Cyberwatch Finland

WEEKLY REVIEW

18/2024

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

18/2024

PASSWORDS AND BRUTE FORCE ATTACKS

When talking about password security, the discussion usually focuses only on what constitutes a secure password. Sometimes one can see references to times, on how long it takes to crack different passwords, or how password length increases the security factor. A longer and more complex password, i.e. one that uses several character types (lowercase, uppercase, numbers, special characters), is secure because it provides better protection against brute force attacks on passwords. In these attacks, the malicious actor tries to guess the password associated with the username simply by trying all possible combinations using automation. Naturally, brute force attacks cannot be used on the login windows themselves, which passwords are intended to penetrate, as these usually limit the number of login attempts allowed to a particular account. Carrying out a brute force attack often requires, for example, the hash value of the password obtained through a data breach. This value is also known as an encrypted password, and simply put, it refers to a password that has been unreadable using an encryption algorithm. A common example of password encryption goes as follows: when a user first registers for a service, a hash value corresponding to their password is created and stored in the service's database. Since the encryption algorithm always produces the same hash value for the same password, there is no need to store the password itself in the service. In the future, when the user returns to the service, the login can be verified by comparing the hash value of the entered password with the value stored in the database. The natural advantage here is that the service provider never gets hold of the actual easy-to-read passwords, which reduces the risk of both internal misuse and data breaches. Done this way, the attacker has the potential to gain access to hash values alone.

There are several different cryptographic algorithms, and there are differences between them, among other features, but also in how well they withstand brute force attacks. At the moment, the popular and well-liked encryption algorithm is called bcrypt, but to some extent the older and much less secure MD5 algorithm is also used. Typically, the user cannot notice or distinguish which or what kind of password protection method is in use, as even the highest level of security algorithms only take a few seconds to change the password to an encrypted form, so the differences in the login process are practically imperceptible. In any case, no matter how high-level the algorithm is, a brute force attack is always theoretically possible if the threat actor gains unlimited access to the hash value. In theory, because passwords encrypted with bcrypt, for example, can take tens, hundreds or thousands of years to crack with modern technology, depending on the characteristics of the password. Most recently, these times have been mapped by US security firm Hive Systems, which measured

theoretical times how long it would take to crack various bcrypt-protected passwords. The attack used twelve high-quality graphics cards as computing power. The power was deliberately chosen so that it could match the computing power held by a mid-level threat actor, either through physical components or a botnet. According to the results of the test, the critical limit would go to eight characters if both numbers and lowercase and uppercase letters are used. It would take about three years to crack a password of this level, and the times increase exponentially as passwords become longer or more complex.

However, neither this chapter nor any other guidance on how long a password is secure should be relied on too much. Tests usually only measure the durability of randomly generated passwords, and since extremely few people actually use completely random passwords, cracking is often easier than what with only a brute force attack. Some of the most common password cracking techniques include a dictionary attack i.e. trying commonly used passwords, phrases or variations of them. It is also common to try passwords stolen from elsewhere by the same user or modifications of these. Nowadays, brute force attacks are more often accompanied by one of these techniques. For example, if it is known what types of passwords a particular person usually uses, the time it takes to carry out a brute force attack will be significantly reduced. To illustrate, if it can be seen from the hijacked passwords that a person usually uses a passphrase consisting of two words, the first letter of which is always uppercase and there are two numbers and a special character at the end a this knowledge can significantly enhance the effectiveness of a brute force attack, as it the amount of possible passwords the attacker has to go through. This can make a long and complex password vulnerable to brute force attacks when supported by other methods of cracking.

Therefore, when creating a good password, one shouldn't just focus on character count and complexity. Of course, they are important factors in improving security, but equally critical are the difficult guess ability and uniqueness of the password. The use of whole plain text words should be avoided, and the same password should under no circumstances be used in multiple places. When talking about passwords, it is important to remember that in many respects it is already considered an outdated solution for authentication, from which the aim is to move away. As a verification method, passwords have a lot of downsides, and their crackability is just one of them. Various biometric authentication methods as well as multi-factor authentication are gradually replacing or at least rising alongside passwords. However, most likely, they will not be completely gone anywhere in the near future, so the protection of passwords is an acute issue, at least for the time being.

CYBER THREATS ARE HIGHLIGHTED IN HEALTH AND WELLNESS APPLICATIONS

The popularity of various health applications has increased considerably in recent years. Especially during the coronavirus pandemic, people's desire to monitor their own health, activity and, for example, recovery increased. In addition, the use of various telemedicine and telecare applications and systems has clearly increased in recent years. As large masses of people have preferred these different wellness applications and devices, the amount of data they collect has also increased significantly. They collect very personal and accurate data about their users. This arouses interest and desire in various parties to utilise this data.

The General Data Protection Regulation (GDPR) also aims to ensure protection and appropriate processing of the data collected by health apps. However, many applications also allow data sharing with third parties. According to a study by the BMJ (formerly British Medical Journal), data from health applications is still shared with third parties, and transparency in the use of data is weak in many places. Information about these applications ends up especially to large corporations such as Alphabet, Amazon and Microsoft. These large corporations, in turn, resell this data to fourth parties, such as multinational technology companies or advertising, telecommunications or a consumer credit reporting agencies. When deploying various health applications, the user must familiarize themselves with the data collected by devices and applications and how to share it further. In many cases, the user can choose to share the data collected by the app outside the app.

Naturally, criminals are also interested in this data collected by various health applications and devices. Criminals seek out sensitive information contained in apps, which apps collect in large quantities. Criminals seek to gain access to this data through data breaches, hacking communication systems, or even exploiting third-party vulnerabilities. The goal of data breaches can be to gain access to and resell large amounts of data on dark web marketplaces, blackmail sensitive information, or exploit it as a tool for social engineering.

Recently, there has also been an increase in attacks on medical records in the healthcare sector. In these cases, blackmail of the system holder and encryption of data have been common, but individuals have also started to be blackmailed with personal and sensitive information. This same trend can be expected for health and wellness applications. Criminals will pursue the personal data contained in the applications and exploit it for their own criminal activities. At the same time as criminals' growing interests in the data of actors in the health and wellbeing sector are growing, studies show that the level of information security in the health and wellbeing sector lags far

behind that of the technology industry. According to a study by Osterman Research, in the field of health and wellbeing, 43% of survey respondents considered it more important to develop new features for systems and applications than to be responsible for maintaining information security. This requires a major change of attitude and tighter supervision of those responsible for managing sensitive data, especially in the health and wellbeing sectors.

In 2018, Polar's wellness and sports app was found to leak the personal information of military and intelligence service employees, among others, openly available, based on training results shared by users on the app's community platform. In addition to heart rate data, dates, routes, times, training length and pace, the platform displayed the users' possible home addresses. This made it possible to identify employees of soldiers, intelligence services, embassies, air bases and many other special branches.

The above-mentioned case is a well-known and dangerous example of the dangers of health and wellbeing applications. It doesn't always take even a breach to bring out sensitive information about these applications. In this case, for example, state actors were able to locate and identify important military and other authorities around the world using the app's intended features alone. The health and wellbeing sector needs a clear change in information security culture and investment in information security practices and expertise. It is necessary to understand the significance of the data contained in different applications and systems and act accordingly. It is also the user's responsibility to find out who collects information about you, what they use it for, and what information the user should share before using an application.

MAY DAY SPECIAL – UNEXPECTED CONSEQUENCES OF CYBERATTACKS

While cyberattacks are by no means fun, they can sometimes have extraordinal consequences. In honour of May Day, Cyberwatch Finland publishes a summary of recent and a few older cyber events with surprising consequences. We hope readers have had a joyful May Day.

STREETLIGHTS IN THE CITY OF LEICESTER WERE LEFT ON

DATE: 7.3.2024
DESCRIPTION: The city of Leicester, which suffered a ransomware attack in March, has been suffering from the effects of the cyberattack well into April. What happened immediately after the attack affected the online operation of several of its services, such as child welfare and homeless services.
ACTOR: INC Ransom, a relatively new threat actor whose victims have been many different governmental organisations around the world.
MOTIVE: Economic
IMPACT: The threat actor has published more than one terabyte of city-related data on the dark web. Sensitive information of municipal residents may also be included. The attack has also had surprising effects. For example, the remote control of streetlights in the city has not yet been restored, which has led to streetlights burning even in broad daylight.

THE ATTACK ON THE LOGISTICS CHAIN AFFECTED SWEDISH ALCOHOL MARKET

DATE: 23.4.2024
DESCRIPTION: The ransomware attack on the Swedish logistics operator Skanlog has had a wide impact on the company's operations. The company's CEO said all systems, such as inventory and finance software, had stopped working. At the time of writing, it is still unclear whether functionality has been restored.
ACTOR: North Korean hackers, the exact perpetrator has not been identified, but well-known North Korean cyber actors include for example Lazarus and Kimsuky, the first of which is known to have previously used ransomware in their attacks.
MOTIVE: Economic
IMPACT: In addition to directly affecting Skanlog, the attack on the logistics chain affected the delivery of alcoholic beverages to Systembologat Sweden, for which Skanlog is a major supplier. Systembolaget warned that certain beers, wines, spirits and even paper bags could run out of its stores. Fortunately, Systembolaget announced that if supply problems continue, they have a backup plan in place for such situations.

AC/DC PLAYING AT IRANIAN NUCLEAR POWER PLANTS

DATE: 2012
DESCRIPTION: According to unverified information, in 2012, hackers managed to penetrate closed networks used by Iran in its nuclear program. The virus used by the hackers was reported to have disrupted the automation processes of nuclear enrichment plants.
ACTOR: Presumably U.S. and Israeli intelligence agencies.
MOTIVE: Obstructing or blocking Iran's nuclear programme.
IMPACT: In addition to disrupting automation processes, the hackers managed to break into the terminals of nuclear facilities and played the classic song Thunderstruck by the rock band AC/DC. Iran's nuclear programme had already before been attacked with malware such as Stuxnet and Flame.

CYBERATTACK CARRIED OUT BY USING A FISH TANK

DATE: 2017
DESCRIPTION: According to a report by cybersecurity company Darktrace, a North American casino, whose name is not disclosed for security reasons, fell victim to a cyberattack. What makes the attack exceptional is the method used to break in.
ACTOR: Unknown
MOTIVE: Unknown
IMPACT: In this case, the casino lost over 10 gigabits of data that was sent to a server in Finland. The data was accessed using the casino's internet-connected aquarium, the management of which opened the way for discovering other vulnerabilities in the network and penetrating deeper into the systems. What happened highlights the risks associated with the so-called Internet of Things (IoT) -devices. As more and more devices are connected to the network, the lack of security of even one can lead to the compromise of valuable data.

REFERENCES:

PASSWORDS AND BRUTE FORCE ATTACKS

https://www.proofpoint.com/us/blog/information-protection/password-cracking-techniques-used-in-cyber-attacks
https://www.hivesystems.com/blog/are-your-passwords-in-the-green
https://www.securityweek.com/new-password-cracking-analysis-targets-bcrypt/
https://guptadeepak.com/password-hashing-algorithms-101/

CYBER THREATS ARE HIGHLIGHTED IN HEALTH AND WELLNESS APPLICATIONS

https://securityaffairs.com/74324/digital-id/polar-data-leak.html
https://www.bmj.com/company/newsroom/data-sharing-by-popular-health-apps-is-routine-and-far-from-transparent/
https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/
https://medtech.citeline.com/MT145768/Mobile-Health-Apps-Are-Falling-Behind-In-Cybersecurity-Report-Finds

MAY DAY SPECIAL – UNEXPECTED CONSEQUENCES OF CYBERATTACKS

https://www.ncsc.gov.uk/blog-post/products-on-your-perimeter
https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/
https://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/index.html
https://securityaffairs.com/162333/cyber-crime/swedens-liquor-supply-ransomware-attack.html
https://therecord.media/sweden-ransomware-liquor-shortage-skanlog-systembolaget
https://www.bbc.com/news/uk-england-leicestershire-68777506
https://therecord.media/leicester-city-council-ransomware-data-breach
https://www.bbc.com/news/uk-england-leicestershire-68881057

Cyberwatch Weekly

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Pixabay
Unsplash

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi