MyFitnessPal Breach

Dabir Hasan Rizvi

1. Introduction

MyFitnessPal is an application about fitness and nutrition that enables the user to track the calories and nutrition in their diet and this app is owned by Under Armour (Newman, 2018b). In 2018, the company suffered a data breach in late February where the hackers were able to gather data from approximately 150 million users including their usernames, email addresses and passwords. In 2019, it was discovered that these accounts were up for sale on the dark web for bitcoin equivalent of $1040-$20,000 (Newcomb, 2019;Williams, 2019). Under Armour was able to discover the intrusion on March 25 2018 and made a public statement on the incident within a week as shown in figure 1, which was commendable as other companies such as Uber took over a year to publicly disclose their data theft woes. (Newman, 2018b). This caused the shares of Under Armour to drop by 4.6%. However, despite having revealed usernames, email addresses and passwords, the company was able to protect a few key information such as bank/credit card details, location and other personal information of the user (wLife, 2019). The application does not collect confidential information of the user such as driving licence number, passport details, national insurance number or social security number, hence that information was not revealed ("MyFitnessPal Account Security Issue",n.d. 2019).

Fig 1. Timeline of the attack (Anna, 2020)

2. Technical description of the attack

Security breaches are a major issue threatening to put companies in jeopardy and can cause large financial ramifications (Hall & Wright, 2018). In the case of Under Armour, the main reason that the breach was partly successful was because they had secured some passwords with an SHA-1 hashing algorithm rather than a more secure Bcrypt algorithm (McGee, 2019). Hashing a password is a procedure that is done by using an encryption algorithm to mask the correct password by converting the password to incomprehensible strings. This cryptographic process will cost the hackers valuable time and resources to crack the hashed password.

The attackers were also able to access the internal database. There were no explicit details available on this as Under Armour is a public company. However, it is known that the hackers were able to steal caches of email addresses, usernames and hashed passwords through phishing. They then used a technique whereby they use brute-force to extract the correct

password from the hashed password. However, this technique was largely unsuccessful due to the Bcrypt algorithm, which has been proven to be highly secure. We can see the attack vector in Figure 2.

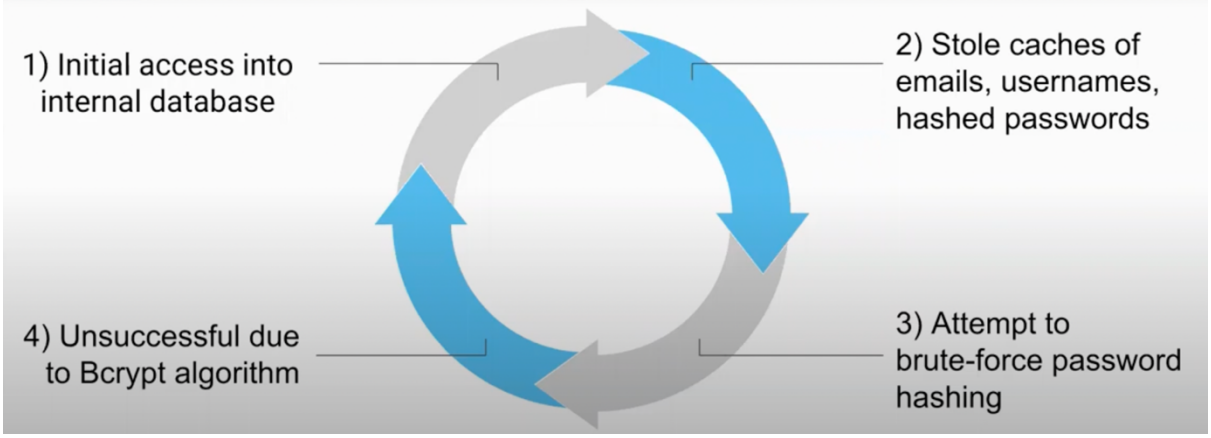

Fig 2. Attack Vector (Anna, 2020)

Under Armour has secured most of the user's passwords by hashing them using the Bcrypt algorithm and the rest using an SHA-1 hashing algorithm. Bcrypt algorithm uses salting, which is used to generate random data that produces a more unique hash. One of the major advantages is that it increases the complexity of the password without increasing the requirements from the user. Overall, it helps to mitigate password attacks and is resistant to brute-force methods commonly used by hackers (Anna, 2020). In addition to this perk, it is also able to prevent a different password-cracking method called the "rainbow table attack". In this method, hackers use a predefined table known as a "rainbow table" to crack the password hashes in a database. In addition, the Bcrypt algorithm also uses blowfish - a symmetric key block cipher. This system is highly effective due to having run through its hashing function repeatedly, which builds up its defence structure in layers and therefore makes the process much more challenging to reverse (Newman, 2018a). In terms of speed, Bcrypt hashing is relatively slow but it is truly adaptable. It has a work factor feature which allows it to determine how expensive or slow the hashing algorithm is. The iteration counter cost increases as the hashing function gets slower which makes it resistant to brute-force attack (Alex, 2020)

Fig 3. Example of a hashing password using Bcrypt algorithm (Alex, 2020)

On the other hand, the SHA-1 algorithm is older and weaker than the Bcrypt algorithm. Its use was deprecated in 2011 as it is not considered secure enough by the data security community. The SHA-1 algorithm is easier to breach using brute-force. SHA-1 is a cryptographic hash function that takes an input and produces a 160-bit hash value known as a message digest and

it is rendered as a hexadecimal value which is 40 digits long. It is more susceptible to collision attacks as seen in figure 4 (Alex, 2020)

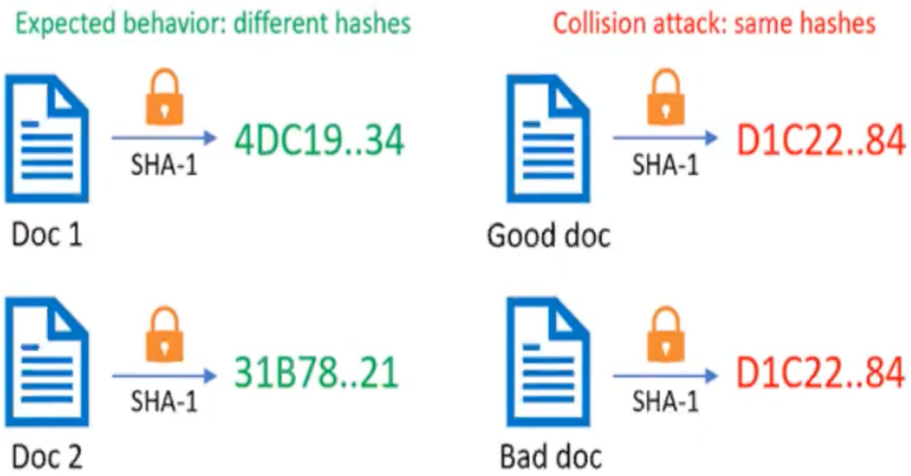

Fig 4. SHA-1 algorithm during collision attack (Alex, 2020)

However, it is still possible for Bcrypt to be cracked. Easy passwords such as "qwerty123" are vulnerable and are easier to guess. Hashing passwords using the stronger algorithm provides more time for the company to act on it. Under Armour has not published much more information regarding this but a statement by Matthew Green speculates that the breach occurred due to a transition between two hashing schemes. It suggests that it happened while they were upgrading their hashing password algorithms from SHA-1 to Bcrypt algorithm but had to store the old data for customers that were not active.

3. Recovery

After a security breach, companies need to have a clearly defined plan of action. During the recovery stage, the company needs to return to a better state and restore stability as soon as it is attainable and their goal is always to regain the faith of the public and consumers (Fearn-Banks, 2009). Under Armour discovered the breach on March 25, 2018 and notified the public within the next few days. Unfortunately, they are still partly in the recovery phase and the case is still in arbitration (Graham B, 2019). Under Armour have been able to recover most of their lost data but some data may still be at large and securing it may be difficult. Under Armour have responded to the security breach in the following way to minimize the harm to the network and to make sure it does not happen again (Torres et al, 2021).

Stop the attack:
First, the breach must be identified. The quicker the breach is identified the better it is for the organisation. Then, the breach must be contained by denying access to the hacker by isolating the system that was exploited or removing the access of the user who is being exploited. After containing the threat, it must be eliminated. If the identification, containment, and elimination of a breach are completed before the hacker breaks out of the network they initially exploited, the damage can be minimised. Under Armour were excellent in this regard as they were able to detect the breach within a month of its exploitation and were able to contain and eliminate the breach by allowing all the users to change their passwords. This was useful as all the data that was leaked were usernames, email addresses and hashed passwords. Some users use the same password across multiple websites and this step enabled the users to be protected from attackers to access their other accounts (Eric, 2020).

Investigating the Attack Method:
Knowledge of the attack is important for the prevention of future attacks so that it does not repeat. The affected networks should be investigated to check if the hacker had left any malware for signs of future compromise. All the logs of the activities that took place during the attack should be stored to be used for forensic analysis which can help identify the source and avoid any other attacks from that source. During the investigation, Under Armour did realise that the hashed passwords which used SHA-1 were targeted as it is fairly easier to brute-force and they are trying to hash the majority of their passwords using the Bcrypt algorithm at present as it is more secure and harder to brute-force (Eric, 2020).

Notifying the affected user:
During investigation, we should be able to identify which systems were affected and which data was stolen and when that is done. Then all users should be notified that they have been compromised and their information is under attack. Under Armour was efficient at this as they were able to notify the users within a week from discovering the attack which saved their reputation and maintained trust in the company. Other companies such as Equifax and Uber took a long time to identify their customers of their stolen data which made them lose trust due to their lack of transparency (Eric, 2020).

Restoring assets on the network:
Restoring of the assets individually affected during the attack can be done in many ways. The data storage drives of the affected networks can either be wiped or replaced or all the lost assets from a backup can be downloaded. Cloud-based replicas of the network environment can also be enabled, which can instantly restore the network. Under Armour were able to identify the problems and rapidly restore every compromised account while also working simultaneously to make them more secure by using Bcrypt hashing algorithm instead of SHA-1 algorithm (Eric, 2020).

Preparing for next attack:
After being attacked once and if the network's weaknesses were exposed, the company is likely to be attacked again by the same source or another attack using the same strategy. That is why the investigation of the attack in detail is necessary to realise the weakness of the cybersecurity network that allowed the attack to happen and make it stronger to prevent another breach. MyFitnessPal were able to identify the gaps they had in the network such as a weaker password hashing algorithm like SHA-1 algorithm and are replacing it with a stronger Bcrypt algorithm to prevent brute-force. They have also modified their policies and only collect required data and avoid collecting personal data such as credit card details or national insurance numbers. This ensures that the user is safe from the exploitation of personal data if an attack takes place again (Eric, 2020).

4. Human aspects of the problem

The Unintentional actions by the user or the employee that lead to, spread or allow a security breach to occur is called a human error. Human error can be broadly classified into two categories: skill-based errors and decision-based errors. The skill-based error comprises of minor mistakes that takes place while carrying out familiar tasks and activities. In this type of error, the correct routine is known but due to a small slip or lapse or negligence, the end-user makes an error. The other type of error is called decision-based error which happens due to a

faulty decision made by the user. This can occur if the user has incomplete knowledge or does not have the right information for a specific circumstance. This can be tackled by effective security awareness training. Under Armour was not immune to these types of errors. These are the few types of errors that caused the breach of MyFitnessPal in 2018 (Micke, 2019).

Misdelivery

This error occurs when the email is sent to the wrong recipient, which is a fairly common problem that occurs daily in the corporate world. It is also one of the most common causes of all types of security breaches. This causes a leak of personal information to unauthorised users. The hackers were able to gather the caches of useful data by performing phishing scams via emails sent to the users where they pretend to be from Under Armour. The attackers had the intention to make the company pay for the data that they were able to gather. This ultimately results in a financial gain to the hackers at the loss of the company. Besides making a profit, the hackers had other motives such as gaining leverage on the user's personal information. Having gathered the initial information, they then have the potential to use that to acquire further confidential information, which they are able to sell (Micke, 2019).

Fig 5. Motivation of the attacker (Anna, 2020)

Password Problems

Passwords and humans don't get along well. In Under Armour's case, all the data that was leaked alone was not compelling enough to use by the hackers. Some users use similar passwords and usernames across all platforms. A survey done by OpenVPN highlights that 25% of the users will have the same passwords across all their accounts and social media sites and marketplaces (Tremblay, 2019) The attackers test the leaked information on all important websites to access further information and users that are unfamiliar with this concept causes the data breaches to be more dangerous than we may realise. Under Armour was recognized and is commended for its ability to detect this problem and act fast on it (Meyer, 2019). The attackers after stealing the data sold it on the dark web and the company made all the users of MyFitnessPal change their passwords and this reaction to the crisis led to the company achieving trust in their customers (Micke, 2019).

Patching

Attackers are continuously looking for new vulnerabilities in software. When they are discovered, there is a race between the developers and the attackers. The developer needs to patch the error before an attacker finds out and is able to breach the weakness of the system. That is why it is always recommended to update all the applications with new security patches as they majorly fix the issue of the previous version and make it more secure. Under Armour had hashed some of their passwords using a weaker hashing algorithm (SHA-1 algorithm) which the attackers were able to breach most of it. Hence, users need to keep their applications up to date so that they are less vulnerable to attack (Micke, 2019).

Human errors generally cause up to 95% of total breaches, the main reason for this error to occur is the lack of knowledge and increasing the opportunity for the attacker due to negligence. To reduce the opportunity, we need to systematically change our work practices, routines and technologies to yield better results. We can also reduce the privilege control allowing the user to only have access to information they need to perform their roles which reduces the exposure. Password management is necessary, and it can be done by encouraging users to use different passwords across all platforms and create a stronger password that can be harder to crack. This can be done by using a password manager application (Micke, 2019).

5. Ethical and legal considerations

The companies policies affect the customers directly. Under Armour's code of conduct highlights strong policies and ideas, but they need to be imposed to be a success. Due to this code of conduct. People at Under Armour wanted to give in-depth knowledge to their customers on the implication of having their personal data being sold on the dark web. The company had to hide some information during their public statement about the breach by not explaining the amount of data that had been stolen. The users had to update their passwords and avoid having similar passwords across multiple platforms and use complicated passwords to make their accounts less vulnerable to attacks. They also need to check online resources to know if their data has been included in the dump (Newcomb, 2019)

Due to the breach, it was an ethical responsibility of the company to not readily suggest their users to change their passwords on other platforms but to provide them with information and severity of the situation to help the customers to follow the procedures to stay more secure and take necessary precautions to prevent from further exploitation (Torres et al, 2021).

During the crisis, Under Armour was a target of a lawsuit. Rebecca Elizabeth Murray filed a class action lawsuit against Under Armour in February 2019 for compensation of financial damages that occurred during the breach. She questioned the company about the steps that were taken to secure the information of the customers. Murray states this in her following case:
Cause of action for:

- Breach of implied contract
- Negligence
- "Unfair competition and unfair business and fraudulent/deceptive business practices in violation of Cal. Bus. & Prof. Code §§ 17200, et. seq".
- Invasion of privacy
- Breach of covenant of duty of good faith and fair dealing
- "Violation of California's data breach statutes, Cal. Civ. Code §§ 1798.80 et seq." (Graham B, 2019, para 2)

Under Armour defence was that the customer agrees to the risk in their terms and condition (McGee, 2019) and they asked to move the case to arbitration (Graham B, 2019;Torres et al, 2021) .

The UK law for data ethics suggests that if personal data is used, the company must act according to the EU General Data Protection Regulation (GDPR) and Data Protection Act (DPA 2018). (UK, 2018). According to GDPR, Under Armour was required to report the breach within 72 hours. The GDPR also required the company to incorporate data security into

their company policies. It will also require the company to explain to the user about the use of the data that is being collected. To correctly protect the passwords and carry out the security requirements of the GDPR, the company should use a strong hashing algorithm and salting user passwords. According to the new policies, Under Armour is notifying the user to change their password and not allowing them to use a previous password as it could have been leaked during the breach (Michael, 2018)

According to Equality Act 2010, the application's automated decision-making outcomes should not lead to discriminations. While sharing the personal data Under Armour follows the Information Commissioner's Code of Practice for Data Sharing which goes along with the ICO's guide to GDPR. Under Armour has the rights to the data which was stolen due to Copyright and Rights in Databases Regulations 1997, so the attackers were not allowed to use the stolen data legally as it belonged to Under Armour (UK, 2018)

6. Futureproofing

Security breaches are a common occurrence in an organisation these days. To prevent and minimize the risks from breaches in the future, the organization needs to follow these methods:

Limit access to important data:
The organization needs to limit access to its crucial data. The confidential information of the user can be exploited even by an employee. It is important to mask that data and narrow it down to a pool of employees to work on a particular data (TechSupport, 2018).

Third-party vendors must comply:
Every organization does work on projects with a wide array of third-party vendors. It is crucial to do research on the company and its employees that your organization is going to work with. Taking such precautions is necessary as the third-party vendors might misuse the personal data you provided which could lead to a big data breach. It is important to have transparency and make sure they comply with the privacy laws (TechSupport, 2018).

Conduct employee security awareness training:
Employees are generally the weakest link in the data security chain. Educating them on security awareness is crucial. The employee can be vulnerable to open suspicious emails and be a target of phishing emails which can lead to the attackers having access of the network that is why it is necessary to educate them on a regular basis to take preventative measures. This training is followed by an anti-phishing test which could be taken by the employees (TechSupport, 2018).

Patching:
Updating the applications regularly as the new patches tackle the weakness of the previous version is crucial and makes the application more secure. Your network is vulnerable to attacks if the applications are not updated when available. Using Microsoft's applications such as Baseline Security Analyzer ensures that all the programs are up-to-date. Endpoint encryption protects data across multiple network endpoints (TechSupport, 2018).

Develop a cyber breach response plan:
Security attacks can occur even if the company manages to create the most secure system. No one is invulnerable to it. That is why it is necessary to have a plan set up for such a scenario. This will lead to a faster response and having such a plan can make the recovery phase faster and more structured. It is vital to create a well-designed plan for all scenarios so that the

company can tackle the problem and recover the damage as quickly as possible. It should begin with an evaluation of the situation and learning the details about the breach which can help the organization to take a swift and decisive decision that can limit the damages and restore the trust among the community (TechSupport, 2018).

Difficult to decipher passwords:
The organization needs to use a secure hashing algorithm to store the passwords which uses techniques such as salt and pepper. Using a weaker hashing algorithm can make the password easier to brute-force. Encouraging the users and employees to use complex passwords and avoid using similar passwords across all platforms should be encouraged. In the Under Armour breach, some passwords were hashed using a weaker hashing algorithm (SHA-1 algorithm) which was easier for attackers to brute-force and was compromised. Using a strong hashing algorithm such as the Bcrypt algorithm can prevent such vulnerabilities (TechSupport, 2018).

7. Conclusion

Online users have a vast range of networks to connect their devices to. Security of the shared data is prone to be attacked. The information security system is essential to stop such attacks. Under Armour experienced a data breach that affected 150 million of MyFitnessPal users disclosing their usernames, email addresses and hashed passwords due to a flaw in the cryptographic process (Newcomb, 2019). Fortunately, they were able to identify the breach early, before any major damage was caused. The company informed the users about the breach within a week. No sensitive information was leaked as the app does not collect information such as credit card details, national insurance number or driving licence number. The passwords were hashed using two hashing algorithms. Most of the passwords were hashed using the Bcrypt algorithm, which is very secure but some accounts suffered because a minority of the passwords were hashed using a weaker SHA-1 algorithm. The company suggested to all the users to change their passwords after being informed of the attack which ensured no more accounts were leaked. The company's share dropped by 4.6% after revealing its breach. Under Armour were able to bounce back as they gained trust from the customers due to their honesty and transparency.

The attacks occur on a regular basis, but organisations should be able to prevent or minimize the risks by taking necessary security measures. This can be done by limiting access to crucial data so that it does not get misused. It can also be achieved by maintaining a transparent relationship with the third-party vendors and making sure that they comply with privacy laws. Conduction of security awareness training is necessary to educate the employees. Regularly updating the software with patches to keep the application more secure is also beneficial. An organisation should always have a cyber breach response plan to act accordingly if a breach occurs. Increasing the difficulty to decipher passwords to maintain the secure data of the users should be of the utmost priority (wLife, 2019).

In conclusion, breaches are bound to occur if a tailored solution is not implemented to overcome the weakness of the network. These attacks can cause severe damage to the company and securing these data should be prioritised. This means that the company should always have a response plan in place if the breach occurs and to learn from past mistakes in order to implement more flawless plans in the future. Therefore, it is essential that these companies take suitable measures towards strengthening the security of an information system (wLife, 2019).

References

[1] Anna, X. (2020, November 11). The MyFitnessPal Data Breach. Available at: https://www.youtube.com/watch?v=Nu4ofghoUgA&t=312s

[2] Alex, G. (2020, November 10). MyFitnessPal Breach 2018. Available at: https://www.youtube.com/watch?v=7U5Ab_he03o&t=399s

[3] Eric, D. (2020, May 15). What is a security breach and how to recover from it. Available at: https://www.compuquip.com/blog/how-to-recover-from-a-security-breach

[4] Fearn-Banks, K. (2009). Crisis communications: A casebook approach. Routledge.

[5] Graham, B. (2019, March 5). Another proposed class action data breach lawsuit ordered to individual arbitration. Available at: https://www.disputingblog. com/another-proposed-class-action-data-breach-lawsuit-ordered-to-individual- arbitration/

[6] Hall, A., & Wright, C. (2018). Data security: A review of major security breaches between 2014 and 2018. Federation of Business Disciplines Journal, 50-63.

[7] McGee, M. K. (2019, June 1). Lawsuit filed in wake of Under Armour data breach. Available at: https://www.bankinfosecurity.com/lawsuit-filed-in-wake-under- armour-data-breach-a-11051

[8] Meyer, S. (2019, May 21). A tale of two data breaches – Under Armour and Panera Bread. Available at: https://www.cpomagazine.com/

[9] Michael, P. (2018, April 4). Cyber Security Lesson Brief from the Under Armour Breach. Available at: https://securityboulevard.com/2018/04/cyber-security-lesson-brief-from-the-under-armour-breach/

[10] Micke, A. (2019, April). The role of human error in successful cyber security breaches. Available at: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

[11] MyFitnessPal Account Security Issue: Frequently Asked Questions. (n.d.). (2019, June 9). Available at: https://content.myfitnesspal.com/security-information/FAQ.html

[12] Newcomb, A. (2019, February14). Hacked MyFitnessPal Data Goes on Sale on the Dark Web—One Year After the Breach. Available at: https://fortune.com/2019/02/14/hacked-myfitnesspal-data-sale-dark-web-one-year-breach/.

[13] Newman, L. H. (2018a, March 30). The Under Armour Hack Was Even Worse Than It Had to Be. Wired [web log]. Available at: https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/.

[14] Newman, L. H. (2018b, September 7). The Worst Cybersecurity Breaches of 2018 So Far. Wired [web log]. Available at: https://www.wired.com/story/2018-worst-hacks-so-far/.

[15] TechSupport, ML. (2018, Febuary 13). 6 Ways to Prevent Cybersecurity Breaches. Available at: https://www.techsupportofmn.com/6-ways-to-prevent-cybersecurity-breaches

[16] Torres, K., Stevenson, A., & Hicks, J. (2021). Case Study: Under Armour Hack. In Privacy Concerns Surrounding Personal Information Sharing on Health and Fitness Mobile Apps (pp. 145-162). IGI Global.

[17] Tremblay, L. (2019, April 23). Password security: How to avoid the most common password mistakes. Available at: https://zapier.com/blog/password-security/

[18] UK, G. (2018). Data Ethics Framework. DCMS. Available at: https://www.gov.uk/data-protection.

[19] Under Armour Code of Conduct. (2019, October 17). Available at: https:// about.underarmour.com/sites/default/files/2019-10/UA_CodeofConduct_2019_ English.pdf

[20] wLife, M. (2019, January22). A case study of security vulnerabilities faced by fashion company Under Armour. Available at: https://wlifemediadotcom.wordpress.com/2019/01/22/a-case-study-of-security-vulnerabilities-faced-by-a-fashion-company-under-armour/

[21] Williams, C. (2019, March 04). 620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts. Available at: https://www.theregister. co.uk/2019/02/11/620_million_hacked_accounts_dark_web/.