Carnegie Mellon
Ph.D. Program in Computation, Organizations & Society

Do Computer Networks Have a Pulse?

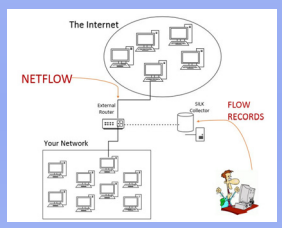
Detecting periodicity and change in autonomic netflow

Geoffrey Dobson
gdobson@cs.cmu.edu

Kathleen M. Carley
kathleen.carley@cs.cmu.edu

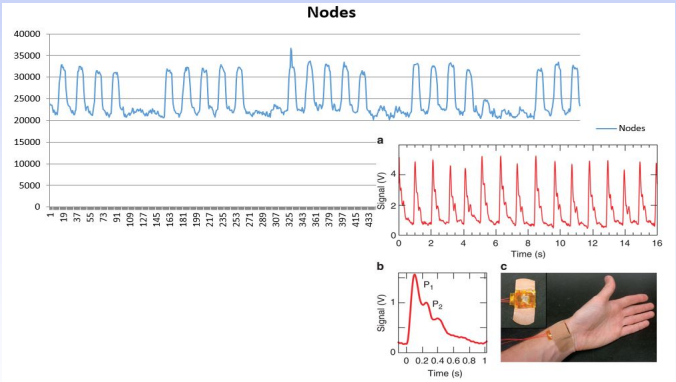
Cyber Situational Awareness continues to prove elusive to IT managers in all sectors of society. Although many tools exist to provide information about what is occurring in cyberspace for organizations, to date, no tool exists that gives information owners perfect awareness. This project aims to improve cyber situational awareness by utilizing network level measures. One full month of Netflow data was collected from a live boundary router on an operational network. The Netflow was partitioned into four categories: human driven inflow, human driven outflow, autonomic inflow, and autonomic outflow. Then, the data was analyzed with ORA's built in dynamic network analysis and change detection tools.

What is Netflow?



One hour of Netflow visualized in ORA

Periodicity clearly detected in nodes present for each one hour meta network of autonomic inflow



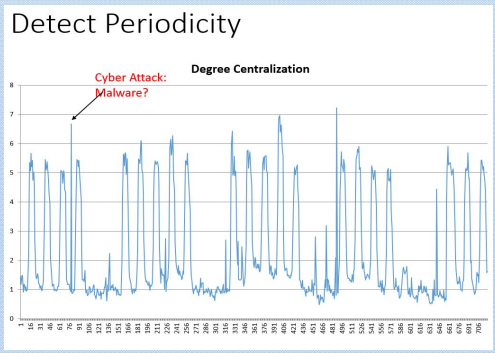
Collect Autonomic Inflow

Bytes = 1 – 96, no flags, packets < 3

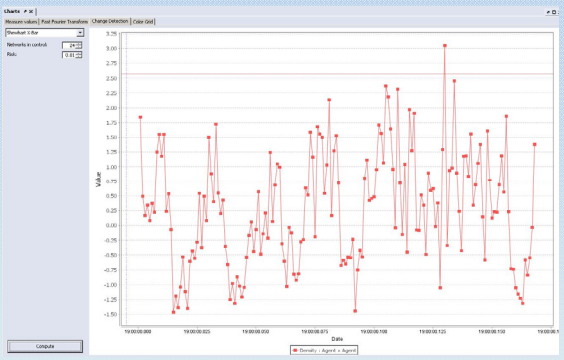
```
gdobson@silk:~
for i in {0,1}{0,1,2,3,4,5,6,7,8,9} 20 21 22 23; do
rwfilter --start=$1'T'$i --type=in,inweb --bytes=1-96 --packets=1-2 --pass=stdout |
rwcut --fields=1-2 -delimited=',' >ai$i.csv
done
```

Create Dynamic Meta Networks

Results



Results



This project provided a proof of concept that network level measures can provide improved cyber situational awareness. Standard volume based netflow analysis lacks level of detail that network science can provide. Future work will include attributing network change detection results to operational network anomalies.

This work was supported in part by the Office of Naval Research (ONR) through a MURI N000140811186 on adversarial reasoning, and the Center for Computational Analysis of Social and Organization Systems (CASOS). Data was provided by the city of Pittsburgh, with support from CERT at the Software Engineering Institute. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, CERT, the city of Pittsburgh, or the U.S. government.

isr institute for SOFTWARE RESEARCH