Password Cracking: Do the Math

- Assumptions
- Pwds are 8 chars, 128 choices per character
  - Then $128^8 = 2^{56}$ possible passwords
- There is a **password file** with 2^{10} pwds
- Attacker has **dictionary** of 2^{20} common pwds
- Probability of 1/4 that a pwd is in dictionary
- **Work** is measured by number of hashes

Password Cracking

- Attack 1 password without dictionary
  - Must try $2^{56}/2 = 2^{55}$ on average
  - Just like exhaustive key search
- Attack 1 password with dictionary
  - Expected work is about

$$1/4\,(2^{19}) + 3/4\,(2^{55}) \approx 2^{54.6}$$

  - But in practice, try all in dictionary and quit if not found —work is at most 2^{20} and probability of success is 1/4

Password Cracking

- Attack any of 1024 passwords in file
- **Without** dictionary
  - Assume all 2^{10} passwords are distinct
  - Need 2^{55} comparisons before expect to find password
  - If no salt, each hash computation gives 2^{10} comparisons $\Rightarrow$ the expected work (number of hashes) is $2^{55}/2^{10} = 2^{45}$
  - If salt is used, expected work is 2^{55} since each comparison requires a new hash computation

Password Cracking

- Attack any of 1024 passwords in file
- **With** dictionary
  - Probability at least one password is in dictionary is $1 - (3/4)^{1024} = 1$
  - We ignore case where no pwd is in dictionary
  - If no salt, work is about $2^{19}/2^{10} = 2^9$
  - If salt, expected work is less than 2^{22}
  - Note: If no salt, we can precompute all dictionary hashes and amortize the work

Other Password Issues

- Too many passwords to remember
  - Results in password reuse
  - Why is this a problem?
- Who suffers from bad password?
  - Login password vs ATM PIN
- Failure to change default passwords
- Social engineering
- Error logs may contain "almost" passwords
- Bugs, keystroke logging, spyware, etc.

Passwords

- The bottom line
- **Password cracking is too easy!**
  - One weak password may break security
  - Users choose bad passwords
  - Social engineering attacks, etc.
- The bad guy has all of the advantages
- All of the math favors bad guys
- Passwords are a **big** security problem

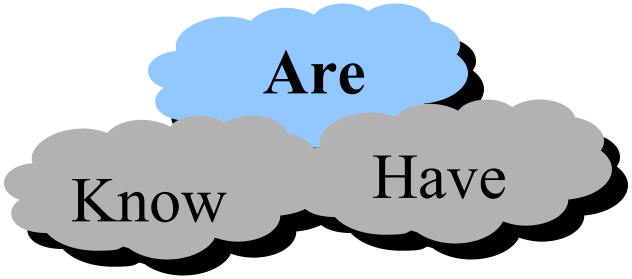
Password Cracking Tools

- Popular password cracking tools
  - Password Crackers
  - Password Portal
  - L0phtCrack and LC4 (Windows)
  - John the Ripper (Unix)
- Admins should use these tools to test for weak passwords since attackers will!
- Good article on password cracking
  - Passwords - Conerstone of Computer Security

Biometrics

Something You Are

- Biometric
  - **"You are your key"** —Schneier
- Examples
  - Fingerprint
  - Handwritten signature
  - Facial recognition
  - Speech recognition
  - Gait (walking) recognition
  - "Digital doggie" (odor recognition)
  - Many more!



Why Biometrics?

- Biometrics seen as desirable replacement for passwords
- Cheap and reliable biometrics needed
- Today, a very active area of research
- Biometrics are used in security today
  - Thumbprint mouse
  - Palm print for secure entry
  - Fingerprint to unlock car door, etc.
- But biometrics not too popular
  - Has not lived up to its promise (yet)

Ideal Biometric

- **Universal** — applies to (almost) everyone
  - In reality, no biometric applies to everyone
- **Distinguishing** — distinguish with certainty
  - In reality, cannot hope for 100% certainty
- **Permanent** — physical characteristic being measured never changes
  - In reality, want it to remain valid for a long time
- **Collectable** — easy to collect required data
  - Depends on whether subjects are cooperative
- Safe, easy to use, etc., etc.

Biometric Modes

- **Identification** — Who goes there?
  - Compare one to many
  - Example: The FBI fingerprint database
- **Authentication** — Is that really you?
  - Compare one to one
  - Example: Thumbprint mouse
- Identification problem more difficult
  - More "random" matches since more comparisons
- We are interested in authentication

Enrollment vs Recognition

- Enrollment phase
  - Subject's biometric info put into database
  - Must carefully measure the required info
  - OK if slow and repeated measurement needed
  - Must be very precise for good recognition
  - A weak point of many biometric schemes
- Recognition phase
  - Biometric detection when used in practice
  - Must be quick and simple
  - But must be reasonably accurate

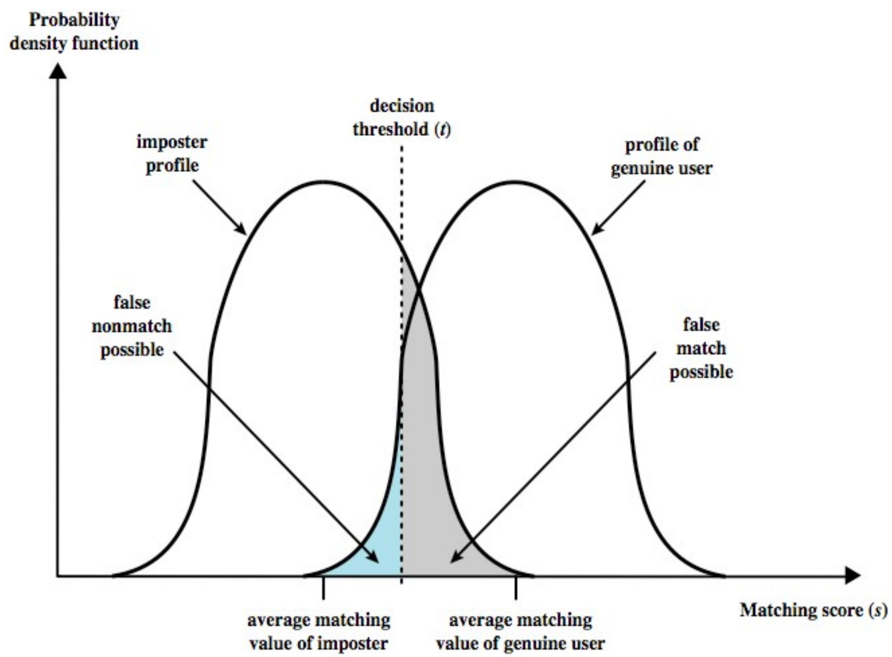
Cooperative Subjects

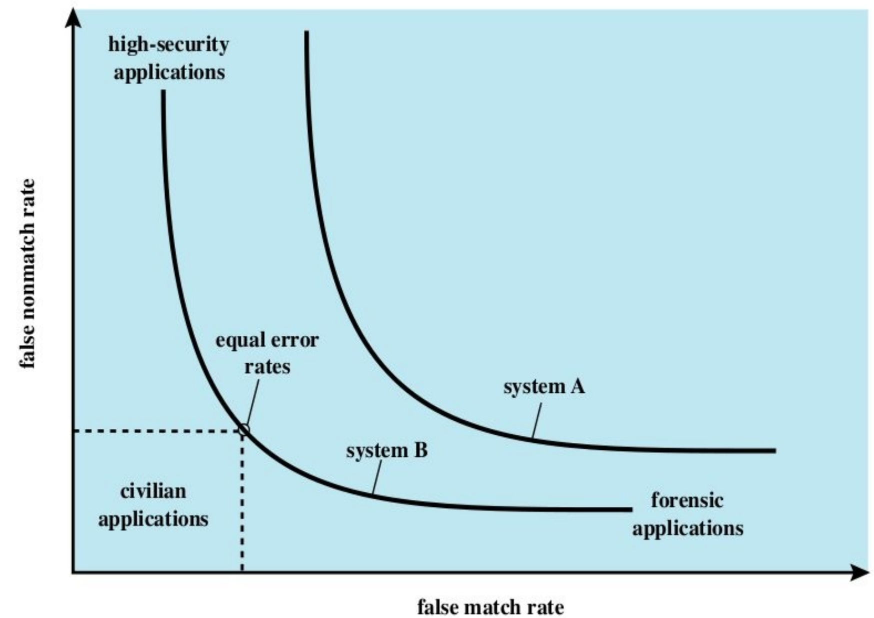
- We are assuming cooperative subjects
- In identification problem often have uncooperative subjects
- For example, facial recognition
  - Proposed for use in Las Vegas casinos to detect known cheaters
  - Also as way to detect terrorists in airports, etc.
  - Probably do not have ideal enrollment conditions
  - Subject will try to confuse recognition phase
- Cooperative subject makes it much easier!
  - In authentication, subjects are cooperative

Biometric Errors

- **Fraud rate** versus **insult rate**
- **(false match X false nonmatch)**
  - Fraud — user A mis-authenticated as user B
  - Insult — user A not authenticate as user A
- For any biometric, can decrease fraud or insult, but other will increase
- For example
  - 99% voiceprint match $\Rightarrow$ low fraud, high insult
  - 30% voiceprint match $\Rightarrow$ high fraud, low insult
- **Equal error rate:** rate where fraud == insult
  - The best measure for comparing biometrics

Biometric Errors





From Computer Security , Principles and Practice by William Stallings, Prentice Hall 2007

Fingerprint History

- 1823 — Professor Johannes Evangelist Purkinje discussed 9 fingerprint patterns
- 1856 — Sir William Hershel used fingerprint (in India) on contracts
- 1880 — Dr. Henry Faulds article in *Nature* about fingerprints for ID
- 1883 — Mark Twain's *Life on the Mississippi* a murderer ID'ed by fingerprint

Fingerprint History

- 1888 — Sir Francis Galton (cousin of Darwin) developed classification system
  - His system of "minutia" is still in use today
  - Also verified that fingerprints do not change
- Some countries require a number of points (i.e., minutia) to match in criminal cases
  - In Britain, 15 points
  - In US, no fixed number of points required

Fingerprint Comparison

- Examples of loops, whorls and arches
- Minutia extracted from these features

Loop (double)

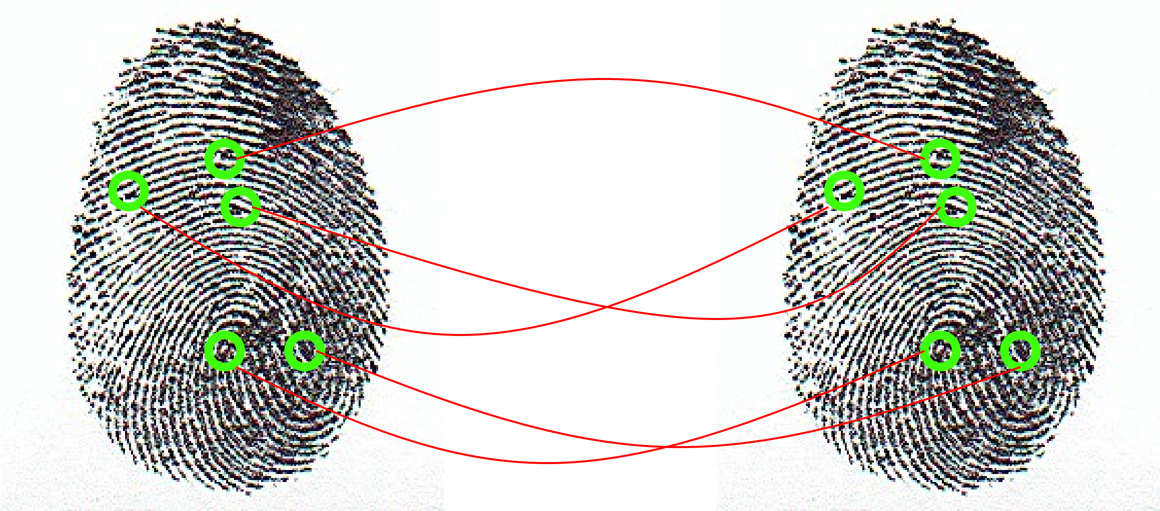
Whorl

Arch

Fingerprint Biometric

- Capture image of fingerprint
- Enhance image
- Identify minutia

Fingerprint Biometric



- Extracted minutia are compared with user's minutia stored in a database
- Is it a statistical match?

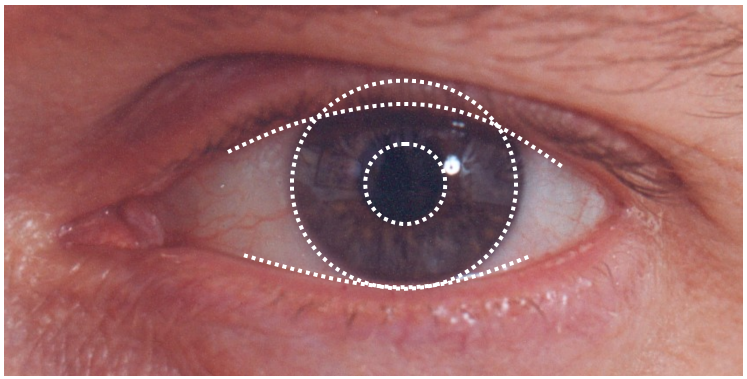
Hand Geometry

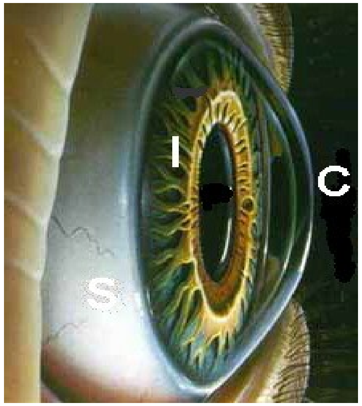
- Popular form of biometric
- Measures shape of hand
  - Width of hand, fingers
  - Length of fingers, etc.
- Human hands not unique
- Hand geometry sufficient for many situations
- Suitable for authentication
- Not useful for ID problem

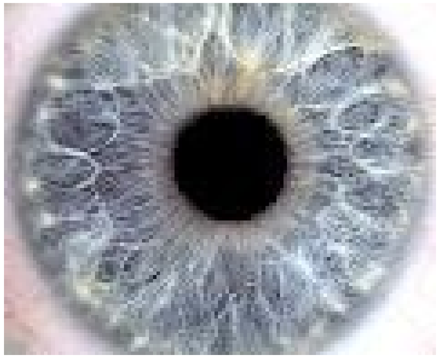
Hand Geometry

- Advantages
  - Quick
  - 1 minute for enrollment
  - 5 seconds for recognition
  - Hands symmetric (use other hand backwards)
- Disadvantages
  - Cannot use on very young or very old
  - Relatively high equal error rate

Iris Patterns







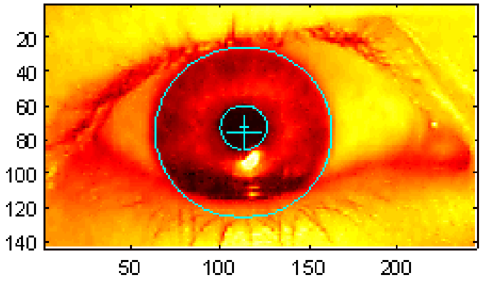
- Iris pattern development is "chaotic"
- Little or no genetic influence
- Different even for identical twins
- Pattern is stable through lifetime

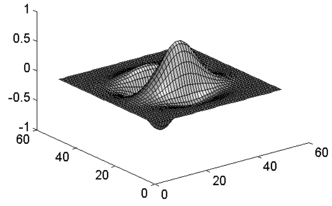
Iris Recognition: History

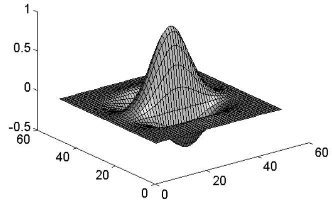
- 1936 — suggested by Frank Burch
- 1980s — James Bond films
- 1986 — first patent appeared
- 1994 — John Daugman patented best current approach
  - Patent owned by Iridian Technologies

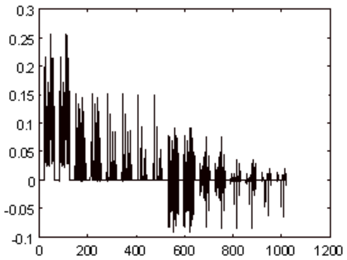
Iris Scan

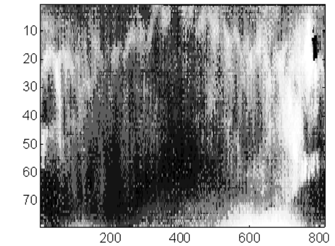
- Scanner locates iris
- Take b/w photo
- Use polar coordinates…
- Find 2-D wavelet trans
- Get 256 byte iris code











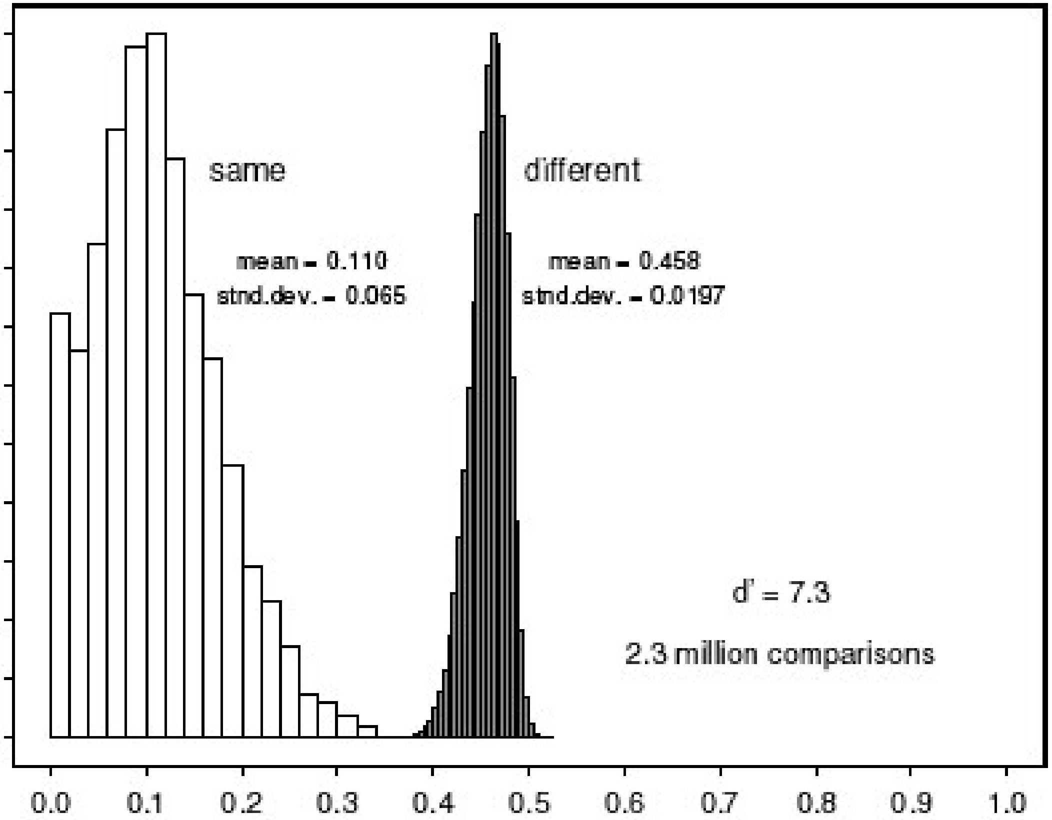
Measuring Iris Similarity

- Based on Hamming distance
- Define $d(x,y)$ to be
  - \# of non match bits/# of bits compared
  - $d(0010,0101) = 3/4$ and $d(101111,101001) = 1/3$
- Compute $d(x,y)$ on 2048-bit iris code
  - Perfect match is $d(x,y) = 0$
  - For same iris, expected distance is 0.08
  - At random, expect distance of 0.50
  - Accept as match if distance less than 0.32

Iris Scan Error Rate

distance	Fraud rate
0.29	1 in $1.3*10^{10}$
0.30	1 in $1.5*10^{9}$
0.31	1 in $1.8*10^{8}$
0.32	1 in $2.6*10^{7}$
0.33	1 in $4.0*10^{6}$
0.34	1 in $6.9*10^{5}$
0.35	1 in $1.3*10^{5}$

: equal error rate



distance

Attack on Iris Scan

- Good **photo** of eye can be scanned
  - Attacker could use photo of eye
- Afghan woman was authenticated by iris scan of old photo
  - Story is here
- To prevent photo attack, scanner could use light to be sure it is a "live" iris

Equal Error Rate Comparison

- Equal error rate (EER): fraud == insult rate
- **Fingerprint** biometric has EER of about 5%
- **Hand geometry** has EER of about 10^{-3}
- In theory, **iris scan** has EER of about 10^{-6}
  - But in practice, hard to achieve
  - Enrollment phase must be extremely accurate
- Most biometrics much worse than fingerprint!
- Biometrics useful for authentication…
- But ID biometrics are almost useless today

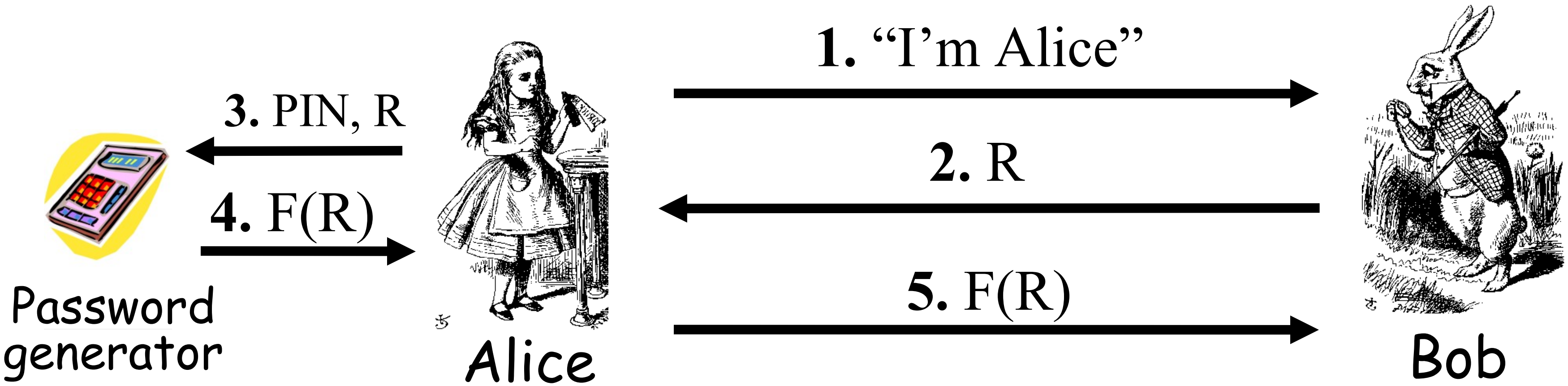
Biometrics: The Bottom Line

- Biometrics are hard to forge
- But attacker could
  - Steal Alice's thumb
  - Photocopy Bob's fingerprint, eye, etc.
  - Subvert software, database, "trusted path", …
- Also, how to revoke a "broken" biometric?
- **Biometrics are not foolproof!**
- Biometric use is limited today
- That should change in the future…

Something You Have

- Something in your possession
- Examples include
  - Car key
  - Laptop computer
    - Or specific MAC address
  - Password generator
    - We'll look at this next
  - ATM card, smartcard, etc.

Password Generator



- Alice gets "challenge" R from Bob
- Alice enters R into password generator
- Alice sends "response" back to Bob
- Alice **has** pwd generator and **knows** PINs

2-factor Authentication

- Requires 2 out of 3 of
  1. Something you know
  2. Something you have
  3. Something you are
- Examples
  - ATM: Card and PIN
  - Credit card: Card and signature
  - Password generator: Device and PIN
  - Smartcard with password/PIN

Single Sign-on

- A hassle to enter password(s) repeatedly
  - Users want to authenticate only once
  - "Credentials" stay with user wherever he goes
  - Subsequent authentication is transparent to user
- Single sign-on for the Internet?
  - Microsoft: **Passport**
  - Everybody else: **Liberty Alliance**
  - Security Assertion Markup Language (**SAML**)

Web Cookies

- Cookie is provided by a Website and stored on user's machine
- Cookie indexes a database at Website
- Cookies **maintain state** across sessions
- Web uses a stateless protocol: HTTP
- Cookies also maintain state within a session
- Like a single sign-on for a website
  - Though a very weak form of authentication
- Cookies and privacy concerns

Next …
Chapter 8
Authorization