AUTHENTICATION

UT LAW 369V

Spring 2024

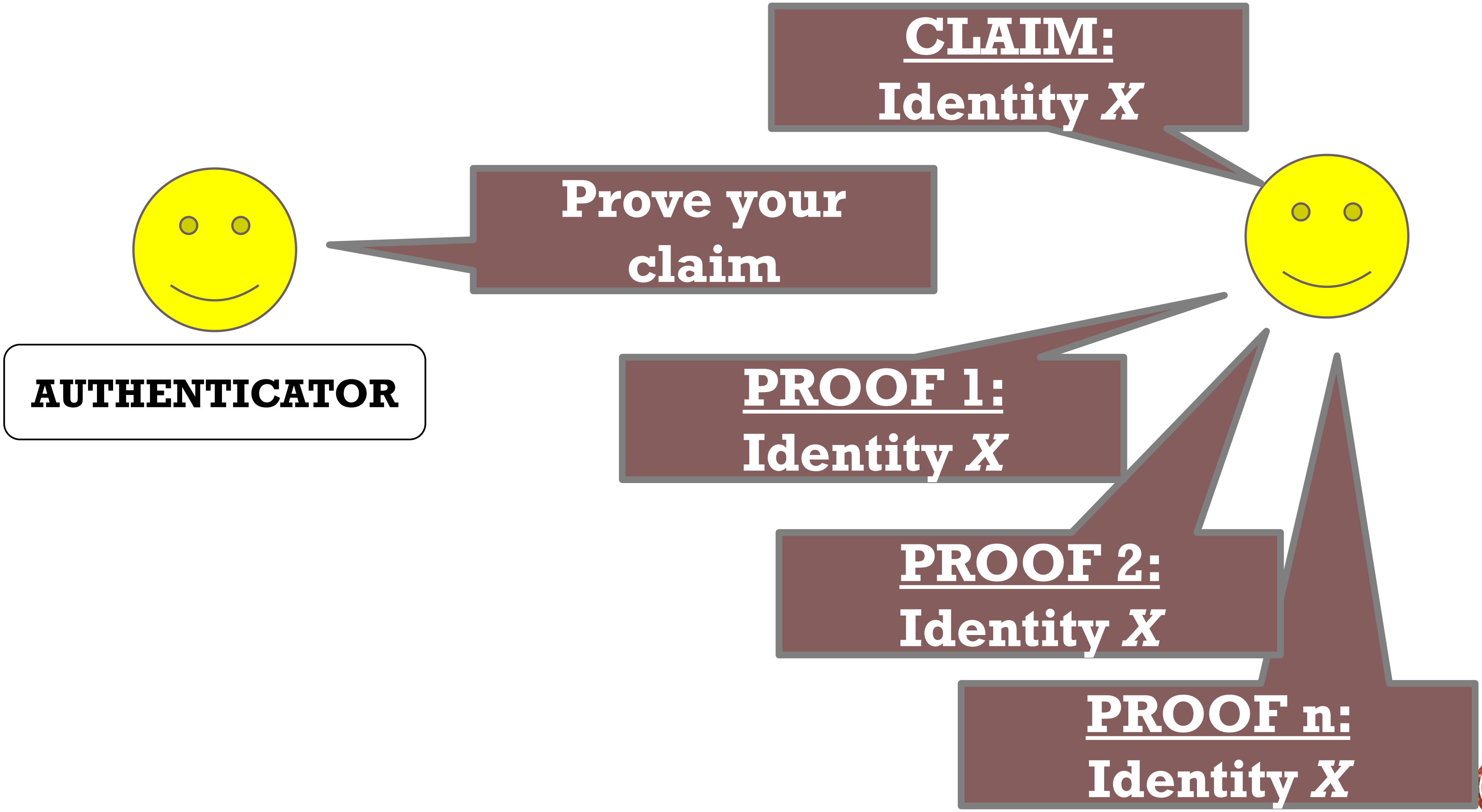
Lecture Notes

AUTHENTICATION/AUTHORIZATION

Validating Identity

Permissions Assigned to a Validated Identity

COMMON AUTHENTICATION PROCESS



CLAIM:
Identity *X*

Prove your claim

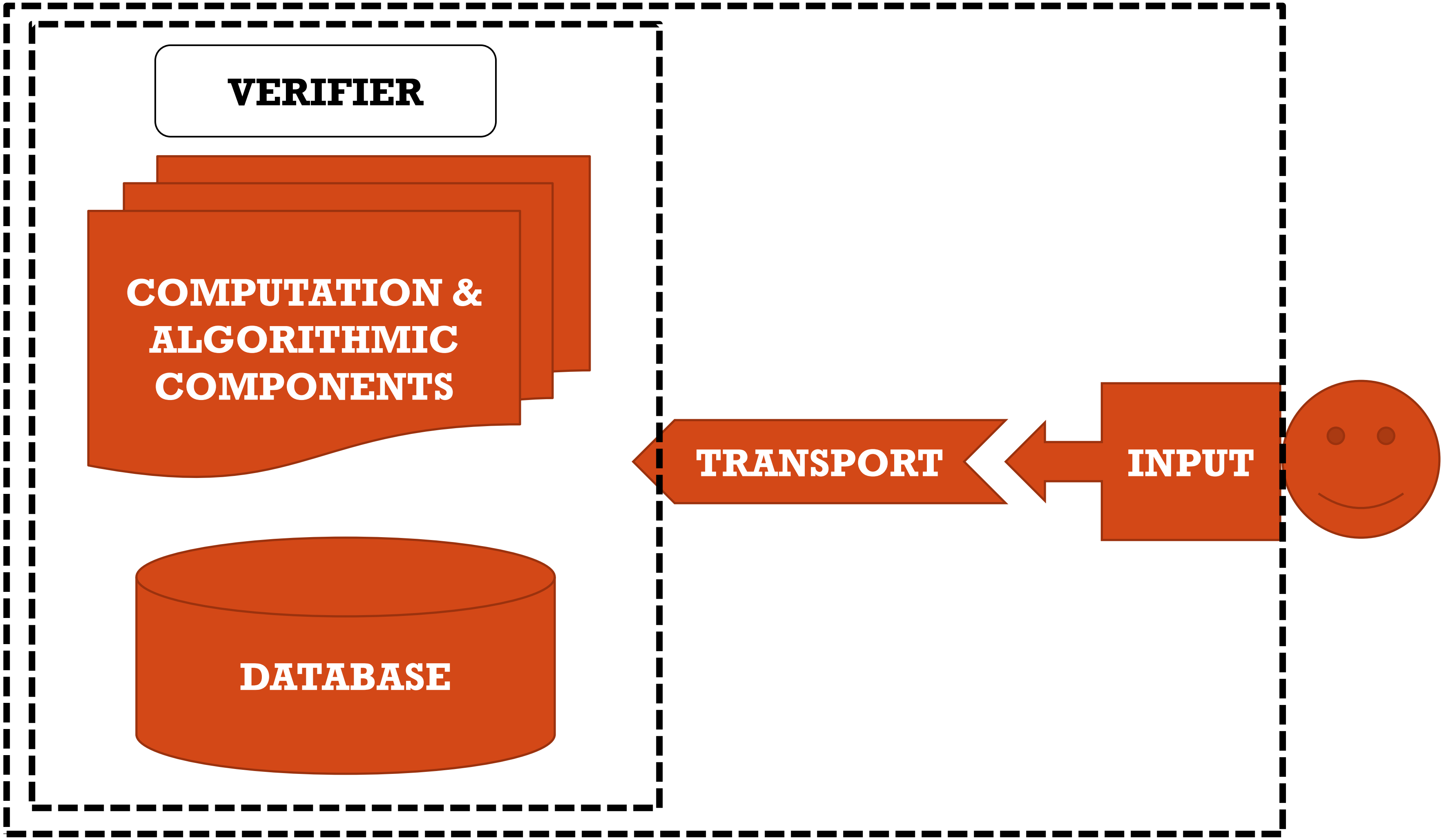
AUTHENTICATOR

PROOF 1:
Identity *X*

PROOF 2:
Identity *X*

PROOF n:
Identity *X*

AUTHENTICATION MECHANISM



VERIFIER

COMPUTATION & ALGORITHMIC COMPONENTS

DATABASE

TRANSPORT

INPUT

THE BIG THREE

Something you **KNOW**

Something you **HAVE**

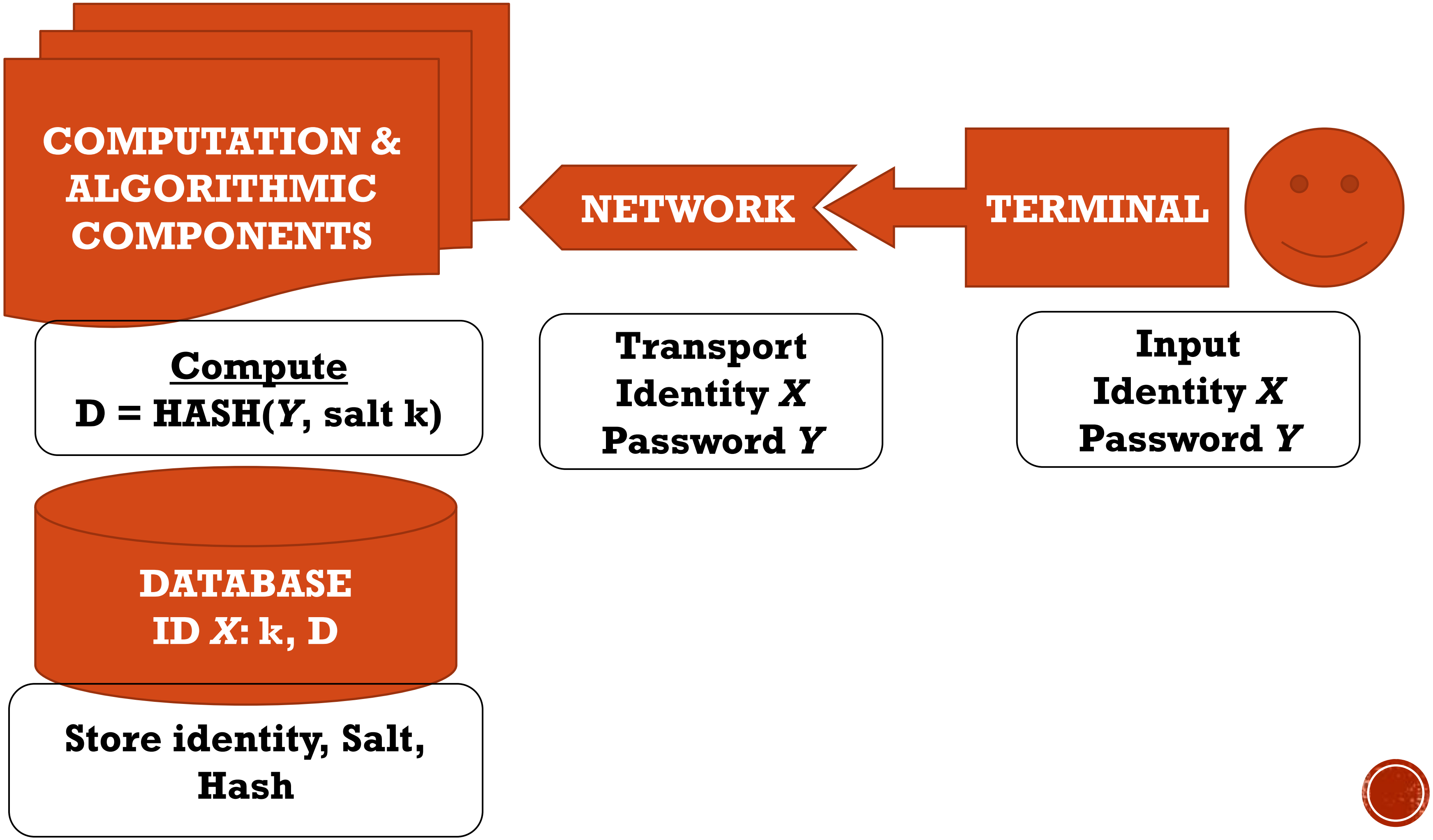
Something you **ARE**

KNOW: PASSWORDS

Security Requirements

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

PASSWORD REGISTRATION



COMPUTATION & ALGORITHMIC COMPONENTS

NETWORK

TERMINAL

<u>Compute</u>
D = HASH(*Y*, salt k)

Transport
Identity *X*
Password *Y*

Input
Identity *X*
Password *Y*

DATABASE
ID *X*: k, D

Store identity, Salt, Hash

BASIC DATABASE OPERATIONS

- **SET –** Insert related data, usually with specific ***types***

EXAMPLE:

set(ID x, HASH D, SALT k)

Inserts (x, D, k) into the database

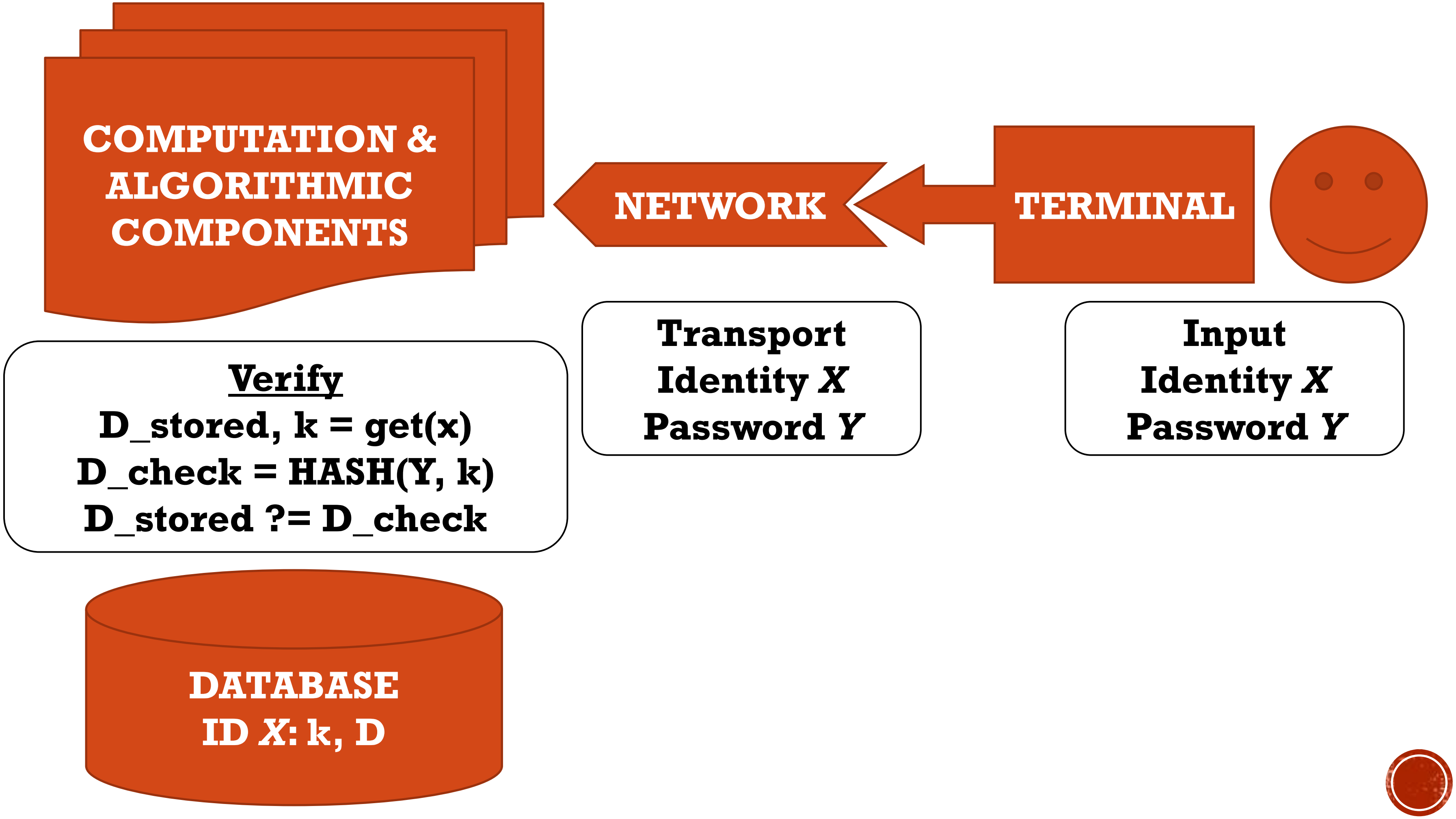
- **GET –** Retrieves related data, usually by specifying ***some*** values

EXAMPLE:

get(ID x) -> D, k

Queries (x) from the database to get D, k

PASSWORD VERIFICATION



COMPUTATION & ALGORITHMIC COMPONENTS

NETWORK

TERMINAL

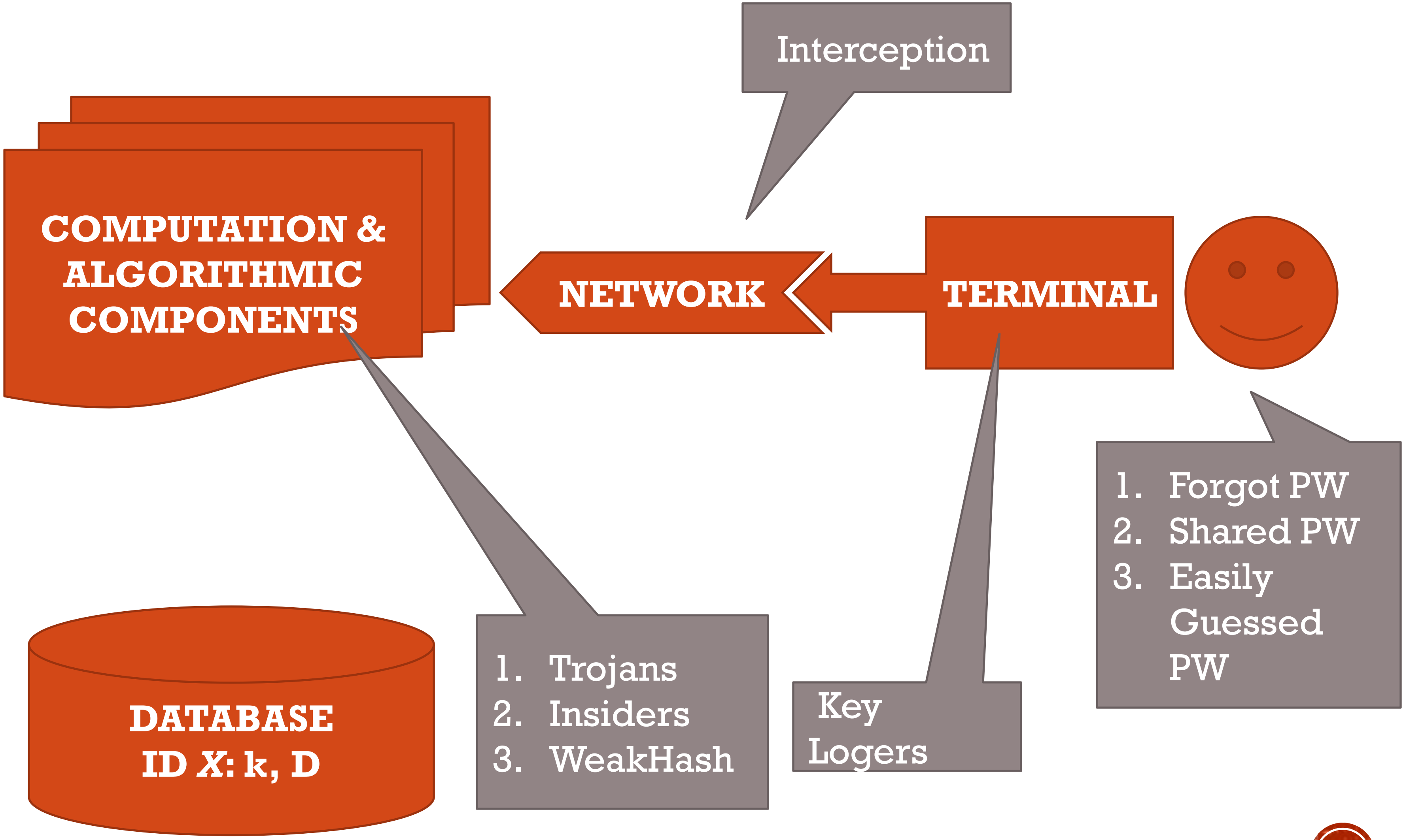
Verify
D_stored, k = get(x)
D_check = HASH(Y, k)
D_stored ?= D_check

Transport
Identity *X*
Password *Y*

Input
Identity *X*
Password *Y*

DATABASE
ID *X*: k, D

COMMON PROBLEMS



COMPUTATION & ALGORITHMIC COMPONENTS

NETWORK

TERMINAL

Interception

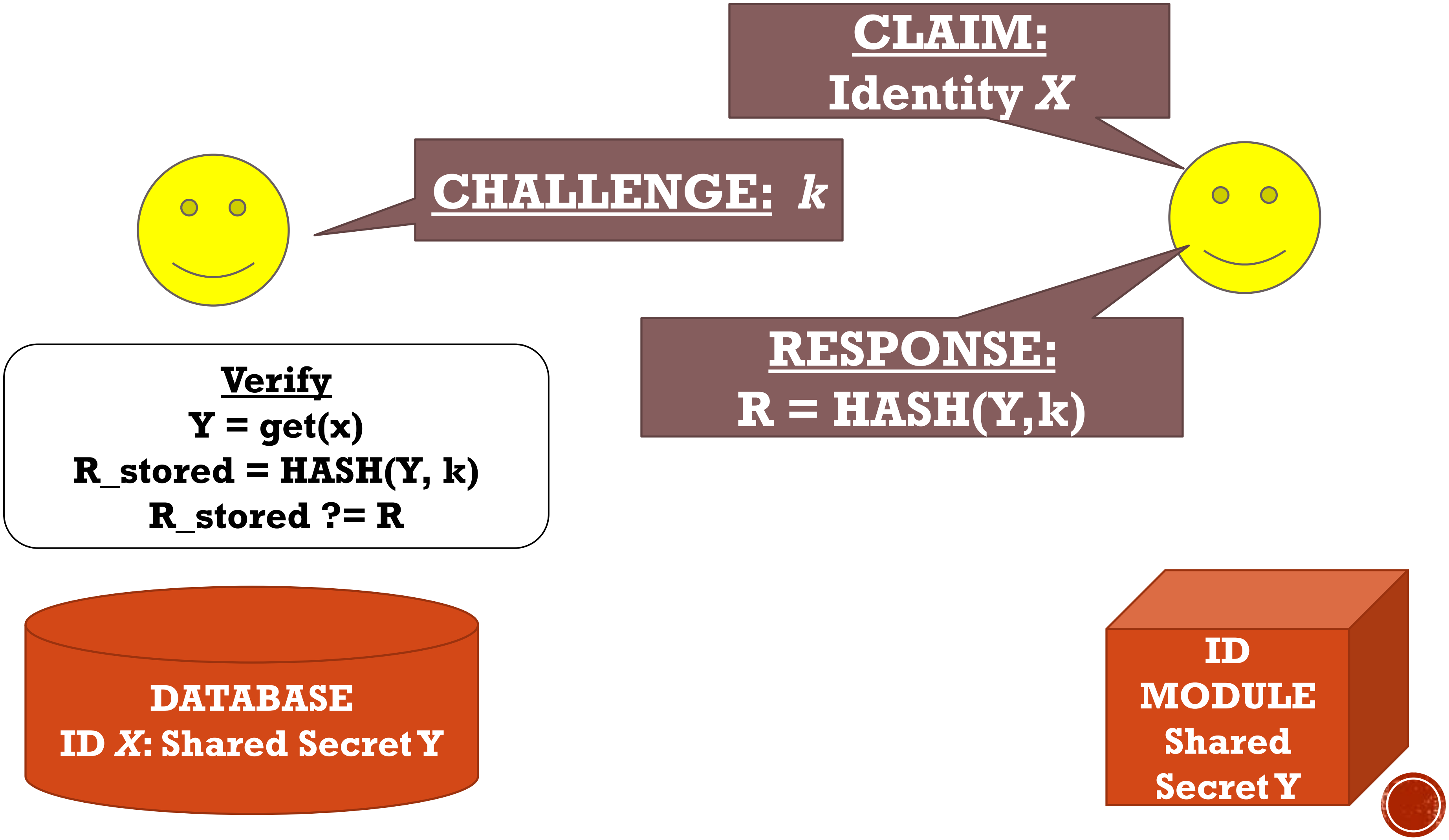
1. Trojans
2. Insiders
3. WeakHash

DATABASE
ID *X*: k, D

Key Logers

1. Forgot PW
2. Shared PW
3. Easily Guessed PW

CHECKING WITHOUT TRANSMITTING



CLAIM:
Identity *X*

CHALLENGE: *k*

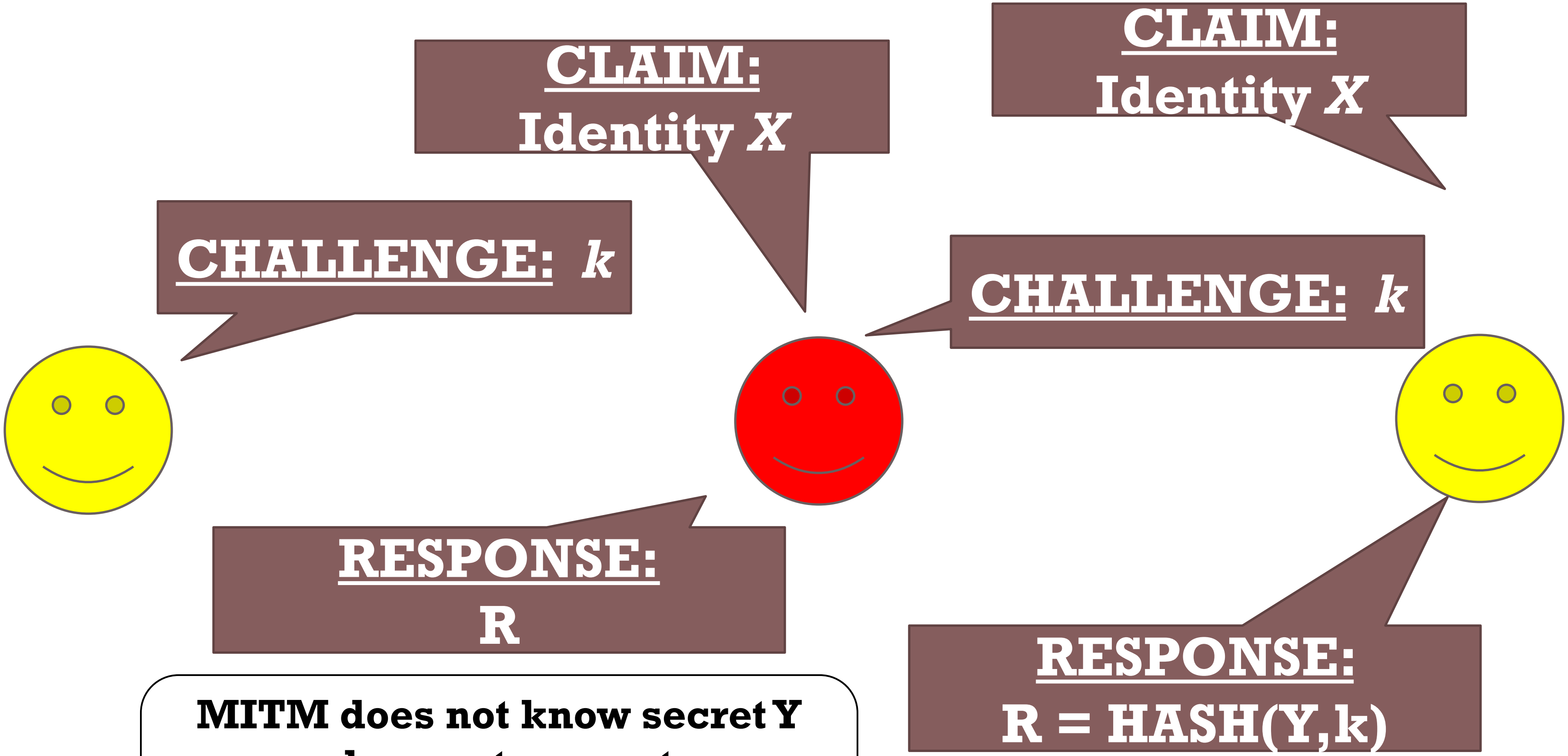
RESPONSE:
R = HASH(Y,k)

Verify
Y = get(x)
R_stored = HASH(Y, k)
R_stored ?= R

DATABASE
ID *X*: Shared Secret Y

ID
MODULE
Shared
Secret Y

MAN-IN-THE-MIDDLE (MITM)



CLAIM:
Identity *X*

CLAIM:
Identity *X*

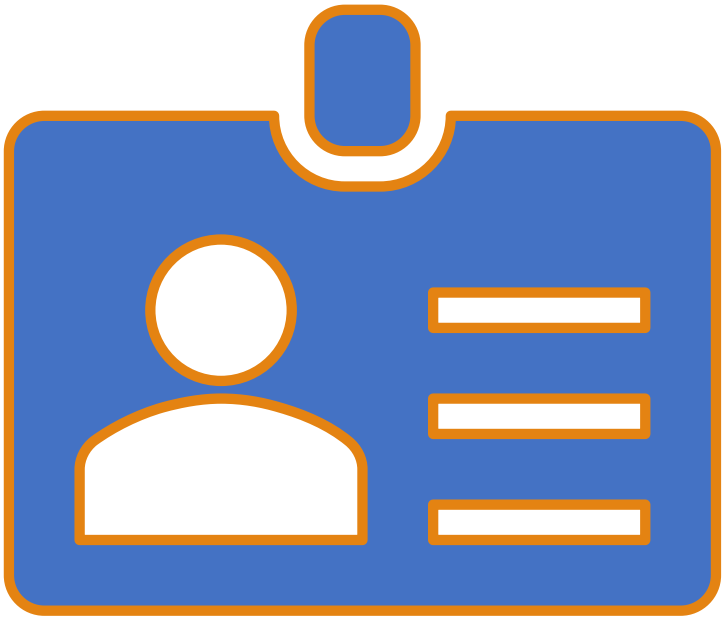
CHALLENGE: *k*

CHALLENGE: *k*

RESPONSE:
R

RESPONSE:
R = HASH(Y,k)

MITM does not know secret Y and cannot computer HASH(Y,k). MITM intercepts and transmits R

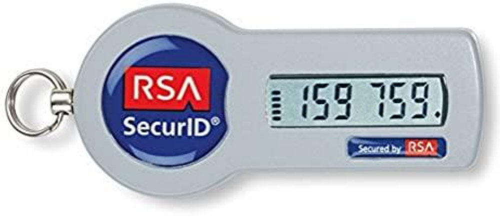


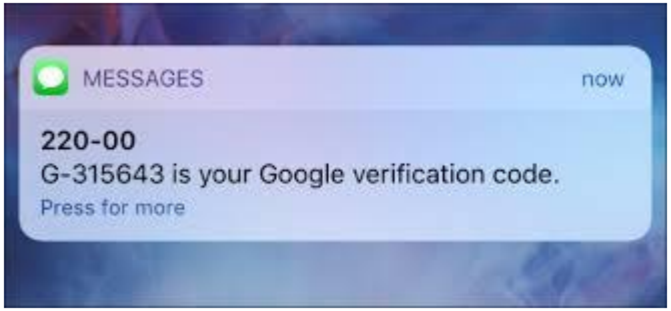
SOMETHING YOU HAVE

- Security Assumptions

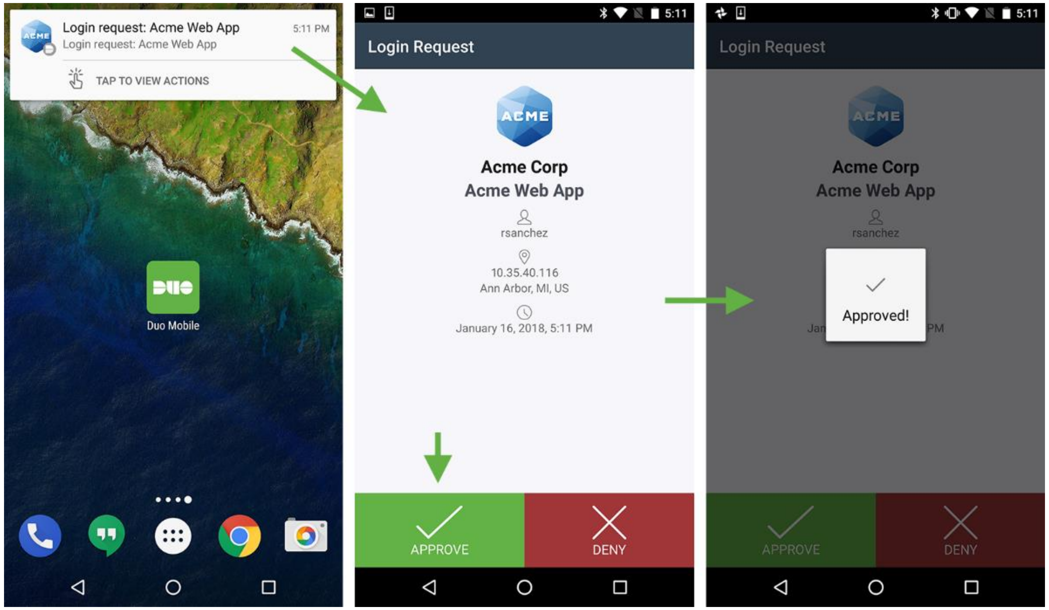
1. The “token” is ONLY possessed by the party seeking authentication
2. The token cannot be easily forged or duplicated
3. ***The authentication protocol is secure***

SOMETHING YOU HAVE EXAMPLES




MESSAGES now

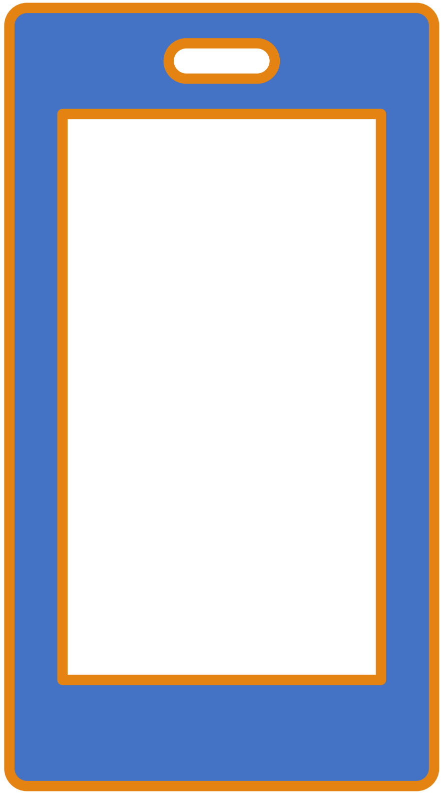
220-00
G-315643 is your Google verification code.
Press for more


Login request: Acme Web App 5:11 PM
Login request: Acme Web App
TAP TO VIEW ACTIONS

Login Request

Acme Corp
Acme Web App
rsanchez
10.35.40.116
Ann Arbor, MI, US
January 16, 2018, 5:11 PM

Approved!



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 some contexts, ***False Negatives*** can be 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**