From: dig-comments@list.nist.gov on behalf of [redacted]
To: dig-comments@nist.gov
Subject: [dig-comments] 800-63C Commentary
Date: Monday, November 4, 2024 10:13:34 PM

Hi,

I'd like to provide some commentary / opinion on the draft NIST publication 800-63C.

I will be brief in stating that I am in broad and probably strongly agreement with almost all of the changes made to these password policies and believe that they are for the most part well balanced and will improve password hygiene.

However I do believe that the one missing element from the recommendations centre around Password hygiene around known bad passwords.

Last year I was engaged with a bank to perform a password audit of their clients after a number of account breaches. The results of that audit were shocking. The most common password in use was 12345678 followed by 87654321. The top 10 passwords in use were all on the "top 100 password" lists, and there were probably 100 passwords in "common" use across all end user accounts.

I believe the guidance should be enhanced with a requirement around known-password lookups for common and compromised passwords. With modern computing power and the infrequency of password changes, implementing 'blocklists' of common or known compromised passwords would be fairly trivial computationally.

For example"
"When processing a request to establish or change a password, verifiers SHALL compare the prospective secret against a blocklist that contains known commonly used, expected, or compromised passwords."

And potentially
"Verifiers and CSP's SHOULD compare password hashes against known compromised passwords at least annually and disable user accounts when compromised passwords are detected as in-use".

Without these requirements, and the reducing in the composition rules, I fear that we may end up with end users choosing particularly weak but long passwords such as 12345678abcdefgh

With Regards

John Griffin