**Ke, Jessica - Intern**

| | |
|---|---|
| **From:** | brook@brookschoenfield.com |
| **Sent:** | Wednesday, June 2, 2021 6:04 PM |
| **To:** | SBOM_RFC |
| **Subject:** | SBOM Comments |

Why should NTIA listen to me?
— I'm the author of 6 books on software security specializing in secure designs and threat modelling
— As a Principal Engineer at Intel, Inc. (Intel's Distinguished Engineer title) I contributed to a SBOM concept (IOW, I have experience with SBOM frameworks)
— I wrote one of the first sets of vendor security criteria when at Cisco, 2005 (still published by Cisco)
— I've technically led 5 security architecture practices. I've assessed hundreds of vendors and 3rd party/OSS components.

If you're convinced that I may have some expertise to offer, here are among the most important conceptual things to consider when creating an SBOM Framework:

1) The threat model is NOT a sum of the threat models of all the components! This is critical to understand: adding a component may add one or more of: Attack surfaces (attack entry points), attack objectives (from attacker's perspective), weaknesses (design or implementation), potential for negative impacts to the whole, use cases, threat possibilities, etc. As we saw in the Target breach, the failure to account in the organization's threat model for the HVAC vendor's security created an opening that resulted in a 30% loss of revenue. Please see Secrets Of A Cyber Security Architect, "4.3.6 Threat Models Are Not Additive!" page 99 for a more detailed analysis of the problem.

2) The most important interaction between components are the assumptions about security (which rarely get discussed, and are documented even less, unfortunately). There's a need for a "security contract" between interacting components. Each interacting component must understand what assumptions have been made by the other components. Of particular concern are assumptions about which component is providing what security needs. Again, on page 99 of Secrets Of A Cyber Security Architect is a discussion and example about security assumptions and contracts. Important for this discussion, if the SBOM does not provide a method for components to declare the controls and defences they have taken, and the precautions that a component expects other, interacting components to take, the SBOM is pretty useless, because security misses will be passed right through any interaction chains without foreknowledge. Which means that consumers of the SBOM components will end up with unmet security needs.

3) Listing vulnerabilities is not enough! Many reported issues never get exploited. According to the mounting body of research in this area (start with Alloddi & Massacci's ground breaking paper 2014), only a small percentage of issue actually get exploited (the research does not agree on the percentage, but I've never seen more than ~25%). Hence the presence of a vulnerability that will never be exploited does not, in and of its presence mean much. Please see Cyentia+Kenna's EPSS research paper (2019) Plus, there are situations where the mere presence of a vulnerability presents very little risk due to other factors: the containing software is not called, or perhaps the vulnerability can only be called with high-privileges that already allow the attacker the leverage that exploitation would grant, etc. there are lots of scenarios where vulnerability exists != actual risk. Taking a vulnerability-count approach merely continues the security industry's fascination with vulnerability without accounting other factors that may increase, decrease, or even virtually eliminate risk. Not every vulnerability is of equal value to attackers, which is what's missing in CVSS (please see any one of my several posts about CVSS' misuse as a risk rating)

I’d love to see what’s been planned for SBOM so that I may comment more specifically.

There was no further collateral other than “comment period” on the announcement that came through my twitter feed. Apologies if you’ve already considered the above problems.

If you want more help from me, all you have to do is ask.

Thanks,

/brook

brook s.e. schoenfield
Author, passionate security architect
Curious questioner
www.brookschoenfield.com