Enabling Cyber Security and Privacy for Trusted Internet and Grid Computing

Internet-based Grid computing is emerging as one of the most promising technologies that may change the world. Dr. Kai Hwang, Dr. Clifford Neuman, Dr. Viktor Prasanna, and their colleagues at the University of Southern California (USC) in Los Angeles, are working on self-defense tools to help distributed computing resources protect themselves from cyber attacks or malicious intrusions, automatically.

Highly shared resources in distributed computer systems or large-scale computational Grids make system insecurity and privacy violations major obstacles hindering distributed supercomputing applications. The US National Science Foundation has recently awarded a two millions research grant to USC, led by Professor Hwang of Electrical Engineering and Computer Science and Director of the Internet and Grid Computing Laboratory.

This project, coded as GridSec, is designed for trusted Grid computing with dynamic resources and automated intrusion responses. The project develops a new self-configuration security and privacy framework to support trusted Grid applications. The new GridSec architecture gives early warning to prevent system failures in grid resource sites from massive cyberspace attacks over the Internet.

Hwang and Neuman are building an automated intrusion response and trust management system to facilitate authentication, authorization, and security binding in using metacomputing Grids or peer-to-peer web services. The fortified grid infrastructure will benefit many security-sensitive applications, such as digital government, electronic commerce, public safety, homeland defense, anti-terrorism activities, cyberspace crime control, etc.

The trusted GridSec infrastructure, once completed, will support any network-based cooperative and pervasive computing with seamless security, assured privacy, data integrity, confidentiality, and optimized resource allocations. The USC team is developing a NetShield library with distributed micro firewalls and intrusion repelling software. The new security system adjusts itself dynamically with changing threat patterns and variations of network traffic conditions.

The NetShield library is supported by special *virtual private networks* (VPN), built on top of the Globus security infrastructure developed at USC Information Science Institute (ISI) jointly with the Argonne National Laboratory. The GridSec team pushes further to block network attacks and to enforce fine-grain, resource-access control at the file, device, and storage levels. Their collective effort involves building special hardware, software library, and encrypted channels across private networks through public networks.

Professor Prasanna of USC Electrical Engineering attacks the problems from a dynamic hardware approach. Dr. Dongho Kim and Dr. Tatyana Ryutov of ISI Network

Research Group are involved in policy management and access control in the project. Presently, six Ph.D.-bound graduate students are working on the project. The research team was formed out of accumulated expertise at USC/ISI in the areas of distributed computer systems and in network security enforcement. The current phase of the NSF-supported GridSec Project runs for 3 years at USC from late 2003. From concept to prototype systems, industrial technology transfer, and global installation, the project is planned to complete in 8 to 10 years.

The USC team collaborates with several world-class research teams in this project. Professor Michel Cosnard of the University of Nice and INRIA Sophia Antipolis in France and Dr. Zhiwei Xu, the Vega Grid Project leader at Chinese Academy of Sciences in Beijing, are both interacting with the USC team. Special benchmark experiments will be tested in these global sites against simulated terrorist attacks, grand thefts, privacy abuses, etc in the next several years.

Highlighted below are core technologies and on-going R/D tasks that are presently under development at the Internet and Grid Computing Lab and the High-Performance Lab on USC main campus and at the ISI Network Research Lab located in Marina Del Rey.

1 *Security-assured resource allocation* (SARA) for optimized Grid resource management through building encrypted virtual channels, called *Grid virtual private networks* (GVPN), among multiple Grid computing sites.

2 Developing the NetShield software library for automated intrusion detection, and responses through risk assessment and Internet traffic datamining. New datamining techniques have been developed for network anomaly detection.

3 Specifically testing NetShield system in benchmark experiments to fight against *distributed denial-of-service* (DDoS) flooding and port canning attacks based on datamining of Internet traffic records.

4 Extending the GAA/API software tools and policy update technique developed at ISI for fine-grain access control and datamining for threat tracking and policy update in using Grid resources

5 System-wide integration of efficient intrusion detection systems and attack databases on *field-programmable gate arrays* (FPGAs) to enable real-time datamining for network security control.

The GridSec work benefits security-sensitive and network-based metacomputing applications and offers protection to highly shared computer and network resources. This project will promote the acceptance of Grid computing and services across international boundaries. These Grid applications can be directed towards global security, crisis management, E-commerce, and reducing vulnerability of the cyberspace. The broader impacts are far reaching in science, education, business, and governments in an era of growing demand of Internet, Web and Grid services. (For additional details, visit the Project web site: **http://GridSec.usc.edu**)