# New proactive approach unveiled to malware in networked computers and data

June 4 2014

Cybercrime comes in all forms these days. One recent headline told of the creepware or silent computer snooping that resulted in the arrest of some 90 people in 19 countries. Miss Teen USA was among the victims. Her computer had been turned into a camera and used to spy on her in her own bedroom.

On the commercial front, Target suffered the largest retail hack in U.S. history during the Christmas shopping season of 2013, and now the Fortune 500 company's outlook is bleak with steep drops in profits.

New research to be announced at the June 2014 ACM Symposium on Information, Computer and Communications Security in Kyoto, Japan has unveiled the causal relations among computer network events.

The work effectively isolates infected computer hosts and detects in advance stealthy malware also known as malicious software.

The work was conducted under the auspices of a 2010 National Science Foundation CAREER Award grant to develop software that differentiates human-user computer interaction from malware. That $530,000 award was presented to Danfeng (Daphne) Yao, associate professor of computer science at Virginia Tech. She worked with Naren Ramakrishnan, the Thomas L. Phillips Professor of Engineering, and her graduate student Hao Zhang of Beijing, China, a doctoral candidate in computer science.

The Virginia Tech computer scientists used causal relations to determine whether or not network activities have justifiable and legitimate causes to occur.

"This type of semantic reasoning is new and very powerful," Yao said.

"The true significance of this security approach is its potential proactive defense capability. Conventional security systems scan for known attack patterns, which is reactive. Our anomaly detection based on enforcing benign properties in network traffic is a clear departure from that," Yao added.

They will present their paper "Detection of Stealthy Malware Activities with Traffic Causality and Scalable Triggering Relation Discovery" on June 4. It will be published in the symposium's proceedings.

Virginia Tech Intellectual Property has filed a patent on this technology, and it is actually a continuation-in-part patent, following one of Yao's earlier patents.

Previously, Yao garnered a 3-year, $450,000 grant from the Office of Naval Research (ONR) on cyber security to quantitatively detect anomalies in Department of Defense (DOD) computers, mobile devices, command and control servers, and embedded systems deployed on navy ships.

Yao's career research focus has been on this methodology development for novel, practical, and quantitative anomaly detection. Specifically, she is analyzing causal relations of events and producing instructions for detecting anomalies in computer programs, systems, and networks.

Provided by Virginia Tech