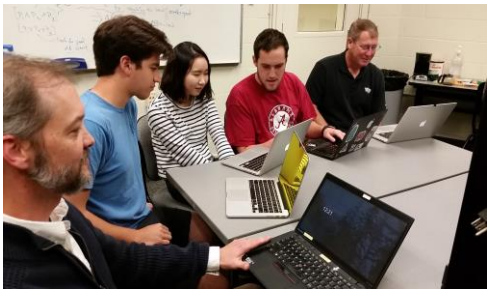
Using genetic principles to manage computer configurations and increase security

Cisco grant supports security research at Wake Forest University

All technology, from the most basic application to the most complex server, relies on a series of configuration parameters to operate, and getting these right can help ensure security. Leaving configuration steps incomplete or configuring a device incorrectly affects performance and can also leave a system vulnerable. What if systems could respond "instinctively" to correct these vulnerabilities?

In nature, species have evolved over time to strengthen their defenses in response to threats, and researchers in Wake Forest University's Department of Computer Science, led by Professor Errin Fulp, sought to discover whether these principles of evolution could be replicated to help facilitate computer security. "Our research aims to develop a new 'moving target' defense strategy using genetic algorithms to manage computer configurations. We want to create an evolution-inspired system that proactively identifies secure computer configurations," Fulp explains. "The goal is to reduce the exposure to vulnerabilities and improve system resiliency, while increasing the complexity and cost for attackers." Fulp adds that moving target environments provide security through diversity, changing system properties that are defined in the computer configuration. Achieving this diversity with computer configurations that are also secure and functional is critical and challenging; to work effectively, the moving target defense strategy must ensure the configurations across multiple computers are unique to maximize a system's resistance to attack.



"Our research aims to develop a new 'moving target' defense strategy using genetic algorithms to manage computer configurations. We want to create an evolution-inspired system that proactively identifies secure computer configurations."

The research at Wake Forest is supported in part by a grant awarded by Cisco, whose Advanced Security Research team provides grants and expertise to guide and advance cybersecurity research at higher education institutions. "Wake Forest has a commitment to student research; from their very first day on campus, students are invited to become involved in research opportunities. We know that this level of engagement gives them meaningful, hands-on practice that complements their time in the classroom," Fulp says. "The support we receive from Cisco gives us valuable funding, but more importantly, is enhanced by the direct involvement of Cisco engineers who help students understand how their research can be applied in the 'real world.' For this project, we've had the privilege of collaborating with Roger Seagle, a Cisco engineer who is also a Wake Forest alum." To combat challenges posed by shared servers on campus, which limited the research team's time to run its experiments, the Cisco grant also included the loan of a Cisco Unified Computing System server, which students installed and configured for their environment.

Recognizing that issues with web security can often be traced back to configuration problems, Fulp and his students began their research with web servers, testing the principles of moving target defense to see if an unsecured server could resolve its issues without the intervention of an administrator and then notify an administrator when resolution was complete. Researchers partnered with Cisco engineers to define a realistic size and scope for the project, and in biweekly meetings, the collaborative team reviewed data and strategized on next steps.

Thanks to support from Cisco, the team was able to publish and present two papers. Fulp notes that these research reviews are an invaluable capstone experience for students as they engage with the academic and scientific community to share what they've discovered. One of these student researchers has since joined Cisco as an employee.

Fulp and his students are now working to determine if these same principles can help secure networked servers, software-defined networks, and cloud-oriented infrastructures. "We have a system that can be applied to a standalone server, but servers are rarely deployed in isolation," he says. "Our next step is to ensure that entire infrastructures can be secured. We're also exploring the concept of co-evolution, the way in which 'species' evolve in nature to create a biosphere." In addition, Wake Forest has integrated this research and the lessons learned into its coursework, bolstering the information available to students in basic security courses.

CISCO

For more information on applying for a grant, visit http://research.cisco.com and visit the Trust and Transparency Center at http://trust.cisco.com