Lies, Pseudoscience, & Hype in the Cybersecurity of Human Factors

Jonathan M Spring

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL 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.

DM20-0947

Lie: “Experts do not need usability”

Security experts have a variety of specialties[1]

- Event monitoring
- Incident management
- Situational awareness
- Vulnerability management

Although the details change, systems used by experts almost never have the usability for the expert considered.

[1] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Areas of concern

- Intelligibility of measurements
  - Hinders inter-organizational communication, especially experts across sectors
- Consistency of human scoring
  - usability of the scoring system, gets into issues of language, non-native English speakers, etc.
- Timely delivery of scoring
  - For example, for CVSS humans need to create the scores

Example

Common Vulnerability Scoring System (CVSS)

- “an open framework for communicating the characteristics and severity of software vulnerabilities.” (https://www.first.org/cvss/specification-document)

Example: **CVE-2019-0708 Base Score:** 9.8 CRITICAL

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Assignment is inconsistent, standardization is opaque, target is one-size-fits-all

The general tone is that if the scoring system doesn’t work for you, it’s your fault

I’m working on a more usable alternative (https://github.com/CERTCC/SSVC)

- Stakeholder-specific Vulnerability Categorization

Discussion

Thanks very much!

spring [@] cmu [dt] edu [dt]