Cashless Payment and Security(Part 1)

Although paying with a credit card or app is becoming a more accepted practice, many Americans would still hesitate to go completely cashless. In this article, we will explore various aspects of security regarding QR code payments.

Security Regarding Payment

When discussing cashless, the most common incident involves the unauthorized use of credit cards. However, with a credit card, it is common for the bank to provide assistance to the user and thus the inflicted damage is oftentimes not very high.

In this article, we would like to discuss payment via QR code, a method steadily increasing in use.

List Based Attack

A list-based attack is also known as password-list attack or list type attack. Briefly stated, it is to impersonate the victim by obtaining their account and password combination through some means.

Common Methods:
・Brute Force Attack: The attacker would target one account, and would start putting in a combination of A~Z and 0~9 in rising order to crack the password.
・Dictionary Attack: Similar to the brute force attack, except it would test a set number of commonly used passwords to try and crack the password.

Since the attack involves the need to login to a single account a large amount of time, the most common way to stop this would be to put a restriction on the number of times a user can make a mistake in the password. There was a case in Japan in which a brute force attack succeeded against the security code of the credit card(3-digit number on the back of the card), because of the lack of a maximum number of inputs for that parameter.

For sites that restrict the number of attempts, password spraying could be used. Password spraying, in contrast to the single target attacks above, would take thousands of accounts and test commonly used passwords. Since this method uses a different account for each login, it is very difficult for the system to detect this kind of attack.

Account List for Password Spraying

There are many methods in which an attacker would obtain the list of accounts, often via the Internet, either from disclosure as explained in the following or from those sold through the Internet.

Many of these lists are based on lists that were leaked from a previous account spill. These accounts are in a combined state without deduplication or name identification. For this reason, lack of name identification or the account being simply too old, the number of usable account would be largely is very small.

Even then, if there was a leak of 2.2 billion and .001% of the leaked account was usable, then there would be twenty thousand accounts that can be exploited, which is still a significant number.

Prevention for Password Spraying

There is no way for users to control the account leakage, but there are ways we can handle it.

You may have heard of the term, 2-factor authentication or simply 2FA. Ordinarily, users would log in using an account ID and password, however, there is still a chance that a third party could impersonate the user. 2FA is an extra layer of security to authenticate the user.

A well-known second verification was text message authentication, where after a user enters their ID and password, the system would send a text message to a preassigned phone number with a code that can be entered into the system to verify the user. A phone number is something that is unique with each individual which makes this security system secure.

The problem with text message identification, however, is that depending on the phone plan the user has registered, it may cost money to receive a text message. That is why text message identification is only done in special cases, such as when the user access through a new device.

A cost-efficient alternative is to identify whether the user is a robot.

Most attacks are done using a robot that would rapidly attempt to log in a large amount of time. To accommodate this, the developers can implement a test that would be easy to a human, but difficult for a machine. The most common ones are introduced below.

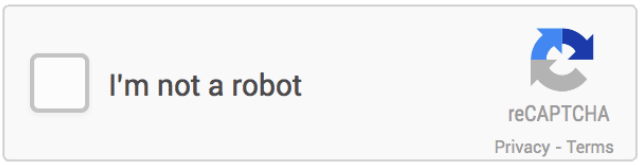
CAPTCHA Authentication

There may have been times when logging in that the system would ask the user to identify a distorted text. These are the CAPTCHA authentication. Humans could read it with little difficulty, contrary to a robot that would have a hard time reading it.

Unfortunately, however, robots are getting smarter to the point where they can recognize it as well as a human, and distorting it any further would make it more difficult for the human users to recognize.

reCAPTCHA Authentication

It is an improved version of CAPTCHA authentication. reCAPTCHA v2 is usually associated with the familiar “Are you a robot?” with a checkbox next to it. Generally, it would give a visual identification of obscure objects.



Recently an improved reCAPTCHA v3 was also released, in which authentication is performed through only behavior (by site history, or cursor movements), so it does not require an image authentication.

The lack of image authentication seems beneficial, however, when judged incorrectly, the cause is not understood and the criteria are not disclosed.

For this reason, the site administrator needs to prepare an alternate authentication method in case the judgment fails.

Capy Captcha

This method originated in Japan and is famous for its authentication that involves fitting pieces of a jigsaw puzzle.

These measures prevent robots from authenticating. However, since the technology to break through is advancing day by day, this measure is not absolute. However, since the attacking side places importance on cost-effectiveness, there is a tendency to target sites that are vulnerable. Therefore, a certain deterrent effect can be expected with increased authentication measures.

There are other methods such as blocking further attempts after a large number of login requests, but attackers use multiple source IPs as countermeasures and try to log in randomly, such as once in tens of minutes. New measures are taken as new ways of attacks are performed and so the cycle continues.

In addition to authentication, there are sites that sends an email when you perform certain operations such as login. This method can also help detect fraud early.

User Measures

Statistically, more than 90 percent of users reuse their passwords.

To avoid getting your account compromised:

- Avoid website that does not offer 2-factor authentication
- Do not reuse the same account name and password for all your account

These may be the best method to avoid the compromise of an account based on the above information.

Remembering passwords is cumbersome, in fact, regardless of list-type attacks, statistically complicated passwords do not increase security. This is because most services currently have a limit on password mistakes, and account locks are made for a certain period of time. Attackers refrain from brute force attacks on such sites because they are inefficient.

In fact, uselessly complex passwords can only lead to forgetting or making mistakes, so passwords that meet the requirements of the system and do not appear in the dictionary are sufficient.

As an example, instead of having a hard to remember character string sequence such as “8Lr4! Z” it is sufficient enough to end your normal passwords with the site abbreviation.

However, it is always recommended to change the password whenever there is an ID leak on a site you are using, including passwords for other sites.

It is safe to manage the password with paper, but if it is difficult, use password management software to keep it as secure as possible.

Lastly, even after all precautions, it is still possible for an account theft to occur, so it is recommended with anything that contains payment information, to make sure to know about damage compensation for any banks that are being used.

Conclusion

This fight between attackers and security will likely continue on for an unseeable future. Against this, we believe that the best defense is to always keep awareness. It would go a long way toward protecting yourself to keep up with new security and modes of attacks.

There will be a part two of this article coming up next time, so stay tuned~