Systems Security

A Sparksee scenario by **Sparsity Technologies**

→ Use Case

Sparksee is used as the database management system in the detection of threats of insiders. Sparksee is able to store all the systems' access log files for pattern analysis.

→ What?

Insiders are those people who work, or have previously worked, in a company and intentionally misused the access to compromise some information available. A popular example is Wikileaks, and how the threat of insiders should be a concern for any company. Nowadays, with the outsourcing done with the “cloud computing”, it is more important to detect insider attacks than ever .

→ How?

This is a research carried by the RMIT University in collaboration with the CA Labs from CA Technologies. From 3 years of logs (2008 to 2011) extracted from the SVN access of a certain CA program they obtained 700M lines of access logs, and 282 unique users. In order to deal with such huge numbers they chose DEX graph database management system, which allowed them to store the following databases:

✓ Log database, with 700M nodes and 3500M edges, a really huge database with a total size of 305GB.

✓ Command database, storing the commands executed by the users accessing the SVN. This is a smaller database of 6GB total size.

Sparksse graph databases were used in the cluster analysis to detect communities, based on the accessed resources, projects and the daily access patterns.

They discovered that a deviation on the daily pattern can be an alert of a possible insider threat.

For more details about the analysis, conclusions and future work we recommend reading the complete article here.

Sparsity Technologies
info@sparsity-technologies.com
sparsity-technologies.com