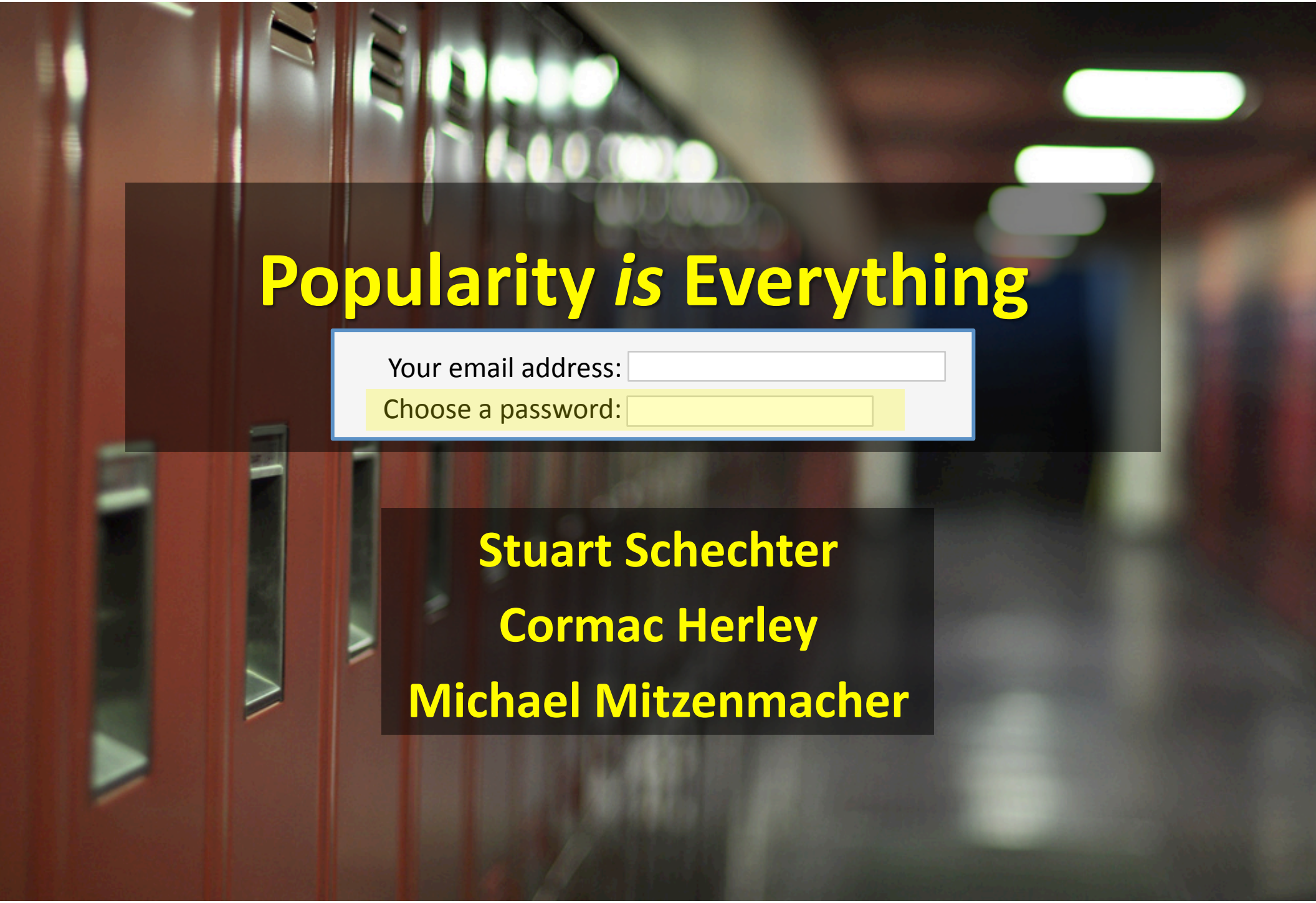
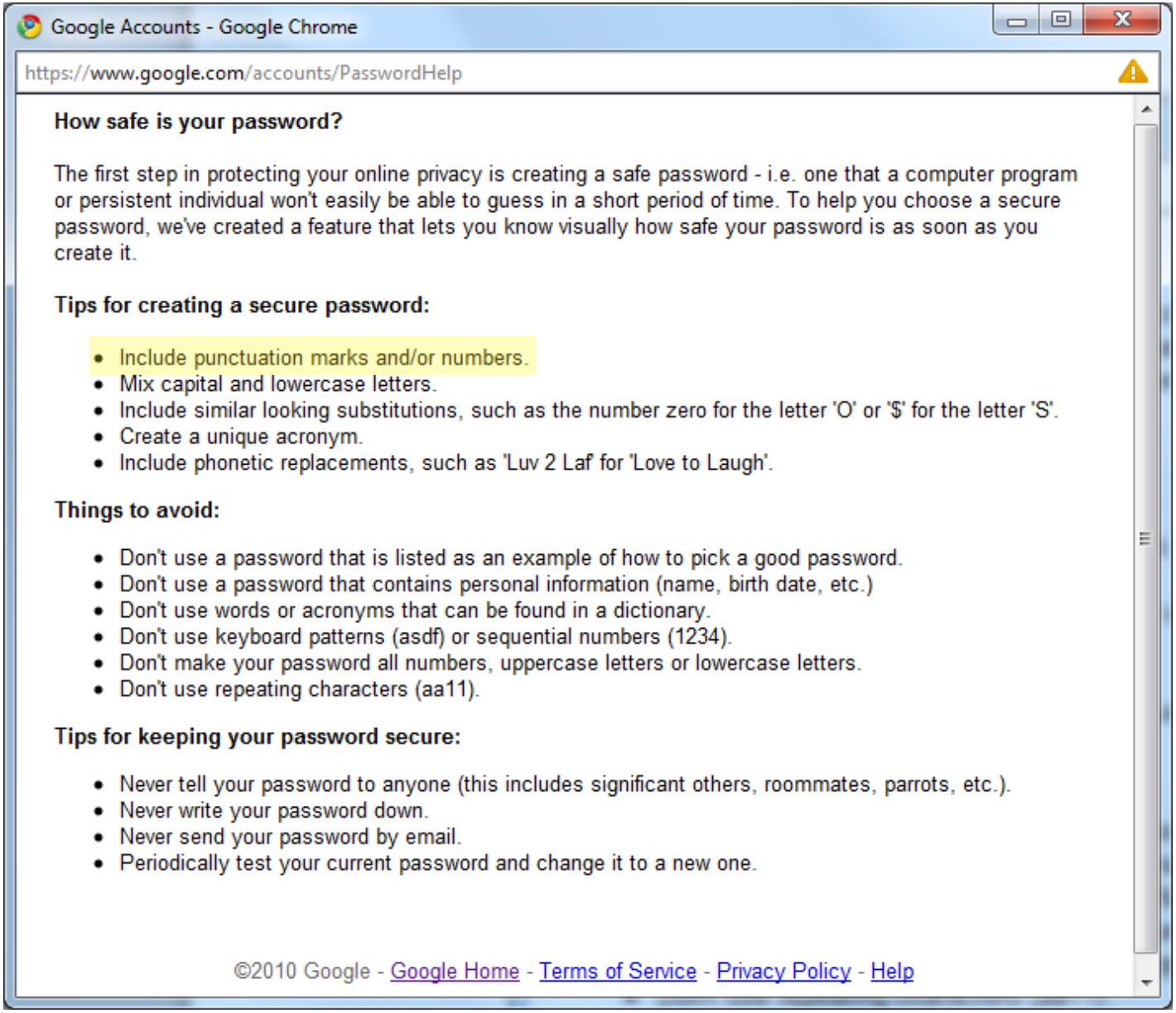
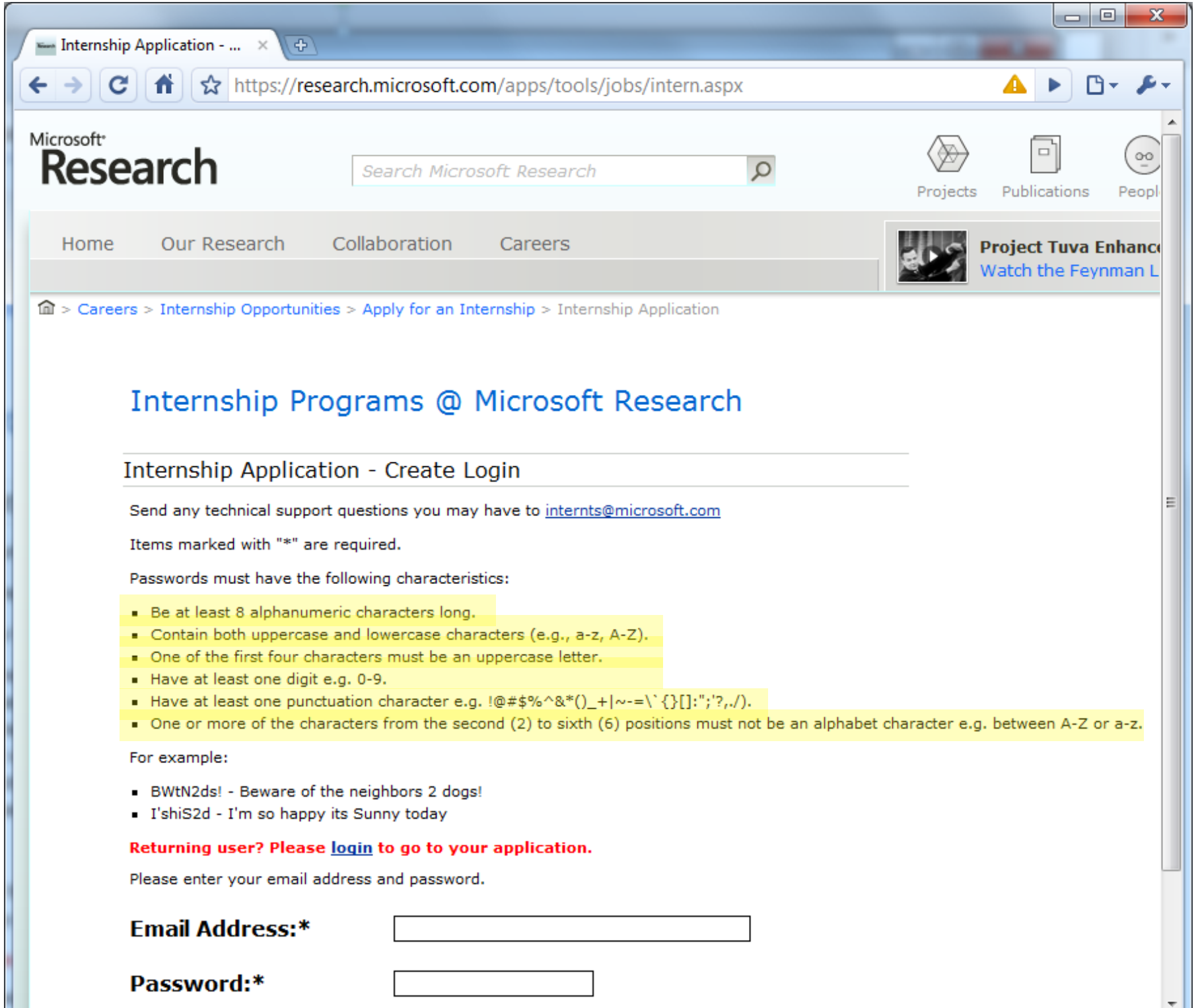
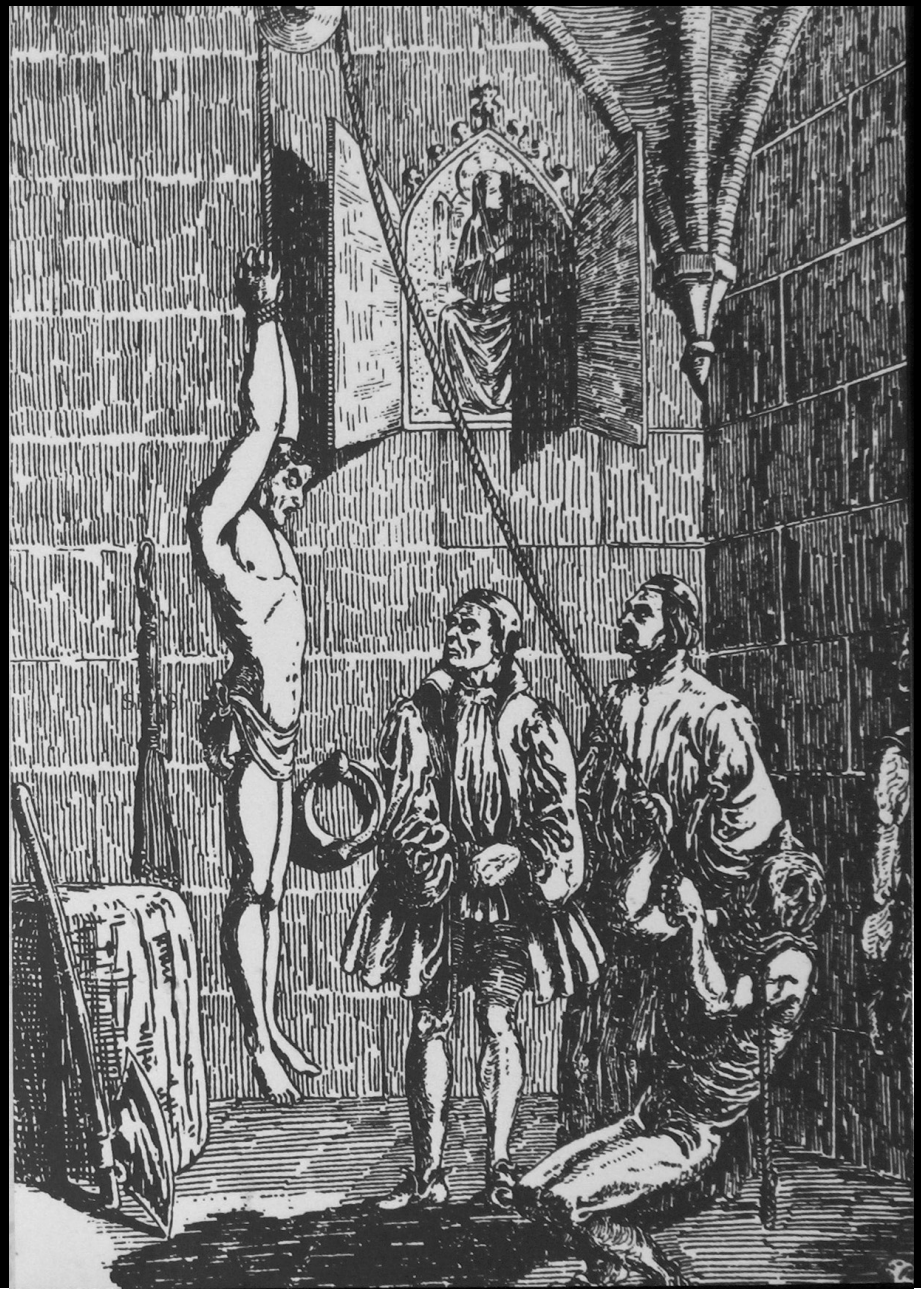

Popularity *is* Everything
Your email address:
Choose a password:
Stuart Schechter
Cormac Herley
Michael Mitzenmacher


Strong Passwords | Micro...
http://www.microsoft.com/protect/fraud/passw
Microsoft Online Safety
Home
Fraud Prevention
Data Protection
Create strong passwords
Strong passwords are important protections to help you have safer online transactions.
Keys to password strength: length and complexity
An ideal password is long and has letters, punctuation, symbols, and numbers.
Whenever possible, use at least 14 characters or more.
The greater the variety of characters in your password, the better.
Use the entire keyboard, not just the letters and characters you use or see most often.
Create a strong password you can remember
There are many ways to create a long, complex password. Here is one way that may make remembering it easier:

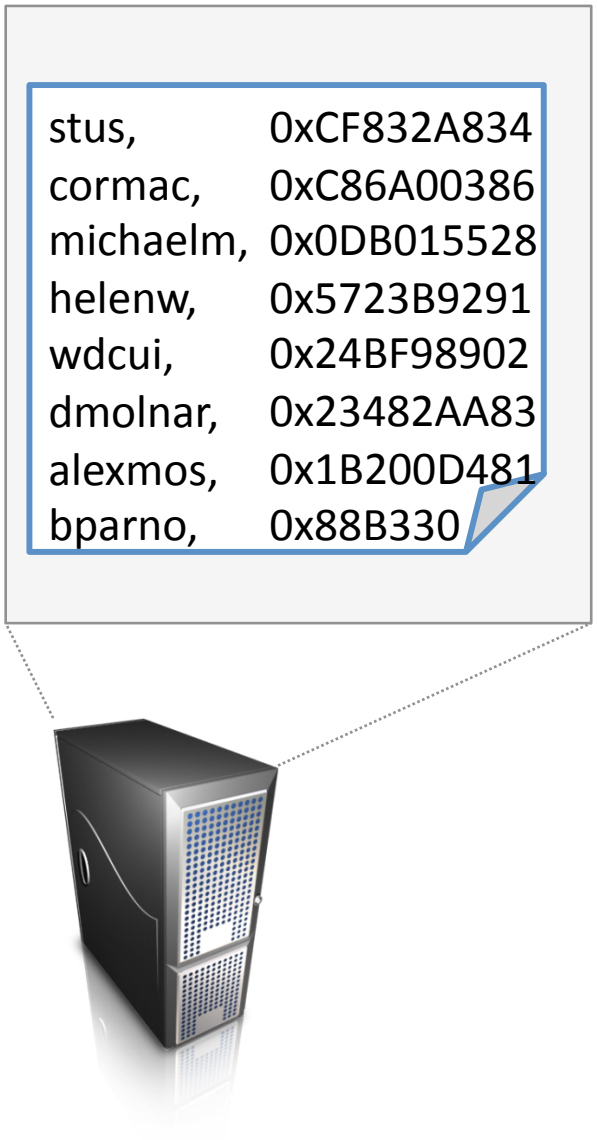

Google Accounts - Google Chrome
https://www.google.com/accounts/PasswordHelp
How safe is your password?
The first step in protecting your online privacy is creating a safe password - i.e. one that a computer program or persistent individual won't easily be able to guess in a short period of time. To help you choose a secure password, we've created a feature that lets you know visually how safe your password is as soon as you create it.
Tips for creating a secure password:
Include punctuation marks and/or numbers.
Mix capital and lowercase letters.
Include similar looking substitutions, such as the number zero for the letter 'O' or '$' for the letter 'S'.
Create a unique acronym.
Include phonetic replacements, such as 'Luv 2 Laf' for 'Love to Laugh'.
Things to avoid:
Don't use a password that is listed as an example of how to pick a good password.
Don't use a password that contains personal information (name, birth date, etc.)
Don't use words or acronyms that can be found in a dictionary.
Don't use keyboard patterns (asdf) or sequential numbers (1234).
Don't make your password all numbers, uppercase letters or lowercase letters.
Don't use repeating characters (aa11).
Tips for keeping your password secure:
Never tell your password to anyone (this includes significant others, roommates, parrots, etc.).
Never write your password down.
Never send your password by email.
Periodically test your current password and change it to a new one.
©2010 Google - Google Home - Terms of Service - Privacy Policy - Help


Internship Application - ...
https://research.microsoft.com/apps/tools/jobs/intern.aspx
Microsoft Research
Search Microsoft Research
Projects
Publications
Peopl
Home
Our Research
Collaboration
Careers
Project Tuva Enhanc
Watch the Feynman L
> Careers > Internship Opportunities > Apply for an Internship > Internship Application
Internship Programs @ Microsoft Research
Internship Application - Create Login
Send any technical support questions you may have to internts@microsoft.com
Items marked with "*" are required.
Passwords must have the following characteristics:
Be at least 8 alphanumeric characters long.
Contain both uppercase and lowercase characters (e.g., a-z, A-Z).
One of the first four characters must be an uppercase letter.
Have at least one digit e.g. 0-9.
Have at least one punctuation character e.g. !@#$%^&*()_+|~-=\`{}[]:";'?,./).
One or more of the characters from the second (2) to sixth (6) positions must not be an alphabet character e.g. between A-Z or a-z.
For example:
BWtN2ds! - Beware of the neighbors 2 dogs!
I'shiS2d - I'm so happy its Sunny today
Returning user? Please login to go to your application.
Please enter your email address and password.
Email Address:*
Password:*

Why are we doing this to our users?



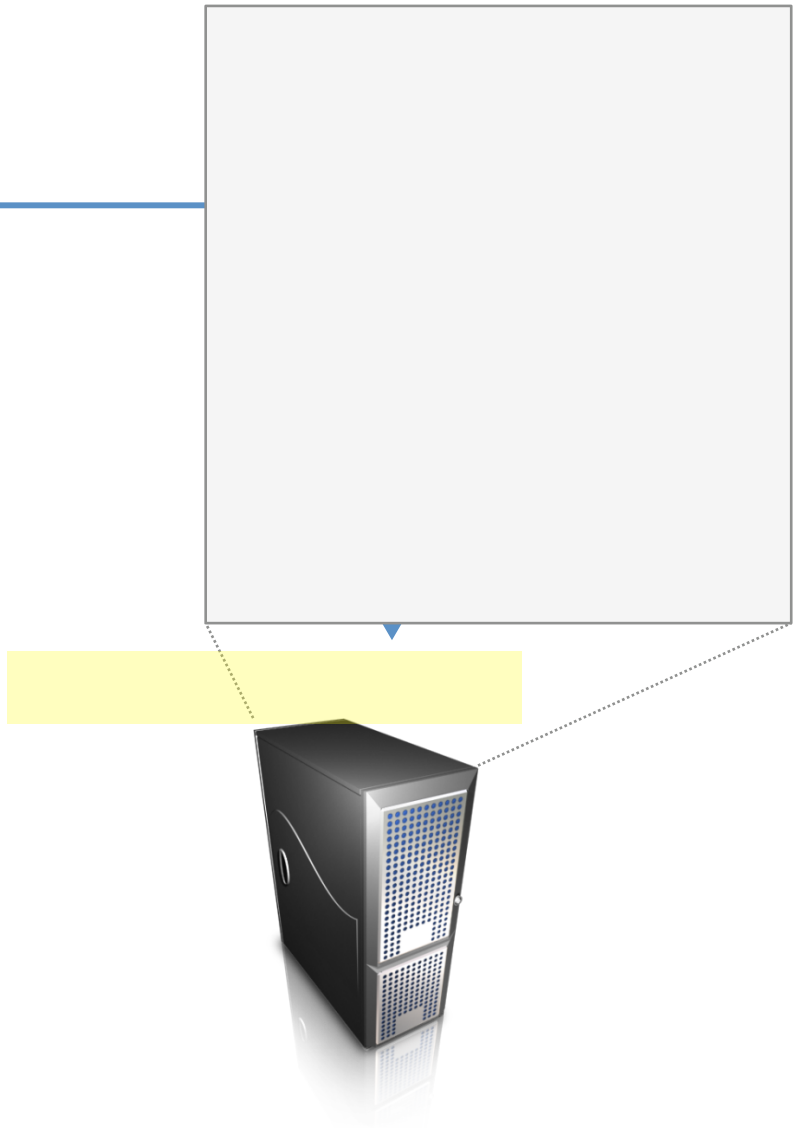
Threat 1: Password file compromised



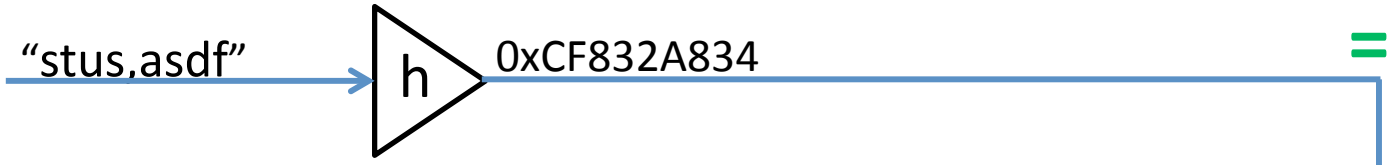
Threat 1: Password file compromised

stus,	0xCF832A834
cormac,	0xC86A00386
michaelm,	0x0DB015528
helenw,	0x5723B9291
wdcui,	0x24BF98902
dmolnar,	0x23482AA83
alexmos,	0x1B200D481
bparno,	0x88B330

xD1F7255CA



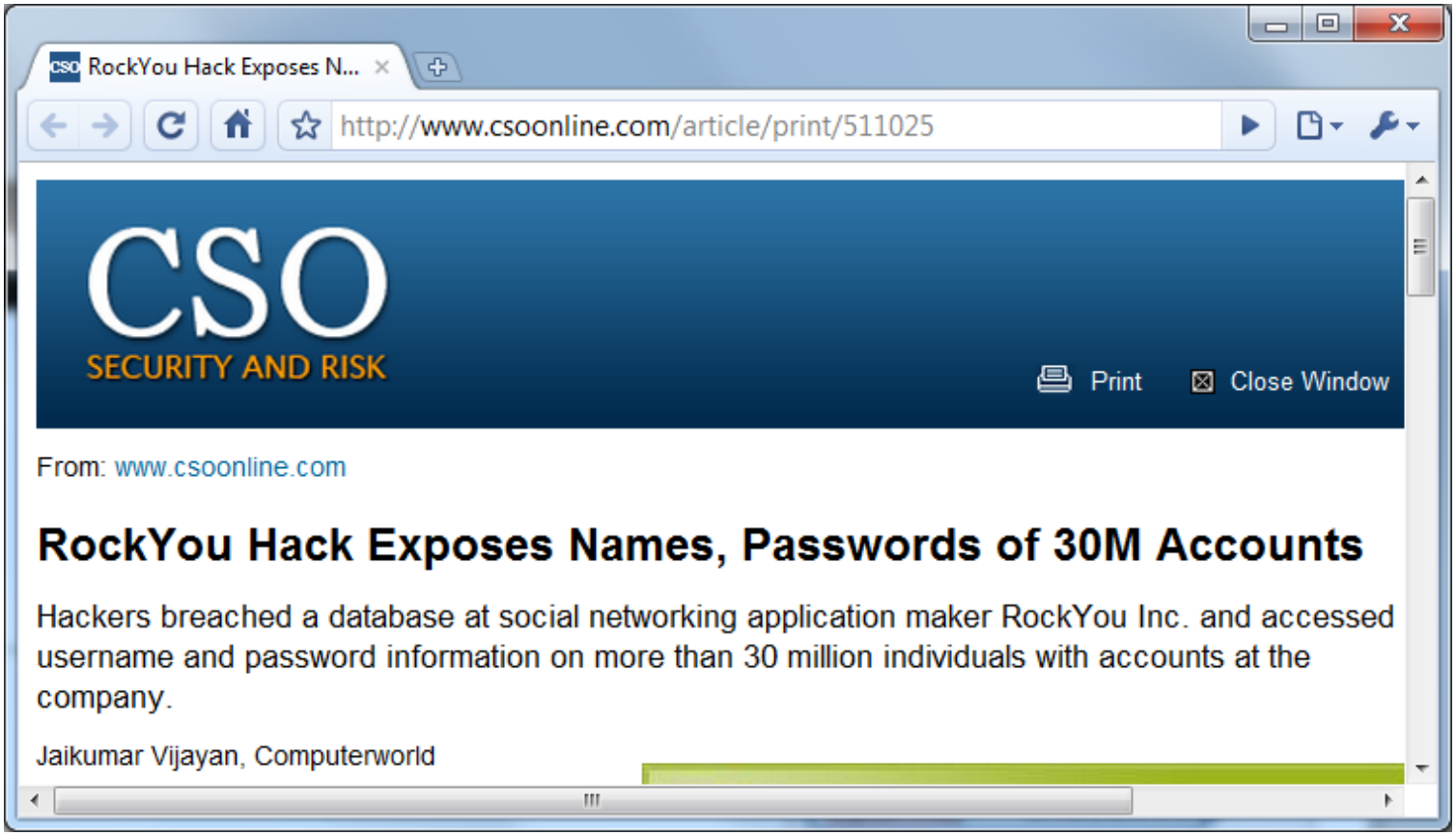
Threat 1: Password file compromised



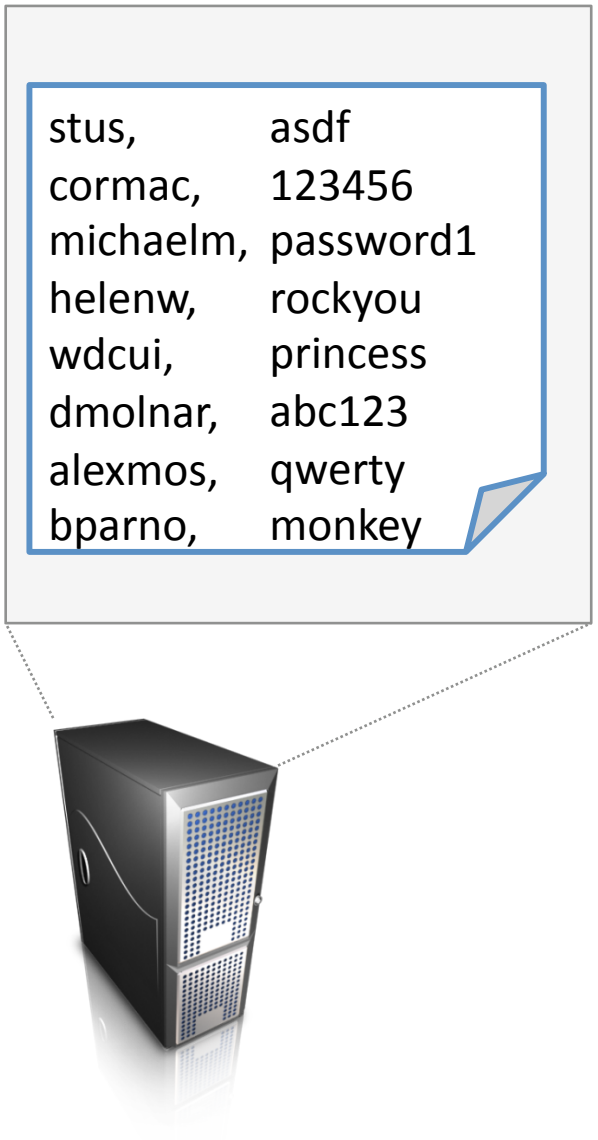
cost of one guess = cost to compute h

stus,	0xCF832A834
cormac,	0xC86A00386
michaelm,	0x0DB015528
helenw,	0x5723B9291
wdcui,	0x24BF98902
dmolnar,	0x23482AA83
alexmos,	0x1B200D481
bparno,	0x88B330

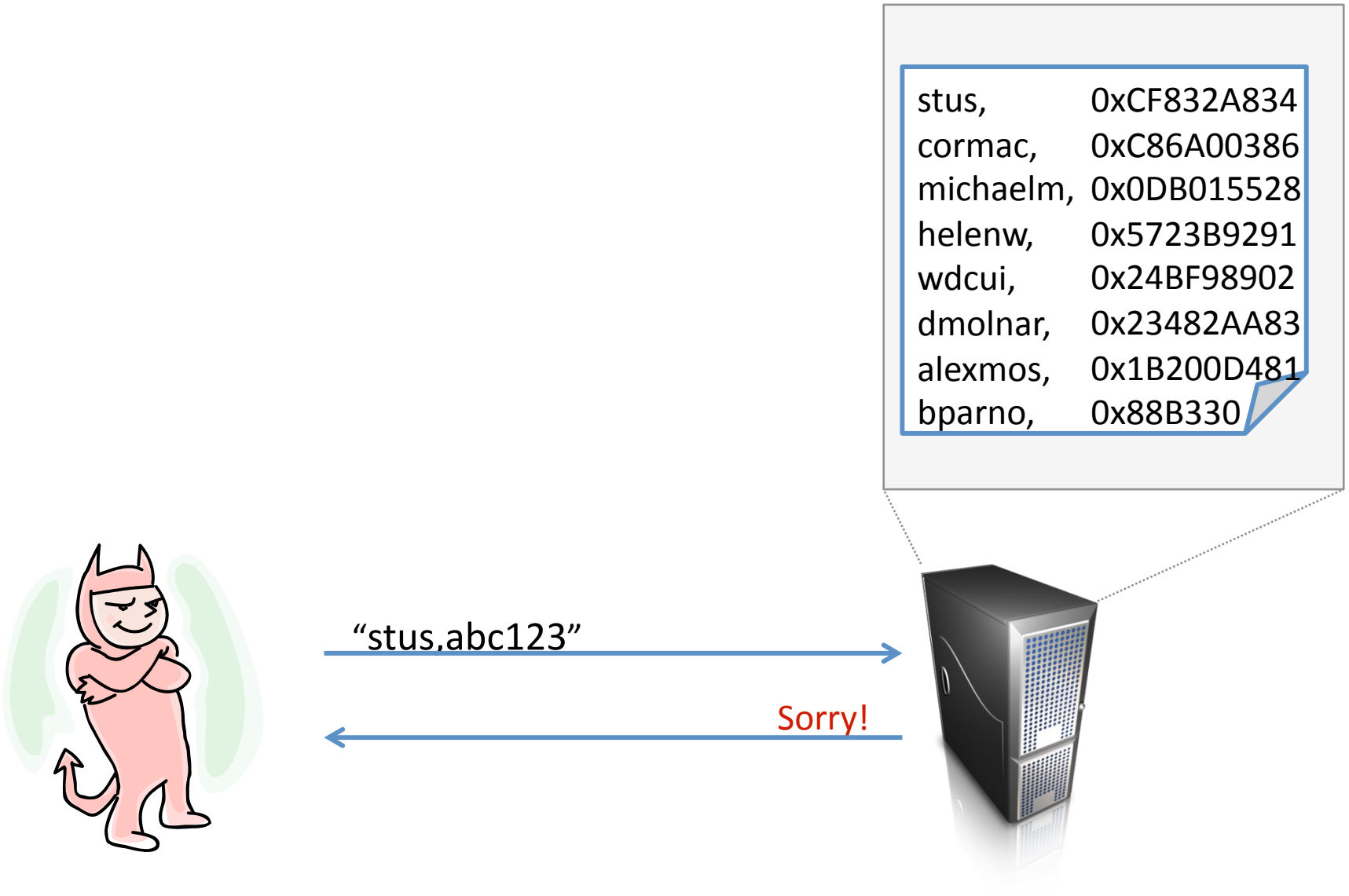
Threat 1: Password file compromised



Threat 1: Password file compromised



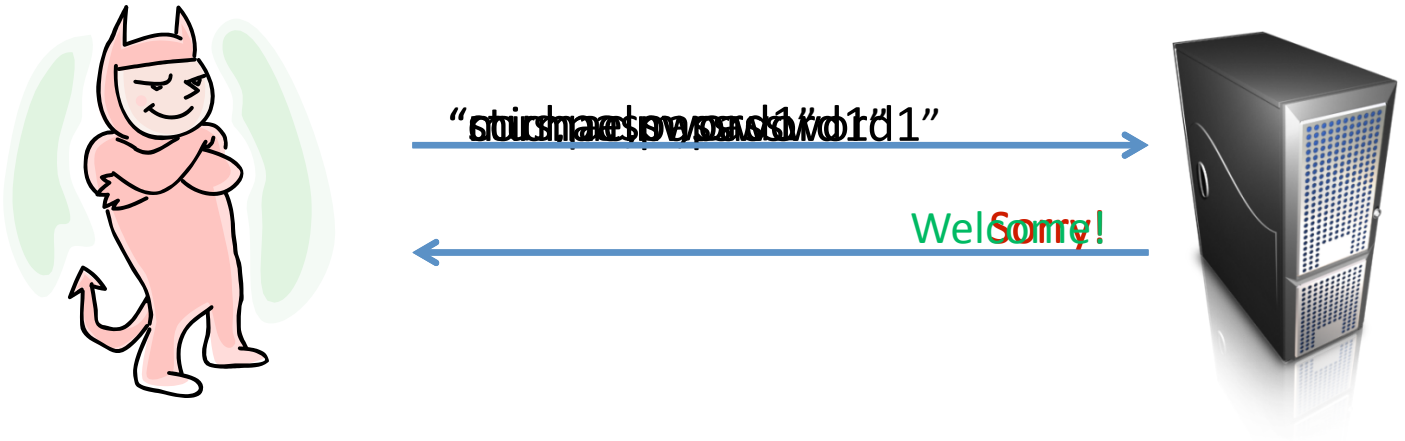
Threat 2: Online dictionary attack



Threat 2a: Online statistical guessing

Common passwords (sorted by popularity)

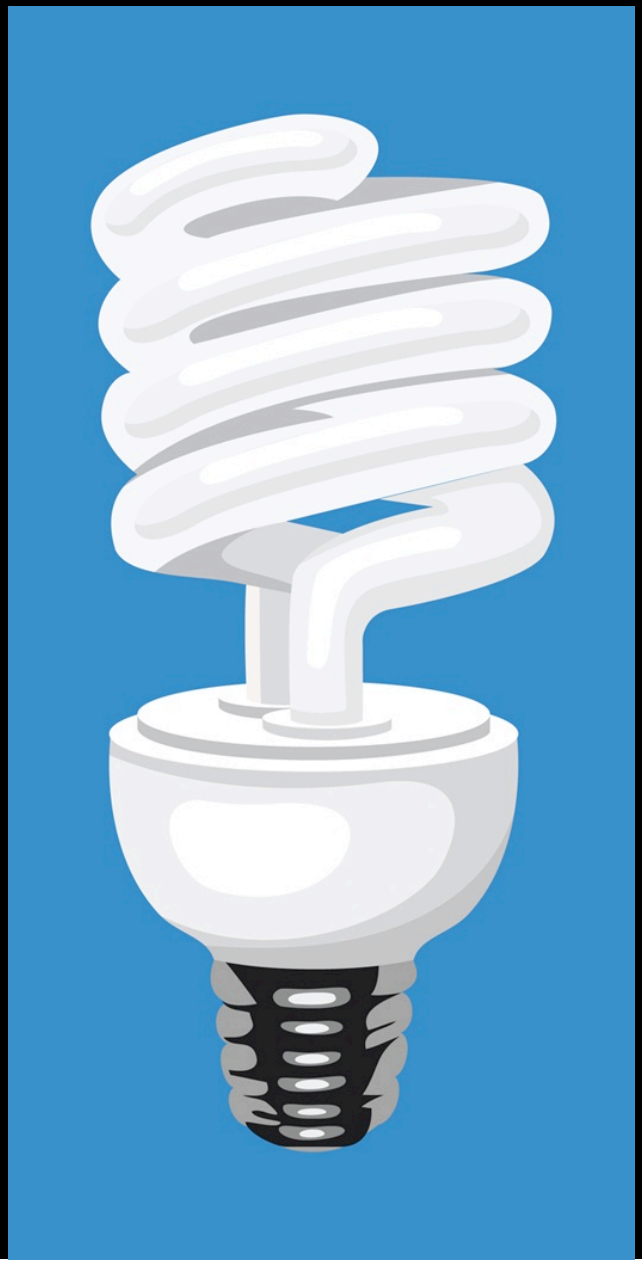
password1
password
abc123
asdf
1234568
p@ssword
iloveyou



Threat 2a: Online statistical guessing

- User-based lockout ineffective
  - 300m users * 10 guesses per user = 3 billion guesses
- IP lockout slightly less ineffective
  - 10m node botnet * 10 guesses per IP = 100M guesses
- Some accounts will be compromised
  - Frequency of most popular password * guesses
  - 100k accounts if 0.1% use most popular password

Here comes the big* idea of the talk…



*yet low carbon

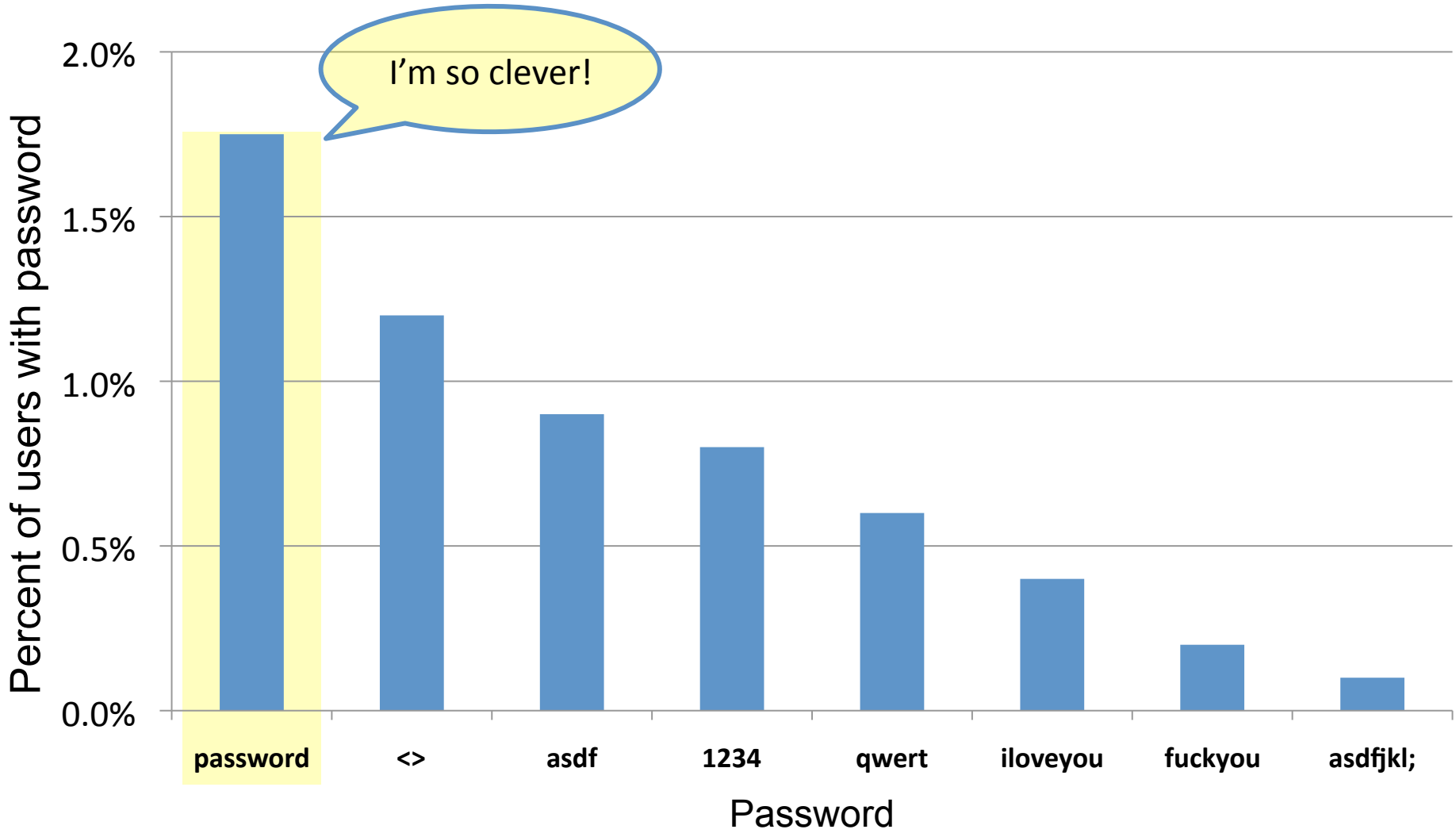
Replace composition rules with one new rule

Don’t password rules already accomplish this?

http://failblog.org/2008/01/03/fail-camera/

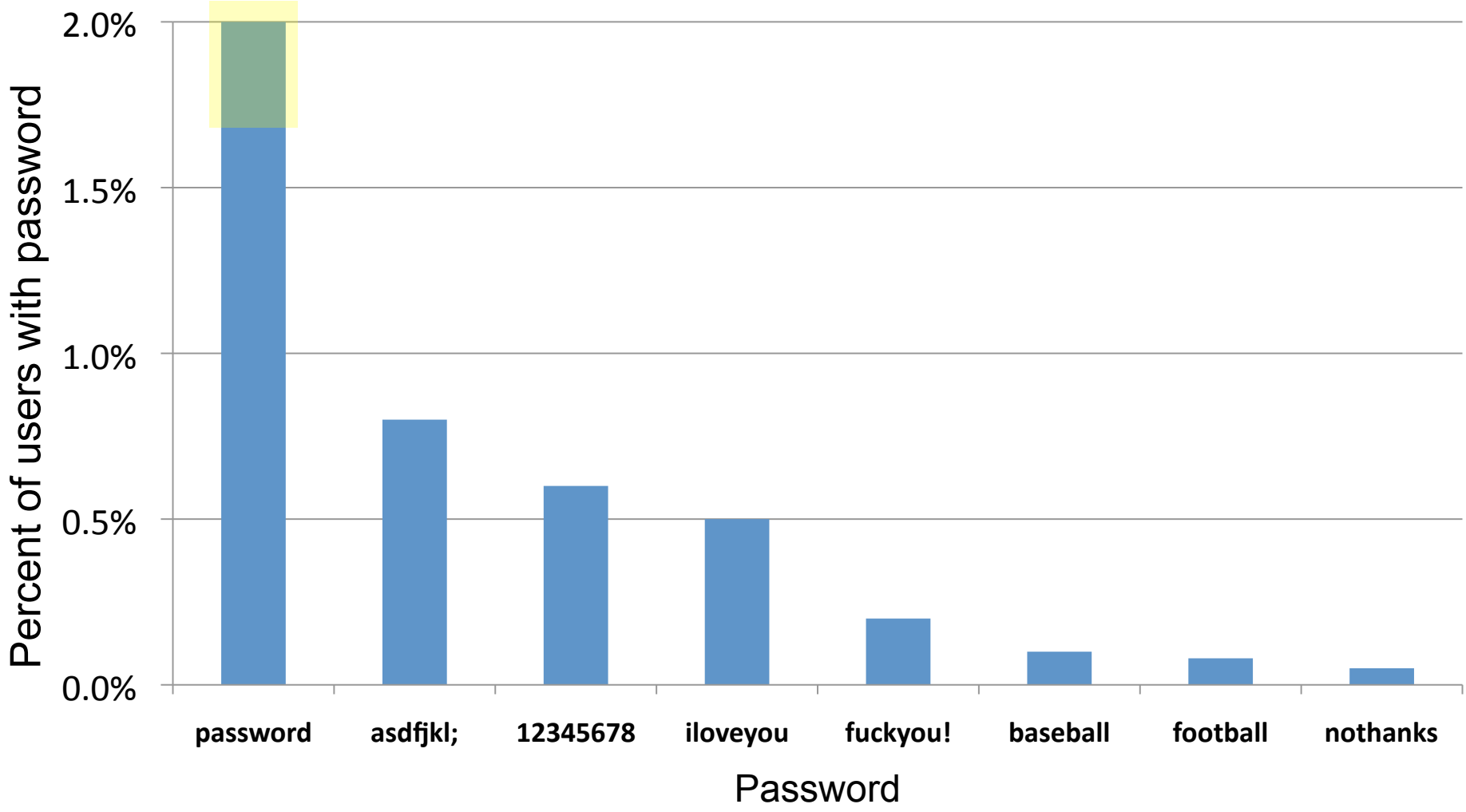
Expected password choices… without rules

Example based on real data… but not real data!

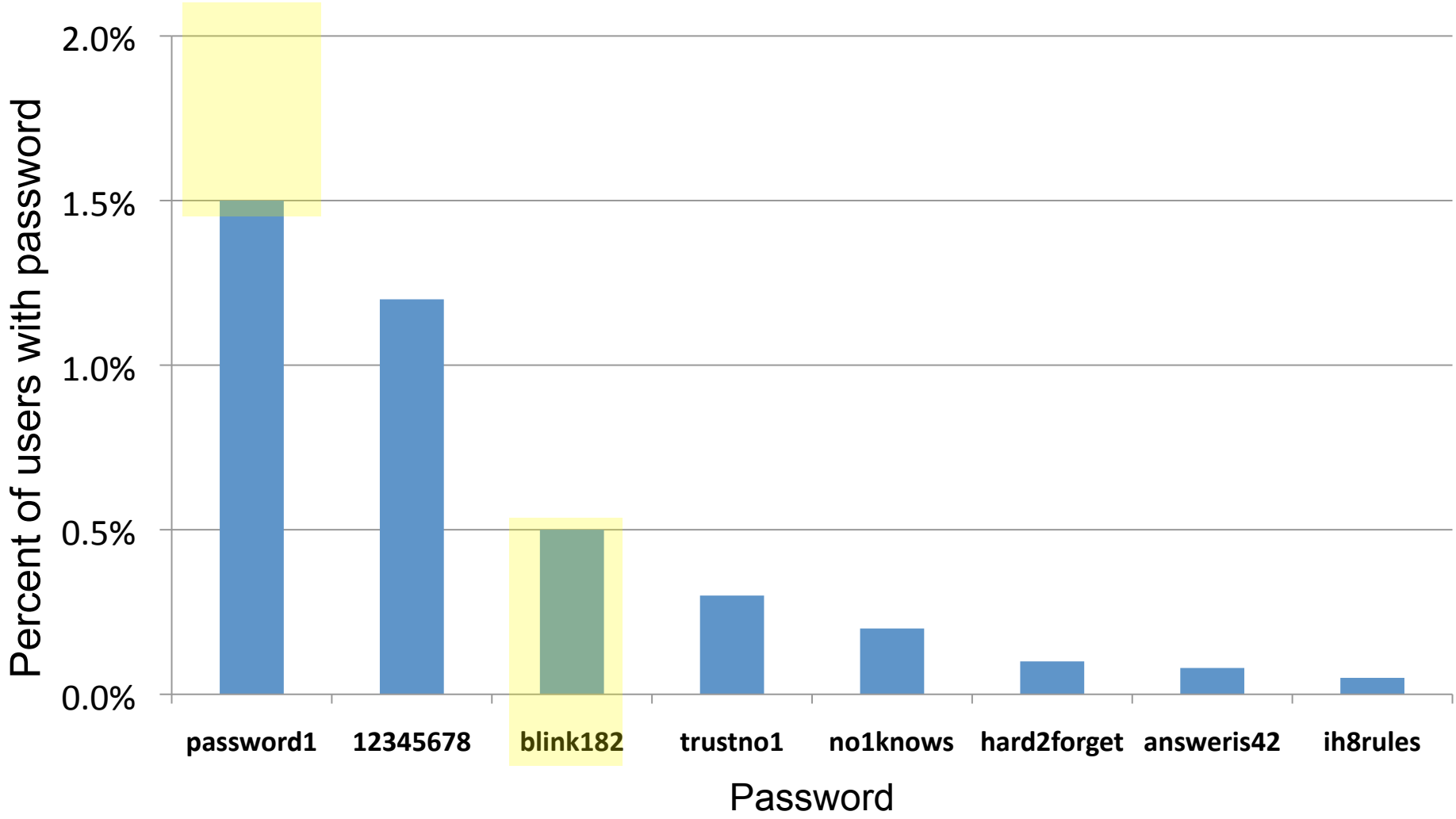


Rule 1: At least 8 characters

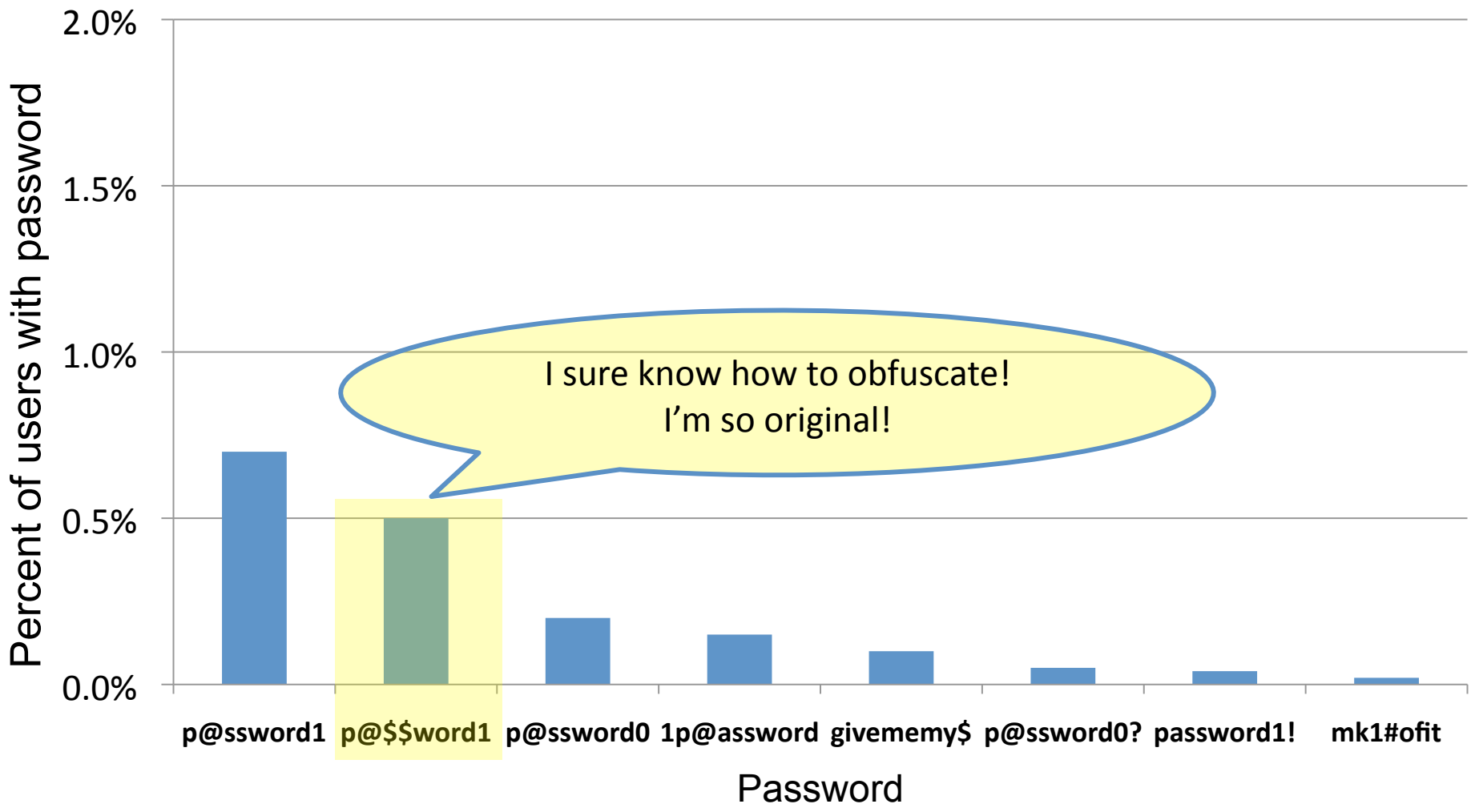
Sometimes rules have unintended consequences



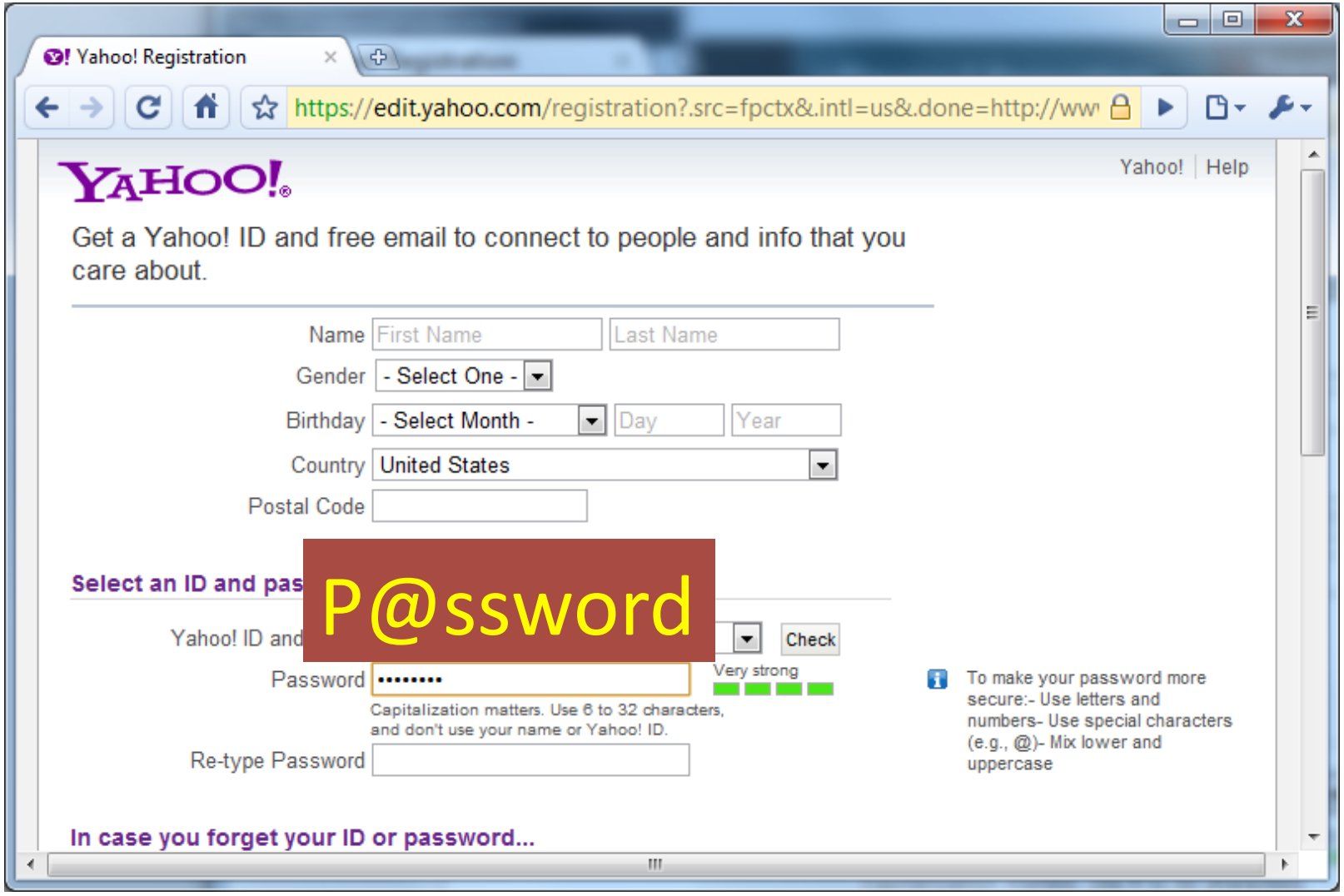
Rule 2: At least 1 number



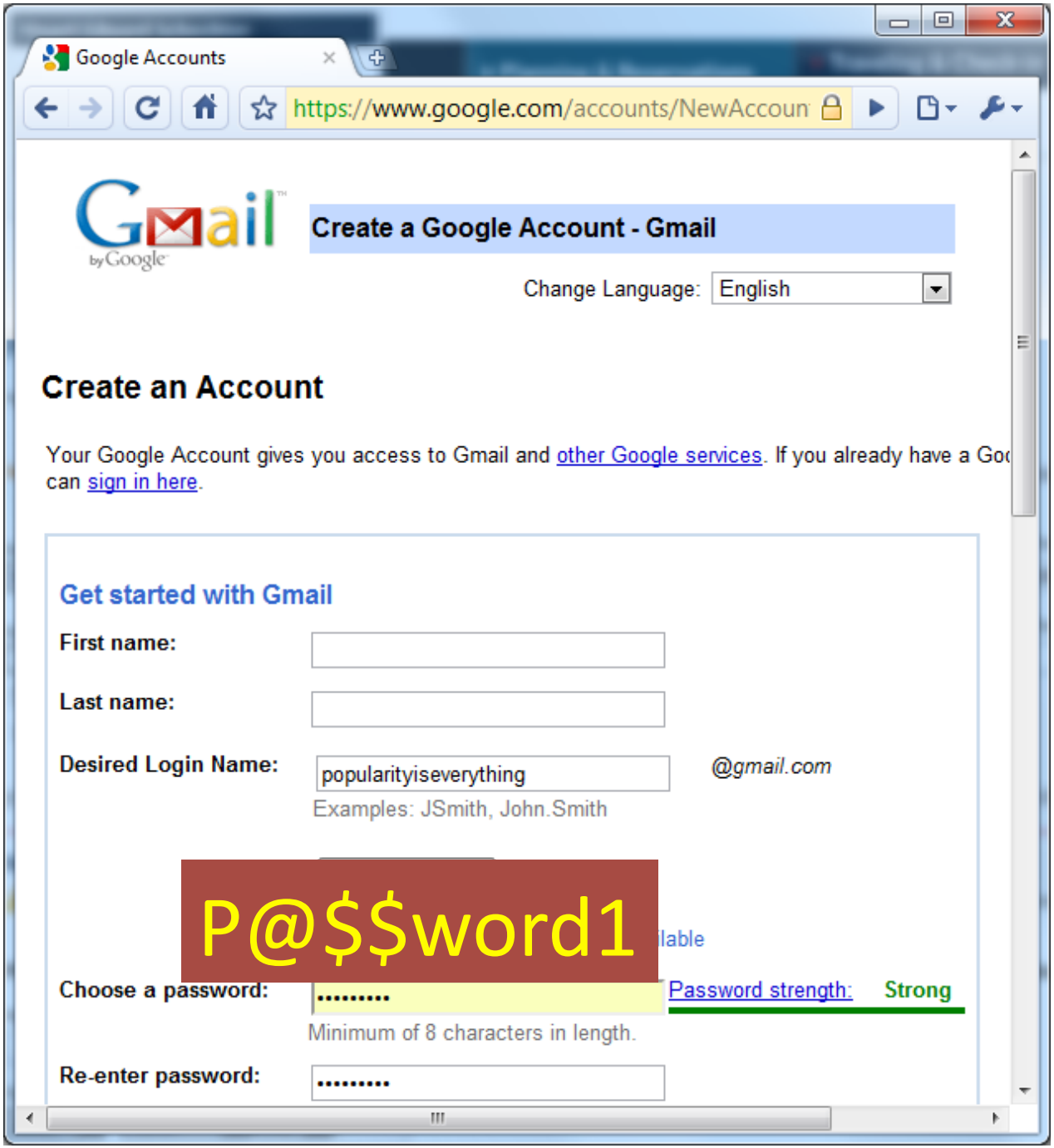
Rule 3: At least 1 “special” character



Large sites favor strength meters over rules




Sign up - Windows Live
https://signup.live.com/signup.aspx?wa=wsignin1.0&rpsnv=11&ct=1279577434&rver
Windows Live™
Create your Windows Live ID
It gets you into all Windows Live services—and other places you see
All information is required.
If you use Hotmail, Messenger, or Xbox LIVE, you already have a Windows Live ID.
Sign in
popularityiseverything@hotmail.com is available.
hotmail.com
password1
address
Create a password:
6-character minimum; case sensitive
Retype password:
Alternate e-mail address:
Or choose a security question for password reset
Medium
Strong passwords contain 7-16 characters, do not include common words or names, and combine uppercase letters, lowercase letters, numbers, and symbols.


Google Accounts
https://www.google.com/accounts/NewAccoun
Gmail by Google
Create a Google Account - Gmail
Change Language: English
Create an Account
Your Google Account gives you access to Gmail and other Google services. If you already have a Goo
can sign in here.
Get started with Gmail
First name:
Last name:
Desired Login Name:
popularityiseverything
@gmail.com
Examples: JSmith, John.Smith
lable
P@$$word1
Choose a password:
Password strength: Strong
Minimum of 8 characters in length.
Re-enter password:

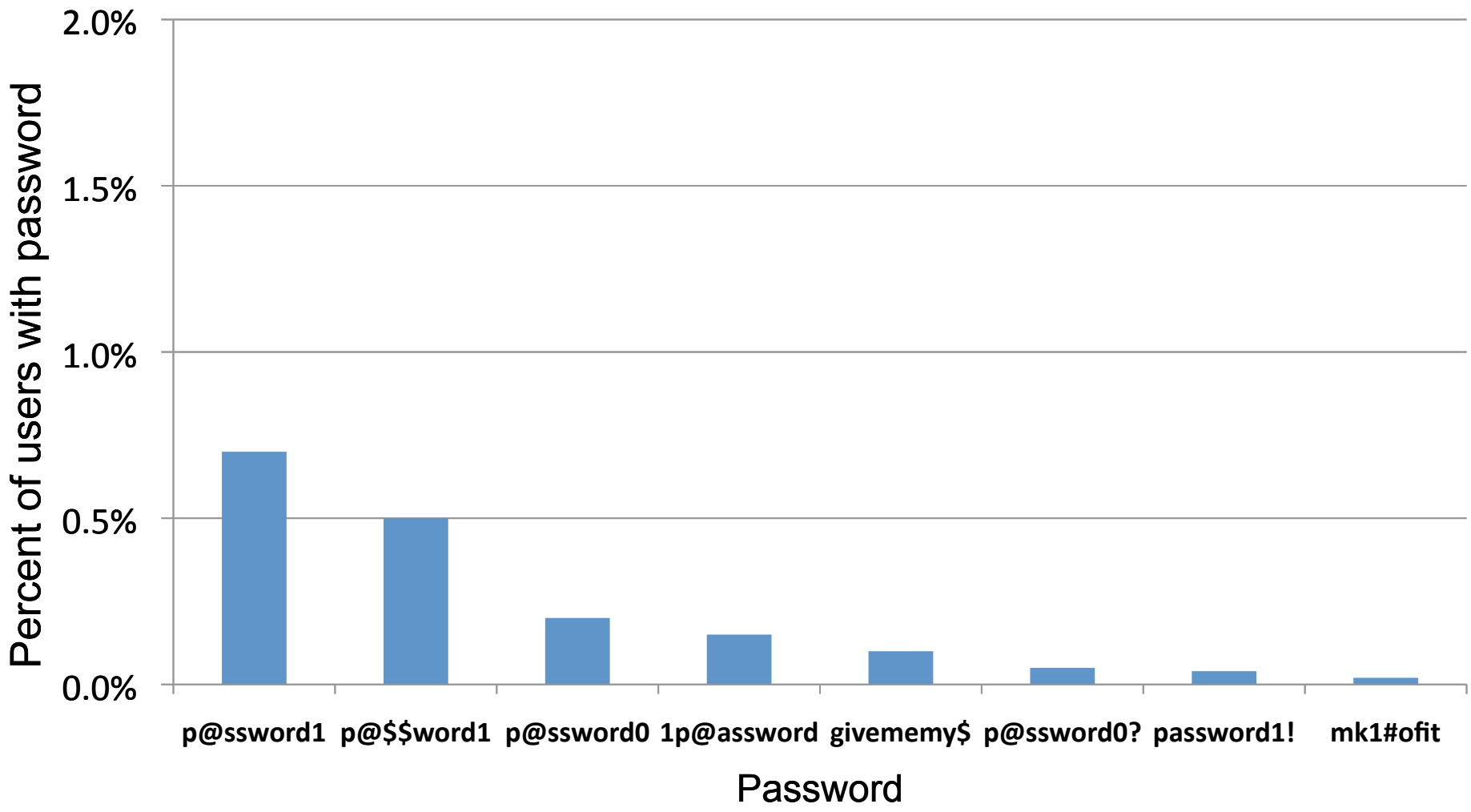
Composition rules  stronger passwords

‘password’  ‘P@$$word1’

Back to our desired policy

Your may not choose a popular password (one already in use by n% of other users.)

If we enforced “no popular passwords”…



Enforcing the “no popular passwords” rule

We must track popularity to prevent it

Common passwords (sorted by popularity)

password1,	2805
password,	2280
abc123,	1568
asdf,	1375
1234568,	583
p@ssword,	390
Iloveyou,	334

Dangers of tracking popular passwords

- Attackers will use this data for statistical guessing
  - ~~Against you~~
  - Against other sites

Tracking popular passwords

Common passwords (sorted by popularity)

password1,	100
password,	100
abc123,	100
asdf,	100
1234568,	100
p@ssword,	100
Iloveyou,	100

Dangers of tracking popular passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~
- Attackers will use for offline statistical guessing
  - Crack using only passwords in the popularity list

Tracking popular passwords

Common passwords (sorted by popularity)

password1,	100
password,	100
abc123,	100
asdf,	100
1234568,	100
p@ssword,	100
iloveyou,	100

Tracking populra passwords

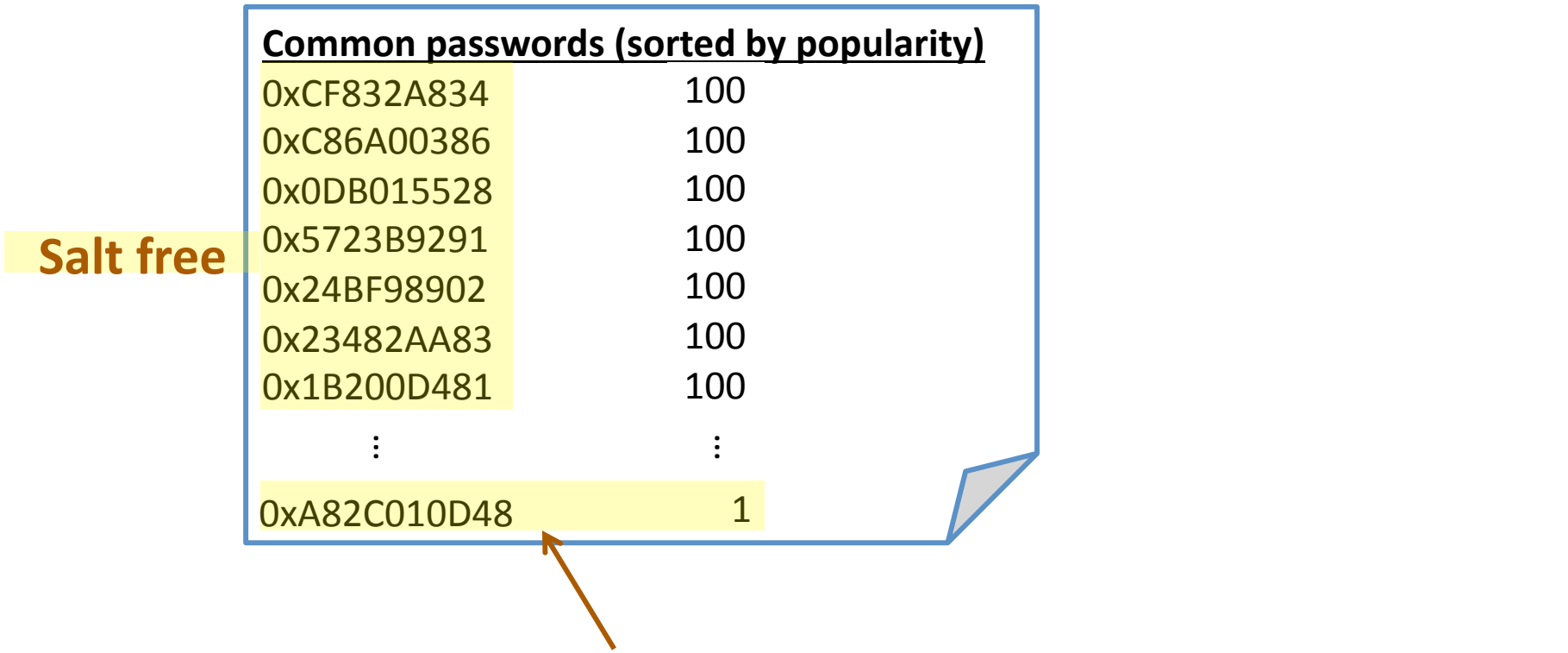
Common passwords (sorted by popularity)

0xCF832A834	100
0xC86A00386	100
0x0DB015528	100
0x5723B9291	100
0x24BF98902	100
0x23482AA83	100
0x1B200D481	100
⋮	⋮
0xA82C010D48	1

Dangers of tracking popular passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~
- Attackers will use for offline statistical guessing
  - ~~Crack using only passwords in the popularity list~~

How can we track popular passwords?



Dangers of tracking popular passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~

- Attackers will use for offline statistical guessing
  - ~~Crack using only passwords in the popularity list~~
  - Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  - Filter candidate password list (with access to oracle)

These seem unavoidable

Requirements for popularity-tracking data structure

add(*p*)

Adds the occurrence (use) of a password *p*

count(p)

Returns # of times *p* has been added

Need not be exact

count(*p*) ≈ number of times *p* added

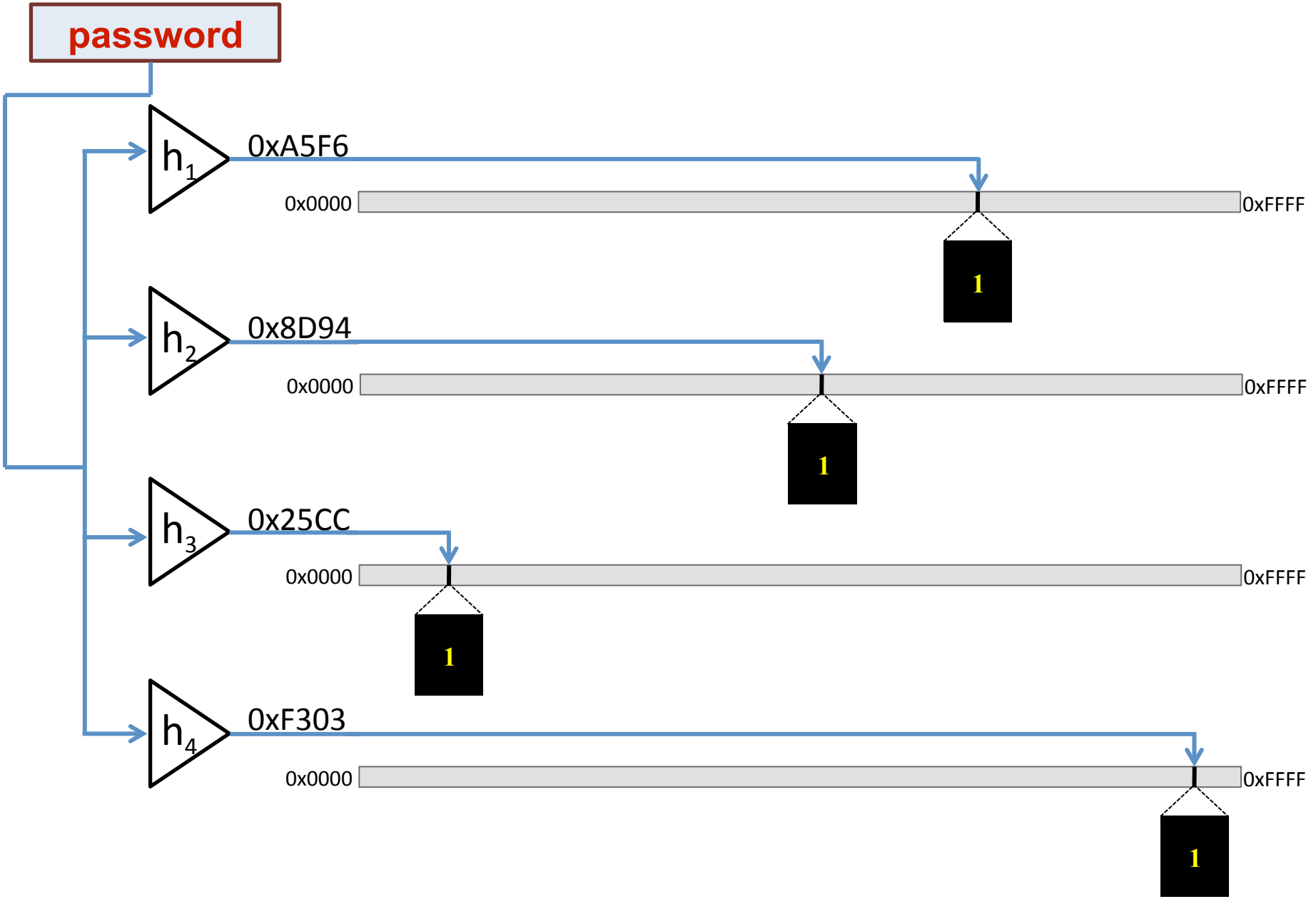
a few false positives are OK

We'll implement a *probabilistic* oracle

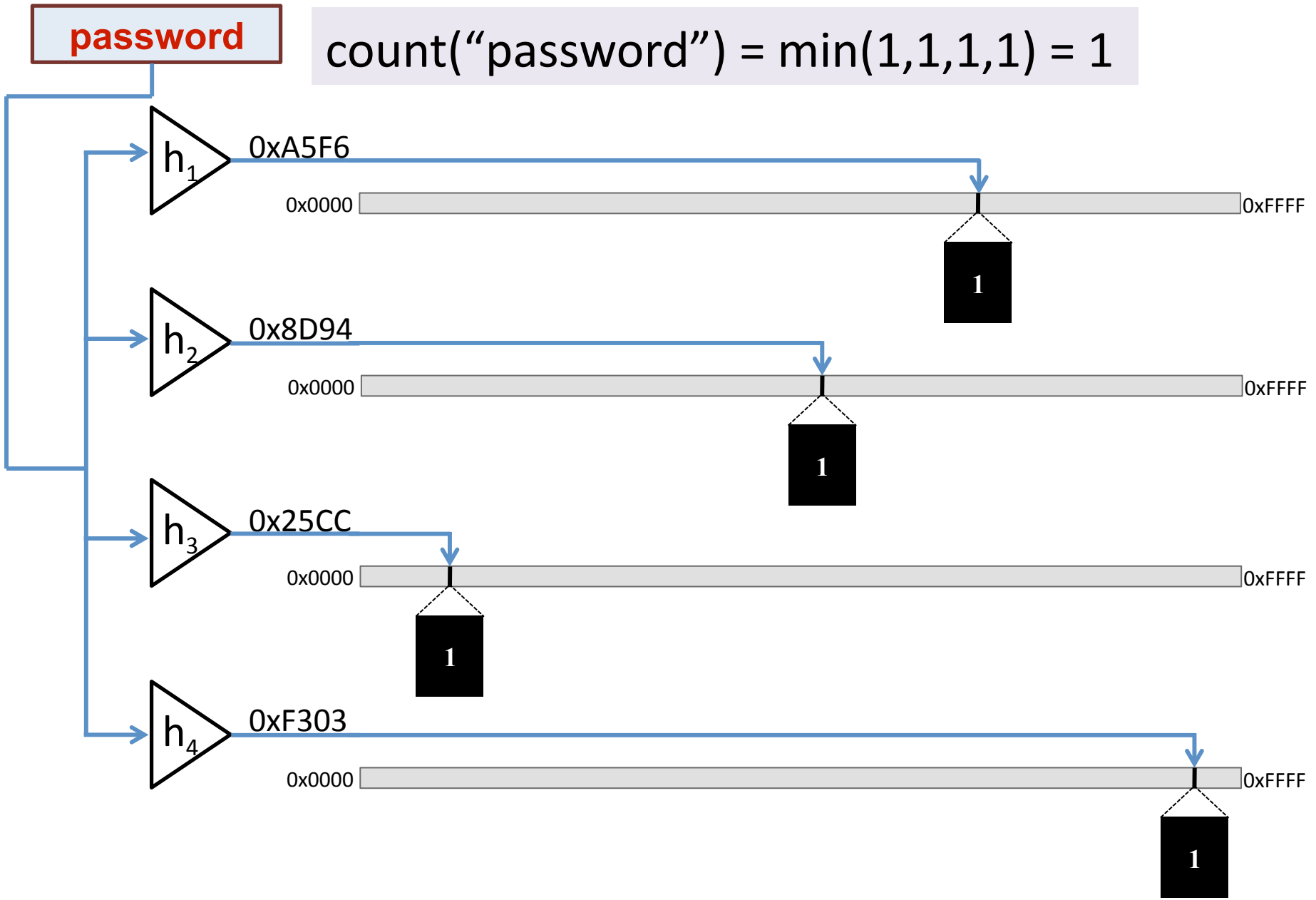
- False positives (falsely popular), no false negatives
- Count-min sketch
  - Relative of bloom filter (and counting bloom filter)

Base case (single table) of a count-min sketch

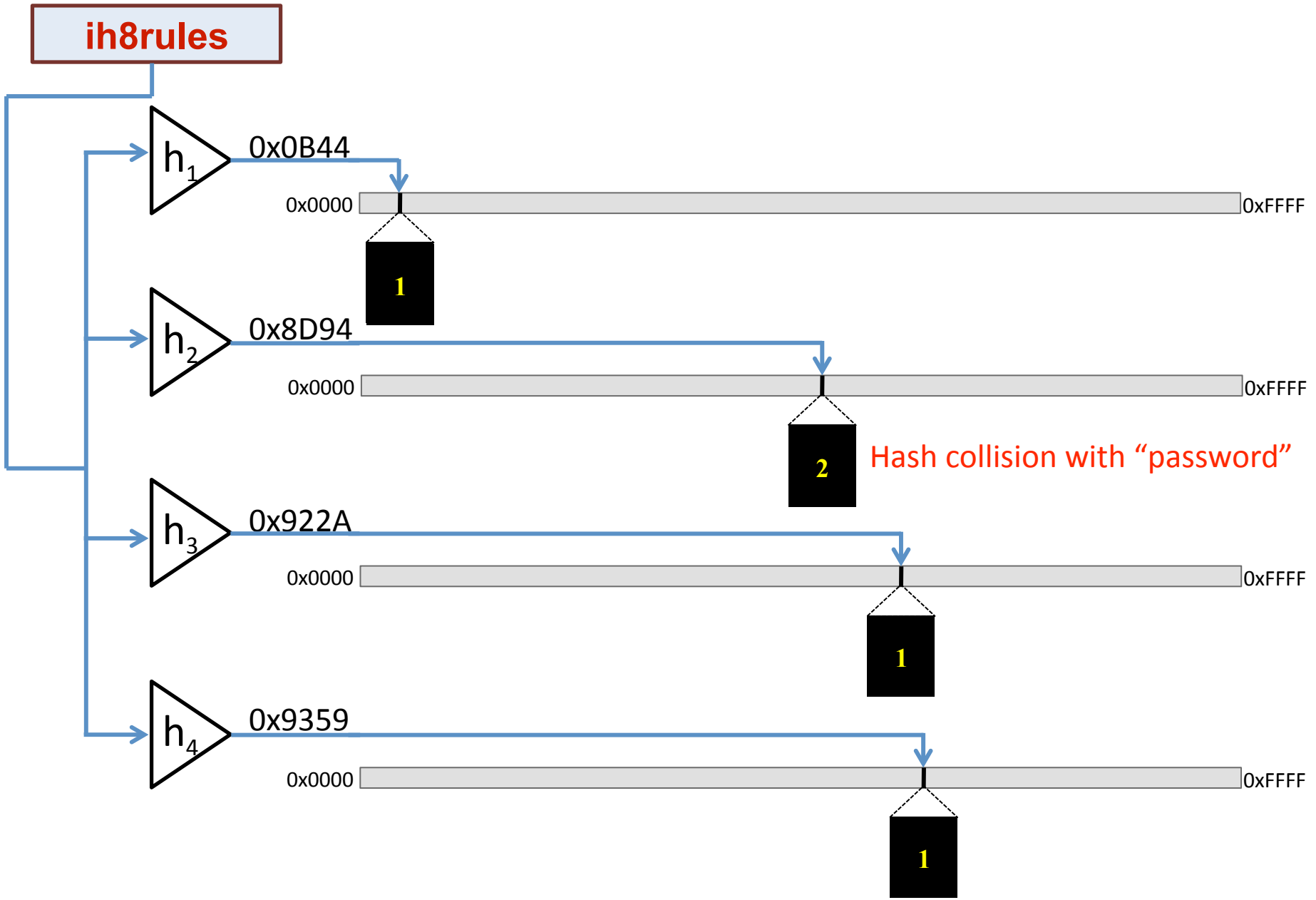
Count-min sketch: add("password")



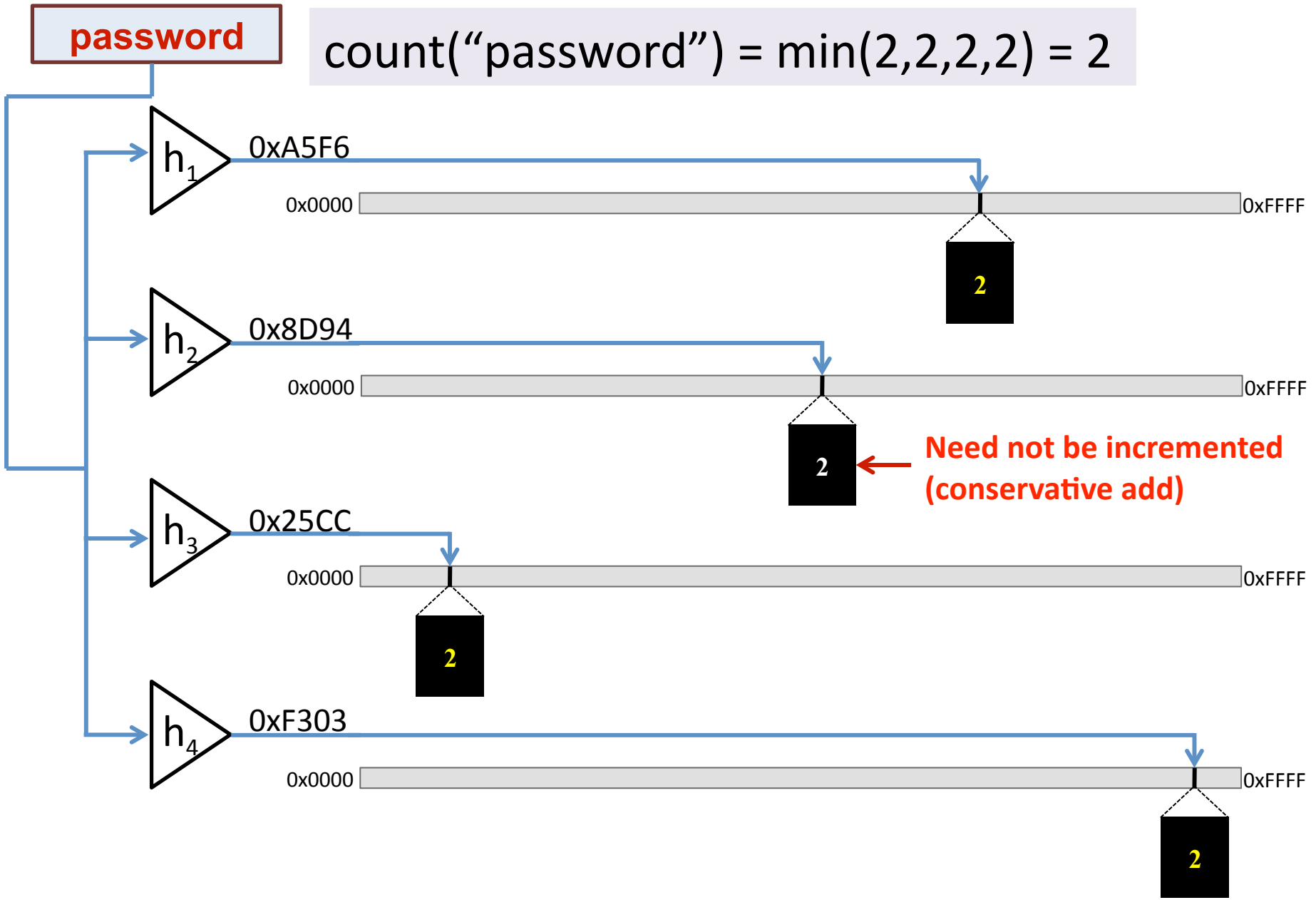
Count-min sketch: count("password")



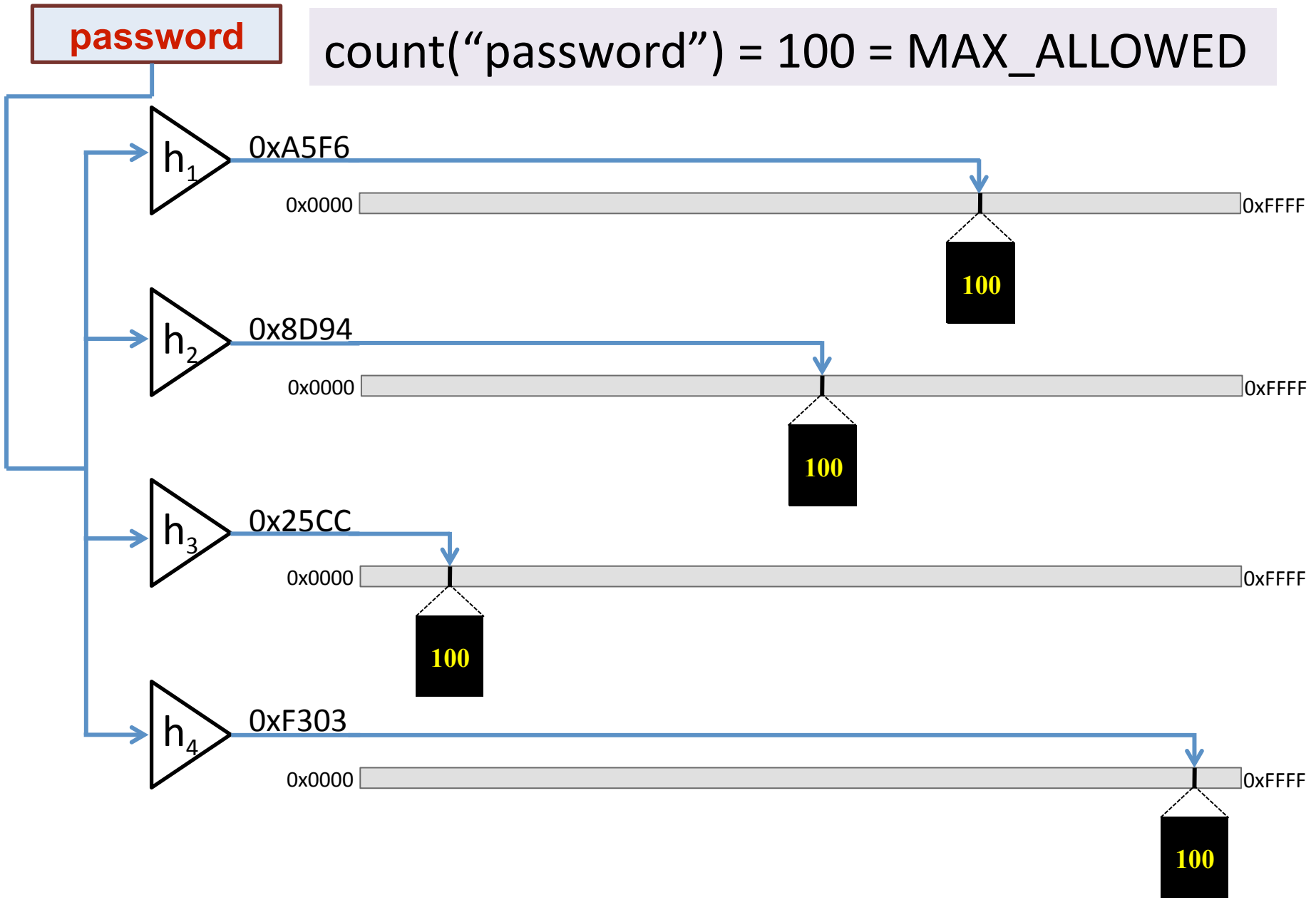
add("ih8rules")



Count-min sketch: add("password")



Count-min sketch: add("password")



Dangers of tracking popular passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~
- Attackers will use for offline statistical guessing
  - ~~Crack using only passwords in the popularity list~~
  - Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)
  - Filter candidate password list (with access to oracle)

False positives to the rescue!

- Randomly generated password x likely to have count(x) > 0

Dangers of tracking user passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~
- Attackers will use for offline statistical guessing
  - ~~Crack using only passwords in the popularity list~~
  - ~~Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)~~
  - Filter candidate password list (with access to oracle)

False positives to the rescue, again!

- Assumptions
  - 2% false positive rate for count-min sketch
  - 20% of user password choices are too popular

- Implications
  - 9% of the passwords rejected as too popular were actually false positives

  - Dictionary of 2^{60} 10 char passwords, filtered to 2^{54} (2% of 2^{60})

If dictionary cracked, force all passwords to be changed.

Dangers of tracking popular passwords

- Attackers will use for statistical guessing attacks
  - ~~Against you~~
  - ~~Against other sites~~
- Attackers will use for offline statistical guessing
  - ~~Walk the password list (if popularity list is plaintext)~~
  - ~~Crack popularity list entries (which are unsalted) to identify passwords in password file (which is salted)~~
  - ~~Filter candidate password list (with access to oracle)~~

One last warning

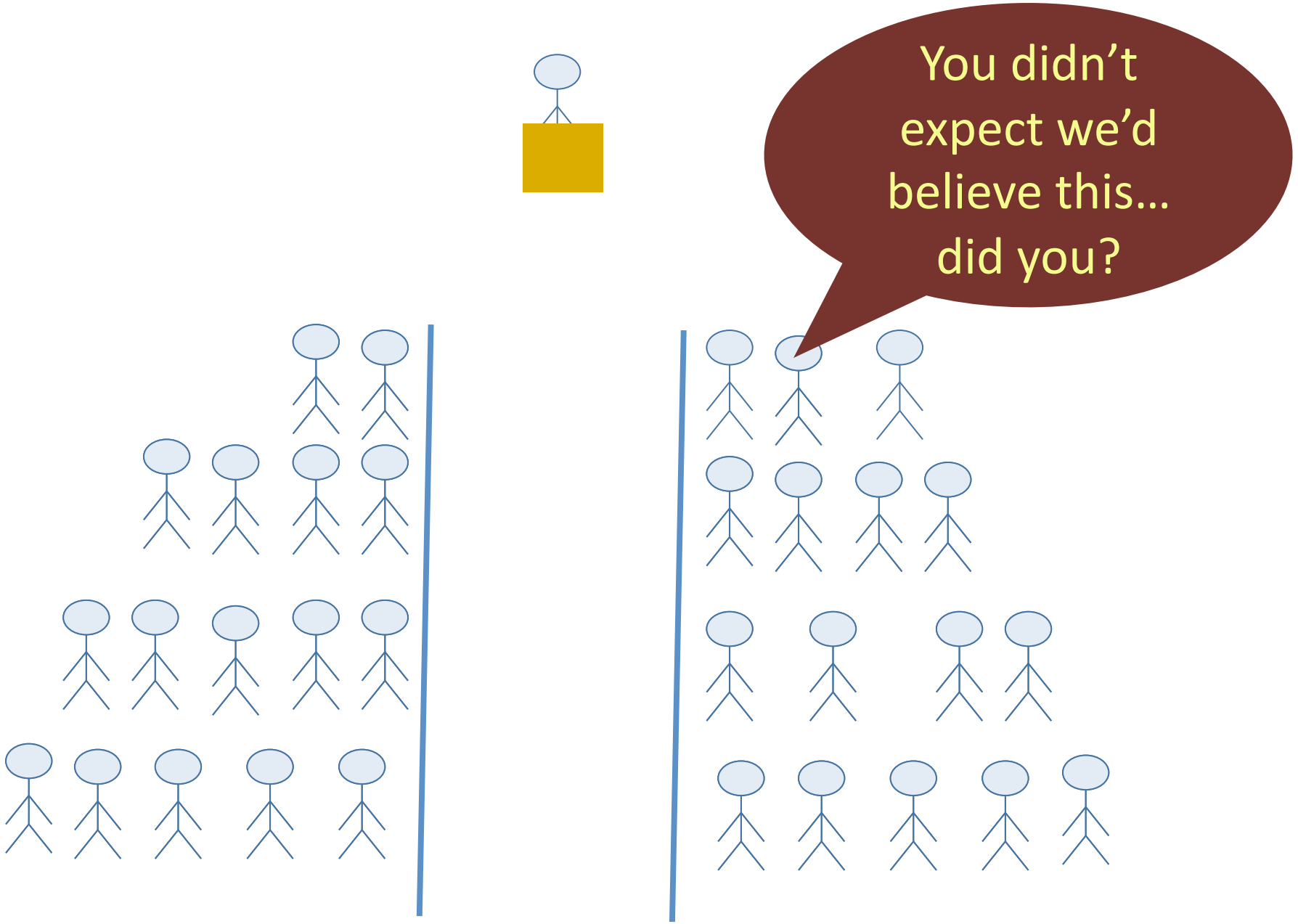
Popular *strategies* can be dangerous even if passwords are unique

Unique passwords, dangerously popular strategies

- Passwords with derivative of username
  - "stuspassword", "sutspassword"

- Passwords containing text that can be found on web search of user
  - http://**bing**.com/?q=stus popularityiseverything

Backup Slide for Responding to Questions



Questions?

I'm sorry dear,
but if this represents
the best presentation
we'll be capable of,
even with millions of
additional years to
evolve, maybe it's best
that we not reproduce.