Authentication II

CSE 565: Fall 2024
Computer Security

Xiangyu Guo (xiangyug@buffalo.edu)

University at Buffalo

Announcement

- Please sign-up at course Piazza.
- Reminder of Quiz 0 (**Due tonight 23:59**).
  - You must obtain full score of the Quiz.
- HW1 & Proj 1 due in 7 days (**09/25, 23:59**)

Review of last lecture

- Overview of Authentication techniques
  - Authentication does not establish secure channel!
- **Password-based authentication**
  - Attack surface
  - Attack & Defense on the user side: Strong passwords; Phishing
  - Attack & Defense on the Remote system: Dictionary attack; Salting; Slow password hashing.
  - Attack & Defense in the Transmission: One-time password.

Today's Topic

- Token-based authentication
  - Application of Challenge-response protocol
- Biometric-based authentication
- Some examples of attacks

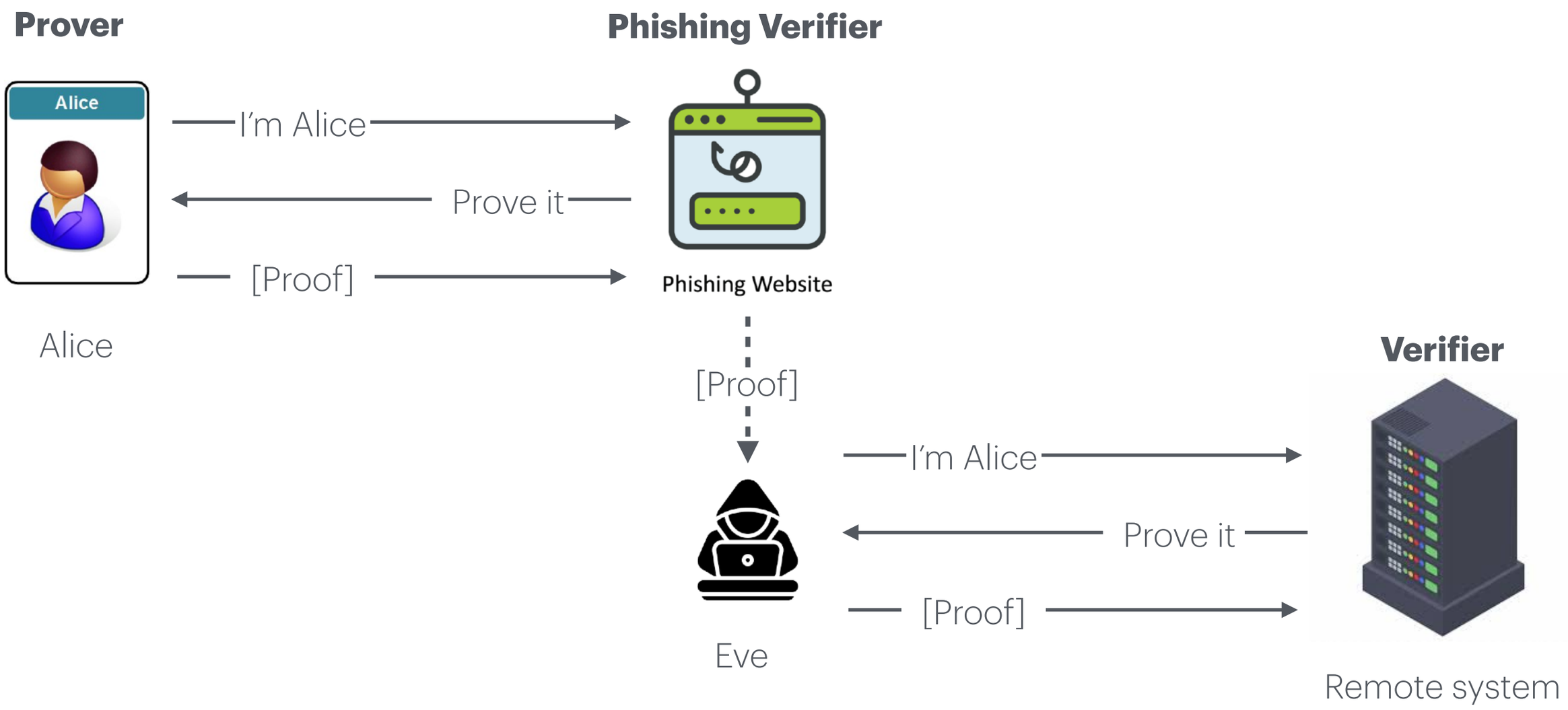
Recall: One-Time Passwords

- Each password is used only once for authentication
  - Establishing shared secret at user registration time
  - Hash-based One-Time Passwords (HOTP)
    - Alice & Remote System maintain a synchronized counter
    - Send MAC of the counter as OTP.
  - Time-based One-Time Passwords (TOTP)
    - Send MAC of the current time as OTP.
  - S/keys
    - Based on one-wayness of iterative hashing
    - No secret stored on remote system
- Often used in Token-based authentication

Challenge-Response Protocol

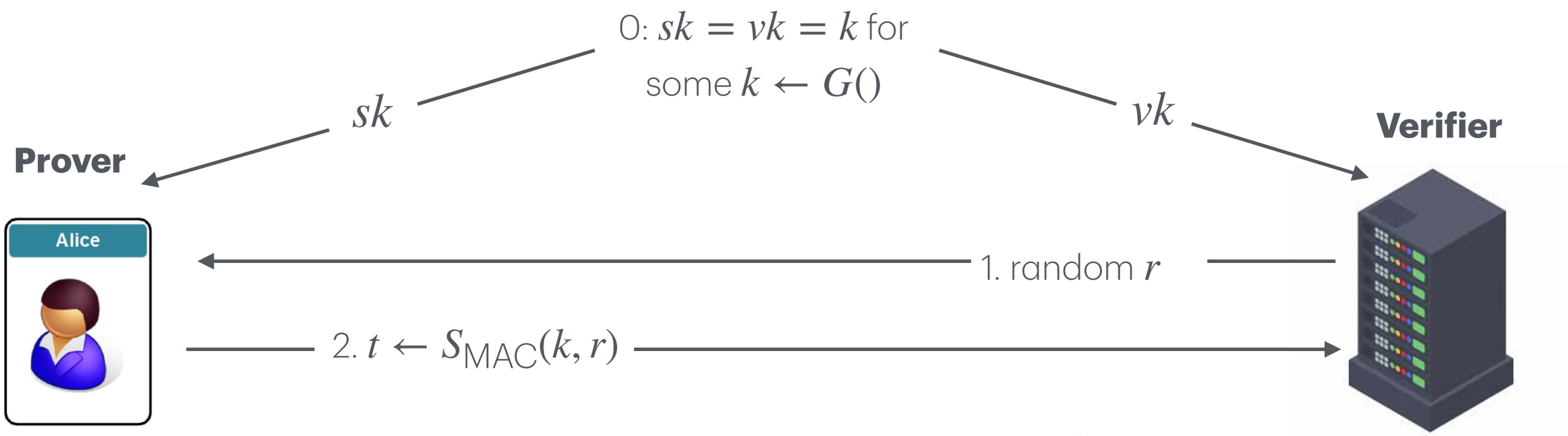
- Defend against phishing (but *not* MiTM)
- Like OTP, needs establishing some secret at user registration time
- No counter / time needed.
- No info of secret stored on the remote server (no SPoF)

Active (Offline) Attack



- **Offline** fake ATM:
  - interacts with user; *later* tries to impersonate user to real ATM
- **Offline** phishing:
  - phishing site interacts with user; *later* authenticates to real site

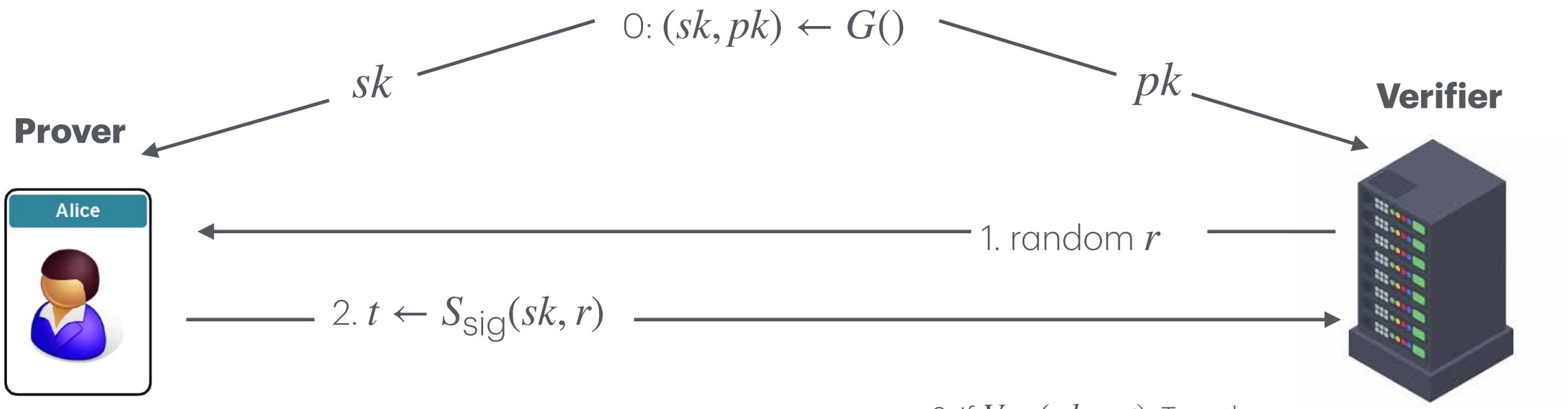
Challenge-response protocols



- $(S_{\text{MAC}}, V_{\text{MAC}})$: a secure MAC.
- Insecure if vk is leaked

Challenge-response protocols

Signed version



- $(S_{\text{sig}}, V_{\text{sig}})$: a secure digital signature
- Secure against an active attacker even if pk is leaked.
  - What about Man-in-The-Middle?

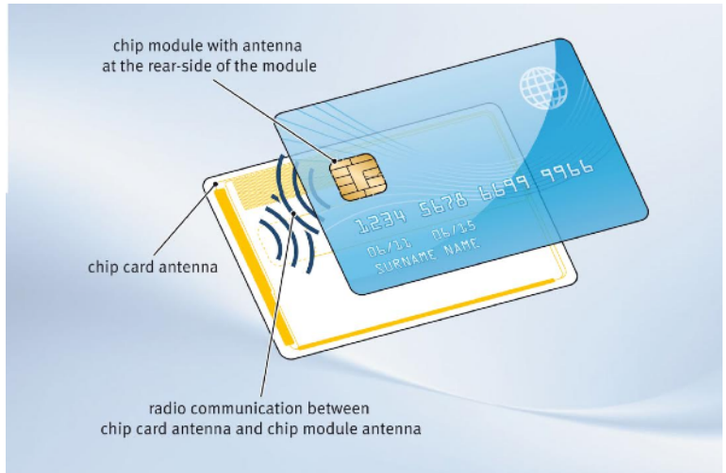
Token-based Authentication

“Something You Have”

- Something only Alice should have
  - Examples: key, smartcard, RFID badge, SecurID token
  - Frequently used as a second factor (in combination with a password)
- 2FA token
  - Technically, only proves possession of the token, not that it’s really Alice
- Tokens get shared, lost, stolen, duplicated

Smartcards

- Idea: Put a (fixed) secret key into a tiny computer that Alice can carry with her
  - Plastic card with an embedded integrated circuit
  - Provisioned with secret keys
  - Interacts with readers through contact pads or short range wireless (NFC)
- Many uses beyond user authentication
  - Stored value payment and transit
  - SIM cards
  - Satellite TV
- Typical authentication protocol: (signed) **Challenge-response**.

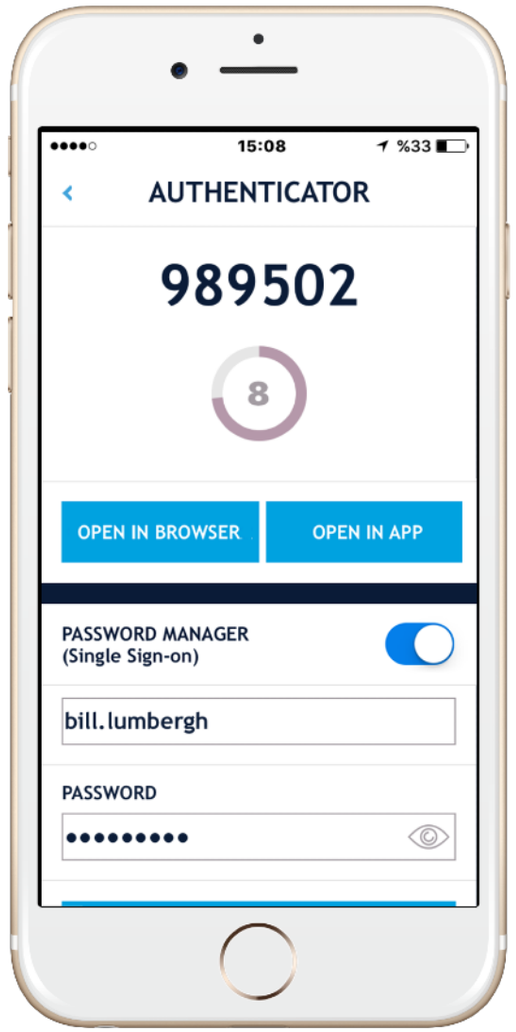


One-Time Password Tokens

- Same basic idea as a smart card: a tiny computer with a secret
  - Typically without a direct computer interface
  - Typically using **Time-based OTP**.
    - OTP is displayed on token screen, user types it into the authentication system.
    - No comm b/w the token & remote server
    - Same weakness: MiTM, Phishing, SPoF
- Some also supports Challenge-response

One-Time Passcode without Tokens

- Virtual edition
  - Everybody (in some parts of the world) already carries a tiny computer. Let's just use that.
  - Strength: better scaling, support
  - Multiple keys with the same physical device.
  - Weakness: the two authentication factors are not as isolated anymore.

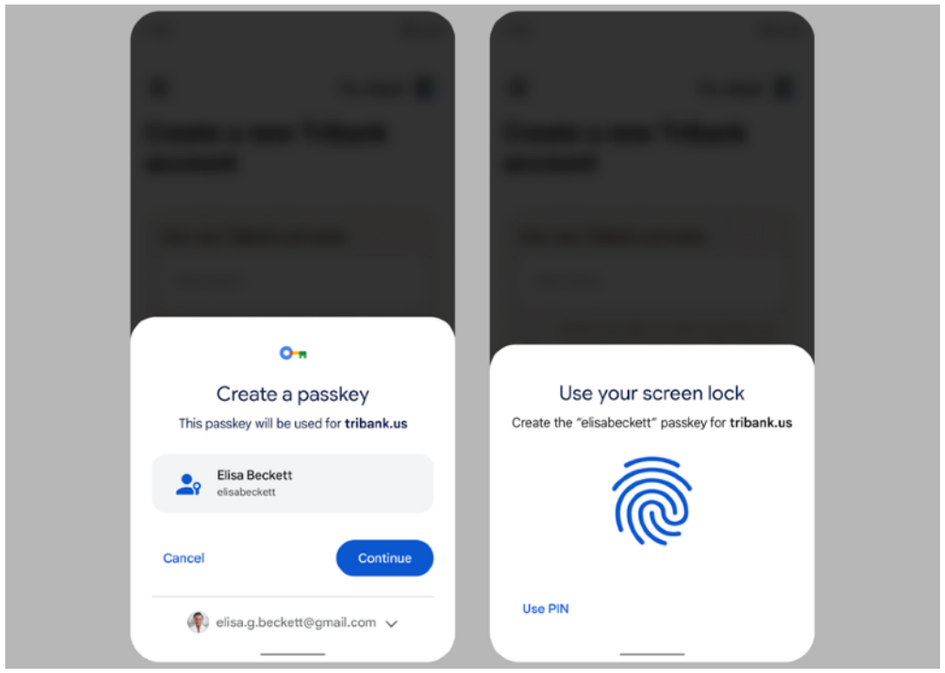


One-Time Passcode without Tokens

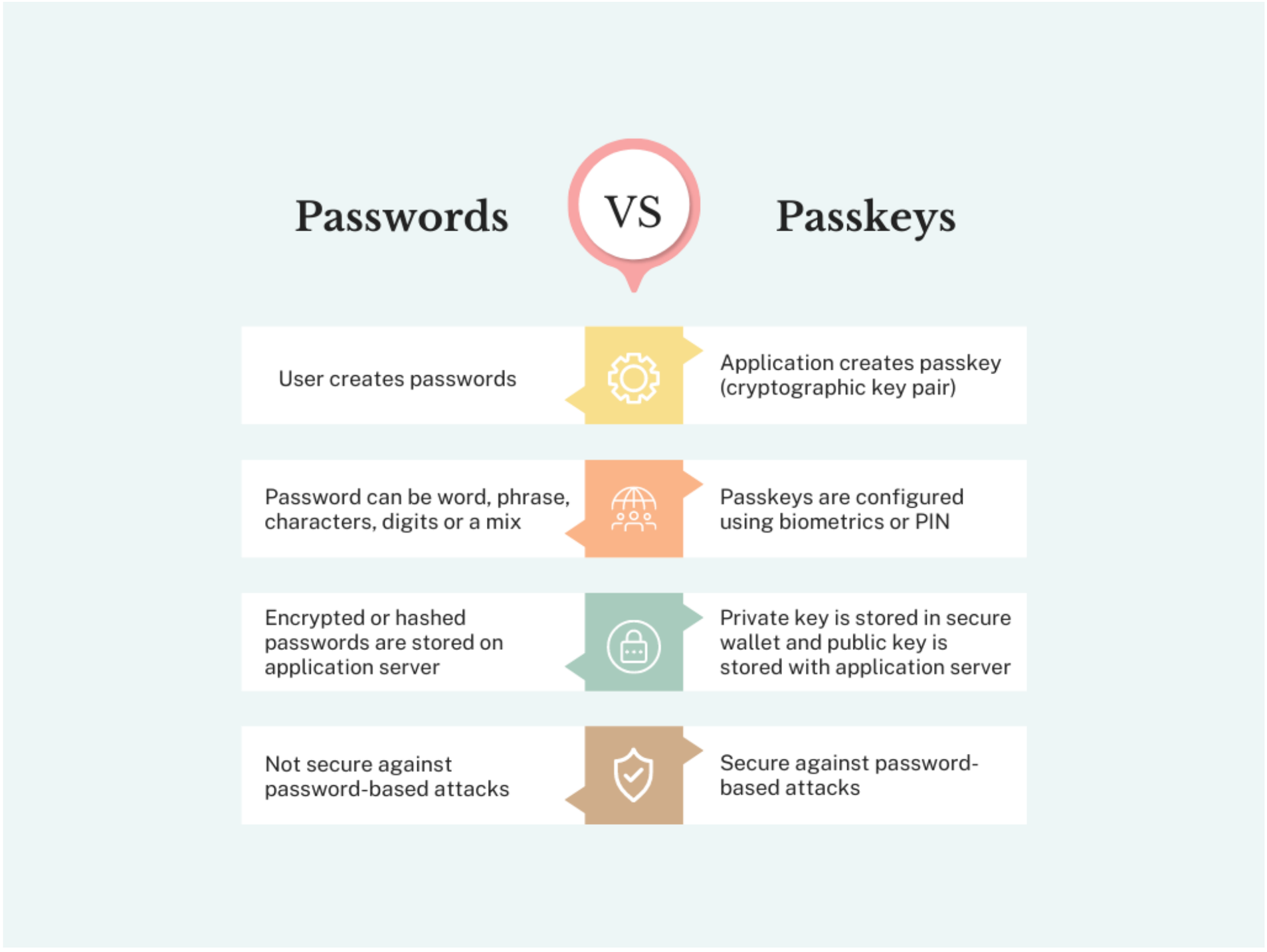
- Extending the idea of using (possession of) your phone as an authentication factor.
- Authenticating server can send Alice a one-time code via SMS.
    - Alice logs in with her password and received code.
- Often used for step-up authentication or account recovery.
    - Step-up authentication: *secondary* (stronger) authentication mechanism invoked based on risk level
        - Examples: When attempting to access *more sensitive* resources, or when behavior patterns do not match routine.
    - Similar solutions use email instead of SMS.
        - Proof that Alice has access to the email account she registered with.
- Widespread use, but weaker against range of threat models (SMS not very secure)

Example: Passkey

- Essentially implementing the signed Challenge-Response Protocol
- **Creation**
  - Local authentication (e.g. password & biometrics)
    - Info for local auth *never leave user device*.
  - Generate (Pub-key, Priv-key) pair.
  - Pub-key sent to the remote sys. Priv-key stored on user device.
- **Verification**
  - Online service sends random challenge
  - User device sends signed response



Example: Passkey



Example: Yubikey

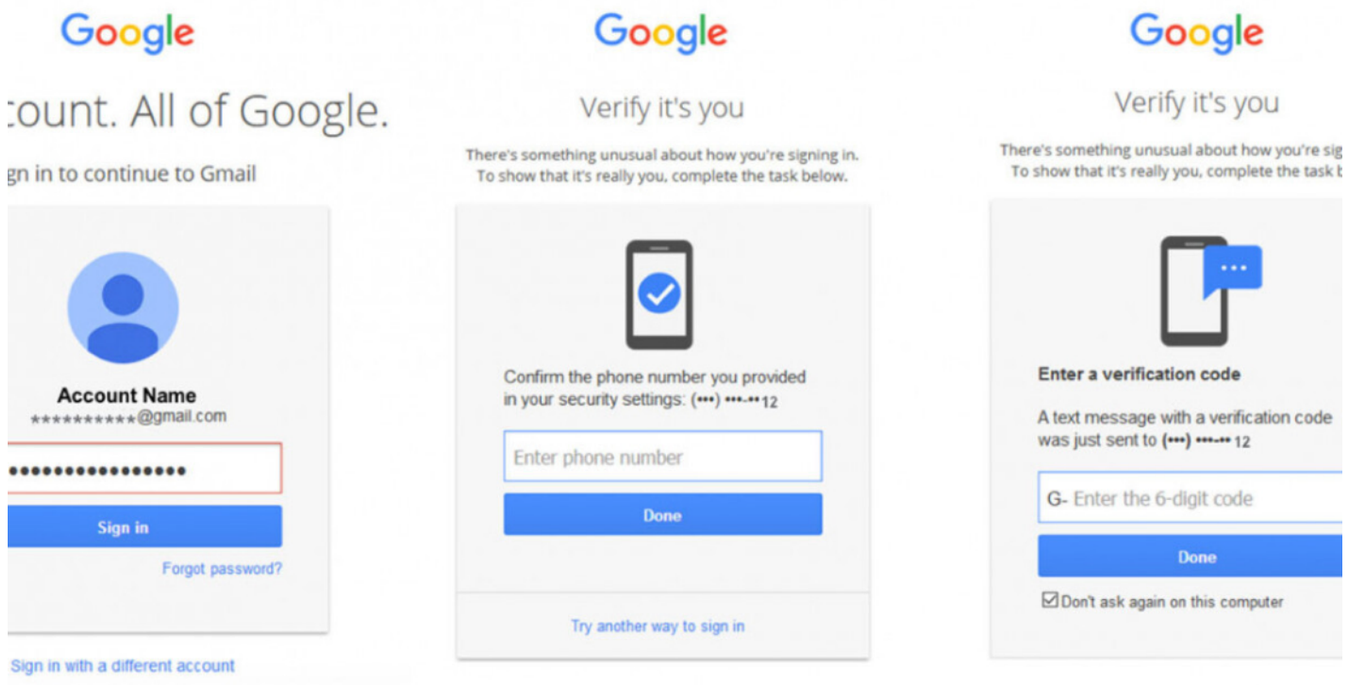
- Like Smartcards, but
  - Usually supports multiple protocols.
  - Most commonly used to generate OTPs.
    - Can be used to register with different remote service. Secret key is dynamically generated rather than built-in.
  - Physically more durable.
- Isolated from vulnerable operating systems and apps.
- Some even supports biometric auth.

Example: Yubikey

	YubiKey passkey	Standard passkey
Storage	Device-bound in the YubiKey's hardware, making them impossible to copy.	Stored on cloud services and within each associated device's TPM (Trusted Platform Module), a dedicated component for protecting authentication secrets.
Portability	Tied to the physical device, supporting possession-based 2FA by requiring the key's presence.	Can be synced across trusted devices, offering more convenience but potentially increasing the attack surface.
Security	Designed with hardware-level protection against extraction or duplication.	Rely on the security of the device or cloud service provider.

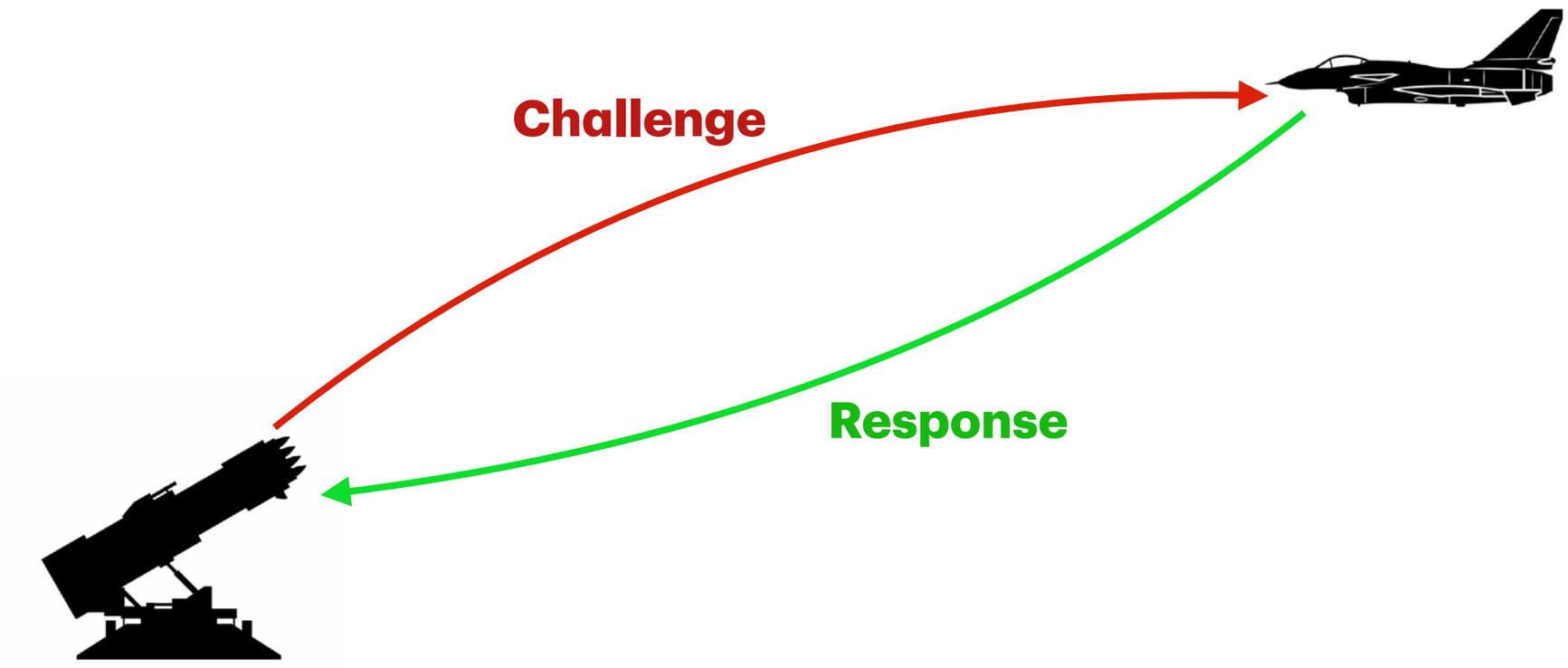
Attack: Bypassing 2FA

- Phishing attacks against SMS-based 2FA
  - Attacker creates phishing website
  - The fake website forwards user's input (password & SMS code) to real login page.



Attack: MIG-in-the-Middle

- **Identification of Friend or Foe (IFF) system**
  - Necessary in nowadays warfare
  - Mostly based on challenge-response



Attack: MIG-in-the-Middle

- **Identification of Friends or Foes (IFF) system**

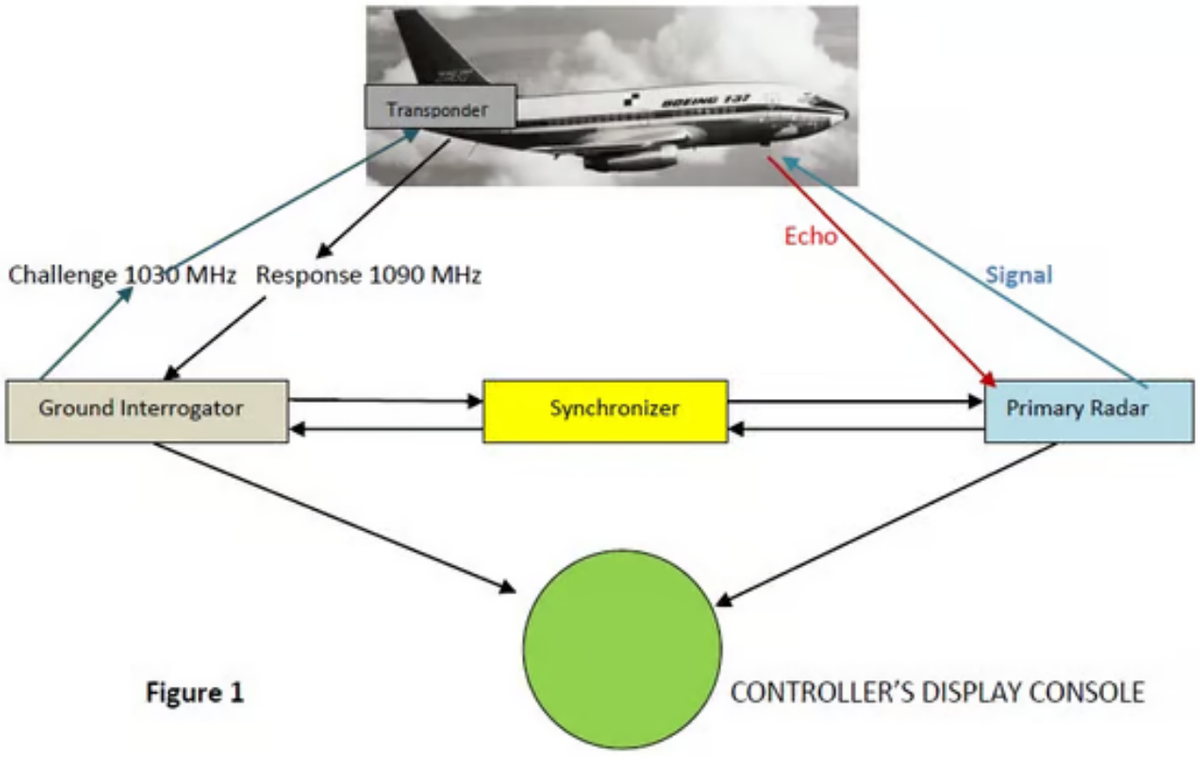
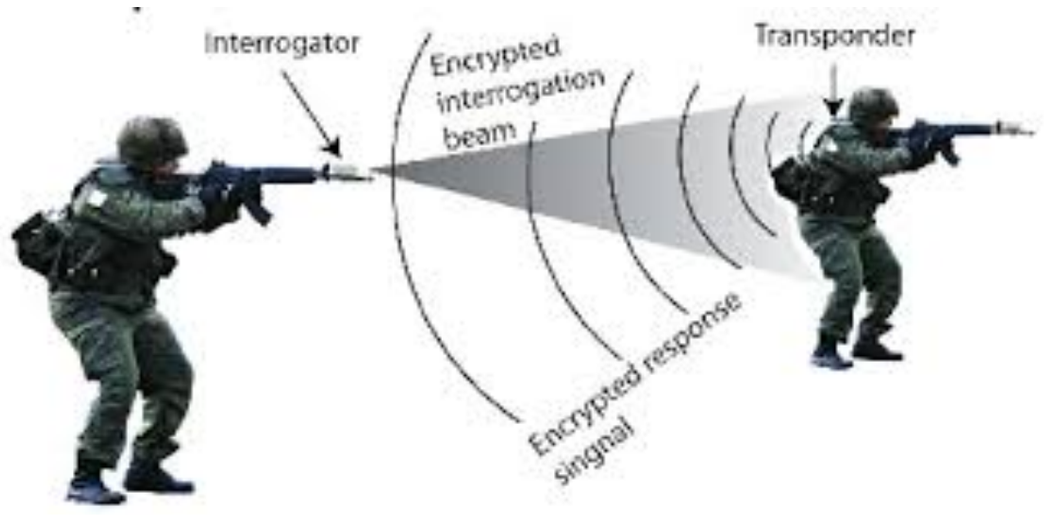


Figure 1



Attack: MIG-in-the-Middle

- **Background: South African Border War a.k.a. the Namibian War of Independence**

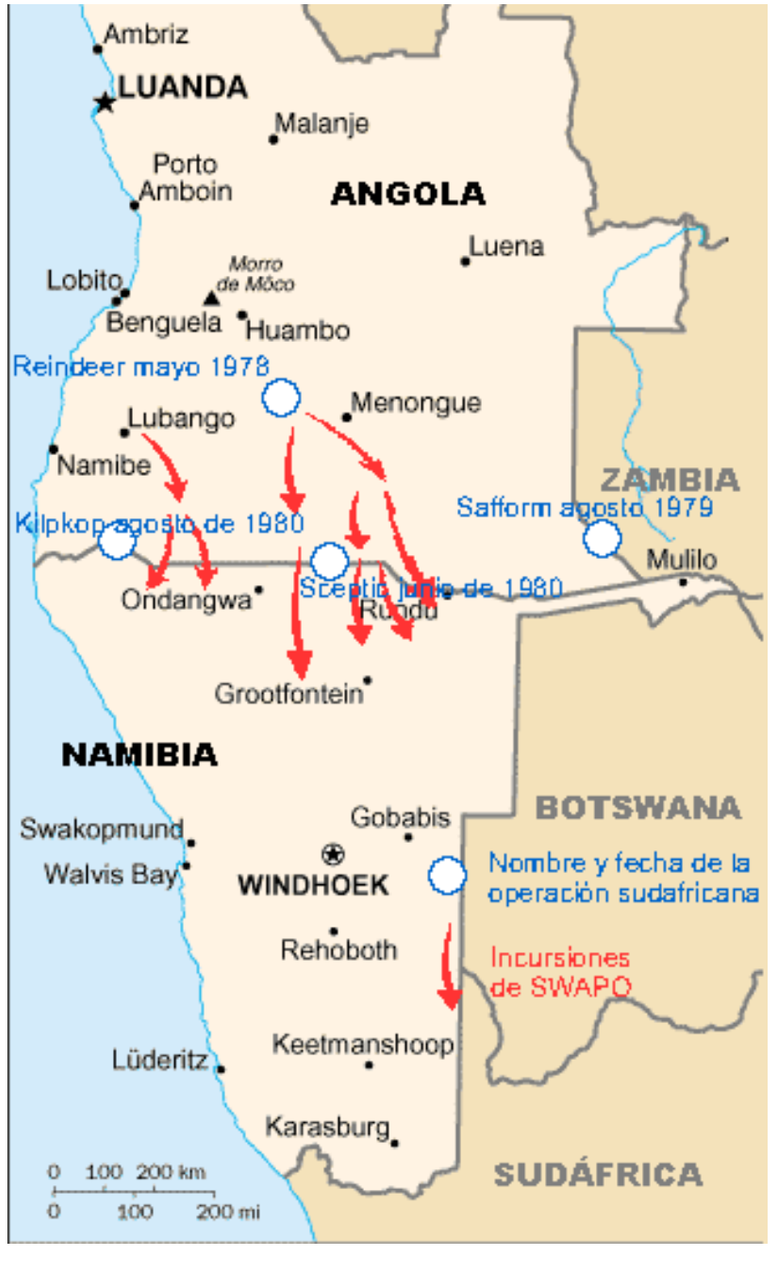
  - Late 1980's, South African troops were fighting a war in northern Namibia and southern Angola.

  - Their goals were to keep Namibia under white rule, and impose a client government (UNITA) on Angola.

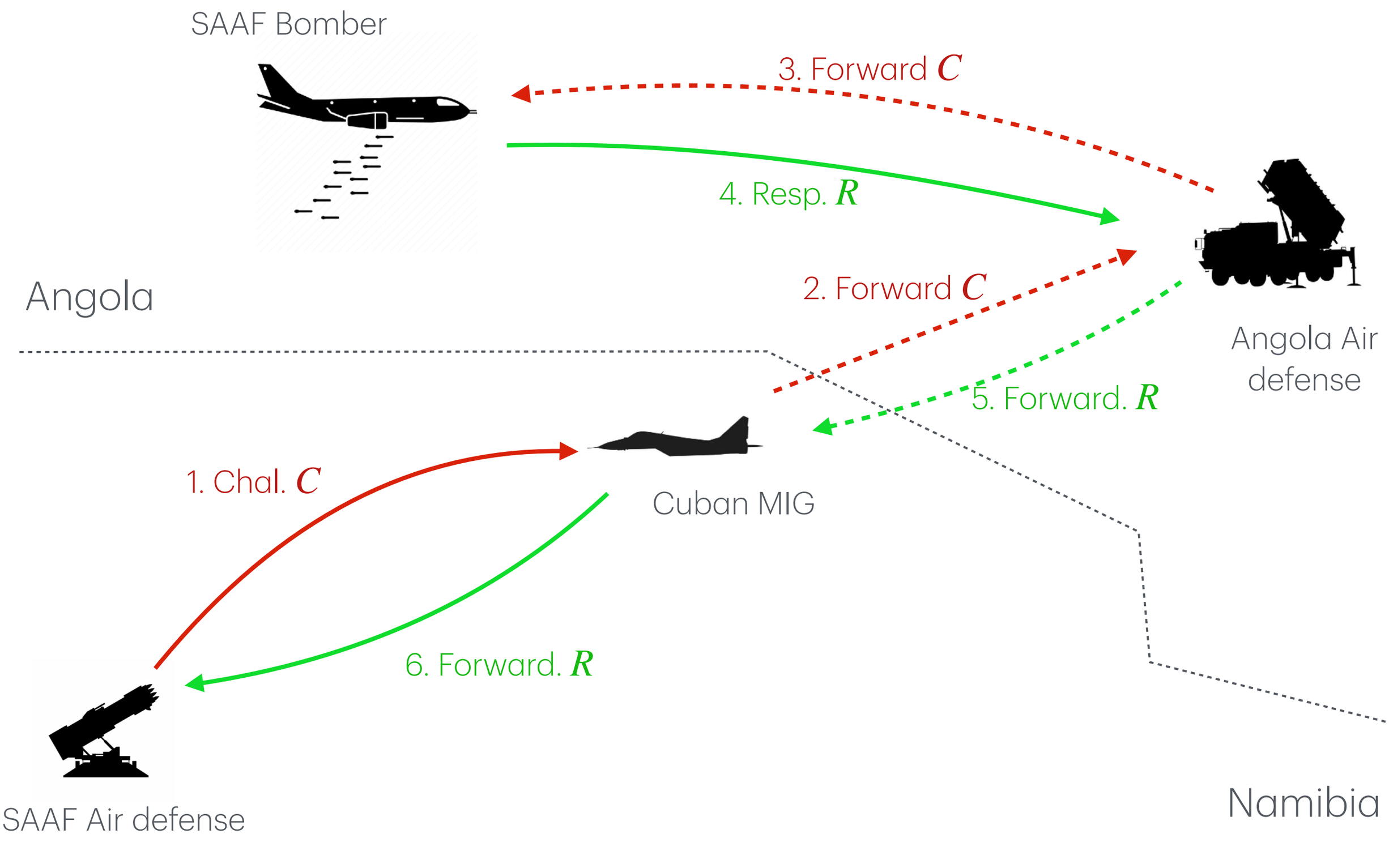
  - Most South African soldiers remained in Namibia on policing duties while the fighting to the north was done by UNITA.

Attack: MIG-in-the-Middle

- South African Air Force (SAAF)'s role
  - Supporting ground operation in Angola, and
    - Provide air defense for SA troops in Namibia
- But one day several Cuban MIG flew *openly* through SAAF's air defense system and bombed the SA ground troop in Namibia.
  - SAAF's IFF was fooled.



Attack: MIG-in-the-Middle



Biometric-based Authentication

“Something You Are”

- Unique identifying characteristic that only Alice has (biometrics)
  - Physical feature: fingerprint, iris print
  - Behavioral characteristic: handwriting, typing
  - Combination thereof: voice, gait
- How do you know that I am the same person that was here last week?
  - Did I provide a password?
  - Did I provide a badge?
- Pretty much all trust boils down to biometric authentication of one human by another.

Biometrics

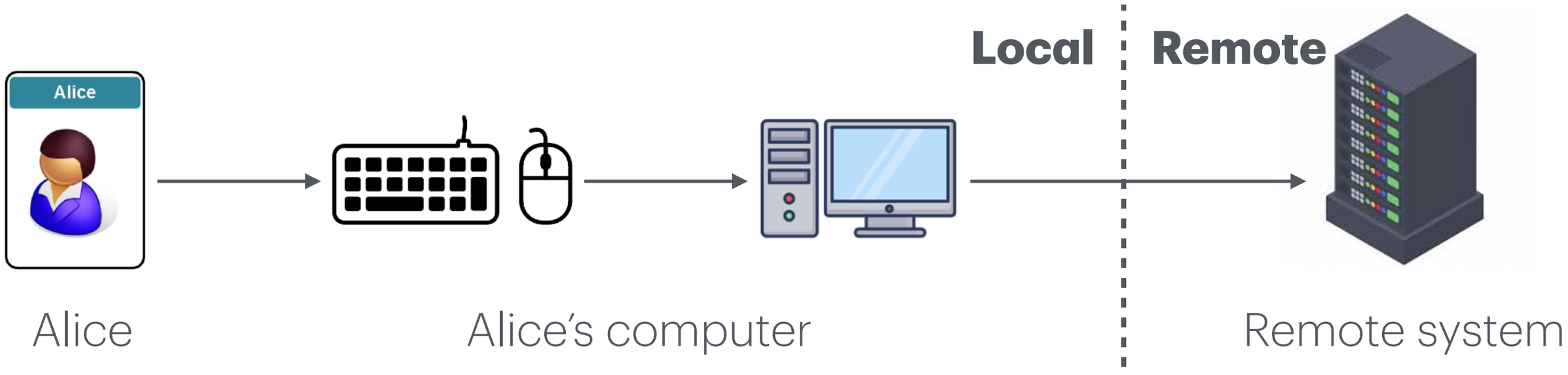
- The only authentication factor that is not designed to be transferable
  - Clear separation of authentication and authorization
  - Nothing to remember, nothing to carry around
- Can be very strong differentiator
  - Unique-ish

Biometrics

- Fingerprint
- Handprint
- Retina
- Iris
- Face recognition
- Vein
    - Vascular pattern in back of hand
- Voiceprint
- Signature
- Typing
    - Timing between character sequences
- Gait recognition
- Heartbeat
- DNA

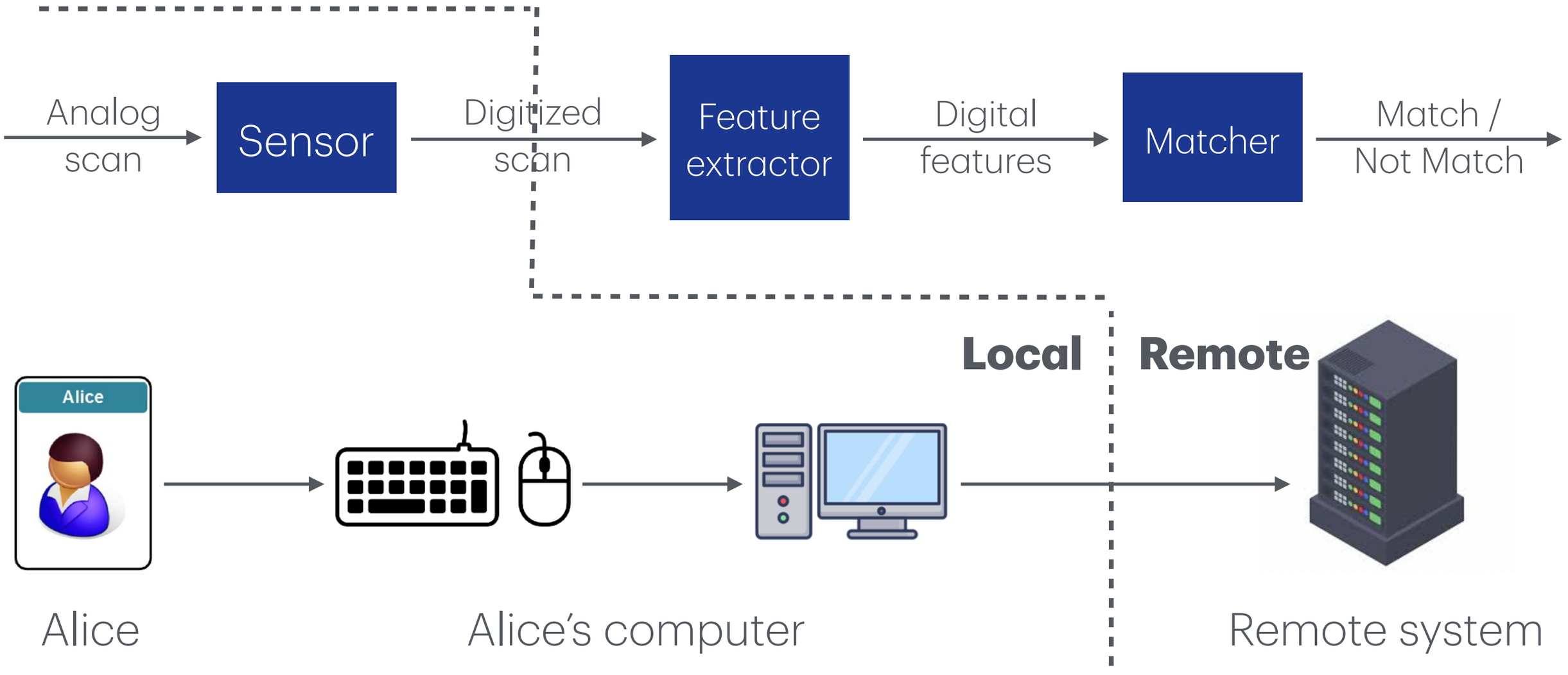
Biometrics Authentication Flow

- Q: Where does each stage happen in the authentication?
- Q: What does the remote system actually get?



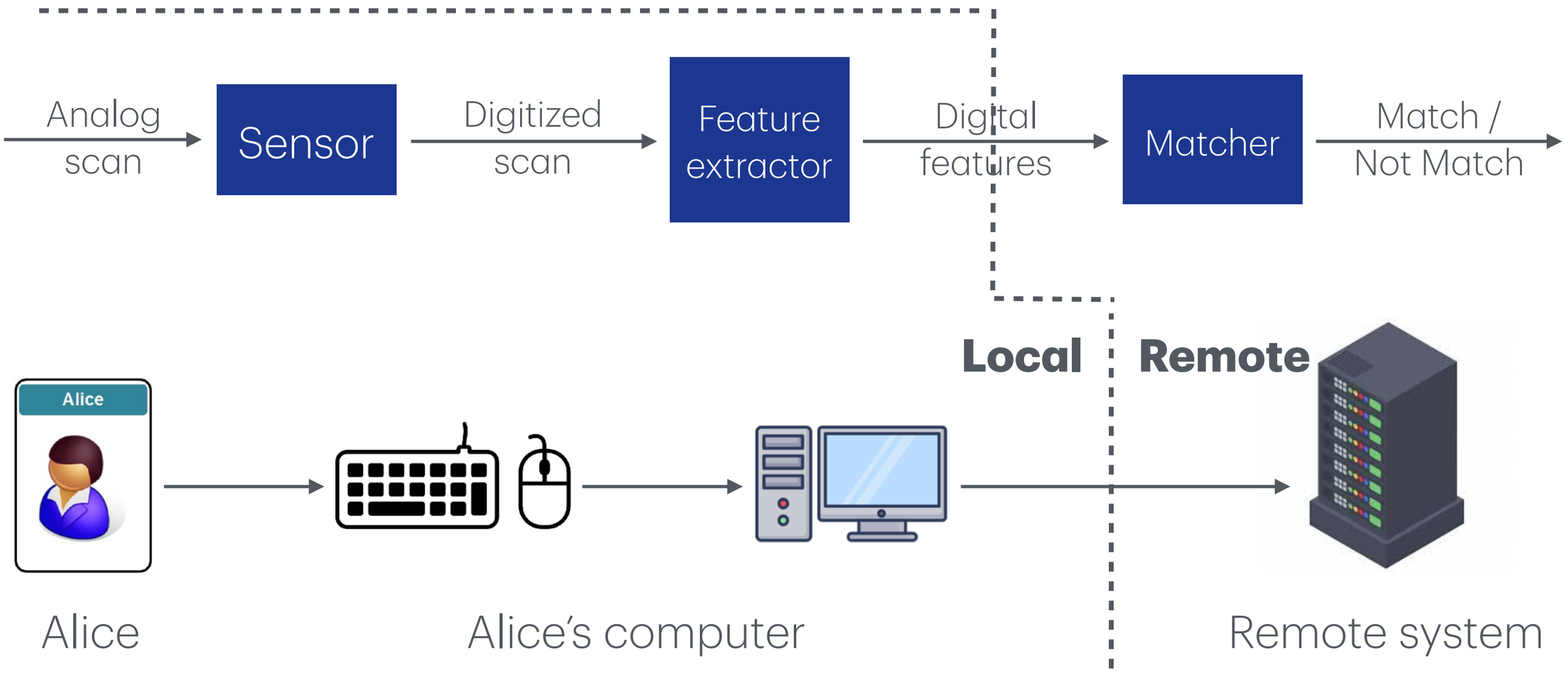
Biometrics Authentication Flow

- Scenario A: : Only the sensor is local to user.
  - Remote system has to trust Alice's computer to provide sensor data.
  - All biometric features data are on a central server.



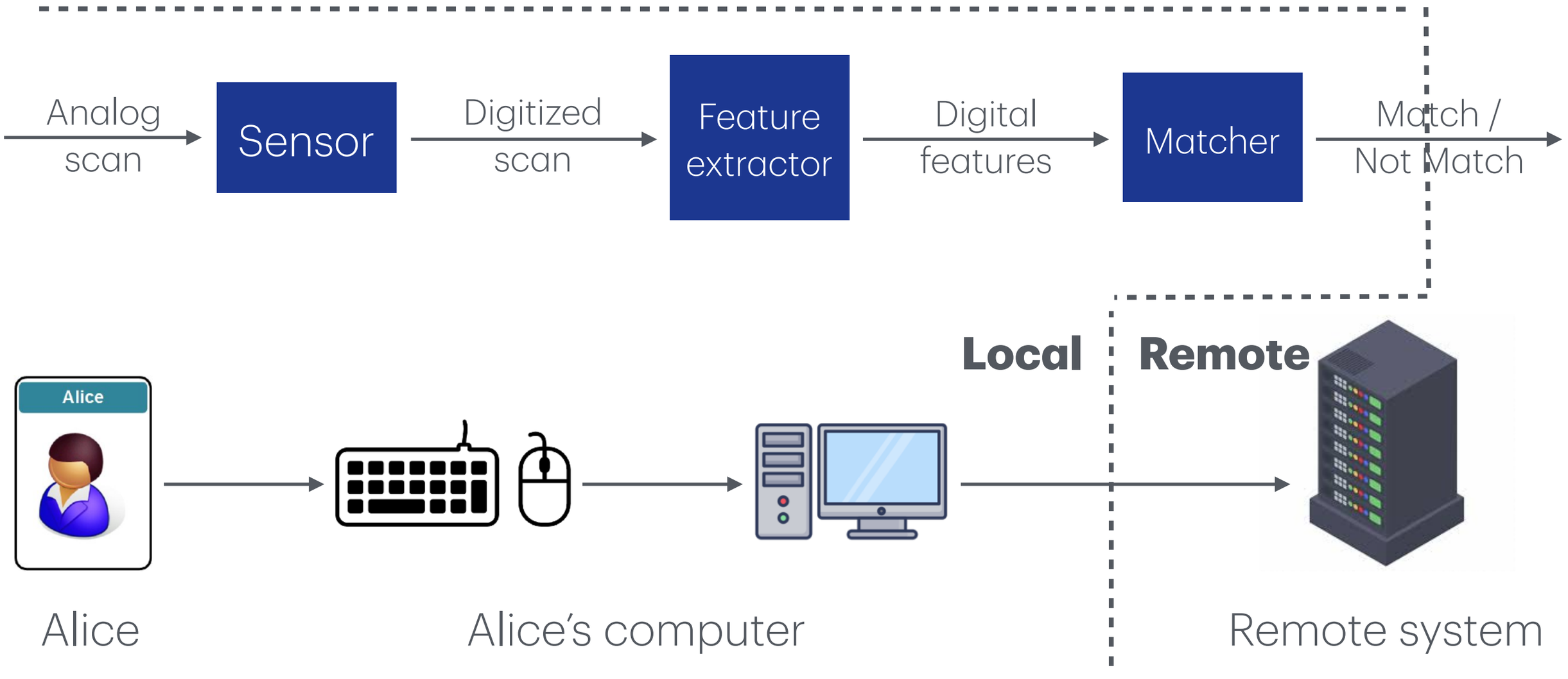
Biometrics Authentication Flow

- Scenario B: : Sensor and feature extractor are local to user.
  - Remote system has to trust Alice's computer to provide authentic data.
  - All biometric features data are still on a central server.



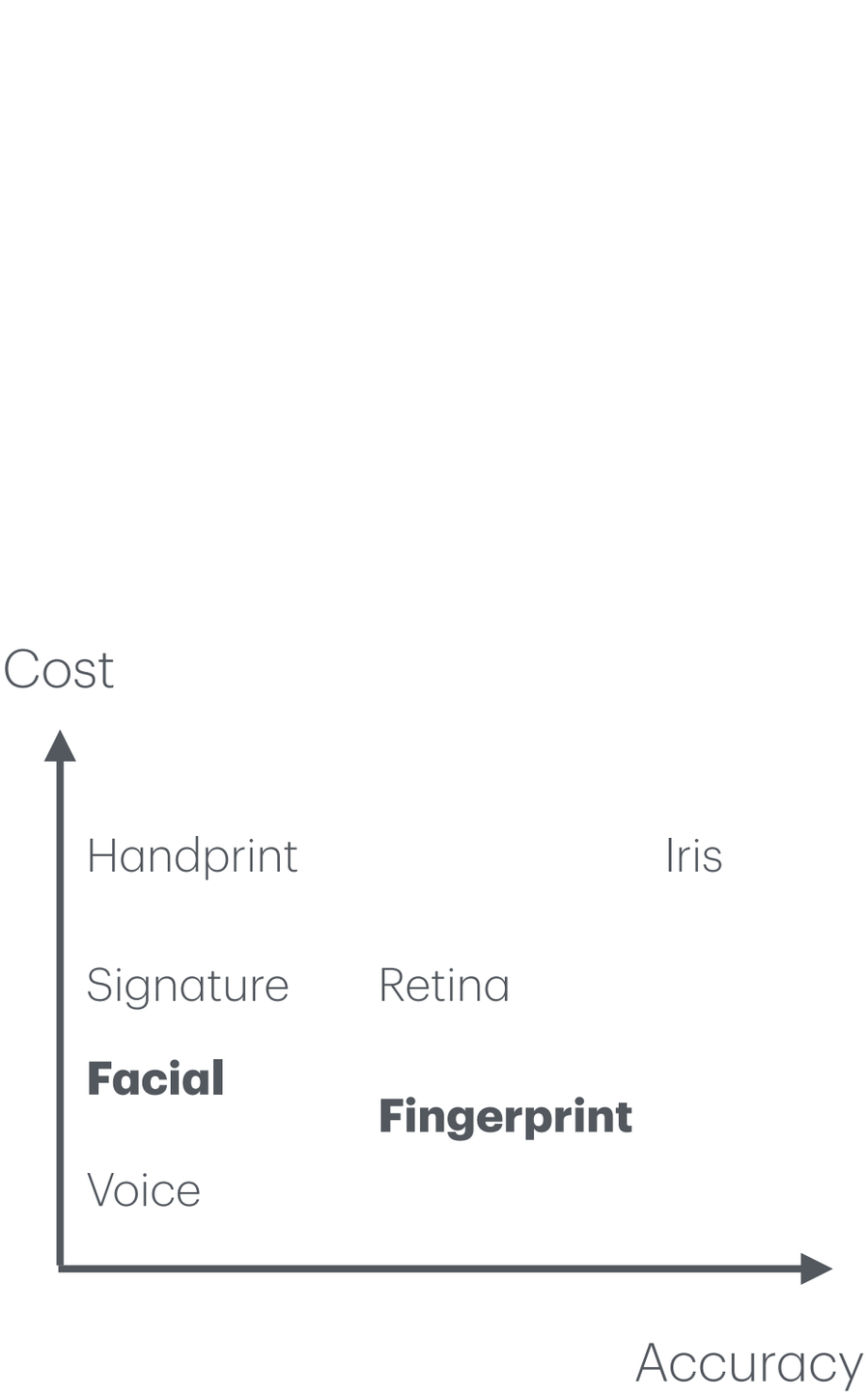
Biometrics Authentication Flow

- Scenario C: : Sensor, feature extractor, and matcher are all local to user.
  - Remote system has to trust Alice's computer to provide authentication.
  - All biometric features data are isolated on the user's device.



Biometrics usage

- Use in distributed systems requires biometric scanner to be trusted and to have secure channel (authenticity, privacy, integrity, no replay) to the server.
- Challenges
  - Accuracy
  - Ease of use (particularly enrollment)
  - User acceptance
  - Feature stability



Enrollment issue

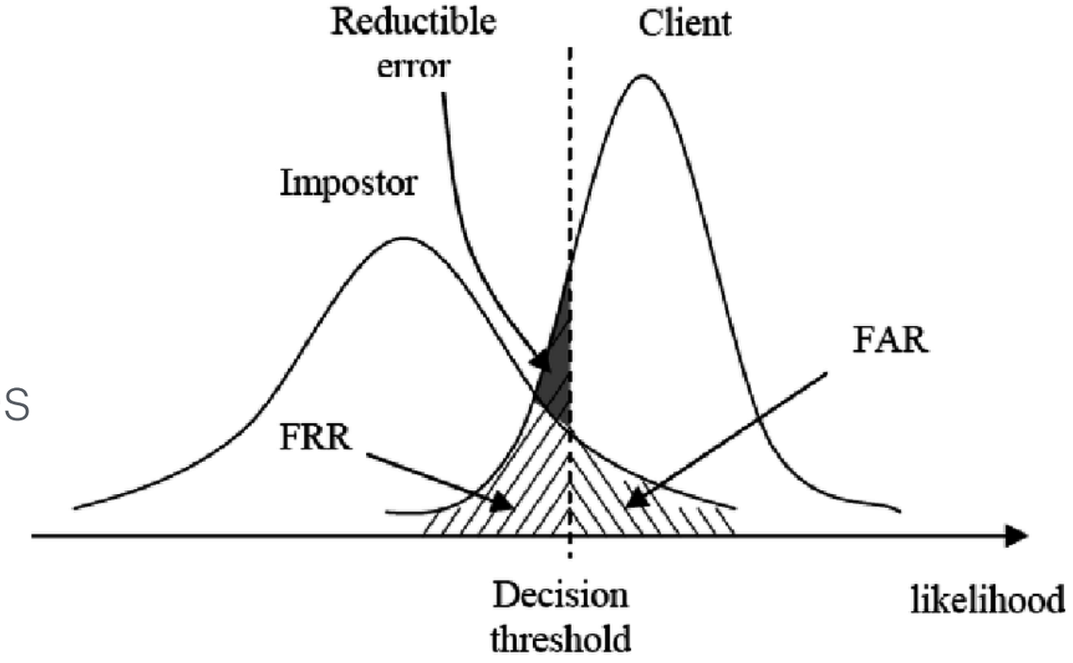
- Unlike passwords, hard to pre-enroll user
- Users must be enrolled interactively
- For many biometrics, getting good accuracy requires multiple readings
  - Build templates and test against registration
  - Repeat
  - Some templates simply tough (e.g. smooth fingerprint)
  - “Goats”: Subjects who have consistently low match scores against themselves.

How strong is a biometric?

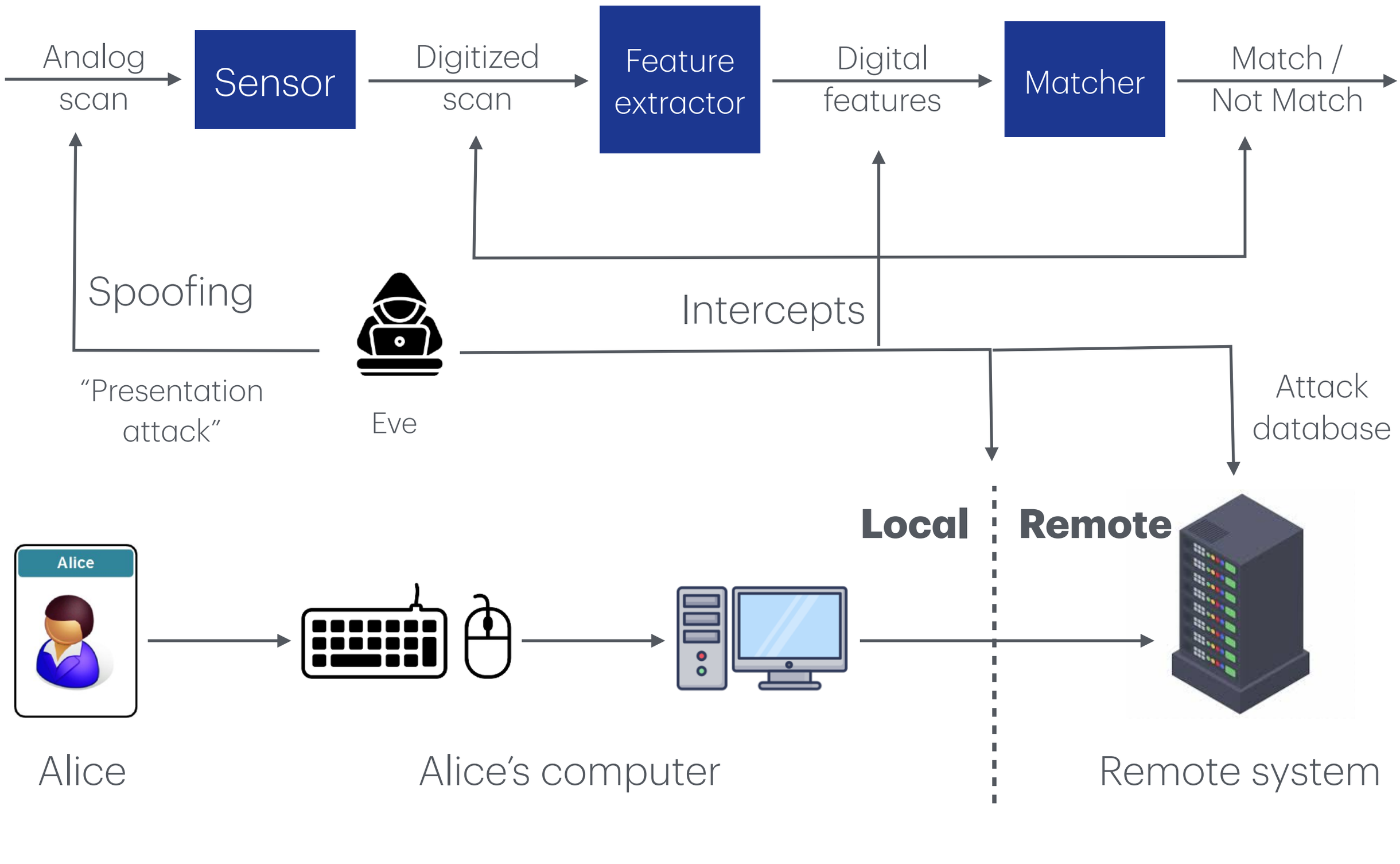
- Non-adversarial
  - False accept rate
  - False reject rate
- Adversarial
  - Intercept
  - Spoofing

Non-adversarial testing

- **False accept rate (FAR)**: rate when imposter biometric is accepted
- **False reject rate (FRR)**: rate when authentic biometric is rejected
- Lower FAR = less tolerant of close matches
  - Harder to attack
  - Necessarily increases FRR
- Lower FRR = more tolerant of close matches
  - Easier to use
  - Necessarily increases FAR
- Since match is approximate can almost always tune for one or other



Attacks on Biometric Auth



Biometrics Spoofing

- Biometrics are private, but not secret
  - Users expose biometric instances everywhere
    - Fingerprints, hand geometry, face, handwriting, iris, gait, etc.
  - Allows attacker to create biometric forgery
  - Very hard to replace a biometric identifier

Biometrics Spoofing

- There are spoofing techniques for virtually all biometrics

WIRED

Inside the OPM Hack, The Cyberattack that Shocked the US Government

A security engineer named Brendan Saulsbury set out to decrypt a portion of the Secure Sockets Layer (SSL) traffic that flows across the agency's digital...

Oct 23, 2016

Deepfake

Hundreds of German politicians hit in hacking attack

Cristina Burack | Darko Janjevic
01/04/2019

German Chancellor Angela Merkel and other senior politicians were reportedly hit by a data hack, with some of their letters, contact details and party memos leaked on Twitter.

Infrared Photo

Forbes
https://www.forbes.com › Innovation › Cybersecurity

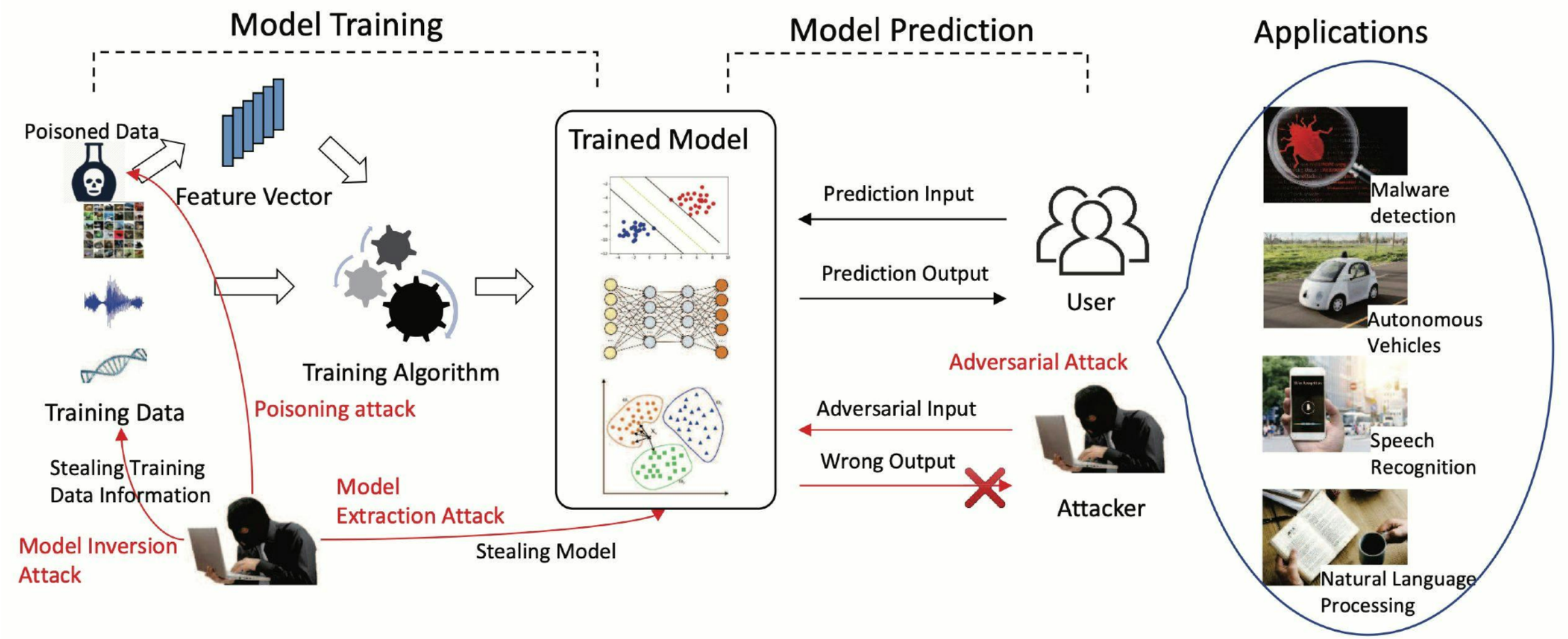
Samsung Galaxy S10 Fingerprint Scanner Hacked

Apr 6, 2019 — Now it appears that **Samsung** has just been proven wrong as a security researcher demonstrated how he fooled the fingerprint scanner with a 3D- ...

3D-print Fingerprint

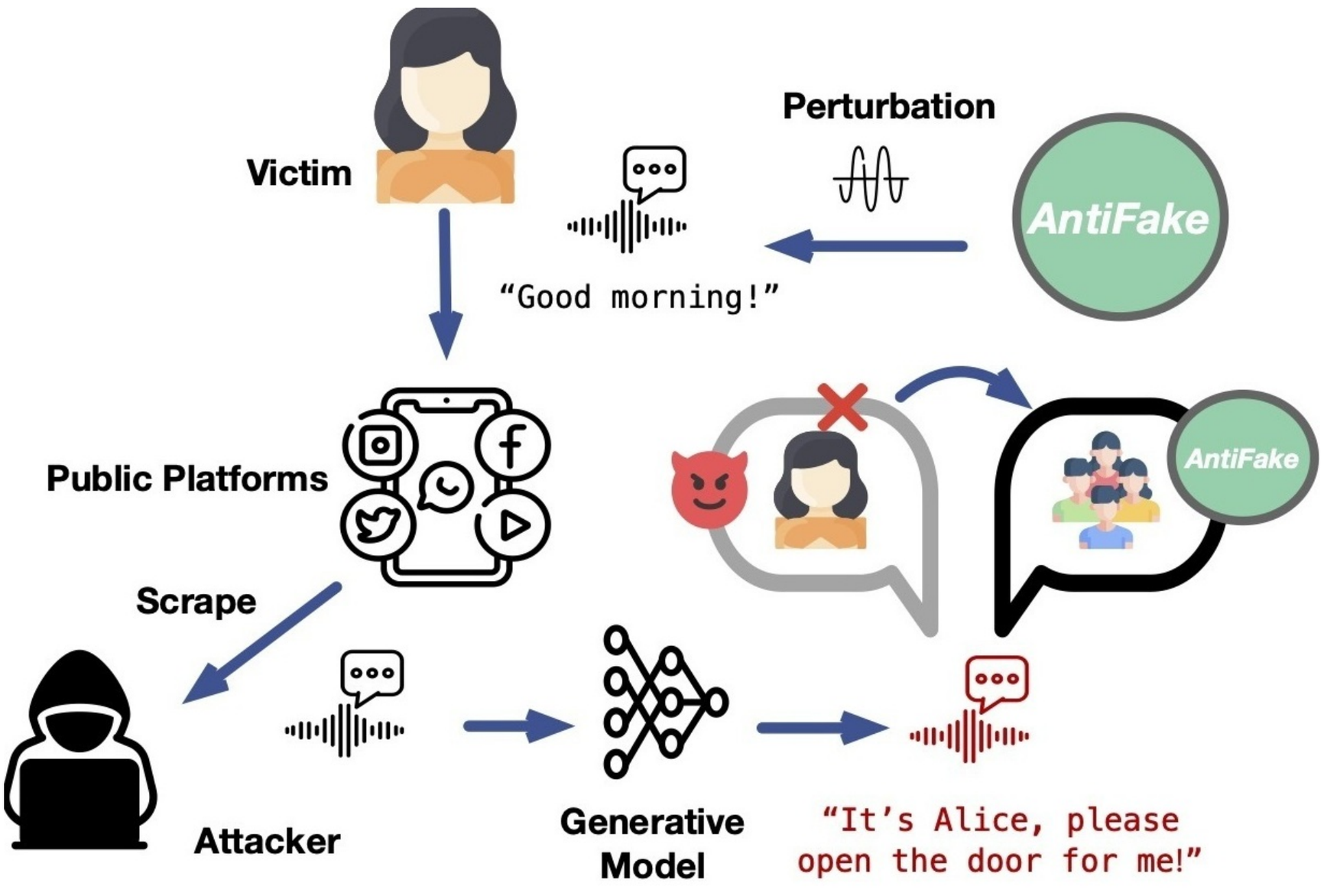
Biometrics Spoofing

Emerging area: Adversarial ML



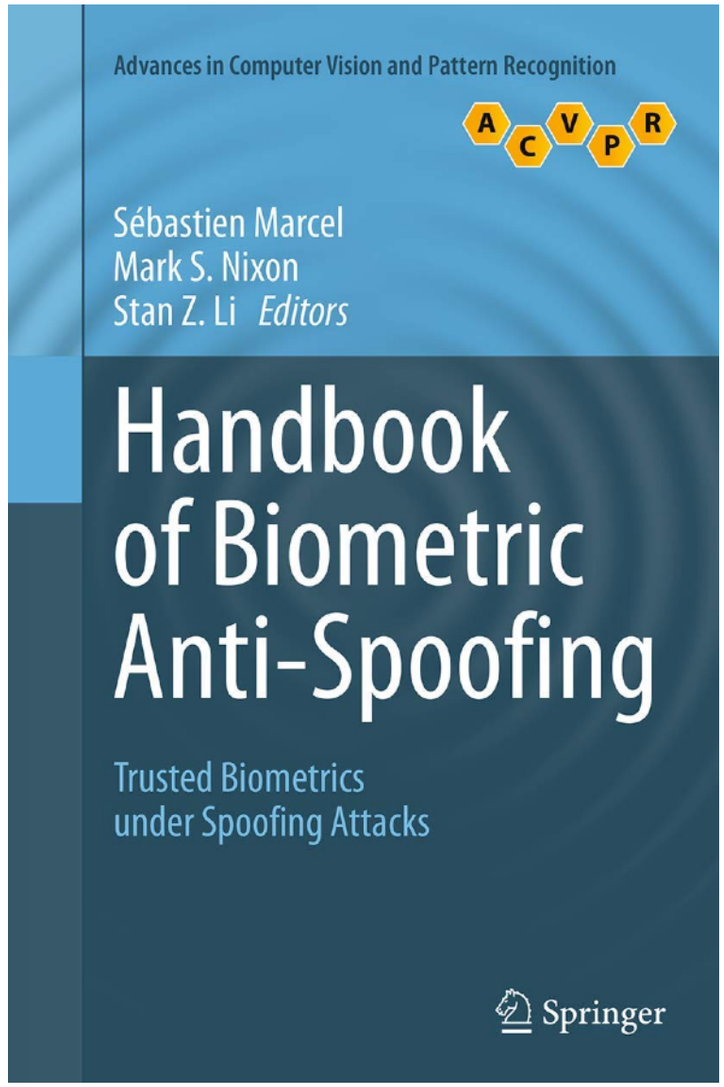
Biometrics Spoofing

Emerging area: Spoofing based on generative models.



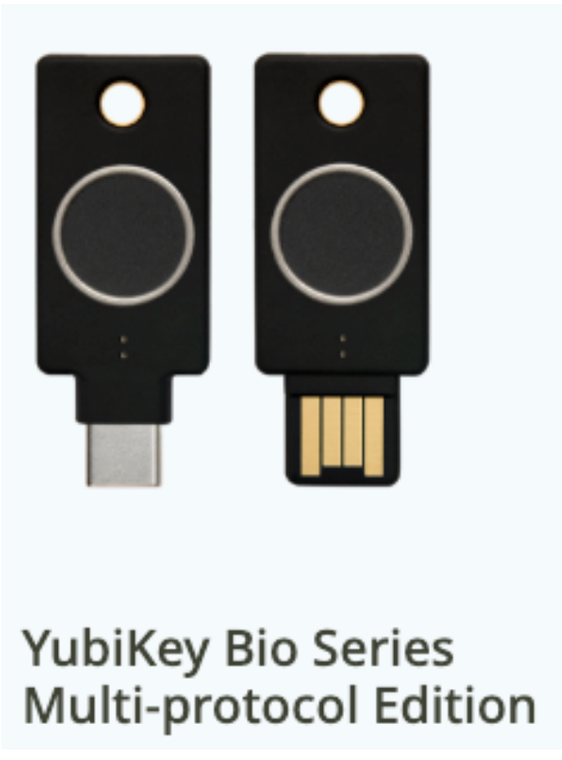
Biometric Spoofing Mitigations

- Replay prevention
  - Save previous image and reject if identical
  - Tricky: can pick up and rotate to fool
- Improved validation prevision
  - Verifier should have higher precision than forger
  - Examples: pore detection, perspiration detection
- “Liveness” detection
  - Examples: temperature, pulse, blood flow



Biometric Spoofing Mitigations

- Multi-modal
  - Combine different biometrics
- Multi-factor
  - Combine with password / tokens



YubiKey Bio Series
Multi-protocol Edition

Summary

- Token-based Authentication
  - Usage of challenge-response protocol
  - Smartcards. Tokens.
  - Attack examples
- Biometrics-based Authentication
  - General flow.
  - Spoofing

Acknowledgement

- The slides of this lecture is developed heavily based on
  - Slides from Prof Nadia Heninger's lecture on Computer Security (https://cseweb.ucsd.edu/classes/wi23/cse127-a/slides/16-authentication.pdf)
  - Slides from Prof Ziming Zhao's past offering of CSE565 (https://zzm7000.github.io/teaching/2023springcse410565/index.html)
  - Slides from Prof Marina Blanton's past offering of CSE565 (https://www.acsu.buffalo.edu/~mblanton/cse565/)
  - Slides from Prof Hongxin Hu's past offering of CSE565

Questions?