
UNSPECIFIED

Available from Middlesex University's Research Repository at http://eprints.mdx.ac.uk/9394/

Copyright:

Middlesex University Research Repository makes the University's research available electronically.

Copyright and moral rights to this thesis/research project are retained by the author and/or other copyright owners. The work is supplied on the understanding that any use for commercial gain is strictly forbidden. A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge. Any use of the thesis/research project for private study or research must be properly acknowledged with reference to the work's full bibliographic details.

This thesis/research project may not be reproduced in any format or medium, or extensive quotations taken from it, or its content changed in any way, without first obtaining permission in writing from the copyright holder(s).

If you believe that any material held in the repository infringes copyright law, please contact the Repository Team at Middlesex University via the following email address:
The item will be removed from the repository while any claim is being investigated.
Choudhury, Sharmin Tinni; Kodagoda, Neesha; Nguyen, Phong; Rooney, Chris; Attfield, Simon; Xu, Kai; Zheng, Yongjun; Wong, B. L. William; Chen, Raymond; Mapp, Glenford E.; Slabbert, Louis; Aiash, Mahdi; Lasebae, Aboubaker, 2012. M-Sieve: a visualisation tool for supporting network security analysts [poster]. Available from Middlesex University’s Research Repository.
M-SIEVE: A visualisation tool for supporting network security analysts

VAST 2012 Mini Challenge 1 Award: “Subject Matter Expert's Award”

Middlesex Spatial Interactive Visualisation Environment (M-SIEVE)

The M-SIEVE interface has three shared views that simultaneously update

1. Map of BankWorld with overlays indicating machine locations
2. Attribute explorer, which represents each attribute as an interactive histogram
3. Interactive time-bar for accessing specific points in time

Facilities legend
Play/pause button used to automatically play through the dataset
Colour is used to indicate the maximum policy status of machines at each location
Menu options to open additional functionality – including the CLA Suggested Alert Level (see below)

Concern Level Assessment (CLA) Rules

The dataset contains a number of independent parameters, which on their own provide very little insight. E.g., Machine X is suffering from a multiple login failure.

The parameters taken together reveal the state of the machine, but only to experts who understand which combination of parameters are important.

Machine X is an office workstation suffering from a multiple login failure but is otherwise normal.

To integrate the insight of experts in to our system, we conducted knowledge elicitation interviews with network security academics and practitioners.

An expert knows that Machine X is not of concern as it is a human facing machine.

Based on the elicited knowledge, we developed a set of heuristics (inference rules) to assign parameter combinations to 6 point scale.

Machine X would have a low alert level as humans forget passwords.

Example heuristics

<table>
<thead>
<tr>
<th>If</th>
<th>CLA Alert Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>All parameters are normal, independent of machine type and time of day</td>
<td>0. Normal: Of no concern</td>
</tr>
<tr>
<td>Office workstation, with normal activity and number of connections, and with low policy-deviation</td>
<td>1. Low</td>
</tr>
<tr>
<td>Teller workstation develops low policy-deviation due to having an external device added during office hours</td>
<td>2. Medium-low</td>
</tr>
<tr>
<td>Office workstation suffers from login failure, is policy-deviated, and has a high number of connections during office hours</td>
<td>3. Medium</td>
</tr>
<tr>
<td>High-use server (e.g. email server) with otherwise normal parameters is suffering from 100% CPU consumption during office hours</td>
<td>4. Medium-high</td>
</tr>
<tr>
<td>Loan workstation (customer facing) is suffering from 100% CPU consumption, a high number of connections, and has policy deviation</td>
<td>5. High: Of high concern</td>
</tr>
</tbody>
</table>

Middlesex University London

School of Science and Technology
The Burroughs, London, NW4 4BT, UK
http://www.eis.mdx.ac.uk/research/idc/