

10/7/26

COMP 435:

Computer Security Concepts



Lecture 20: Authentication, Biometrics



The University
of North Carolina
at Chapel Hill

<https://tinyurl.com/comp435-fa26>

Logistics Update



- Lab 2 Released! Due 10/14
- Details about final project posted
 - First milestone due 10/21
- Quiz Friday

Quiz Topics



- **OS Security & Access Control**

- Responsibilities of the OS
- users, processes, privileges, RUID vs. EUID
- access-control decisions and privilege boundaries
- capabilities: object + allowed operations; possession conveys authority

- **Security Models**

- confidentiality vs. integrity policies
- interpreting simple read/write restrictions
- Bell-LaPadula / Biba at a conceptual level

- **Race Conditions**

- TOCTTOU: check → state changes → use
- why race conditions can become security vulnerabilities
- identifying the security-relevant fix (atomicity / avoid separate check-and-use)

- **Password Security**

- password search space and guessing
- online vs. offline guessing
- hashes and password verification
- salts: what they do and do not do

Plan for Class Today



- 10:10-10:25 – Finish Authentication Concepts/Definitions
- 10:35-10:50 – Biometrics
- 10:50-11:00 – Maybe intro to crypto!

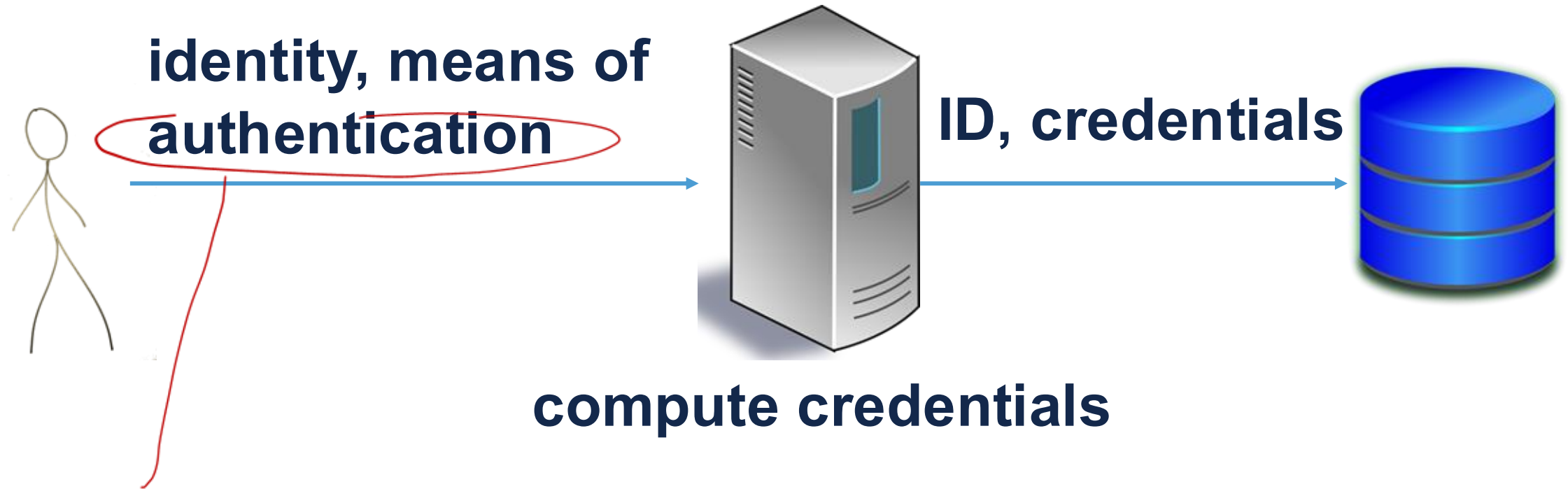
Guiding Question 😊

How do we
authenticate our
systems?



User Authentication... in *Computer Systems!*

Phase 1: Registration

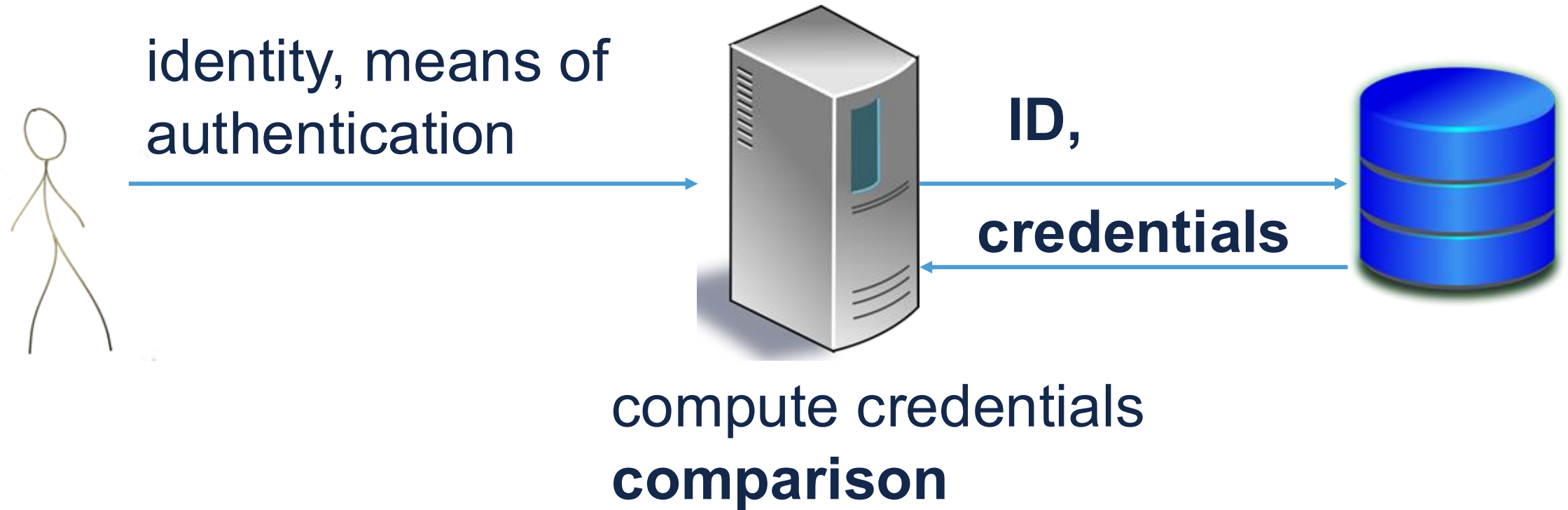


login, pw

1

5

Phase 2: Authentication



Means of Authentication



biometrics

|

What you
know

|

What you
do or what
you are

What you
have

Where you
are

passwords



Passwords

Means of Authentication

What you
know

What you
do or what
you are

What you
have

Where you
are

passwords

Passwords



- Ubiquitous
- Easy to use
- No extra hardware

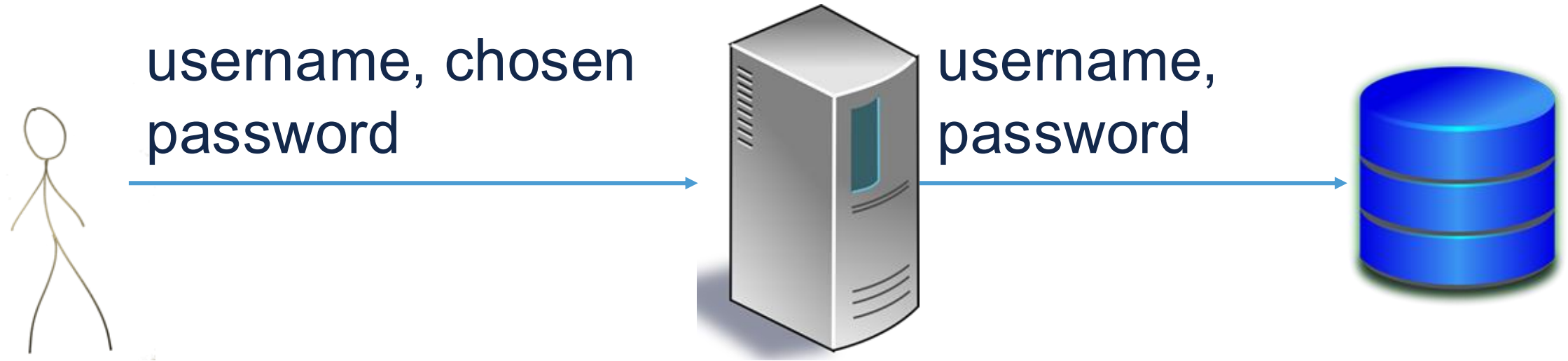
Pros



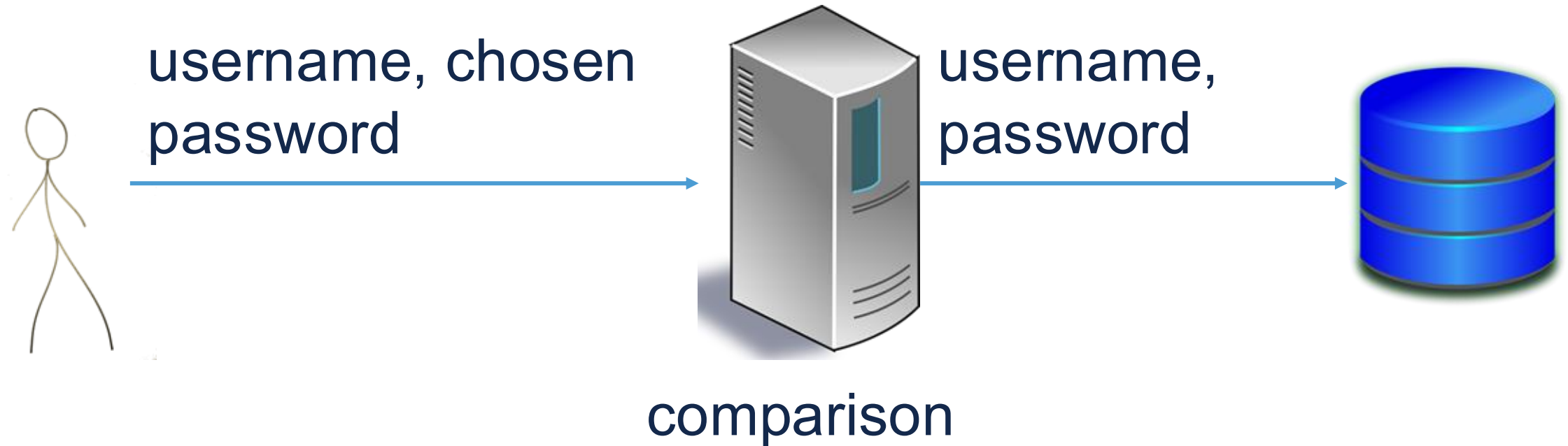
- Easy to attack
- Difficult to use well

Cons

Phase 1: Registration



Phase 2: Authentication





What is the attacker's chance of guessing correctly?

8-character passwords

printable characters (excluding space)

WS Q1

- 52 alphabetic
- 10 numeric
- 32 add'l (excluding space)

94.94.94.---94 → 948

1 2 3 --- 8



Take your answer from Q1... convert it to a power of 2!

$$\underline{\underline{94^8}} \sim = \underline{\underline{100^8}} = \left(10^2\right)^8$$

10^{16}

$$10^{16} = \underline{\underline{10^{12}}} \cdot \underline{\underline{10^3}} \cdot 10$$

$$\underline{\underline{2^{90}}} \cdot \underline{\underline{2^{10}}} \cdot 10 \Rightarrow 2^{50} \cdot \underline{\underline{10}}$$

$$\left(\begin{matrix} 2^3 \\ 2 \end{matrix} \right)$$

$\approx 14,300$



If there are 2^{53} possible passwords, how long will it take, on average, for the attacker to guess the right one assuming the attacker can try **10,000 passwords per second**

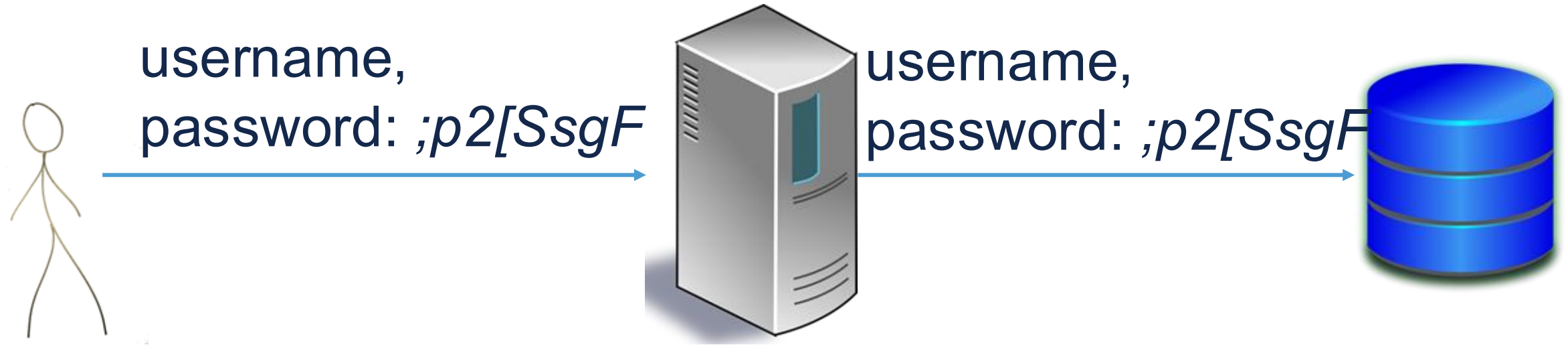
$$\frac{2^{53}}{2} \Rightarrow 2^{52}$$

$$\frac{2^{52} \text{ guesses}}{10,000 \text{ guesses/sec}} = 15 \text{ sec}$$

$$\frac{2^{52}}{2^{10} \cdot 10} \rightarrow \frac{2^{42}}{10}$$

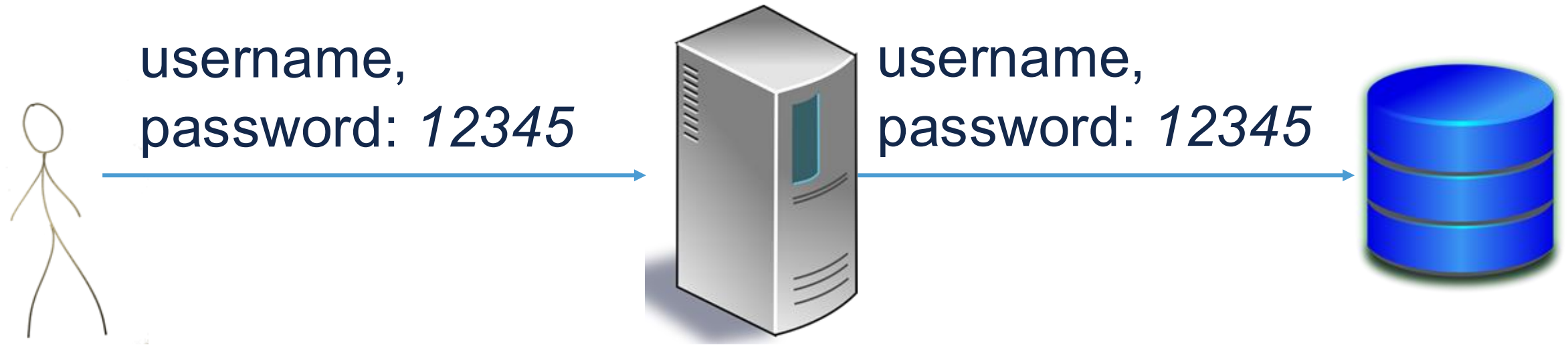
WS Q2

Phase 1: Registration



People unfortunately do not choose passwords that look like this.

Registration



People choose passwords that look like this! Easier to remember....



Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions

Passwords are not chosen uniformly at random.

Attackers start with the most common passwords.



Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



learnable online,
small set

Common Passwords



- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



600,000 English
words



Common Passwords

- “qwerty”
- “12345678”
- “password”
- “11111111”
- family names
- pet names
- words in the dictionary
- common number substitutions



e:3, o:0, t:7,
l:1, for:4



Biometrics

Means of Authentication

What you
know

What you
do or what
you are

What you
have

Where you
are

biometrics

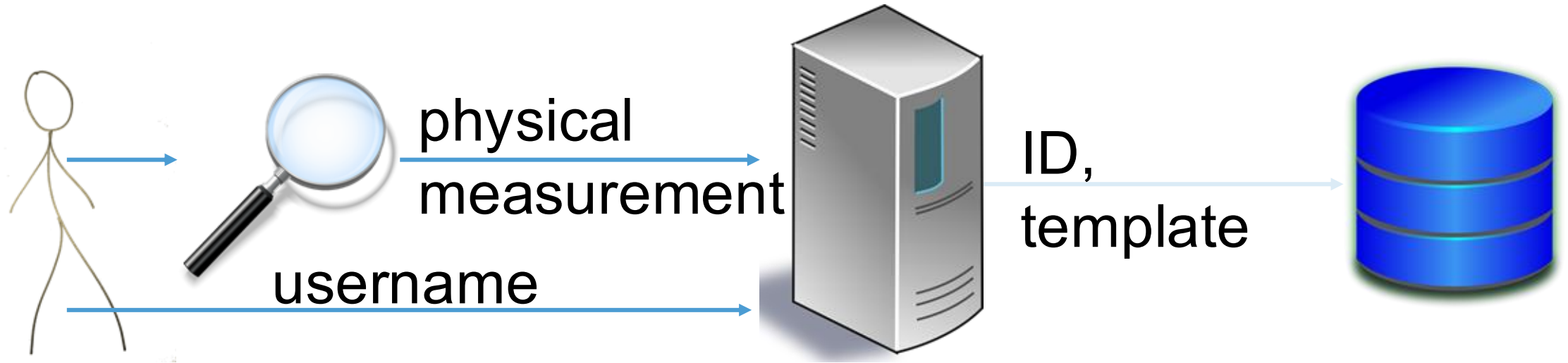
Biometrics



Def'n: Measurement of a physical characteristic

E.g., fingerprints, hand geometry, retina measurement, iris scan, voice, facial features

Phase 1: Registration

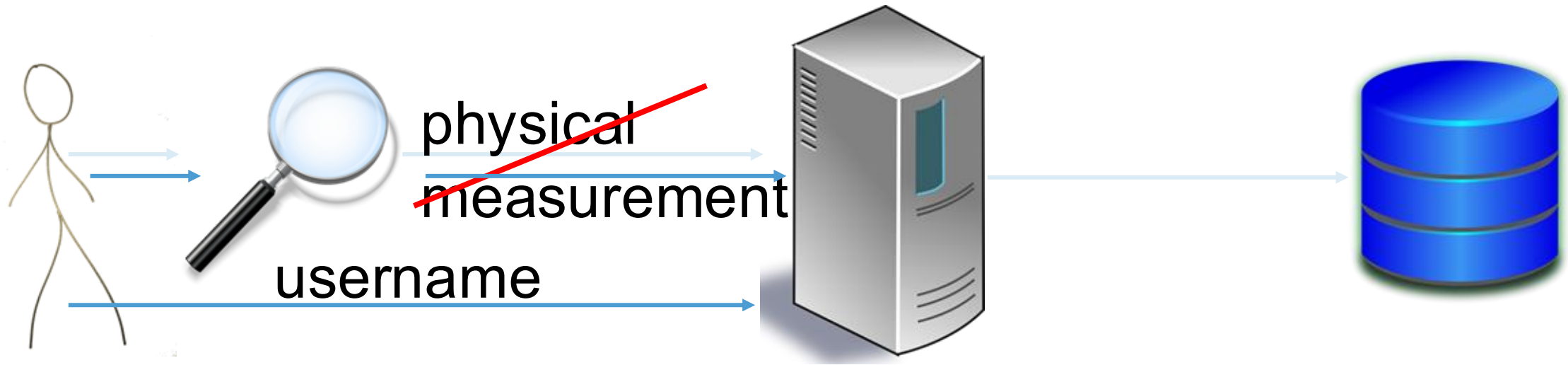


1. digitization
2. feature (template) extraction

Registration Issue: Failure to Enroll (FTE)



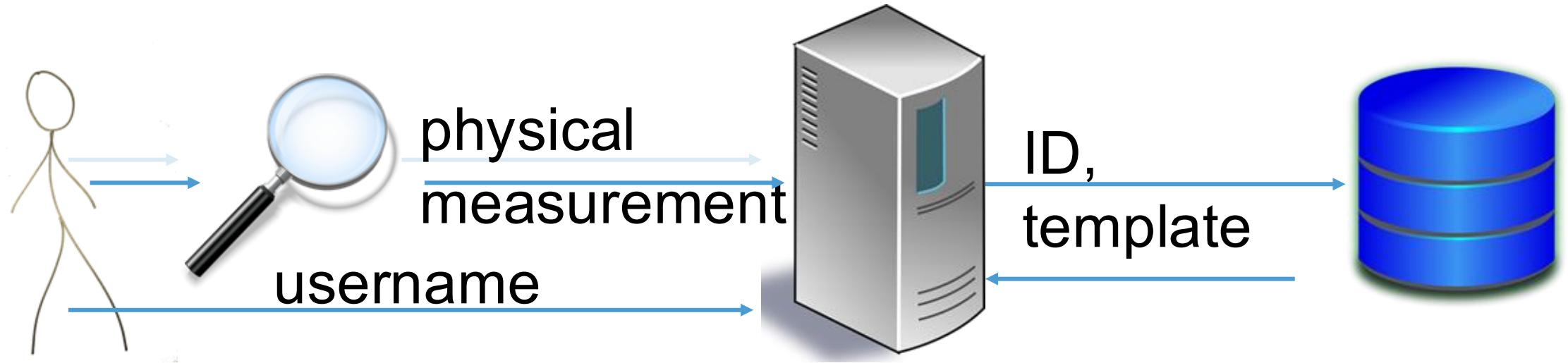
Def'n: The sensing mechanism is unable to capture an adequate sample.



Any of these processes
could go awry

1. ~~digitization~~
2. ~~feature (template)
extraction~~

Phase 2: Authentication

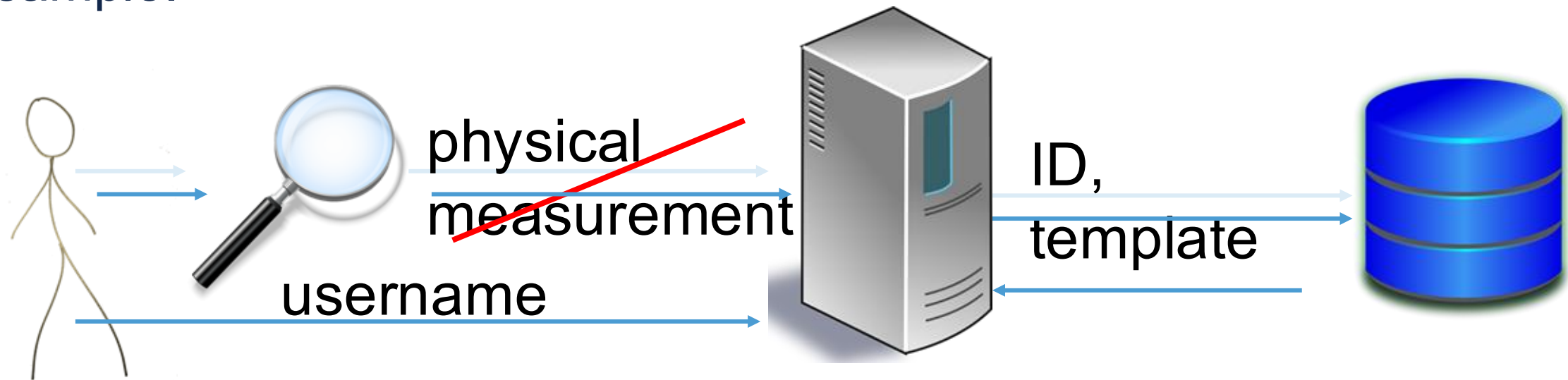


1. digitization
2. feature (template) extraction
3. comparison

Authentication Issue: Failure to Capture (FTC)



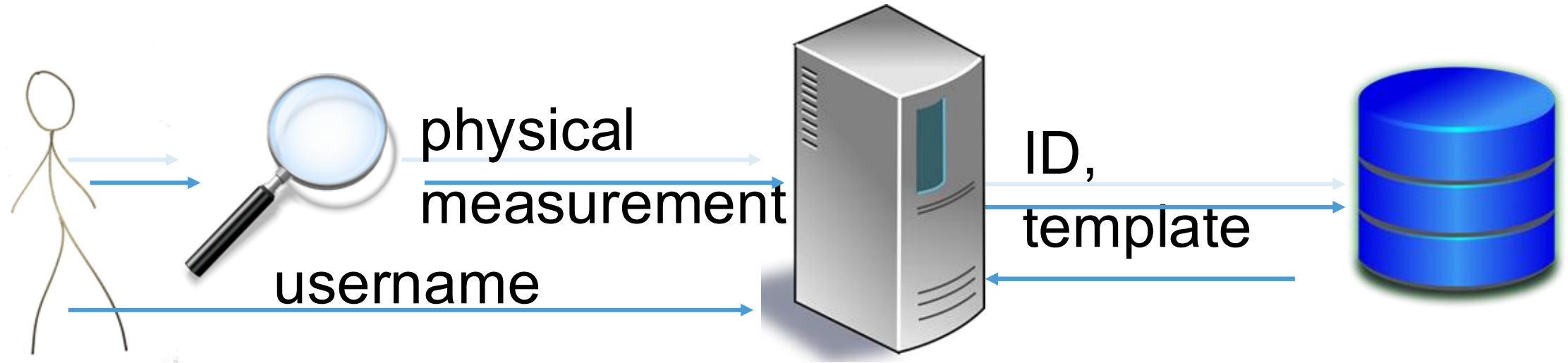
Def'n: The sensing mechanism is unable to capture an adequate sample.



Any of these processes
could go awry

1. ~~digitization~~
2. ~~feature (template)~~
extraction
3. comparison

Authentication Challenge In Practice: Comparison



1. digitization
2. feature (template) extraction
3. comparison

Authentication via Biometrics



	Is the identified user	Is not the identified user
Considered a match	True Positive	False Positive
Considered not a match	False Negative	True Negative

Biometrics + Templates



- **Reference template:** feature-based, digital representation of a person's biometric trait

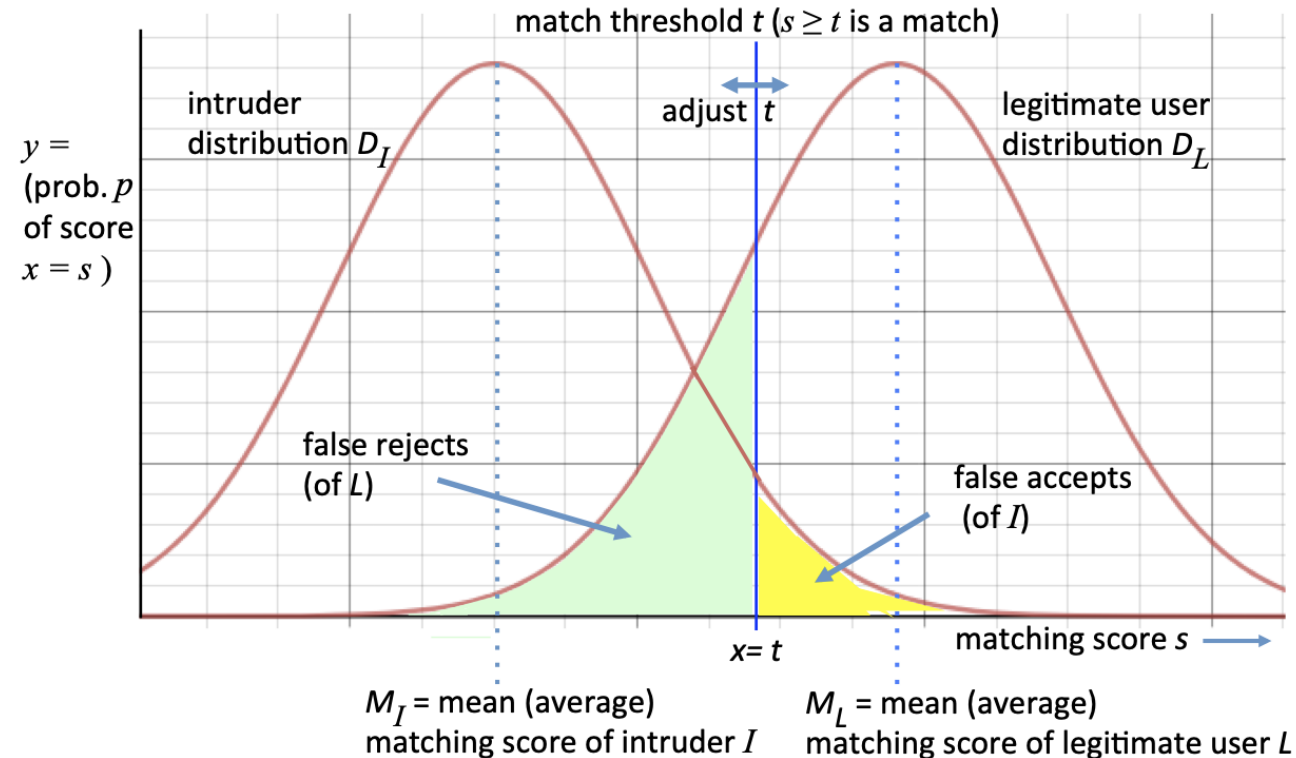
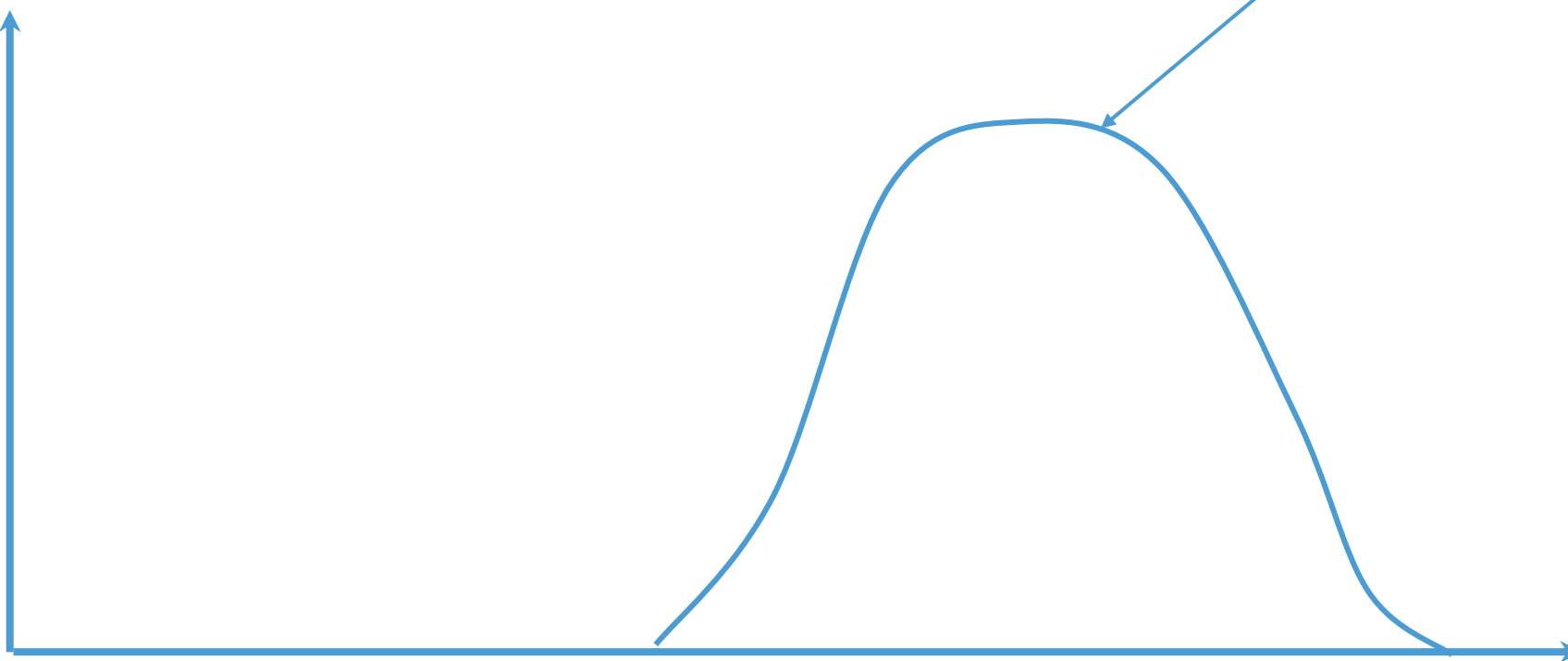


Figure 3.6: Biometric system tradeoffs. Curves model probability distributions for an intruder and legitimate user's matching scores; higher scores match the user's biometric template better. The y axis reflects how many biometric samples get matching score $x = s$.

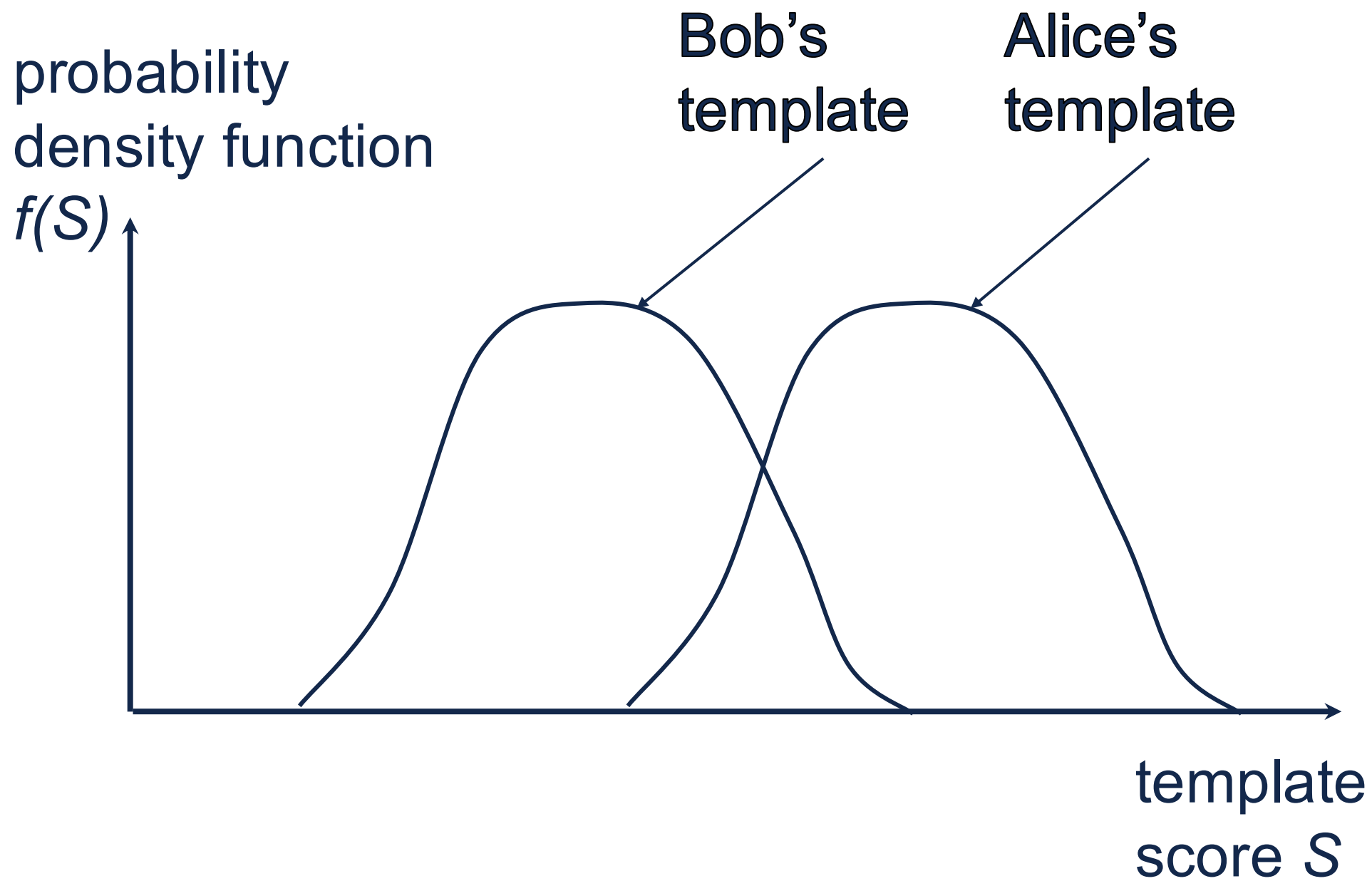


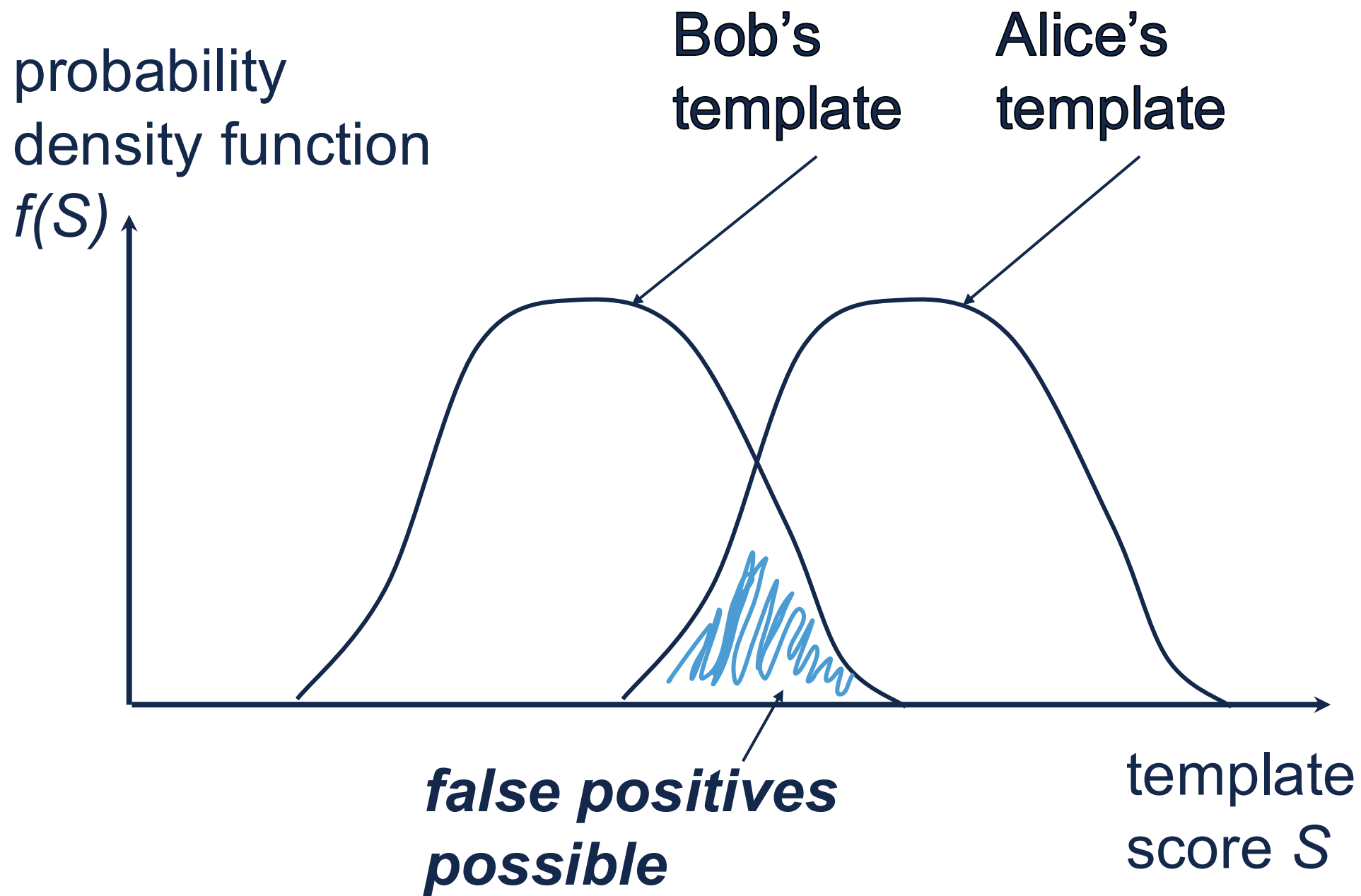
probability
density function
 $f(S)$

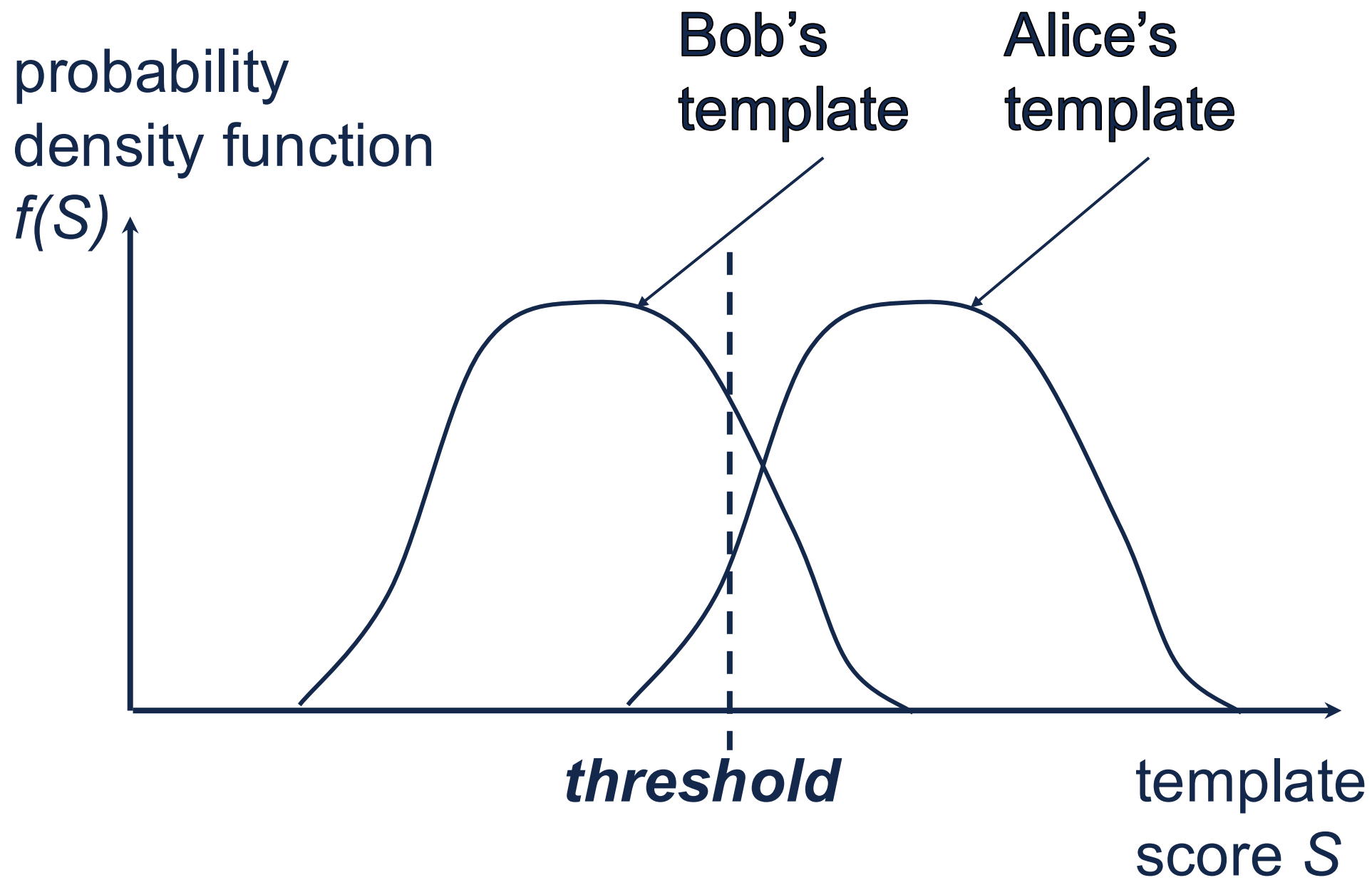
Alice's
template

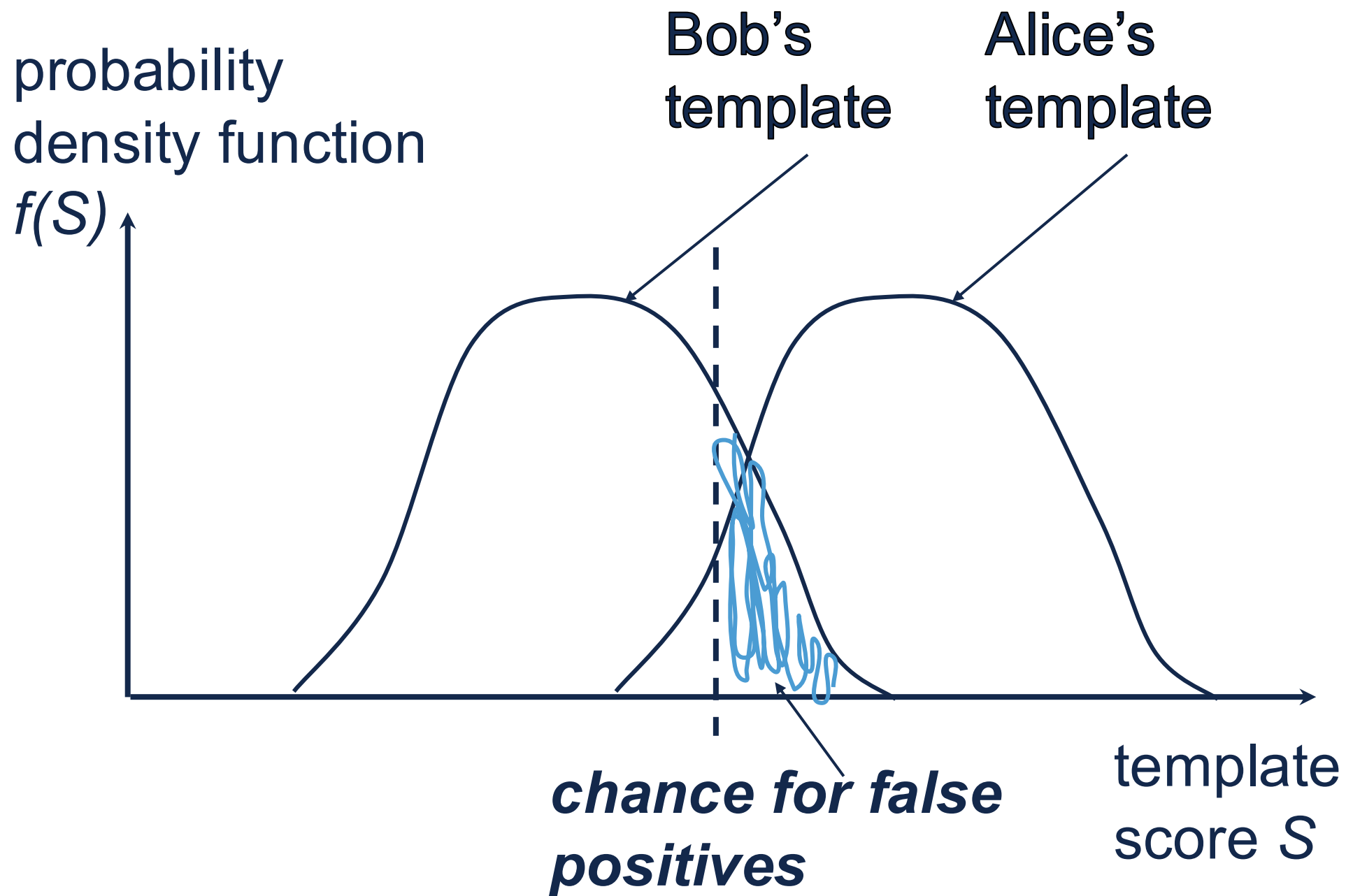


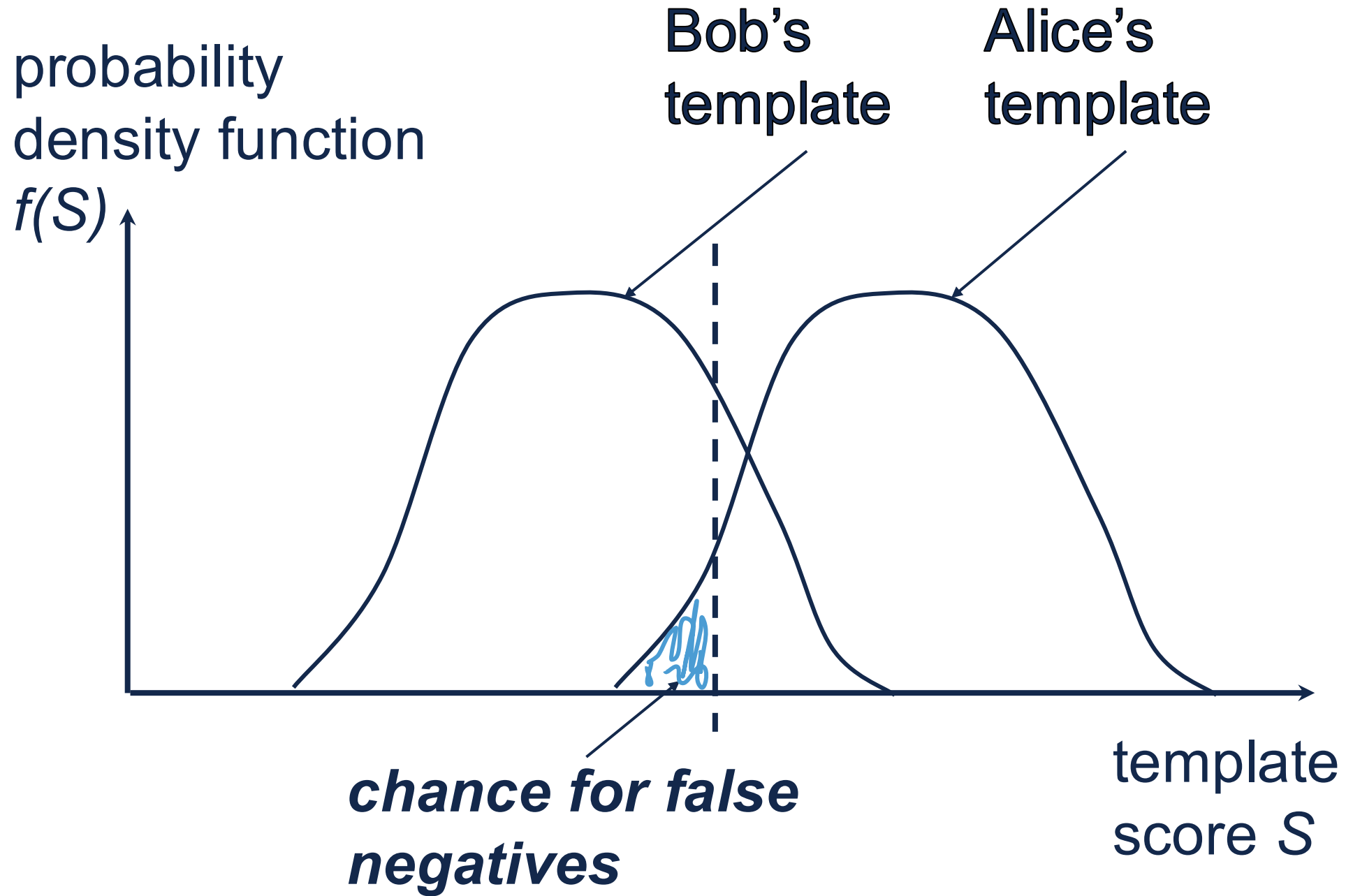
template
score S











Usability of Biometrics



- low cognitive load
- nothing extra to carry
- scales well for users

Pros



- failure to enroll
- failure to capture
- false negatives
- privacy concerns

Cons

Security of Biometrics for User Authentication



- physical characteristics are unique

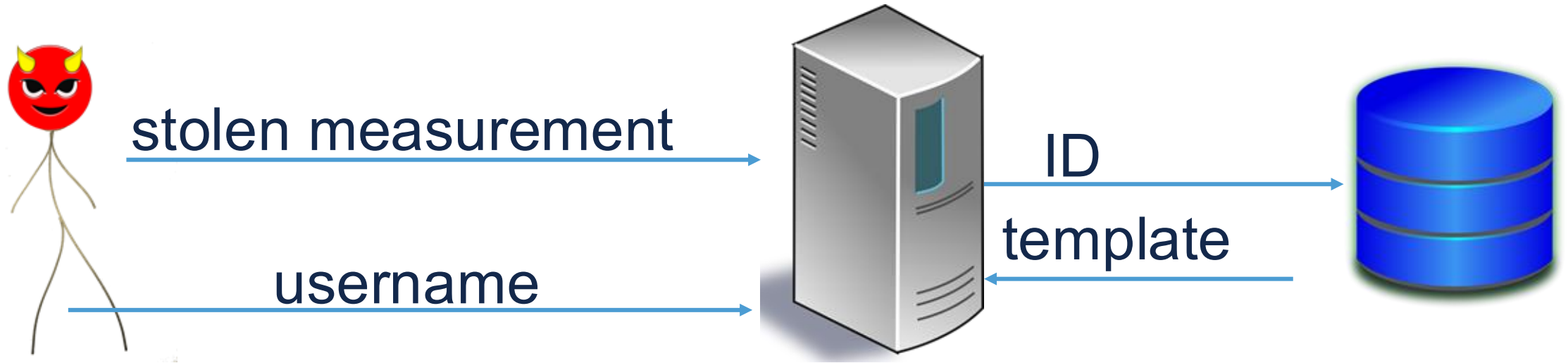
Pros



- insecure in remote or unsupervised setting

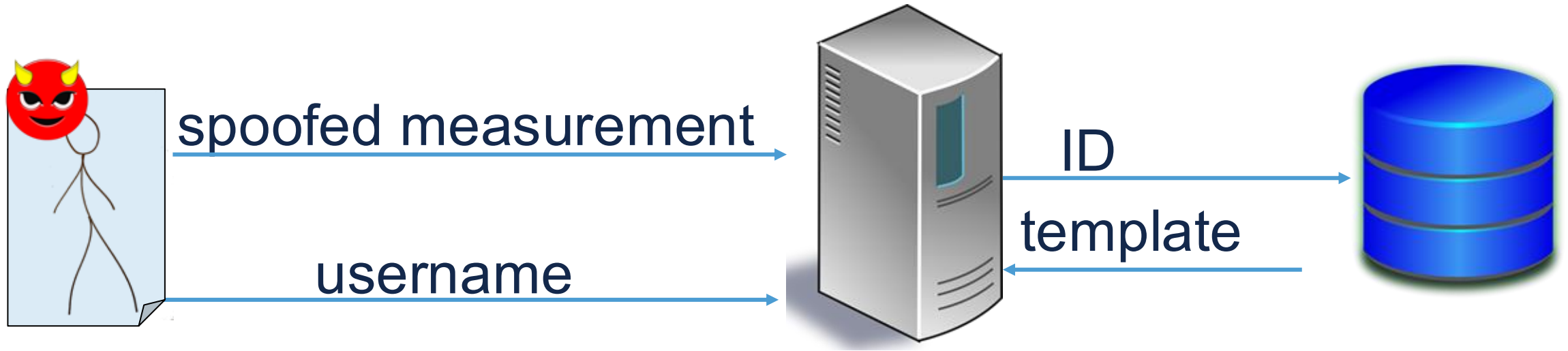
Cons

Remote Authentication



1. feature extraction
2. comparison

Unsupervised Authentication



1. digitization
2. feature extraction
3. comparison

Security of Biometrics for User Authentication



- physical characteristics are unique

Pros



- insecure in remote or unsupervised setting
- cannot be revoked
- false positives

Cons

Summary: Biometrics



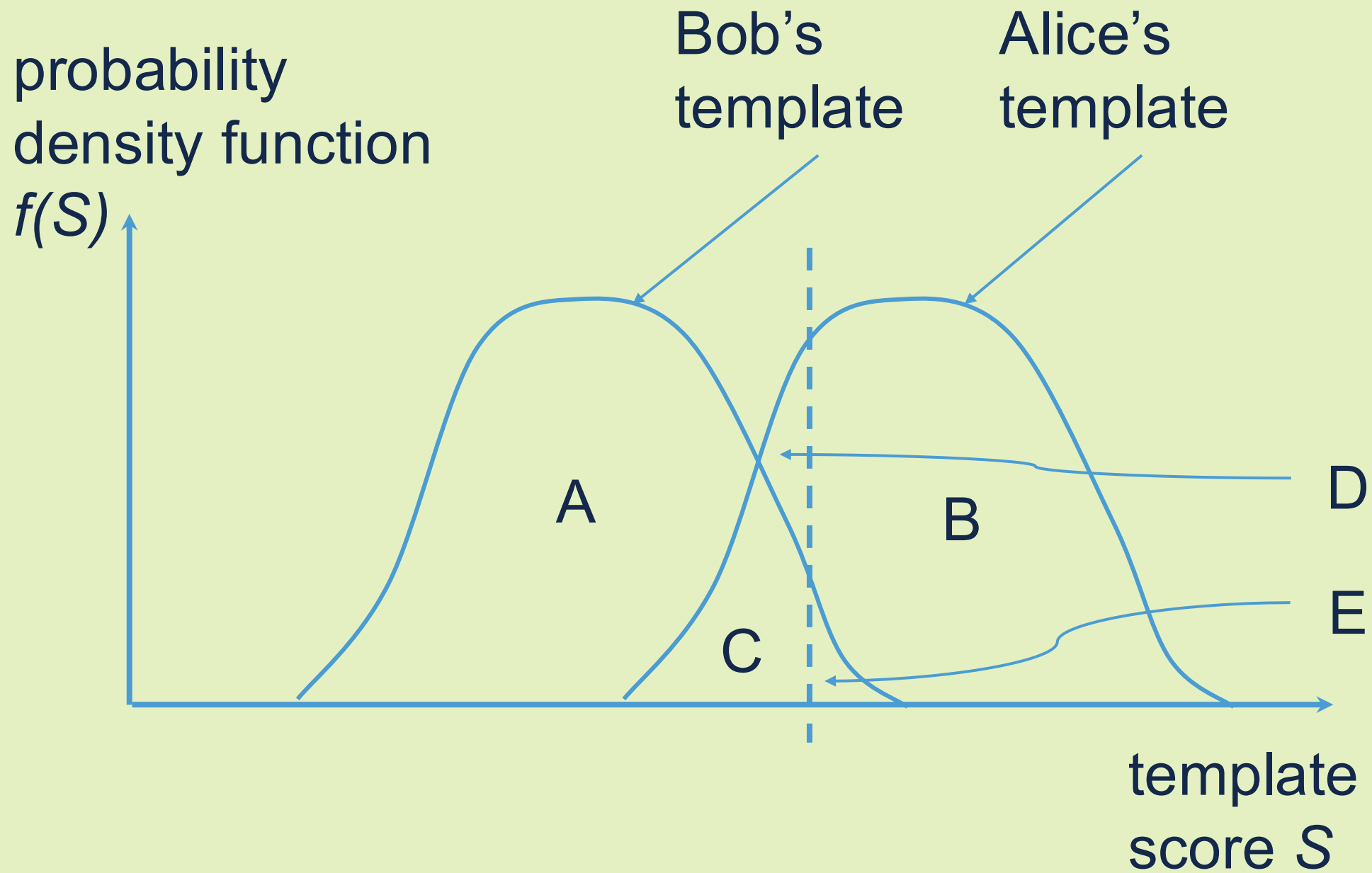
- Low cognitive burden
- Easy to use

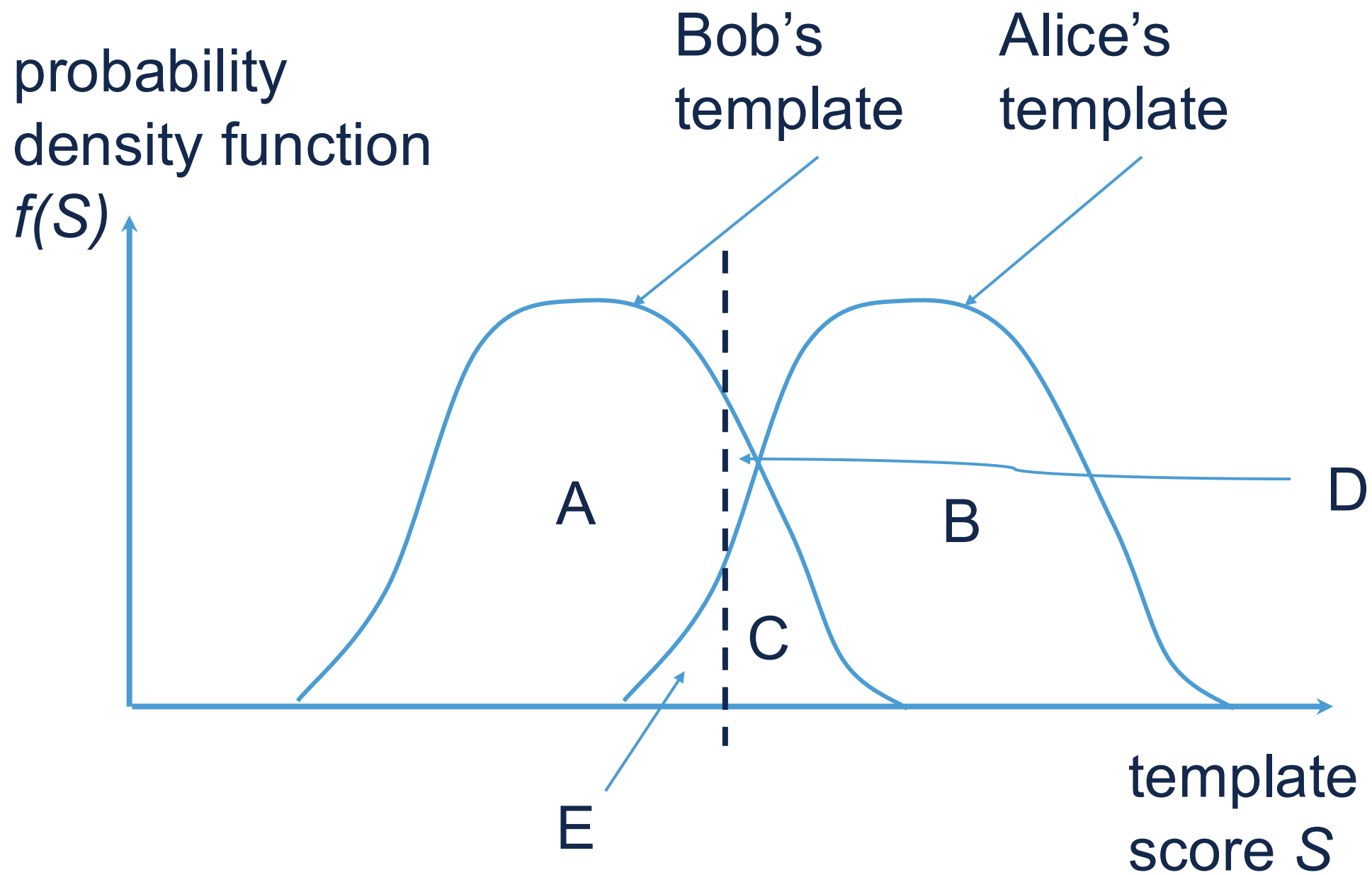
Pros



- Security is lower than expected
- Privacy concerns

Cons







What You Have, Two- Factor Authentication

Means of Authentication



What you
know

What you
do or what
you are

What you
have

Where you
are

tokens

Authentication by what you have



Def'n: Possession of an item is sufficient for authentication

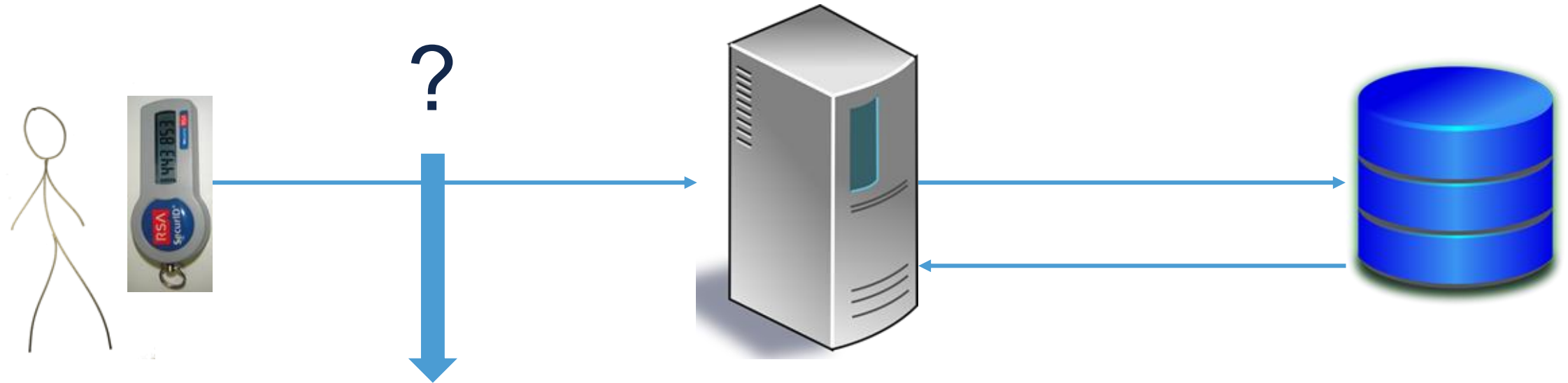
E.g.,

- keys
- credit card
- hardware token

Hardware Tokens



Demonstrating Possession Remotely



- Challenge-Response
- Synchronized Passcodes

The Challenge-Response piece involves some crypto... We will revisit!

Synchronized Passcodes



generate new
passcode

passcode



generate new
passcode



Two-factor Authentication



Def'n: require two independent means of authentication

E.g., Driver's license:

license: a physical token

picture: biometric authentication



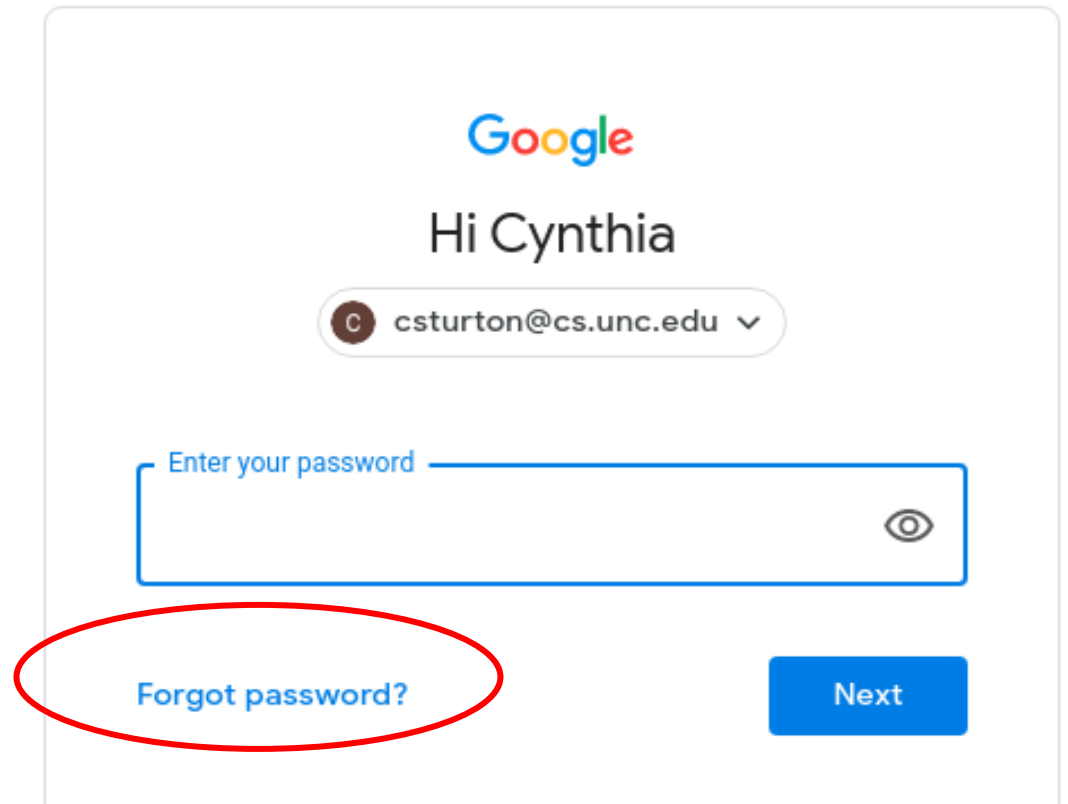
Revocation & Resetting

Revocation



Def'n: cancelling a means of authentication

- Passwords
- Biometrics
- Tokens

A screenshot of the Google login interface. At the top is the Google logo. Below it, the text 'Hi Cynthia' is displayed. Underneath is a rounded rectangle containing a small circular profile icon with the letter 'C' and the email address 'csturton@cs.unc.edu' followed by a downward arrow. Below this is a password input field with the placeholder text 'Enter your password' and a toggle icon (an eye) on the right. At the bottom left, the text 'Forgot password?' is circled in red. At the bottom right is a blue button with the text 'Next'.

Resetting a Password



1. Authenticate as user
2. Reset password

Q&A



Question 1 of 5

What is your favorite pizza topping? ▼

Question 2 of 5

Select question* ▼

Question 3 of 5

Select question* ▼

Question 4 of 5

Select question* ▼

Question 5 of 5

Select your answer* ▼

Artichoke
Bacon
Barbecue chicken
Basil
Black olive
Cheese
Chicken
Chili peppers
Chorizo
Garlic
Giardiniera
Green pepper
Ham
Jalapeño
Mashed potato
Mushroom