image: Marsmettnn Tallahassee

Heartbleed & staying secure online

A presentation for WordPress Findhorn, April 2014, by Mark Rowatt Anderson

rowatt

What we'll cover

- What is heartbleed & why should I care?
- Dealing with heartbleed
- Good password hygiene
- Keeping WordPress secure

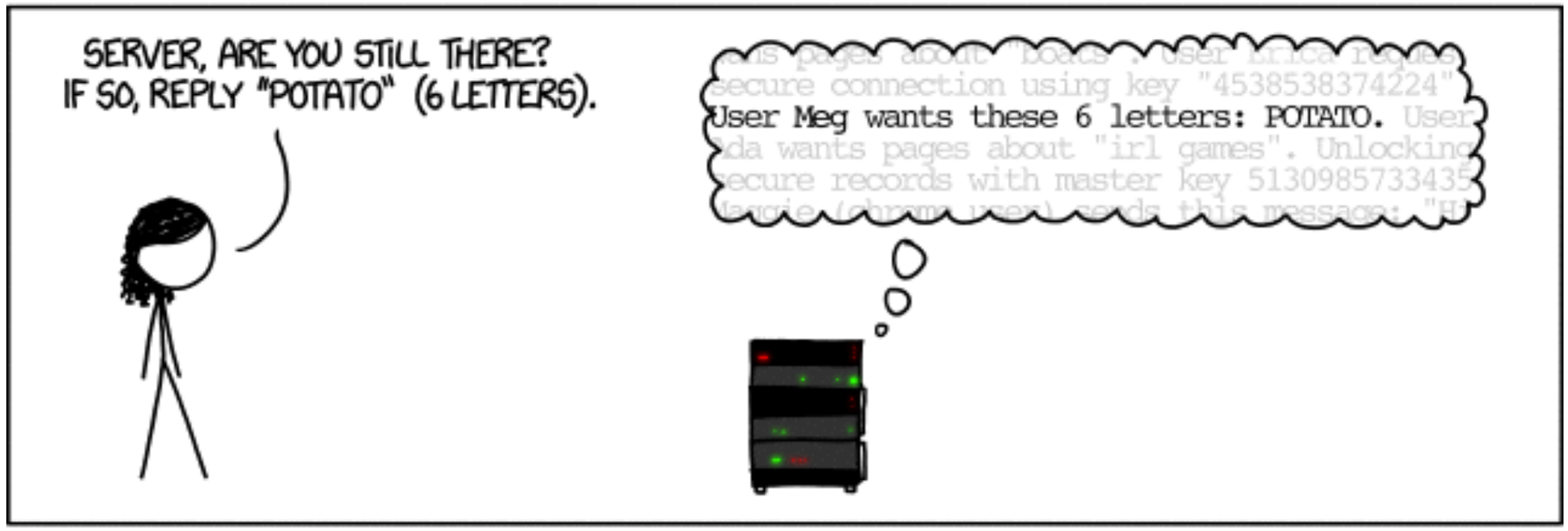
rowatt

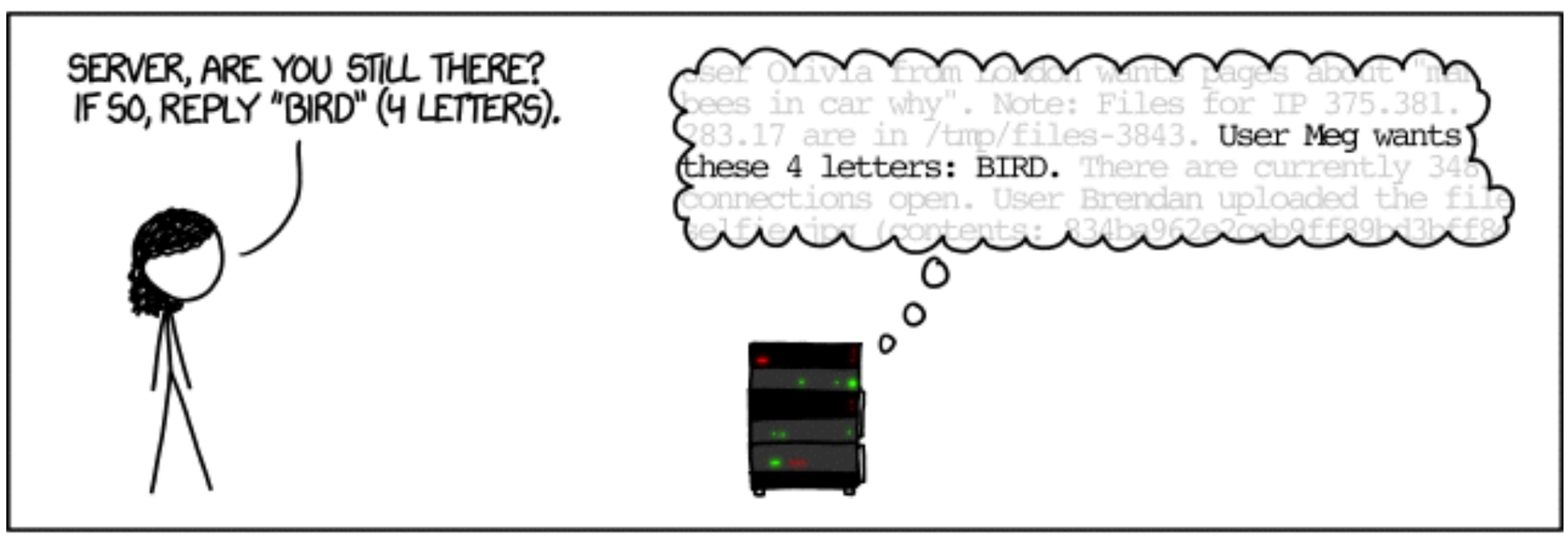
What is the heartbleed bug?

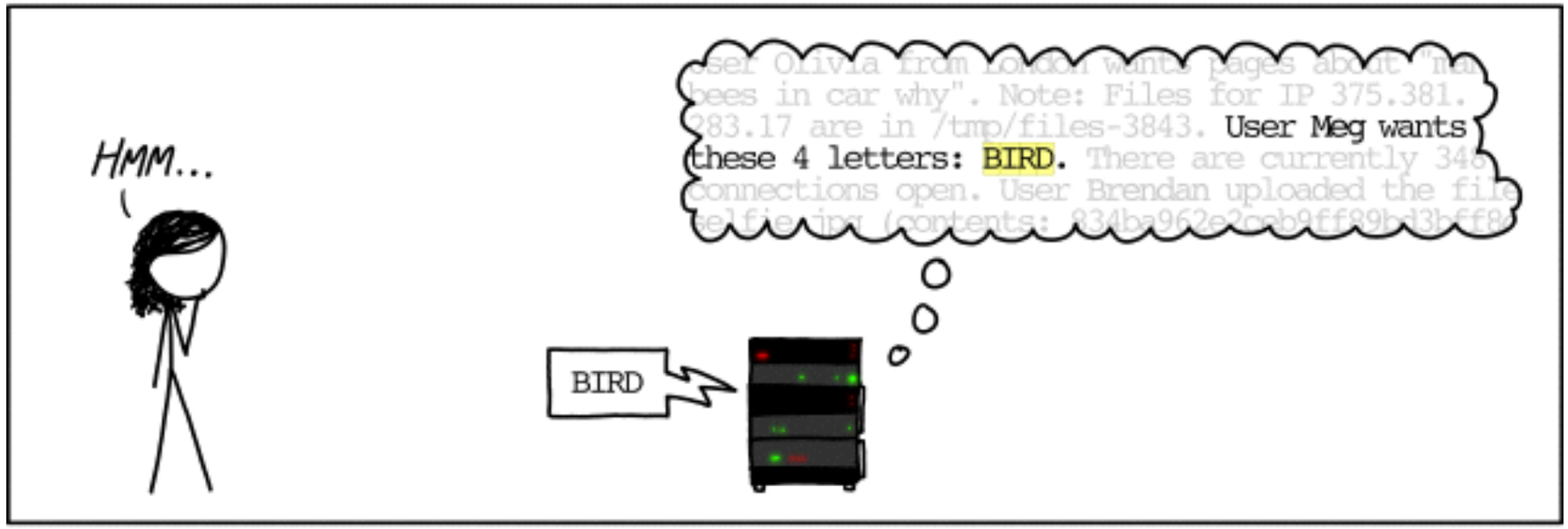
- A bug in OpenSSL (server security software) heartbeat system
- Allows hackers to decrypt encrypted pages
- Affected SW in use for 2 years
    - nobody knew, but maybe some hackers did?
- Left many major sites vulnerable for a few days
    - hackers have exploited this
- As of 17th April 2014
    - Top 1,000 sites: 0 sites vulnerable
    - Top 10,000 sites: 53 sites vulnerable (only 0.53% vulnerable)
    - Top 100,000 sites: 1595 sites vulnerable (1.5% still vulnerable)
    - Top 1,000,000 sites: 20320 sites vulnerable (2% still vulnerable)

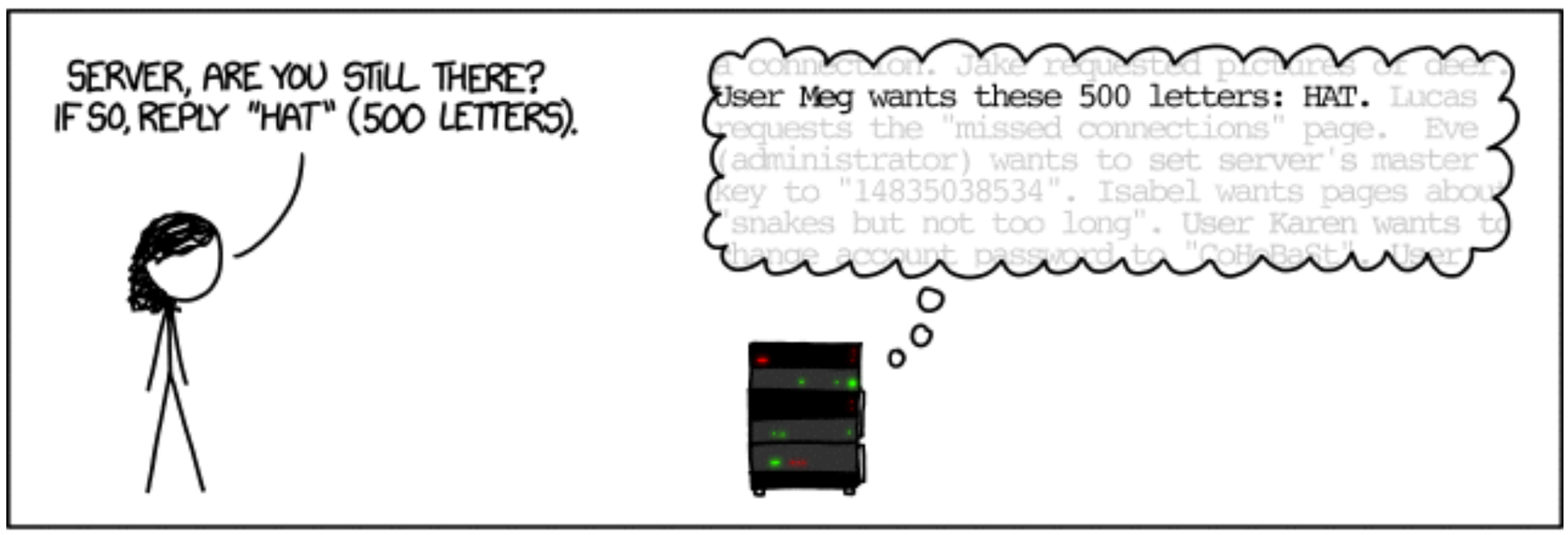
rowatt

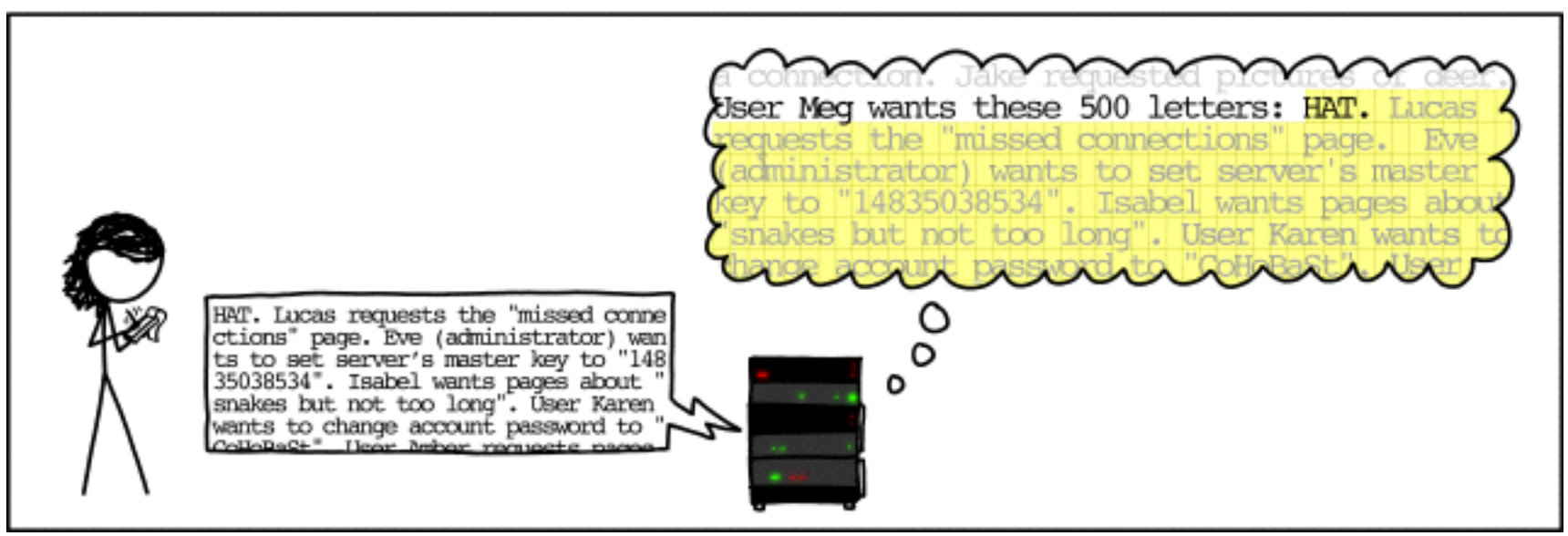
HOW THE HEARTBLEED BUG WORKS:






HMM...
BIRD
User Olivia from London wants pages about "man bees in car why". Note: Files for IP 375.381. 283.17 are in /tmp/files-3843. User Meg wants these 4 letters: BIRD. There are currently 34 connections open. User Brendan uploaded the file selfie.jpg (contents: 034ba962e2ceb9ff89bd3bf8


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHeRaSt". User


User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHeRaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "

source: xkcd

Why do I care?

- Hackers may have YOUR password for any sites which were vulnerable (even if those sites now fixed)

- If you used that password anywhere else, all those online accounts are vulnerable

- Many sites have been affected…

rowatt

Change your passwords on all these sites

- Facebook
- Instagram
- Pinterest
- Tumblr
- Google
- Yahoo
- Godaddy
- Flickr
- Netflix
- YouTube
- Dropbox
- WordPress.com

rowatt

Sites known to have been hacked

- Mumsnet
- Canada Revenue Agency

rowatt

What to do about it?

- Change passwords
  - on most important sites
  - on any sites you use same password
  - on any site specifically recommended
- Follow good password practice

Which password is strongest?

1. password
2. 147258369
3. p@$$w0rd
4. shown resort curd annoy
5. rrwfatml?
6. Tr0ub4dor&3

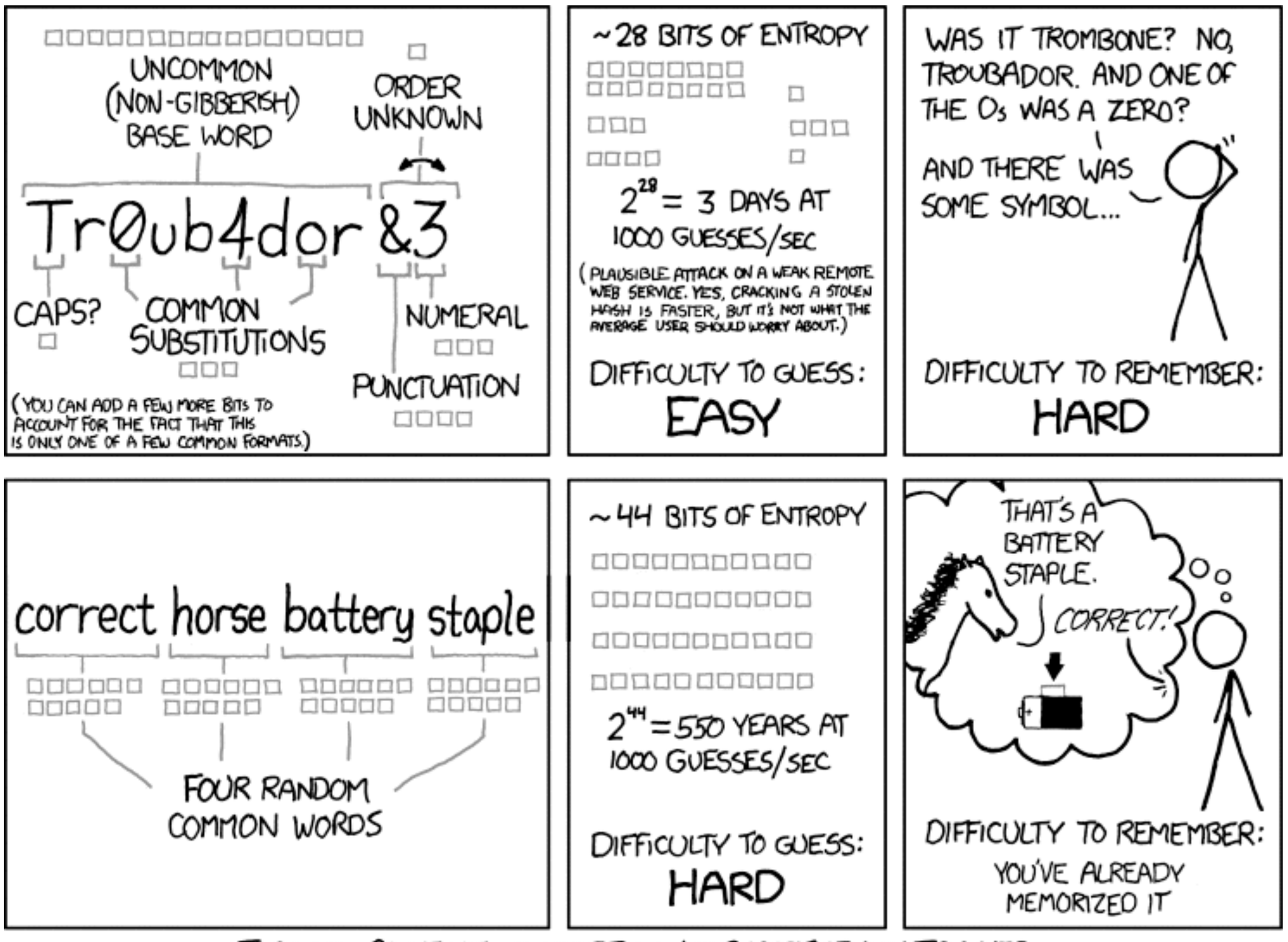
rowatt

What makes a good password

- Lots of entropy (randomness)
- Hard to guess but easy to remember
- Which password was strongest?

shown resort curd annoy

rowatt



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

source: xkcd

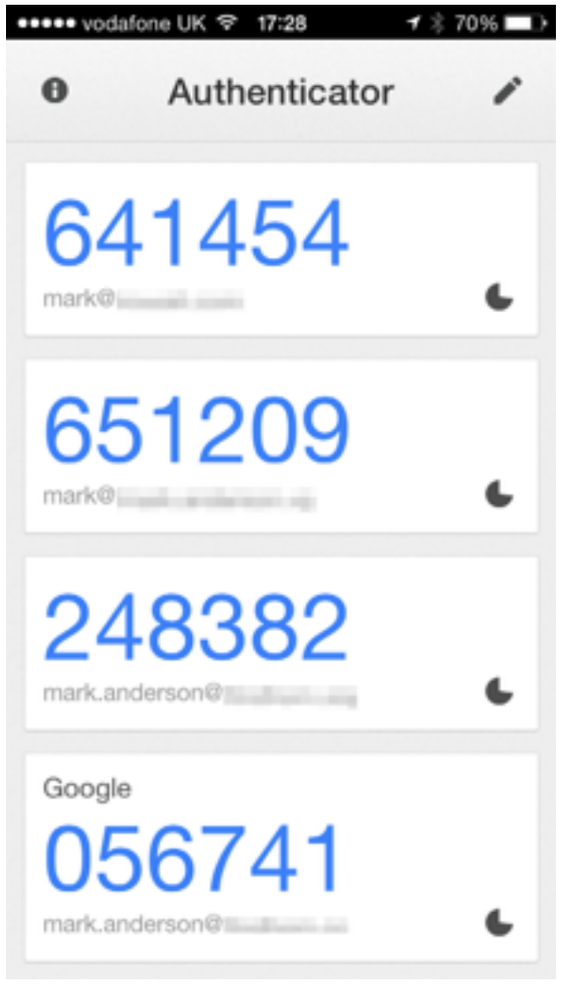
Good password hygiene

- Never (ever) use the same password on different sites
- Use totally random passwords (the longer the better)
- Use a password manager
- Use 2 factor authentication where possible
- Make doubly sure that your email account is secure

rowatt

2 Factor Authentication

- Much harder to crack than a single password
- Requires a device
  - secure key
  - smartphone app
  - SMS to phone
- Available for many sites
  - Google, Microsoft, Dropbox, Facebook, WordPress, Evernote… and many more



rowatt

What about WordPress?

- Don’t use the ‘admin’ user account
- Use a good password
- Use 2 Factor Authentication with JetPack (or wordpress.com)
- Only use reputable plugins/themes (e.g. from wordpress.org)
- Keep WP & plugins updated
- Backup your site regularly
- Scan your site with Sucuri

rowatt

Useful resources

- mashable.com
- Major sites affected by heartbleed
- 1Password Watchtower
- Diceware
- Presentation on WordPress security

rowatt

Password Managers

- Dashlane (free version available)
- LastPass (free version available)
- KeePass (free, open source)
- 1Password
- Roboform

rowatt

image: Tim Kirman/Flickr

Thanks for listening!

rowatt