Secure Software Systems

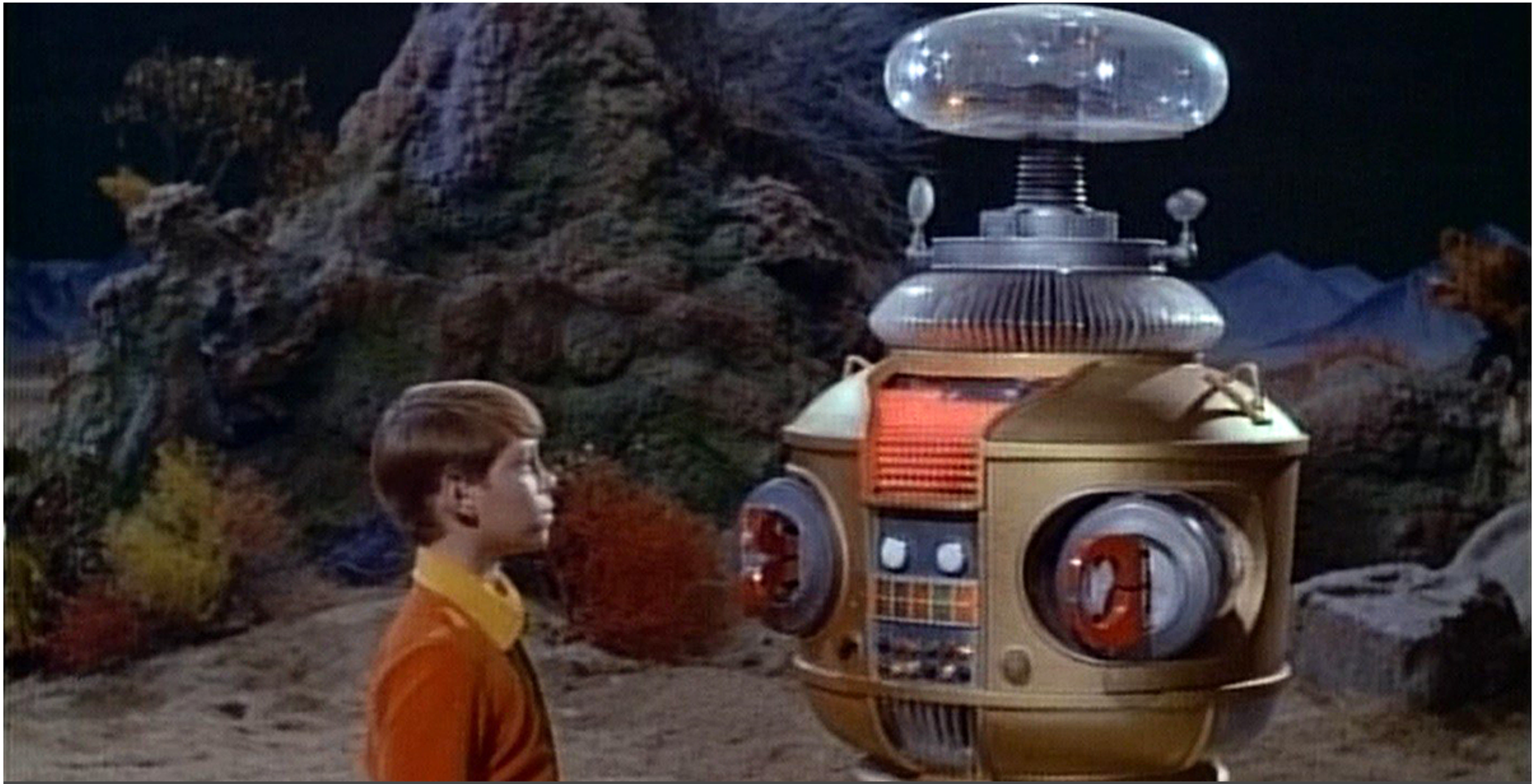
CYBR 200 | Fall 2018 | University of the Pacific | Jeff Shafer

Authentication

Content adapted from CS 5430 (System Security), Cornell University, Dr. Michael Clarkson

Authentication

- Authentication of Humans
- Passwords
- Tokens
- Certificates
- Bonus Round!
  - Second Factor Authentication
    - SMS, TOTP, FIDO U2F
  - Google Advanced Protection Program
  - OAuth / OpenID Connect
  - Kerberos

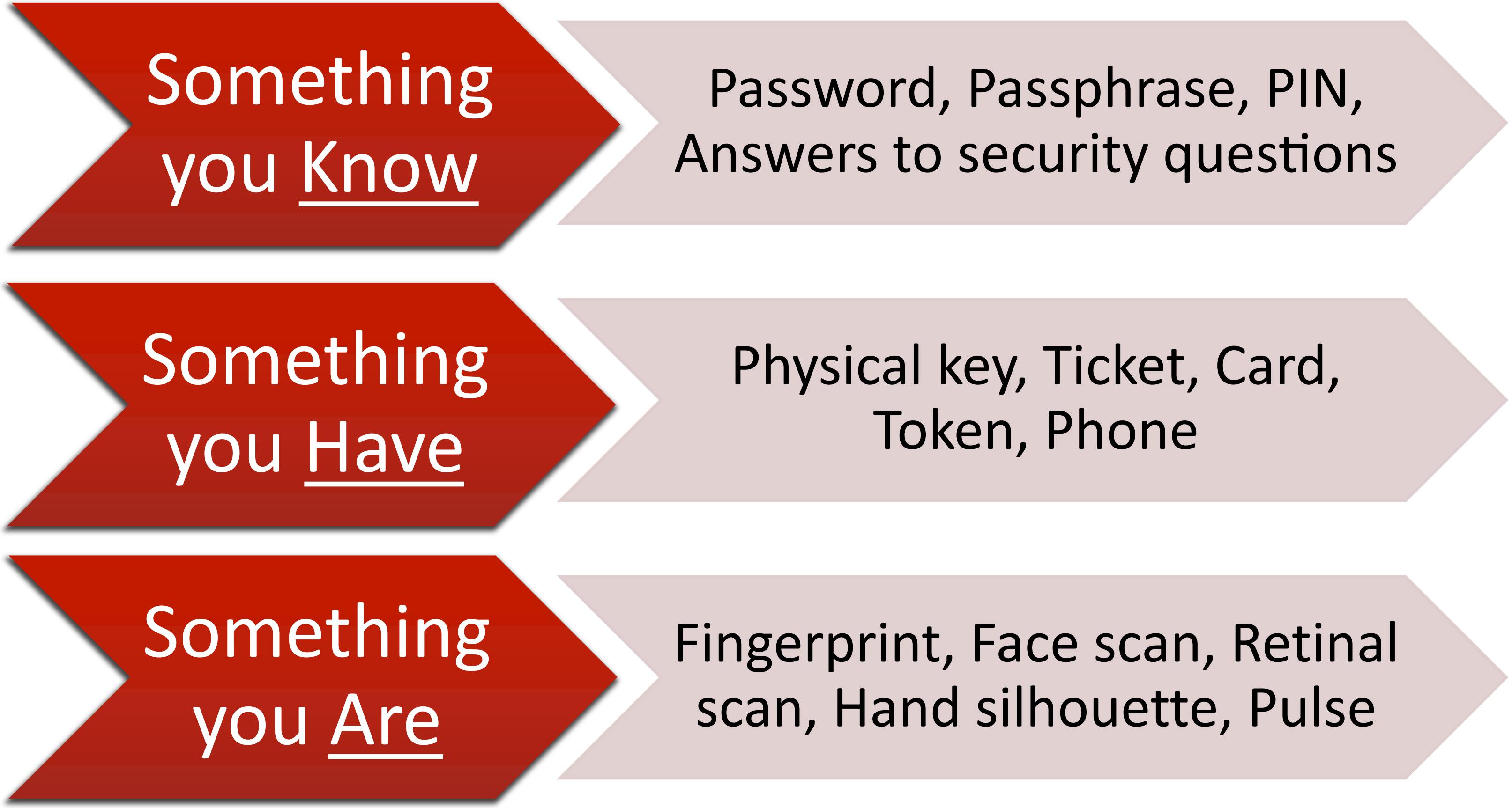


Authentication of Humans

> “Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy… They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.”

Charlie Kaufman, Radia Perlman and Mike Speciner
Network Security: Private Communication in a Public World (1995)

Authentication of Humans



Something you Know

Password, Passphrase, PIN, Answers to security questions

Something you Have

Physical key, Ticket, Card, Token, Phone

Something you Are

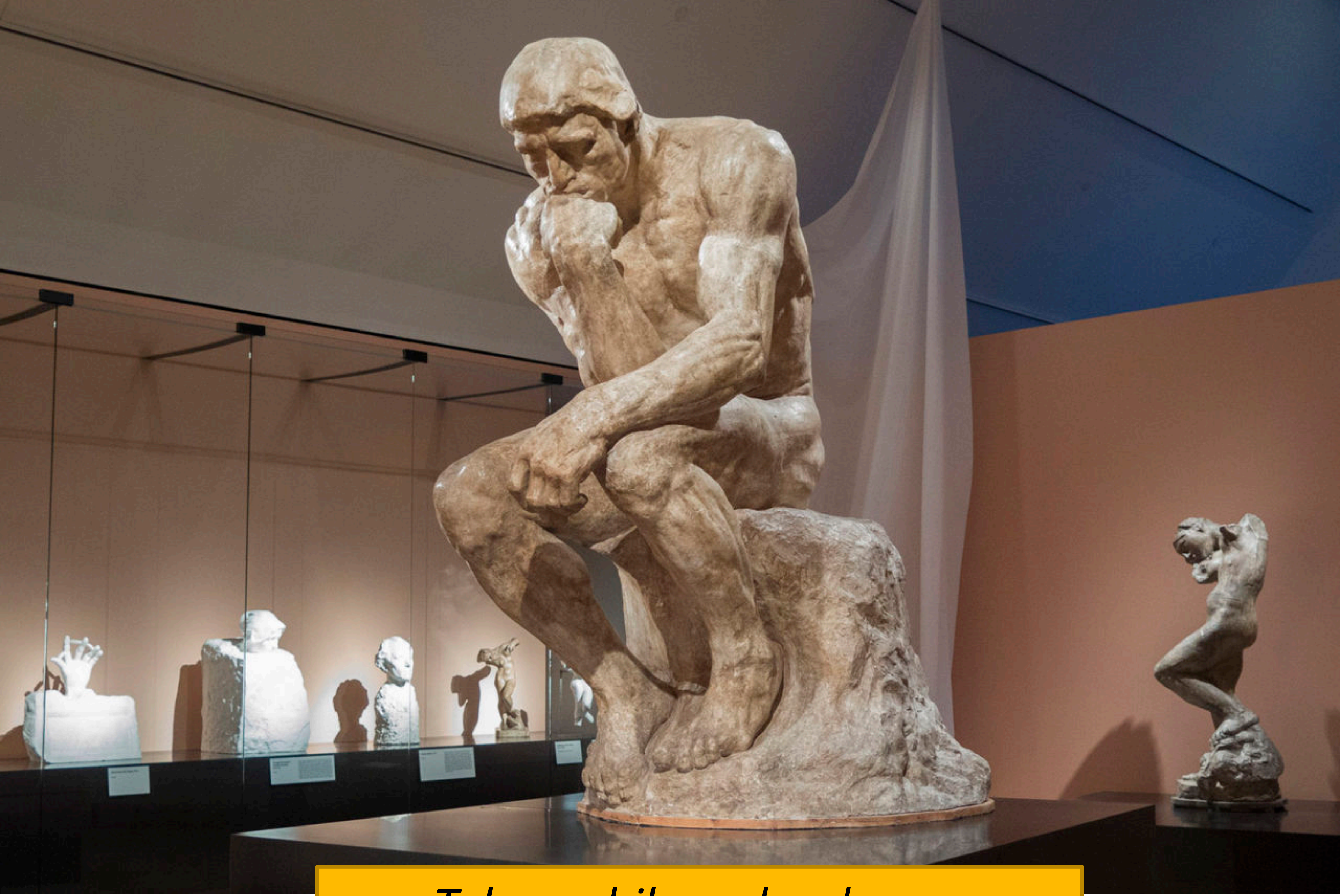
Fingerprint, Face scan, Retinal scan, Hand silhouette, Pulse

Authentication of Humans

- Two-factor authentication
  - Authenticate based on two <u>independent</u> methods
- Examples
  - Password (*know*) + Text msg to mobile phone (*have*)
  - ATM card (*have*) + PIN (*know*)
  - Eye scan (*are*) + PIN (*know*)
- Two factor is most useful when methods are independent, not from same category

Authentication of Humans

- What is being authenticated?
- What is *identity*, anyway?



Take a philosophy class....

Digital Identity

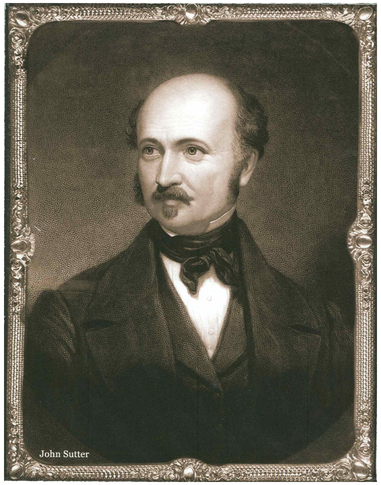
- Data that describes a person and their relationship to others
  - Not the person itself!
  - Could be fictional people, dead people, virtual people (AI)
- Person could have many digital identities
  - Some overlapping, some contradictory

Digital Identity

- Name
- NetID
- Email address
- URL
- IP address
- Citizenship
- Political party
- …

Identity

- **Attribute**: Property of a *principal*
  - *Name:* John Sutter
  - *DOB:* February 20, 1803
  - *Favorite Color:* Gold Gold Gold!



- **Identity**: Set of attributes
- **Identifier**: Attribute that is unique within a population
- **Verifier:** Attribute that is hard to produce, and can be used as basis for authentication

Identity

- Enrollment: Establishing identity within system
  - Create an account
  - Get an ID card
  - Register computer on network
  - …
- System might (or might not) verify claimed attributes during enrollment
  - Bank? Yes
  - Reddit? No