been awarded a $7.5 million grant from the National Science Foundation (NSF) as part of the Future Internet Architecture (FIA) program.

"This is the type of multi-institutional, leading-edge research project that can have tremendous impact to the industry at large," says Dr. Michael Bruno, Dean of the Schaefer School of Engineering at Stevens. "Dr. Nicolosi's reputation in cryptography and information assurance has allowed him this opportunity to work with other top minds in the field."

Nebula's moniker, which is Latin for "cloud," refers to the team's vision of FIA in which distributed networks and cloud computing heighten Internet security and efficiency. As a cryptographer for the Nebula team, Dr. Nicolosi's contribution will be in the use of advanced cryptographic techniques to support trustworthiness in computer-based transactions such as information sharing, policy agreements, and purchases. Dr. Nicolosi will be working together with Stevens PhD students to study methods of increasing performance while simultaneously strengthening resource-intensive cryptographic security tools.

Stevens Institute of Technology, The Innovation University, is a designated National Center of Academic Excellence in Information Assurance Research and National Center of Academic Excellence in

Information Assurance Education. These federal designations recognize outstanding efforts in reducing the vulnerability of our national information infrastructure through research and student instruction. The Center for the Advancement of Secure Systems and Information Assurance (CASSIA) coordinates these efforts at Stevens and manages government scholarship and grant programs made possible by the designations.

Dr. Nicolosi will be collaborating with scholars from Cornell University, the Massachusetts Institute of Technology, Princeton University, Purdue University, Stanford University, the University of California, Berkeley, the University of Delaware, the University of Illinois at Urbana-Champaign, the University of Texas, Austin, and the University of Washington. The team will also work closely with research scientists from Cisco Systems, Inc.

To source and test FIA hardware, Nebula will utilize an industrial Cisco Systems lab in California and the Laboratory for Telecommunication Sciences in College Park, Maryland.

"This is a highly-visible, game-changing research program in which the goal is to redesign the Internet to be fundamentally secure," says Dr. Dan Duchamp, Department Director for Computer Science at Stevens. "These projects will anticipate and define how the Internet is experienced in the future."

The NSF program challenges funded teams to explore how to design an Internet without the constraints imposed by its current, outdated architecture and imagine how the Internet might look if the infrastructure could be refreshed from a clean slate. Cloud-based FIA offers radical departures from the modern Internet that would accelerate data transfer while patching up network vulnerabilities.

Some of the possibilities of the Future Internet, as suggested by Dr. Nicolosi, include:

- Receiver-invoked third-party functionalities. Users could configure their network connection so that all traffic they receive is passed through a service offered by a third-party of their choice (for example, a sophisticated anti-virus offered by a security company).

- On-demand bandwidth: New architectures could allow Internet service providers to offer various bandwidth speeds at user-configurable prices for on-demand bandwidth.

- Secure global private networks. Data services, such as provided by a private company's secure servers, could move massive amounts of data, like medical histories, around the globe using an assured connection that would ensure privacy, security, reliability, and speed, while still relying on the public Internet.

- Networking mobility. Users could have the ability to travel between network service nodes without losing connection or sacrificing data security. For example, a user could make a video call at work, transfer the Internet connection to a 3G network for the ride home, and then connect to a home wireless network in the evening—without ever dropping the call.

- Secure public access. FIA cloud computing policies could protect the individual's access to information or destinations on the Internet, making it virtually impossible for a third party—like a hacker or a totalitarian government—to intercept data or restrict access to any part of the Web.

As Dr. Nicolosi further explains, "Something similar to some of these scenarios could perhaps be more or less realized in the current Internet—but without the assurances of availability, reliability, trustworthiness, and security that we ought to demand from a critically important infrastructure such as the Internet of tomorrow. The NSF wants teams to go beyond the typical incremental modifications to Internet architecture, and imagine large configuration changes capable of supporting these emerging needs. The ideas that will be developed in the context of the FIA projects will have a direct impact on the next generation of Internet users."

Provided by Stevens Institute of Technology

Citation: Multi-university collaboration to re-engineer internet (2010, September 20) retrieved 26 April 2024 from https://phys.org/news/2010-09-multi-university-collaboration-re-engineer-internet.html