PASSWORDS

Passwords

- Have long been associated with security to:
  - Unlock a door
  - To pass a guard
  - To distinguish friend from enemy
- We use them to:
  - Withdraw money from an ATM
  - Banking online
  - Buy and sell on the internet

Our Passwords

- Have some weaknesses:
  - You have no guarantee that someone has your password; with or without your knowledge
  - Human behaviour – no one would really want to know my password

Weak Password lists

- Have some weaknesses:
  - Words with numbers deer2000
  - With simple obfuscation j@ke
  - License plate – kissme
  - Doubled words – patpat
  - Patterns – qwerty 123456 abc123

People Select Poor Passwords

- And do little to protect them
- Password theft is a huge problem
- Websites are attractive targets

Think Piece

- Why My Password?

Meet Your Opponent
The Cracker

How do they do it?

- Smart Guesses
- Dictionary attacks
- Brute-force attacks
- Rainbow tables
- Social Engineering
- Key loggers
- Sniffers

Character Diversity

- Numbers
- Letters
- Case
- Special Characters

Password Mania

- Average Person has do know 17 passwords, pin codes etc
- IT people average around 50

500 Worst Passwords

- 1 out of every 9 people have used at least 1 password shown on the list
- 1 out of every 50 people have used 1 of the top 20 passwords
- Consider the following:

500 Worst Passwords

- **ncc1701** The ship number for the Starship Enterprise
  thx1138 The name of George Lucas's first movie, a 1971 remake of an earlier student project
  qazwsx Follows a simple pattern when typed on a typical keyboard
  666666 Six sixes
  7777777 Seven sevens
  ou812 The title of a 1988 Van Halen album
  8675309 The number mentioned in the 1982 Tommy Tutone song. The song supposedly caused an epidemic of people dialing 867- 5309 and asking for "Jenny”

Good Passwords

- **A good password[1]:**
  - **Has both upper and lower case letters**
  - **Has digits and/or punctuation characters as well as letters**
  - **Is easy to remember, so they do not have to be written down**
  - **Can be typed quickly, so someone else cannot look over your shoulder**

Password Length

- Depends on who you ask
- Many consider 8 characters a good minimum
  - NIST suggests this, and less than 64 characters
- Others view 12 as an ideal minimum.
- Still others view 16 characters as an ideal minimum.

DO This

- **Make your password as long as possible.**
- **Use as many different characters as possible**
- **Change your password on a regular basis.**

DO NOT DO THIS

- **Do not use personal information** in your password
- Do not use that are **listed in standard dictionaries**.
- Never use a password that is **the same as your account number**
- Do not use passwords that are **easy to spot while you're typing them in**. Passwords like 12345, qwerty (i.e., all keys right next to each other), or nnnnnn should be avoided.

Aging Passwords

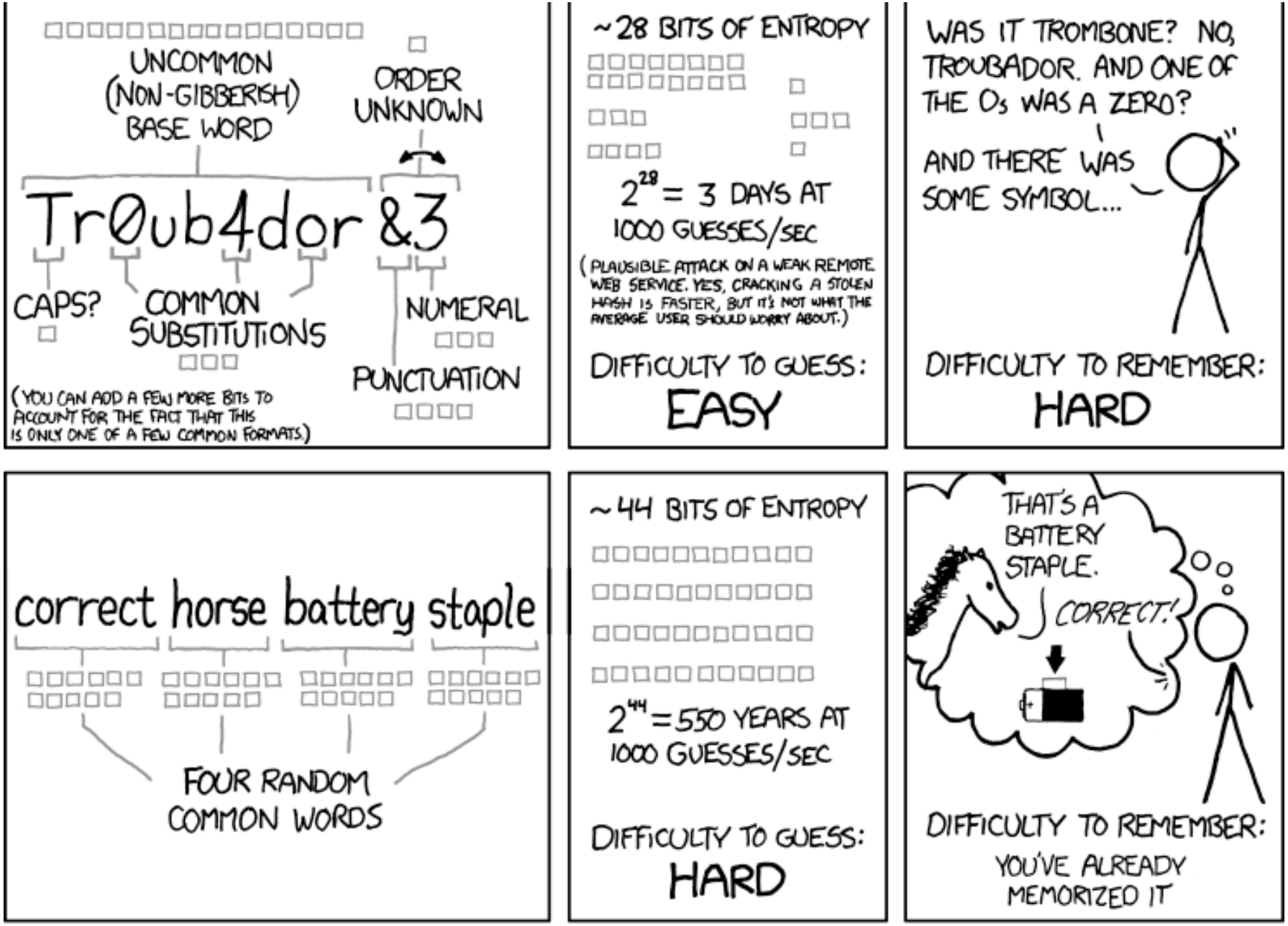
- **Overbearing policies**
- Password Histories
- Who wins?

Managing Passwords

- **Obscurity**
- Secret Questions

Building Strong Passwords

1. Three words
2. Email Address
3. The URL
4. The Title
5. Number Rhymes
6. Get to the Point
7. The Confession
8. The Elbow Mambo
9. Phone Number
10. Letter Swapping



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.

From xkcd.com

Two Step Verification

- Recent events have brought poor authentication processes into sharper view, and drawn attention to a new way of managing the risks associated with password authentication
- Two step verification is a process where the user logs in as normal with a username/password combination, and a 2nd verification token is sent to some device or account, valid for a very short amount of time (30 seconds or so)

Finally
Test Your Password

- Make sure it isn't in the "common list of passwords.txt"
- Try running password hacking tools
  - John the Ripper
  - Cain & Abel

Consequences

- Improper password management has lead to many failed systems
- User accounts info gleaned from other hacks are used to gain system access to databases or admin access to servers
- One compromise can lead to others

Consequences

- Criminal/tortious consequences
  - Ashley Madison – divorce and suicide
- Embarrassment
- Brand integrity

Online checking tools

- You can go to https://haveibeenpwned.com/ to verify if your credentials have been compromised.
  - Passwords may be compromised on these sites as well, even if you haven't found your password in an online dictionary.