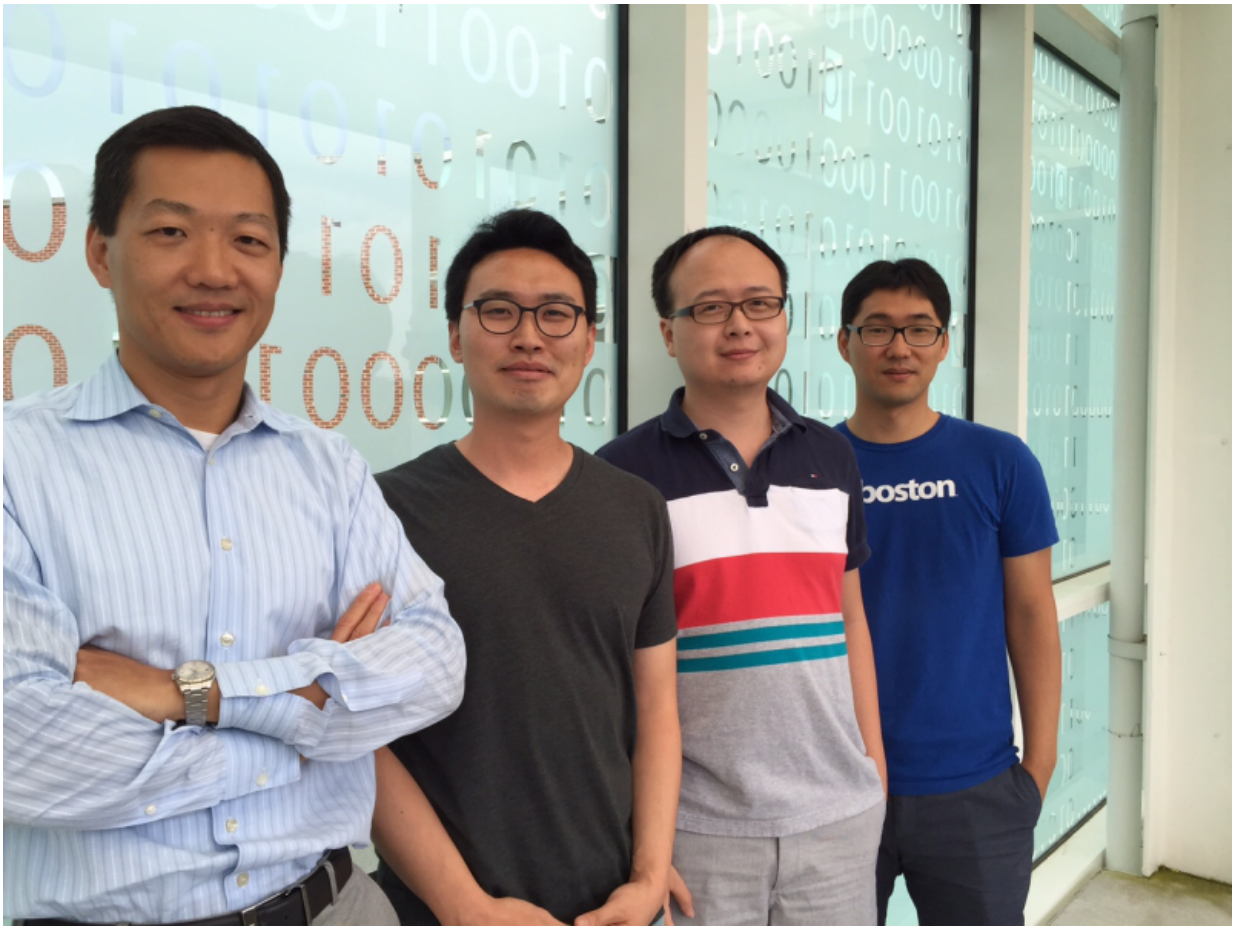
Team finds 11 security flaws in popular internet browsers using new analysis method

August 13 2015



Georgia Tech's winning team at the 24th USENIX Security Symposium are: (from left to right): Wenke Lee, Byoungyoung Lee, Chengyu Song, and Taesoo Kim. Credit: Georgia Tech

Researchers from the Georgia Institute of Technology College of Computing developed a new cyber security analysis method that discovered 11 previously unknown Internet browser security flaws. Their findings were honored with the Internet Defense Prize, an award presented by Facebook in partnership with USENIX this week at the 24th USENIX Security Symposium.

Ph.D. students Byoungyoung Lee and Chengyu Song, with Professors Taesoo Kim and Wenke Lee, of Georgia Tech received $100,000 from Facebook to continue their research and increase its impact to make the Internet safer.

Their research, "Type Casting Verification: Stopping an Emerging Attack Vector," explores vulnerabilities in C++ programs (such as Chrome and Firefox) that result from "bad casting" or "type confusion." Bad casting enables an attacker to corrupt the memory in a browser so that it follows a malicious logic instead of proper instructions. The researchers developed a new, proprietary detection tool called CAVER to catch them. CAVER is a run-time detection tool with 7.6 percent - 64.6 percent overhead on browser performance (Chrome and Firefox, respectively). The 11 vulnerabilities identified by Georgia Tech have been confirmed and fixed by vendors.

"It is time for the Internet community to start addressing the more difficult, deeper security problems," says Wenke Lee, professor in the School of Computer Science and an adviser to the team. "The security research community has been working on various ways to detect and fix memory safety bugs for decades, and have made progress on 'stack overflow' and 'heap overflow' bugs, but these have now become relatively easy problems. Our work studied the much harder and deeper bugs—in particular 'use-after-free' and 'bad casting'—and our tools discovered serious security bugs in widely used software, such as Firefox and libstdc++. We are grateful to Facebook for this recognition."

The work was selected for Facebook's second ever Internet Defense Prize award, which recognizes superior quality research that combines a working prototype with significant contributions to the security of the Internet—particularly in the areas of protection and defense. The award is meant to recognize the direction of the research and to inspire researchers to focus on high-impact areas.

"Designing defensive security technology has never been more important, and that's why we are once again offering the Internet Defense Prize to stimulate high quality research in this area," said Ioannis Papagiannis, security engineering manager at Facebook. "The Georgia Tech team's novel technique for detecting bad type casts in C++ programs is the type of standout approach we want to encourage. We look forward to seeing what the team does next to create broader impact and improve security on the Internet."

"Georgia Tech's award-winning entry exemplifies the groundbreaking security research that has become a hallmark of the USENIX Security Symposium," said Casey Henderson, executive director of the USENIX Association. "Their trailblazing work stood out among the many outstanding submissions judged by the USENIX Security Awards Committee and Facebook. We look forward to their continued progress enabled by the Internet Defense Prize in the coming year."

Provided by Georgia Institute of Technology