Process Mining on Company Data for Detecting Security Breaches

Toon Calders (ULB)

According to a recent report of Price Waterhouse Cooper, the most common source of security incidents are current employees, followed at a distance by former employees and only after that truly external threats such as hactivists. [http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml?region=&industry=] This observation leads to the conclusion that in an intelligent security event management system, should also concentrate on internal threats to security.

The goal of the thesis is to analyze the possibility of using process mining to help in the detection of silent attacks. We will concentrate on company-specific data. From this data typical behavior will be detected and modeled as a process or workflow. We consider three aspects of a workflow: the actor(s), the resources, and the activities. By modeling the normal behavior in the system we are able to detect deviating cases. Based on historical data, the goal is to build models of typical behavior, including the use of resources such as patient records. Such a system would be able to detect for instance if a certain patient record is consulted much more often than usual, or by more people, or outside of the normal workflow (e.g., only reading information, but not writing). Such a pattern could indicate unjustified access to for instance the patient record of a famous patient.

For modeling the workflows, we propose the use of process mining (Van der Aalst, 2011). Process mining is a state-of-the-art technology concerned with the automatic extraction of process models from event logs. Consider, e.g., a hospital registering all activities that are carried out for the treatment of patients, ranging from the admission, various measurements being taken from the patient, medicine administered, surgical procedures, to the resignation of the patient. Process mining could be used to extrapolate from these examples, a common model of how the hospital deals with a patient. There are several applications of process mining; first it can be used to improve the processes by standardizing them; many companies and organizations may only have informal procedures. By process mining the process logs are used to extract a general model of the actual business processes. Such a model can guide the automation process.

In this thesis the goal is to analyze how process mining could be used for anomaly detection; how can the discovered models be used to detect abnormal behavior in a company network? Much like in credit card fraud detection, the approach is to first model normal behavior, in this case using process mining, in order to detect diverging behavior that could indicate security breaches in the network.

Van der Aalst, W. M. (2011). *Process Mining: Discovery, Conformance and Enhancement of Business Processes*. Springer.