Research team identifies methods to predict future cyberattacks

April 4 2022, by Ingrid Wright

Credit: Pixabay/CC0 Public Domain

Malicious software activities, commonly known as "malware," represent a big threat against modern society.

A University of Texas at San Antonio (UTSA)-led research team is investigating ways to accurately predict these attacks. Mechanical Engineering Professor Yusheng Feng and doctoral student Van Trieu-Do in the Margie and Bill Klesse College of Engineering and Integrated Design, in collaboration with professor Shouhuai Xu from the Department of Computer Science at the University of Colorado at Colorado Springs, are studying how to use mathematical tools and computer simulation to foresee cyberattacks.

According to a 2019 report by ForgeRock, 2.8 billion consumer data records were breached in 2018, costing more than $654 billion to U.S. organizations, posing a massive industry threat.

The current pervasive security threats motivated the UTSA researchers to develop and use cyber defense tools and sensors to monitor the threats and collect data, which can be used for various purposes in developing defense mechanisms.

"The current damages call for studies to understand and characterize cyberattacks from different perspectives and at various levels of intrusion. There are multiple variables that go into predicting the potential damage these attacks may cause as the aggressors get more sophisticated," said Feng.

Using predictive situational awareness analysis, the team studied the distinctive nature of the attacks to accurately predict the threats that target and potentially harm personal devices, servers and networks.

"Most studies on cyberattacks focus on microscopic levels of abstractions, meaning how to defend against a particular attack," Feng said. "Cyber attackers can successfully break in by exploiting a single weakness in a computer system."

The study aims to analyze the macroscopic levels of abstractions.

"Such macroscopic-level studies are important because they would offer insights towards holistic solutions to defending cyberattacks," he added.

Feng explains, "It's very hard to single out the cause of each attack, however, we have big data with time series for each IP address (location). In this research, we use 'causality' when there are inter-relationships among IP addresses that have similar patterns of temporal features for identifying the threat."

The researchers utilized Granger causality (G-causality) to study the vulnerabilities from a regional perspective of multiple threats, analyzing the cause and effect to identify cyber vulnerabilities or how the infiltrators attack an entity, in this case IP addresses.

G-causality is a statistical concept of causation that is based on prediction, in order to characterize causality, a well-defined mathematical notion has to be established. The research team used Granger causality to determine the nature of the cyberattack signals so the signals can be compared and analyzed in a holistic way.

The team also plans to expand the current body of research and study further on what other kinds of causality will impact users and how to develop the appropriate defense tools to protect against sophisticated attacks.

More information: The 2019 report by ForgeRock is available as a PDF.

Provided by University of Texas at San Antonio