Mitigating attacks based on knowing the length of a Windows Hello PIN

devblogs.microsoft.com/oldnewthing/20240227-00

February 27, 2024

Raymond Chen

When you set up a numeric PIN with Windows Hello, the system will immediately sign you in with that PIN once you enter the correct number of digits, saving you the trouble of having to press `Enter`. For example, if you set up an 8-digit PIN, then once you enter the eighth digit, the PIN validation process begins.

An attacker can use this behavior to discover the length of the PIN: Try to sign in once with some initial guess like “all ones” and see how many ones can be entered before the system starts validating the PIN.

Is this a problem?

Well, the length of the PIN isn’t really a tightly-guarded secret, because anybody who watches the screen while you sign in can count the dots that appear, or (if they have sharp ears) listen to the number of clacks of the keyboard.

The security team have done their own cost-benefit analysis of this behavior and and have tuned the system so that the convenience does not come at a significant loss of security: Through a combination of increasing the minimum PIN length, rejecting PINs that follow certain patterns, and decreasing the TPM’s anti-hammering threshold, the value of knowing the number of digits in the PIN is significantly reduced. Even with the shortest allowable PIN length, you won’t be able to make many guesses before the TPM temporarily locks out any further attempts to validate the PIN. Furthermore, the PIN length is not revealed to remote logons; anybody trying to steal this data must have physical access.

If you feel strongly about it, you can set your organization’s PIN policy to force alphanumeric PINs. For alphanumeric PINs, Windows requires that the user press `Enter`; it does not provide the convenience of accepting a PIN once the character count is reached.

Armed with this information, you may be able to address this security issue that was submitted:

> Windows allows me to sign in with the wrong PIN.
>
> To reproduce, set the user's PIN to 122222. At the sign-screen, enter a 1, followed by any number of 2's. All of them are accepted and sign the user in, even though the seven-digit and longer PINs are incorrect.

Bonus chatter: In the days before cell phones, companies would take advantage of a similar behavior of telephone switching hardware: Once the number you dialed formed a complete telephone number, the telephone system began connecting the call. Any numbers you dialed after that point were ignored. A company could advertise its telephone number with an eight-digit mnemonic ("Call 555-FABRIKAM to order!"), even though the last digit was ignored.