File and Database Security

Assignment - 2

19CSE311 – Computer Security

Date: *April 9, 2022*

Team Members:

S. No	Name of the Student	Roll No.
1.	PENUGONDA KOUSHIK	CB.EN.U4CSE19449
2.	RAVELLA ABHINAV	CB.EN.U4CSE19453
3.	ROHIT P M	CB.EN.U4CSE19454
4.	SINGADI SHANTHAN REDDY	CB.EN.U4CSE19459
5.	SINGAMANENI LIKHITHA	CB.EN.U4CSE19460

Abstract

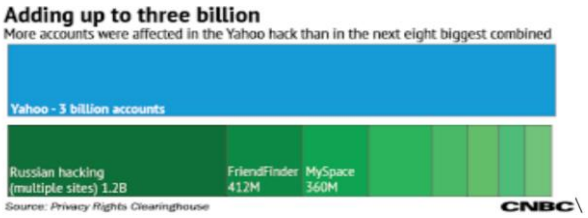
Database security has evolved; data security professionals have developed numerous techniques and approaches to assure data confidentiality, integrity, and availability. Our aim to help to learn many methods and techniques that will be helpful in securing, monitoring the database environments. Security issues are often a matter of misconfiguration, and the fact that the database implements a rich security model does not that it is being used or that it is being used correctly. If you are like 90% of database administrators or security administrators, you are probably aware that your database has a big gaping holes.

In early 2000, online music retailer CD Universe was compromised by a hacker named "Maxus". The hacker stole the credit card number from the merchant's database and tried to extort money from the merchant. When his claim was denied, he posted credit card details for thousands of customers online.

P. SAI KOUSHIK
CB.EN.U4CSE19449

Yahoo Database Attack:

The Yahoo data breach back in 2013 went through 2016 became the largest data breach in the internet history as you can see form the below reporting graph that up to 3 billion accounts were stolen during a period of time in 2013, 3billion adds up to be more than the total number of hacked accounts in the next 8 largest events that's a lot of people



How Yahoo got hacked:

The hack was carried out using a standard technique using the spam emails that you get with an attachment that leads to an intrusion, they call this spear fishing. Spear phishing is different than a regular fishing because it's more accurate it's targeted at somebody special whether it's a technician or a CEO of a company or just anyone that happens to work inside of Yahoo and so nobody actually knows what the message was or who delivered it or who opened it but it was enough to let the hackers and get inside once they were inside, they began to search around to see what valuable assets. there was a case open by the US government against Russian operatives and they brought them to court the court the actual case ended with the some of them declaring themselves to be guilty they declared a plebe bargain and at least one of them got five years in prison with a two hundred and fifty thousand dollars fine. the first thing they have to do is create a backdoor account so they can slip back in create new users and download things at a later date so one event to hack into the system and once they have that backdoor account created, they're ready to go to create other havoc so when they got inside what did they get the treasure chest boxed it contains the names of everyone in the accounts it shows their phone number and then importantly it shows their password challenge questions and answers. they also had the recovery emails so if they wanted to reset somebody's password, they would have the email address of where that message would go then also a proprietary system that was built by Yahoo used something called a nonce value.

What happened in the Yahoo data breach?

ROHIT P M
CB.EN.U4CSE19454

Web service provider, Yahoo, reported two major data breaches that compromised over 1.5 billion Yahoo user accounts. The hack began with a spear-phishing email sent to a Yahoo employee. The hacker, Aleksey Belan, managed to gain access to Yahoo's User database and

account management tool. Soon the hacker installed a backdoor on a Yahoo server where a backup copy of the user database was stolen.

Once the targeted accounts where identified, the hackers were using stolen cryptographic values," nonces", to generate access cookies using a script installed on the Yahoo server. These cookies were generated many times during 2014 – 2016 and gave the hackers free access to the accounts without needing any password.

Things to learn:

- Reviewing Intrusion detection system is essential.
- Updating systems to latest security standards is crucial as in the case of Yahoo, they were using discredited data encryption.
- Hiring a security team to monitor devices for malicious activity Yahoo's security team requests were turned down as they were too complicated.
- Using reCAPTCHA to keep spam emails away and digitize books and publications.
- Ensure employees use a standard password policy.
- Deploying firewalls and security software.

Users must change their passwords after breaches are detected. Yahoo failed to give timely notification of the breaches.

S.Likhitha

CB.EN.U4CSE19460

What Security Measures did Yahoo have in Place?

Most Yahoo passwords are cryptographically protected using a hash scheme. This is called Bcrypt. Its mathematical function is to convert plain text passwords into long text strings. These are stored on your company's servers. Security experts say this is safe because it slows down hackers. Prevents "brute force" attacks in which the program executes character combinations to break the code. However, your date of birth is usually not encrypted this way. This is because it is used for marketing and advertising purposes and all websites need access to this type of information.

Another issue is that pre-2014 Yahoo accounts may be protected by MD5 algorithms that have been shown to be vulnerable to brute force attacks.

Hackers steal your data and pretend that your personal information has been stolen. For example, to use a credit line such as a loan on your behalf. Victims of identity theft are usually unaware that they are the victim until a credit problem occurs.

How did Yahoo react to the Attacks?

Since the cyberattack, Yahoo has disabled fake cookies used in security breaches. It cannot be reused. You can no longer access your email account with unencrypted security questions

and answers. These also need to be reset. Yahoo has also set up a two-step verification process. The one-time security code is sent to the user's mobile phone via a text message or generated by the application when someone logs in with a password. You will not be able to access your account without this code.

Still, some experts say that Yahoo's response was "too little, too late." Yahoo should be more proactive in implementing security measures. Hacking is the price we pay for the internet. Whether for financial reasons or not, there will always be people who want to compete with security systems. Yahoo has failed to protect its users. Some people in the field of Internet security feel that Yahoo's security system is significantly underfunded.

There are also unanswered questions about when Yahoo learned of the attack. Yahoo's response to the seriousness of cyberattacks has changed dramatically, which is very mysterious. In September, Yahoo "pushed" password changes to users. By December, Yahoo had forced users to change their passwords. It is difficult to interpret their reasoning.

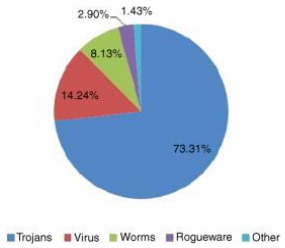
R.ABHINAV

CB.EN.U4CSE19453

Various tools for the Yahoo attack:

Malware:

Phishing: The hack began with a spear-phishing email sent in early 2014 to a Yahoo company employee. It's unclear how many employees were targeted and how many emails were sent, but it only takes one person to click on a link, and it happened. Unimaginable that Yahoo did not sufficiently step employees through new-school security awareness training to prevent disasters like this.



Solution to Database & File Security problem:

A complete solution to either the security or the privacy problem requires the following three steps:

1. **Policy:** The first step is to create a security or privacy policy. This policy accurately defines the requirements implemented inside the hardware and software of the computer system and outside the computer system. This includes physical, human and procedural control.

2. **Mechanism**: Security or privacy policies are embodied in the mechanisms required to implement the policy requirements. It is important that the mechanism performs the intended function.
3. **Assurance:** The final step deals with warranty issues. It contains guidelines to ensure that the mechanism meets policy requirements with a high level of security. Security is directly related to the work required to break the mechanism. The low warranty mechanism is easy to implement, but relatively easy to break. High-guaranteed mechanisms, on the other hand, are notorious for being difficult to implement.

   The high-level objectives of security are well known:
   1. **Secrecy**, which is concerned with unauthorized disclosure of information.
   2. **Integrity**, which is concerned with unauthorized modification of information.
   3. **Availability**, which is concerned with improper denial of access to information.

S.SHANTHAN

CB.EN.U4CSE19459

Measures to be taking to prevent attacks:

Your password is your first line of defence. Everyone understands that a simple number sequence or the phrase 'p-a-s-s-w-o-r-d' should never be used as a password. But how can you come up with a password?

A password should be strong, long, and unique, according to experts.

Don't make it obvious: There must be at least 12 characters, with a combination of uppercase, numerals, and punctuation symbols. There are no repeat characters or sequences.

Online Protection: Security questions and answers are your second line of defence against hackers when using the internet. The identical questions pop up on a lot of websites. If one of your systems gets hacked, all of your accounts are at risk. You should never use information that is freely available on the internet.

Protection Against Phishing and Identity Theft:

Scammers can obtain your personal information in a variety of methods, including when you unintentionally provide it. Place the phone on them and call them back in 10 minutes, preferably from a different device. Scammers might trick you into believing they have hung up by recording their dialling tone. You're still speaking with the scammers when you phone your bank's number for verification. Never give any personal information over the phone, including your PIN. Furthermore, you should never give a courier any of your bank cards to replace your card.

References:

1. Implementing database security and auditing, Natan, Ron Ben [ASE Library]
2. https://www.cnbc.com/how-the-yahoo-hack-stacks-up-to-previous-data-breaches.html