From: Perlner, Ray (Fed)
To: Chen, Lily (Fed)
Subject: Questions for 800-158 Review
Date: Tuesday, August 2, 2016 4:37:00 PM

---

1) Which of the following audiences do you think would benefit from reading SP 800-158?
    a. Protocol Designers
    b. Protocol Implementers
    c. IT Procurement Agents
    d. System Integrators
    e. System Administrators
    f. CMVP Test Labs
2) Is it reasonable to limit the scope of the document to "search resistance" (leaving authentication, collision resistance, online attacks, crypto misuse, and quantum-resistance out of scope)?
3) Is the calculation assigning a numerical value to the search resistance of a data protection key useful?
4) Do you think that NIST should
    a. Proceed developing SP 800-158 as it is currently scoped?
    b. Significantly alter the scope of the document. (e.g. focus more on examples of how a weak component can enable specific attacks elsewhere in the system)? Do you have suggestions for how we could do this?
    c. Redirect resources towards other projects which may address similar needs (e.g. by expanding our protocol-specific guidance in SP 800-57 part 3 and SP 800-52 to give more details or cover more protocols)? Can you give suggestions?