-　Help unravel the conundrum over NIST’s Guideline　-

I submitted the following suggestion on NIST's Draft Digital Authentication Guideline on August 2.

……………………

5.2.3 reads "(The biometric system SHALL allow no more than 10 consecutive failed authentication attempts.) Once that limit has been reached, the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret."

It is desirable to see the above sentence in 5.2.3 followed by such a footnote as "It should be noted that the security in such cases is necessarily lower than when the second authenticator alone is used".

NIST abruptly closed the thread of my suggestion registered as #193 for the reasons which are just unintelligible to me after the exchange of a couple of odd messages as outlined below.

First, a NIST person indicated in their reply that NIST allows or even forces the OR/Disjunction operation adding "it is still two-factor".　I submitted a suggestion on the assumption that NIST allows OR/Disjunction operation.

The person’s second reply said "If two-factors are required, 2-factors need to be authenticated or the claimant will not get access."　It led me to assume that NIST does not allow OR/Disjunction and forces AND/Conjunction.　I submitted a new suggestion accordingly.

Then, the second NIST person abruptly stepped in and closed this thread after supposedly alleging that the OR/Disjunction operation is valid for security.　My appeal for continuing the discussion was met with silence and the thread was finally locked.

I am unable to follow their logic for justifying the closure of this thread. I wonder if some of you can help unravel this conundrum for me.

Hitoshi Kokumai

< Epilogue >

Following the abrupt closure of the above thread, I tried to submit a fresh suggestion reading

"It is desirable to see the above sentence in 5.2.3 followed by such a footnote as "This way of operating biometrics with a second authenticator by OR/Disjunction shall be recommend where convenience matters, not where security matter since the security in such cases is necessarily lower than when the second authenticator alone is used. It is convenience that is improved by this way of operating biometrics and a fallback means, and this improvement is obtained by the sacrifice of security".

NIST closed this new thread (#286) the following day without any comment whatsoever.

Attachments

1. The whole history of the #193 thread (P3)
2. The whole text of the new suggestion #286 (P9)
3. Description for publication on Slide Share (P11)

< The whole history of the #193 thread >

hitoshikokumai commented 20 days ago
Organization:3

Type: Security design

Document (63-3, 63A, 63B, or 63C):63B

Reference (Include section and paragraph number):5.2.3

Comment (Include rationale for comment): It reads "(The biometric system SHALL allow no more than 10 consecutive failed authentication attempts.) Once that limit has been reached, the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret."

This implies that the second authenticator(factor) and the biometrics are used by OR/Disjunction, which necessarily makes the security lower than that of the second factor alone. In other words, the security is better when the second factor alone is used.

There is a 2-minute video outlining the rationale.

Biometrics in Cyber Space - "below-one" factor authentication
https://youtu.be/wuhB5vxKYlg

This article may also help.

Misuse of Biometrics Technology
http://www.paymentsjournal.com/Content/Blogs/Industry_Blog/30986/

Biometrics authentications are good for physical security but ruin the security of password protection and generate a false sense of security in cyber space. Deployed with a fallback password against false rejection, they provide the level of security that is even poorer than a password-only authentication.

Suggested Change: It is desirable to see the above sentence in 5.2.3 followed by such a footnote as "It should be noted that the security in such cases is necessarily lower than when the second authenticator alone is used".

Organization: 1 = Federal, 2 = Industry, 3 = Other

hitoshikokumai referenced this issue 9 days ago
 Open Suggestion for AAL 2 #221

“A NIST person” commented 6 days ago

Thank you for your review. The intention behind the draft of 800-63-3-B's inclusion of biometrics is that they are always used with a second factor. If the biometric check fails, a different second factor has to be used. In other words, if users/attackers are locked out of the biometric check, they could be offered an alternative second factor. It's still two factor. If the wording needs to be fixed to reflect this, please suggest an alternative because the interpretation that a failure of the biometric check means no second factor check is not what we were allowing in the text.

hitoshikokumai commented 5 days ago

Thanks for taking up my suggestion for consideration.

There should be nothing wrong in operating biometrics with a second factor by OR/Disjunction PROVIDED the people concerned are all accurately aware of its consequences and all the users explicitly informed. Most important is to avoid the false sense of security trapping the users in it.

If allowed, I would like to suggest such an alternative as follows:

The biometric system SHALL allow no more than 10 consecutive failed authentication attempts. Once that limit has been reached, the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret.

It should be noted, however, that the security in such cases is necessarily lower than when the second authenticator(factor) alone is used like a house with two entrances placed in parallel (not in tandem) is more vulnerable to burglars than a house with one entrance.

Remark: Two different factors can be operated in two ways - (1) by AND/Conjunction (we need to go through both of the two) or (2) by OR/Disjunction (we need only to go through either of the two). Operation of two factors by (1) AND/Conjunction provides higher security and lower convenience while that by (2) OR/Disjunction provides higher convenience and lower security.

People who wish to use biometrics for achieving the level of security higher than passwords are advised to operate the biometrics and passwords by (1) AND/Conjunction and inform the users that they will be able to enjoy better security although they will have to give up the access altogether if rejected by biometrics even when they are able to feed the correct passwords.

People who wish to use biometrics for better convenience are advised to operate the biometrics and passwords (fallback means against false rejection) by (2) OR/Disjunction and inform the users that they will be able to enjoy better convenience although the level of security that they can expect is necessarily lower than that of password-only authentication.

Should you want to see a more comprehensive and explanatory alternative, I would be ready to compress my article published on the likes of Payments Journal.

Please let me have your feedback.

Hitoshi Kokumai

PS I would appreciate it if you could also have a quick look at my recent short writing posted at

http://www.slideshare.net/HitoshiKokumai/discussed-on-elseviers-btt-62502162?qid=8cc17e97-6fa9-4ac6-a470-bac14aada916&v=&b=&from_search=1

http://www.slideshare.net/HitoshiKokumai/appeal-to-media-writers-over-security-misconception?qid=8cc17e97-6fa9-4ac6-a470-bac14aada916&v=&b=&from_search=3

“The same NIST person” commented 3 days ago

We are not allowing biometrics to be used as a single factor for multiple reasons, summarized in 800-63-3. I believe your suggested text is allowing that by adding an option for "OR." Since we do not want to allow that, there is no need for the sentence to say "OR/Disjuntion" is lower security. If two-factors are required, 2-factors need to be authenticated or the claimant will not get access.

hitoshikokumai commented 3 days ago・edited

This latest comment of yours seems to make sense. But it does not appears to be compatible with your original draft which sounds to allow or even force the operation of two factors by OR/Disjunction.

The original statement "the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret." appears to be forcing or allowing the claimant to use a second authenticator/factor as a fallback means against false rejection. This is no different to using the biometrics and the second authenticator/factor (as fallback means) by OR/Disjunction.

If your intention was to allow the operation of biometrics and the second factor only by AND/Conjunction, your draft could simply be altered to

"Once that limit has been reached, the claimant SHALL not get an access. Rescue means SHALL be considered separately from this particular process of access trials".

It would also be desirable to refer to the merits and demerits of the operation of two factors by OR/Disjunction in view of the observation that we are actually watching many such cases on the market.

hitoshikokumai commented 3 days ago

Whether explicitly called as the fallback means or not, a fallback means for rescue of the claimant who gets rejected by the first factor is nothing but a second factor operated by

OR/Disjunction.

I hope you are with me.

“The second NIST person” commented 2 days ago

While having two means of activating a multi-factor authenticator is theoretically weaker than having only one means of activation, the threat profiles of biometric vs. memorized secret activation are considerably different. For example, a user in a public place would probably be well advised to use a biometric to activate their mobile device rather than type a PIN to unlock it where it can be readily observed by others. Having a choice of activation methods is therefore not necessarily weaker than having a memorized secret only.

Note also that the association of multiple authenticators with a subscriber account is encouraged. This could also be seen as being weaker than having only a single authenticator, but it mitigates the real-world problems of authenticator loss, breakage, and theft. Currently, account recovery practices are often a weak point in authentication systems and are rarely multi-factor. The benefit of making account recovery less frequent (and more stringent) outweighs the risks associated with having a reasonable number of authenticators associated with the account.

In both cases, there is sufficient margin built into entropy, biometric performance, and throttling requirements to provide sufficient security given the existence of multiple authenticators and activation modes.

“This NIST person” closed this 2 days ago

hitoshikokumai commented 2 days ago

I would appreciate it if you could reconsider about the closure of this thread for the following reasons.

It would be fruitless to spend time for comparing the strength of biometrics used on its own with that of passwords used on its own. There are no objective data on the vulnerability of biometric products (not just false acceptance rate when false rejection is sufficiently low but also the risk of forgery of body features and the risk of use when the user is unconscious) and that of the passwords (not only that the entropy may be as low as 10 bits or as high as 100 bits but also that it can be stolen and leaked.)

Even assuming that biometrics were though to be 10 times less vulnerable than memorized secrets despite the abovementioned observation, the operation of those two factors by OR/Disjunction would necessarily result in the overall security being lower than that of the memorized secrets as well as that of the biometrics. Given that the biometrics has the (x) vulnerability, a very weak fallback password has $(y1)$ vulnerability and a very strong fallback password having $(y2)$, the math of vulnerability $(x + y - xy) > y$ leads us to $(x + y1 - xy1) > (y1)$ and $(x + y2 - xy2) > (y2)$. This means that we are safer when we use only the very weak password than when we use the biometrics with the very weak fallback password, and that we are also safer when we use only the very strong password than when we use the biometrics with the very strong fallback password.

We could consider the comparison between $(x + y2 - xy2)$ and $(y1)$ but it could lead us nowhere. Whoever can manage a very strong password together with biometrics must be able to manage the very strong password on its own. Then, again, we are safer when we use only the very strong password. Moreover, rarely used/recalled passwords tend to be very weak, i.e., what we actually get could well be $(x + y1 - xy1) >>> (y2)$.

As such it is not possible to count a case that the biometrics used together with a fallback password is stronger than a password used on its own.

“The third NIST person” locked the thread.

(The above was copied from the NIST site 6 days ago and persons’ names anonymized.)

< The whole text of the new suggestion #286 >

Title:　Security effects of operation of two-factors by OR/Disjunction

Reference (Include section and paragraph number):　5.2.3

Comment (Include rationale for comment):　It reads “The biometric system SHALL allow no more than 10 consecutive failed authentication attempts. Once that limit has been reached, the claimant SHALL be required to use a different authenticator or to activate their authenticator with a different factor such as a memorized secret” at another place.

There should be nothing wrong in operating biometrics with a second authenticator/factor by OR/Disjunction (we need only to go through either of the two) as against AND/Conjunction (we need to go through both of the two) PROVIDED the people concerned are all accurately aware of its consequences and all the users explicitly informed of them.

It should be noted that the security in such cases is necessarily lower than when the second authenticator(factor) alone is used like a house with two entrances placed in parallel (not in tandem) is more vulnerable to burglars than a house with one entrance. This is logically proven as follows:

It would be fruitless to spend time for comparing the strength of biometrics used on its own with that of passwords used on its own. There are no objective data on the vulnerability of biometric products (not just false acceptance rate when false rejection is sufficiently low but also the risk of forgery of body features and the risk of use when the user is unconscious) and that of the passwords (not only that the entropy may be as low as 10 bits or as high as 100 bits but also that it can be stolen and leaked.)

Even assuming that biometrics were thought to be 10 times less vulnerable than memorized secrets despite the abovementioned observation, the operation of those two factors by OR/Disjunction would necessarily result in the overall security being lower than that of the memorized secrets as well as that of the biometrics.　Given that the biometrics has the (x) vulnerability, a very weak fallback password has (y1) vulnerability and a very strong fallback password having (y2), the math of vulnerability

$(x + y - xy) > y$ leads us to $(x + y1 - xy1) > (y1)$ and $(x + y2 - xy2) > (y2)$. This means that we are safer when we use only the very weak password than when we use the biometrics with the very weak fallback password, and that we are also safer when we use only the very strong password than when we use the biometrics with the very strong fallback password.

We could consider the comparison between $(x + y2 - xy2)$ and $(y1)$ but it could lead us nowhere. Whoever can manage a very strong password together with biometrics must be able to manage the very strong password on its own. Then, again, we are safer when we use only the very strong password. Moreover, rarely used/recalled passwords tend to be very weak, i.e., what we actually get could well be $(x + y1 - xy1) >>> (y2)$.

As such it is not possible to count a case that the biometrics used together with a fallback password is stronger than a password used on its own.

Should NIST disagree to the logic of this suggestion, NIST would be expected to logically demonstrate that a house with two entrances placed in parallel (not in tandem) is not less vulnerable against burglars than a house with one entrance.

Most important is to avoid the false sense of security trapping the users in it.

Suggested Change: It is desirable to see the above sentence in 5.2.3 followed by such a footnote as "This way of operating biometrics with a second authenticator by OR/Disjunction shall be recommend where convenience matters, not where security matter since the security in such cases is necessarily lower than when the second authenticator alone is used. It is convenience that is improved by this way of operating biometrics and a fallback means, and this improvement is obtained by the sacrifice of security".

This new thread (#286) was unilaterally closed without any comment whatsoever.

< Description for publication on Slide Share >

It appears that NIST is of the view that a house with two entrances placed in parallel, not in tandem, is less vulnerable to burglars than a one-entrance house. We are unable to understand their logic behind such observations. We wonder if some of you can help unravel this conundrum.