A Graph-based Representation of Relations in Network Security Alert Sharing Platforms

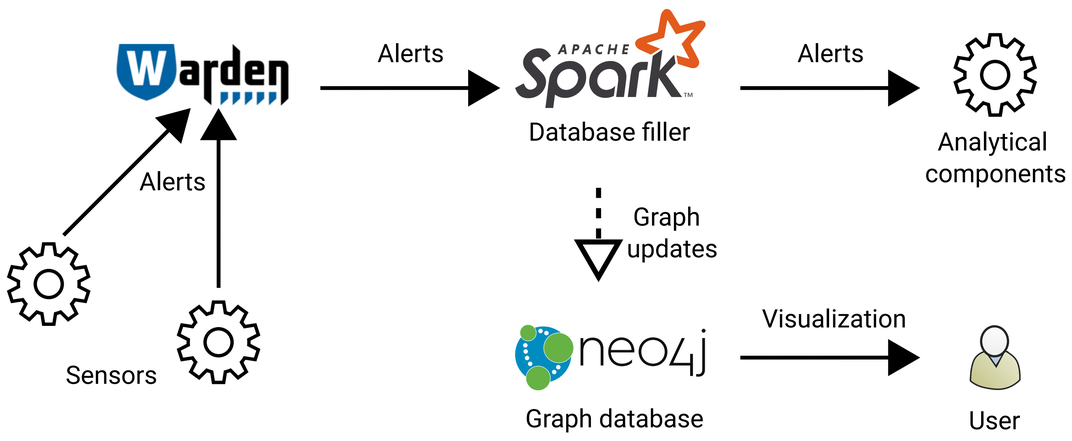
Martin Husák, Milan Čermák
Institute of Computer Science, Masaryk University
Brno, Czech Republic
{husakm|cermak}@ics.muni.cz

Abstract

We present a framework for graph-based representation of relation between sensors and alert types in a security alert sharing platform. Nodes in a graph represent either sensors or alert types, while edges represent various relations between them, such as common type of reported alerts or duplicated alerts. The graph is automatically updated, stored in a graph database, and visualized. The resulting graph will be used by network administrators and security analysts as a visual guide and situational awareness tool in a complex environment of security alert sharing. [1]

System Architecture

Our framework is based on stream processing of alerts in the alert platform SABU. It consists of two main parts, database filler and web interface. The database filler is implemented in Apache Spark and is placed in the alert processing pipeline of SABU platform. The web interface consists of a single web page, that can be run in a stand-alone mode or included as a panel in a control dashboard of SABU platform. [1]



List of components and technologies used:

- *Sensors* – various sensors, e.g., IDS and honeypots, that contribute with alerts.
- *Warden* – hub for exchange of security alerts, e.g., from sensors to analytical tools and mitigation connectors, a central point of SABU platform.
- *Apache Spark* – engine for large-scale data processing. The database filler, as well as other alert processing and analytical tools in SABU, is implemented as a Spark module.
- *Neo4j* – a graph database, where the graph-based representation is stored.
- *Web interface* – a web page for displaying and querying the graph. It can be either stand-alone or frame in a larger dashboard. The web interface is built on Angular 2 and D3.js.

Monitored Relations

In the demonstration, we are going to show the relations between sensors and alert types in the SABU alert sharing platform. Sensors and alert types are represented as nodes. For both node types, we store the following information:

- node type (*sensor* or *alert_type*),
- sensor name or alert type,
- number of reported alerts in total and in the last hour,
- number of duplicate and continuing alerts [2].

The edges represent the relations between arbitrary nodes and an edge can has a type representing the watched relation. Each edge has the following properties:

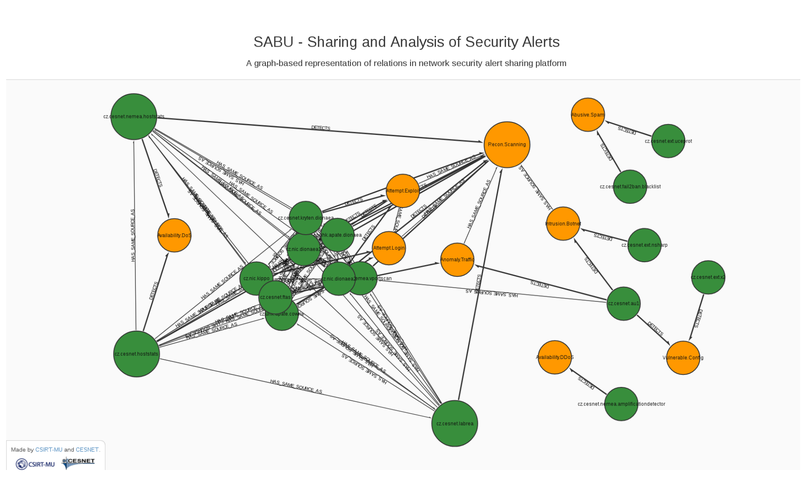
- edge type (one of the relations, see below),
- number of observations in total and in the last hour,
- average, minimal, and maximal time differences between the correlated alerts.

Currently, we monitor the following relations:

- *detects* – A sensor reports alert of a certain type.
- *same_source_sensor* – The two sensors reported the same source of an event.
- *same_target_sensor* – The two sensors reported the same target of an event.
- *same_source_alert* – The two alerts of different categories are sharing the same source.
- *same_target_alert* – The two alerts of different categories are sharing the same target.
- *duplicate* – The two sensors reported duplicate alerts, i.e., alerts with the same type, source, and target [2].

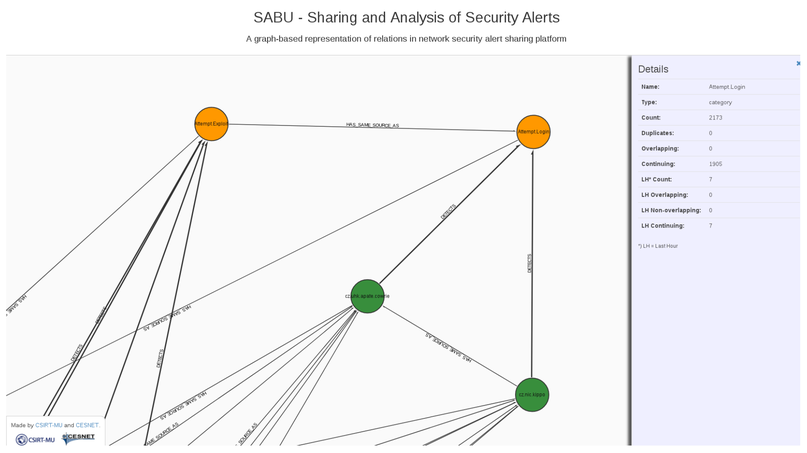
Web Interface

Title screen provides an overview of all the nodes and edges in the graph:



A user can zoom in and out and move the nodes around:

The details on each node and edge are available on click:



Acknowledgement and References

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019029 The Sharing and analysis of security events in the Czech Republic.

https://sabu.cesnet.cz/

https://csirt.muni.cz/

@CESNET_CERTS

@csirtmu

[1] Martin Husák and Milan Čermák, A Graph-Based Representation of Relations in Network Security Alert Sharing Platforms in 2017 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2017.

[2] Martin Husák, Milan Čermák, Martin Laštovička, and Jan Vykopal, Exchanging Security Events: Which And How Many Alerts Can We Aggregate? in 2017 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2017.

CSIRT-MU