USENIX Security '25 Artifact Appendix: Red Bleed: A Pragmatic Near-Infrared Presentation Attack on Facial Biometric Authentication Systems

Bowen Hu
School of Electrical and Electronic Engineering
Nanyang Technological University

Kuo Wang
School of Electrical and Electronic Engineering
Nanyang Technological University

Chip Hong Chang
School of Electrical and Electronic Engineering
Nanyang Technological University

A Artifact Appendix

A.1 Abstract

Our work demonstrates a practical attack against Windows Hello face recognition under its default configuration. The underlying vulnerability, designated CVE-2025-26644, was patched on April 9, 2025. All systems running Windows 10 or Windows 11 versions prior to 24H2 are susceptible to this exploit.

We provide comprehensive documentation of the hardware design and the attack procedure using our assembled module. Additionally, our research introduces a cross-spectral face generation model, with full source code and pretrained checkpoints publicly released. To support reproducibility, we have also prepared a Google Colab demo to facilitate hands-on experimentation.

A.2 Description & Requirements

Our work requires specialized hardware—a self-assembled near-infrared (NIR) LCD. The bill of materials (BOM) is provided in the main text, while the printed circuit board (PCB) files, 3D-printed enclosure design, and detailed assembly instructions are available on Zenodo. In addition to the NIR LCD, the attack setup requires: 1) A target machine running Windows 10 or Windows 11 with the Windows Hello facial recognition module in its default configuration. 2) An HDMI media source (e.g., another computer) to supply video content to the NIR LCD. Due to the time and cost associated with hardware setup, we have also prepared a web-based demo for evaluation.

The cross-spectral face generation model can be executed on any machine or platform capable of running PyTorch-based deep learning models. To train the model, a publicly available dataset is required, along with at least one pair of near-infrared (NIR) and visible (VIS) images from the target subject. For ease of use, we provide a Google Colab notebook to facilitate the testing process.

A.2.1 Security, privacy, and ethical concerns

Our work does not involve any destructive modifications to the target system. The only ethical consideration is that the test subject must consent to providing their facial biometric data to unlock the registered Windows device.

A.2.2 How to access

We prepared a hardware demo of unlocking the target machine using the Windows Hello module at `http://16.176.135.204/`. Also, we prepare a Google Colab cross-spectral face generation demo in `https://colab.research.google.com/drive/14pasM4oz7O_vQSFr_6-wM_9WUELhKjeo?usp=sharing`.

The above-mentioned link is provided solely for evaluation convenience. Readers can independently assemble the NIR display and reproduce the experiments locally using the materials and instructions we have released.

A.2.3 Hardware dependencies

We do not have hardware requirement in the weblink demo. If the readers want to reproduce the experiment locally, the hardware requires the following items:

- **NIR LCD**: The self-assembled NIR LCD functions as a standard HDMI display, with all technical details—including design files and assembly instructions—available in our paper and Zenodo submission.
- **Target Windows machine**: The target device must be a Windows machine running Windows 10 or Windows 11, with any version earlier than 24H2 without the patch released on Apr 9, 2025.

- **Windows Hello module**: This work requires a Windows Hello module, which can be either integrated into the Windows laptop or desktop, or connected externally via USB.
- **OmniVision OV9281 monochrome camera module**: This module is used for NIR face image sample collection.
- **Raspberry Pi 4 Model B with camera module 3 12MP**: This module is used for VIS face image sample collection.
- **A GPU machine**: A separate machine is required to run the cross-spectral face generation experiments. In our setup, we used a server equipped with an Intel Xeon w7-3465X CPU (56 cores), 512 GB RAM, and an NVIDIA RTX 4090 GPU with 24 GB of memory. However, such high CPU and memory resources are not essential—the primary requirement is a GPU with at least 24 GB of memory for model training. CPU and system memory usage remain minimal during the process.

A.2.4 Software dependencies

There is no software requirement in this demo. If the readers want to train with their own face biometric data, the software requires the following items:

- **DeepFaceLab**: We download the Windows release from https://github.com/iperov/DeepFaceLab?utm_source=chatgpt.com. This model is used for the face region of interest (ROI) crop and face swapping after the cross-spectral generation.
- **CASIA NIR-VIS 2.0 Face Database**: this publicly available dataset is required for training. It can be downloaded from http://www.cbsr.ia.ac.cn/english/NIR-VIS-2.0-Database.html.

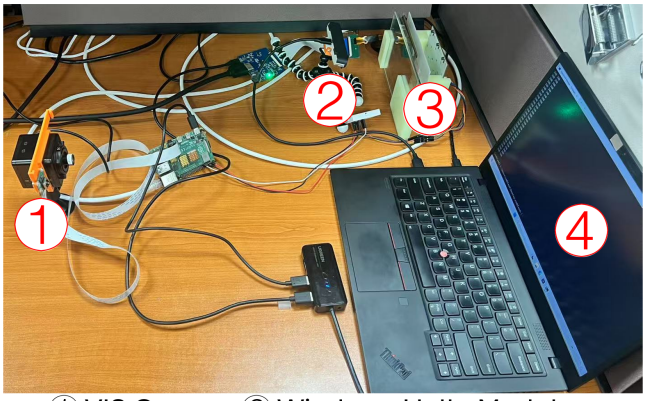
A.2.5 Benchmarks

None.

A.3 Set-up

If not assembling the hardware, the remote demo can be accessed from http://16.176.135.204/. Our web demo is shown in Figure 1. The Raspberry Pi module is used for the Windows machine control and sending back the captured frames. We display the registered subject NIR video on the 850nm LCD in front of the Windows Hello module. The target machine installed Windows 11 23H2 with version released before Apr 9, 2025.

No setup requirement for the Colab. The demo can run directly. https://colab.research.google.com/drive/14pasM4oz7O_vQSFr_6-wM_9WUELhKjeo?usp=sharing.



① VIS Camera ② Windows Hello Module
③ NIR LCD ④ Target Windows Machine

Figure 1: Web demo setting.

A.3.1 Installation

None.

A.3.2 Basic Test

Hardware Web Demo: Press the "Turn On Light" Button to turn on the 850 nm backlight. Press "Send Space" button to start the face unlock. It is able to enter the system bypassing Windows Hello.
Cross-spectral Face Generation: Run the whole Colab Notebook. It is able to generate NIR image samples from the provided VIS image sample.

A.4 Evaluation workflow

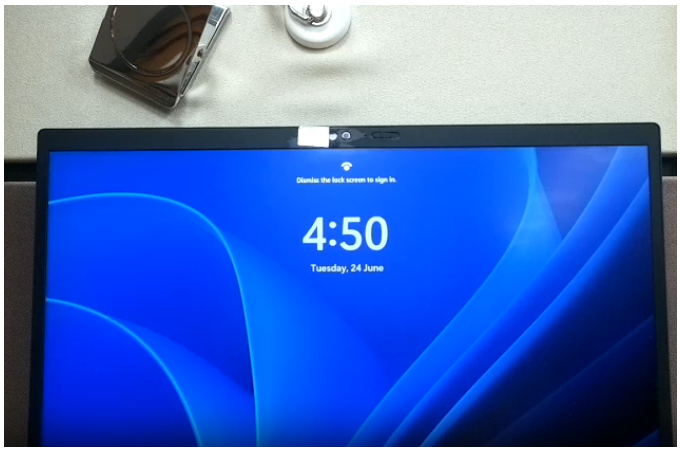
A.4.1 Major Claims

(C1): Using the NIR display is able to bypass the Windows Hello face recognition.
(C2): Using the Variational Autoencoder (VAE) is able to generate NIR image samples from the VIS image samples.

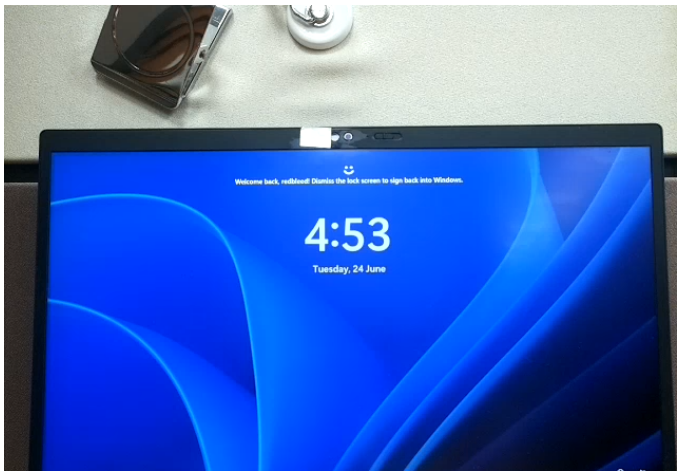
A.4.2 Experiments

(E1): *[Hardware Web Demo] [10 human-minutes]:* There may be few seconds delay in the live video stream due to the network.
How to:

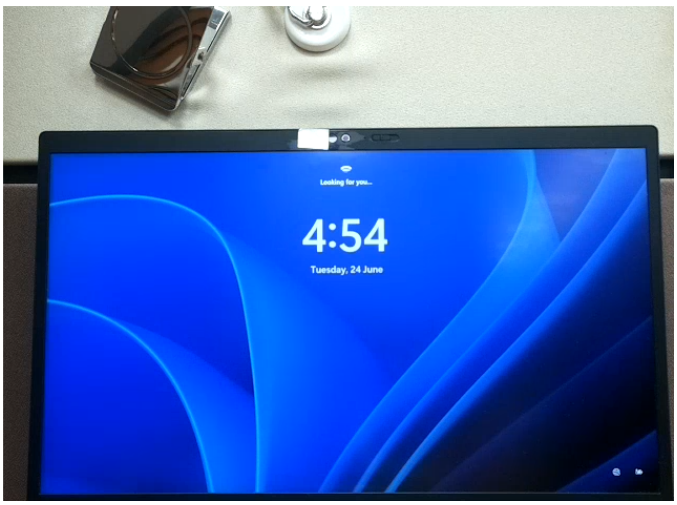
1. The web page is opened, and the video stream shows the target Windows 11 device. It should be in the stand by mode as shown in Figure 2a.
2. Click **"Turn On Light"** to turn on the 850 nm light on the NIR LCD for one minute. Press **"Send Space"** to activate the face unlock routine. The screen will show the machine is ready to unlock as



(a) The target machine in the "standby" mode.



(b) The target machine in the "unlock ready" mode.



(c) The target machine in the "looking for face" mode.

shown in Figure 2b. If we click the **"Send Space"** again, it will enter the system.

3. Click **"Send Lock (Win+L)"** to lock the screen. Click the **"Turn Off Light"** button, now the Windows Hello module cannot find the face, it will keep looking for the face as shown in Figure 2c. If we turn on the light again, it will be back in the unlock ready state again.
4. If it fails to unlock and enters the input pin mode, click the **"Send PIN"** to unlock the system, and Lock again by clicking **"Send Lock"**.

Results: It successfully bypasses Windows Hello facial recognition and gains access to the system by displaying a crafted NIR video on the NIR screen.

(E2): *[Cross-spectral Face Generation.] [20 human-minutes]:*

How to: Executing the entire notebook will automatically initiate the download of sample data and pretrained models, and subsequently perform the complete experimental procedure without further user intervention.

Results: Generating NIR image samples from the provided VIS images.

A.5 Version

Based on the LaTeX template for Artifact Evaluation V20231005. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2025/.