From: [redacted]
To: dig-comments@nist.gov
Subject: [dig-comments] Comment on NIST SP 800-63B-4 (Second Public Draft)
Date: Thursday, October 3, 2024 10:36:39 AM
Attachments: image001.png

Intern

Dear writers,

I want to start by complimenting the Revision 4 update. The new version is less abstract and uses less technical jargon, showing more empathy toward implementers and real-life users. I'm happy to review the new documents after publication and apply the principles to our own policies and internal standards.. I've already noticed refreshed topics that will help smooth out existing issues in my environment. Wish I could have been working earlier on the drafts

My apologies for not using the comment template as my comment is a bit broader than what the template is catering for.

Now, for my comment:

3.2.5 Phishing (Verifier Impersonation) Resistance

In the scenario starting at line 1345, the phishing flow could also be reversed. For example, an attacker could initiate a session pretending to be the legitimate subscriber. The verifier would then contact the authenticator, and the subscriber would be asked to authenticate. This is sometimes referred to as MFA spam or fatigue, where the attacker overwhelms the user with MFA requests until they approve one.

Attack Classification: According to the definition in 800-63B-4.2, this attack doesn't seem to qualify as phishing since no secret is transferred. Also, the user isn't tricked into visiting a fake website.

Suggestions for Alternative Definition and Classification:

- This could fall under "Authentication Intent". The current definition however only includes "physical intent" from the legitimate user (to prevent authentication via malware, trojans, remote control, etc.). It could be expanded to include "functional intent": preventing the legitimate user from being misled into performing authentication actions for illegitimate purposes.
- It could also be labeled "Entrapment" (new), where the user is manipulated into taking actions that favor the attacker. This could be defined as an attack in which the subscriber is tricked into approving actions that have unintended or unknown

consequences.

Clarification Needed: As MFA becomes more popular, MFA attacks are also increasing and evolving. In the real-world scenario described, it's unclear if AAL3 requires protection against the former mentioned type of attack.

Technical Measures: What technical measures in authentication can prevent this particular attack, and perhaps evolving, more sophisticated versions of it? Session binding came to mind, but from 5.1 Session Bindings, it's not clear, as session binding seems to only occur after initial authentication.

At AAL3, I would expect the authenticator to be bound to the subscriber's session, possibly through an in-band, device-embedded cryptographic authenticator (like Windows Hello, passkeys, or FIDO2). However, syncable authenticators could complicate this, and it might affect usability (if the authenticator has to be inseparable from the device where the session is initiated).

Being a popular and successful authentication attack type addressing or at least clarifying this in a clear manner in 800-63B would be extremely helpful for my work and in discussions with solution architects and engineers. This issue is likely not unique to me, so it could benefit others in similar positions.

Note: Some vendors address this issue with solutions like number matching. While it's not completely phishing-resistant, the popularity of this method might merit a mention in the document.

Kind regards,

Ben Meijer
[redacted]

Informatie vennootschap

Intern