IDS WG Meeting Minutes
July 14, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on July 14, 2022.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Jeremy Leber	Lexmark
Alan Sukert	
Mike Trent	Xerox
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 6/16/22
   - Special Topic on updated status of the Cybersecurity Executive Order of May 2021
   - 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 summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 6/16/22.
   - The HCD iTC and NIAP representatives had a meeting with Matsumoto-san from to discuss JISEC's request to make the FPT_WIPE_EXT.1 SFR mandatory. JISEC's main concern was that Cryptographic Erase (CE) had to be mandatory. The result of the meeting was that JISEC agreed that for Version 1.0 it was OK if FPT_WIPE_EXT.1 SFR remained an optional SFR as long as (1) CE was a mandatory selection in FPT_WIPE_EXT.1 SFR and (2) FPT_WIPE_EXT.1 SFR would become a mandatory SFR in a later version of the HCD cPP (preferably the next one). It turned out that NIAP would also prefer that FPT_WIPE_EXT.1 be a mandatory SFR eventually, but was also OK with it being an optional SFR in Version 1.0.
   - Another big issue was around what data was being encrypted and then "purged" by the CE function as part of the FPT_WIPE_EXT.1 SFR. This actually goes back to the FDP_DSK_EXT.1 (Protection of Data on Disk) SFR that requires that encryption be performed so that and Nonvolatile Storage Device does not contain any plaintext USER.DOC or TSF.CONF[1] data. The issue really centered around the question of how to address the situation where CE is performed

[1] USER.DOC (User Document Data): Information contained in a User's Document, in electronic or hardcopy form; USER.JOB (User Job Data): Information related to a User's Document or Document Processing Job; TSF.PROT (Protected TSF Data): TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable; TSF.CONF (Confidential TSF Data): TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE

on other data like USER.JOB or TSF.PROT that are encrypted that is not covered by FDP_DSK_EXT.1.

After much discussion it was determined that changes were required to both FPT_WIPE_EXT.1 and to FDP_DSK_EXT.1 to address the problem of addressing both the encryption of and the "purging" of customer-supplied data that wasn't categorized as either USER.DOC or TSF.CONF data.

- An Application Note was added to the FPT_WIPE_EXT.1 SFR as follows: "Cryptographic erase covers D.USER.DOC and D.TSF.CONF (as per requirement of FDP_DSK_EXT.1). Encryption of additional data types is optional; therefore, cryptographic erase may not apply to additional data types." The purpose of the Application Note was to ensure that since FPT_WIPE_EXT.1 was still an optional SFR that the use of CE was consistent with the requirements in FDP_DSK_EXT.1 from a requirements perspective, while still allowing for FPT_WIPE_EXT.1 and CE to apply optionally to USER.JOB and TSF.PROT data.
- A new TSS Assurance Activity was added to the AAs for the FPT_WIPE_EXT.1 SFR in the HCD SD as follows: "If FPT_WIPE_EXT.1 claims all the customer-supplied information is made unavailable using cryptographic erase only, the evaluator shall confirm that all the customer-supplied information is encrypted by the TSF according to FDP_DSK_EXT.1." This allowed for the optional use of CE for all encrypted data, including USER.JOB and TSF.PROT, as long as it can be shown that all the data has been encrypted.
- Another comment from Jerry Colunga involved Test 4 of the Test AAs for the FPT_WIPE_EXT.1 SFR. Jerry's concern was that the in the table associated with Test 4, the second row referred to Storage Media type as "Wear-Leveling Media (e.g., SSD)". However, non-magnetic media doesn't always have to be ware-leveling media; it could also be flash devices. To address this valid concern, the HCD iTC agreed to change the heading for this media type in the table to "Flash-based storage (including wear-leveling media)".
- Finally, JISEC felt that changes were also needed to the Organizational Security Policies (OSPs) in Section 3 of the Security Problem Definition in the HCD cPP for Storage Encryption (Section 3.5.4) and Purge Data (Section 3.5.7) to clarify that the two key destruction SFRs FCS_CKM.4 and FCS_CKM_EXT.4 both apply to CE.

  The issue with the phrasing for the sentence in Section 3.5.4 is that Storage Encryption is a mandatory SFR but FPT_WIPE_EXT.1 is an optional SFR, so the phrasing had to make sure it didn't imply that FPT_WIPE_EXT.1 was mandatory is any way. After some discussion, the HCD iTC agreed to add the following sentence to the definition of the OSP P.STORAGE_ENCRYPTION – "And the TOE shall provide a function that an authorized administrator can initiate to destroy encryption keys or keying material if the TOE supports a function for removing the TOE from its Operational Environment."

  For Section 3.4.7, the HCD iTC agreed to modify the Note at the end of the discussion of Purge Data in Section 3.4.7 to read as follows: Note: Cryptographic erase which is covered in the mandatory requirement of FCS_CKM_EXT.4 and FCS_CKM.4 can be used as a method to remove some parts of User Data and TSF Data, but it cannot be a single method to remove User Data and TSF Data unless all the data are encrypted.

Al indicated that at the latest HCD iTC Meeting on 7/11 the HCD iTC agreed that there would be no more changes to ether the FDP_UDU_EXT.1 or FPT_WIPE_EXT.1 SFRs; what we had as of this date was acceptable to JISEC, ITSCC and NIAP and would go into the Final Drafts of the HCD cPP and HCD SD.

- Finally, Al showed an updated HCD iTC schedule based on the status as of the 7/11 meeting. The previous schedule had the Final Drafts of the HCD cPP and HCD SD being published on 6/15 leading to Version 1.0 of the HCD cPP and HCD SD being published on 8/2/22. The new scheduled essentially delayed everything approximately 5 weeks as follows:
  - Submit Final Draft: 7/18/22

- Review Final Public Draft: 7/19/ – 8/22
- Review comments and update documents: 8/23/22 – 9/6/22
- Publish Version 1.0: 9/7/22

Al made the comment that at the May IDS Face to Face Meeting he had indicated that he thought that realistically Version 1.0 of the HCD cPP and HCD SD would probably be published around the end of August/beginning of September; this new updated schedule showed his thoughts at the time were correct.

4. Al then went through his special topic for the meeting, which was an update on the talk he had given back in 2021 on the Executive Order (EO) 14028 on Improving the Nation's Cybersecurity issued on May 12, 2021 by President Biden. The goal of this session was to update the meeting attendees on the progress that had been made on implementing the EO 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/Cybersecurity Executive Order Update.pdf.

   Al started of with a brief summary of what the key areas covered by of EO 14028 were:

   - Policy – Federal Government must
     - Bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
     - Must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).
     - Sharing Threat Information
   - Cyber Incident Reporting
   - Enhancing Software Supply Chain Security
   - Standardizing the federal government's playbook for responding to cybersecurity vulnerabilities and incident
   - Improving detection of cybersecurity vulnerabilities and incidents on federal government networks
   - Improving the federal government's investigative and remediation capabilities

   Then Al summarized the main documents that NIST has produced to date that resulted from EO 14028:

   - **Software Security Practices documents (Released Feb 4, 2022)**
     - Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-cybersecurity-producers-and)
     - NIST Special Publication 800-218, Secure Software Development Framework (SSDF) Version 1.1:Recommendations for Mitigating the Risk of Software Vulnerabilities (https://csrc.nist.gov/publications/detail/sp/800-218/final)
   - **Software Security Labeling documents (Released Feb 4, 2022)**
     - Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products (https://doi.org/10.6028/NIST.CSWP.02042022-2)
     - Recommended Criteria for Cybersecurity Labeling of Consumer Software (https://doi.org/10.6028/NIST.CSWP.02042022-1)
     - Consumer Cybersecurity Labeling Pilots: The Approach and Feedback (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/consumer-cybersecurity-labeling-pilots)

- Security Measures for “EO-Critical Software” Use Under Executive Order (EO) 14028 - (https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eocritical-software-use-2) – Published Jul 9, 2021
- NISTIR 8397 Guidelines on Minimum Standards for Developer Verification of Software (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/recommendedminimum-standards-vendor-or) – Published Oct 2021
- 2nd Draft of NIST Special Publication 800-161 Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (https://doi.org/10.6028/NIST.SP.800-161r1-draft2) – Published Oct 2021

Al indicated that he planned to do a more “deep dive” into several of these documents and present his analysis to the IDS WG at future meetings. For example, he had given a previous discussion on the draft of NIST Special Publication 800-218; now that the final Special Publication 800-218 has been released he wants to see what the differences are between the draft and final versions are – what has been added, deleted, changed, etc.

5. Round Table
   - International Cryptographic Module Conference (ICMC22) is Sep 14-16 in Arlington VA
   - International Common Criteria Conference (ICCC2022) is Nov 15-17 in Toledo Spain
   - Al and Paul Tykodi will be giving a paper on “Developing Common Criteria Based 3D Printing Equipment Cyber Security Certification**”** at the ASTM International Conference on Additive Manufacturing (ICAM 2022) in Orlando FL on Nov 4th
6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be July 28, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the HCD iTC Meetings since this meeting and a special topic.
- The next IDS Face to Face Session as part of the August PWG Face to Face Meetings is tentatively set for August 18th from 10-12 ET.