Monitoring Trends in Network Flow for Situational Awareness

Soumyo D. Moitra
SEI CERT NetSA

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Introduction

Network monitoring plays a vital role in network security and network situational awareness

Monitoring > traffic data over time

Time series data > Spikes, trends, periodicities

Some attacks may result in other changes in patterns

Underlying patterns often difficult to discern

Overview

Propose some new metrics to track changes

Four groups of metrics

Estimate ***relative changes***

Output can be displayed as a dashboard

Possible extensions

References

Proposed metrics

A) Parameters from the distribution

{Mean; Std. Dev. Skewness Kurtosis}

B) Percentile-based

{10% 30% 70% 90%]

- Robust around median
- Remove outliers

Soumyo D. Moitra
NetSA/CERT SEI

Time Series-based Metrics

Time domain

> autocorrelation (by lags)

>partial autocorrelation (by lags)

ARIMA models

> “autoregressive” component (PACF)

> “moving average” components (ACF)

C) Track ACF(1) ACF(2) ACF(3) PACF(2) PACF(3)

Can be extended to more lags

Soumyo D. Moitra
NetSA/CERT SEI

Other time series properties

D) Trends and Variances

Linear trend

Quadratic trend

Burstiness (alternative measures)

Heteroscedasticity (variance of the variance)

Extension: “Self-similarity”

Estimation

For all measures:

D = [m(2) – m(1)]/m(1) ~ Relative change

- Display on dashboard
- Keep repeating over each pair of consecutive periods

Alerts based on thresholds:

D > T

Situational Awareness and Alerts

Setting a threshold:

CI-based | Need trial data; location specific

Set from empirical experience

Calibrate to balance FPs and FNs

Setting Alerts | Threshold

1. Any individual D > T
2. Function of the Ds: A(D; w) > L
3. Special case: Alert when *n* out of the 16 Ds are greater than T
4. Calibrate thresholds for the individual Ds

Indicator I(i) = 1 if any D(i) > T(i)

0 otherwise

> Alert if ΣI(i) ≥ n

Soumyo D. Moitra
NetSA/CERT SEI

Simplified Algorithm

Select an IP set (or IP) of interest

Select other conditions (service/protocol/ports/etc.)

Decide on time periods to compare (24 hours or other)

Decide on bin size (time slices to compute the time series)

Set data collection for two preceding time periods

Collect the two time series data

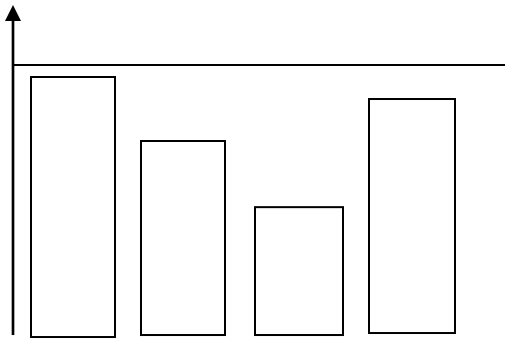
Estimate the 16 metrics (4 each in the four groups)

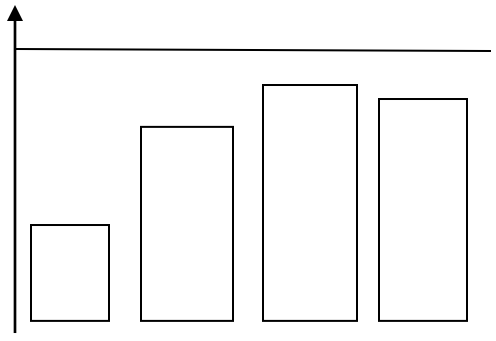
Decide on thresholds

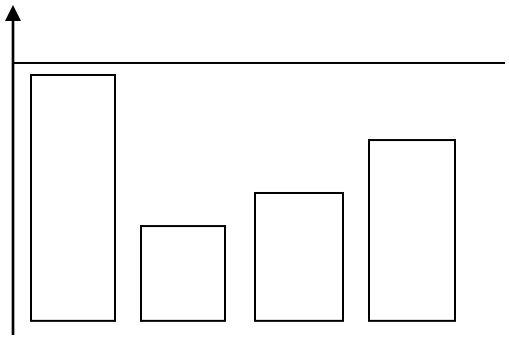
Display /(Set alerts)

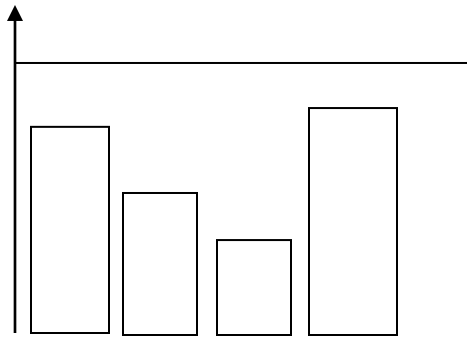
Soumyo D. Moitra
NetSA/CERT SEI

Example of a dashboard









Soumyo D. Moitra
NetSA/CERT SEI

Conclusions and Future Directions

Proposed some new metrics to extract more information from flow data

Try out with known test cases

Try alternative metrics

Develop and validate interpretation of these metrics

Generalize to other analyses: DNS traffic

References

Statistics

Statistics for Business and Economics
D. R. Anderson, D. J. Sweeney and T. A. Williams

Multivariate Data Analysis
J. F., B. Black, B. Babin and R. E. Anderson

Statistics for Business and Economics
J. T. McClave, P. George Benson and Terry Sincich

Time Series

Introduction to Time Series and Forecasting - P. J. Brockwell and R. A. Davis

Introduction to Time Series Analysis and Forecasting
D. C. Motgomery, C. L. Jennings and M. Kulhaci

Times Series Analysis – G. E. P. Box, G. M. Jenkins and G. C. Reinsel

Security Metrics

IT Security Metrics
L. Hayden

Complete Guide to Security and Privacy Metrics
D. S. Herrmann

Security Metrics
A. Jaquith

Statistical Packages: Any standard package

THANK YOU!

smoitra@cert.org