Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc. Thesis M.Sc. IDP

Models for Normal and Attack Traffic in Traffic Causality Graphs

Motivation

Advanced Persistent Threats (APT) are on the rise. They are used for cyber espionage and other kinds of attacks against predominently high value targets. Attackers try to remain hidden and adapt to a given network instead of blasting out a massive amount of messages like computer worms have done. An APT typcially consists of a variety of phases: reconnaisance, delivery, initial intrusion, command and control, lateral movement, data exfiltration.
Our assumption is that despite of that, APTs still do not have perfect knowledge of the situation and they lack keying material that might be needed. So, the APT will show a different behaviour in some of the phases than normal applications deployed in a company network. It is a requirement for APT defense that the network provides more protection than a typical open networks that do not significantly restrict what is allowed or do not implement more than the usualy security measures.
So, in each of the phases, there may be a different behaviour between what the applications on this machine should do and what the APT needs to do. We want to better understand this. We see Traffic Causality Graphs (TCG) as good candidate model to describe and compare related application and attack behaviours on the network.

Your Task

- Study TCGs and other related Work
- Develop software to generate TCGs (unless existing software is found)
- Model TCGs that result from certain attack patterns
- Generate TCGs from applications in a testbed environment
- Evaluate how and if TCGs can help to separate honest and malicious behavior

Contact

Dr. Heiko Niedermayer niedermayer@net.in.tum.de
tba.