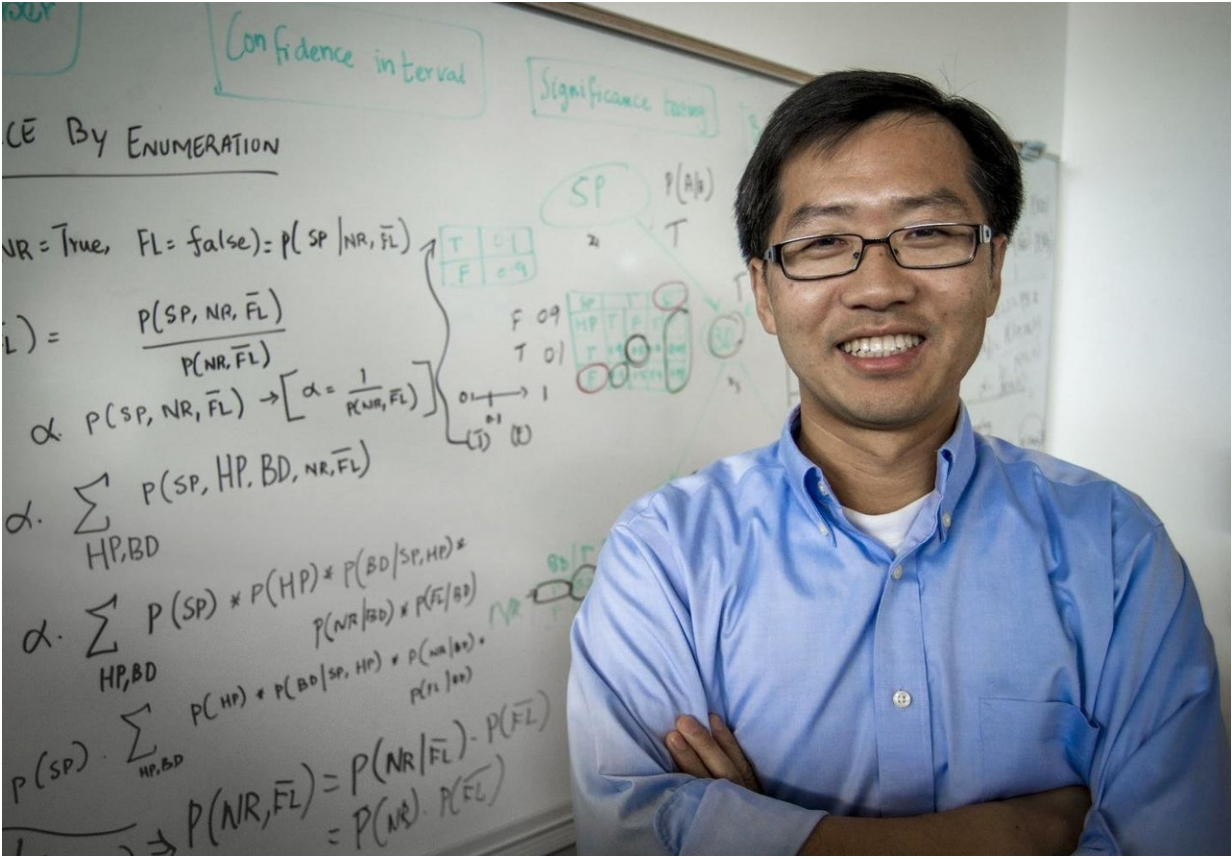


Computer scientist working to test security of IoT systems, blockchains

September 18 2018



Jeff Lei. Credit: UT Arlington

Computer data breaches cost companies millions of dollars each year. When combined with the damage leaks of private information do to consumers, the total cost of security issues is even greater.

Designers have created [secure systems](#) through blockchains and Internet of Things systems, but mistakes in their implementation of those systems often make them vulnerable. Jeff Lei, University of Texas at Arlington computer scientist, and his partner, Dimitris Simos of SBA Research Inc., recently were awarded a three-year, \$585,000 grant from the National Institute of Standards and Technology to develop a new approach to secure testing of [software systems](#) and avoid these vulnerabilities.

A [blockchain](#) is a growing list of data, arranged in groups called blocks, which are linked using cryptography. It is a highly secure, distributed system, with data stored across millions of computers. The Internet of Things describes multiple devices linked through the Internet that allow people to control appliances and devices in their homes and offices remotely. Software developers extensively test software systems at the macro level to detect any vulnerabilities that might exist and fix them prior to implementation. However, mistakes made by an end user during the installation process could compromise an otherwise secure system, and there is currently no way to detect those mistakes.

Lei and Simos will use interaction testing, a technique that systematically exercises interactions between factors to trigger [security vulnerabilities](#), to generate test cases and check whether any security properties have been compromised. The researchers said it's similar to hacking, but with a noble purpose.

Interaction testing has been widely used to tested general software systems, but has not been applied to security testing. In general testing, scenarios are applied to systems as they are designed and used as developers anticipated. Security testing requires testers to develop environmental scenarios that were not anticipated and could be used for negative purposes."Interaction testing for security is challenging because the negatives are often much larger than the positives and it requires

creativity to come up with scenarios to break the system. We are trying to develop a fundamental approach with these techniques, then use them to create a more efficient testing system than current methods," Lei said.

"Blockchains have the potential to change the way we do business, significantly reducing costs and increasing efficiency. Machines can do many things better than humans, but first people must have confidence that the security factors work."

Lei's research is an example of data-driven discovery, one of the themes of UTA's Strategic Plan 2020: Bold Solutions | Global Impact, said Hong Jiang, chair of the Computer Science and Engineering Department.

"Dr. Lei is well-known for his work in systems testing and the development of standards in the computing world, and this new grant is an excellent opportunity for him to apply his knowledge to one of the fastest-growing areas of information [security](#). What he discovers could go a long way toward truly securing software systems," Jiang said.

Provided by University of Texas at Arlington

Citation: Computer scientist working to test security of IoT systems, blockchains (2018, September 18) retrieved 16 April 2024 from <https://techxplore.com/news/2018-09-scientist-iot-blockchains.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.