From: [redacted]
[redacted] dig-comments@nist.gov
Subject: [dig-comments] the problem with sms is that it is often the only option, is required, and can be used to "recover" an account
Date: Friday, November 1, 2024 1:22:01 PM

i have been reading through the comments on r3 of 800-63 concerning the deprecation of sms for 2fa, which i was made aware of after hearing about and reading some of r4 (ibid.). i know i am past the comment deadline, and i know i am just some joe internet. i wanted to give the point of view of the user. a lot of the comments on this were from industry worried about how hard it would be to change and how hard it is to get people to use 2fa at all, much less ones that require more setup than using the phone number, which is often already required for the account creation.

the maintenance of sms as delivery for otp, even if restricted, is problematic because it allows for companies holding things valuable to me, be it pii or money, to be compliant without actually being secure. i agree that sms otp is better than no 2fa, but it is not enough when literally all my retirement savings are on the line. it is not enough when the company holds basically all my pii. right now, many companies i do business with ONLY provide sms based otp authentication. even though i want to, i am unable to implement more secure methods of mfa on those accounts. MY FUCKING THROW-AWAY EMAIL ACCOUNT HAS BETTER SECURITY ON IT! this is because they can and will do only the barest of minimums, so they can swagger about touting their security practices. and because doing it better is "hard" (read: expensive).

having sms otp authentication arguably increases attack surface as now an attacker can take over an account using recovery methods that are near universally tied to the sms otp authentication. i recognize that the blame for this rests on the companies, and myself for doing business with them. but it also rests on the guidelines that tell them that a password plus a text is enough.

according to the guidelines as sms otp is restricted and those accounts should have other options for mfa, but they do not, so i take it these entities are out of compliance. and they do not seem to care as it has now been years since the release of r3. i want to be able to remove sms authentication from all my accounts, as i have and use whereever possible stronger measures to secure my accounts. but the messaging of the guidelines is "meh, sms good enough". which goes out through the companies providing the accounts to the consumers, and they develop the belief that they are doing good because they use sms 2fa. thus they become resistant to other methods of mfa and the companies in turn do as well.

i know that you are more knowlegeable about all this than i, and are weighing valid concerns from all sides. i am just writing to put my two-cents on the scale for further reducing or eliminating sms otp authentication methods perceivability as viable for securing accounts.

https://youtu.be/wVyu7NB7W6Y?si=VYdihpUmRgZpDmR7

just some guy on the internet

--
To unsubscribe from this group, send email to dig-comments+unsubscribe@list.nist.gov

View this message at https://list.nist.gov/dig-comments
To unsubscribe from this group and stop receiving emails from it, send an email to DIG-Comments+unsubscribe@list.nist.gov.