MISSISSIPPI STATE UNIVERSITY

HIGH PERFORMANCE DATA ANALYTICS

DASI

Large-Scale Graph Analytics and Risk Modeling for Detecting Malicious Cyber Nodes

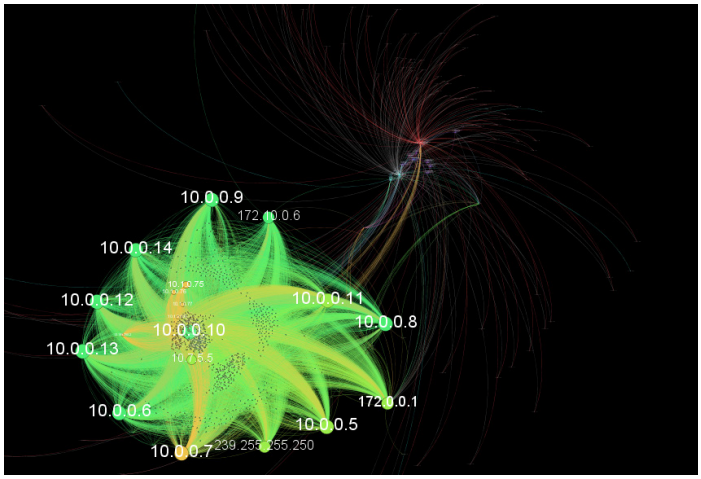
CHALLENGE

Although many approaches exist for detecting malicious nodes in a cyber network, most of these approaches assume a static attacker who does not adapt behavior according to the characteristics of the detection algorithm. However, research has shown that these methods are vulnerable to manipulation or evasion by an attacker. For example, a botmaster planning a DDoS attack may explicitly try to evade detection by modifying the behavior of the botnet so as to "poison" the data observed by an anomaly-based detection algorithm. Thus, there is a need to develop detection approaches that explicitly account for an evasive attacker. Some anti-evasive approaches have been developed, but none of these use graph analytics. While graph-analytic approaches show promise due to their ability to capture complex relationships between nodes, they can be computationally expensive.

TECHNICAL APPROACH

Our project goal is to quantify the effect of evasion on graph-based detection algorithms. In our experiment, we are generating a simulated NetFlow dataset with billion nodes and edges on shadow II with MPI programming. We will replicate the characteristics of dataset which is presently available like VAST dataset. We will then inject malicious activity into the dataset, we will begin with non-evasive and later extend with evasive malicious activity. We will implement method for monitoring graph characteristics to detect non-evasive anomalies. We will compare the detection performance of our technique e.g. success and false alarm rate for non-evasive and evasive malicious activity.

Developing large-scale, graph-based methods for detecting evasive cyber adversaries



Network for VAST dataset

CURRENT PRACTICE

Detection techniques are classified into two main categories: those based on setting up honey-nets and/or Intrusion Detection systems. The later one can further be subdivided into anomaly-based and signature-based detection systems. Anomaly-based detection systems can be either host based or network based. But regardless of the efforts by the researchers, bot detection remains a challenging task because bot developers continuously adopt advanced evasion techniques to make bots stealthier. Very few works have been done on this sector.

EXPECTED ACCOMPLISHMENT

We are expected to develop anti-evasive monitoring and detection tool: source code and documentation of verification. We are also supposed to apply this tool to multiple type of graphs and check its generality. Our long term goal is to develop new anti-evasion dynamic graph-based anomaly detection algorithms and new anti-evasion dynamic graph-based malicious node detection algorithms.

IMPACT

If our project is successful, it will result in increased understanding of how evasion can degrade the effectiveness of malicious node detection tools. As a result, companies and institutions will be more aware of the effect of evasion, so that they can take steps to mitigate its effect.

Contacts

Dr. Hugh Medal
hmedal@ise.msstate.edu

Dr. Song Zang
szhang@cse.msstate.edu

Dr. Mohammad Marufuzzaman
maruf@ise.msstate.edu

Dr. Linkian Bian
bian@ise.msstate.edu

Funding provided by a grant from Pacific Northwest National Laboratory.