AUTHENTICATION

UT CS361S

Fall 2021

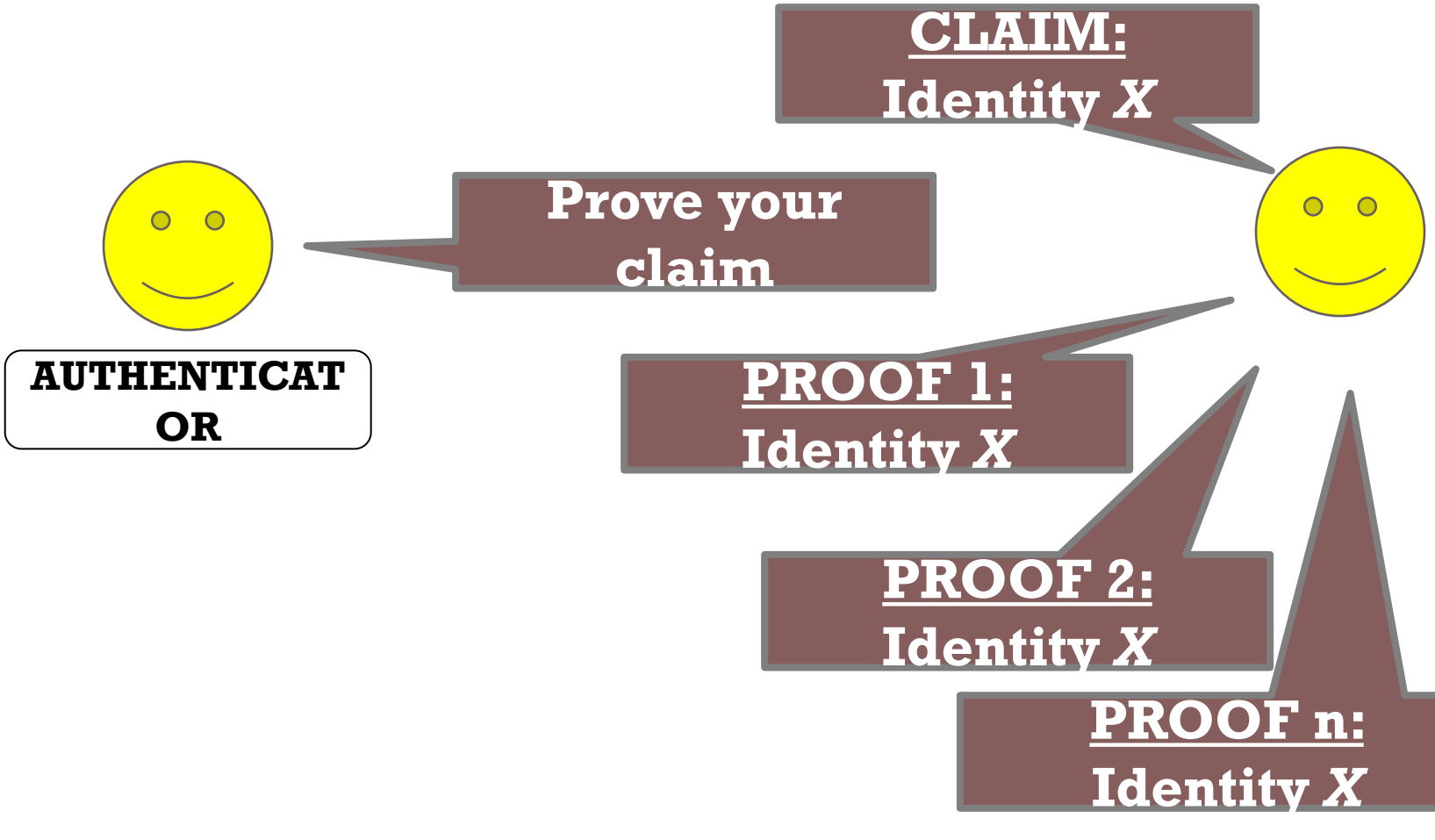
Lecture Notes

AUTHENTICATION / AUTHORIZATION

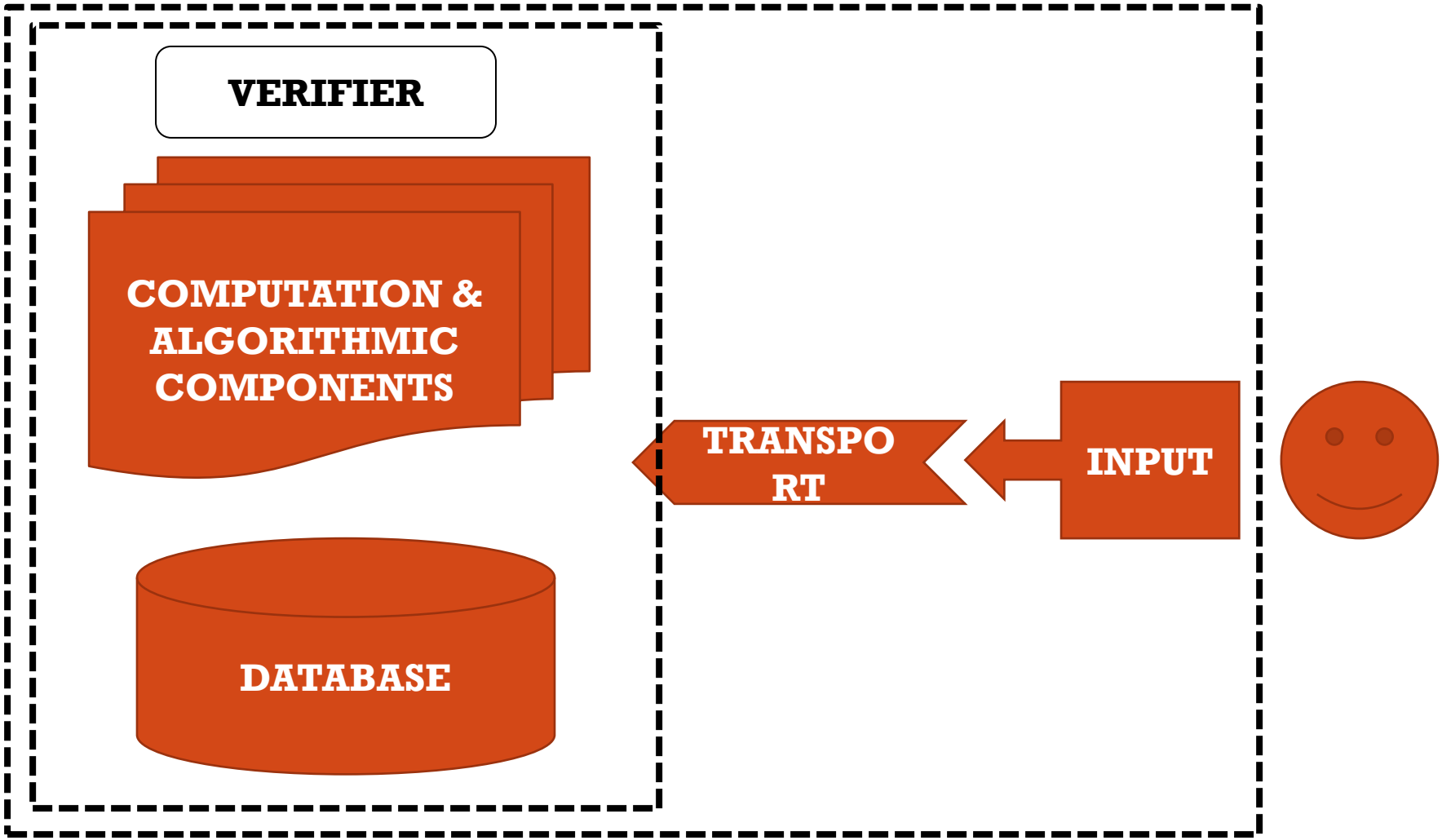
Validating Identity

Permissions Assigned to a Validated Identity

THE AUTHENTICATION PROCESS



AUTHENTICATION MECHANISM



THE BIG THREE

Something you **KNOW**

Something you **HAVE**

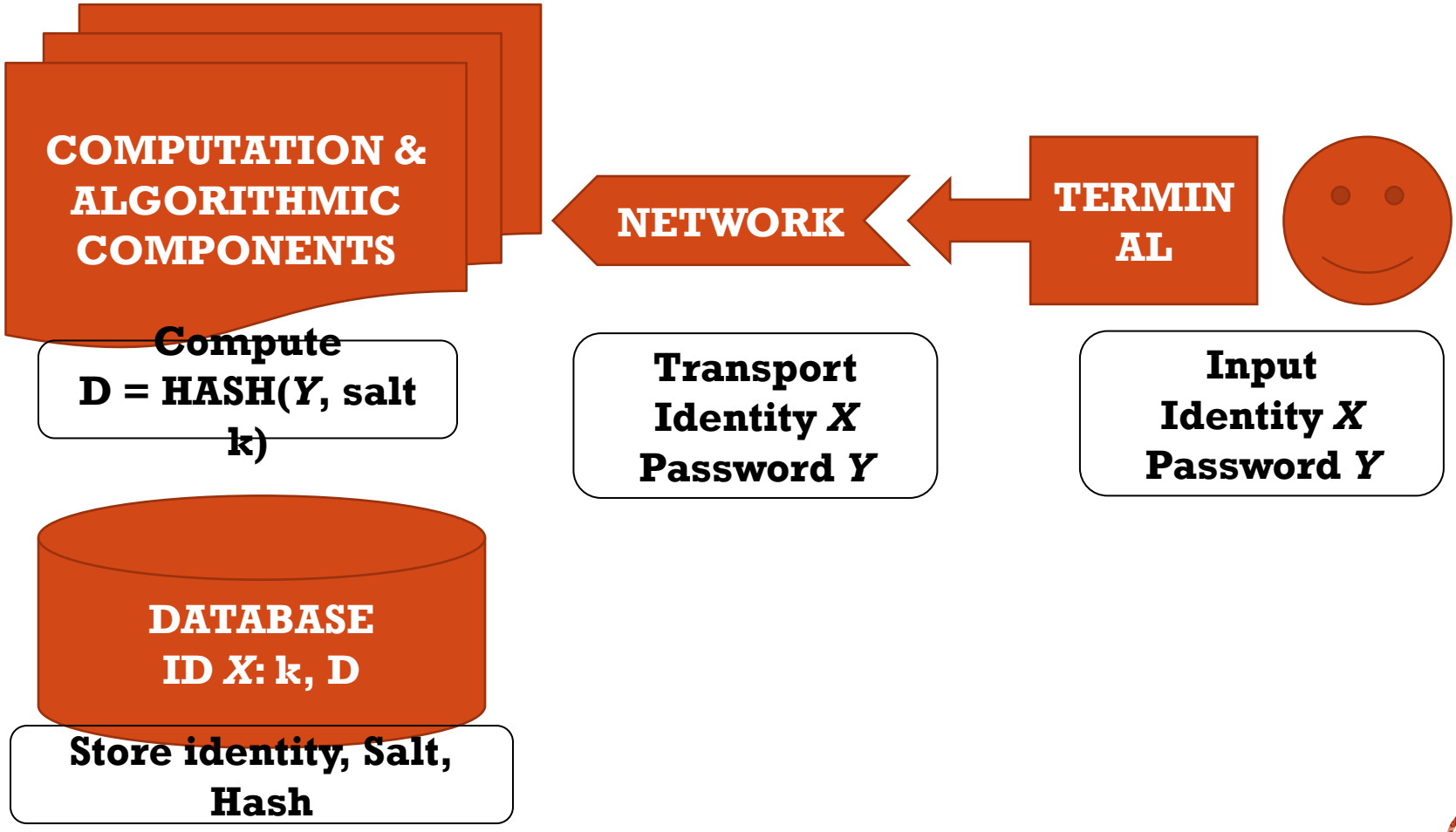
Something you **ARE**

KNOW: PASSWORDS

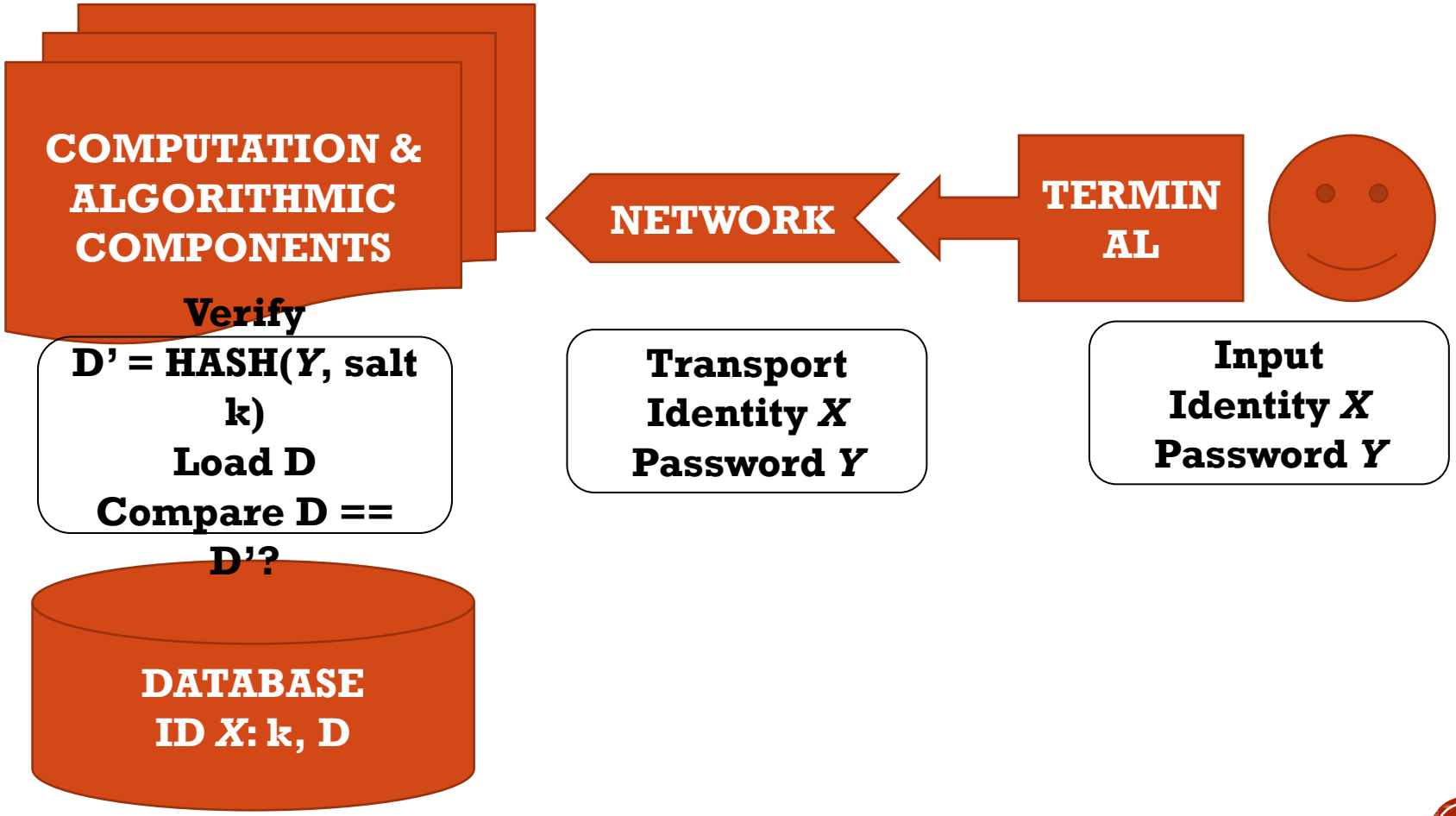
Security Requirements

1. The password is ONLY known by the party seeking authentication
2. The password cannot be easily guessed by human or computer
3. The password will not be forgotten by the party seeking authentication

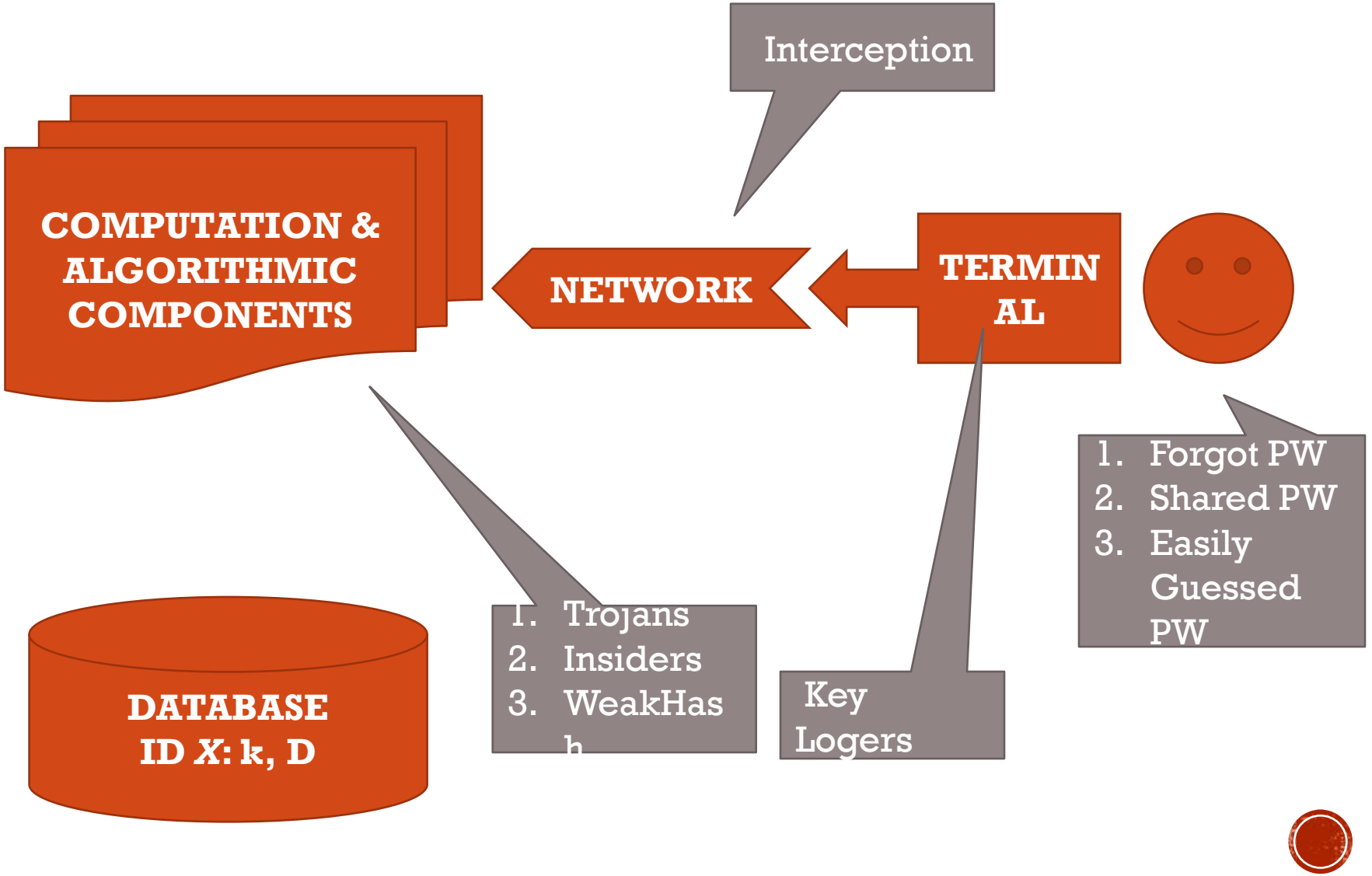
PASSWORD REGISTRATION



PASSWORD VERIFICATION



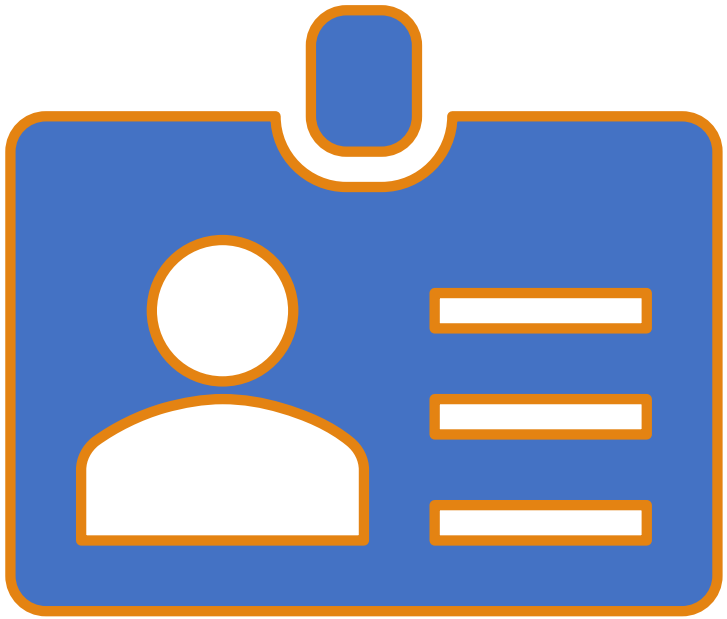
COMMON PROBLEMS



CHALLENGE RESPONSE SYMMETRIC

CHALLENGE RESPONSE ASYMMETRIC

MAN-IN-THE-MIDDLE (MITM)

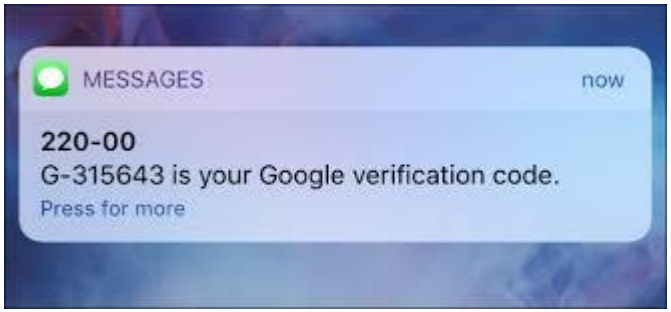


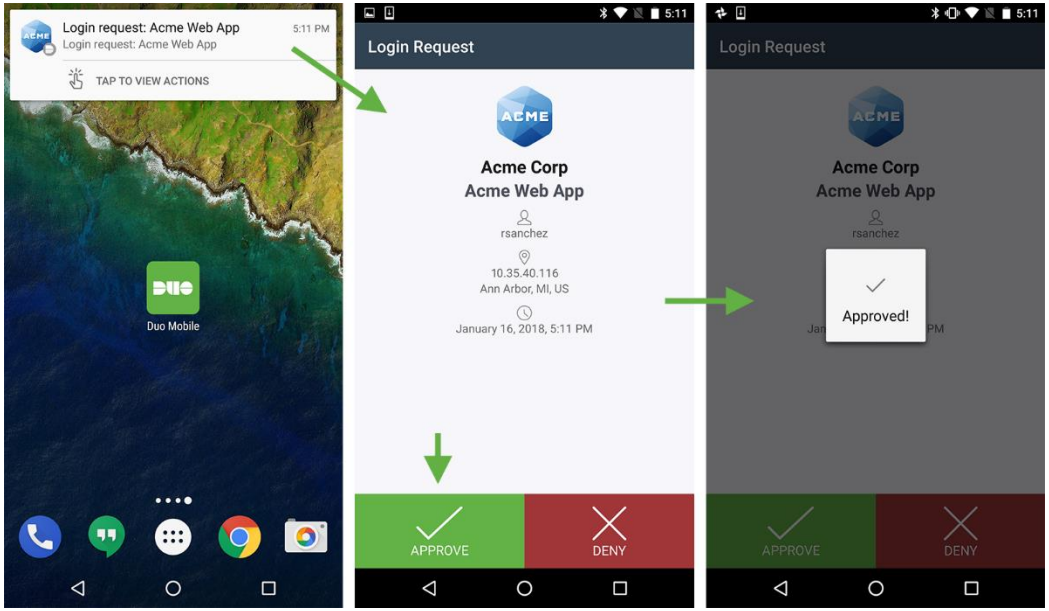
SOMETHING YOU HAVE

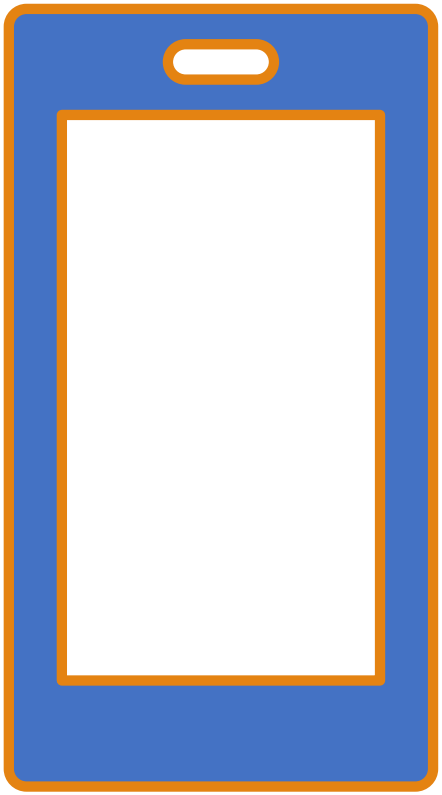
- Security Assumptions

1. The "token" is ONLY possessed by the party seeking authentication
2. The token cannot be easily forged or duplicated
3. ***The authentication protocol is secure***

SOMETHING YOU HAVE EXAMPLES







PROBLEMS WITH "TOKENS"

- Is it ***REALLY*** something you have?
- Is sending a code by email 2-factor?
- What about phone cloning?
- What about network interception?
- Is an RSA Token's seed just ***something you know***?
- "Something you can respond with"

Security Assumptions

1. The "characteristic" is effectively unique
2. Can effectively measure, record, or detect the characteristic
3. Characteristic cannot be forged, replicated, or otherwise "lost"
4. Characteristic will not change (too much) over time
5. Characteristic will never need to be revoked
6. ***The Authentication Protocol is Secure!***

SOMETHING YOU ARE

FALSE POSITIVES VS FALSE NEGATIVES

✕ False Negative – Do not authorize party with valid characteristic

✓ False Positive – Authorize party with invalid characteristic

RECEIVER OPERATING CHARACTERISTIC

- The trade off between FP and FN
- Decreasing one typically increases the other
- Equal Error Rate is when FP approximately equals FN
- In most biometrics, ***False Negatives*** are worse

PROBLEMS WITH BIOMETRICS

1. Fingerprinting has been *seriously* misused in Courts (see Anderson at pp. 469-470)
2. ***Interpretation of results and understanding of statistics***
3. Variable accuracy in scanning mechanism
4. "Freshness"
5. Belief in infallibility leads to security culture problems
6. Biometrics exclude a *lot* of people (e.g., differently abled)
7. Cvil Rights and Privacy issues
8. Injury that alter the characteristic (e.g., fingerprint)

ONE OTHER "AUTHENTICATION"

- "Some**WHERE** you Are"
- Almost universally used as an ancillary form of authentication
- Generally used do **disprove rather than prove identity**