At the forefront of cyber security research

August 12 2011, By Suzanna Schmeelk

DETER testbed server bank. Credit: DETER Testbed

Suzanna Schmeelk works at the forefront of cyber security research. In her role as both Berkeley R&D Engineer and a member of the Team for Research in Ubiquitous Secure Technology (TRUST), she examines critical cyber security issues.

TRUST is a university and industry consortium that's focused on cyber security issues and it significantly impacts computer technologies around the globe. Specifically, TRUST examines cyber security issues related to health care, national infrastructures, law and other issues facing the general public.

"TRUST is an international flagship program that explores a multitude of cyber security aspects that will directly impact the future of the

United States--and the planet at large," Schmeelk said. "My role has been to design and test cyber security tools and mentor students as they learn about cyber security issues."

TRUST testing

Many cyber security issues can be recreated and researched on a test bed. The cyber-Defense Technology Experimental Research (DETER) test bed was developed to conduct repeatable experiments in computer security and it is also used for components of TRUST-related research. Co-located at the Information Science Institute at the University of Southern California and the University of California at Berkeley, the test bed provides a safe venue to explore cyber security vulnerabilities since it is isolated from the outside internet.

The test bed is useful for exploring aspects of traditional information security, including integrity, availability and confidentiality. Availability assures that users can access information without interference or obstruction and in a usable format. Confidentiality assures that information can only be accessed by humans with sufficient privileges and adequate motivations. Integrity is the state of information being whole, complete and uncorrupted.

Cyber security research uses various combinations of theory, simulation and emulation-based experimentations. Theoretical research examines security threats through purely formal mathematical models. Simulation research traditionally studies an abstract system model. Emulation research examines actual system scenarios where a full-blown realistic system is constructed to duplicate the system under study. The research techniques can be blended to examine theoretical and/or realistic scenarios. After such an experiment is created, it can be executed on DETER to obtain repeatable results.

Gaining TRUST

"The best parts of my personal TRUST experience have been working with the brilliant individuals associated with TRUST coupled with the avant-garde and dynamic nature of the investigated issues and solutions," said Schmeelk.

Schmeelk explained that TRUST also sponsors the TRUST Academy Online, a web-based portal providing cyber security teaching and learning resources to interested faculty and researchers. Resources include literature, presentations, videos, sample code and open courseware to help facility cyber security understanding. The academy also offers courseware in information security, network security, trustworthy systems and social sciences.

For undergraduates interested in TRUST, the TRUST Research Experiences for Undergraduates (TRUST-REU) provides excellent summer research opportunities and a great introduction to cyber security research led by world class experts.

Provided by National Science Foundation