Computer Security Seminar

Security Engineering R. Anderson
Chapter 15: Biometrics

Ben Mussay
Supervised by: Prof. Orr Dunkelman

Computer Science Department

Sunday 8th December, 2019
Outline

- Introduction
- Handwritten Signatures
- Face Recognition
- Fingerprint
- Biometric Database Law
- If everybody think it’s secure, it probably isn’t
- Summary
Introduction

- Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).
Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).

A person can be recognized based on 3 methods:
Introduction

- Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).
- A person can be recognized based on 3 methods:
  1. What you know - passwords
  2. What you have - RFID Chip
  3. What you are - fingerprint
Introduction

- Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).
- A person can be recognized based on 3 methods:
  1. What you know - passwords
  2. What you have - RFID Chip
  3. What you are - fingerprint
Introduction

- Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).
- A person can be recognized based on 3 methods:
  1. What you know - passwords
  2. What you have - RFID Chip
  3. What you are - fingerprint
Introduction

- Identify individuals uniquely has been crucial to the fabric of human society (Regulation of international border crossings).
- A person can be recognized based on 3 methods:
  1. What you know - passwords
  2. What you have - RFID Chip
  3. What you are - fingerprint
- Biometrics is the science of establishing the identity of an individual based on the physical and/or behavioral characteristics.
Introduction - Usage

- Law enforcement and Forensic
Introduction - Usage

- Law enforcement and Forensic
- Military - Know your enemy
Introduction - Usage

- Law enforcement and Forensic
- Military - Know your enemy
- Border control, travel, and migration (US-VISIT)
Introduction - Usage

- Law enforcement and Forensic
- Military - Know your enemy
- Border control, travel, and migration (US-VISIT)
- Civil Identity (i.e. Biometric database of the government)
Introduction - Usage

- Law enforcement and Forensic
- Military - Know your enemy
- Border control, travel, and migration (US-VISIT)
- Civil Identity (i.e. Biometric database of the government)
- ...

Ben Mussay, Supervised by: Prof. Orr Dunkelman
Computer Security Seminar
Introduction - Usage

- Law enforcement and Forensic
- Military - Know your enemy
- Border control, travel, and migration (US-VISIT)
- Civil Identity (i.e. Biometric database of the government)
- ...

Ben Mussay, Supervised by: Prof. Orr Dunkelman
University of Haifa
Computer Security Seminar
Introduction - Definitions

- **FAR (False Accept Rate):** an invalid user is accepted by the system
- **FRR (False Reject Rate):** a valid user is rejected by the system

Signatures

- Behavioral characteristic

Source: blog.bcdb.com/lies-disney-told/walt-disneys-signature/
Signatures

- Behavioral characteristic
- Essential tool to conduct business in China (Chop or Seal)

Signatures

- Behavioral characteristic
- Essential tool to conduct business in China (Chop or Seal)
- Very Popular
Signatures

- Behavioral characteristic
- Essential tool to conduct business in China (Chop or Seal)
- Very Popular
- Weak authentication - liability for forgery?
Signatures

- Behavioral characteristic
- Essential tool to conduct business in China (Chop or Seal)
- Very Popular
- Weak authentication - liability for forgery?
- Solutions:
  1. Deep Learning
  2. Signature Tablet
  3. PIN

Source: signature.wacom.eu/awards_certificates/wacom-signature
Face Recognition


Ben Mussay, Supervised by: Prof. Orr Dunkelman
Computer Security Seminar
Face Recognition

- 15% of the market
Face Recognition

- 15% of the market
- Surveillance
Face Recognition

- 15% of the market
- Surveillance
- Both humans and Deep Learning perform with similar levels of accuracy
Face Recognition

- 15% of the market
- Surveillance
- Both humans and Deep Learning perform with similar levels of accuracy
- Very important! The registration starts by presenting photo-ID
The registration is done by the banker
The registration is done by the banker

How good are we at identifying strangers by photo ID?
The registration is done by the banker

How good are we at identifying strangers by photo ID?
We are not!
Face Recognition - Man Versus Machine

- The registration is done by the banker
- How good are we at identifying strangers by photo ID? **We are not!**
- Error rates (Human): 20%-30%

The registration is done by the banker

How good are we at identifying strangers by photo ID?
We are not!

Error rates (Human): 20%-30%

Error rates (Deep Learning): 4%
Face Recognition - Man Versus Machine

- The registration is done by the banker
- How good are we at identifying strangers by photo ID? We are not!
- Error rates (Human): 20%-30%
- Error rates (Deep Learning): 4%
- Deep Learning is the future of facial recognition of banking
The registration is done by the banker

How good are we at identifying strangers by photo ID?  
We are not!

Error rates (Human): 20%-30%

Error rates (Deep Learning): 4%

Deep Learning is the future of facial recognition of banking

Attacks: printed images, Deep Learning
Fingerprint

- 31% of the market
Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
- 3 levels of feature extraction
Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
- 3 levels of feature extraction
- Birthday Paradox

Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
- 3 levels of feature extraction
- Birthday Paradox
- Classes of fingerprint (Henry-Galton Classification System)

Source: American Academy of Hand Analysis
Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
- 3 levels of feature extraction
- Birthday Paradox
- Classes of fingerprint (Henry-Galton Classification System)
- Attacks
Fingerprint

- 31% of the market
- AFIS (The Automated Fingerprint Identification System) is Everywhere: Forensic (FBI), Government (Aadhaar), Homeland-Security (US-VISIT)
- 3 levels of feature extraction
- Birthday Paradox
- Classes of fingerprint (Henry-Galton Classification System)
- Attacks
- Deterrent Effect
Fingerprint - Attacks

- Change the class of the fingerprint
Fingerprint - Attacks

- Change the class of the fingerprint
- Gelatin
Fingerprint - Attacks

- Change the class of the fingerprint
- Gelatin
- Latent fingerprint + Adhesive tape
Fingerprint - Attacks

- Change the class of the fingerprint
- Gelatin
- Latent fingerprint + Adhesive tape
- White Glue

Source: www.sciencedirect.com/science/article/pii/S0379073810002331
Biometric Database Law

- December 2009

Biometric Database Law

- December 2009
- Fingerprint and Faces - "Big Brother"

Biometric Database Law

- December 2009
- Fingerprint and Faces - "Big Brother"
- Iraq, Indonesia, Pakistan, Kenya and Argentina

Biometric Database Law

- December 2009
- Fingerprint and Faces - "Big Brother"
- Iraq, Indonesia, Pakistan, Kenya and Argentina
- Save your Identity

Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...

Ben Mussay, Supervised by: Prof. Orr Dunkelman

Computer Security Seminar
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship

Source: knowledge.wharton.upenn.edu/article/almost-everyone-underestimates-true-economic-power-china/
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship
- Cyber, Cyber, Cyber

Source: nocamels.com/2017/06/cyber-week-netanyahu-israel-security/
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship
- Cyber, Cyber, Cyber
- You need to believe the next government
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship
- Cyber, Cyber, Cyber
- You need to believe the next government
- Maybe the Mossad, Shin Beit will steal my identity
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship
- Cyber, Cyber, Cyber
- You need to believe the next government
- Maybe the Mossad, Shin Beit will steal my identity
- Data Leaking
Biometric Database Law - Why not?

- Prof. Eli Biham, Prof. Omer Reingold ...
- Saved only 2 identities
- Dictatorship
- Cyber, Cyber, Cyber
- You need to believe the next government
- Maybe the Mossad, Shin Beit will steal my identity
- Data Leaking
- It is not smart-ID
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
  3. Biometric systems is not accurate for all people
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
  3. Biometric systems is not accurate for all people
  4. Collusion
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency

- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.

- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
  3. Biometric systems is not accurate for all people
  4. Collusion
  5. Template reconstruction
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
  3. Biometric systems is not accurate for all people
  4. Collusion
  5. Template reconstruction
  6. Birthday Paradox
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.
- General Attacks:
  1. Biometric sampled might be planted by the police (Age of sample)
  2. Recording the samples
  3. Biometric systems is not accurate for all people
  4. Collusion
  5. Template reconstruction
  6. Birthday Paradox
- Combination with security protocols
If everybody think it’s secure, it probably isn’t

- Bugs, Blunders and Complacency
- Any protection measure that’s believed to be infallible will make its operators careless enough to break it.

General Attacks:

1. Biometric sampled might be planted by the police (Age of sample)
2. Recording the samples
3. Biometric systems is not accurate for all people
4. Collusion
5. Template reconstruction
6. Birthday Paradox

- Combination with security protocols
- Combination with human
Summary

- What is biometrics?
Summary

- What is biometrics?
- Examples of Biometric Recognition
Summary

- What is biometrics?
- Examples of Biometric Recognition
- Examples of Attacks
Summary

- What is biometrics?
- Examples of Biometric Recognition
- Examples of Attacks
- The Biometric Database Law
Summary

- What is biometrics?
- Examples of Biometric Recognition
- Examples of Attacks
- The Biometric Database Law
- Biometric is not as secure as you think!
References

- no2bio.org
- www.bayometric.com
List of Figures

- computerworld.com
- economictimes.indiatimes.com
- geektime.co.il
- blog.bcdb.com
- china-briefing.com
- signature.wacom.eu
- theconversation.com
- nytimes.com
- www.sciencedirect.com
List of Figures

- omereingold.wordpress.com
- en.wikipedia.org/wiki/Eli_Biham
- aao.org
- mantratec.com