New Statistical Measures for Network Security

Soumyo D. Moitra

Carnegie Mellon University

smoitra@cert.org

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

How much protection to provide to a network?

Prioritization for allocation of resources

What factors determine the need for protection?

Answer: Many potential factors

Focus > **Visibility**

[UNCLASSIFIED]

Concept of Visibility

Analogous to famous/visible individuals

Outgoing information

Volume of out-going traffic

Range of “receiving units”

Weighted index

A composite metric

[UNCLASSIFIED]

Soumyo D. Moitra
NetSA/CERT SEI

Measures and Notation

Volume of out_traffic

- by destination j {v(j)}
- total volume {V}

Range of destinations {R}

- [Threshold]

Weighted index ~ proportion of traffic to j

$p(j) = v(j)/V$

Composite index: I * V * R

[UNCLASSIFIED]

Index: Measures of Diversity

Simpson:
$1 - [\{\Sigma v(j)*(v(j) - 1)\}/\{V(V-1)\}]$

Greenberg:
$1-[\Sigma\{p(j)^2\}]$

Entropy: (Shannon)
$-\Sigma[p(j)*\log\{p(j)\}]$

Out of several others: -> Greenberg Diversity Index (GDI)

[UNCLASSIFIED]

Composite Metrics and Scaling

A) GDI by itself

B) V * GDI

$$V' = V/V_{max}$$

C) GDI * R

$$R' = R/R_{max}$$

D) V * GDI * R

[UNCLASSIFIED]

Soumyo D. Moitra
NetSA/CERT SEI

Applications: Changes/Trends/Interactions

Three Metrics:

GDI	GDI*V’	GDI*V’*R’
(Basic)	(Weighted)	(Composite)

Distribution of each metric over i (or origins)

Identify outliers & Investigate

Correlate with specific external hosts

Variations and Trends; Comparisons across networks

[UNCLASSIFIED]

Initial Indications

Illustrative Example from Randomized Data
Two Hosts; Two time periods
GDI increased for both hosts
V*GDI balances out
GDI*R tends to be stable
V*GDI*R sensitive to changes
They reflect alternative aspects of “Visibility” OR “Internet Footprint”

Statistical Properties:
V ~ Exponential
GDI ~ Uniform
R ~ Poisson
Composite > Product of these distributions
Effect of scaling

[UNCLASSIFIED]

Thank you!

smoitra@cert.org

[UNCLASSIFIED]