Expanding Microsoft Hello with behaviour monitoring

The objection of this text is to discuss the extension of established authentication methods of Microsoft Hello with *behaviour monitoring* or *active authentification*.

Microsoft Hello[1] is an authentication module integrated in Windows 10 and available for personal computer as well as for smartphones. It has the ability to use various biometrical characteristics of the user to allow convenient but secure unlocking of the device. Current versions support the reading of fingerprints, face recognition and for devices with high quality cameras also iris scanning.

The service is promoted as a flexible framework which is also extendable with further authentication methods, recently Microsoft partnered with Fujitsu to offer an additional module to scan the users veins.

These ambitions to remove the needs of passwords are reasonable. In the last years a high number of massive password leaks occurred after hacks of databases. These passwords are exposed to public and afterwards considered insecure. Web services were found[2] to test quality and previous leakage of any given password. Parallel to this process various new recommendations by the N.I.S.T[3] where published, on how to design secret passwords.

It is unnatural for humans to remember complex and long combinations of words. And therefore a simplification required. While this is broadly established and managed with password managers, it does not prevent the security risk on secret exposition. Once leaked a instant change of user passwords is required, resulting in additional secrets to remember and management overhead.

Instead of memorizing secrets it is possible to use biometrical features as a secret. If unique, they can be a replacement for long passwords due to their complexity. However, the past has shown that authentication based on biometrical features is dangerous due to its simplicity of stealing. These features can, just like a password, be filmed or copied and after reproduced to successfully login. Well known attacks are the circumvention of Apples Touch[4] & Face[5] ID as well as Microsofts Hello face recognition method[6].

This points out the problem of one time authentications, where the input of a secret (password of biometrical characteristic) unlocks a device, without further checks. A completely different approach on using biometrical characteristics is to use the users behaviour, as an unconscious secret.

The main idea of using behaviour as authentication is to monitor the users input and constantly evaluate the variation of known behaviour. As Microsoft Hello is deeply integrated into the Windows operating system, bot mobile and on personal computer, it is possible to gather all these meta information.

Possible implementation

To initialize such a system a user trains the used device, comparable to setting up a fingerprint on smartphones. In this case the training consists of normal device usage, with the limitation that during training time only the intended user access the system.

The monitored data may varies between smartphones and complete desktop environments, illustratively including the following metrics which are constantly monitored:

- Opening of applications or programs
- Keyboard type speed, time between two key strokes

[1] https://www.microsoft.com/en-us/windows/windows-hello
[2] https://haveibeenpwned.com/Passwords
[3] https://pages.nist.gov/800-63-3/
[4] https://www.youtube.com/watch?v=HM8b8d8kSNQ
[5] https://www.youtube.com/watch?v=i4YQRLQVixM
[6] https://www.youtube.com/watch?v=Qq8WqLxSkGs

- Mouse movements, speed and angles
- Viewed websites and time spend there
- Contacted persons
- Usage of keywords

As the devices are likely routinely used, reparative patters are found within recorded metrics. An example is given for a theoretical user of a smartphone:

1. Activate screen
2. Open E-Mail program
3. Open Browser
4. Type in URL of social network
5. Write messages
6. Check calendar app
7. Deactivate screen

This short device usage already delivers a huge amount of possible monitoring data. Algorithms divide the input in smaller steps to allow other sequences of tasks. During all usage a percentage is calculated how likely it is, the correct owner uses the devices. In unusual events, like opening a number of never visited websites, searching messages of unusual contacts or changing device settings, the trust score may lower under a specified threshold and device access is lowered or even denied. Once denied Microsoft Hello would require authentication via other characteristics then behaviour, like a special PIN or combination of fingerprint and face detection.

The extension could be implemented in a way that an initial login via a classical biometric characteristic gives the user a defined level of trust, as an illustrative value 40%. Routinely usage increases the value quickly and the user can conveniently use the device. Uncommon behaviour will lower the score until another verification with other secrets is required.

Combining existing solutions with this approach can generally improve device security especially for mobile devices. An attacker may film a victim which performs a notebook login via password. On leaving the device unattended, like in a library, the attacker may access the device with full privileges. The herewith explained approach may let the attacker access the device but quickly block certain areas due to unusual behaviour.

Adoption & research

Generally the monitoring of behaviour to secure services is not a new approach as it is already actively used at tools from Google and Microsoft. Logging in from anomalous location request the user to provide additional information. However this did not yet enter user devices like laptops and smartphones.

Lastly, behaviour monitoring as an active and continuous way of authentication is actively research in various places. The U.S. military research department DARPA works in this field and tries to find a generic way to remove password usage[1]. For mobile devices an extensive study was performed [2] which shows the feasibility of the approach in general for mobile devices. Additionally

References

[1] R. P. Guidorizzi, “Security: Active authentication,” *IT Professional*, vol. 15, no. 4, pp. 4–7, 2013.

[2] F. Li, N. Clarke, M. Papadaki, and P. Dowland, “Active authentication for mobile devices utilising behaviour profiling,” *International journal of information security*, vol. 13, no. 3, pp. 229–244, 2014.