Runtime Methods for Detecting Attacks in Big Data Systems

Researchers at the University of South Florida have developed a runtime intrusion detection technique for big data platforms. This technique understands and works according to the properties of such computer platforms.

Big data is an important factor that contributes to a successful company and its relevant software and information systems. The big data universe is growing aggressively with an estimated market of 50 billion dollars by 2018. Big data platforms like Hadoop and Spark have been widely adopted both by academia and industry. Users have to trust the big data platforms that host their data, and such trust is built on an underlying assumption that the platforms or their security methods will never be compromised. However, unexpected issues such as insider attacks or control-flow attacks due to programmer errors can happen in any system at anytime.

Our inventors have designed a novel method for detecting insider attacks in big data platforms during runtime. This method analyzes multiple features of memory access of a process, packages it as a process behavior profile, and shares that profile with other replica data-nodes in the system for verification. The replica data-nodes then verify the memory access of local processes using the received profiles. This approach will detect in real-time an insider attack that cannot be detected with the traditional analysis metrics.

ADVANTAGES:
- Runtime detection of insider attack
- Performs application level statistical analysis
- Determines memory access patterns

Reliable Technique for Detecting Attack in Big Data Systems

A Secure Framework for a Big Data System

Tech ID # 16B197