Challenge/Response Authentication

- Authentication by what questions you can answer correctly
  - Again, by what you know
- The system asks the user to provide some information
- If it's provided correctly, the user is authenticated

Differences From Passwords

- Challenge/response systems ask for different information every time
- Or at least the questions come from a large set
- Best security achieved by requiring what amounts to encryption of the challenge
  - But that requires special hardware
  - Essentially, a smart card

Challenge/Response Problems

- Either the question is too hard to answer without special hardware
- Or the question is too easy for intruders to spoof the answer
- Still, commonly used in real-world situations
  - E.g., authenticating you by asking your childhood pet's name
  - "Security questions" used as an alternative to passwords

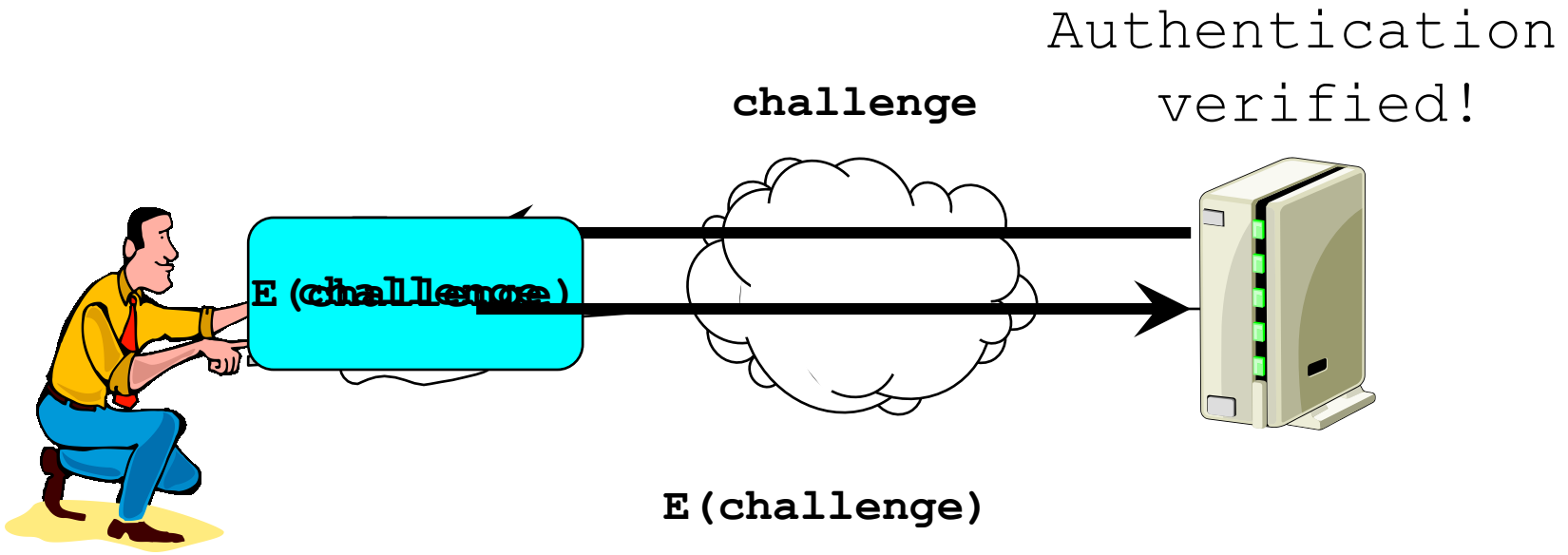
Identification Devices

- Authentication by what you have
- A smart card or other hardware device that is readable by the computer
- Authenticate by providing the device to the computer

Simple Use of Authentication Tokens

- If you have the token, you are identified
- Generally requires connecting the authentication device to computer
  - Unless done via wireless
- Weak, because it's subject to theft and spoofing
- How can we do better?

Authentication With Smart Cards



How can the server be sure of the remote user's identity?

Some Details on Smart Cards

- Cryptography performed only on smart card
  - So compromised client machine can't steal keys
- Often user must enter password to activate card
  - Should it be entered to the card or the computer?

Problems With Identification Devices

- If lost or stolen, you can't authenticate yourself
  - And maybe someone else can
  - Often combined with passwords to avoid this problem
- Unless cleverly done, susceptible to sniffing attacks
- Requires special hardware

Attacks on Smart Cards

- Often based on fake terminals
  - E.g., fake or altered ATM machine
- Ideally, card shouldn't respond to fake or tampered terminal
- Alas, they often do
  - European Chip & Pin standard broken in 2011, for example

Another Form of Attack

- Smart cards sometimes used to protect or hide stuff from the card's owner
- E.g., smart cards that allow access to rapid transit systems
- Owner has total access
- Some attacks based on hacking card hardware
  - Recent research makes this more feasible
- Or observing card behavior

Authentication Through Biometrics

- Authentication based on who you are
- Things like fingerprints, voice patterns, retinal patterns, etc.
- To authenticate to the system, allow system to measure the appropriate physical characteristics
- Biometric converted to binary and compared to stored values
  - With some level of match required

Problems With Biometric Authentication

- Requires very special hardware
  - Except systems that use typing patterns
- May not be as foolproof as you think
- Many physical characteristics vary too much for practical use
- Generally not helpful for authenticating programs or roles
- What happens when it's cracked?
  - You only have two retinas, after all

When Do Biometrics (Maybe) Work Well?

- When you use them for authentication
  - Carefully obtain clean readings from legitimate users
  - Compare those to attempts to authenticate
- When biometric readers are themselves secure
- In conjunction with other authentication

When Do Biometrics (Definitely) Work Poorly?

- Finding "needles in haystacks"
  - Face recognition of terrorists in airports
- When working off low-quality readings
- When the biometric reader is easy to bypass or spoof
  - Anything across a network is suspect
- When the biometric is "noisy"
  - Too many false negatives

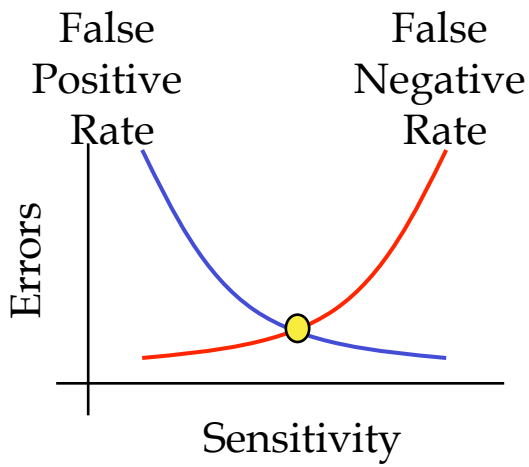
Characterizing Biometric Accuracy

How many false positives?

Match made when it shouldn't have been

Versus how many false negatives?

Match not made when it should have been



The Crossover Error Rate (CER)

Generally, the lower the CER is, the better the system

But sometimes one rate more important than the other

Some Typical Crossover Error Rates

Technology	Rate
Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Facial Recognition	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50

Data as of 2002

- Things can improve a lot in this area over time
- Also depends on how you use them
- And on what's important to your use

Biometrics and Usability

- Always a tradeoff in false positives vs. false negatives
- For consumer devices, false negatives are very, very bad
  - People discard devices that won't let the legitimate user in
- Can you make the false positive rate non-trivial with almost no false negs?

Didn't Carnegie Mellon Just Perfect Facial Recognition?

- Not really
- Quick and dirty version got 1 in 3 right
- With more photos and time, did better
- But think about how accurate your use of biometrics needs to be
- In many cases, you need 5 nines or so

Another Cautionary Tale

- British cameras captured faces of many rioters in London in 2011
- Tried to use facial recognition software to automatically identify them
- Very poor results, in terms of accuracy
  - Because camera images were of poor quality
- Current technology requires good image quality

Authentication by Where You Are

- Sometimes useful in ubiquitous computing
- The issue is whether the message in question is coming from the machine that's nearby
- Less important who owns that machine
- Requires sufficient proof of physical location
- And ability to tie a device at that location to its messages
- Sometimes used in conjunction with other authentication methods
  - E.g., the door opens only if an authorized user is right outside it