Your face is NOT your password

Duc Nguyen
Bkis, Vietnam

http://www.bkav.com.vn

Contents

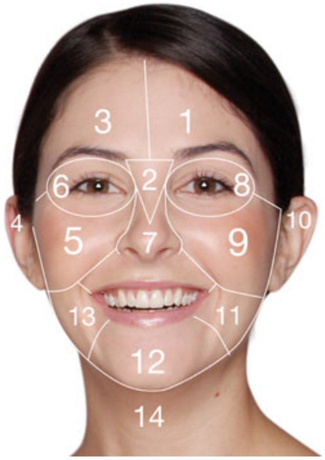
1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Contents

1. **Face recognition authentication and drawbacks**
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Face Recognition

- Face recognition is one of the biometric technologies
- Face recognition has 2 applications:
- Identification (Search for an unknown face in a database of faces…)
- Access Control (Authentication in buildings, in computers …)
- Bkis research focus on access control systems and their security drawbacks.



Face recognition authentication

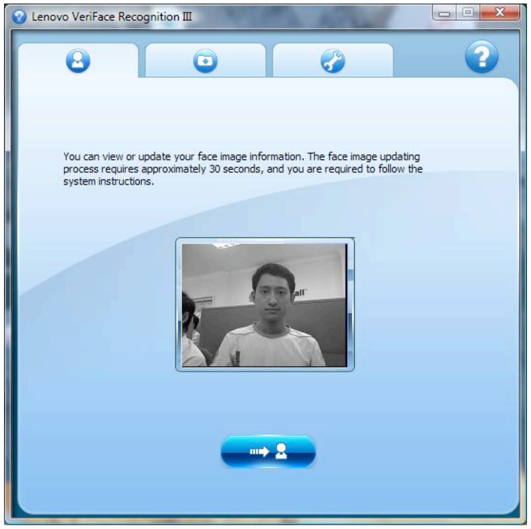
- Let me show you a short video clip on Face Recognition Authentication
  Video
- We have just seen an advertisement video of a new feature of current laptops, which is authentication using face recognition technology.
- We observe that Candy, the owner of the laptop, does not have to type in her password to log in. She sits in front of the computer and let it recognize her face.

Face recognition authentication

- At the moment, there are 3 laptop manufacturers that make use of this technology in their products.
- They are ASUS, TOSHIBA and LENOVO.

Face recognition authentication

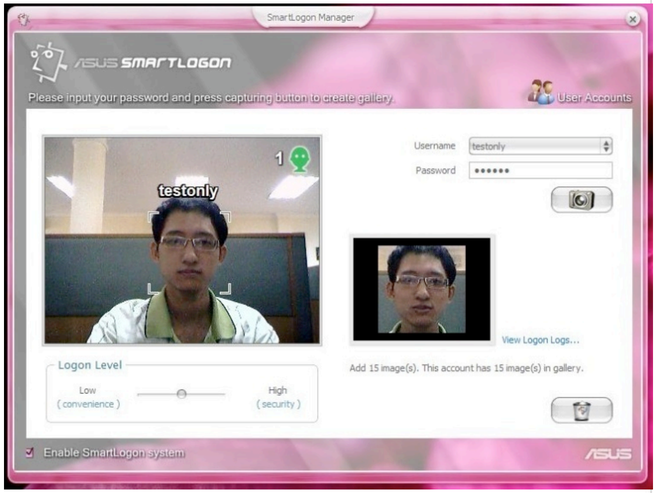
- Develop their own software with their own algorithms



You can view or update your face image information. The face image updating process requires approximately 30 seconds, and you are required to follow the system instructions.

Lenovo: Veriface

Asus: Smart Logon



Please input your password and press capturing button to create gallery.

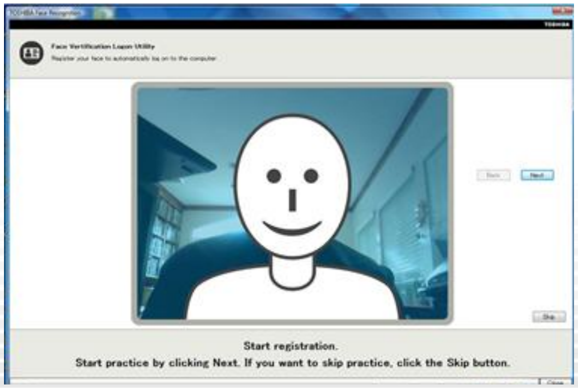
Username: testonly

Password: ••••••

Logon Level: Low (convenience) — High (security)

Add 15 image(s). This account has 15 image(s) in gallery.

☑ Enable SmartLogon system



Face Verification Logon Utility

Register your face to automatically log on to the computer

Start registration.

Start practice by clicking Next. If you want to skip practice, click the Skip button.

Toshiba: Face Recognition

Face Recognition Authentication

- Drawbacks: Let’s see

Contents

1. Face recognition authentication and drawbacks
2. **Test on Asus laptop**
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

ASUS

Laptop: **F6S Series**, **X80 Series**
Software: ASUS SmartLogin ver 1.0.0005

Link to the software

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. **Why ?**
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Why ?

- The answer is that during the research on the algorithm on face recognition technology applied for laptops, we found that the algorithm has some weaknesses.
- Based on that, a bad guy can create a fake face recognition. That can start from some simple pictures of the real owner, and combining with the manufacturer's algorithm, they can create the fake face recognition, as you have just seen.

Why ?

Face Recognition drawbacks

1. Influences of changes in lighting

- The basic algorithms have not worked well when there are changes in lighting.
- In the latest performance measurement report of face recognition algorithms, the result was good only when the lighting did not change.
- Will further modifications of the technology proposed by the three manufacturers solve this lighting problem?

Why ?

Face Recognition drawbacks

2. Influences of image capturing devices

- Built-in cameras manufactured by those three companies have low resolution (0.3 Megapixel, 1.3 Megapixel and highest being 2.0 Megapixel).
- Might low resolution images become flaws that can be taken advantage of?
- It’s not the main reason of the vulnerability but it could make the algorithms easier to be broken.

Why ?

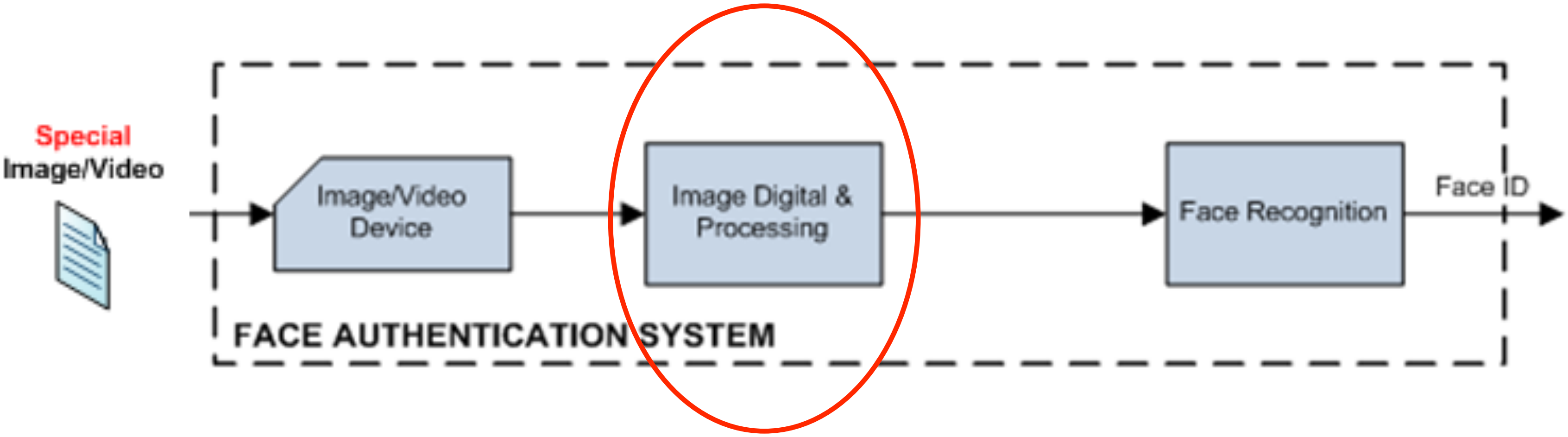
Face Recognition drawbacks

3. Influences of Image Processing

- All of the algorithms use digitalized images, which go through image processing.
- This is the weakest security flaw in face recognition systems.

Why ?

Face Authentication System



Face Recognition Bypass Model

How to have special images ? We will discuss more details later

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. **Do the manufacturers know about it ?**
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Do the manufacturers know about it ?

- When the manufacturers introduced this feature into these all laptops, did they recognize its weaknesses ?
- And to find out the answer, let me invite you to see another video clip.
- Watch the Video

Do the manufacturers know about it ?

- Yes
- The manufacturers have already paid attention to this issue.
- However, the algorithm has a fundamental flaw.
- Even though they have applied more technical modifications to reduce the weakness, they have not been able to solve it completely.
- It is not secure enough to serve as a security feature as advertised by manufacturers.

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. **Test on Lenovo and Toshiba laptops**
6. Research results
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Laptop: **L310**, **M300**
Software: Toshiba Face Recognition ver 2.0.2.32

TOSHIBA

Lenovo

Laptop: Lenovo **Y410**, **Y430**
Software: Lenovo Veriface III

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. **Research results**
7. Attack Scenarios
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Research results

The Rate of Bypass Face Recognition Authentication Mechanism

	Lenovo		Asus		Toshiba	
	Gray Image	*Color Image*	*Gray Image*	*Color Image*	*Gray Image*	*Color Image*
BruteForce	High	High	-	High	-	High
No BruteForce	High	High	-	Medium	-	Low

- Gray image
- Color image
- Brute Force
- No Brute Force

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. **Attack Scenarios**
8. Live demonstration
9. Recommendation for manufacturers
10. Questions and Answers

Attack Scenarios

1. Obtain images of owner’s face.
2. Regenerate the fake face recognition suite → Special images.
3. Bypass the face authentication using these images

Attack Scenarios

Video chat: MSN, Yahoo Messenger, AOL, Skype…

Internet : Flickr, Yahoo Blog, Facebook …

Tele cameras: capturing from the far distance

Invite owner to take a photograph with him/her

…

Attack Scenarios

Attack Scenarios

- This attack method is more difficult to notice: There is no change in your systems, and you still believe that your laptop is being protected, without knowing that somebody has logged on to your laptop with your photo.
- Different from someone resetting your password or connecting your laptop's hard drive to his computer.

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. **Live demonstration**
9. Recommendation for manufacturers
10. Questions and Answers

Live demonstration

- Method of testing
- Lenovo Y430

Live demonstration

- While we are waiting for the result of creating the fake face recognition picture, we shall watch another short video.
- Watch the Video

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Research results
7. Attack Scenarios
8. Live demonstration
9. **Recommendation for manufacturers**
10. Questions and Answers

Recommendation for manufacturers

- When we found out about the vulnerability, we sent warnings to manufacturers: Asus, Lenovo, and Toshiba.
- However, they have not given any official response yet.
- This is an irresponsible act of these three manufacturers toward their customers.

Recommendation for manufacturers

- Our research results show that the face recognition technology being used by Asus, Lenovo and Toshiba is not secure enough to protect users.
- We assert that, there is no way to fix this vulnerability.

Recommendation for manufacturers

- Below are our recommendations to the manufacturers Asus, Lenovo, Toshiba:

1. Stop developing this technology and remove it from all the models of their laptops.
2. Give an official advisory to global users: Stop using this function.

Contents

1. Face recognition authentication and drawbacks
2. Test on Asus laptop
3. Why ?
4. Do the manufacturers know about it ?
5. Test on Lenovo and Toshiba laptops
6. Live demonstration
7. Research results
8. Attack Scenarios
9. Recommendation for manufacturers
10. **Questions and Answers**

Questions and Answers

Contact Information

- Mr. Duc Nguyen
- Manager of Application Security Department
- Email: DucNM@bkav.com.vn
- Bkis, Vietnam
- www.bkis.vn, www.bkav.com.vn

Thank you for listening !