Improving Cyber Ecosystem Health through Metrics, Measurement and Mitigation Support

GFCE Community Showcase
September 2021
Yurie Ito
Executive Director, CyberGreen Institute
The CyberGreen Institute is a global non-profit organization focused on helping to improve the health of the global Cyber Ecosystem.

- Cyber Health Measurement. We measure **Risk-to-others**.
- Conduct weekly Internet scans for risk condition data
- Provide a clearinghouse for Risk Mitigation BCPs.
- Capacity Building needs analysis and impact measurement
- Advocacy

A global community to measure and improve cyber health

Copyright © CyberGreen 2021 All Rights Reserved.
Who we are

Dr Paul Twomey
Board Chair CyberGreen, Former President of ICANN

Dr Richard Soley
Board and treasurer of CyberGreen, Executive Director Industrial Internet Consortium
CEO and Chair of OMG

Prof Jun Murai
Board director, CyberGreen
Dean Keio University, Father of Internet Japan

Yurie Ito
Board Director, Executive Director, CyberGreen

Arastoo Taslim
Director of CyberGreen Business Operation

Technical Collaborator

Adam Shostack
Author of “Thread modeling”
President at Shostack Associates
Applying Public Healthcare approach to Cyber

Incidents;
Patients disease counts
e.g. Malaria Patients counts

Transmission vector;
e.g. mosquitoes counts,

Environmental Conditions;
e.g. level of untreated swamp water, Hygiene level

Presence of Malware, Botnets Infection

Number of observable Incidents

OS Update, Misconfiguration, Vulnerable nodes, Education, Readiness,
CyberGreen: What we do

- Collect and analyze data for five open recursive protocols (NTP, DNS, SSDP, SNMP, CHARGEN) commonly used to execute DDoS reflection attacks
  - stats.cybergreen.net

- Conduct Cyber health check-up and analyze policy and mitigation needs for improvement
  - ASEAN Internet Health Analysis (Economic Research Institute for ASEAN and East Asia sponsored)
  - East Africa Internet Health Analysis (GFCE and World Bank workshop)

- Develop robust metrics to measure cyber health
  - (Phase 1) Internet Infrastructure Health Metrics Framework v.1 in 2020
  - (Phase 2) Developing Internet Public Health Scoring Prototype System in 2021
  - (Phase 3) Feasibility study and scoring operation in 2022
  - (Phase 4) Policy design, Advocacy beyond 2023
Internet Infrastructure Health Metrics Framework
The Internet Infrastructure Health Metrics Framework (v.1) (IIHMF)

- The Internet Infrastructure Health Metrics Framework (IIHMF) is a set of models and metrics to measure the “public health” of Internet infrastructure.
- The IIHMF will allow states to measure their overall risk, understand how it changes over time, and compare to other states.
- It also enables us to measure the health of Internet infrastructure using metrics and a model based on public health.
In the context of being able to diagnose the health of Internet Infrastructure, we have classified six components based on a combination of underlying, fundamental technologies and services. We grappled with what counts as Internet Infrastructure, and what is measurable from quantitative measurement perspective.

- Open Services
- Routing
- Domain Name System
- Email
- Certificates
- Security protocols & services

We will continue to refine the definition of critical Internet infrastructure.
<table>
<thead>
<tr>
<th>Indicator</th>
<th>Open Services</th>
<th>Open DNS</th>
<th>Open SNMP</th>
<th>Open SSDP</th>
<th>Routing</th>
<th>Domain Name Service (DNS)</th>
<th>Email</th>
<th>Certificates</th>
<th>Security protocols &amp; services</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHARGEN</td>
<td>Number of CHARGEN open ports (UDP19)</td>
<td>Number of DNS recursive resolvers that answer to any query (UDP 53)</td>
<td>Number of SNMP servers that answer to any query (UDP 161)</td>
<td>Number of SSDP servers that answer to any query (UDP 1900)</td>
<td># of ROA</td>
<td>No of domains with DNSKEY Resource Records</td>
<td>DMARC implemented</td>
<td>Digital certificate: % of certificates that expired and validity needed to be updated</td>
<td>SSL / TLS protocol versions accepted for negotiation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bad ROA payloads</td>
<td>Invalid routes</td>
<td>Not registered routes</td>
<td>Are they using, managing ROA</td>
<td>Number of zones that have a public/private key pair associated with it</td>
<td>DMARC policy</td>
<td>Policies that pass &quot;implemented&quot; include &quot;none&quot;, &quot;quarantine&quot; and &quot;reject&quot;</td>
<td>SSL/TLS Cipher Suite Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>There's a problem if someone is issuing bad ROA</td>
<td>Whether multiple keys are valid and in use</td>
<td>Servers that support STARTTLS</td>
<td>DMARC policy</td>
<td>Digital certificate: algorithm used to generate key pair</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Key sizes and algorithms in prevalent use</td>
<td>SPF implemented</td>
<td>Whether digital certificates which instantiate identity or give authorization are used while being invalid</td>
<td>SSH Version</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Key sizes</td>
<td>Digital certificate: key lengths used</td>
<td>Key sizes in prevalent use</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Health Metaphors

(1) Medicine

Much of the work on enterprise risk management is analogous to medicine

• One goal of this work has been to create a framework similar to physical health related aspects where yearly health checkups result in indicator data measurements (e.g. cholesterol levels, creatinine levels, blood sugar levels) and the results are used in a diagnostic process to assess certain health risks.
Health Metaphors

(2) Public Health

Public health complements medicine; Cyber public health complements enterprise risk management

- Public health’s focus on the health of communities.
- Focus on harms of various sorts to health of communities
- Public health allows us to look at things which impact an individual (lack of exercise), other specific people (communicable disease), or communities (pollution).

- Cyber public health includes the health of others and the unhygienic conditions which allow other problems to thrive.

→ CyberGreen’s IIHMF scoring
Risk Models

Framing technical risks to Public Health

This IIHMF is designed to align the technical risks and mitigations to commonly understood public-health concepts.

- As part of this work, we crafted three models which connect computer security issues to public health. Each is focused on the impact of an activity, and thus we call them Impact Model 1, Impact Model 2, and Impact Model 3.

- For this phase of this project, we are using **Impact Model 3**.

- Impact Model 3 is simply that a problem has, as its most obvious outcome, either harm to self or harm to others:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Primary harm</th>
<th>Explanation</th>
<th>Other effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out of date software</td>
<td>Harm to self</td>
<td>Attacker runs code on my computer; Attacker installs a bot used to attack others</td>
<td></td>
</tr>
<tr>
<td>Misconfigured software</td>
<td>Harm to self</td>
<td>Attacker reroutes my network packets because of a lack of ROA.</td>
<td></td>
</tr>
<tr>
<td>Open port (amplification)</td>
<td>Harm to others</td>
<td>Attacker uses my computer for DDoS amplification</td>
<td>I spend more on network fees</td>
</tr>
</tbody>
</table>
Internet Infrastructure Health Scorecard

• We seek to measure a set of things which we believe are crucial to an assessment of public health of Internet infrastructure.
• Having measured those, we can put them into a “scorecard”

Next Step:
• Create a formula for an Internet infrastructure health scorecard, and engage with local and international civil society on its content and uses.
• Run a pilot to measure internet infrastructure health and engage with the questions raised by preliminary data collection, analysis and comparison.
Overall process of scoring system

1. We compile a list of components and indicators, based on selection criteria which includes being externally visible and measurable.

2. We define a list of targeted systems by IP address, domain or other qualifier.

3. We perform some set of measurement activity, and record direct output of measure 1, measure 2, etc.

4. We conduct evaluations by applying criteria to the output. For example, one criterion might be that only TLS 1.3 or keys longer than 1025 bits are acceptable.

5. For some measures, we can simply say “there is an open port 19” and, knowing that port 19 can be used in attacks, continue. For other measures, we need to evaluate what we see (is a certificate still valid?). In each case, the measures are recorded in a results database.

6. With those results and a set of weighting, scoring and normalization choices, we can select data either or both by country or over time, and produce reports or scorecards.
2021 – 2023 plan and call for collaboration
Proposal-1

Mitigation Inhibition Study

- Mitigation inhibition study - why are people not mitigating, and which mitigations are effective? This can start with either a literature review or a particular mitigation which "appears obviously good" in some sense, analysis of why it's not happening, and what might be done about that
Proposal-2

General support and Participation to the feasibility study
High level IIHMF plan over the next three years:

Promote cyber public health to make digital society resilient against cyber problems using metrics and measurement

- **2021**
  - Internet public health model / scoring R+D

- **2022**
  - Feasibility/case study
  - Refine/expand scoring system

- **2023**
  - Cyber Health Org
  - Professional service of cyber public health measurement and scoring

Copyright © CyberGreen 2021 All Rights Reserved.