UANews

UA Researchers Awarded $3.6M to Design Metaphorical Cybersecurity Map

ARIZONA

By Pete Brown - June 7, 2012, 12:35 pm

University of Arizona engineering and computer science researchers have won a $3.6 million cybersecurity research contract from the Office of Naval Research to develop dynamic maps that visualize suspicious activity on computer networks.

The project is rooted in the fact that monitoring a network for suspicious activity is a daunting task – the amount of data that has to be monitored is enormous, and it is a cacophony of malicious and normal traffic originating from disparate sources.

The human brain is not wired to detect patterns or anomalies in thousands of lines of text-based network activity reports. However, the visual cortex is the brain's largest subsystem, which makes humans extremely adept at making sense out of complex data presented in familiar visual forms.

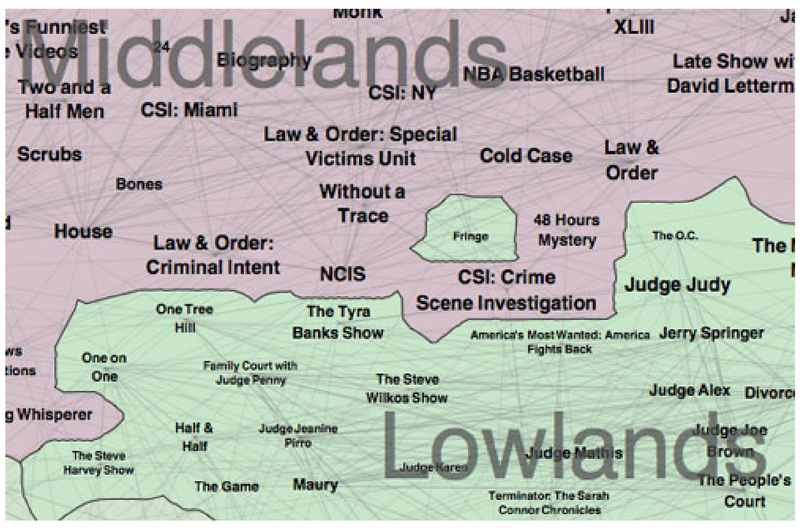
The research team consists of associate professors Christian Collberg and Stephen Kobourov from the computer science department, and assistant professor Loukas Lazos and associate professor Srinivasan Ramasubramanian from the electrical and computer engineering department.

The visualization techniques developed for this project are based on converting large-scale relational data into what looks like a geographic map, but is in fact a metaphorical map. "As people are familiar with the concept of geographical maps in day-to-day life, it is easier to use maps as a means to convey complex data in a meaningful form," Kobourov said.

The award is part of the Computer Network Defense and Information Assurance, or CND/IA, project to study visualization of malicious network activity, which falls under the ONR's Future Naval Capabilities program. The UA's contribution to the CND/IA project will be research and development of a natural, easy to learn, comprehensive, and real-time visualization system. The system will employ a familiar metaphor – the geographic map – to visualize network activity that could indicate security threats from without or within.

For instance, such a map could represent the global Internet topology, organized at different levels of granularity. The Internet is made up of approximately 35,000 autonomous systems, connected to and passing traffic between one another based on contractual agreements.

"Visualizing this complex system requires the development of efficient data gathering, filtering, storing, updating and eventually displaying mechanisms that would suppress normal network activities while highlighting suspicious traffic in real time," Ramasubramanian said.



Detail from TVLand, a map-based view depicting relationships between the 1000 most-watched TV shows. Each show is linked to 10 most similar shows, and map clusters, or *countries*, are represented by different colors.

"A significant challenge in this research is using the visualization system for detecting and displaying ongoing attacks, which are otherwise left unnoticed when examining raw data logs or performing automated detection," Ramasubramanian said.

"Our visualization system will be able to visualize suspicious network activity without overwhelming the cognitive ability of human analysts and exhausting available computational and communication resources," Kobourov said.

Similar mapping metaphors have been designed to study TV viewing patterns, by analyzing and visually presenting data from more than a million digital TV set-top boxes. Netflix movie preferences and international trade relations can also be rendered more accessible by these visualization techniques.

Underlying this research is the belief that such a powerful and familiar metaphor as a geographic map will result in an effective real-time visualization system that provides quick high-level information to the least specialized user, comprehensive information to the network expert, and a high degree of interactivity and customization to the specialized human analyst, all with a single visualization tool.

"Our previous experience with the geographic map metaphor has included visualizing TV viewers' preferences, and this has shown us that it is intuitively understandable by users of various levels of technical expertise," Kobourov said.

Principal Investigators

Christian Collberg

Stephen Kobourov

Loukas Lazos

Srinivasan Ramasubramanian