Cloud storage and data security

Contents

Introduction

In the era of cloud computing maintaining the security of your data is paramount, with the recent iCloud breach providing a stark example of what can happen if passwords or account security is breached. This report provides a brief introduction to the concept of cloud storage before going on to review key elements of account security, including password strength, brute-force attacks and two-factor authentication. For those seeking further details of data encryption and common cryptographic techniques, we will soon be releasing a series of Cryptographic Primers.

What is cloud storage?

There is a consistent move towards cloud storage with a number of well-known service providers, including iCloud, Google Drive, Dropbox and OneDrive, all of which perform a broadly similar function; a user leases storage space from the provider and then sends copies of their files via the internet to the appropriate data server, which records the information (Figure 1). When the user subsequently wishes to retrieve or modify their information, they use a web-based interface to either retrieve the files from the server or to access and manipulate files on the server itself. The data is stored in 'logical pools' across multiple servers, which provides a greater degree of storage space and also creates redundancy, ensuring continued access for the user in the event of a localised disruption (1).

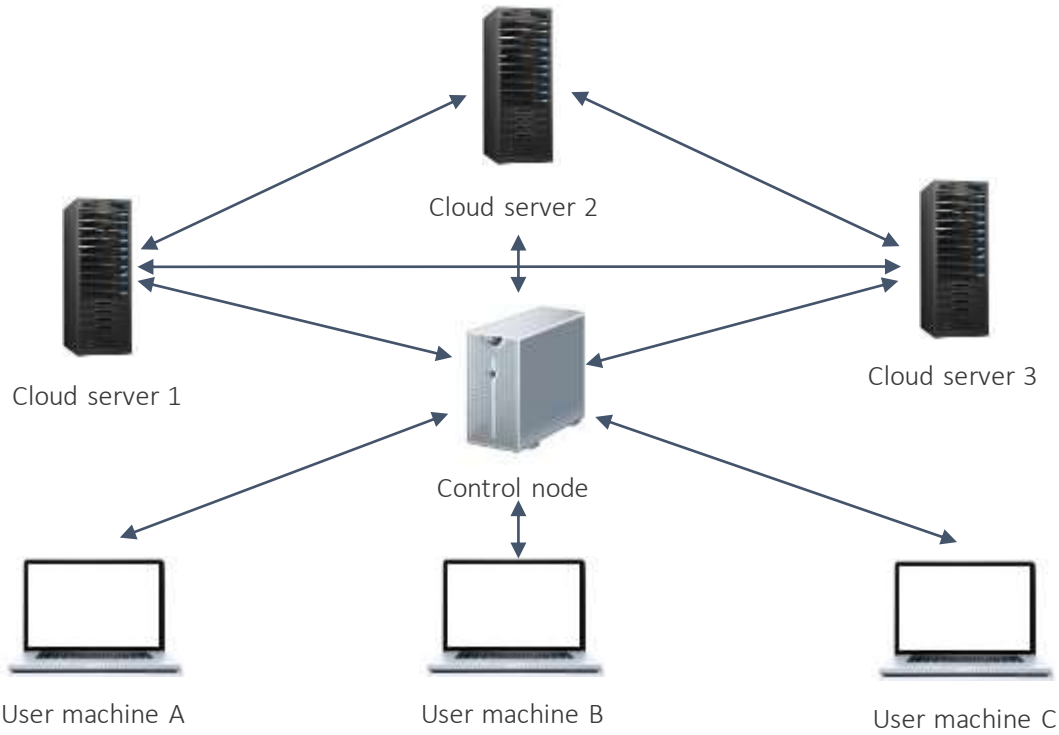

Figure 1: a schematic representation of cloud data storage

Benefits and risks

As with all new forms of data storage there are a number of advantages and disadvantages to cloud computing, the most prominent of which are:

Benefits	Risks
Improved efficiency: both in terms of remote access and more flexible working arrangements; users are able to access data from anywhere with internet access without the need to move physical machinery. There is also often a substantial cost saving following the initial investment, with users avoiding having to purchase multiple licence fees (2).	**Dependency:** also known as "vendor-lock-in", refers to the difficulties in moving from one cloud vendor to another due to the huge data migration involved. There are similar concerns over control, since services run on a remote virtual environment, the user has limited control over the associated hardware and software (3).
Greater collaboration: cloud storage systems allow users to grant other people access to their data, meaning efforts and input can be pooled in a central document and edited in real time to facilitate collaboration and further improve efficiency (1).	**Another avenue for attack:** as mentioned, as a cloud user you are relinquishing a degree of control over your data, which is no longer stored solely on a physical machine in your possession. If there is a compromise on the server(s) on which your data is stored then it may be possible for your information to be extracted by an unauthorised user (4; 5).
Back-up and recovery: since all data is stored online, backing-up and restoration is much easier compared with physical storage. Moreover, most cloud service providers possess the skills and capacity to handle information recovery, if it is required (6).	**Unintended permanence:** certain victims of the recent iCloud 'hack' have claimed that some of the images were thought to have been deleted (7). Cloud service providers are trying to avoid losing customer data and encourage users to make use of back-up facilities. As a result, redundant copies of files may be retained on the server(s), even if the user believes that these files have been deleted. There are ways to permanently delete information from cloud accounts; however, these techniques are often not widely known and the user still has to trust that the vendor has complied with the request.

Fortunately, hybrid solutions do exist which allow users to offset some of the disadvantages mentioned above. For example, those prioritising security may which to consider vendors who offer 'zero-knowledge privacy' as part of their cloud service. Under this system, user files are encrypted before they are sent to the company server(s). As such, the data is only readable by the user, as the key is stored locally on the individual machine, meaning employees at the cloud service provider, and by extension outside observers, cannot access the information. This increased focus on security may come at the expense of integration with wider productivity suites, which can restrict user access to Office-style apps or online collaboration tools (8). The viability of this trade-off depends on the needs of the individual user or the organisation, and a decision must be taken to determine the respective significance of security versus convenience.

Maintaining data security in the cloud

Irrespective of the specific cloud service chosen, there are a number of important security considerations that users should remain mindful of to reduce the probability of unauthorised individuals gaining access to their data.

Secure passwords and sensitive information

First and foremost users should ensure that the passwords protecting their cloud accounts are suitably secure; avoid obvious choices, such as 123456, which continue to top the lists in annual reviews of the worst password options (9). Thankfully, most cloud service providers force users to conform to certain password rules, such as 'one lowercase and one uppercase character, one number and a least 8 characters' (10); however, in several instances this still allows the user to select from numerous common variants, e.g. Pa55word. To be more secure, consider using a random nonsense phrase made up of common words and/or numbers, which is easy to remember but extremely difficult for a machine to crack (11) (Figure 2).

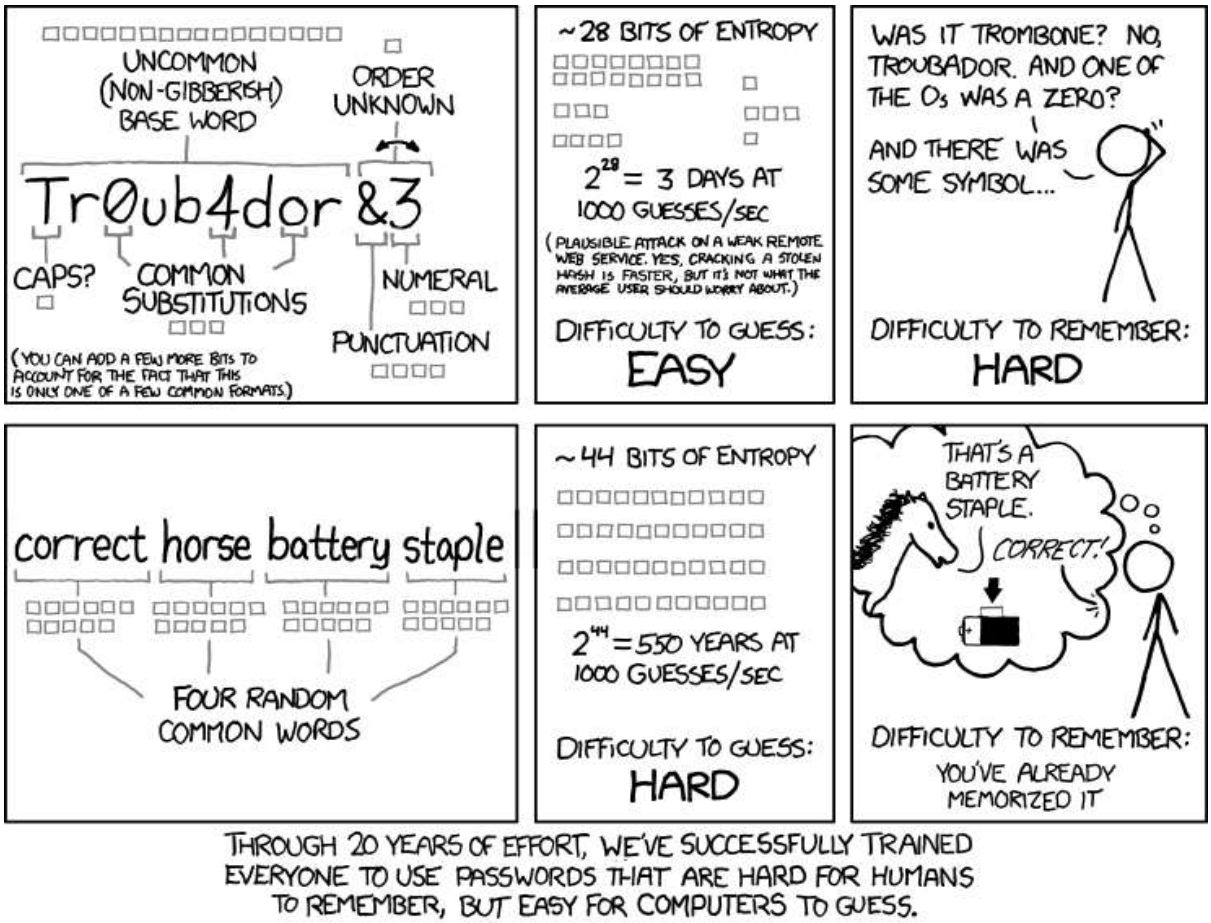

Figure 2: A cartoon illustrating the respective strength of different password formats (12).

It's also important to remember that malicious individuals may not need the account password in order to access content. In the case of iCloud, accessing someone's account "requires only three things: their email address, their date of birth, and the answers to two out of three security questions. This is assuming they don't have two-step verification enabled" (13). If an attacker possesses this information then they can reset an Apple ID password to one that only they know and gain access to user iTunes and iCloud accounts, including recent photos and back-ups, provided these features have been activated (13).

Apple are not the only company to be affected by this issue, Sarah Palin's Yahoo! account was once breached when a college student obtained her date of birth from a Wikipedia page, whilst Paris Hilton's T-Mobile account was compromised when attackers correctly entered the name of her dog in response to a security question (14). As such, it is important to ensure obvious information – or information that can be easily sourced from social media – is avoided in 'secret answers' linked to account reset features and that associated email addresses are not distributed widely via public forums. Indeed, hackers show

remarkable ingenuity in the use of any such data, pooling resources and information to accurately guess answers to security questions. For example, in the case of the common query "where did your parents meet?", attackers have been observed sharing tips on how to use the target's name to identify the social media accounts of their parents and then matching information on the cities these individuals have resided in, to correctly deduce the appropriate answer (Figure 3) (15).

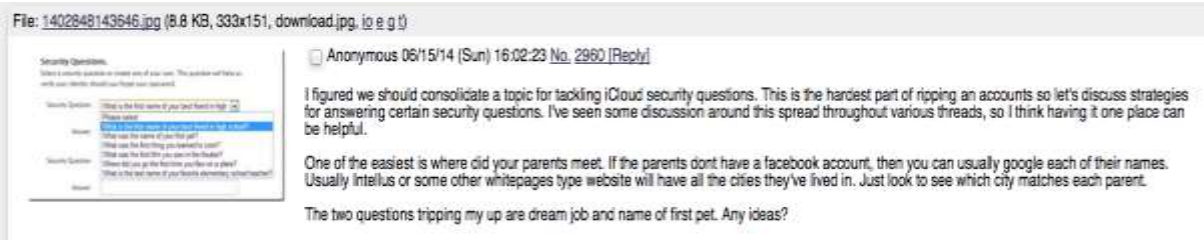

Figure 3: An excerpt from an online discussion between attackers sharing tips to help correctly identify the answer to a user's 'secret questions' (15).

Understandably, the number of passwords and sensitive pieces of information users need to remember can prove difficult and there are obvious security concerns around writing information down or storing details in an unencrypted format on a local machine. As such, users should consider using a password manager; a software application which stores and organises passwords in an encrypted format. The user need only remember one, ideally very strong, master password, which grants access to the entire password database. Some password managers store data on the user's computer, whereas other's make use of cloud storage; notable examples include Robo Form and Last Pass. Many service providers also offer additional features, such as fields to store further login information, as well as tools to generate random passwords of suitable strength (16).

There is an obvious risk associated with the use of password managers, in that an attacker only needs to obtain your master password in order to gain access to, and take over, all of your accounts (17). However, several easy steps can be taken to reduce the probability of this problem occurring, including using a password of sufficient strength, never writing down or otherwise distributing details of your master password, and changing the password regularly, to limit the window of opportunity for any attacker who does gain access.

Password cracking and brute-force attacks

Of particular interest during the recent iCloud 'hack' was a security exploit termed 'ibrute', which was published on Github at the end of August; Apple have since refuted suggestions that this technique was used to access account information (18). Allegedly, the exploit allowed attackers to conduct a brute force attack; this does not involve any attempt to decrypt information but rather focusses on trying a large combination of different passwords, words or letters to gain access to an account (19).

ibrute operated by exploiting a vulnerability in the Find My iPhone software, which allowed attackers to run a python script to conduct an infinite number of password entry attempts, using various combinations of login details, without the account becoming locked (20); Apple have since reported that the bug has been fixed (21). Importantly, the potential success of the exploit relied on account owners possessing weak login credentials, with ibrute selecting from a list of just 500 common passwords (22). Once again this emphasises the importance of having strong passwords in place and suggests that vendors and system owners should impose a limit on the number of password attempts that a user can make within a specific time-frame, to reduce the risk of a successful brute-force attack.

Two-factor authentication (2FA)

Another means of improving account security is to implement or enable additional features, particularly two-factor authentication (2FA), which makes it significantly harder for potential intruders to gain access and steal a person's personal data. Using this system, account access requires a password and username, plus a specific piece of information that only the user will know or have access to (23); the latter could be a physical token or digital code sent directly to the user's phone as an SMS. This additional security feature can be enabled for all of the main cloud service providers (22) and is used by CERT-UK to authenticate users on the Cyber-security Information Sharing Partnership (CiSP, Figure 4). In 2FA systems, the secondary token can be long-term or single use, however the latter is more secure, creating a very limited window during which an attacker could intercept and use the token.

In the case of the recent iCloud 'hack', 2FA was not enabled by default, which has been suggested as a potential contributory factor; this was referenced in Apple's subsequent statement in which users were advised to "always use a strong password and enable two-step verification" to protect against these types of attack (24). None of the other main cloud service providers currently enable 2FA by default, although there are a number of articles which provide instructions on how users can activate these services (22). Whilst 2FA doesn't offer protection if your photos or data have already been breached, it does provide an additional layer of security for data currently stored in the cloud and will help to reduce the probability of unauthorised users accessing your account in future.

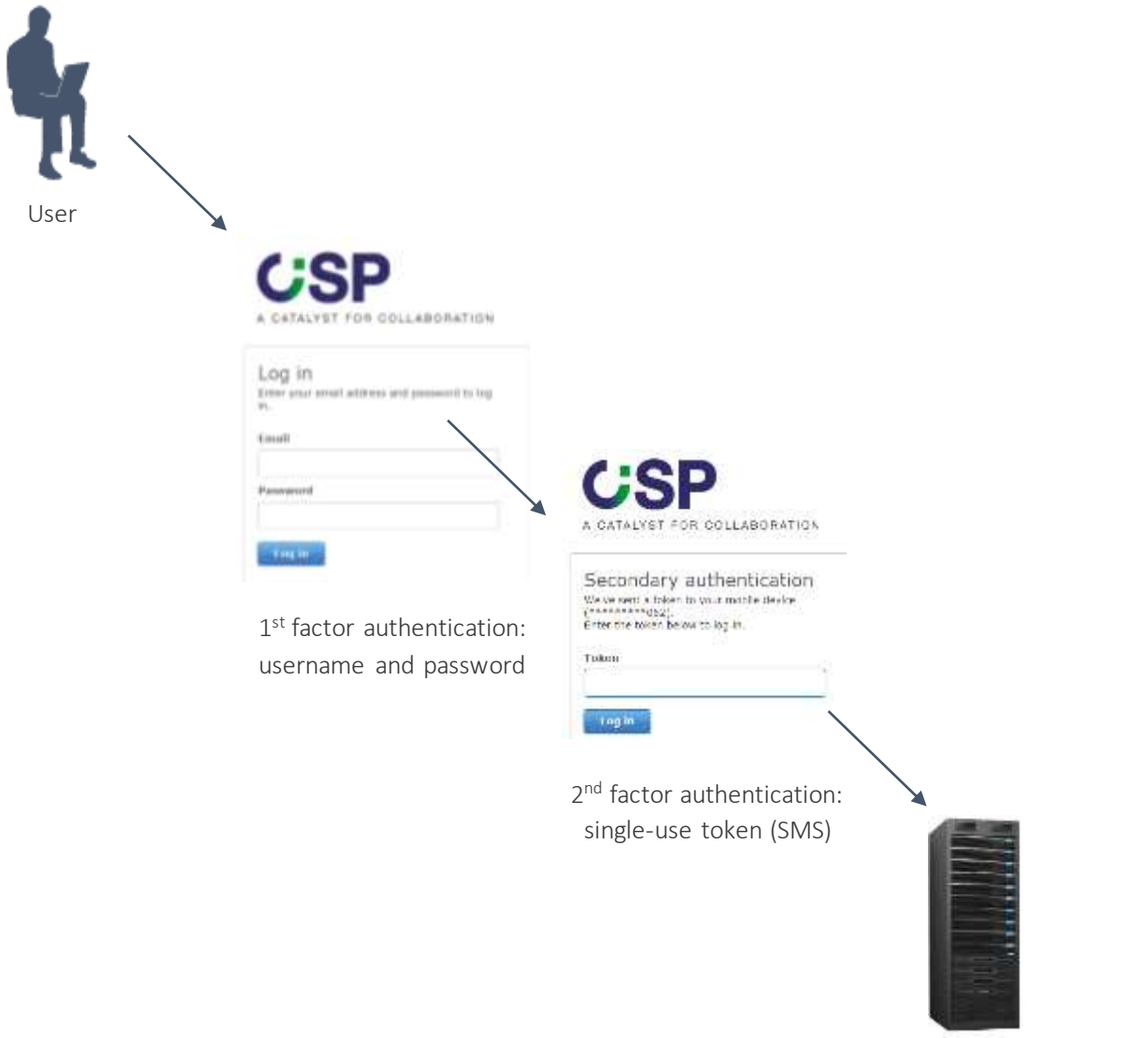

Figure 4: a schematic overview of two-factor authentication.

Conclusion

There will never be a means of completely securing information stored either locally or on the cloud. Malicious attackers will always seek to gain access to sensitive information, with efforts and resources increasing in line with the profile of the company, individual or information targeted. Unfortunately,, there is an ever increasing number of routes for 'hackers' to gain unauthorised access, with cloud computing presenting its own particular blend of risks; meanwhile criminals continue to pool resources and efforts to devise new methods to circumvent existing security features. In the case of the recent iCloud 'hack', the exact route of entry is unclear; however, the best way to mitigate against similar attacks in future is to ensure that all possible security systems are enabled and to remain abreast of current techniques in order to identify new attack vectors.

Bibliography

1. Strickland, J. How Cloud Storage Works. [Online] http://computer.howstuffworks.com/cloud-computing/cloud-storage1.htm.

2. Cloud Computing Insights. Cloud Computing Advantages and Disadvantages. [Online] http://www.cloudcomputinginsights.com/management/cloud-computing-advantages-and-disadvantages/?mode=featured.

3. Pal, K. Introduction to the Practical Advantages and Disadvantages of Cloud Computing. [Online] July 2014. http://www.devx.com/dbzone/introduction-to-the-practical-advantages-and-disadvantages-of-cloud-computing.html.

4. Jefford, C. Why Apple's Tim Cook shouldn't apologise for the celebrity iCloud hack. [Online] September 2014. http://www.marketingmagazine.co.uk/article/1311052/why-apples-tim-cook-shouldnt-apologise-celebrity-icloud-hack.

5. Morris, K. Five advantages and disadvantages of cloud computing. [Online] September 2011. http://www.examiner.com/article/five-advantages-and-disadvantages-of-cloud-computing.

6. Viswanathan, P. Cloud Computing – Is it Really All That Beneficial? [Online] http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm.

7. Hall, S. Countless celebrity nude photo leaks being blamed on supposed iCloud hack (updated). [Online] August 2014. http://9to5mac.com/2014/08/31/countless-celebrity-nude-photo-leaks-being-blamed-on-supposed-icloud-hack/.

8. Casserly, M. 7 best cloud storage services - 2014's best online storage sites revealed. [Online] March 2014. http://www.pcadvisor.co.uk/features/internet/3506734/best-cloud-storage-services-review/.

9. SplashData. "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list. [Online] http://splashdata.com/press/worstpasswords2013.htm.

10. Apple. Security and your Apple ID. [Online] http://support.apple.com/kb/ht4232.

11. Vaughn-Nichols, S. J. Cartoon makes better password point than many security experts. [Online] April 2011. http://www.zdnet.com/blog/networking/cartoon-makes-better-password-point-than-many-security-experts/1340.

12. Munroe, R. Password Strength. [Online] http://xkcd.com/936/.

13. Evershed, N and Farrell, P. How easy is it to crack into an Apple iCloud account? We tried to find out. [Online] September 2014. http://www.theguardian.com/world/blog/2014/sep/03/after-nude-celebrity-photos-i-tried-to-hack-my-colleagues-apple-icloud-account.

14. Robertson, J. Apple Celebrity Nude-Photo Hack Shows Risk in Security Questions. [Online] September 2014. http://www.bloomberg.com/news/2014-09-03/apple-celebrity-nude-photo-hack-shows-risk-in-security-questions.html.

15. Cook, J. Inside The iCloud-Hacking Ring That Leaked Those Naked Celebrity Photos. [Online] September 2014. http://www.businessinsider.com/the-underground-icloud-hacking-ring-that-leaked-naked-celebrity-photos-2014-9.

16. Parker, J. Take control of password chaos with these six password managers. [Online] April 2014. http://www.cnet.com/news/best-password-managers/.

17. Crawford, S. How Password Management Software Works. [Online] http://computer.howstuffworks.com/password-management-software3.htm.

18. Spickernell, S. Apple share price soars after refuting iBrute celebrity photo hack, then plummets in biggest fall since January. [Online] September 2014. http://www.cityam.com/1409690218/apple-share-price-soars-news-no-security-breach-celebrity-photo-scandal.

19. Computer Hope. Brute-force attack. [Online] http://www.computerhope.com/jargon/b/brutforc.htm.

20. Williams, O. This could be the iCloud flaw that led to celebrity photos being leaked (Update: Apple is investigating). [Online] September 2014. http://thenextweb.com/apple/2014/09/01/this-could-be-the-apple-icloud-flaw-that-led-to-celebrity-photos-being-leaked/.

21. McCoy, K. Report: Apple fixes bug exposing nude celeb photos. [Online] September 2014. http://www.usatoday.com/story/tech/personal/2014/09/01/apple-plugs-iphone-bug/14925033/.

22. Vaughan-Nichols, S. After alleged iCloud breach, here's how to secure your personal cloud. [Online] September 2014. http://www.zdnet.com/after-alleged-icloud-breach-heres-how-to-secure-your-personal-cloud-7000033177/.

23. SecurEnvoy. What is 2FA? [Online] https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm.

24. Nichols, S. Hot Celebrity? Stash of SELFIES where you're wearing sweet FA? Get 2FA. Now. [Online] September 2014. http://www.theregister.co.uk/2014/09/02/apple_says_icloud_not_compromised_in_celeb_hacks.

www.cert.gov.uk

@CERT_UK

A CERT-UK PUBLICATION