Situational Awareness Metrics from Flow and Other Data Sources

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

Need a more flexible set of metrics for
network situational awareness

-Aggregate (over large IP sets)
-Composite (multiple measures or counts)
-Can detect changes in traffic patterns
-Amenable to visualization
-Fast and scalable (simple algorithms)

Overview

Propose some new metrics for SA

Uses Flow Data

Some require additional data:

- Information on Assets
- Organizational Level Data
- Elicited Data
- Various Lists of Sites/Hosts/Domains

- DNS
- Topology

Proposed metrics

Threats - Risks - Impacts

A) Mainly flow data and results from SIMS

N(attack category) – N(method of operation) – N(system or host)

Estimate (N): <TP> + <FN> | exercises & pen tests

B) Flow and other data

Match attack sources with malicious domain lists

- intersection of the IP sets

Implementation levels & Compliance levels

- priority of patches or tasking orders
- criticality of hosts

Probabilities of success * Expected damage | Attack category

Flow-based Metrics: Threats

N(i) | {I} = distribution of attacks by category i in set {I}
= attack scenario

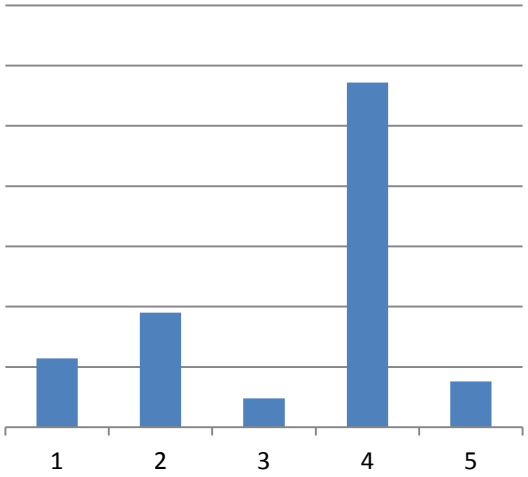
[w(i)*N(i) | $\underline{w}$] = seriousness-weighted attack distribution
= attack intensity

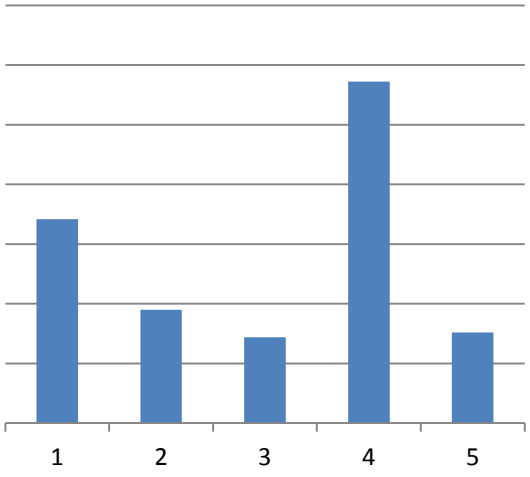
Σ_i[w(i)*N(i)] = Overall seriousness > Trends

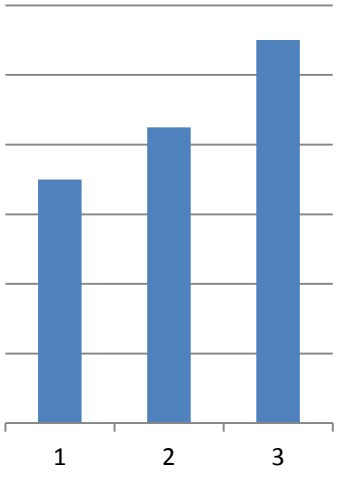
[Σ_iw(i) = 1]

Soumyo D. Moitra
NetSA/CERT SEI

Illustrative Example: Numbers, Intensity, Trends







Soumyo D. Moitra
NetSA/CERT SEI

Flow-based Metrics: Risks

N(m) = Distribution of attacks by “method of operation”

[s(m)*N(m)|s] = Severity-based risk scenario

Σ_m[s(m)*N(m)] = Overall severity metric

$[\Sigma_m s(m) = 1]$

Flow-based Metrics - Impacts

N(h) = Distribution of attacks by system/host “h”

[v(h)*N(h)|v] = Value-weighted impact of attacks

Σ_h[v(h)*N(h)] = Overall value of network assets
that are being attacked by their attack rate

Other Data Needed

{Attack Categories} and {Relative Seriousness}

{Taxonomy for MOs} and {Potential Severity}

{Classification of Network Assets – value & criticality}

{True Positives | Alerts & Verification} and {False Negatives}
<- Exercises and Testing

{Lists of Malicious Domains/Ips} [Some exist]

{Status of Assets w.r.t. Compliance: Yes/No |patch or TO}

{Success rate of attacks by category | recent reports}

{Expected damage from successful attacks}

Estimation of metrics based on non-flow data

Maliciousness of Attacker Set:
{A} ~ attacker set
{M} ~ lists of known malicious hosts
{A} ∩ {M} = Degree of Attribution by Maliciousness

Risk ≡ Non-compliance (+ other factors) >> Compliance level
$\Sigma_h J(h,p)*c(h) / \Sigma_h Y(h,p)*c(h) = I(p)$ = Implementation level of patch p
$J \supset Y$
$\Sigma_p u(p)*I(p)$ = Compliance level with respect to patching
Compliance by criticality & urgency

Impact:
Likelihood * Consequence
= π * D = {probability of successful attack * expected damage}

{π(k) * D(k); by level of damage k}

Benefits for Situational Awareness

New metrics to supplement current measures

Additional aspects of SA

Identification of important data to be collected

Fast estimation procedures

Can track changes over time

Summary and Conclusions

Summary

Set of SA metrics: ***Threats-Risk-Impact***
Properties and interpretation of the metrics
Flow data and additional data (as identified)
Benefits from applying these metrics

Key Challenges

A processing and analysis layer between queries & reporting
Data availability
Problems with the numbers (NATs, Proxies, inconsistencies, etc.)

Future Work in Brief

Develop, validate & interpret these metrics
Collect the needed data systematically
Include the intermediate analytics capabilities

THANK YOU!

smoitra@cert.org