CS 114: Network Security

Lecture 7 - Authentication Part I

Prof. Daniel Votipka
Spring 2023

(some slides courtesy of Prof. Micah Sherr, Patrick McDaniel, and Vitaly Shmatikov)

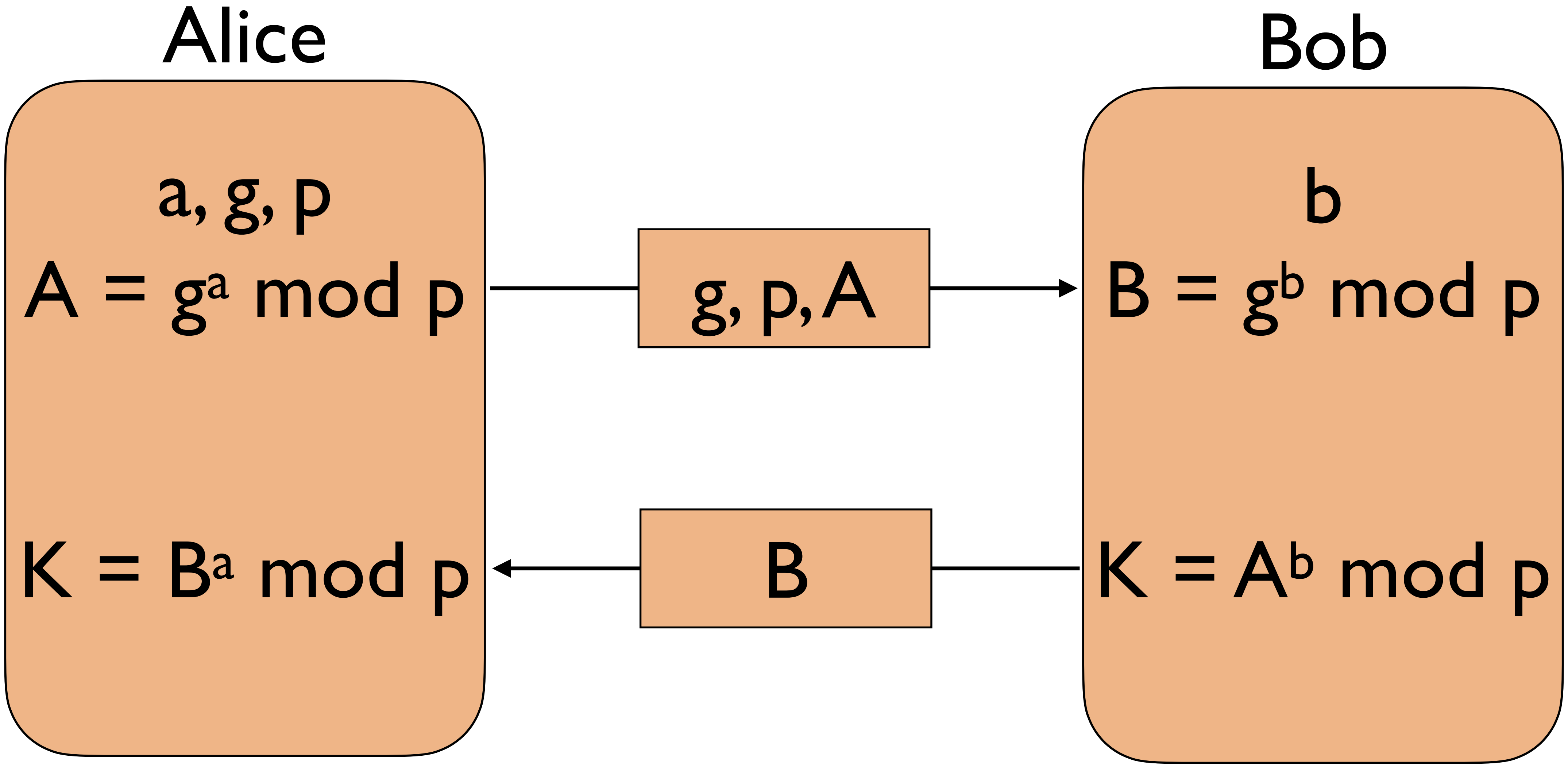
Tufts
UNIVERSITY

Key Distribution and Key Agreement

- **Key Distribution** is the process where we assign and transfer keys to a participant
- **Key Agreement** is the process whereby two or more parties negotiate a key

Diffie-Hellman (DH) Key Agreement

- Proposed by Whitfield Diffie and Martin Hellman in 1976
- g=base, p=prime, a=Alice's secret, b=Bob's secret
- Eve cannot compute K without knowing either a or b (neither of which is transmitted), even if she (passively) intercepts all communication!



Alice

a, g, p

$A = g^a \bmod p$

$K = B^a \bmod p$

g, p, A

B

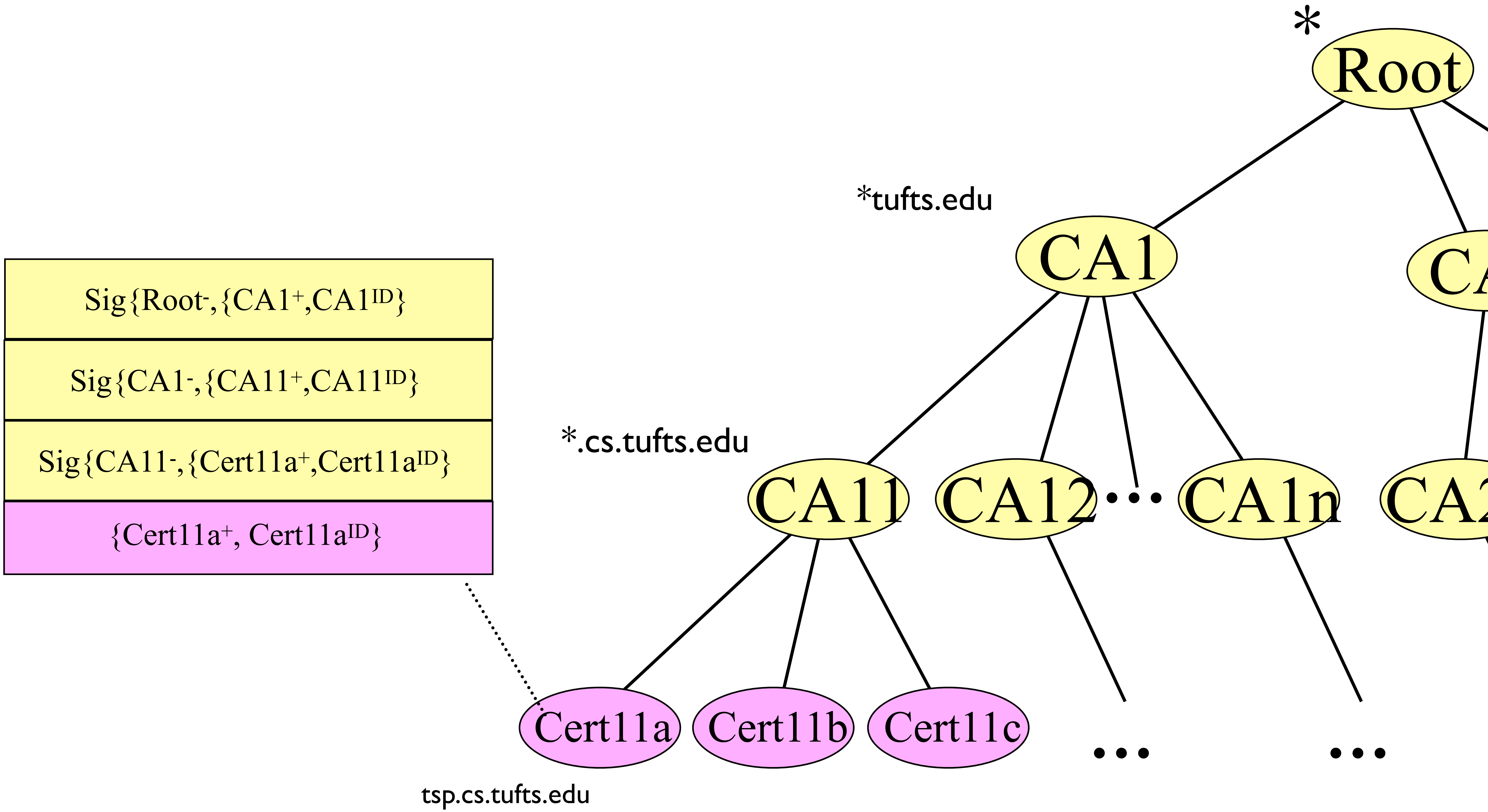
Bob

b

$B = g^b \bmod p$

$K = A^b \bmod p$

Certificate Validation



Sig{Root$^-$,{CA1$^+$,CA1^{ID}}

Sig{CA1$^-$,{CA11$^+$,CA11^{ID}}

Sig{CA11$^-$,{Cert11a$^+$,Cert11a^{ID}}

{Cert11a$^+$, Cert11a^{ID}}

Meta-Issue:
How much should we trust CAs?

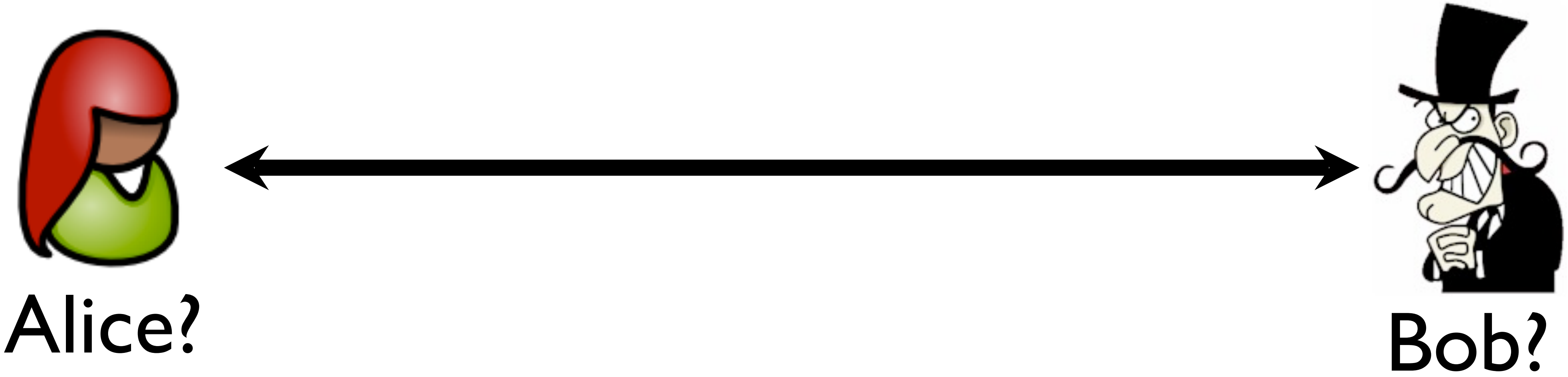
- Revocation is hard
- Any CA may sign any certificate

60% not revoked

20% 2 yrs+ TTL

"Analysis of SSL Certificate Reissues and Revocations in the Wake of Heartbleed", Zhang et. al., IMC '14

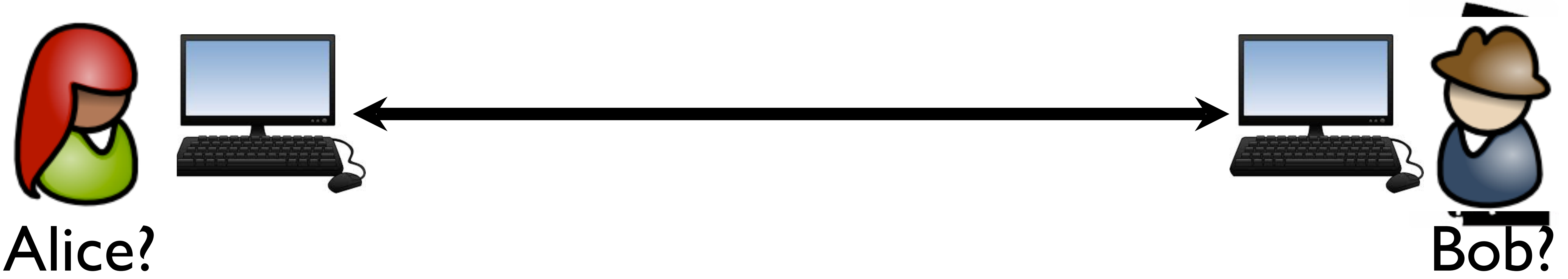
Authentication



Alice?

Bob?

Authentication

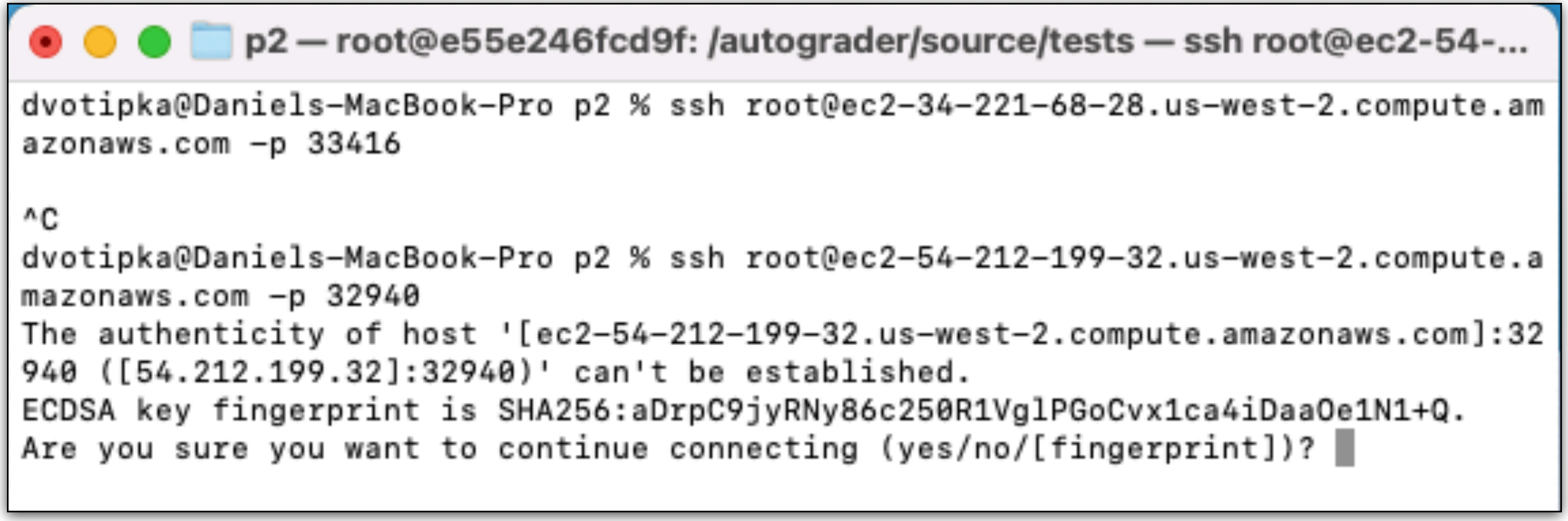


What is Authentication?

- Establishes identity
  - Answers the question: To whom am I speaking?
  - Credential – proof of identity
  - Evaluation – process that assesses the correctness of the association between credential and claimed identity

- **Computer security is critically dependent on the proper design, management, and application of authentication systems**

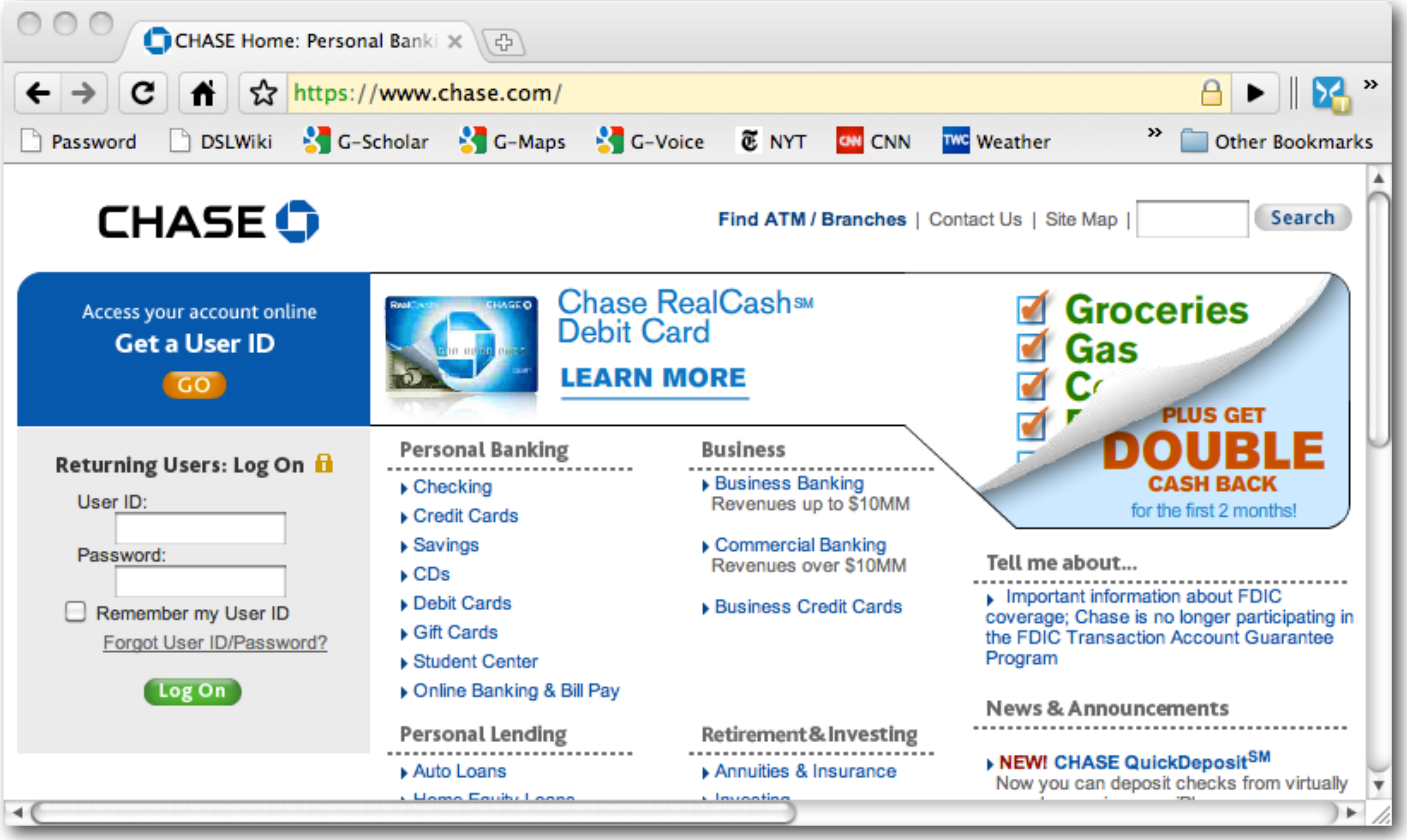
What are the consequences of getting this wrong?


p2 — root@e55e246fcd9f: /autograder/source/tests — ssh root@ec2-54-...

```
dvotipka@Daniels-MacBook-Pro p2 % ssh root@ec2-34-221-68-28.us-west-2.compute.am
azonaws.com -p 33416

^C
dvotipka@Daniels-MacBook-Pro p2 % ssh root@ec2-54-212-199-32.us-west-2.compute.a
mazonaws.com -p 32940
The authenticity of host '[ec2-54-212-199-32.us-west-2.compute.amazonaws.com]:32
940 ([54.212.199.32]:32940)' can't be established.
ECDSA key fingerprint is SHA256:aDrpC9jyRNy86c250R1VglPGoCvx1ca4iDaaOe1N1+Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

What are the consequences of getting this wrong?



CHASE

Find ATM / Branches | Contact Us | Site Map | Search

Access your account online

Get a User ID

GO

Chase RealCash℠ Debit Card

LEARN MORE

☑ Groceries
☑ Gas
☑ C

PLUS GET DOUBLE CASH BACK for the first 2 months!

Returning Users: Log On

User ID:

Password:

□ Remember my User ID

Forgot User ID/Password?

Log On

Personal Banking

- Checking
- Credit Cards
- Savings
- CDs
- Debit Cards
- Gift Cards
- Student Center
- Online Banking & Bill Pay

Personal Lending

- Auto Loans
- Home Equity Loans

Business

- Business Banking
  Revenues up to $10MM
- Commercial Banking
  Revenues over $10MM
- Business Credit Cards

Retirement & Investing

- Annuities & Insurance
- Investing

Tell me about...

- Important information about FDIC coverage; Chase is no longer participating in the FDIC Transaction Account Guarantee Program

News & Announcements

- NEW! CHASE QuickDeposit℠
  Now you can deposit checks from virtually

Three Flavors of Credentials

- … are evidence used to prove identity
- Credentials can be

1. **Something I am**
2. **Something I know**
3. **Something I have**

Credential: Something I Am

Credential:
Something I am.

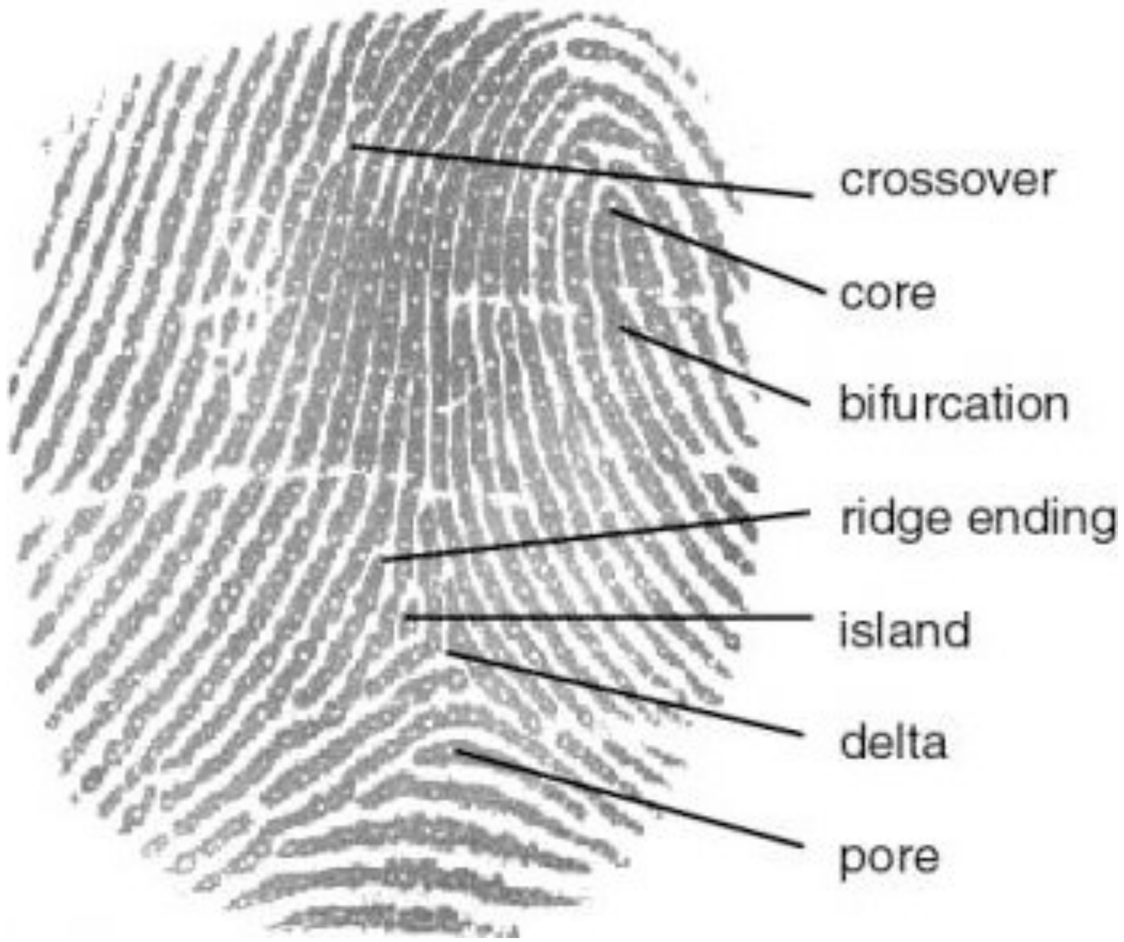
But how do you prove who you are in the digital world?

Biometrics

- Biometrics measure some physical characteristic
  - Fingerprint, face recognition, retina scanners, voice, signature, DNA
  - Can be extremely accurate and fast
- Issues with biometrics?
  - Revocation – lost fingerprint?
  - “Fuzzy” credential, e.g., your face changes based on mood
  - Privacy?

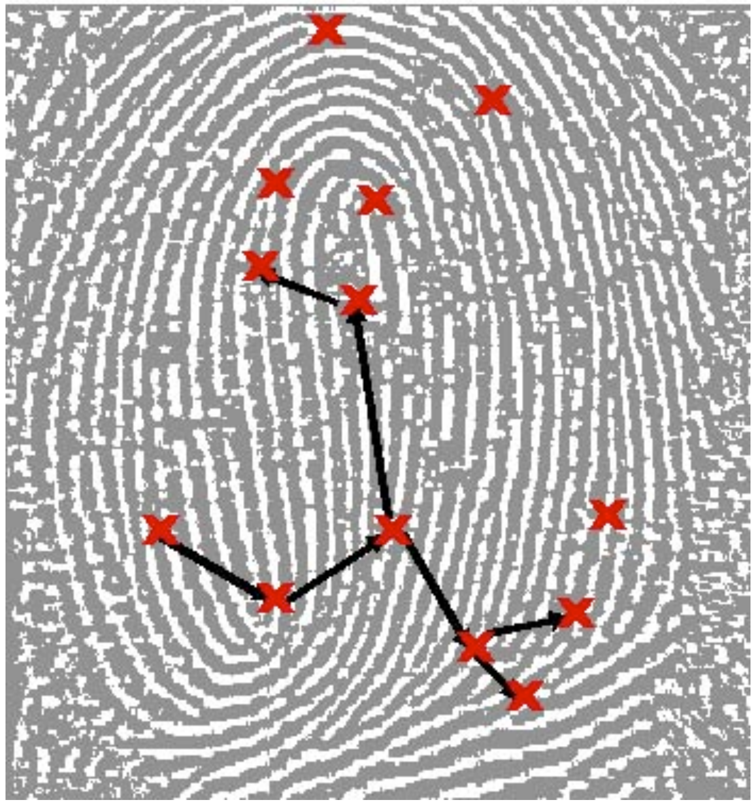
Biometrics Example

- Fingerprint readers record the conductivity of the surface of your finger to build a "map" of the ridges
- Scanned map converted into a graph by looking for landmarks, e.g., ridges, cores, ...



Fingerprint Biometrics

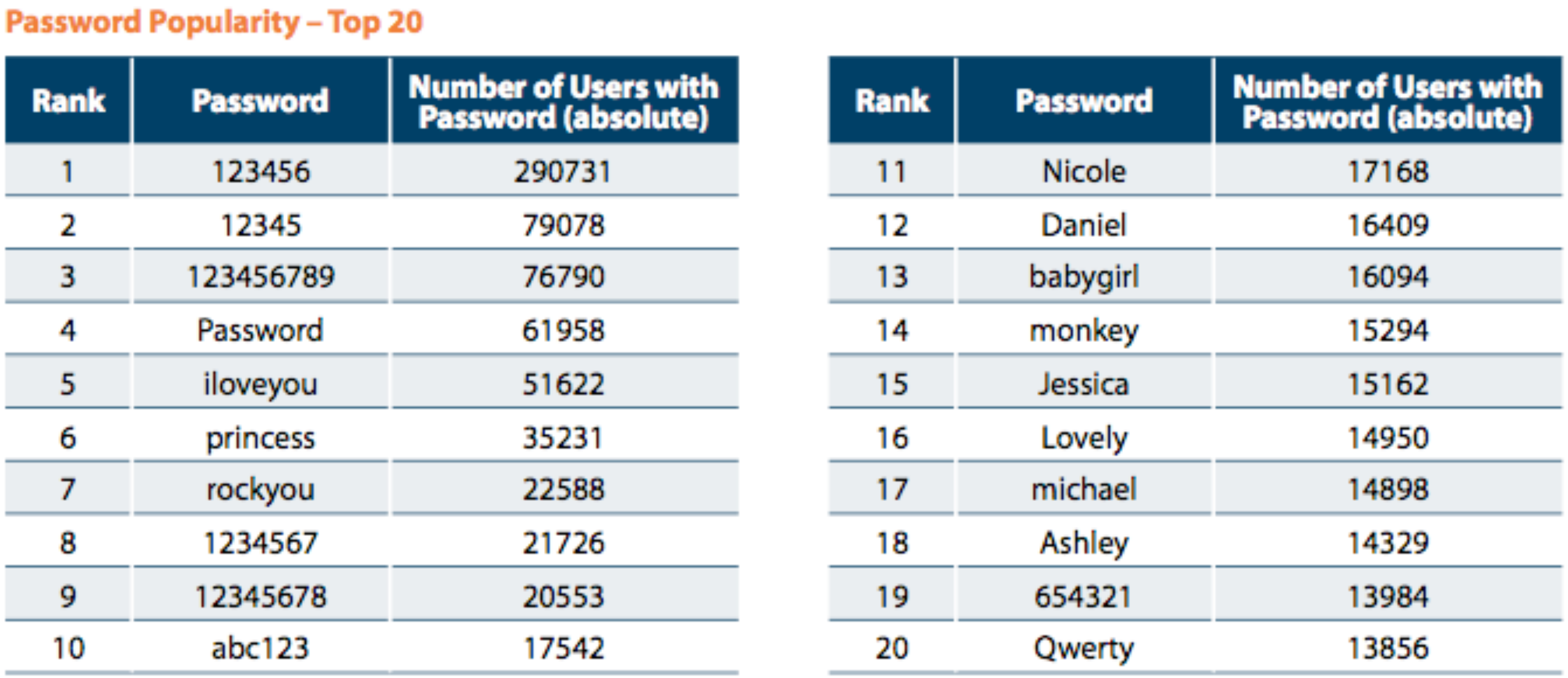
- Graph is compared to database of authentic identities
- If graph is same, then person deemed "authentic"
  - Problem: what does it mean to be "same enough"
    - rotation
    - imperfect contact
    - finger damage
  - ***Fundamental Problem***: False accept (FP) vs. false reject rates (FN)?



Credential: Something I Know

Something I know…

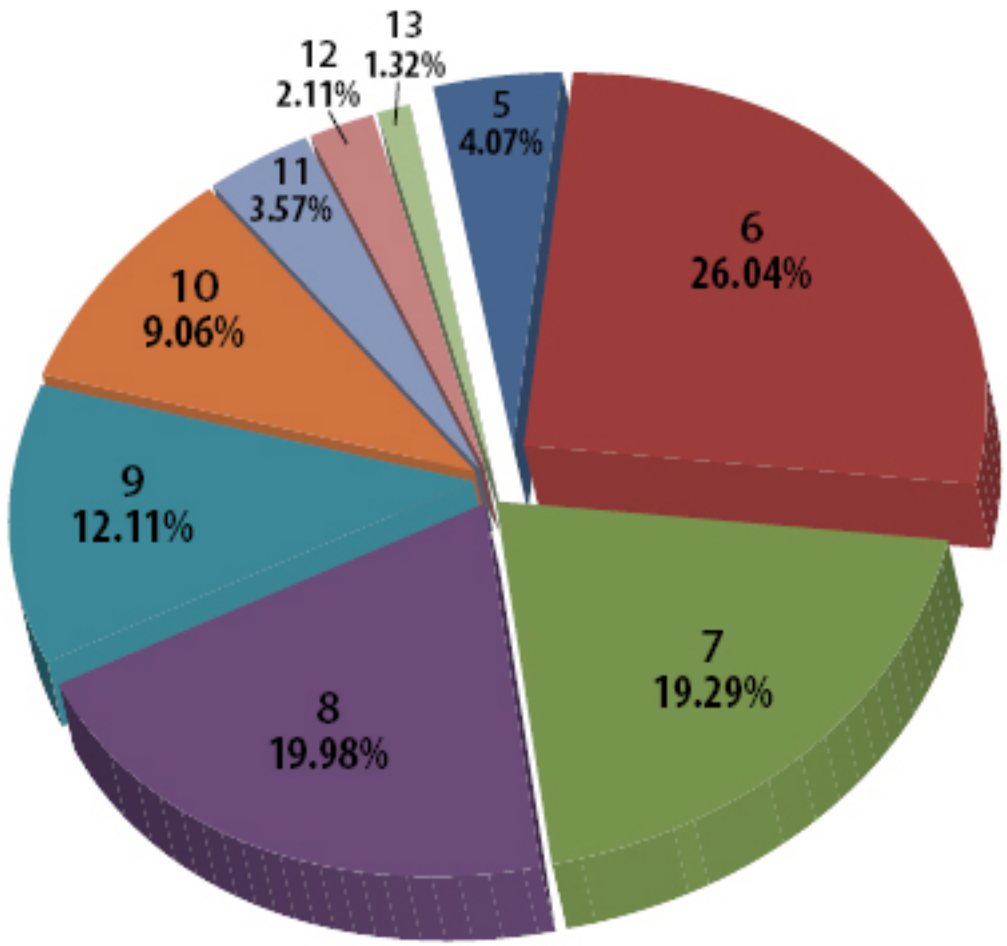
- Passport number, mother's maiden name, last 4 digits of your social security, credit card number
  - **Q: Are these good credentials?**
- Passwords and pass-phrases
  - Note: passwords are generally pretty weak, and may be used in more than one place (https://xkcd.com/792/)



Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409
13	babygirl	16094
14	monkey	15294
15	Jessica	15162
16	Lovely	14950
17	michael	14898
18	Ashley	14329
19	654321	13984
20	Qwerty	13856

Password Length Distribution



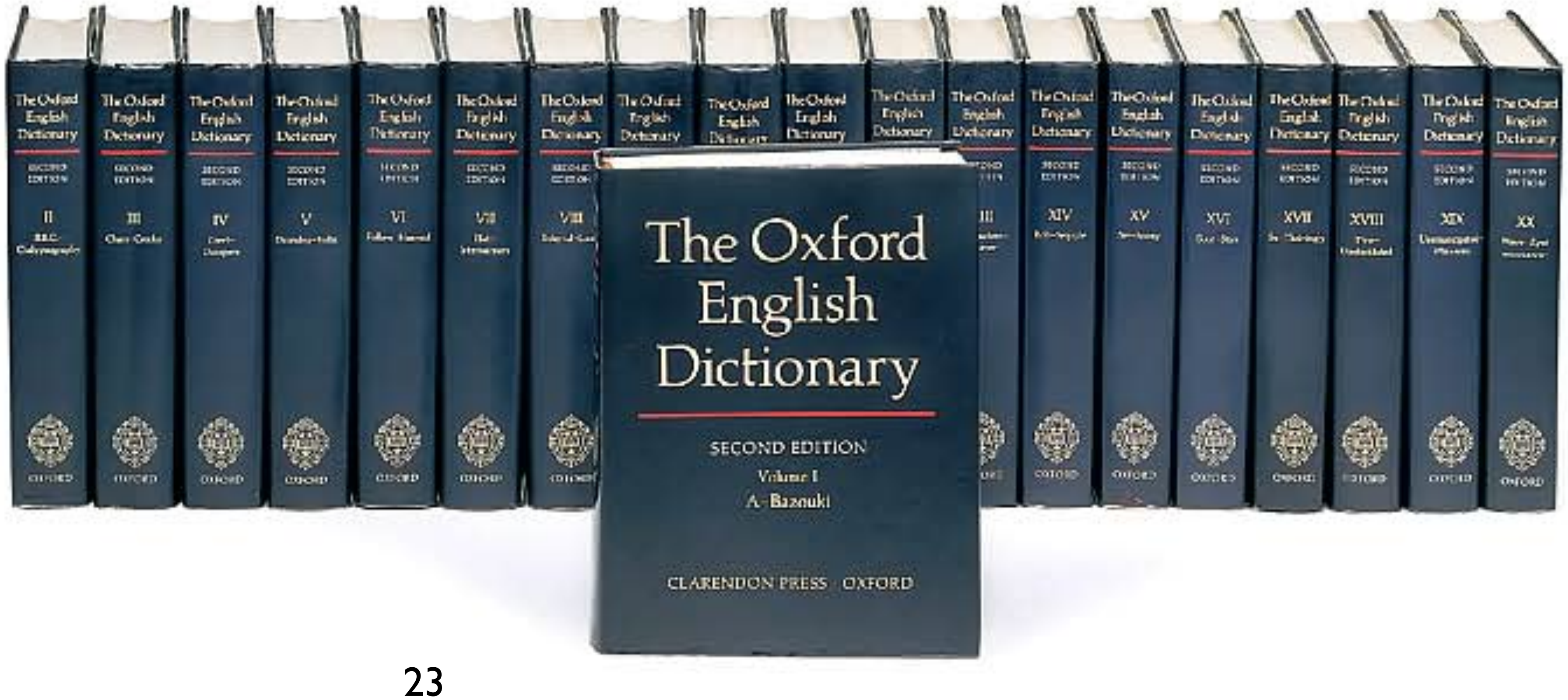
Source: iMPERVA 2010 study

Something I know…

- Passport number, mother's maiden name, last 4 digits of your social security, credit card number
  - **Q: Are these good credentials?**
- Passwords and pass-phrases
  - Note: passwords are generally pretty weak, and may be used in more than one place (https://xkcd.com/792/)
- Attacks:
  - Online - hard when certain countermeasures are implemented
  - Offline - easy to mount, simple passwords can be found quickly

Dictionary Attacks

- Brute-force password by trying every word in a "dictionary"
- Plenty of automated tools: e.g., John the Ripper
- Pre-computed lists of hashes (rainbow tables)



“Salt”ing passwords

- Suppose you want to make an *offline dictionary attack* more difficult
- A *salt* is a random number added to the password
- This is the approach taken by any reasonable system

$$
\begin{gathered}
salt_1, h(salt_1, pw_1) \\
salt_i, h(salt_2, pw_2) \\
salt_i, h(salt_3, pw_3) \\
\ldots \\
salt_n, h(salt_n, pw_n)
\end{gathered}
$$

How to create a good password?

NIST's Recommendation

(2006-2016)

- Minimum of 8 characters
- At least one uppercase
- At least one lowercase
- At least one digit
- At least one special character
- No dictionary words

G0J*mb0s2

Password Selection Goal

- Passwords should be uniformly distributed
- Any structural commonalities can be attacked
- People aren’t good at this!

“Fast, Lean, and Accurate: Modeling Password Guessability Using Neural Networks”, Melicher et al., 2016

NIST’s Recommendation

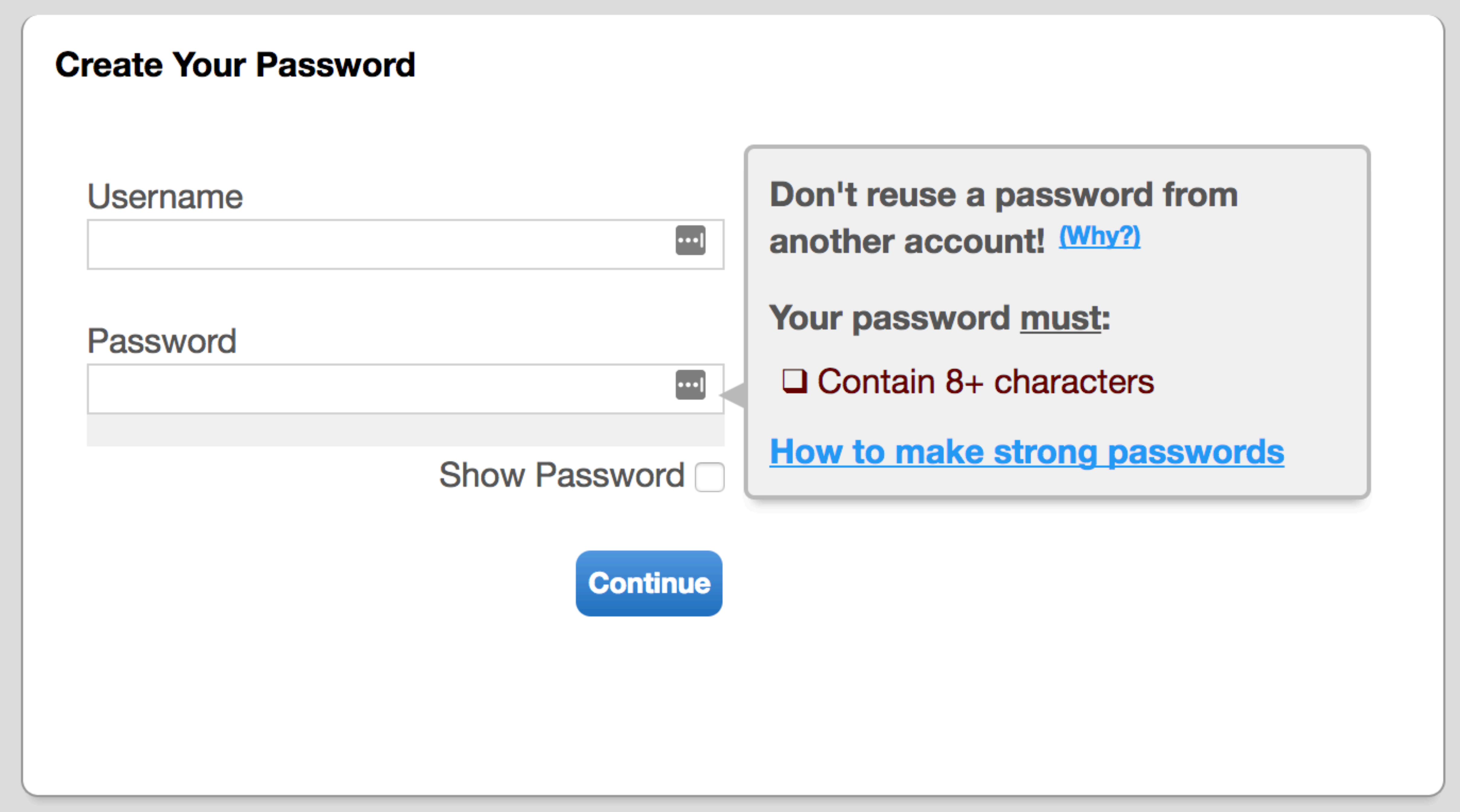
(2006-2016)

- Minimum of 8 characters
- At least one uppercase
- At least one lowercase
- At least one digit
- At least one special character
- No dictionary words

(2017-Present)

- Minimum of 8 characters
- No complexity requirements (predictable patterns)
- No periodic reset (password reuse)
- No dictionary words
- No common passwords (predictable patterns)
- Screen context-specific words

CMU/CUPS Password Meter



Create Your Password

Username

Password

Show Password □

Continue

Don't reuse a password from another account! (Why?)

Your password **must**:

❑ Contain 8+ characters

How to make strong passwords

https://cups.cs.cmu.edu/meter/

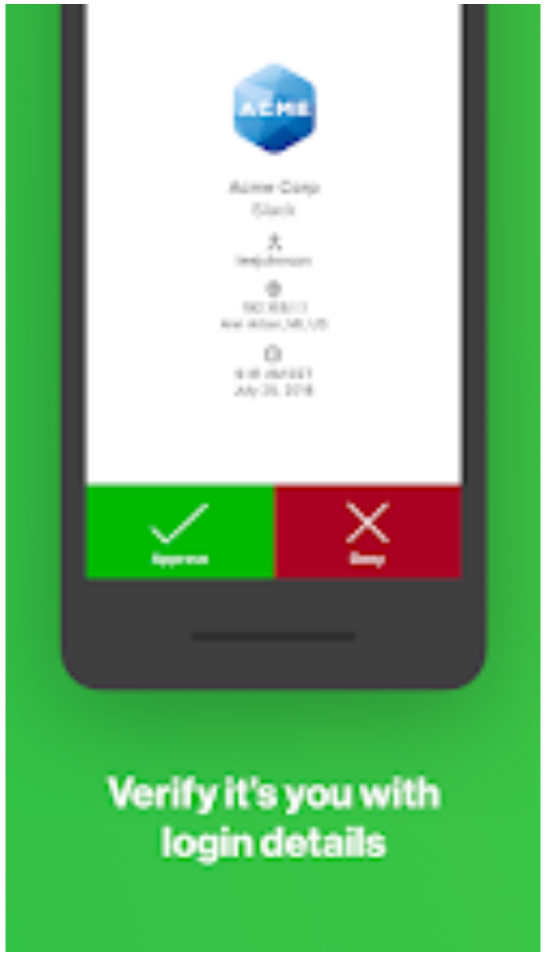
Password Managers

- Many options (in-browser, LastPass, KeePass, etc.)
- Considerations:
  - Where is the database stored?
  - How is the database protected?
  - Integration with mobile OSes?

Credential: Something I Have

Credential: Something I have

- Digital Certificates
- Smartcards
  - Unpowered processors
  - Small NV storage
  - Tamper *resistant*
- Tokens (transponders, …)
  - EZ-pass
  - SecurID
  - Duo Security



Verify it's you with login details

A (simplified) sample token device

- A one-time password (or half of a two-factor authentication system)
- Secret key K
  - One-time password for epoch i is $\mathrm{MAC}_K(i)$
  - Tamperproof token encodes K in firmware
  - Time synchronization allows authentication server to know what i is expected, and authenticate the user.
- *Note*: somebody can see your token display at some time but learn nothing useful for later periods.

Multifactor Authentication

- While passwords are the standard, the other factors (are, can) be combined to enhance security
- Examples:
    - Duo’s 2-step verification
    - SMS messages

Kerberos