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

Middlesex University London

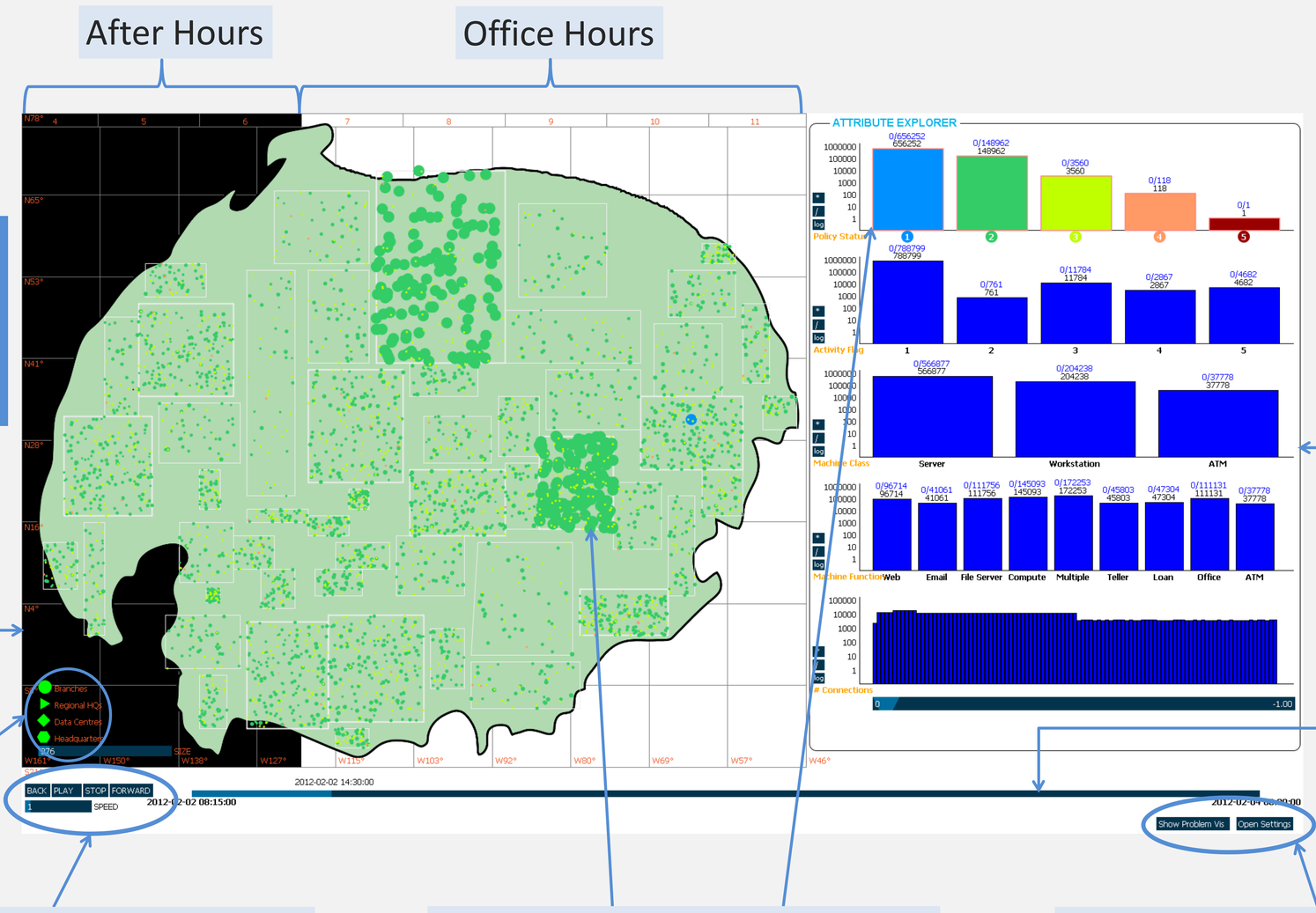
M-SIEVE: A visualisation tool for supporting network security analysts

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



1. Map of BankWorld with overlays indicating machine locations

Facilities legend

2. Attribute explorer, which represents each attribute as an interactive histogram

3. Interactive time-bar for accessing specific points in time

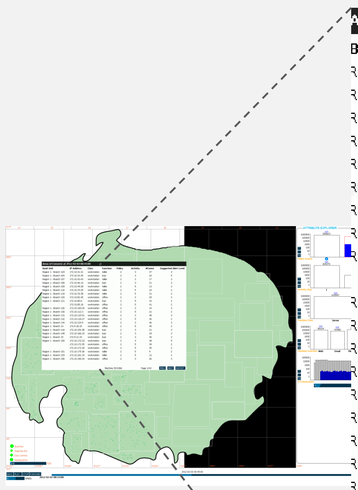
Play/pause button used to automatically play through the dataset

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.	The parameters taken together reveal the state of the machine, but only to experts who understand which combination of parameters are important.	To integrate the insight of experts in to our system, we conducted knowledge elicitation interviews with network security academics and practitioners	Based on the elicited knowledge, we developed a set of heuristics (inference rules) to assign parameter combinations to 6 point scale
E.g., Machine X is suffering from a multiple login failure	Machine X is an office workstation suffering from a multiple login failure but is otherwise normal	An expert knows that Machine X is not of concern as it is a human facing machine	Machine X would have a low alert level as humans forget passwords



Areas of Concerns at 2012-02-03 00:45:00

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
Region 1 - Branch 120	172.10.82.45	workstation	office	2	3	29	3
Region 1 - Branch 121	172.10.85.6	workstation	loan	2	5	10	2
	172.10.85.16	workstation	office	2	5	41	2
Region 1 - Branch 126	172.10.100.34	workstation	office	2	3	14	3
Region 1 - Branch 130	172.10.112.3	workstation	office	2	5	21	2
Region 1 - Branch 131	172.10.115.51	workstation	office	2	3	48	3
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
Region 1 - Branch 148	172.10.166.15	workstation	loan	2	3	29	3
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

Machine 25/1066 Page 1/43 PREV NEXT EXPORT

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