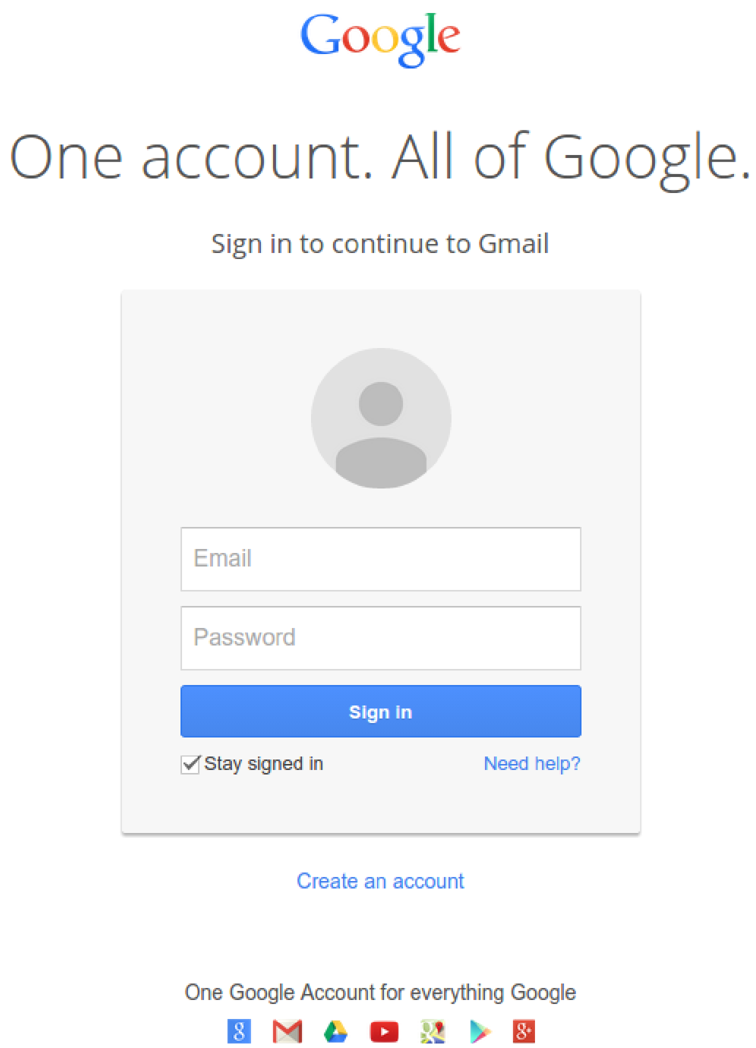
# Passwords and Authentication

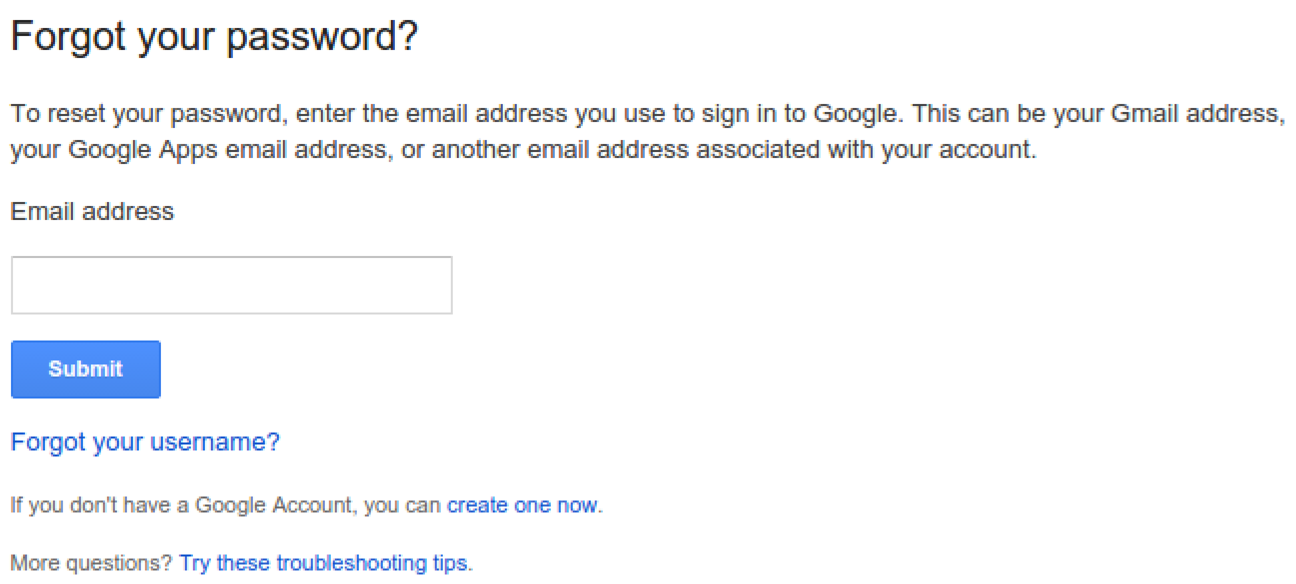
EECS 388: Introduction to Computer Security
March 30, 2015

# Passwords



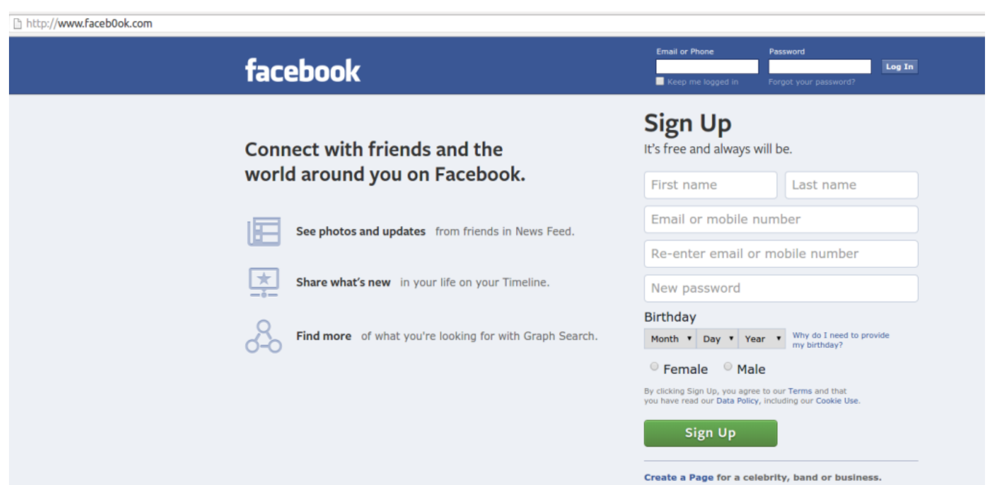
Google
One account. All of Google.
Sign in to continue to Gmail
Email
Password
Sign in
Stay signed in
Need help?
Create an account
One Google Account for everything Google

# Passwords – Usability



# Attacks – Stealing passwords

- From the user
  - Key loggers (hardware, malware, shoulder surfing)
  - Phishing attacks
  - Network attacks



# Attacks – Stealing passwords

- From the website
  - Malware on website
  - Database dump (SQL Injection, shell injection)

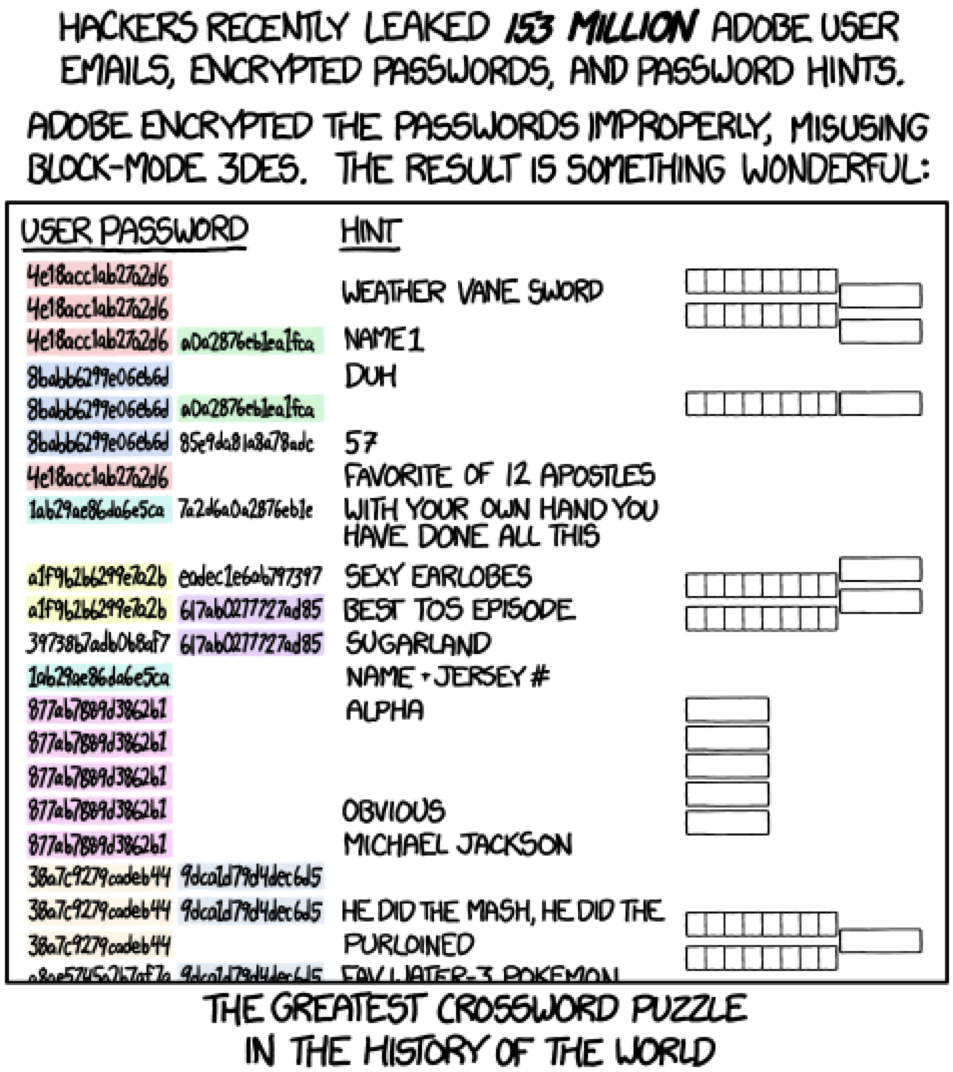
| Site | # | Year | Hashed? |
|---|---|---|---|
| csdn.net | 6428630 | 2011 | no |
| gawker.com | 748559 | 2010 | yes |
| voices.yahoo.com | 442837 | 2012 | no |
| militarysingles.com | 163482 | 2012 | yes |
| rootkit.com | 81450 | 2011 | yes |
| myspace.com | 49711 | 2006 | no |
| porn.com | 25934 | 2011 | no |
| hotmail.com | 8504 | 2009 | no |
| facebook.com | 8183 | 2011 | no |
| youporn.com | 5388 | 2012 | no |

# Attacks – Stealing passwords

- From **other** websites
  - Password reuse

| Adobe password data | | Password hint | |
|---|---|---|---|
| 110edf2294fb8bf4 | -> | numbers 123456 | ❶ 123456 |
| 110edf2294fb8bf4 | -> | ==123456 | |
| 110edf2294fb8bf4 | -> | c'est "123456" | |
| 8fda7e1f0b56593f e2a311ba09ab4707 | -> | numbers | ❷ 12345678 |
| 8fda7e1f0b56593f e2a311ba09ab4707 | -> | 1-8 | |
| 8fda7e1f0b56593f e2a311ba09ab4707 | -> | 8digit | |
| 2fca9b003de39778 e2a311ba09ab4707 | -> | the password is password | ❸ password |
| 2fca9b003de39778 e2a311ba09ab4707 | -> | password | |
| 2fca9b003de39778 e2a311ba09ab4707 | -> | rhymes with assword | |
| e5d8efed9088db0b | -> | q w e r t y | ❹ qwerty |
| e5d8efed9088db0b | -> | ytrewq tagurpidi | |
| e5d8efed9088db0b | -> | 6 long qwert | |
| ecba98cca55eabc2 | -> | sixxone | ❺ 111111 |
| ecba98cca55eabc2 | -> | 1*6 | |
| ecba98cca55eabc2 | -> | sixones | |

# Attacks – Stealing passwords



# Attacks – Password guessing

# Attacks – Password guessing

| PIN | Frequency |
|---|---|
| 1234 | 10.713% |
| 1111 | 6.016% |
| 0000 | 1.881% |
| 1212 | 1.197% |
| 7777 | 0.745% |
| 1004 | 0.616% |
| 2000 | 0.613% |
| 4444 | 0.526% |
| 2222 | 0.516% |
| 6969 | 0.512% |
| 9999 | 0.451% |
| 3333 | 0.419% |
| 5555 | 0.395% |
| 6666 | 0.391% |
| 1122 | 0.366% |
| 1313 | 0.304% |
| 8888 | 0.303% |
| 4321 | 0.293% |
| 2001 | 0.290% |
| 1010 | 0.285% |

# Attacks – Password Databases

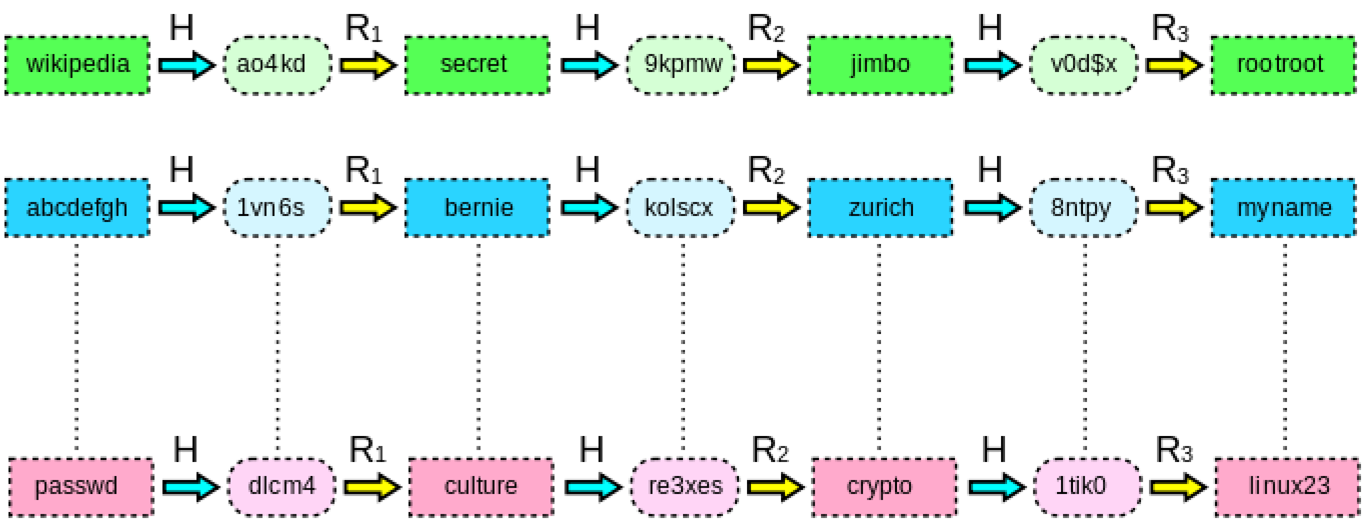
- Server must be able to authenticate users
  - Could store username/password in database
  - Better solutions?

# Password Hashing

- Simple:
  - store **H(Password)**
  - Attacks?

# Rainbow tables

- Similar to a lookup table
- Attacker(s) can trade-off disk-space vs. CPU time
  - Recovered **90%** of **6.5M** LinkedIn passwords in **6 days**



# Rainbow table defense

- Good: salted hashes
  - Store **H(Password + user-specific salt)**
- Better: slow hash functions
  - Bcrypt
    - Based off expensive key-setup of Blowfish
  - Scrypt
    - Requires large amounts of memory
      - Though can be traded off for CPU time
    - Cryptocurrencies have spurred ASIC implementations

# Password Hashing Future

## Password Hashing Competition

INTRODUCTION / CALL FOR SUBMISSIONS / CANDIDATES / TIMELINE / INTERACTION / EVENTS / FAQ / DISCLAIMER

### Candidates

24 submissions have been accepted. The packages available for download include a subdirectory containing the submission received (with documentation and source code) and a text file `info` containing the name of the submitted algorithms and contact information of the authors. Versions are numbered from v( (version at the time of the submission deadline), to v1, v2, etc. A direct link to the specifications is also available. A wiki provides more information on the submissions.

Finalists have been announced on December 8, 2014 and are (in alphabetical order): Argon, battcrypt, Catena, Lyra2, Makwa, Parallel, POMELO, Pufferfish yescrypt. Rationale for this selection are documented in a status report, first published on February 3, 2015.

| Name | Downloads | Designer(s) |
|---|---|---|
| AntCrypt | v0 PDF | Markus Duermuth, Ralf Zimmerman |
| Argon | v2 PDF | Alex Biryukov, Dmitry Khovratovich |
| battcrypt | v0 PDF | Steve Thomas |
| Catena | v3 PDF | Christian Forler, Stefan Lucks, Jakob Wenzel |
| ~~Catfish~~ | | Bo Zhu, Xinxin Fan, Qi Chai, Guang Gong |
| Centrifuge | v0 PDF | Rafael Alvarez |
| EARWORM | v0 PDF | Daniel Franke |
| Gambit | v1 PDF | Krisztián Pintér |
| Lanarea | v0 PDF | Haneef Mubarak |
| Lyra2 | v3 PDF | Marcos A. Simplicio Jr, Leonardo C. Almeida, Ewerton R. Andrade, Paulo C. F. dos Santos, Paulo S. L. M. Barreto |
| ~~M3lcrypt~~ | | Isaiah Paul Makwakwa |

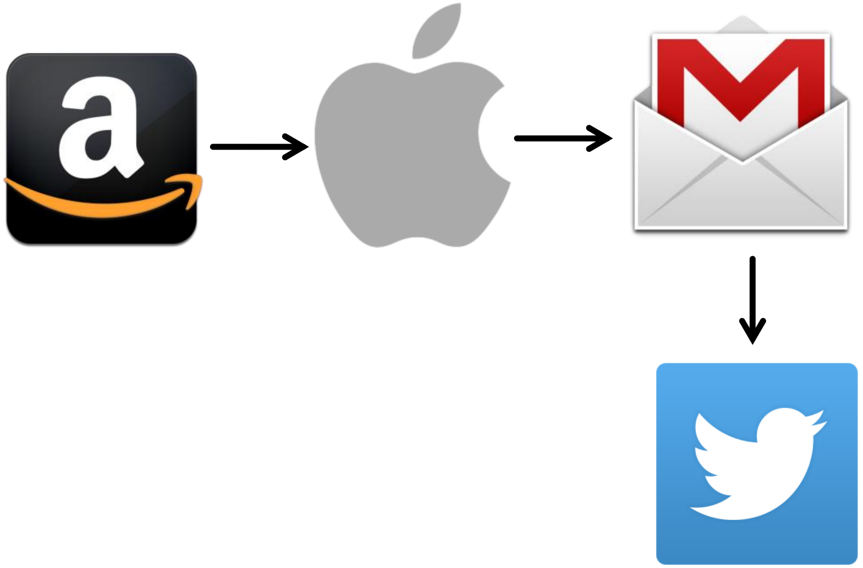
# Password Recovery

- Sometimes users forget passwords
  - Or are locked out!
- Reset vs. Recovery
- Have to authenticate – but how?

# Password recovery gone wrong

Mat Honan

*Photo: Ariel Zambelich/Wired. Illustration: Ross Patton/Wired*

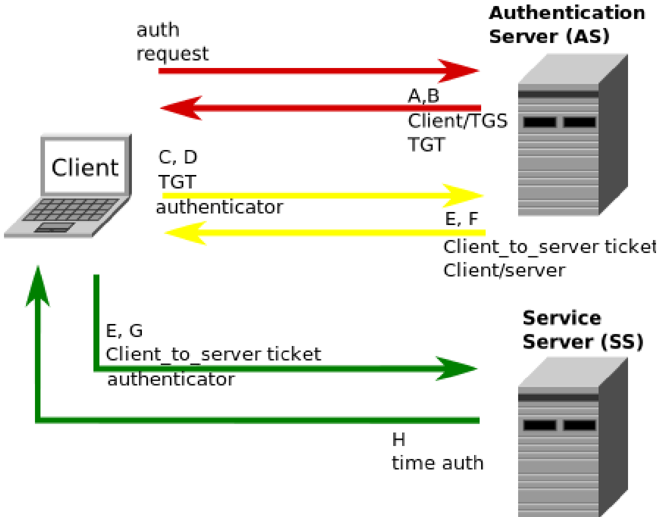


# Password Managers

- Store passwords
  - Generally encrypted under master password
- Generate passwords
  - Allows easier unique passwords per site

# Network authentication

- User sends password
  - Hopefully over encrypted channel (TLS/SSH)
- Challenge-based authentication
  - Server sends challenge (nonce)
  - User sends response (H(password, nonce))
- Kerberos



# Multi-factor authentication

- Something you know, something you have, something you are

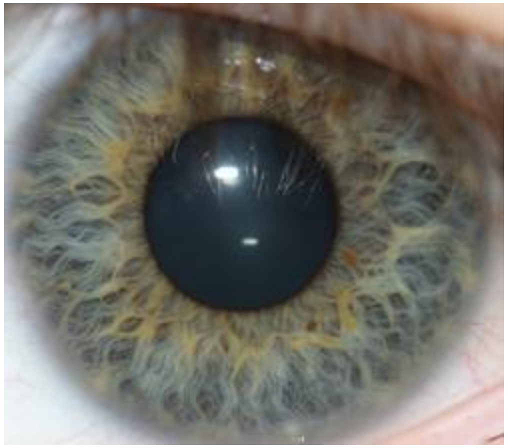
# Something you have

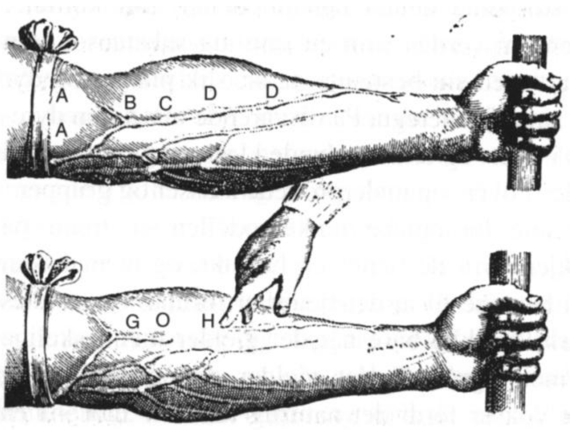
- Physical (hardware) token
  - RSA token
  - Yubikey
  - Smartphone?


- Common Protocols
  - HOTP: $(\mathrm{HMAC}(K,C)\ \&\ \mathtt{0x7FFFFFFF})\ \mathrm{mod}\ 10^{d}$
  - TOTP: HOTP, where $C = (\mathrm{now} - T_0)\ /\ T_{step}$

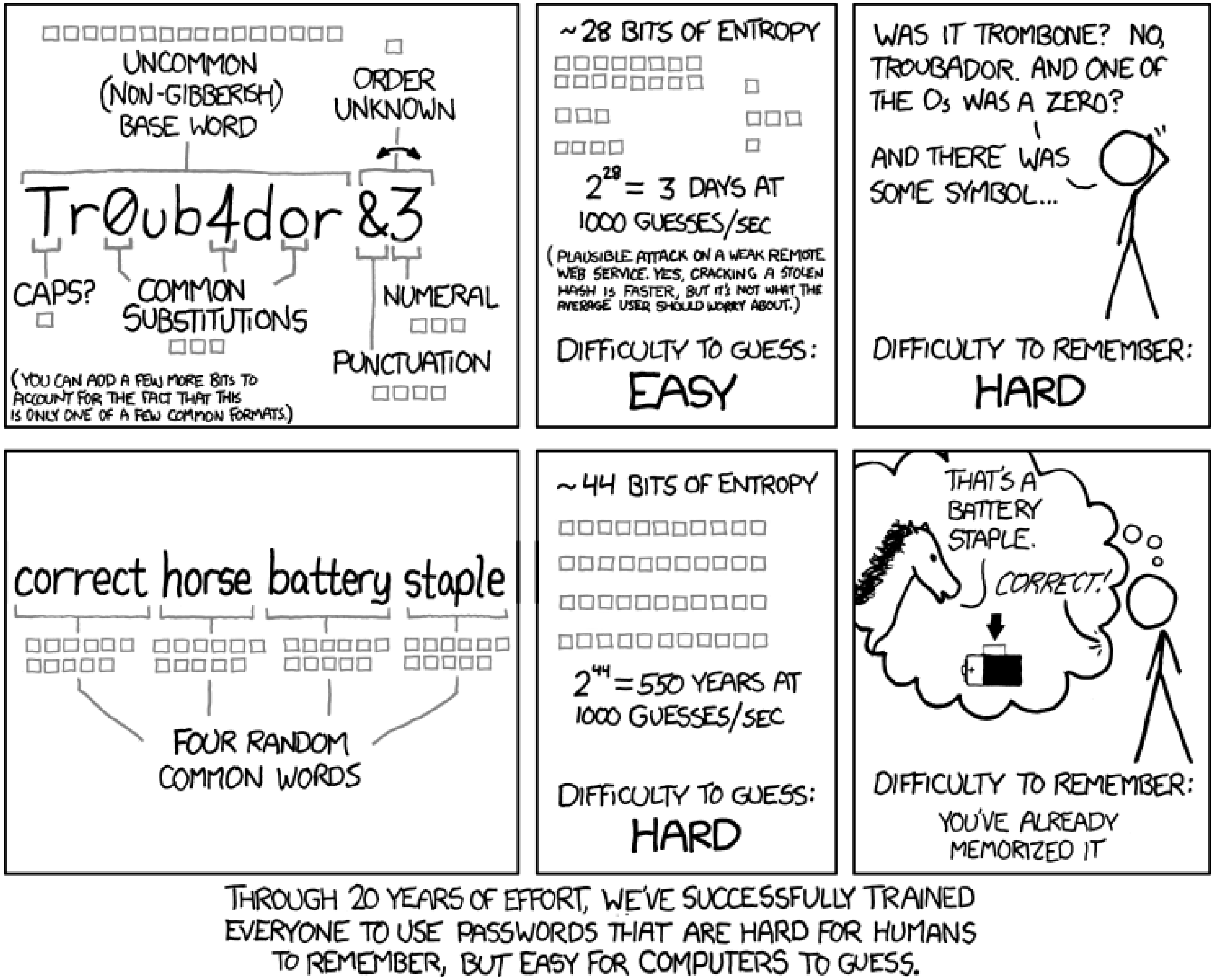
# Something you are

- Biometrics
  - Hopefully unique to you
  - Disadvantages?
  - Challenges?






# Password strength



# Users *can* memorize long passwords

## Towards reliable storage of 56-bit secrets in human memory

Joseph Bonneau
*Princeton University*

Stuart Schechter
*Microsoft Research*

**Abstract**

Challenging the conventional wisdom that users cannot remember cryptographically-strong secrets, we test the hypothesis that users can learn randomly-assigned 56-bit codes (encoded as either 6 words or 12 characters) through *spaced repetition*. We asked remote research participants to perform a distractor task that required logging into a website 90 times, over up to two weeks, with a password of their choosing. After they entered their chosen password correctly we displayed a short code (4 letters or 2 words, 18.8 bits) that we required them to type. For subsequent logins we added an increasing delay prior to displaying the code, which participants could avoid by typing the code from memory. As participants learned, we added two more codes to comprise a 56.4-bit secret. Overall, 94% of participants eventually typed their entire secret from memory, learning it after a median of 36 logins. The learning component of our system added a median delay of just 6.9 s per login and a total of less than 12 minutes over an average of ten days. 88% were able to recall their codes exactly when asked at least three days later, with only 21% reporting having written their secret down. As one participant wrote with surprise, "the words are branded into my brain." While our study is preliminary in nature, we believe it debunks the myth that users are inherently incapable of remembering cryptographically-strong secrets for a select few high-stakes scenarios, such as a password for enterprise login or as a master key to protect other credentials (e.g., in a password manager).

### 1 Introduction

*Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (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.)*

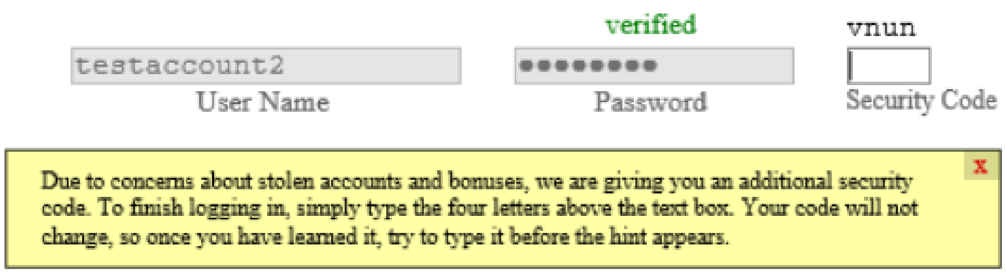
—Kaufman, Perlman and Speciner, 2002 [60]

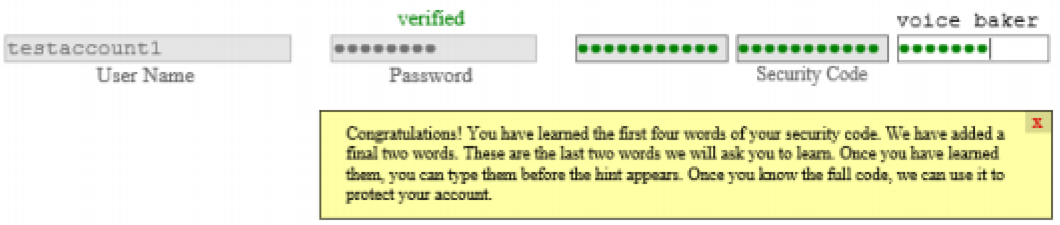
The dismissal of human memory by the security community reached the point of parody long ago. While assigning random passwords to users was considered standard as recently in the mid-1980s [2], the practice died out in the 90s [5] and NIST guidelines now presume all passwords are user-chosen [35]. Most banks have even given up on expecting customers to memorize random four-digits PINs [25].

We hypothesized that perceived limits on humans' ability to remember secrets are an artifact of today's systems, which provide users with a single brief opportunity during enrollment to permanently imprint a secret password into long-term memory. By contrast, modern theories of the brain posit that it is important to *forget* random information seen once, with no connection to past experience, so as to avoid being overwhelmed by the constant flow of new sensory information [11].

We hypothesized that, if we could relax time constraints under which users are expected to learn, most could memorize a randomly-assigned secret of 56 bits. To allow for this memorization period, we propose using an alternate form of authentication while learning, which may be weaker or less convenient than we would like in the long-term. For example, while learning a strong secret used to protect an enterprise account, users might be allowed to login using a user-chosen password, but only from their assigned computer on the corporate network and only for a probationary period. Or, if learning a master key for their password manager, which maintains a database of all personal credentials, users might only be allowed to upload this database to the network after learning a strong secret used to encrypt it.

By relaxing this time constraint we are able to exploit *spaced repetition*, in which information is learned



# Future of authentication?

## I Think, Therefore I Am: Usability and Security of Authentication Using Brainwaves*

John Chuang[1], Hamilton Nguyen[2], Charles Wang[2], and Benjamin Johnson[3]

[1] School of Information, UC Berkeley
chuang@ischool.berkeley.edu
[2] Department of EECS, UC Berkeley
{hamiltonnguyen,charleswang}@berkeley.edu
[3] Department of Mathematics, UC Berkeley
benjamin@math.berkeley.edu

**Abstract.** With the embedding of EEG (electro-encephalography) sensors in wireless headsets and other consumer electronics, authenticating users based on their brainwave signals has become a realistic possibility. We undertake an experimental study of the usability and performance of user authentication using consumer-grade EEG sensor technology. By choosing custom tasks and custom acceptance thresholds for each subject, we can achieve 99% authentication accuracy using single-channel EEG signals, which is on par with previous research employing multi-channel EEG signals using clinical-grade devices. In addition to the usability improvement offered by the single-channel dry-contact EEG sensor, we also study the usability of different classes of mental tasks. We find that subjects have little difficulty recalling chosen "pass-thoughts" (e.g., their previously selected song to sing in their mind). They also have different preferences for tasks based on the perceived difficulty and enjoyability of the tasks. These results can inform the design of authentication systems that guide users in choosing tasks that are both usable and secure.

**Keywords:** pass-thoughts, EEG, authentication, usability.

### 1 Introduction

Advances in EEG (electro-encephalography) bio-sensor technologies have opened up brainwave research and application development at an unprecedented level in recent years. Traditionally, EEG data capture has been performed in clinical settings using invasive probes under the skull or wet-gel electrodes arrayed over the scalp. Now, similar data can be collected using consumer-grade non-invasive dry-contact sensors built into audio headsets and other consumer electronics. This opens up immense possibilities for using brainwave signals in different application domains. Originally limited to neuroscience research and clinical treatment

* This research was supported in part by the National Science Foundation under award CCF-0424422 (TRUST).

A.A. Adam, M. Brenner, and M. Smith (Eds.): FC 2013, LNCS 7862, pp. 1–16, 2013.