Windows Hello: Researchers bypass face authentication

December 23 2017, by Nancy Owano

In the course of a research project, security experts Matthias Deeg and Philipp Buchegger of penetration-testing company SySS found out something that put Windows Hello in spoofing-attack news this week: They were able to trick Windows Hello face authentication by Microsoft

on different versions of the Microsoft Windows 10 operating system.

What is Windows Hello? Mark Kaufman in *Mashable*: This is Microsoft's password-free security software.

"Windows Hello is a more personal way to sign in to your Windows 10 devices with just a look or a touch. You'll get enterprise-grade security without having to type in a password," according to Microsoft.

How did they trick it? By specially prepared photos. As a result, the security researchers are urging Windows 10 users to update their systems to prevent such attacks. SecLists.Org, the security resource site, has the details, titled "Microsoft Windows Hello Face Authentication - Authentication Bypass by Spoofing (CWE-290)."

Microsoft Windows 10's biometric mechanism involves near infrared face recognition technology with specific Windows Hello compatible cameras. But the researchers' videos showed that a modified printed photo of the authorized person was able to carry out the bypass.

Namely, the attack involved taking a headshot of the authenticated user with the near-infrared (IR) camera.

"Windows Hello uses near-IR imaging to unlock Windows devices," said Liam Tung, *ZDNet*. Microsoft chose near-IR imaging for authentication because it worked in poor lighting and offered some protection against spoofing attacks, since IR images aren't typically displayed in photos or on a screen."

Kaufman explained what can go awry: Hello Windows uses an infrared camera (either built-in the or added separately) to recognize the unique shape and contours of a face before granting or denying access to a Windows account. But a flaw was found in an insecure implementation

of biometric face recognition.

Who is especially vulnerable? They say anyone with a Windows 10 system that did not yet receive the Fall Creators Update (but see text below).

Tung said the attack works against different hardware. He discussed how they tested:

"SySS printed out a modified version of the near-IR captured headshot in various resolutions and colors. Holding the printout up to a locked device's camera successfully unlocked it. Another method involved placing opaque sticky tape over the RGB camera lens and then holding the same printout up."

Tung in *ZDNet* recapped the solutions available. Fall Creators Update was not the whole story. Tung noted that "just applying the Fall Creators Update is not enough to block the spoofing attack, according to SYSS." Tung said users would need to set up Windows Hello face authentication from scratch after the update, as well as enabling anti-spoofing.

Tung described recommendations in more detail. As indicated in their test results, the newer Windows 10 branches 1703 and 1709 are not vulnerable to the described spoofing attack by using a paper printout if the enhanced anti-spoofing feature is used with respective compatible hardware.

SySS recommended updating the Windows 10 operating system to the latest revision of branch 1709, enabling the "enhanced anti-spoofing" feature, and reconfiguring Windows Hello face authentication afterwards.

They said on their Dec 18 blog: "Thus, concerning the use of Windows

Hello face authentication, SySS recommend updating the Windows 10 operating system to the latest revision of branch 1709, enabling the "enhanced anti-spoofing" feature, and reconfiguring Windows Hello face authentication afterwards."

Kaufman remarked that "it might help to view Windows Hello as a convenience feature, not a security feature."

This news came as no surprise to Lucian Armasu in *Tom's Hardware*. Armasu said, "as we've come to learn by now, virtually all face authentication systems are eventually spoofed by researchers or malicious hackers, either with a simple photo or one that has a few modifications to fool the more advanced systems."

More information: www.syss.de/pentest-blog/article/2017/12/18/460/ seclists.org/fulldisclosure/2017/Dec/77