CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Computer Security Principles

Lecture 11: Authentication

Authentication

Passwords and passphrases are one example of a form of security measure called **authentication**

We give them to people so that they can use them to prove that they are entitled to use something to which **access is restricted**

Authentication would be used in:

- a restricted area
- a computer system
- an Internet service
- encrypted document

An **authentication factor** is a procedure or chunk of information used to authenticate an individual, that is, to verify that he or she has **access rights**

Authentication Factors

Authentication factors generally fall into one of **three** classes:

- **Inherence** (or human) factors — “Something you are (or do).” These include **biometric measures** for identifying the individual by a physical characteristic such as fingerprints, iris or retina recognition, or automated face recognition, or alternatively by behavioral characteristics such as typing rhythm or voice mannerisms. Location (IP or GPS) also falls into this category.
- **Ownership** (or technical) factors — “Something you have.” These include **identity cards**, communications devices such as passcode tokens, or even a traditional metal key.

Authentication Factors

Authentication factors generally fall into one of three classes:

- **Knowledge** (or personal) factors — "Something you know." These include **passwords** or passphrases, a PIN (personal identification number) or other passcode, the entry combination for a door unlocked by keypad, the answers to a series of questions (challenge-response) and so on.

Authentication Factors

Where more than one authentication factor is used, this is referred to as two- or three-factor (or even **multi-factor**) authentication.

- A "**chip and pin**" bank card, which requires both the possession of the card and the knowledge of the PIN that goes with it.
- Hardware tokens are often implemented as a two-factor measure, since the user needs both possession of the token and knowledge of a PIN in order to use it.
- The addition of other measures such as a username/password combination to access a specific device or service, or a biometric device such as a fingerprint scanner built into a mouse or laptop, increases the authentication factor count, and hopefully the **security** of the access control system.

Types of Two-Factor Authentication

Tokens

- In the most common implementations of **two factor authentication**, the **something you have** component is provided by a small token card.
- The **token card** is a compact electronic device which displays a number on a small screen. By entering this number into the system when you attempt to authenticate (login), you prove that that you are in possession of the card.
- The number displayed by the card changes **frequently**, usually every 30 or 60 seconds.
- To increase security, the electronic device is sometimes protected with a PIN. In these systems, you must enter the correct PIN before the correct numbers are displayed.

Types of Two-Factor Authentication

Biometrics

- Biometric authentication satisfies the regulatory definition of **true multi-factor** authentication.
- Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault.
- There is **great user resistance** to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes.

Types of Two-Factor Authentication

Biometrics

- For many biometric identifiers, the actual biometric information is rendered into **string or mathematic information**.
- The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data.
- Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved.
- It may be appreciated that choice of how much data to match, and to what degree of accuracy, governs the accuracy/speed ratio of the biometric device.
- **Possibility of false positives and negatives**.

Types of Two-Factor Authentication

Biometrics

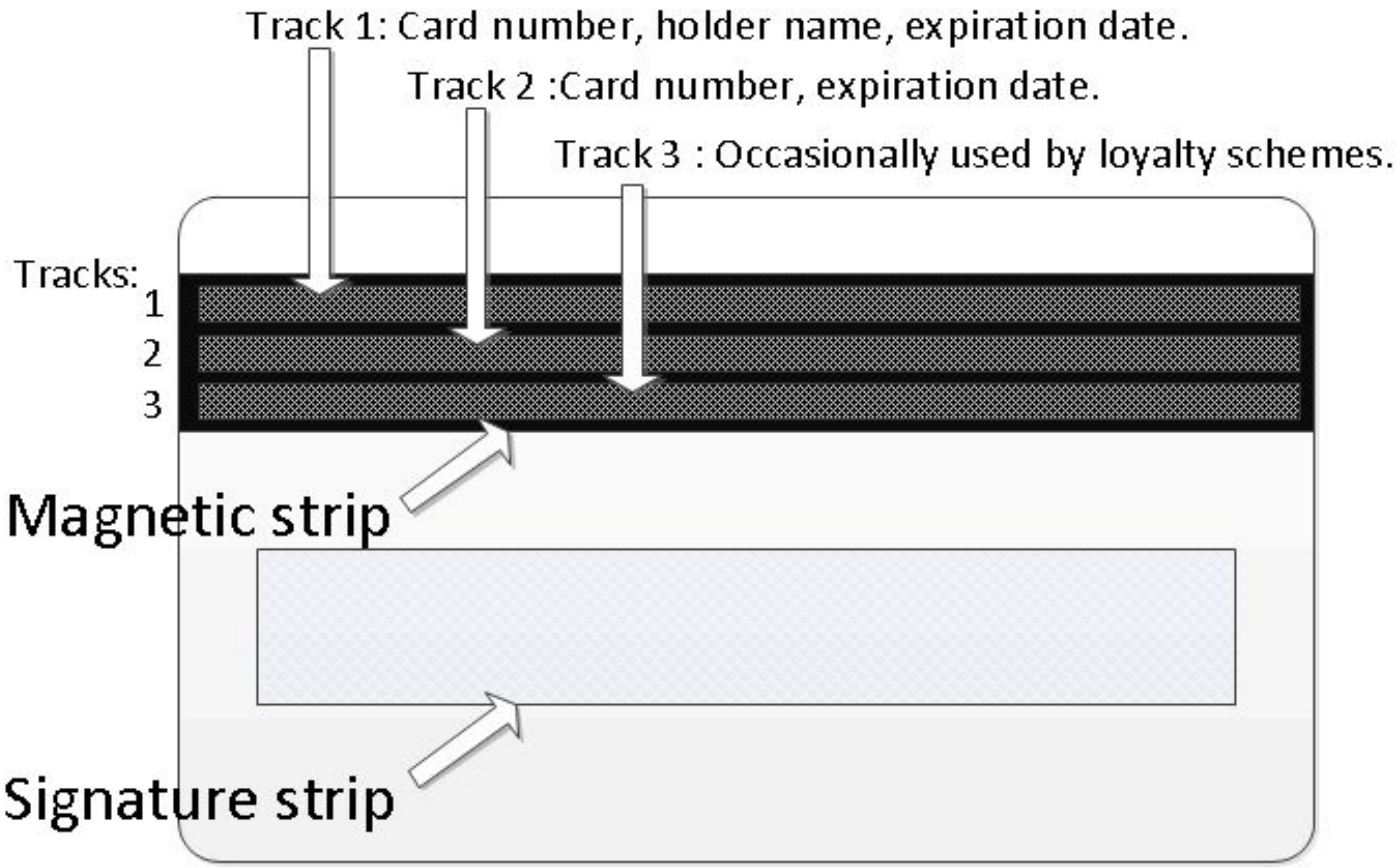
- Biometric information may be mechanically copied and they **cannot be easily changed**. This is perceived as a disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his/her password, however, a user cannot change their fingerprint.
- A bio-identifier **can also be faked**. For example, fingerprints can be captured on sticky tape and false gelatine copies made, or simple photos of eye retinas can be presented. More expensive biometrics sensors should be capable to distinguish between live original and dead replicas, but such devices are not practical for mass distribution

Types of Two-Factor Authentication

Magnetic Cards

- Magnetic cards (credit cards, debit cards, ATM cards, gift cards, etc) combined with secure, encrypting card readers provide a possible solution for two-factor/strong authentication.
- Each magnetic stripe card has **unique characteristics** much like the card's own fingerprint called a magnetic fingerprint.
- The advantage is that a magnetic fingerprint already exists on every magnetic stripe card because it is an **intrinsic characteristic** and no cards would need to be re-issued.
- Each swipe of the card provides a correlative number called a dynamic digital identifier that can be scored and "matched" to the originating value to determine the cards authenticity.

Magnetic Cards



Track 1: Card number, holder name, expiration date.
Track 2 :Card number, expiration date.
Track 3 : Occasionally used by loyalty schemes.
Tracks:
1
2
3
Magnetic strip
Signature strip

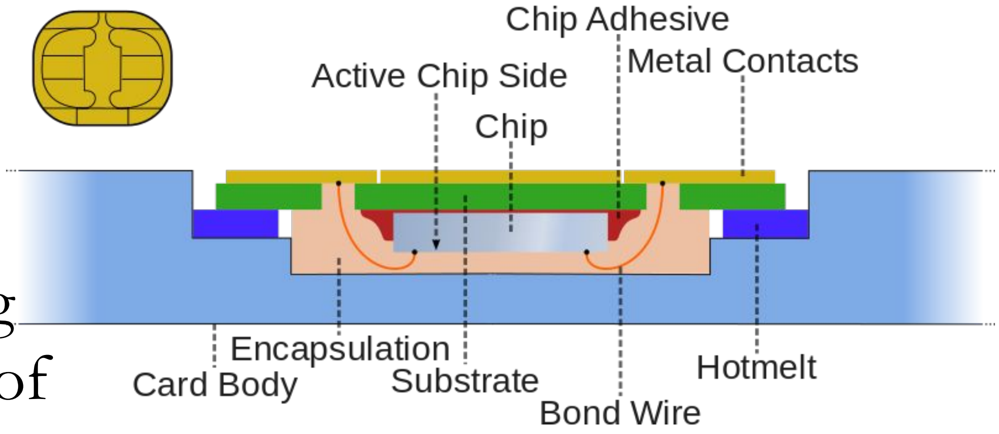
Smart Card

Either contact or contactless

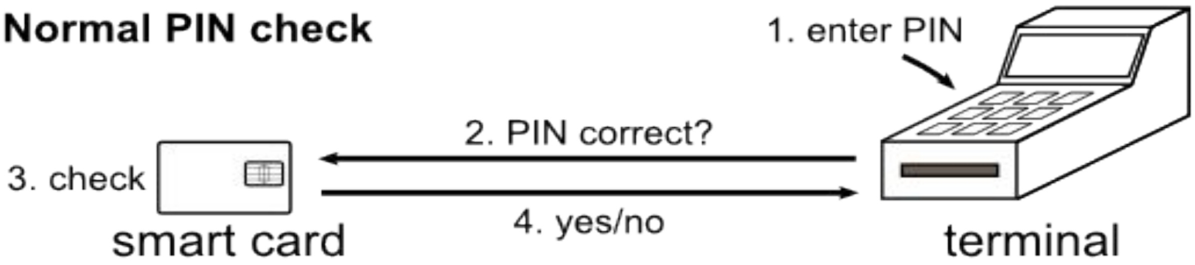
EMV (Europay MasterCard Visa) is the most commonly used standard

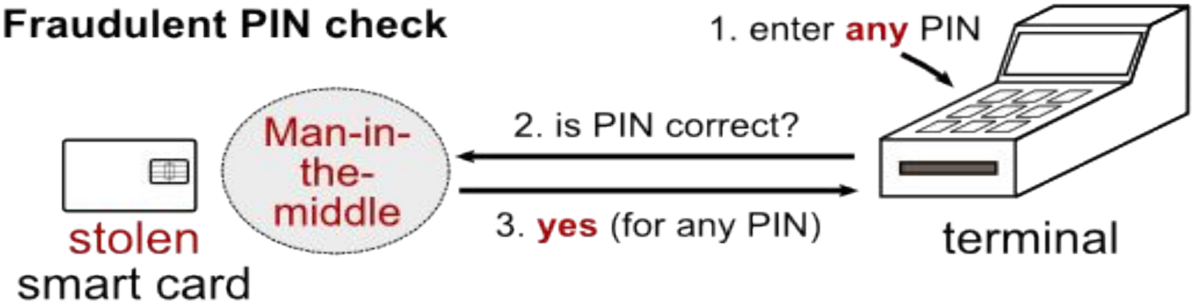
Smart cards can be physically disassembled to gain unrestricted access to the chip → risky, may permanently damage card

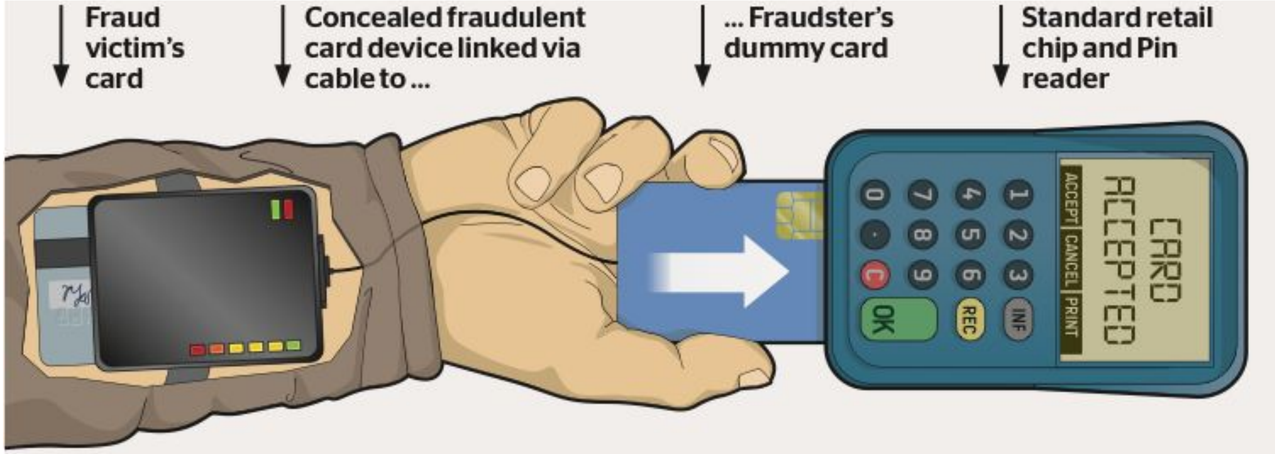
Side channel attacks are used more often →attack targeting the physical implementation of a system



Smart Card Fraud






Fraud victim's card

Concealed fraudulent card device linked via cable to ...

... Fraudster's dummy card

Standard retail chip and Pin reader

For more insight checkout: http://sec.soup.io/tag/Banking%20security

Trojans

"A Trojan horse, or Trojan, in computing is any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a victim to install it."

Trojan horses take many forms, and many of them are intended to steal passwords and other sensitive data. Treat any uninvited program with **suspicion**, from whatever apparent source.

If you're told you need to access a given resource for some convincing reason, **verify the link independently** to ensure that you're not accessing a fake site set up specifically to capture your account name and password.

Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves.

Principle of Least Privilege

"The principle of least privilege requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose."

This practice is just good common sense as it prevents a number of problems, some of the benefits of such a system:

- Better Stability – users cannot break systems they do not have access to
- Better Security – Malware is limited in it's propagation
- Easier to Deploy – applications designed with this in mind are easier to deploy and maintain

Why do you need a good password?

One of the most common forms of automated attack on a corporate system is **password guessing**, while attempting to steal passwords from targeted individuals by various forms of social is also used.

On many systems, most untrusted services are still **protected primarily by passwords** rather than by more glamorous methodologies such as smart cards, biometric systems, hand-held authentication and so on.

Insecure passwording, whether as a result of bad systems practice or bad user practice, may endanger data in breach of **data protection legislation**, contractual obligation, or corporate policy.

Good User Practise

It has been estimated by CERT-CC that "**80 percent of all network security problems (are) generated by bad passwords**."

We can't actually demonstrate the accuracy of that statistic, but it does at least indicate anecdotally how seriously the security community regards the issue of password security.

So here are some ideas that should make you less vulnerable to password-related problems as an end-user.

Don’t Share Passwords

Don’t share passwords unless there’s a formal protocol set up to allow it. More than one person sharing an account is (except under “very” controlled conditions) a major threat to security.

- The more people with access, the greater the risk.
- Attacks on computer systems can come from inside as well as outside. This should be of particular concern to an end-user who is not cautious about sharing account information.
- If an attack is traced to a particular account, the holder of that account will be the prime suspect. Accidental or deliberate extension of access to intruders.

Anti-Social Engineering

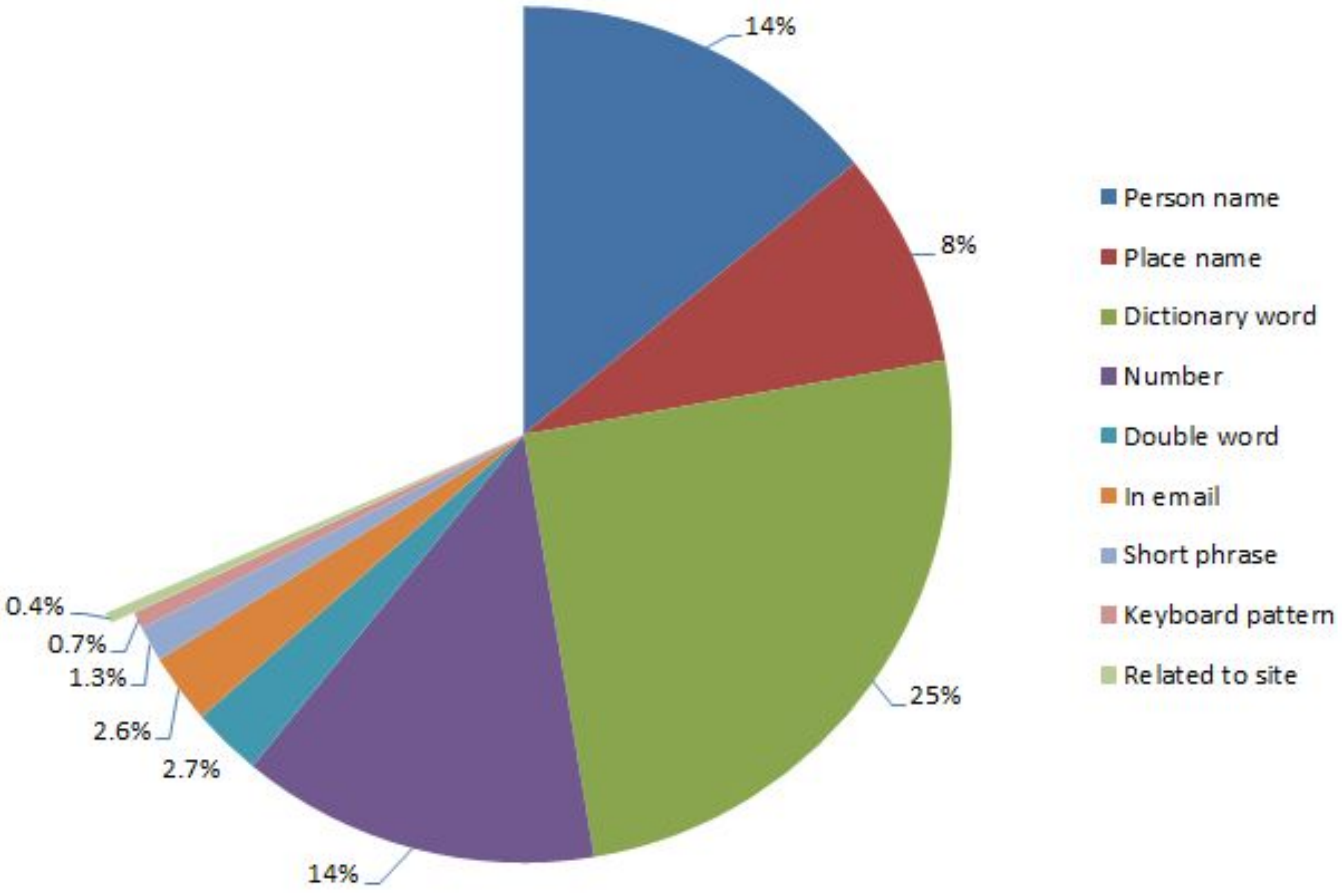
Be aware of the **social engineering** approach to cracking passwords.

The quickest route to appropriating a password (especially a shared one) can be via a phone call and a bluff.

Don’t disclose passwords to anyone whose identity you can’t verify, or whose right/need to know is in doubt.

A good rule of thumb is that anyone who contacts you in order to ask for your credentials should be treated with suspicion. However convincing their story is, verify that they are who they say they are.

Password Selection Practise



Password Selection Strategies

It's good practice to **avoid** the following common strategies when deciding on a password.

- Any **correctly spelled English** word, especially one which is likely to be recognized by operating system or application spell-checkers and so on
- Any correctly spelled non-English word
- Any part of your own **name or username**
- Any part of the name of a member of your extended family (including pets) or, worse, a colleague, your boss, or, in fact, **anyone's name**
- Place names are often easily guessed
- The **name** of the OS you're using, or the name of the PC you're using or the hostname of a server you're accessing

Password Selection Strategies

- Personally significant numbers (phone number, car license number, PPS, someone's birth date)
- Your favorite or most-hated objects, food, movies, TV programs
- Song, book and movie titles, famous people, cartoon characters
- Anything so unmemorable you have to write it down
- Reusing passwords

Password Selection Strategies

Techniques that may help in slowing down password breaking by guessing or simple dictionary attacks include the following.

- The **more combinations** of techniques you use in a single password, the more effective they're likely to be
- Embed control characters or **non-alphanumeric symbols**
- Unorthodox caPitaliZation
- Use a personally significant **acronym**, e.g., ICRMFPW (I Can't Remember My Friendly Password)
- USE A **PASSPHRASE**

Password Selection Strategies

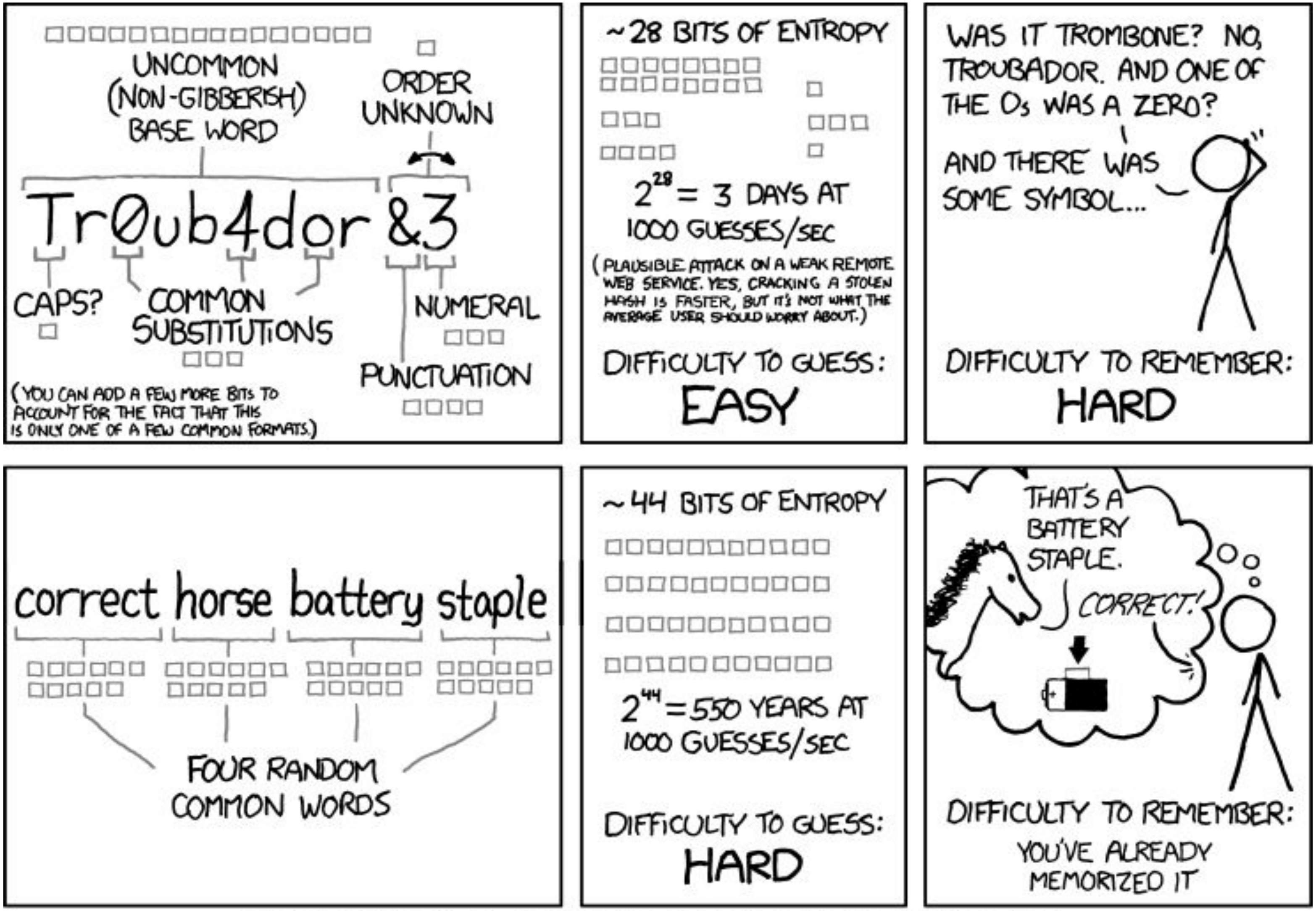
Changing your password regularly is important.

- How frequently you change your password will depend upon how important the information you are protecting is
- Generally**, once every three months** is a really good idea. That way, by the time a computer has cracked a good strong password, you will have already changed it!

One of the problems with multiple passwords is remembering them all.

- Tools are available to do this
- Just remember that you need to keep your "**keysafe**" application on a very safe computer, and back up the password file.

Password Selection Strategies


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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.