Draft Consumer Software Labeling Criteria

Paul Wertz and Sushmita Senmajumdar

NIST GCTC-Smart Secure Cities and Communities Challenge: Smart Security and Privacy (SSP)1

December 15, 2021

Comments

1. If the target audience is the consumer, there needs to be a real simplification in presentation.

- Date relevancy
  What date was this software deemed compliant? How do I check to see if there have been any updates since then?
- How simple can you really make it
  labeling examples discussed included food, cigarette, Material Safety Data Sheets or MSDS for public safety.
- What data will the public deem important?
  Hide complexity behind common terms that the consumer cares about. What is included on the label (software language, dependencies, authors, etc.)
- Issue handling
  The consumer needs to know whom /where to contact for updates /issues. The manufacturer, or the consumer?

2. Supporting activities to make it a success

Should there be a certification process and what would that look like? Would there be a good, better, best framework? If so, how does this fit into the different categories:

- What data is impacted (financial, healthcare, location, etc.)?
- Who would own the certification process or would companies self-certify?
- Who would own the liability for any problems?
- Would compliance provide any legal protection?
- Could the label potentially not give specifics, but rather represent a maturity level? This could be applied to the software or the organization.

3. Time factor

The Software Bill of Materials was seen as a static representation of a dynamic environment and as such must provide at least two things. First is a point of reference in time (being when

the software was created and then certified). Second would be a resource that can be engaged to check status, this can be a certifying body, or a link with documentation.

4. A question on using software composition analysis (SCA) tools in a CI/CD pipeline asking if the Software Bill of Materials tell you anything the SCA doesn't? (Assuming the SCA tool has a comprehensive software catalog). This led to asking about possible conflicts in certification, and what might be legal ramifications? Would this possibly lead to an automated scanning or would it remain a manual process?

5. There was also some discussion of how logging would be managed. Would there be a requirement to see events in a historical context?

In summary, the feeling was that there will be an evolution in labeling. Parties will develop a more appropriate understanding as time goes on. This will lead to a trusted label, or brand where consumers will use a form of shorthand that allows them to make a quick decision based on trust, as the recent Log4J responses and the earlier CMMC handling by the federal government have demonstrated.

Background

The Smart Security & Privacy supercluster (SSP) is a public private partnership that supports NIST GCTC Smart Secure Cities and Communities Challenge https://pages.nist.gov/GCTC/. SSP held a virtual meeting attended by 20 participants to discuss public input on Consumer Cybersecurity Labeling for IoT products on December 14th,2021, The participants represented a wide variety of interests including individuals with experience in business development, software development, network management, software deployment, and consumer engagement. We had private, government and non-profit points of view represented.

https://smartsecurityprivacy.org/

https://www.linkedin.com/company/nistgctcsmartsecurityprivacy/