

Middlesex University Research Repository:

an open access repository of Middlesex University research

http://eprints.mdx.ac.uk

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.

Copyright:

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

Copyright and moral rights to this work are retained by the author and/or other copyright owners. No part of the work may be sold or exploited commercially in any format or medium without the prior written permission of the copyright holder(s). A copy may be downloaded for personal, non-commercial, research or study without prior permission and without charge. Any use of the work for private study or research must be properly acknowledged with reference to the work's full bibliographic details.

This work 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: eprints@mdx.ac.uk

The item will be removed from the repository while any claim is being investigated.





M-SIEVE: A visualisation tool for supporting network security analysts

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

S. Choudhury, N. Kodagoda, P. Nguyen, C. Rooney, S. Attfield, K. Xu, Y. Zheng, B.L.W. Wong, R. Chen, G. Mapp, L. Slabbert, M. Aiash, A. Lasebae

Middlesex Spatial Interactive Visualisation Environment (M-SIEVE) The M-Sieve interface has three shared views that simultaneously update After Hours Office Hours 2. Attribute explorer, 1. Map of which represents BankWorld with each attribute as an overlays indicating interactive histogram machine locations 0/96714 0/41061 0/111756 0/145093 0/172253 0/45803 0/47304 0/111131 0/111131 0/111131 3. Interactive timebar for accessing specific points in ltime Facilities legend Play/pause button used to Menu options to open additional Colour is used to indicate the maximum policy status of functionality – including the CLA automatically play through the Suggested Alert Level (see below) machines at each location dataset

PREV NEXT EXPORT

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

Machine 25/1066

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

	·	2012 02 02 02 1	5.00					
	Areas of Concerns at 2	2012-02-03 00:4	5:00		100			
	Bank Unit	IP Address	Class	Function	Policy	Activity	#Conns	Suggested Alert Level
	Region 1 - Branch 103	172.10.31.31	workstation	teller	2	3	37	3
	Region 1 - Branch 104	172.10.34.45	workstation	loan	2	4	16	5
	Region 1 - Branch 107	172.10.43.43	workstation	teller	2	3	17	3
	Region 1 - Branch 108	172.10.46.14	workstation	loan	2	3	21	3
	Region 1 - Branch 109	172.10.49.38	workstation	teller	2	5	13	2
	Region 1 - Branch 116	172.10.70.25	workstation	teller	2	5	23	2
	Region 1 - Branch 118	172.10.76.38	workstation	teller	2	5	31	2
ATTRIBUTE EXPLORER 100000 1000 1000 1000 1000 1000 1000	Region 1 - Branch 120	172.10.82.45	workstation	office	2	3	29	3
THE AT COMMAN & 2010 BO 100 COM	egion 1 - Branch 121	172.10.85.6	workstation	loan	2	5	10	2
Seek Unit Dec Alberton Common		172.10.85.16	workstation	office	2	5	41	2
Region Description 120 120 141 workstorm law 2 2 2 2 2 2 2 2 2	Region 1 - Branch 126	172.10.100.34	workstation	office	2	3	14	3
Image 1 - Beach 13 123 133 135	Region 1 - Branch 130	172.10.112.3	workstation	office	2	5	21	2
120.017.55 violation effice 2 5 30 2 100.017.65 violation effice 2 5 35 2 100.017.65 violation effice 2 5 35 2 100.017.65 violation this 2 5 5 5 2 100.	Region 1 - Branch 131	172.10.115.51	workstation	office	2	3	48	3
Region 1-Branch 105 12:23:23:03 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:03 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:03 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:03 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:03 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 Market 90:100:06 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 Market 90:100 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 Market 90:100 Region 1-Branch 105 12:23:23 N - volutions office 2 3 26 3 20 20 20 20 20 20 20 20 20 20 20 20 20	Region 1 - Branch 132	172.10.118.27	workstation	office	2	5	30	2
	Region 1 - Branch 134	172.10.124.5	workstation	office	2	3	46	3
	Region 1 - Branch 14	172.9.18.15	workstation	office	2	5	45	2
	Region 1 - Branch 144	172.10.154.38	workstation	loan	2	3	21	3
Programmy (ST) (NEW PROGRAMM) (NEW P	Region 1 - Branch 148	172.10.166.15	workstation	loan	2	3	29	3
20 20 10 00 000000000000000000000000000	– Region 1 - Branch 15	172.9.21.43	workstation	loan	2	3	46	3
	Region 1 - Branch 150	172.10.172.23	workstation	loan	2	4	38	5
		172.10.172.35	workstation	office	2	5	39	2
		172.10.172.45	workstation	office	2	5	35	2
	Region 1 - Branch 151	172.10.175.36	workstation	teller	2	5	9	2
	Region 1 - Branch 153	172.10.181.15	workstation	teller	2	5	12	2
	Region 1 - Branch 156	172.10.190.34	workstation	office	2	3	26	3

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