After all these hacks, tech firms could do more – but better security starts with you

September 24 2014, by Barry Avery

A belt and braces approach is wise. Credit: Modern Relics, CC BY

After various celebrities' accounts on Apple's iCloud servers were hacked, the company has made a point of addressing these issues. It has made new claims for the security of iOS 8, the firm's latest phone operating system, and for its cloud services. Similarly, Google announced the next version of its Android phone operating system will encrypt all data by default. But what sort of security do these measures provide?

Security in the hand

All phones and tablets provide a device lock that requires a passcode or swipe gesture to unlock. But many owners – up to 50% – either don't use the feature, or use a trivial passcode such as 1234. Fingerprint readers, as introduced in the iPhone 5, are perhaps the way forward and through ease of use are likely to increase the number of users locking their phones.

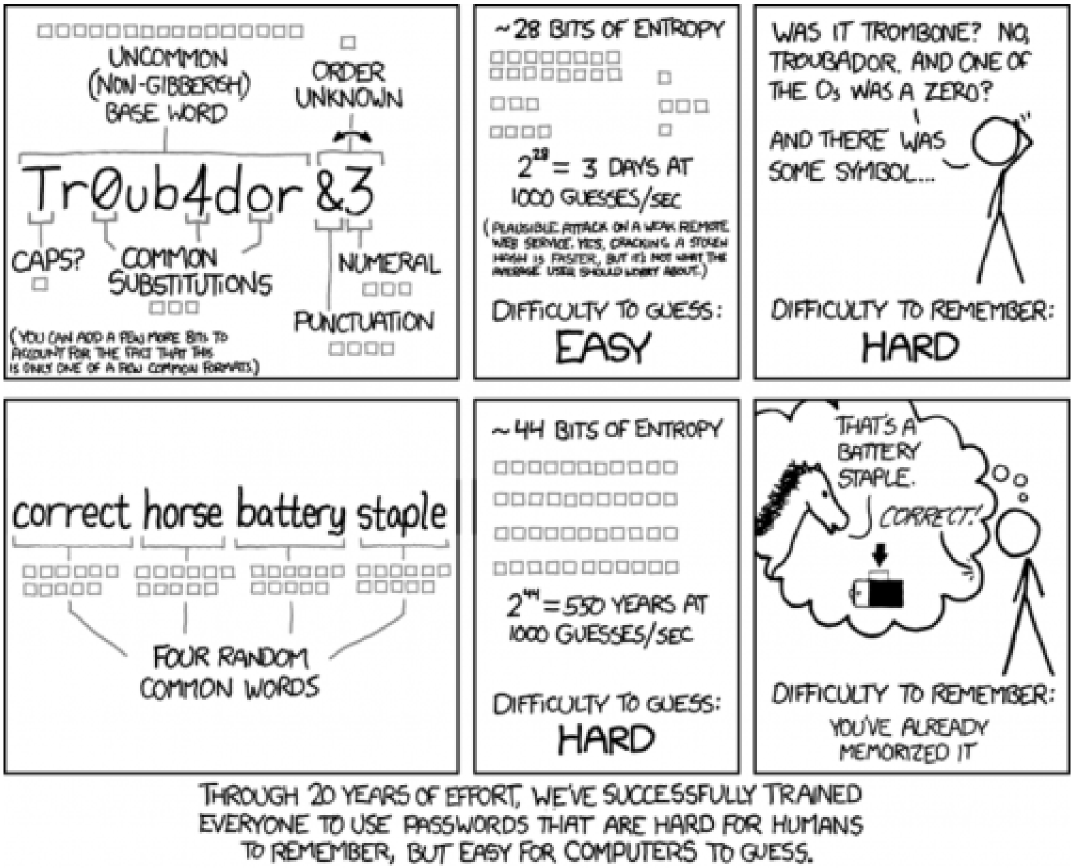
While a device lock provides some protection, it's still possible that a hacker, or the authorities, could extract data given physical access to the device. Encryption, as offered by both Apple's iOS and Google's Android platforms, would defeat this (or make it extremely difficult) by requiring a passcode to decrypt the contents and make them readable.

Android has offered this since 2011, while for Apple it was introduced with iOS 7 in September 2013 for mail and data in third-party apps. With iOS 8, this is extended to the phone's messages, mail, calendar, contacts and photos. Additionally Apple claims that it no longer stores a copy of the encryption key used, making it unable to respond to a warrant demanding access to the data, whether backed up in the cloud or on the device.

In the UK, police will seize mobile phones after a car crash in order to see if drivers were texting and driving. This follows a pilot scheme in which police stations equipped with specialist readers are able to swiftly extract the entire contents of a phone. Whether this will be defeated by the encryption introduced by iOS and Android remains to be seen. Certainly the UK Regulation of Investigatory Powers Act 2000 (RIPA) empowers the authorities to compel a user to supply decryption keys or passcodes.

Apple's new payment system built around its near field communication (NFC) chip and protocol does not store or transmit credit card details. This makes it fairly secure, and should massively reduce the number of skimming techniques that are possible with other card payments, as neither the card number nor the pin code will be accessible during the payment process, stored as they are in a secure hardware chip in the phone.

Security in the cloud


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.

Credit: xkcd, CC BY-NC-ND

Most smartphones now back-up data to the cloud and it was through this that hackers gained access to the images that were then leaked. There's no evidence that Apple's servers were hacked and compromised – unfortunately this privacy breach was made possible by poorly chosen passwords and a weak security questions system that allowed repeat guesses without raising the alarm.

There are files containing millions of popular passwords available on the internet and it's likely hackers simply ran programs that tried various combinations until they succeeded – a "brute force" attack – together with answers to security questions guessed based on publicly known information. Apple has now firmed up its security procedure by introducing a maximum number of incorrect answers to security questions and notifying users when their online accounts are accessed.

Security starts with you

So make sure the weak link in the security isn't you. Choose a strong password – it isn't hard. Don't use an obvious passcode, and use a fingerprint scanner if fitted. Use Apple Find My Phone or Android's Device Manager so a lost or stolen phone can be locked, traced or even remotely wiped.

For iPhones, upgrade to iOS 8 or at the very least upgrade to iOS 5 or higher. For Android, look into encrypting the device's contents and when installing a new app be aware of what it is asking access to – don't blindly click on messages that say "Let this app have access to…" as malicious apps could wrestle data from your phone and send it out over the internet. Some companies have a terrible reputation when it comes to privacy (for example Facebook), so be cautious of default settings.

Use the best tools available

Currently the best way to secure online accounts is (together with a strong password) to turn on two-factor authentication – as offered by Apple, Google, Facebook and Twitter.

You register a phone number, which the service will call or text with a pin number. This will be required in addition to your password to gain access. This is set up per device, for example once for your phone and once for your laptop. Trusted devices will work as they did, but someone else (or you) attempting to access your account from another device will need not only your password, but access to your phone to get the pin number the service sends.

Google goes further, allowing you to generate new, random passwords for each of its online services you use or each device, so that if someone compromises one password it won't open any others.

While it's a bit more of a hassle, try to have different passwords for different accounts as re-using passwords is as bad as having weak passwords. Use the tools available – web browers save passwords and there are software tools such as password managers that can simplify the task – but make sure you know how they work.

And even at the end of their lives, computers, phones and other devices need to be securely wiped to remove all traces of personal data (including the passwords and financial details we've been so keen to protect) before being given away or sold. Not doing so is little different than handing your keys to a burglar.

Blaming the companies for security failures is too easy – consumers have to get wiser about locking their data away.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: After all these hacks, tech firms could do more – but better security starts with you (2014, September 24) retrieved 10 April 2024 from https://phys.org/news/2014-09-hacks-tech-firms.html