IDS WG Meeting Minutes
September 8, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on September 8, 2022.

Attendees

Jim Gorski	Xerox
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Mike Trent	Xerox
Brian Volkoff	Ricoh
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
    - Review of the HCD iTC Meetings since our last IDS WG Meeting on 8/11/22
    - Special Topic on the Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e
    - Round Table
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust- policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al provided a quick summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 8/11/22:
    - Al stated that since the Final Drafts of v1.0 for both the HCD cPP and HCD SD were submitted for public review on August 1st, with comments due to the HCD iTC by Sep 5th, the HCD iTC has spent all the meetings since the 8/11/22 IDS WG Meeting reviewing comments against the Final Drafts of both the HCD cPP and HCD SD.

      What was significant is that in the period between Aug 31st and Sep 5th a large number of comments came in. This was something that Ira McDonald predicted would happen over a year ago, because the Final Draft is often the first time many reviewers actually take the time to review the documents. What was important in the comments that came in after Aug 31st was that most of them came from either the Japanese Scheme JISEC, the Korean Scheme ITSCC, various members of JBMIA, or individuals associated with NIAP. Also, most of the comments that came in after Aug 31st were more technical in nature rather than editorial in nature. Al went through several actual examples of the types of comments received from ITSCC, JISEC and others to show what types of technical issues were being raised at this late date.

      Al then went through the schedule slide he had presented at the IDS Face to Face Meeting (F2F) on Aug 18th. The official schedule had called for:

        - Submit Final Draft: 7/18/22
        - Review Final Public Draft: 7/19/ – 8/22 (28d)
        - Review comments and update documents: 8/23/22 – 9/6/22 (10d)
        - Publish Version 1.0: 9/7/22

      At the IDS F2F Al had indicated that since both the HCD cPP and HCD SD Final Drafts had been submitted for review on 8/1/22 and comments were due on 9/5/22, the schedule was already 3 weeks behind. Based on that Al at the time expected that barring any large number of comments the best case would be that HCD cPP v1.0 and HCD SD v1.0 would be published around the end of Sep or beginning of Oct.

The number of comments received during the first week of Sep, and the technical nature of many of these comments caused Alto change his assessment of when HCD cPP v1.0 and HCD SD v1.0 would likely be published. Given that fact that there are a large number of comments that came in the first week of Sep and the fact that technical comments take longer to address than editorial comments, Al felt that it would take the HCD iTC through all of Sep and probably all of Oct to go through and resolve all of the comments. Based on that Al feels that now the earliest that HCD cPP v1.0 and HCD SD v1.0 would be published would be around the end of Oct or beginning of Nov 2022.

- Al then went through the HCD iTC Interpretation Team (HIT) information he presented at the August IDS F2F (see the minutes from the August IDS F2F at https://ftp.pwg.org/pub/pwg/ids/minutes/ids-f2f-minutes-20220818.pdf for the HIT information), because the HCD iTC will have to set up the HIT (e.g., agree on the HIT procedures, determine how many will be on the HIT and who they will be) before the HCD cPP v1.0 and HCD SD v1.0 are published. To date, the only HIT-related item done is a draft set of HIT procedures that have to be reviewed by the iTC. Al noted this factored into the determination that it would be the end of Oct 2022 at best when the HCD cPP and HCD SD would be published.
    - the time frame for the minor and major releases will be.

4. Al then went through his special topic for the meeting, which was a review of Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e, one of the documents he mentioned at the talk he gave at the 7/14/22 IDS WG Meeting and the 8/18/22 IDS f2f Meeting on the progress that had been made on implementing the Executive Order (EO) 14028 on Improving the Nation's Cybersecurity since it had been issued in May 2021. The slides Al presented at the meeting can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Software Supply Chain Security Guidance.pdf.

   Some of the points Al made while reviewing the guidance were:

   - To put things in proper perspective, Executive Order (EO) 14028 Section 4e states "*Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section*".

     In response to Executive Order (EO) 14028 Section 4e NIST issued NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities. However, NIST SP 800-18 is written from the perspective of a software developer or software producer. The purpose of the Software Supply Chain Security Guidance was to address Section 4e from the prospective of a Federal Agency procuring software to help Federal Agencies ensure "that the producers of software they procure have been following a risk-based approach for secure software development throughout the software life cycle"

   - The scope of this guidance is Federal Agency procurement of software, which includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software; i.e., all software developed for Federal Agencies. That includes Open-source software that is bundled, integrated, or otherwise used by software purchased by a Federal Agency.

     The only software not in scope of this guidance is software developed by Federal Agencies or open-source software freely and directly obtained by Federal Agencies.

- To properly understand the guidance in the document, the following key terminology is necessary:
  - ***Conformity assessment***: a "demonstration that specified requirements are fulfilled"
  - ***Attestation***: the "issue of a statement, based on a decision, that fulfillment of specified requirements has been demonstrated"
  - If the software producer itself attests that it conforms to secure software development practices, this is known by several terms, including ***first-party attestation***, ***selfattestation***, ***declaration***, and ***supplier's declaration of conformity (SDoC)***
  - If the software purchaser attests to the software producer's conformity with secure software development practices, this is known as ***second-party attestation***
  - If an independent third-party attests to the software producer's conformity with secure software development practices, this is known as ***third-party attestation*** or ***certification***

    Al noted that Common Criteria certification is definitely a type of third-party attestation, especially under the old "EAL" approach for EALs 3 and greater.
  - ***Artifact***: "a piece of evidence."
  - ***Evidence***: "grounds for belief or disbelief; data on which to base proof or to establish truth or falsehood"
  - **Low-level artifacts** will be generated during software development, such as threat models, log entries, source code files, source code vulnerability scan reports, testing results, telemetry, or risk-based mitigation decisions for a particular piece of software.
    These artifacts may be generated manually or by automated means, and they are maintained by the software producer
  - **High-level artifacts** may be generated by summarizing secure software development practices derived from the low-level artifacts. An example of a high-level artifact is a publicly accessible document describing the methodology, procedures, and processes a software producer uses for its secure practices for software development.
- The key guidance in the document is:
  - When a federal agency (purchaser) acquires software or a product containing software, the agency should receive attestation from the software producer that the software's development complies with government-specified secure software development practices

    The essentially means that software producer has to attest that they have a secure software development process following the framework in NIST SP 800-218 or something similar.
  - The federal agency might also request artifacts from the software producer that support its attestation of conformity with the secure software development practices described in Section 4e subsections (i), iii), and (iv).

    Al pointed out that artifacts that will be required will be something new for both most Federal Agencies and many software producers.
  - Prescribed software practices in Section 4e are:
    - *(i) secure software development environments, including such actions as:*
      - *(A) using administratively separate build environments;*
      - *(B) auditing trust relationships;*
      - *(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;*

      - *(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;*
      - *(E) employing encryption for data; and*
      - *(F) monitoring operations and alerts and responding to attempted and actual cyber incidents;*
    - *(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;*
    - *(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;*

  Al noted that the practices noted on this list, like encryption of data, multi-fact authentication, auditing and checking for known vulnerabilities, are the types of practices that are included as requirements in the HCD cPP.

  In discussing checking for known vulnerabilities, Bill asked how this was done for Open Source or 3rd Party Components. Brian stated that part of the solution is that the software producer has to produce a Software Bill of Materials (SBOM) that lists all the components, including Open Source or 3rd Party Components, and their version. This led to a good discussion which, in summary, answered Bill's question by saying that the way you check for vulnerabilities in Open Source or 3rd Party Components is:

  - Once you know the version of each Open Source or 3rd Party component you can check one or more of available public national vulnerability databases for known vulnerabilities against the version you have of each component.
  - You then do the manual (and often time-consuming) analysis to determine whether your software product is or is not vulnerable to each of the known vulnerabilities found from the public vulnerability search.
    - If it isn't you provide a rationale why it isn't
    - If it is, you determine what type of mitigation is required and implement that mitigation

- Guidelines for Attesting to Conformity with Secure Software Development Practices
  - Use the SSDF's terminology and structure to organize communications about secure software development requirements
  - Require attestation to cover secure software development practices performed as part of processes and procedures throughout the software life cycle
  - Accept first-party attestation of conformity with SSDF practices unless a risk-based approach determines that second or third-party attestation is required
  - When requesting artifacts of conformance, request high-level artifacts

  Al indicated that this guidance could have a big impact in the future depending on what Federal Agencies adopt this guidance. For example, Al noted that since Common Criteria provides a known and accepted third-party attestation method, implementation of this guidance could result in Common Criteria being applied in newer areas involving IoT applications, where procuring agencies (not just at the Federal level) might require some form of attestation.

  There is also the point that the guidance only requires high-level artifacts – i.e., policies and procedures – rather that the detailed types of artifacts Common Criteria certifications require. Al interpreted that to mean that the big concern was that the software producer had a documented secure software development process and that this process was being followed.

5. There was no Round Table for today’s meeting
6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be September 22, 2022 at 3:30P ET / 12:30N PT (Note the special late start time because of a doctor appointment). Main topics will be review of the HCD iTC Meetings since this IDS WG meeting and possibly a special topic.