TO: Javed Ali and Carl Landwehr
FROM: Chia Wen Cheng
SUBJECT: Policy Recommendations for the Weakness of Two-factor Authentication
DATE: November 15, 2021

Summary
Two-factor authentication is an evolutionary improve of password cryptology. Strong passwords are no longer "strong" without another layer of verification because the hackers have exceeded these technologies. However, according to the rapid progress in cyber technologies, traditional two-factor authentication also faces challenges of insufficient security. It is estimated that in the near future, some types of two-factor authentication systems will otherwise provide chances for the hackers to infect targets' smartphones. In order to protect the cyber security for account holders, government, server providers, online account maintainers, and the consumers need to work together to ensure that these weaknesses are quickly addressed and fixed.

Threat Scenario Assessment
Over the past ten years, two-factor authentication has become a trend in terms of enhancing the security of online accounts. A two-factor authentication creates another way for the server to confirm the person trying to log in to its platform is the one that he/she claims he/she is. So an account protected with dual authentication is much harder to hack into, even if the user password is easy to compromise.[1] Servers from banks, emails, social media, retailers, and so on, started asking their customers to set up a two-factor authentication for their apps because they were notified that the consumers preferred service with it.[2] The two-factor authentication is a mechanism that asks users to verify their identifications by accurately completing additional steps after entering login information. The second security factor can be either something the user has (one's cellphone or hardware OTP token) or something the user is (one's fingerprint). OTP tokens can be sent through SMS texts, emails, or other verification apps that connect with users' devices. If companies were unable to offer this level of security, consumers would turn to competitors, seeking similar service with "better security" instead.

Despite its function of providing extra security, two-factor authentication is still a technology that is vulnerable to hackers, and will become weaker and weaker over time. Hackers can insert a piece of code into the original programming to disrupt the system and send out erroneous messages to clients. Or, they can pose as a verification system itself by imitating verification messages, and trick the users to click on links, through which personal data is leaked to the hackers without the user noticing anything amiss. However, not until Mat Honan, a journalist, revealed his experience of digital life being dissolved in 2012, very few firms and consumers were aware of the weaknesses in two-factor authentication.[3] Many large-scale companies have subsequently reported hacks related to two-factor authentication ever since then, including the Reddit Hack in 2018.[4]

---

[1] Anna. (September 16, 2019). 2FA Security Flaws You Should Know About. *Protectimus.* Retrieved on November 12, 2021, from https://www.protectimus.com/blog/2fa-security-flaws/
[2] Russell Brandom. (July 10, 2017). Two-factor Authentication is a Mess. *The Verge.* Retrieved on November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess
[3] Russell Brandom. (July 10, 2017). Two-factor Authentication is a Mess. *The Verge.* Retrieved on November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess
[4] Sarah Meyer. (August 9, 2018). Reddit Hack Exposes Two-factor Authentication Weakness. *CPO Magazine.*

The issues of a two-factor authentication are typically related to things around it, not the system itself.[5] For example, the hackers only need to get the ownership of one's phone number to deliver an OTP, which stands for a one-time password, via SMS. As long as a criminal is able to compromise the AT&T, Verizon, or T-Mobile account that supports a person's phone number, he/she can usually hijack any call or text that is sent to his/her targets. Users of mobile apps like Signal, which are tied entirely to a given phone number, can be the most vulnerable under this circumstance.[6] Another example is closely related to the smartphone's Internet connection. It is easy to infect a smartphone with malware and intercept the OTP SMS.[7] In the era of the Internet, it has become harder and harder to predict and prevent such attacks as technologies continue to advance.

Furthermore, it has been proven to be difficult to discontinue particular types of two-factor even when they are known to be insecure, making it more crucial to break the myths and to better secure the cyber networks. Among all the methods to authenticate, a hardware token is the best way to achieve. Yubikey, which works for Google, Facebook, and many other major services, is a good example of a hardware token. It cannot be spoofed even if the user sticks it in a wrong computer thanks to the FIDO spec. A dedicated app such as Google Authenticator is good enough for the users to rely on. It is easy to get most of the protection offering by two-factor. SMS has been the worst that sits at the center of many recent two-factor hacks, but it is also the easiest one to accomplish. High-security accounts are already moving away from it, but a frightening number of services still keep it as an option, giving anyone who compromises your carrier account an easy way in.[8] The National Institute of Standards and Technology quietly withdrew support for SMS-based two-factor authentication in August, pointing to the risk of interception or spoofing, but tech companies have been slow to respond. Even large-scale companies such as Twitter and PayPal look to tie accounts more closely to users' phone numbers, showing that the unconsciousness of the weakness will lead to potential threats of two-factor authentication in the near future.[9]

The threats of two-factor authentication can be seen in a measure that United States government will take: in order to put an end to the phishing attacks, United States government employees will soon be required to use a stronger measure of multi-factor authentication to access their work accounts, most likely a hardware security key, taking place the less secure SMS text messages and app-based authenticators. These keys would have to be physically inserted into a USB or similar

---

Retrieved on November 14, 2021, from https://www.cpomagazine.com/cyber-security/reddit-hack-exposes-two-factor-authentication-weakness/

[5] Sarah Meyer. (August 9, 2018). Reddit Hack Exposes Two-factor Authentication Weakness. *CPO Magazine.* Retrieved on November 14, 2021, https://www.cpomagazine.com/cyber-security/reddit-hack-exposes-two-factor-authentication-weakness/

[6] Russell Brandom. (July 10, 2017). Two-factor Authentication is a Mess. *The Verge.* Retrieved on November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

[7] Anna. (September 16, 2019). 2FA Security Flaws You Should Know About. *Protectimus.* Retrieved on November 12, 2021, from https://www.protectimus.com/blog/2fa-security-flaws/

[8] Russell Brandom. (July 10, 2017). Two-factor Authentication is a Mess. *The Verge.* Retrieved on November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

[9] Russell Brandom. (July 10, 2017). Two-factor Authentication is a Mess. *The Verge.* Retrieved on November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

port at the time of login to verify the government employee's identity.[10] Though phishing has become much more targeted and sophisticated, one of the primary concerns in taking this action of improvement is automated and inexpensive attacks that can be scaled when victims are found. Even these relatively simple attacks have the ability to convincingly spoof government websites and capture multi-factor authentication tokens sent over text message or email, forcing the government to take an early action in preventing itself from the worst scenario that it is attacked too severely to keep operating, which is highly likely to happen right after the large-scale companies.[11]

Courses of Action

While the accounts with previously recognized strong passwords became more vulnerable to be hacked into, it is essential that we look forward to the possible near future threats of the currently regarded strong two-factor authentication, and to make policies in advance. The three courses of action that should be considered are: enforcing random updates of the two-factor authentication systems, asking online stores using weak authentication measure to add another dual verification system when needed, elevating citizens' awareness through education.

Option 1: Enforce Updating the Two-factor Authentication Systems from Time to Time

While the two-factor authentication systems leverage the difficulties for a hacker to successfully attack, they are still digital systems that should be updated frequently just like others. Without random updates, potential hackers are able to prepare for the attacks and cause as much inconvenience as possible before they get what they want. Thus, it is critical that the two-factor authentication servers update their systems frequently from time to time to be able to defend against hacks.

Benefits

Requiring servers to update their two-factor authentication systems frequently will boost them to provide better service with higher quality of security. They will benefit from being one of the top priorities for the companies looking for a reliable authentication server to cooperate with. Moreover, when many companies cooperate with one authentication server, the server can gain financial and non-financial benefits from the economies of scale.

Risks

The process of anticipating future attacks, and trying to get rid of them with continuously coding, debugging, updating the software can be annoying. Nonetheless, without proper updates, the weakness in a system is easy to discover. The burden to keep one's accounts secure falls to each user because the security function has eliminated over time if the servers refused to update their systems constantly. To further encourage the servers in doing so, and to defend for the security, subsidizing the servers may be a good incentive.

[10] Scott Ikeda. (October 27, 2021). Retrieved November 11, 2021, from https://www.cpomagazine.com/cyber-security/phishing-resistant-multi-factor-authentication-coming-for-us-government-employees-as-zero-trust-architecture-rolls-out/

[11] Scott Ikeda. (October 27, 2021). Retrieved November 11, 2021, from https://www.cpomagazine.com/cyber-security/phishing-resistant-multi-factor-authentication-coming-for-us-government-employees-as-zero-trust-architecture-rolls-out/

Option 2: Online Stores Using SMS Verification Must Add a Different Two-factor Authentication in the Payment Process

As discussed above, SMS is the least secure way to complete a two-factor authentication. However, it's the easiest way to do so, and thus is the most common method in use today. In order to create a safer Internet environment for people to enjoy easy shopping, it is essential to ensure a secure environment for financial transactions. The more layers of verification there are, the more secure the environment is. Hence, forcing the online stores that have weak verification access to adapt a stronger access during a high-risk process is necessary.

Benefits

Compared to forcing all the online stores to transfer to a new mechanism, adding another verification during a high-risk process is easier to implement. The stronger authentication protects both the consumer and the supplier in a transaction from frauds or bankrupting. Moreover, it affects only a number of consumers who are willing to ease their shopping experience through online access but who still care about their financial security. A second authentication during payment process would preserve both the convenience of online shopping and increased financial security.

Risks

The costs for establishing double two-factor authentication systems for an online store can be high, enough to discourage online businesses from doing so. Additionally, it may draw the clients away from shopping at those stores with the complaints of the repetition in verification process, which could put the business at risk of closing. The balance between economic prosperity and security is difficult to strike and should be carefully assessed before implementing.

Option 3: Prioritize Consumer Education and Awareness in Selecting a Higher Secure Method through Education

Although the providers of authentication systems have an important role in offering consumers secure ways of accessing their accounts, it is still crucial that consumers themselves understand the mechanisms and the pros and cons of each method and choose wisely under different circumstances. Education is an effective and the most long-lasting way to encourage rational consumers to make the most efficient measure, and to urge the servers to improve their service at the same time.

Benefits

Technologies of big data has connected Internet users together, forming complicated but fragile networks behind numerous websites and social media. Once part of the network is attacked, the whole network can be easily destroyed, affecting millions of people within short time. The external costs can be extremely tremendous in merely one attack. Like many other public security issues, if every person is aware of the potential dangers, the external costs to society are reduced. In addition, education is a general public service that nearly everyone as a citizen is able to enjoy. Thus, education can make broad and lasting changes at less cost.

Risks

Education is the most basic way to make an evolution in values and thoughts. However, there still exist some obstacles or exclusions in education--the dropouts and the unreported children are just a few examples. These exclusions may not be easily found or may be tough to solve, but are crucial

in establishing a safe Internet environment. If the obstacles are kept being neglected, the results of enhancing awareness in cybersecurity from education will turn out to be ineffective, and the government may need to pay more for the failure.

Recommendation

As online accounts become general options for almost every industry, it is vital that government, server providers, online account maintainers, and the consumers collaborate to defend cyber security by strengthening two-factor authentication, which is known as the strictest measure in verifying identification so far. Although a hardware token is the most recommended for its high security, it is difficult to request every online account holders to transform to it, for the complexity and the inconvenience will reduce the willingness to two-factor authentication significantly. Within the limitation of humanities and among the three policy options, Option 1: Enforce Updating the Two-factor Authentication Systems from Time to Time can be applied to the most users in short-term and create the largest benefits to the society.

Randomly updating the programming offers higher quality of service and security to users and demanded companies. However, from the lenses of economics, this requirement burdens system managers too much that may shrink them back in terms of the willingness to provide qualified service. As a result, problematic circumstances in bearing these social costs emerge. In order to encourage the managers to participate in the cooperation, subsidies may be efficient incentives to them. Even with subsidies, the society can still benefit from Policy Option 1 for the fact that it costs much more to recover from a cyber catastrophe.