Biometricks: Bypassing an Enterprise-Grade Biometric Face Authentication System

October 13, 2018

Who am I?

Dipl.-Inf. Matthias Deeg
Expert IT Security Consultant
CISSP, CISA, OSCP, OSCE

- Interested in information technology – especially IT security – since his early days
- Studied computer science at the University of Ulm, Germany
- IT Security Consultant since 2007
- Head of Research & Development

Agenda

1. Short Introduction to Used Technology
2. Previous Work of Other Researchers
3. Overview of Our Research
4. Attack Surface and Attack Scenario
5. Found Security Vulnerability
6. Demo
7. Conclusion & Recommendations
8. Q&A

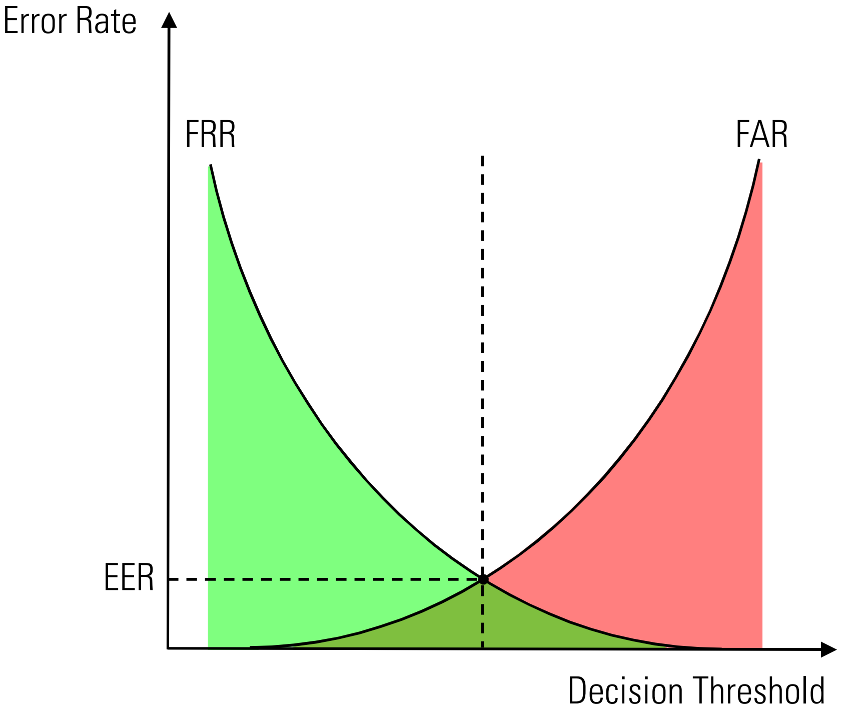
Short Introduction to Used Technology

- Biometric Face Recognition
  - Biometric sensor: camera
  - Feature extraction (landmarks/alignment points)
  - Mathematical representation of face (model)
  - Performance metrics, False Accept Rate (FAR), False Reject Rate (FRR), Equal Error Rate (ERR), Crossover Error Rate (CER), Accuracy, Confidence
  - Enrollment
  - Purpose: Identification (one-to-many) or verification (one-to-one) system
  - Liveliness detection

Short Introduction to Used Technology

- False Reject Rate (FRR):
  Measure of an authorized user being incorrectly rejected
- False Accept Rate (FAR):
  Measure of an unauthorized user (e. g. attacker) being incorrectly accepted
- Equal Error Rate (EER) or Crossover Error Rate (CER):
  Measure of FAR and FRR being (nearly) the same

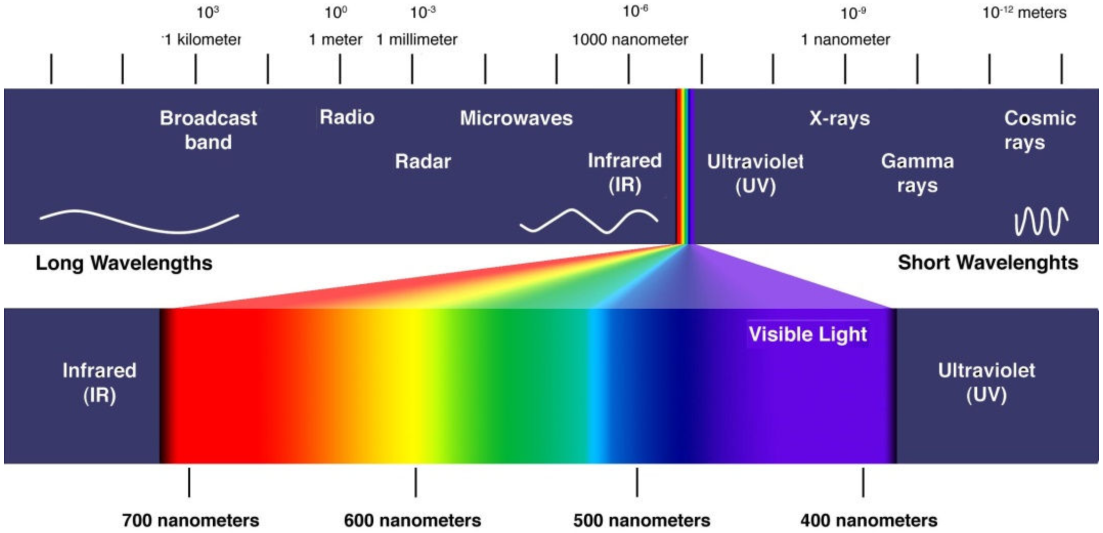
Short Introduction to Used Technology



- False Accept Rate (FAR)
- False Reject Rate (FRR)
- Equal Error Rate (EER) / Crossover Error Rate (CER)

Short Introduction to Used Technology

- Near infrared
  - Electromagnetic radiation
  - Frequency: 100 - 385 THz
  - Wavelength: 780 nm - 3 µm

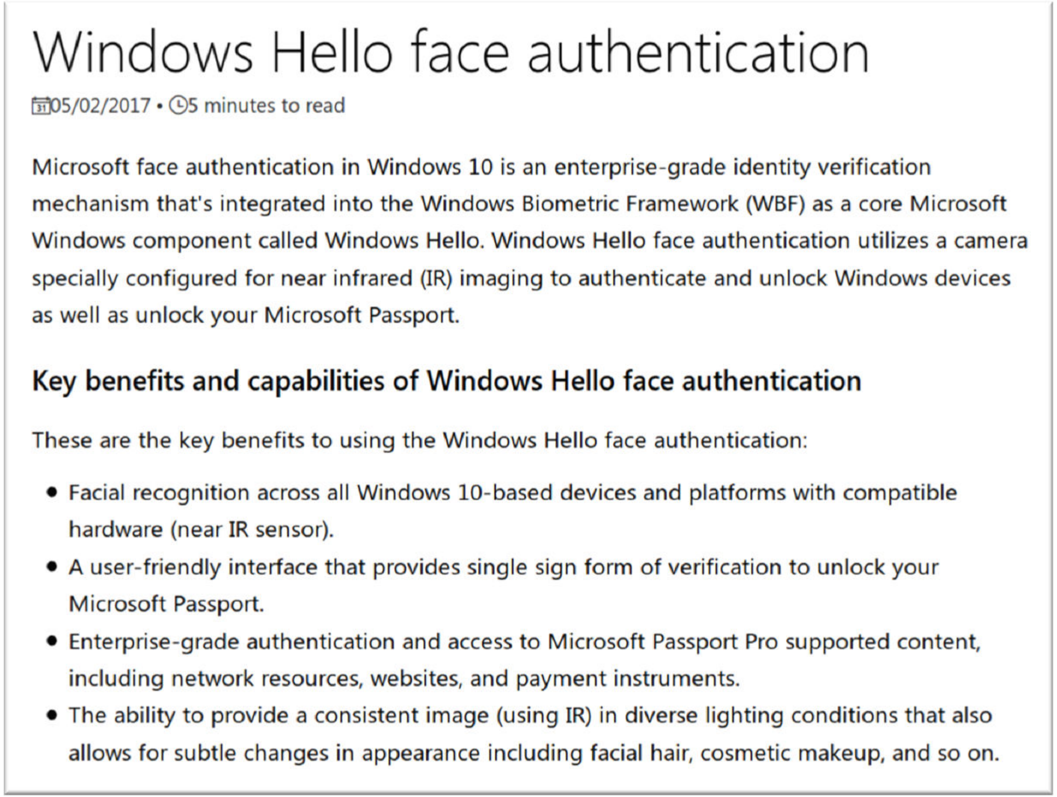


(Source: astronomersgroup.org)

Short Introduction to Used Technology

- Microsoft Windows Hello
  - Available since Windows 10 (2015)
  - Windows Biometric Framework (WBF)
  - Biometric User Authentication
    - Fingerprint Sign-in
    - Face Sign-in

Short Introduction to Used Technology



Windows Hello face authentication

05/02/2017 • 5 minutes to read

Microsoft face authentication in Windows 10 is an enterprise-grade identity verification mechanism that's integrated into the Windows Biometric Framework (WBF) as a core Microsoft Windows component called Windows Hello. Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock Windows devices as well as unlock your Microsoft Passport.

Key benefits and capabilities of Windows Hello face authentication

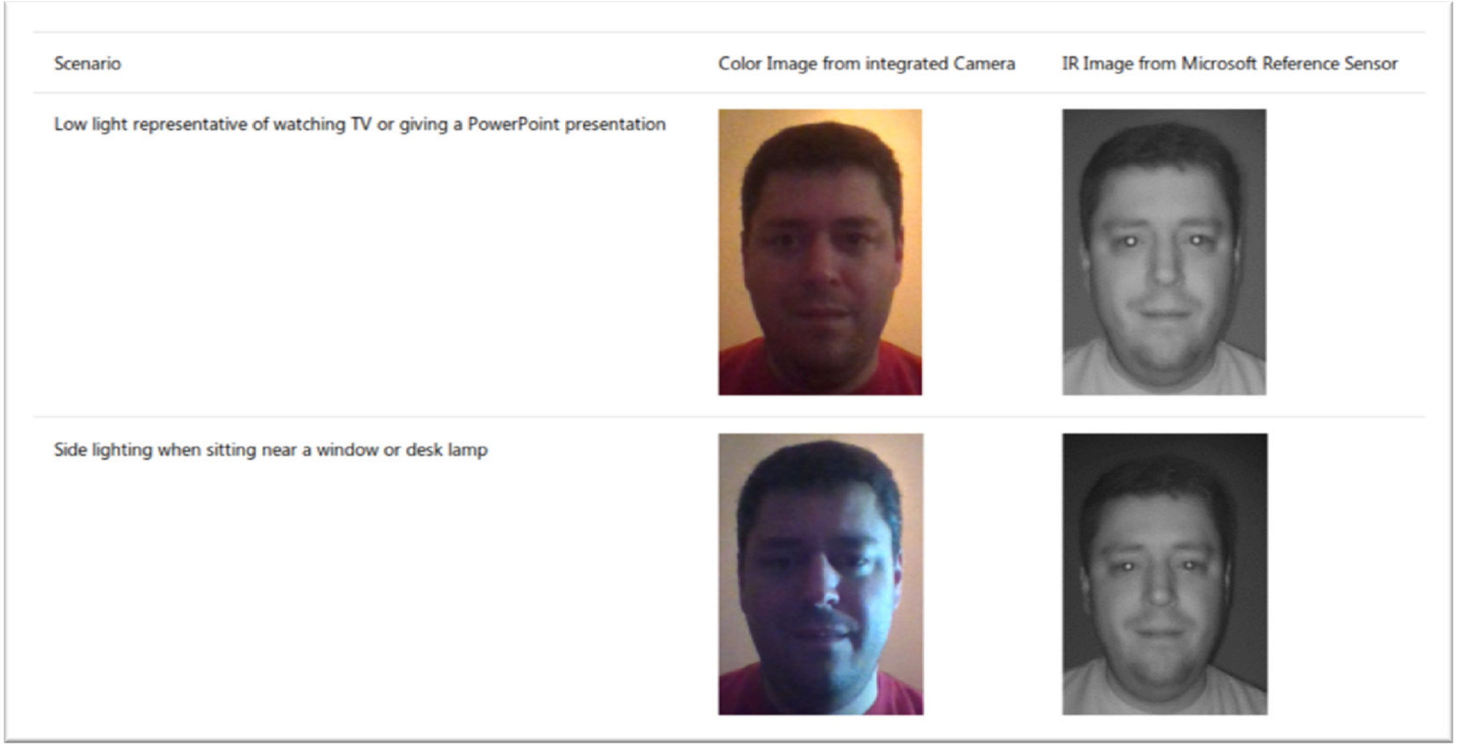
These are the key benefits to using the Windows Hello face authentication:

- Facial recognition across all Windows 10-based devices and platforms with compatible hardware (near IR sensor).
- A user-friendly interface that provides single sign form of verification to unlock your Microsoft Passport.
- Enterprise-grade authentication and access to Microsoft Passport Pro supported content, including network resources, websites, and payment instruments.
- The ability to provide a consistent image (using IR) in diverse lighting conditions that also allows for subtle changes in appearance including facial hair, cosmetic makeup, and so on.

(Source: Microsoft [1])

Short Introduction to Used Technology

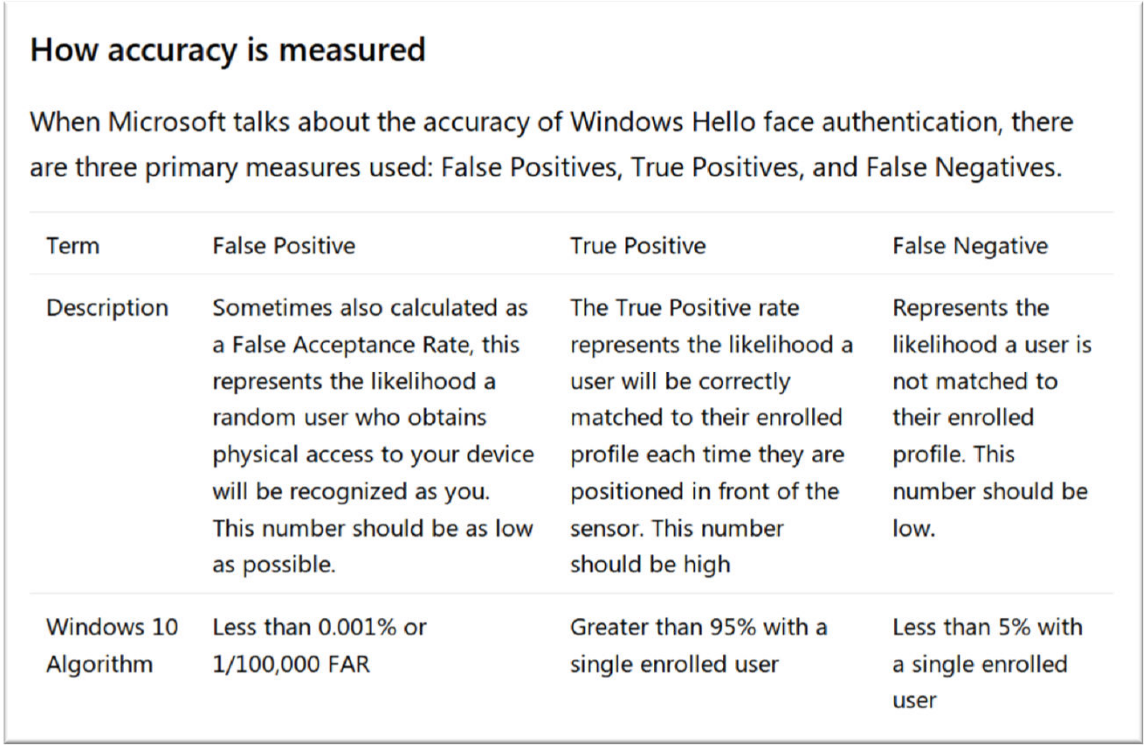
Benefits of near infrared concerning feature extraction



Scenario	Color Image from integrated Camera	IR Image from Microsoft Reference Sensor
Low light representative of watching TV or giving a PowerPoint presentation		
Side lighting when sitting near a window or desk lamp		

(Source: Microsoft [1])

Short Introduction to Used Technology



How accuracy is measured

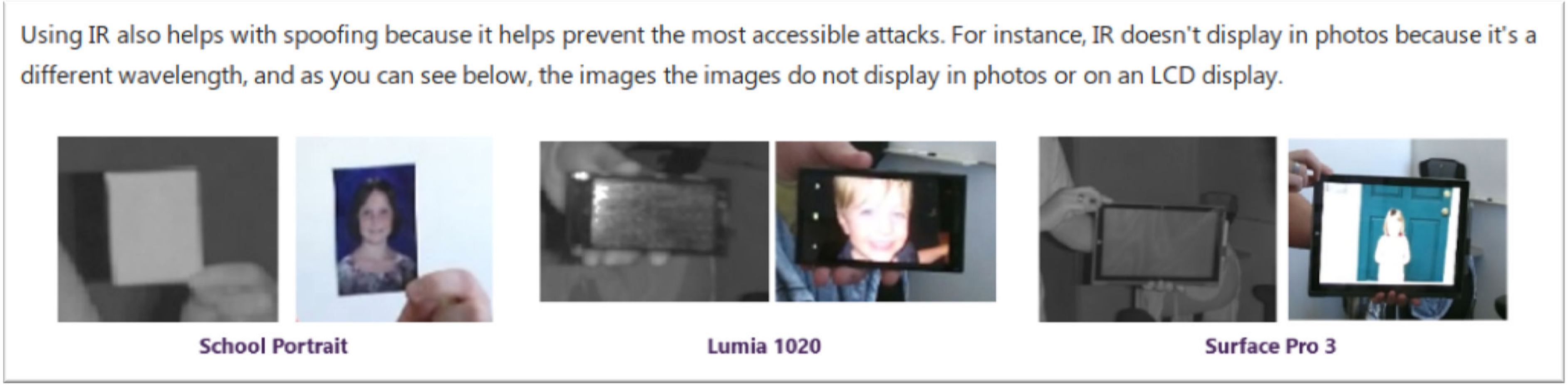
When Microsoft talks about the accuracy of Windows Hello face authentication, there are three primary measures used: False Positives, True Positives, and False Negatives.

Term	False Positive	True Positive	False Negative
Description	Sometimes also calculated as a False Acceptance Rate, this represents the likelihood a random user who obtains physical access to your device will be recognized as you. This number should be as low as possible.	The True Positive rate represents the likelihood a user will be correctly matched to their enrolled profile each time they are positioned in front of the sensor. This number should be high	Represents the likelihood a user is not matched to their enrolled profile. This number should be low.
Windows 10 Algorithm	Less than 0.001% or 1/100,000 FAR	Greater than 95% with a single enrolled user	Less than 5% with a single enrolled user

(Source: Microsoft [1])

Short Introduction to Used Technology

Benefits of near infrared concerning spoofing

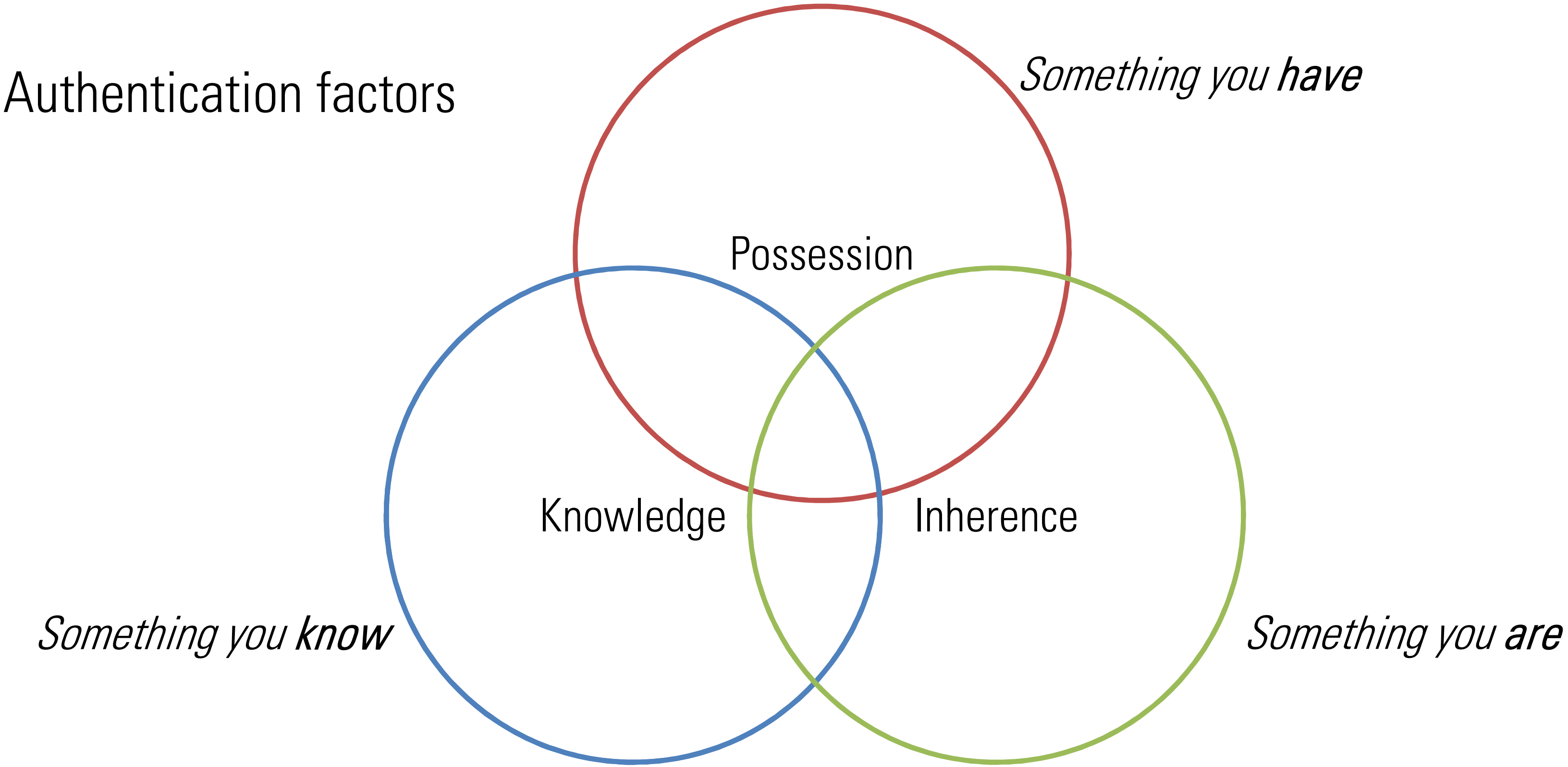


Using IR also helps with spoofing because it helps prevent the most accessible attacks. For instance, IR doesn't display in photos because it's a different wavelength, and as you can see below, the images the images do not display in photos or on an LCD display.

(Source: Microsoft [1])

Short Introduction to Used Technology

Authentication factors


Something you ***have***
Possession
Knowledge
Inherence
Something you ***know***
Something you ***are***

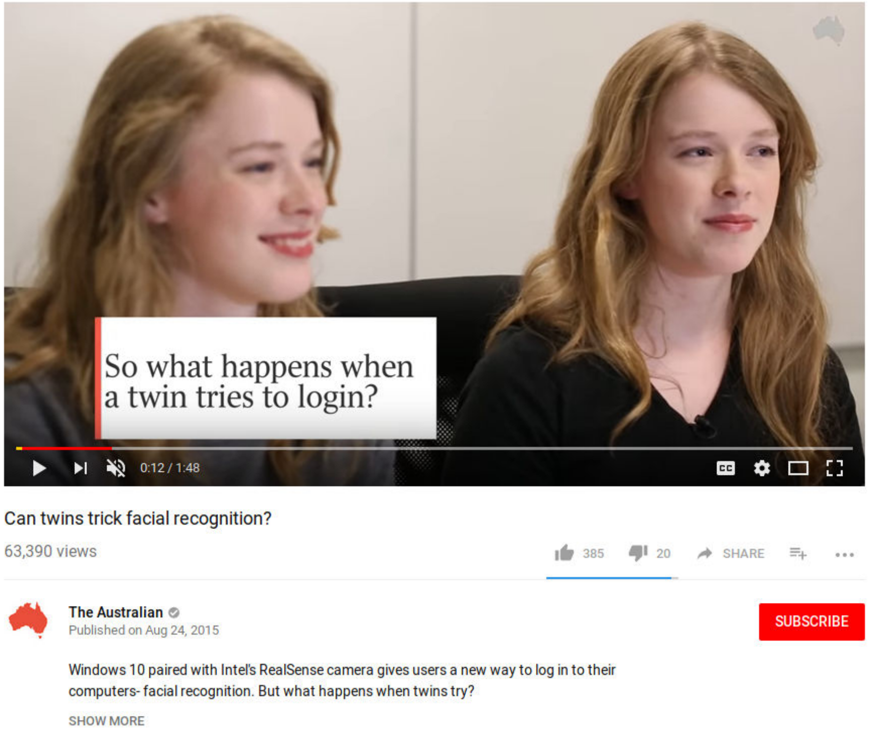
Previous Work of Other Researchers

- *Your face is NOT your password* by Nguyen Minh Duc and Bui Quang Minh, 2009
- *Ich sehe, also bin ich ... Du* by Jan Krissler (starbug), 2014
- *Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos* by Yi Xu, True Price, Jan-Michael Frahm, and Fabian Monrose, 2016
- *Hacking Galaxy S8 Iris Recognition* by Jan Krissler (starbug), 2017
- *Bkav's new mask beats Face ID in 'twin way'*, Bkav, 2017

Overview of Our Research

- Project Background:
  - Customer project with open questions concerning the security of Windows Hello Face Authentication
  - Publicly available information about the security of Windows Hello Face Authentication was scarce
  - iPhone X with Apple Face ID was to be released in a few weeks (November 2017)
- Windows Hello seemed an interesting target to us for learning about face authentication systems using IR technology
- Authentication bypass attack as primary research objective

Overview of Our Research



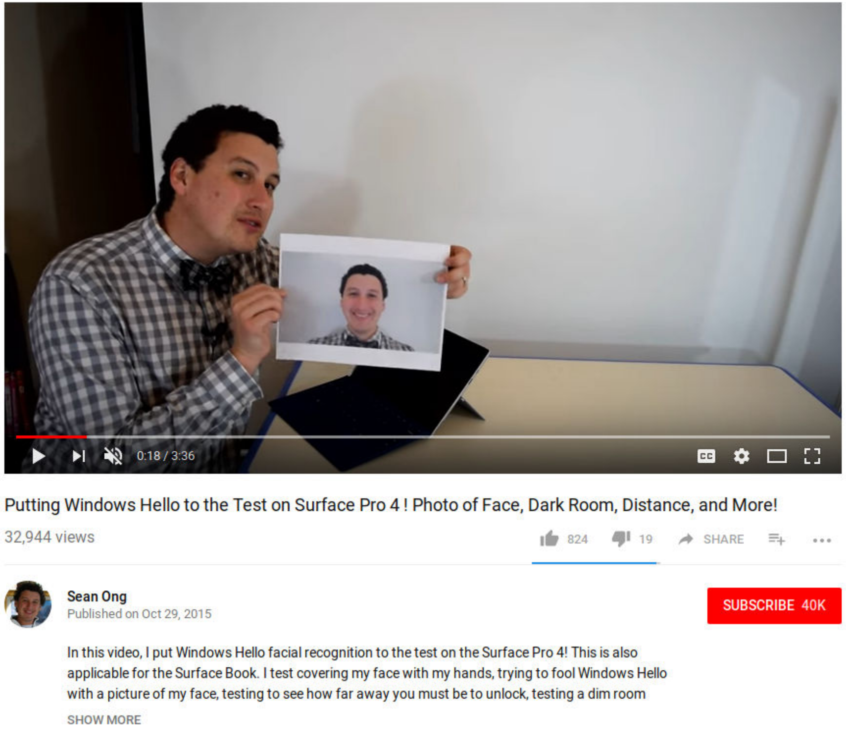
Can twins trick facial recognition?

63,390 views

The Australian
Published on Aug 24, 2015

Windows 10 paired with Intel's RealSense camera gives users a new way to log in to their computers- facial recognition. But what happens when twins try?

(Source: YouTube [2])



Putting Windows Hello to the Test on Surface Pro 4 ! Photo of Face, Dark Room, Distance, and More!

32,944 views

Sean Ong
Published on Oct 29, 2015

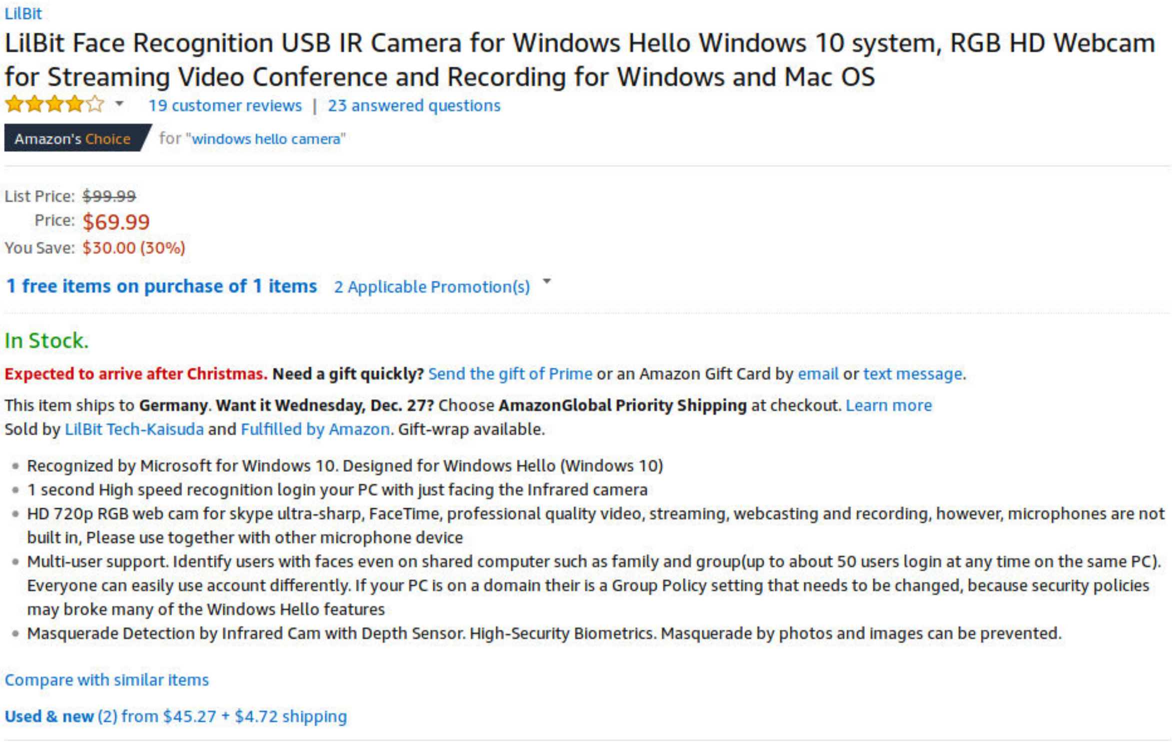
In this video, I put Windows Hello facial recognition to the test on the Surface Pro 4! This is also applicable for the Surface Book. I test covering my face with my hands, trying to fool Windows Hello with a picture of my face, testing to see how far away you must be to unlock, testing a dim room

(Source: YouTube [3])

Test Setup

- Two test devices:
  1. Dell Latitude E7470 with LilBit USB IR Camera
  2. Microsoft Surface Pro 4 with integrated IR camera
- Different versions and OS builds (revisions) of Windows 10

Test Setup



LilBit

LilBit Face Recognition USB IR Camera for Windows Hello Windows 10 system, RGB HD Webcam for Streaming Video Conference and Recording for Windows and Mac OS

★★★★☆ 19 customer reviews | 23 answered questions

Amazon's Choice for "windows hello camera"

List Price: ~~$99.99~~
Price: $69.99
You Save: $30.00 (30%)

1 free items on purchase of 1 items 2 Applicable Promotion(s)

In Stock.

Expected to arrive after Christmas. Need a gift quickly? Send the gift of Prime or an Amazon Gift Card by email or text message.

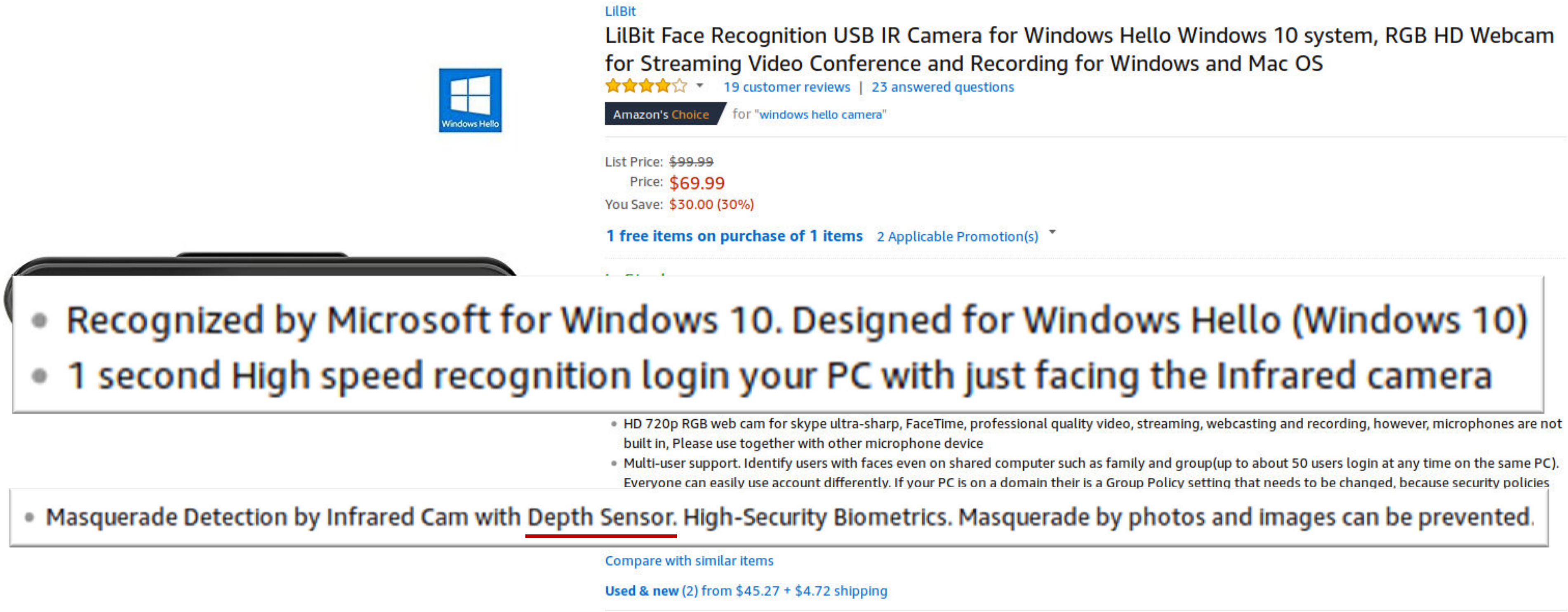
This item ships to **Germany**. **Want it Wednesday, Dec. 27?** Choose **AmazonGlobal Priority Shipping** at checkout. Learn more
Sold by LilBit Tech-Kaisuda and Fulfilled by Amazon. Gift-wrap available.

- Recognized by Microsoft for Windows 10. Designed for Windows Hello (Windows 10)
- 1 second High speed recognition login your PC with just facing the Infrared camera
- HD 720p RGB web cam for skype ultra-sharp, FaceTime, professional quality video, streaming, webcasting and recording, however, microphones are not built in, Please use together with other microphone device
- Multi-user support. Identify users with faces even on shared computer such as family and group(up to about 50 users login at any time on the same PC). Everyone can easily use account differently. If your PC is on a domain their is a Group Policy setting that needs to be changed, because security policies may broke many of the Windows Hello features
- Masquerade Detection by Infrared Cam with Depth Sensor. High-Security Biometrics. Masquerade by photos and images can be prevented.

Compare with similar items

Used & new (2) from $45.27 + $4.72 shipping

Test Setup



LilBit

LilBit Face Recognition USB IR Camera for Windows Hello Windows 10 system, RGB HD Webcam for Streaming Video Conference and Recording for Windows and Mac OS

★★★★☆ 19 customer reviews | 23 answered questions

Amazon's Choice for "windows hello camera"

List Price: ~~$99.99~~

Price: $69.99

You Save: $30.00 (30%)

1 free items on purchase of 1 items 2 Applicable Promotion(s)

- Recognized by Microsoft for Windows 10. Designed for Windows Hello (Windows 10)
- 1 second High speed recognition login your PC with just facing the Infrared camera

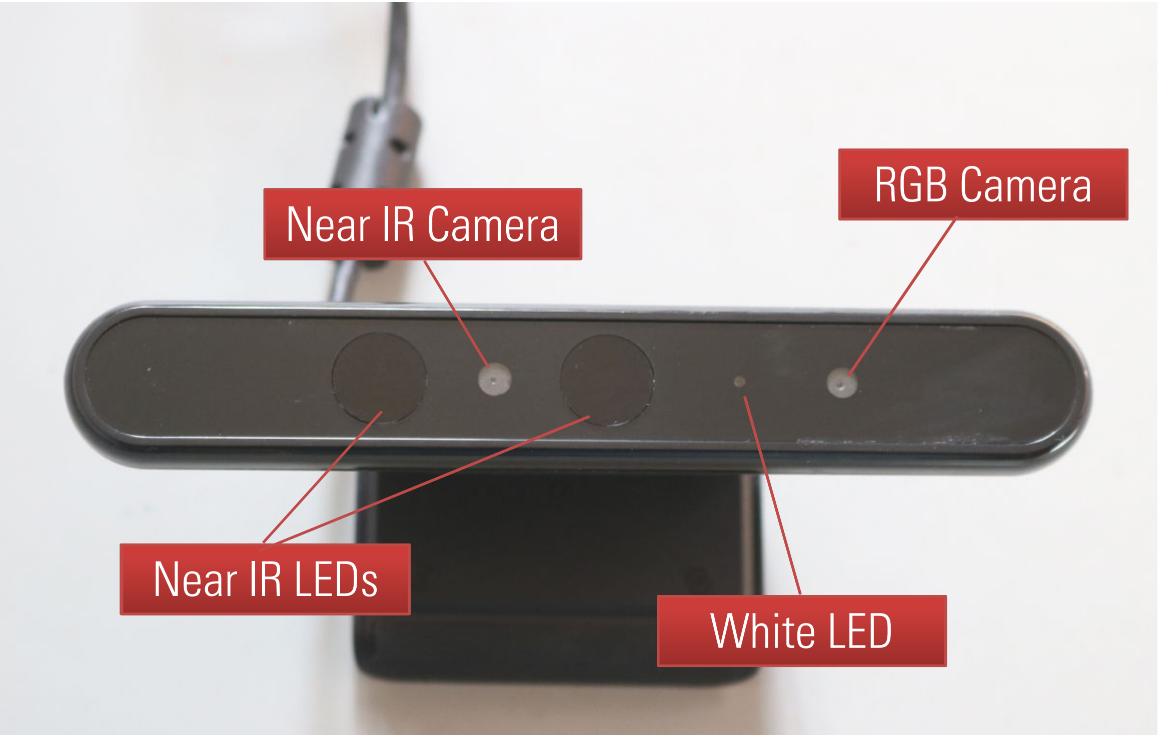
- HD 720p RGB web cam for skype ultra-sharp, FaceTime, professional quality video, streaming, webcasting and recording, however, microphones are not built in, Please use together with other microphone device
- Multi-user support. Identify users with faces even on shared computer such as family and group(up to about 50 users login at any time on the same PC). Everyone can easily use account differently. If your PC is on a domain their is a Group Policy setting that needs to be changed, because security policies

- Masquerade Detection by Infrared Cam with Depth Sensor. High-Security Biometrics. Masquerade by photos and images can be prevented.

Compare with similar items

Used & new (2) from $45.27 + $4.72 shipping

Test Setup



LilBit USB IR Camera

- Supports Windows Hello (according to vendor description)
- 720p RGB camera
- Near infrared camera (Realtek)

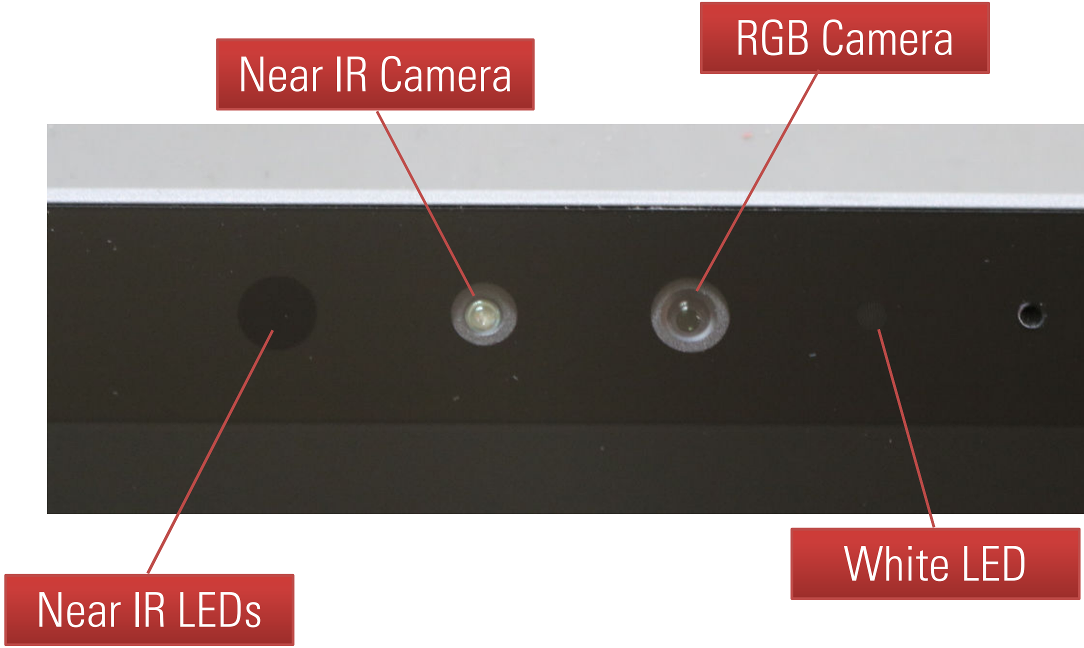
Test Setup

Microsoft Surface Pro 4

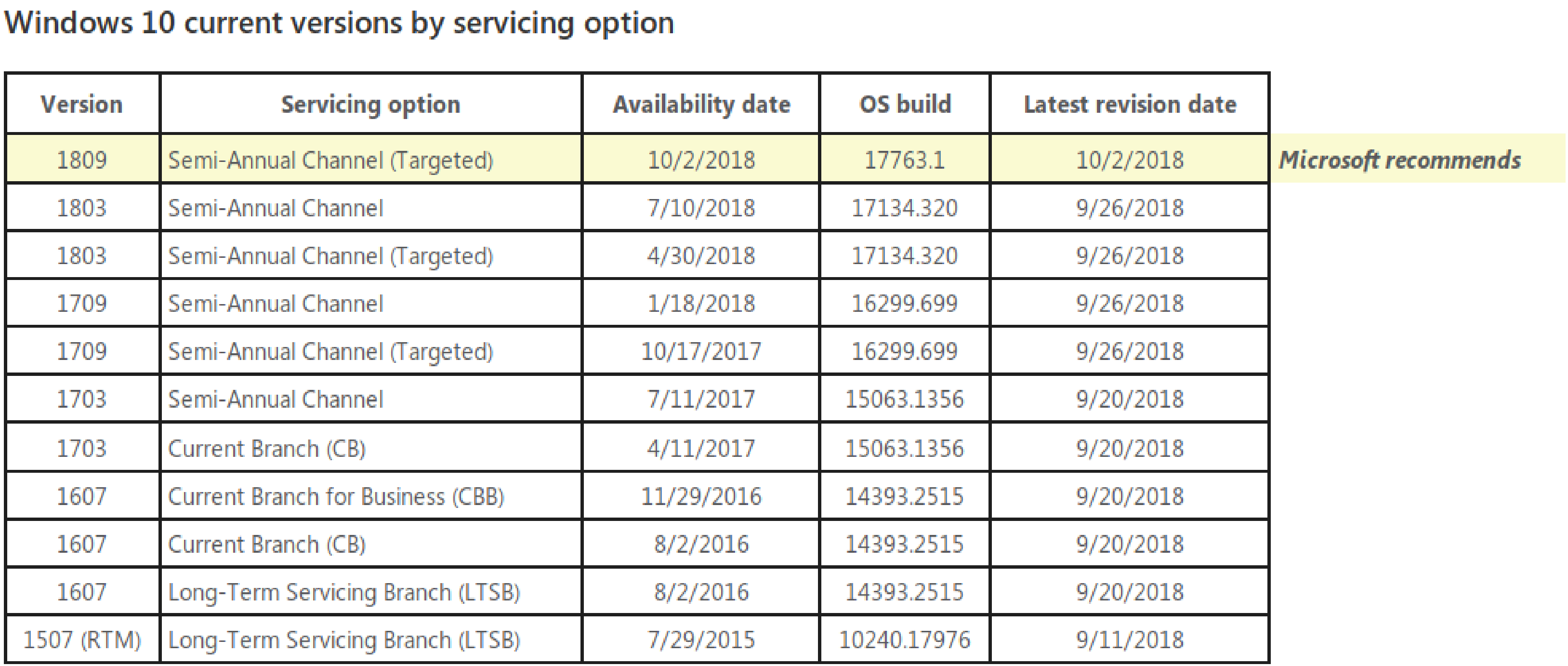
- Supports Windows Hello
- Integrated front-facing 1080p RGB camera (5.0 MP)
- Integrated Windows Hello face authentication camera (near infrared camera)

Test Setup

Microsoft Surface Pro 4 front-facing cameras



Test Setup



Windows 10 current versions by servicing option

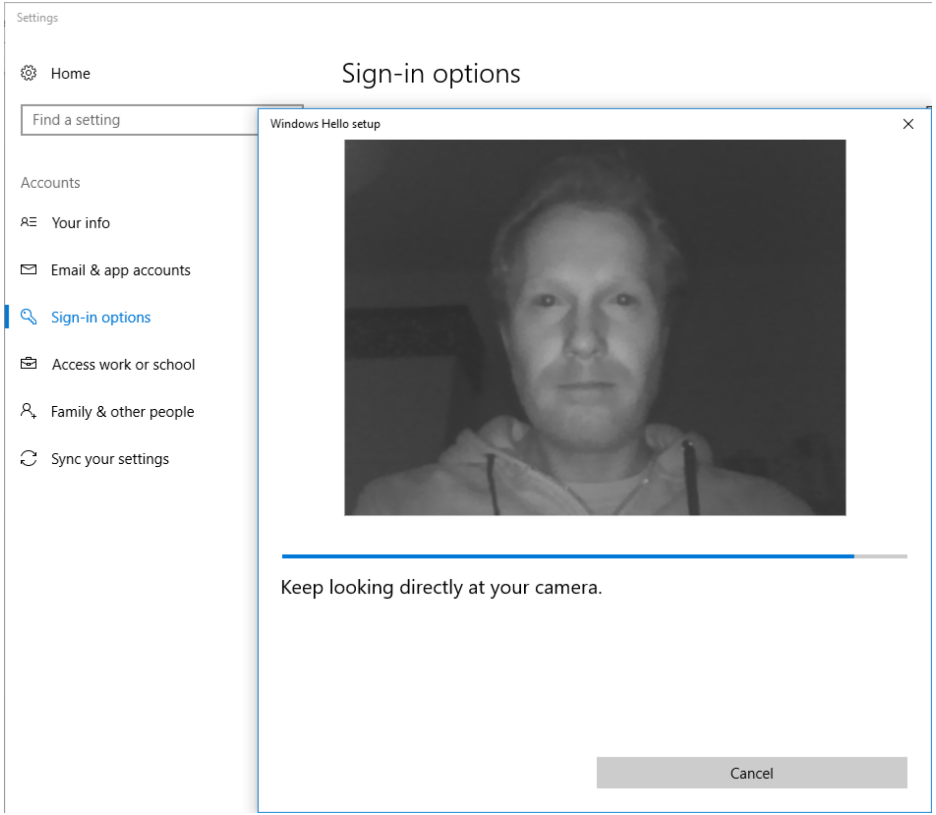
Version	Servicing option	Availability date	OS build	Latest revision date
1809	Semi-Annual Channel (Targeted)	10/2/2018	17763.1	10/2/2018
1803	Semi-Annual Channel	7/10/2018	17134.320	9/26/2018
1803	Semi-Annual Channel (Targeted)	4/30/2018	17134.320	9/26/2018
1709	Semi-Annual Channel	1/18/2018	16299.699	9/26/2018
1709	Semi-Annual Channel (Targeted)	10/17/2017	16299.699	9/26/2018
1703	Semi-Annual Channel	7/11/2017	15063.1356	9/20/2018
1703	Current Branch (CB)	4/11/2017	15063.1356	9/20/2018
1607	Current Branch for Business (CBB)	11/29/2016	14393.2515	9/20/2018
1607	Current Branch (CB)	8/2/2016	14393.2515	9/20/2018
1607	Long-Term Servicing Branch (LTSB)	8/2/2016	14393.2515	9/20/2018
1507 (RTM)	Long-Term Servicing Branch (LTSB)	7/29/2015	10240.17976	9/11/2018

Microsoft recommends

(Source: Microsoft [4])

Test Setup

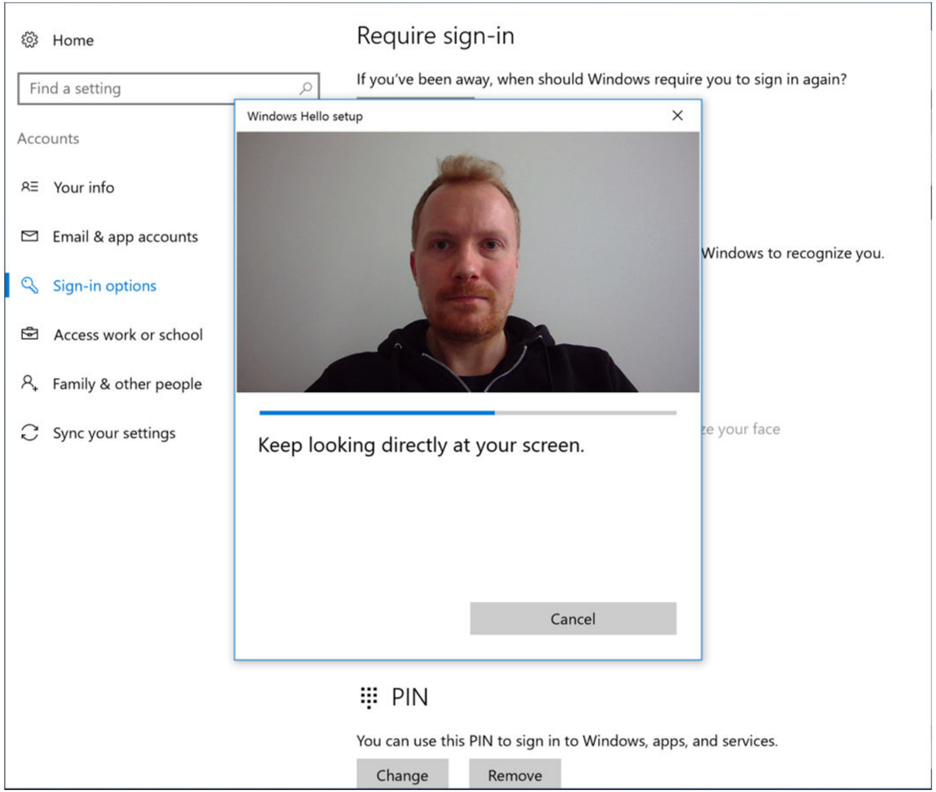
- Enrollment process using the LilBit USB IR Camera (Windows 10 Version 1709)



Keep looking directly at your camera.

Test Setup

- Enrollment process using the built-in near IR camera of the Microsoft Surface Pro 4 (Windows 10 Version 1607)



Require sign-in

If you've been away, when should Windows require you to sign in again?

Windows to recognize you.

ze your face

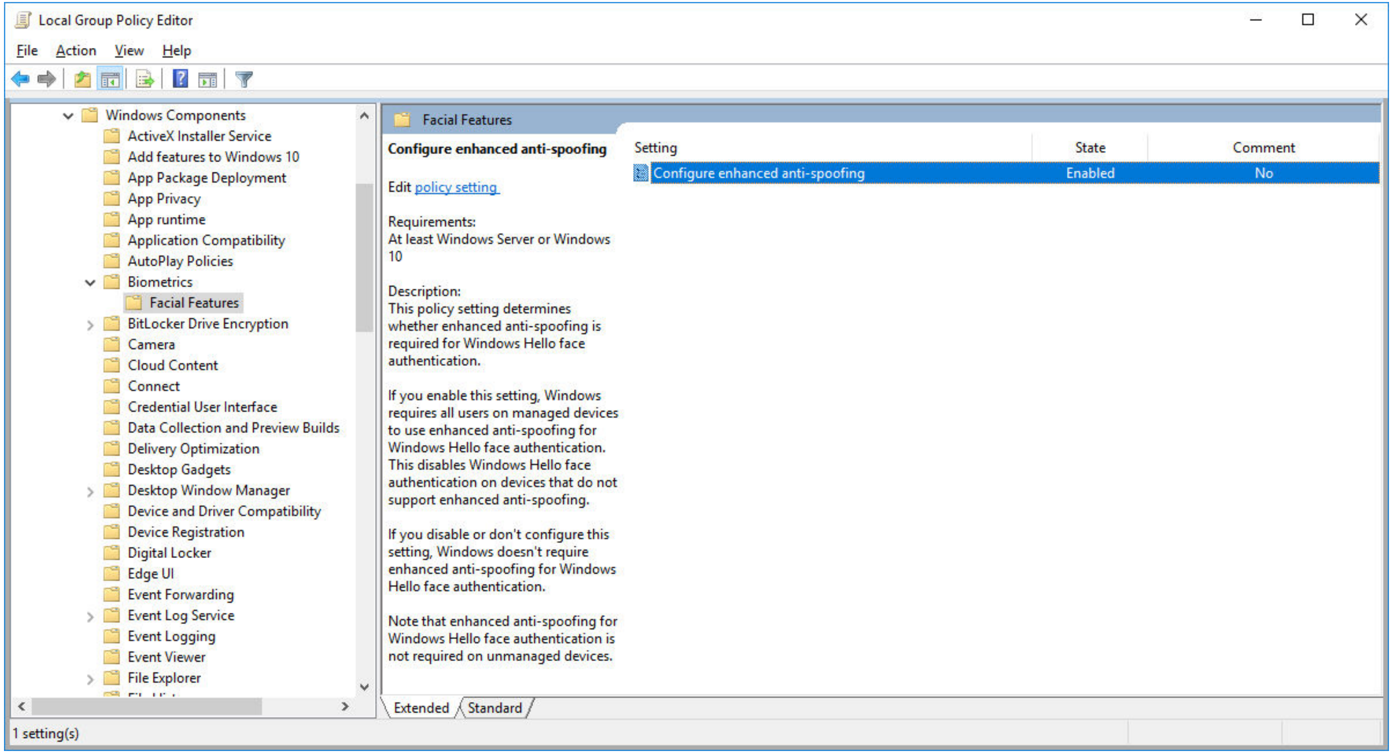
Windows Hello setup

Keep looking directly at your screen.

PIN

You can use this PIN to sign in to Windows, apps, and services.

Test Setup



Facial Features

Configure enhanced anti-spoofing

Edit policy setting

Requirements:
At least Windows Server or Windows 10

Description:
This policy setting determines whether enhanced anti-spoofing is required for Windows Hello face authentication.

If you enable this setting, Windows requires all users on managed devices to use enhanced anti-spoofing for Windows Hello face authentication. This disables Windows Hello face authentication on devices that do not support enhanced anti-spoofing.

If you disable or don't configure this setting, Windows doesn't require enhanced anti-spoofing for Windows Hello face authentication.

Note that enhanced anti-spoofing for Windows Hello face authentication is not required on unmanaged devices.

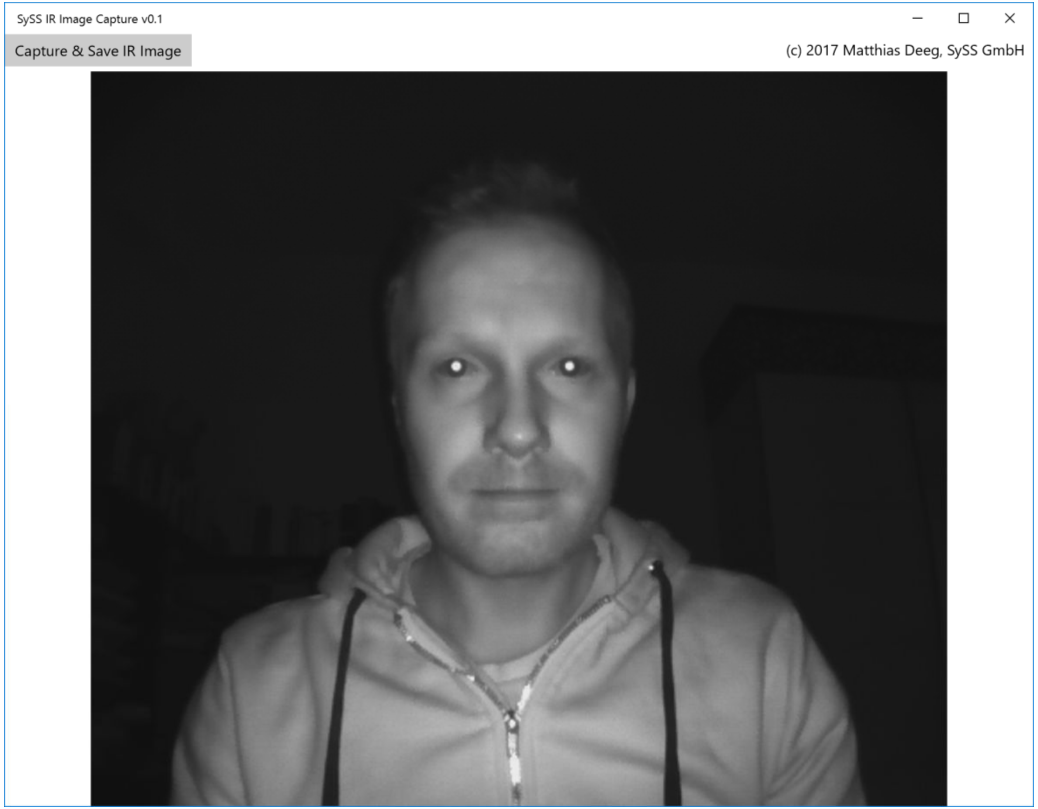
Setting	State	Comment
Configure enhanced anti-spoofing	Enabled	No

Test Methodology

- Black-box testing
- Assumptions about inner workings of Windows Hello Face Authentication
- Understanding the capabilities of near infrared cameras and exploiting their way of perceiving the real world
- Development of software tools to simplify tests
  - IR Image Capture: Windows Software Tool for taking IR pictures (source code [15])
  - PIRI: Python tool for simple image processing (source code [15])
- Trial & error (verification/falsification of generated hypotheses)

Test Methodology

- A matter of perception …
- Simple software tool IR Image Capture based on publicly available source code by Mike Taulty and kaorun 55 ([15], [16])



Test Methodology

- A matter of perception … and reflectance

Display Option	Result
LED display (e.g. iPad 4)	X image cannot be *seen* by near IR camera
Printout on glossy photo paper	X image only badly be *seen* by near IR camera
Inkjet paper printout (Canon PIXMA MP450)	X image cannot be *seen* by near IR camera
Cathode Ray Tube (CRT, old TV set)	X image cannot be *seen* by near IR camera
Offset print (e.g. fashion magazine)	✓ image can be *seen* perfectly by near IR camera
Laser printout out (e.g. HP LaserJet Pro MFP M277dw)	✓ image can be *seen* well by near IR camera

Test Methodology

- Simple image processing regarding brightness …

```
def simple_brightness_rgba(im, factor):
    """Simple brightness function for RGBA images"""

    data = im.load()
    v = int(256 * (factor - 1))

    for x in range(im.width):
        for y in range(im.height):
            c = data[x, y]
            r = saturate(c[0] + v, 255)
            g = saturate(c[1] + v, 255)
            b = saturate(c[2] + v, 255)
            data[x, y] = (r, g, b)
```

Test Methodology

- … and contrast

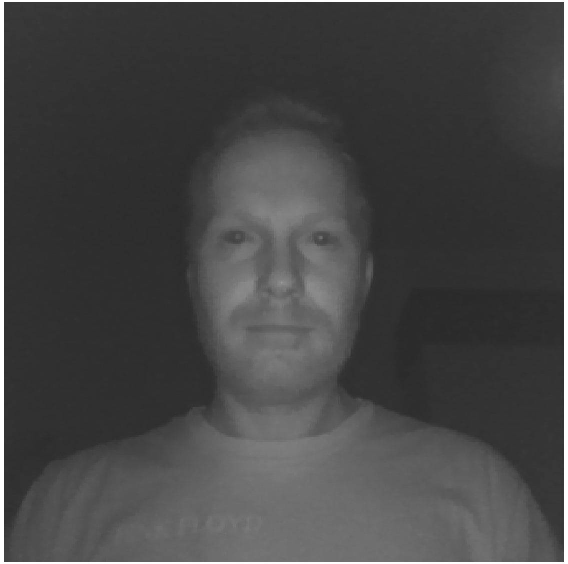
```
def simple_contrast_rgba(im, factor):
    """Simple contrast function for RGBA images"""

    data = im.load()
    level = int(256 * (factor - 1))
    f = (259.0 * (level + 255)) / (255.0 * (259 - level))

    for x in range(im.width):
        for y in range(im.height):
            c = data[x, y]
            r = saturate(f * (c[0] - 128) + 128)
            g = saturate(f * (c[1] - 128) + 128)
            b = saturate(f * (c[2] - 128) + 128)
            data[x, y] = (r, g, b)
```

Test Methodology

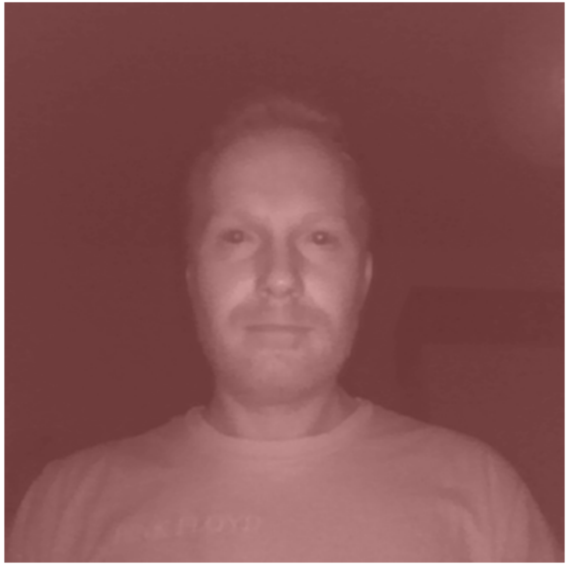
- Used Near IR cameras supported different image resolutions
  - 340x340 px: LilBit USB IR Camera
  - 480x480 px: Microsoft Surface Pro 4 camera
- Primarily, these two cameras were used in combination with the developed software tool IR Image Capture for taking test pictures
- Observation regarding enhanced anti-spoofing feature:
  - Disabled: Only the near IR camera is used
  - Enabled: Both the near IR camera and the RGB camera are used

Test Methodology

Examples of test images:

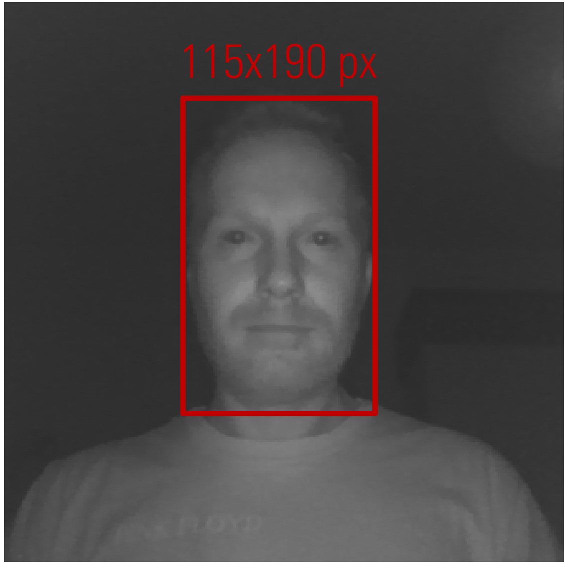


340x340 px, grayscale image (raw)



340x340 px, colored image (processed)

Test Methodology



340x340 px, grayscale image (raw)

- The size of the actual data used for face recognition is even smaller
- For example,115x190 px in the 340x340 px example image (shown left), or 160x270 px in an 480x480 px example image

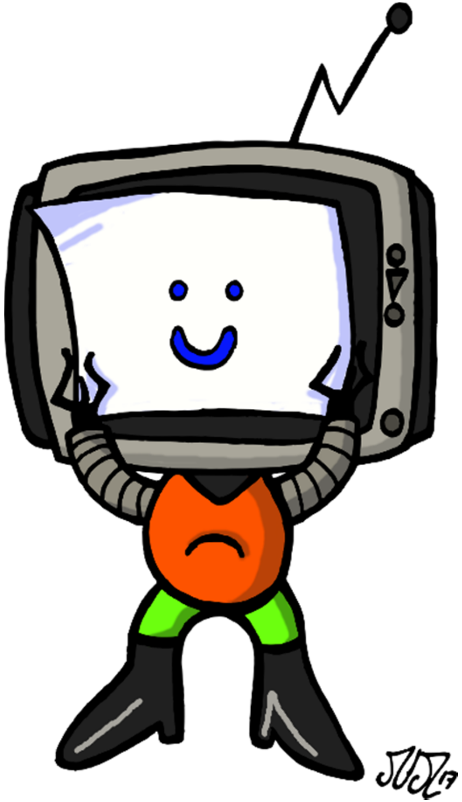
Attack Surface and Attack Scenario

- Attack surface
  - Windows logon/lock screen
  - Windows Hello compatible camera used for Face Authentication
- Attack scenario
  - Attacker with physical access to target device providing access to Windows logon/lock screen gains unauthorized access to Windows operating system and stored sensitive data
    - Thief (stolen device)
    - Evil maid / cleaning staff (temporary physical access)

Found Security Vulnerability

- Authentication Bypass by Spoofing (CWE-290)
- It is possible to bypass the Windows Hello face authentication via a simple spoofing attack using a printed photo of an authorized person
- The paper printout for the attack has the following properties:
  1. The image shows a frontal view of the person’s face
  2. The image was taken with a near-infrared camera
  3. Brightness and contrast were modified via simple image processing methods
  4. The paper printout was created with a laser printer

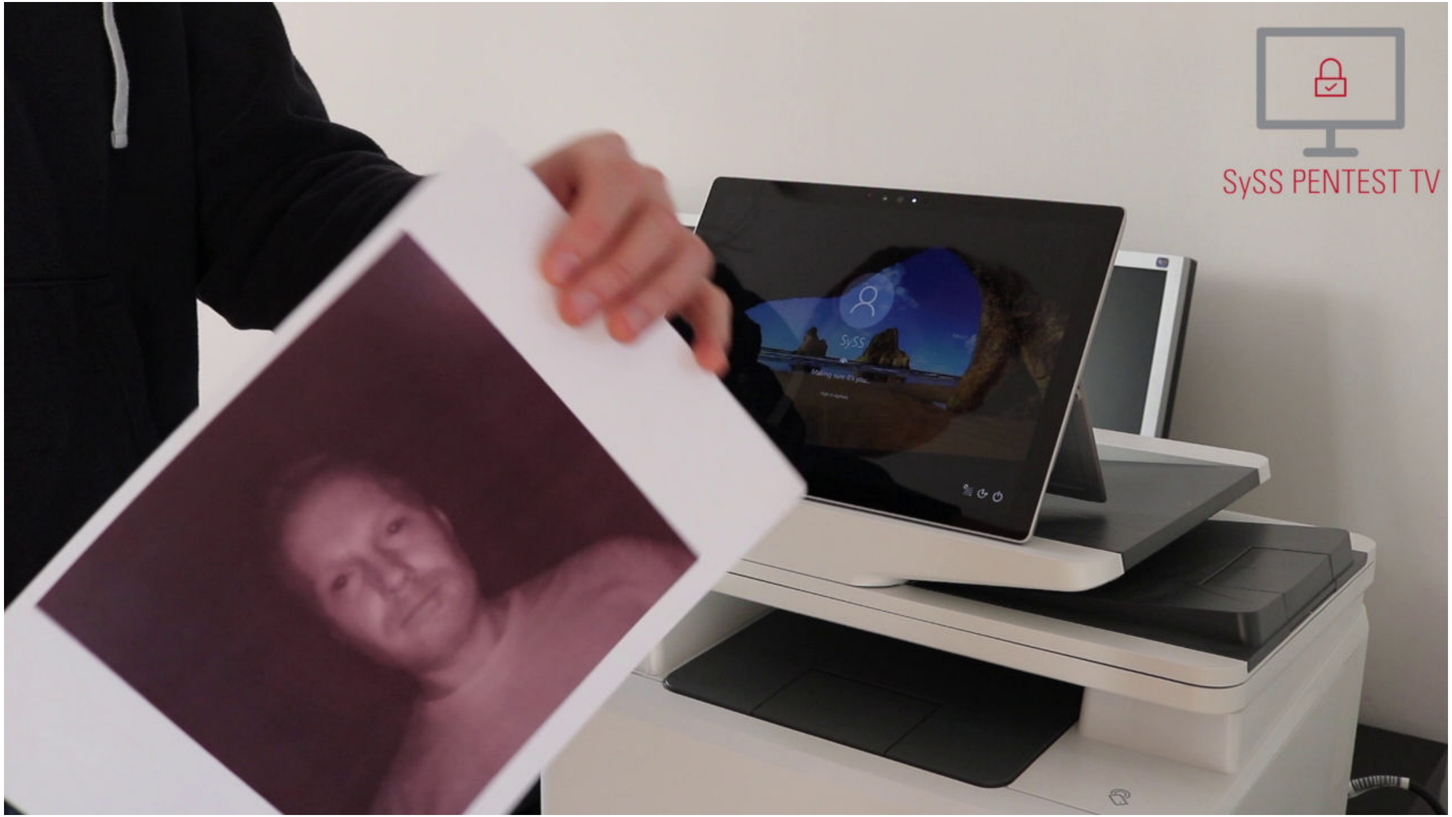
Authentication Bypass via Spoofing



„Here's Johnny!"

Unauthorized access to a computer system

Demo



Test Results

Windows Version	Test Device 1 Dell Latitude E7470 with LilBit Camera		Test Device 2 Microsoft Surface Pro 4	
	with enhanced anti-spoofing	*without enhanced anti-spoofing*	*with enhanced anti-spoofing*	*without enhanced anti-spoofing*
Windows 10 Pro (Version 1709, OS Build 16299.98)	n/a	yes	no	yes
Windows 10 Pro (Version 1709, OS Build 16299.19)	n/a	yes	untested	untested
Windows 10 Pro (Version 1703, OS Build 15063.726)	n/a	yes	no	yes
Windows 10 Pro (Version 1703, OS Build 15063.674)	n/a	yes	untested	untested
Windows 10 Pro (Version 1703, OS Build 15063.483)	n/a	yes	untested	untested
Windows 10 Pro (Version 1607, OS Build 14393.1914)	n/a	yes	yes	yes
Windows 10 Pro (Version 1607, OS Build 14393.1770)	n/a	yes	yes	yes
Windows 10 Pro (Version 1511, OS Build 10586.1232)	n/a	yes	untested	untested

Conclusion

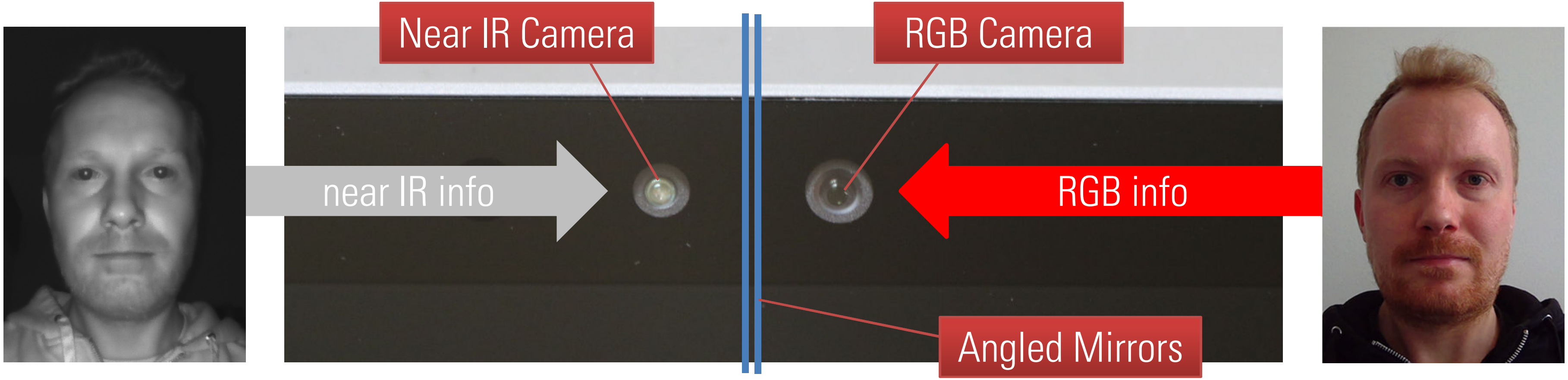
- Windows Hello Face Authentication can be bypassed by rather simple means on different Windows 10 versions with different hardware and software configurations
- The enhanced anti-spoofing feature is not supported by all near-infrared cameras that support the default configuration

Recommendations

- Update the Windows operating system to the latest version and OS build (revision), at least Version 1703, OS Build 15063.726 according to our test results
- Only use Windows Hello compatible cameras that support the enhanced anti-spoofing feature
- Enable enhanced anti-spoofing feature of Windows Hello (Administrative Templates → Windows Components → Biometrics → Facial Features → Configure enhanced anti-spoofing)
- Reconfigure Windows Hello Face Authentication after software update from vulnerable version and after configuration changes

Further Research

- Authentication bypass attack against Windows Hello Face Authentication in current Windows 10 versions (e.g. 1803, 1809)
- Maybe a single paper printout is not sufficient anymore, but an attack with two images could work (near infrared and RGB)?



References

1. *Windows Hello face authentication*, Microsoft, https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-face-authentication, 2017
2. *Can Twins Trick Facial Recognition?,* The Australian, https://www.youtube.com/watch?v=J1NL246P9Vg
3. *Putting Windows Hello to the Test on a Surface Pro 4,* Sean Ong, https://www.youtube.com/watch?v=nMdVHDqJsEs
4. *Windows 10 Release Information*, Microsoft, *https://www.microsoft.com/en-us/itpro/windows-10/release-information, 2018*
5. *Biometricks: Bypassing an Enterprise-Grade Biometric Face Authentication System*, Matthias Deeg, https://www.syss.de/pentest-blog/article/2017/12/18/460/, 2017
6. *SySS Security Advisory SYSS-2017-027*, Matthias Deeg and Philipp Buchegger, https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2017-027.txt, 2017
7. *SySS Proof-of-Concept Video, Windows Hello Face Authentication Bypass PoC*, Matthias Deeg, https://www.youtube.com/watch?v=Qq8WqLxSkGs, 2017

References

8. *SySS Proof-of-Concept Video, Windows Hello Face Authentication Bypass PoC II*, Matthias Deeg, https://www.youtube.com/watch?v=GVKKcoOZHwk, 2017
9. *SySS Proof-of-Concept Video, Windows Hello Face Authentication Bypass PoC III*, Matthias Deeg, https://www.youtube.com/watch?v=cayqU3WCOso, 2017
10. *Your face is NOT your password*, Nguyen Minh Duc and Bui Quang Minh, https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password-slides.pdf, 2009
11. *Ich sehe, also bin ich … Du*, Jan Krissler (starbug), https://media.ccc.de/v/31c3_-_6450_-_de_-_saal_1_-_201412272030_-_ich_sehe_also_bin_ich_du_-_starbug, 2014
12. *Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos*, Yi Xu, True Price, Jan-Michael Frahm, and Fabian Monrose, https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_xu.pdf, 2016

References

13. *Hacking Galaxy S8 Iris Recognition* by Jan Krissler (starbug), https://media.ccc.de/v/biometrie-s8-iris-en, 2017
14. *Bkav's new mask beats Face ID in 'twin way'*, Bkav, http://www.bkav.com/d/top-news/-/view_content/content/103968/bkav%92s-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions, 2017
15. *Kinect V2, Windows Hello and Perception APIs*, Mike Taulty, https://mtaulty.com/2015/12/03/m_15988/, 2015
16. *PerceptionSamples*, kaorun55, https://github.com/kaorun55/PerceptionSamples, 2015
17. *SySS Biometricks GitHub Repository*, SySS GmbH, https://github.com/SySS-Research/biometricks, 2018

Thank you very much ...

. . . for your attention.

Do you have any questions?

E-mail: matthias.deeg@syss.de

PGP Fingerprint: D1F0 A035 F06C E675 CDB9 0514 D9A4 BF6A 34AD 4DAB

THE PENTEST EXPERTS

WWW.SYSS.DE