Possible Attacks on Match-in-Database Fingerprint Authentication

...

By: Jadyn Sondrol

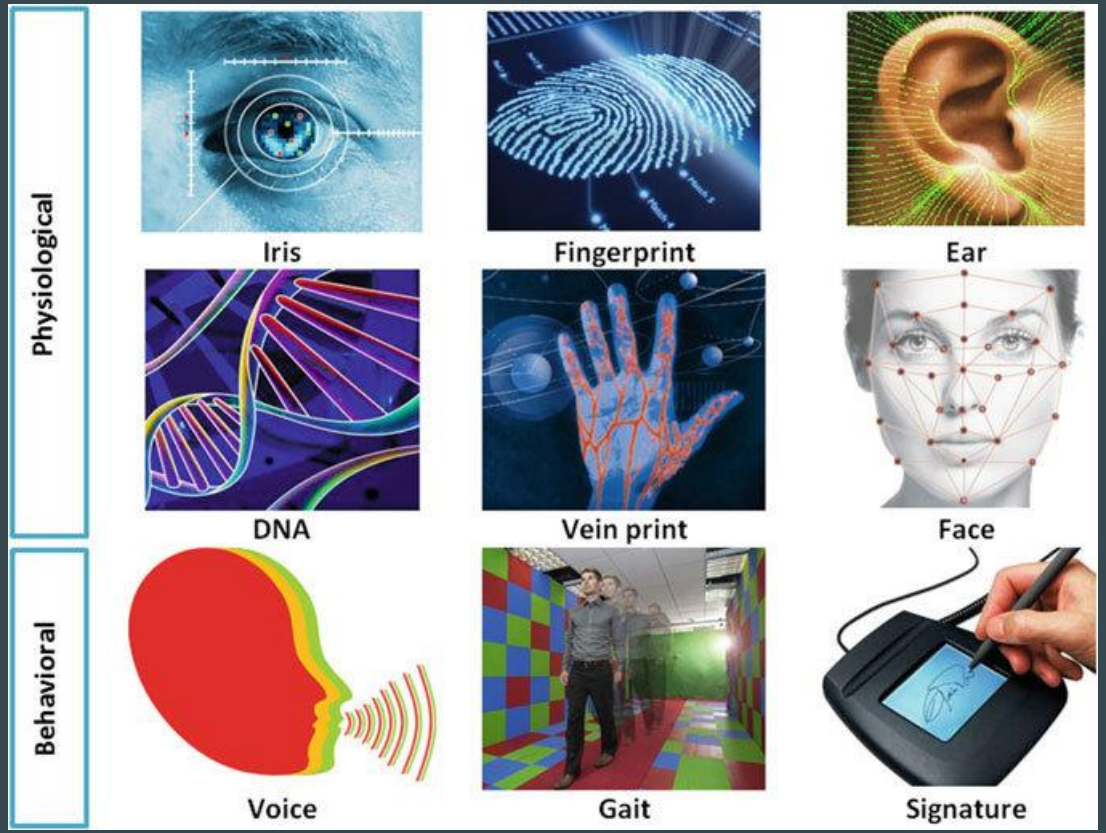
Introduction

Biometrics

Global Biometric market will exceed 70 billion by 2027

80% of Americans have used biometrics

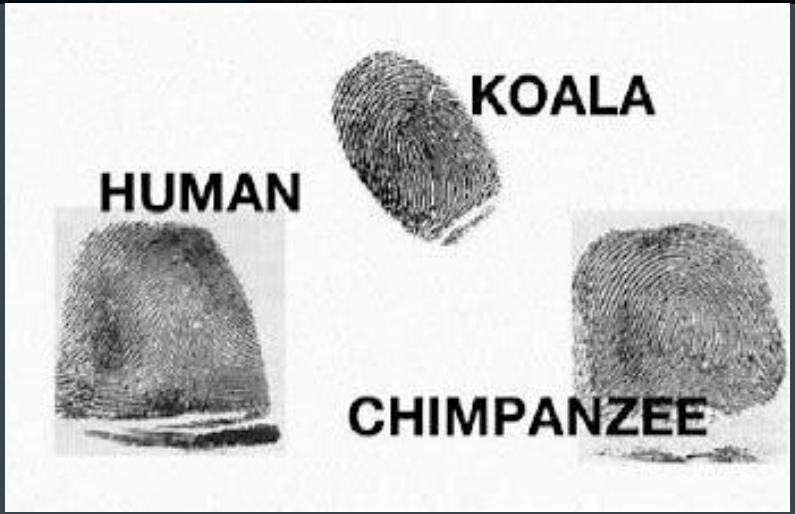
- What are they?
- Used For?
- Types?



Source: Gait Recognition (2018)

Fingerprint Fun Facts

- Unique to everyone
  - Identical twins
  - Formed from struggle in the womb
  - Friction ridges
- Loss of fingerprints
  - Gene mutation
    - 4 families
  - Bricklayers, lime workers, chemo drugs
  - Burning off
  - Will grow back
- Animals have them too
  - Apes, Chimpanzees, Koalas



Possible Attacks on Match-In-Database Fingerprint Authentication

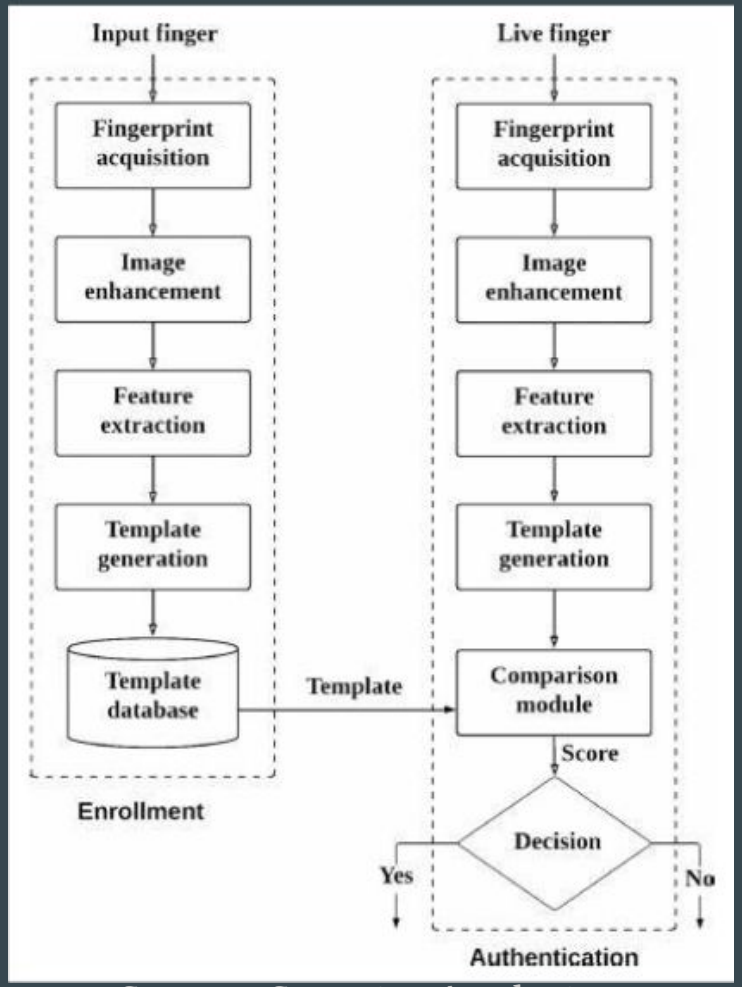
Outline

- Fingerprint Authentication
  - How it works/ modules
  - Threshold variants
- Threat Model
  - Proposed model
- Types of Attacks
  - Spoofing
  - Denial-Of-Service
  - Replay
  - Trojan Horse
- Conclusion

Source: PECB Insights (2018)

Match-in-Database Fingerprint Authentication System

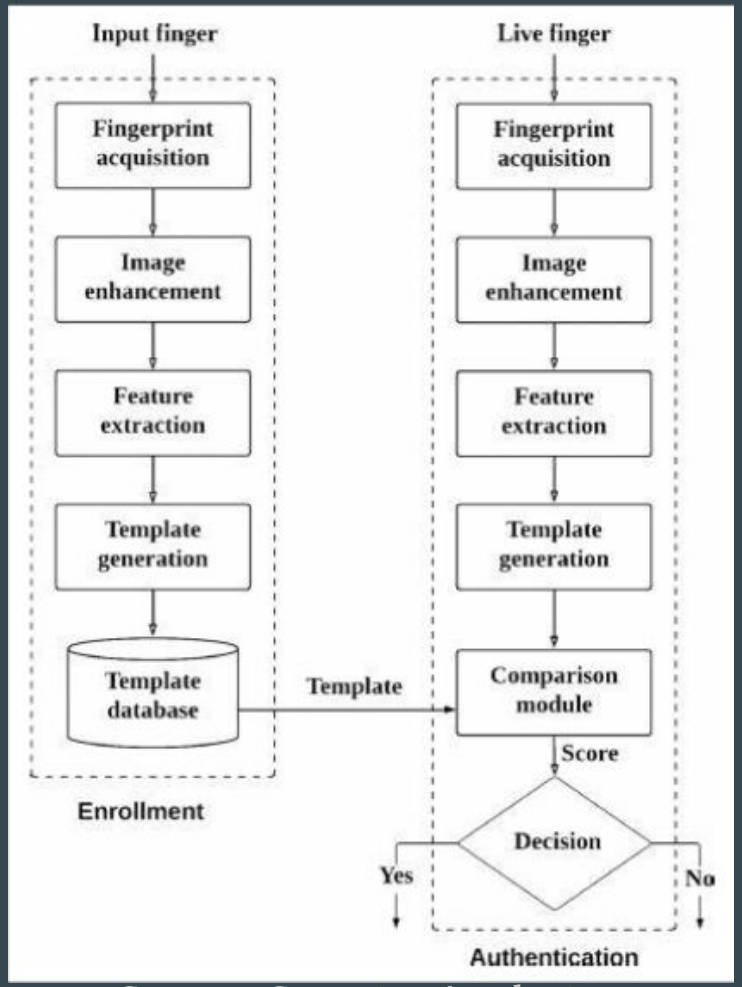
- MiD Fingerprint Authentication
  - Uses a remote database to store template
  - Template: digital representation of a fingerprint that has been encrypted
- Input Finger = Enrollment
- Live Finger = Authentication
- Verification vs. Identification
  - Fingerprint matches claimed registered user
  - Unknown identity



Source: Security Analysis

Fingerprint Acquisition/ Image Enhancement

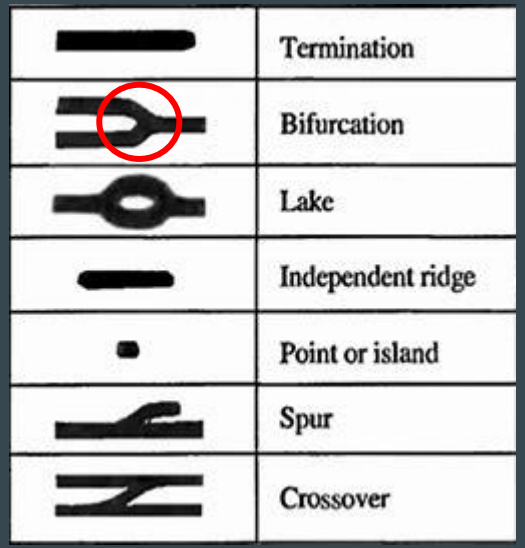
- Physical Factors
  - Sweat
  - Pressure
  - Cut
- Environmental Factors
  - Humidity
  - Temperature
  - Durability



Source: Security Analysis

Feature Extraction/ Template Generation

- Characteristic Features
  - Ridges/ Valleys
- Minutia



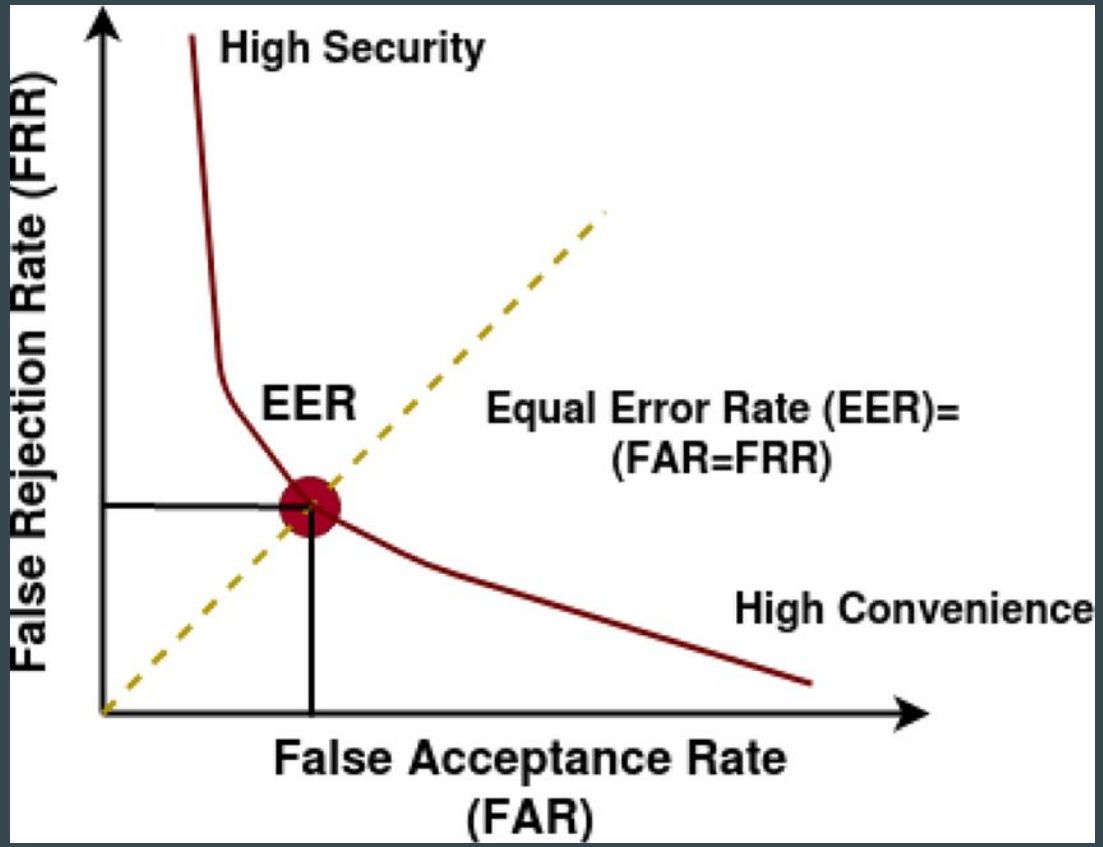
Source: Characteristic Features (2014)

Binary Strings

10001100
11001010
00110101
10011010
00110101
.
.
.
00010111

Comparison Module

- Threshold
- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
- Equal Error Rate (EER)



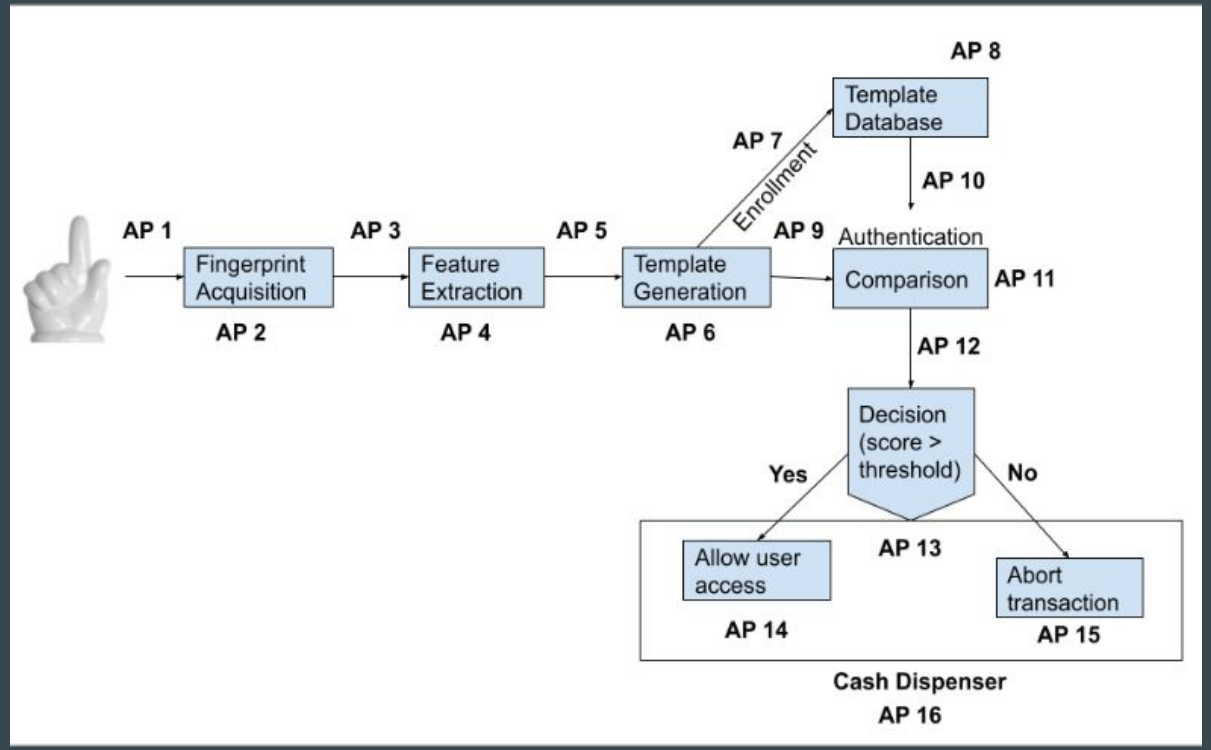
Outline

- Fingerprint Authentication
  - How it works
  - Threshold variants
- Threat Model
  - Proposed model
- Types of Attacks
  - Spoofing
  - Denial-Of-Service
  - Replay
  - Trojan Horse
- Conclusion

Source: PECB Insights (2018)

Threat Model

- Process of identifying, and prioritizing potential security threats
- Diagram the system
- Identify where threats could occur (Attack Points: 16)
- Threat Level
- Mitigation techniques



Proposed by: Security Analysis (2020)

Outline

- Fingerprint Authentication
  - How it works/ modules
  - Threshold variants
- Threat Model
  - Proposed model
- Types of Attacks
  - Spoofing
  - Denial-Of-Service
  - Replay
  - Trojan Horse
- Conclusion

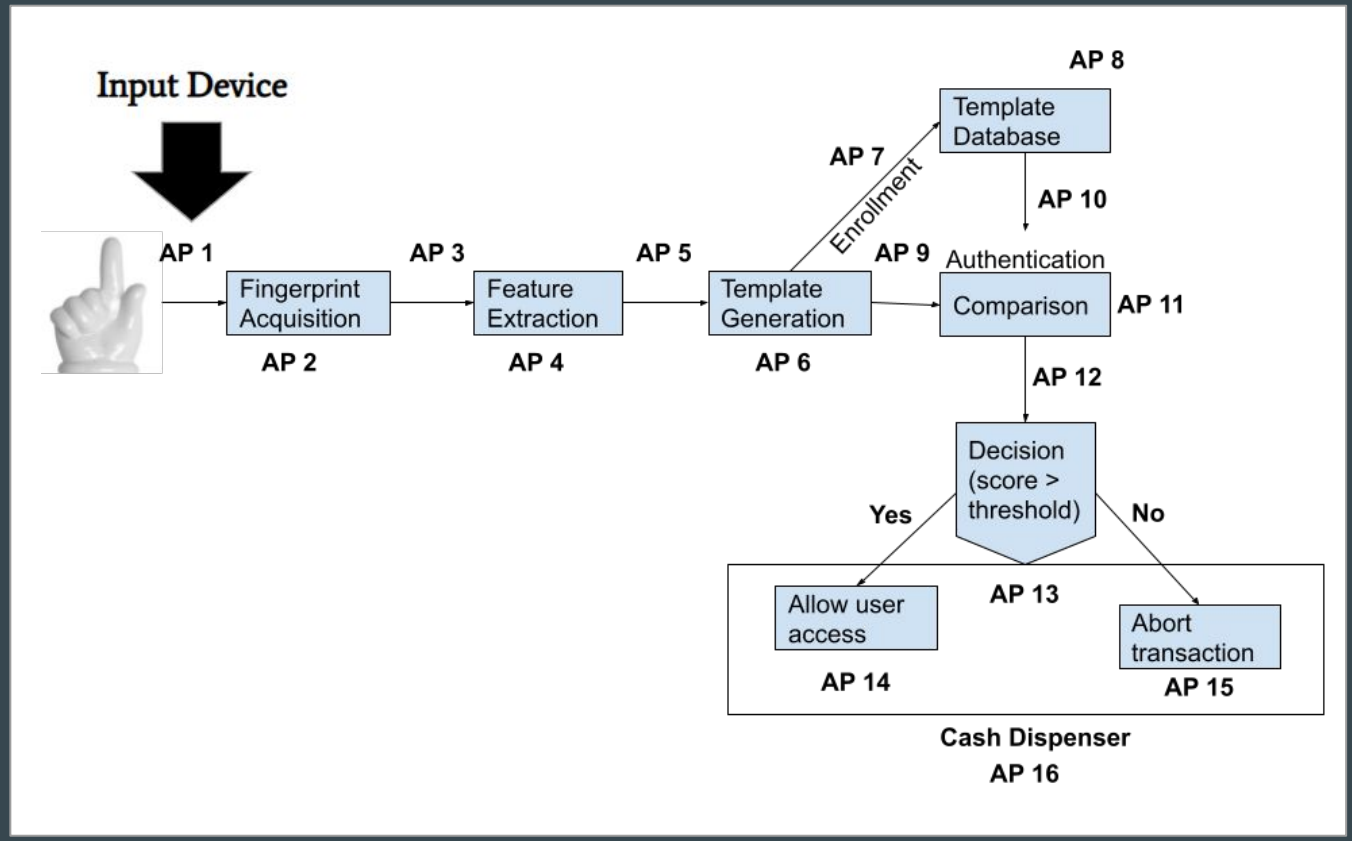
Source: PECB Insights (2018)

Types Of Attacks

- Direct: Attack to the scanner or cash dispenser itself
  - AP 1, 2, 16
- Indirect: Attack to a component within the system

Spoofing Attack

- Direct attack
- AP 1
- Provides false biometric data



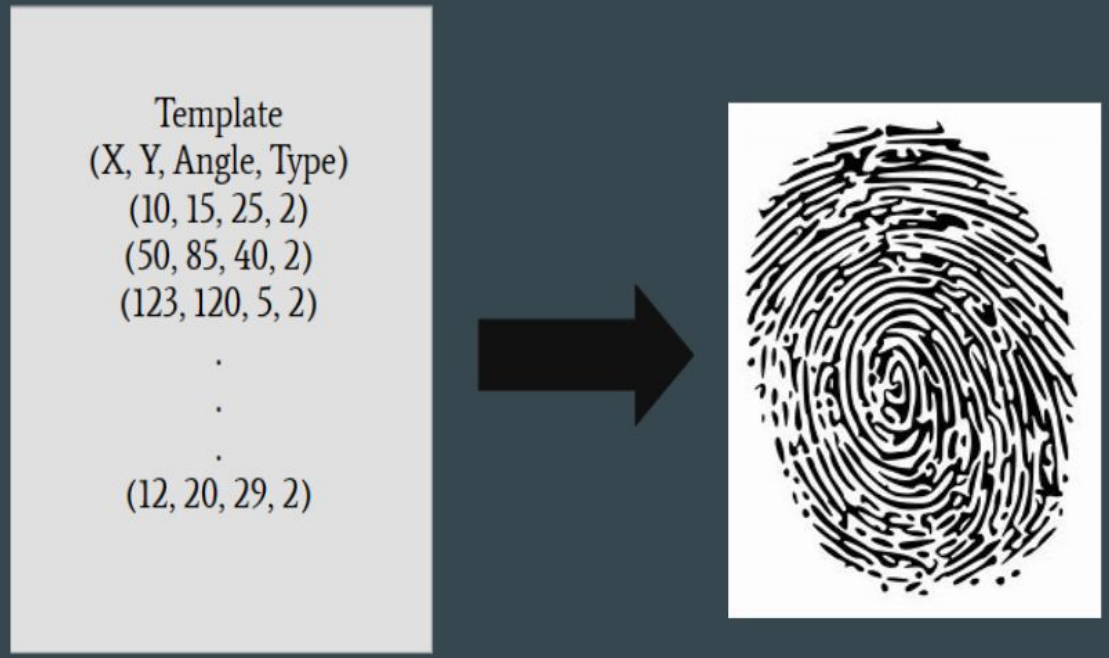
Spoofing Attack- spoofing methods

Cooperative

- ➢ Direct Mold

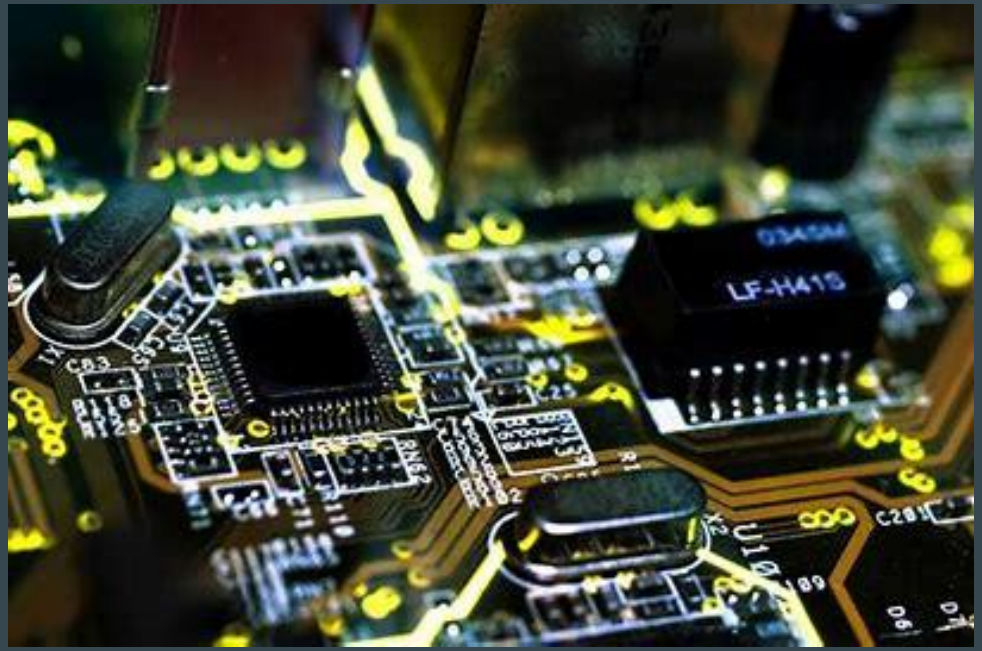
Non- Cooperative

- ❖ Latent Fingerprint
  - ➢ Invisible
  - ➢ Powder, Brush, Tape
- ❖ Fingerprint Reactivation
  - ➢ From scanner itself
  - ➢ Heavy breathing, water filled bag, graphite powder
- ❖ Cadaver
  - ➢ Enrolled user dead
- ❖ Fingerprint Synthesis
  - ➢ From template
  - ➢ Need access to database



Spoofing Attack- Anti-spoof methods -Hardware

- Costly
- Add another problem
  - Leak confidential info through patterns of electromagnetic waves
  - Power consumption



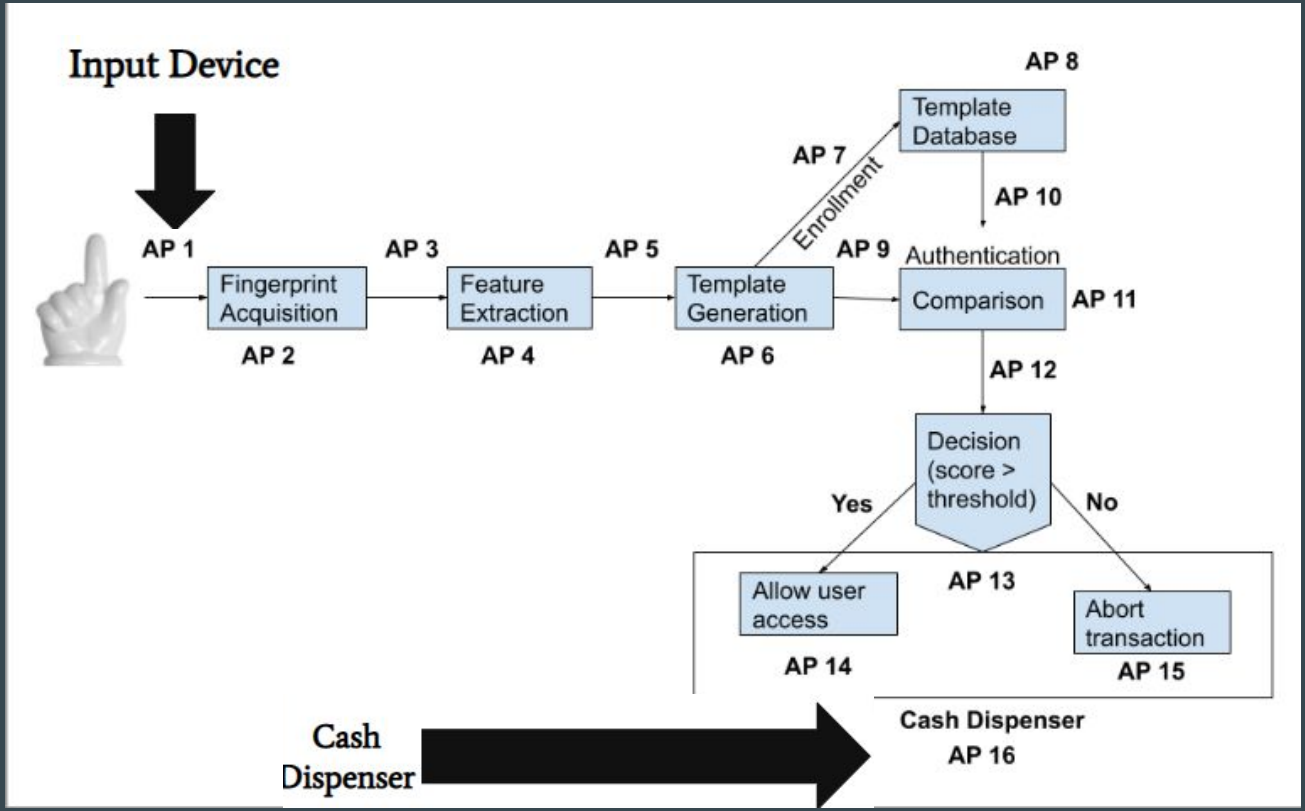
Spoofing Attack- Anti-spoof methods -Software

- Static
  - Pore-based
    - Quantity
    - Distribution
    - High resolution
  - Perspiration
    - Shading
    - Depends on pressure applied
  - Texture
    - Coarseness
    - Multi-resolution texture analysis
  - Commonly used together
- Dynamic
  - Snapshots
  - Perspiration
  - Ridge Distortion

- High Risk
  - Ease of creating fake fingerprint
  - Not implementing antispoof methods

Denial-Of-Service (DOS) Attack

- Direct
- AP 1, AP 16
- Overload the system
- Unusable for everyone

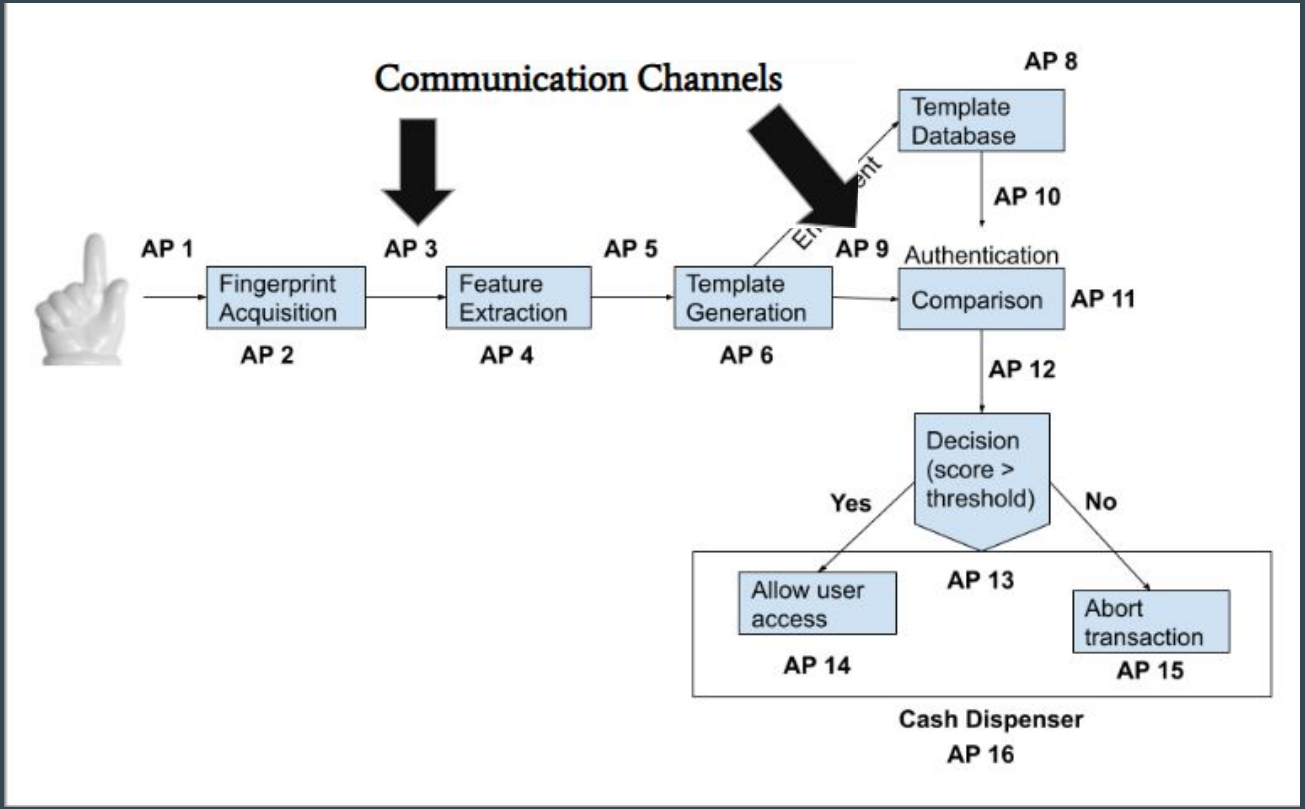


Denial-Of-Service (DOS) Attack- Mitigation

- Eye on the scanner
  - Video cameras
  - Security guards
- Rugged devices
  - Created to withstand unusual circumstances
- Low threat
  - No info
  - Annoyance

Replay Attack

- Indirect attack
- AP 3, AP 9
- Eavesdrops on the communication channels
- Intercepts
- Resends previous user input

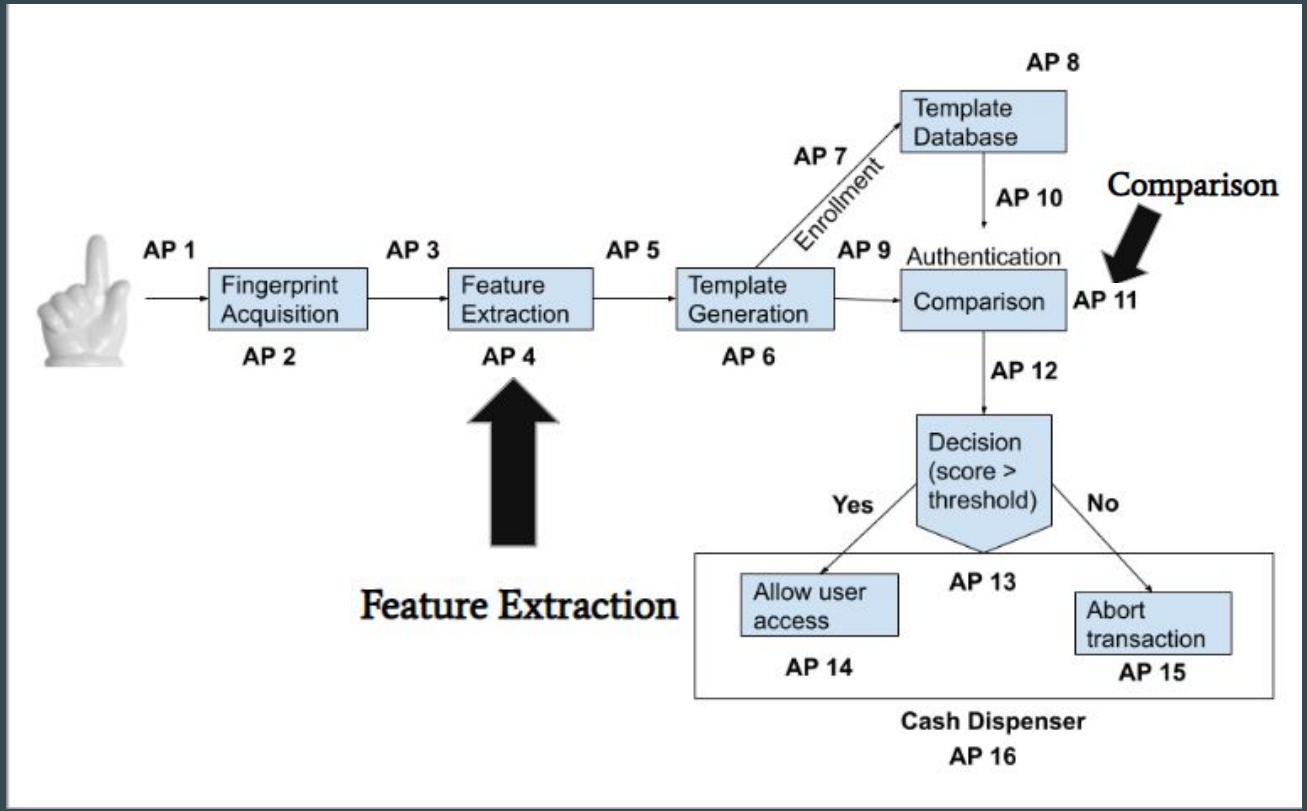


Replay Attack- Mitigation

- Challenge/Response method
  - Query system
  - Transaction server
    - Different pixel value sent every time
    - Scanner and Feature Extraction
    - Have to match
- Global Clock
  - Timestamps
- Liveliness Test
  - Active = swipe
  - Passive
    - Texture, pore distribution, ridge distortion
- Medium Threat Level
  - Challenging to gain access to the channel
  - Get all the info

Trojan Horse Attack

- Indirect
- AP 4, AP 11
- Trojan embedded
- Activated
  - Modify, copy, delete



Trojan Horse- Mitigation

- Trusted Biometric System (TBS)
  - Mutual Authentication
    - Both sides of channel verify each other at the same time
  - Increase computation power & time
- Code Signing
  - Each module's digital signature
- Hardware
  - Tamper resistant
  - Communication channels
- Medium Threat Level
  - Hard to introduce Trojan
  - Easy to modify software

Conclusion

Spoofing Attack | Replay Attack | Trojan Horse Attack | DOS Attack

Increase in biometrics - Threshold

- Biometrics are increasing
- With more users
  - 0.1% FAR currently
    - 1 out of 1000
    - FBI: 6,000 out of 6 million
    - US pop: 332,000 out of 332 million

Questions?

References

Biometrics: Definition, use cases, latest news. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

Saad Bin Ahmed, Muhammad Imran Razzak, and Bandar Alhaqbani. 2016. The Minutiae Based Latent Fingerprint Recognition System. In Proceedings of the International Conference on Internet of Things and Cloud Computing (Cambridge, United Kingdom) (ICC '16). Association for Computing Machinery, New York, NY, USA, Article 49, 9 pages. https://doi.org/10.1145/2896387.2896434

Heeseung Choi, Raechoong Kang, Kyungtaek Choi, and Jaihie Kim. 2007. Aliveness Detection of Fingerprints using Multiple Static Features. World Academy of Science, Engineering and Technology 2 (01-2007).

Markus Dürmuth, David Oswald, and Niklas Pastewka. 2016. Side-Channel Attacks on Fingerprint Matching Algorithms. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (Vienna, Austria) (TrustED '16). Association for Computing Machinery, New York, NY, USA, 3–13.
https://doi.org/10.1145/2995289.2995294

Mahesh Joshi, Bodhisatwa Mazumdar, and Somnath Dey. 2020. comprehensive security analysis of match-in-database fingerprint biometric system. Pattern Recognition Letters 138 (2020), 247–266. https://doi.org/10.1016/j.patrec.2020.07.024

K. K. H. Karunathilake, A. R. M. Shahan, M. N. M. Shamry, M. W. D. S. De Silva, Amila Senarathne, and Kanishka Yapa. 2021. A steganography-based fingerprint authentication mechanism to counter fake physical biometrics and trojan horse attacks. In 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) . 0286–0292. https://doi.org/10.1109/IEMCON53756.2021.9623240

Ram Prakash Sharma and Somnath Dey. 2019. Fingerprint Liveness Detection Using Local Quality Features. Vis. Comput. 35, 10 (oct 2019), 1393–1410. https://doi.org/10.1007/s00371-018-01618-x

Wioletta Wójtowicz. 2014. A Fingerprint-Based Digital Images Watermarking for Identity Authentication. Annales UMCS, Informatica 14 (10 2014).
https://doi.org/10.2478/umcsinfo-2014-0008