Combination of techniques could improve security for IoT devices

11 October 2019

Credit: CC0 Public Domain

A multi-pronged data analysis approach that can strengthen the security of Internet of Things (IoT) devices—such as smart TVs, home video cameras and baby monitors—against current risks and threats has created by a team of Penn State World Campus students pursuing master of professional studies degrees in information sciences.

"By 2020, more than 20 billion IoT devices will be in operation, and these devices can leave people vulnerable to security breaches that can put their personal data at risk or worse, affect their safety," said Beulah Samuel, a student in the Penn State World Campus information sciences and technology program. "Yet no strategy exists to identify when and where a network security attack on these devices is taking place and what such an attack even looks like."

The team applied a combination of approaches often used in traditional network security management to an IoT network simulated by the University of New South Wales Canberra. Specifically, they showed how statistical data, machine learning and other data analysis methods could be applied to assure the security of IoT systems across their lifecycle. They then used intrusion detection and a visualization tool, to determine whether or not an attack had already occurred or was in progress within that network.

The researchers describe their approach and findings in a paper to be presented today (Oct. 10) at the 2019 IEEE Ubiquitous Computing, Electronics and Mobile Communication Conference. The team received the "Best Paper" award for their work.

One of the data analysis techniques the team applied was the open-source freely available R statistical suite, which they used to characterize the IoT systems in use on the Canberra network. In addition, they used machine learning solutions to search for patterns in the data that were not apparent using R.

"One of the challenges in maintaining security for IoT networks is simply identifying all the devices that are operating on the network," said John Haller, a student in the Penn State World Campus information sciences and technology program. "Statistical programs, like R, can characterize and identify the user agents."

The researchers used the widely available Splunk intrusion detection tool, which comprises software for searching, monitoring and analyzing network traffic, via a Web-style interface.

"Splunk is an analytical tool that is often used in traditional network traffic monitoring, but had only seen limited application to IoT traffic, until now," said Melanie Seekins.

Using these tools, and others, the team identified three IP addresses that were actively trying to break into the Canberra network's devices.

"We observed three IP addresses attempting to

attach to the IoT devices multiple times over a period of time using different protocols," said Andrew Brandon. "This clearly indicates a Distributed Denial of Service attack, which aims to disrupt and/or render devices unavailable to the owners."

As the basis for their approach, the researchers compared it to a common framework used to help manage risk, the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

"The NIST RMF was not created for IoT systems, but it provides a framework that organizations can use to tailor, test, and monitor implemented security controls. This lends credibility to our approach," said Brandon.

Ultimately, Seekins said, the ability to analyze IoT data using the team's approach may enable security professionals to identify and manage controls to mitigate risk and analyze incidents as they occur.

"Knowing what has taken place in an actual attack helps us write scripts and monitors to look for those patterns," she said. "These predictive patterns and the use of machine learning and artificial intelligence can help us anticipate and prepare for major attacks using IoT devices."

The team hopes their approach will contribute to the creation of a standard protocol for IoT network security.

"There is no standardization for IoT security," said Seekins. "Each manufacturer or vendor creates their own idea of what security looks like, and this can become proprietary and may or may not work with other devices. Our strategy is a good first step toward alleviating this problem."

Provided by Pennsylvania State University