Sarah Hall-Swan

Comp116 Security

Two-Factor Authentication: Could We Do Better?

Abstract

Multi-factor authentication is a mechanism that requires users to supply multiple forms of authentication before they are granted access. The idea is that the user must provide more than one piece of evidence as to who they are. Two-factor authentication is a very common tool used to secure online accounts. Most of the time, two-factor authentication uses a user's mobile device as the second factor, requiring the user to input a username and password, plus a code sent to their mobile device in order to log in. Many services now use two-factor authentication for username or password recovery. This paper will explore the effectiveness of two-factor authentication and analyze some context-based security alternatives.

Introduction

The authentication of users is an important part of web and computer-based systems. Ensuring that each user is who they say they are is vital to maintaining a secure system. Traditionally, this authentication is in the form of a username and password, but it is becoming increasingly clear that this is not enough to prevent unauthorized access. A survey of 500 IT managers by IS Decisions, 45% of organizations suffered a security breach as a result of compromised credentials.[1] To prevent these breaches, some turn to multi-factor authentication.

Multi-factor authentication is a method of authentication in which the user is only granted access after providing multiple pieces of evidence that they are whom they claim to be. The most common form of multi-factor authentication is two-factor. In the context of online or other

electronic accounts, the first factor is usually a password, and the second factor could be anything. Two-factor authentication is lauded as a solution to the ever-growing security issue in cyber tech, and increasing platforms require or at least offer the option of including a second factor on top of the usual password. However, although two-factor authentication can be considered more secure than one-factor, it is not the final solution to security issues that it is sometimes made out to be.

To the Community

Chances are many of your online accounts have asked you to set up two-factor authentication to increase the security of your account. This is probably in the form of a mobile phone number, or maybe an email address. This is a common form of two-factor authentication, but it does not add as much security as they claim. It is important to understand the reasons behind two-factor authentication, as it has merits and in more secure in certain forms than in others. I will also explore alternatives that could replace or be used in conjunction with two-factor authentication.

What is Two-Factor Authentication?

Two-factor authentication (2FA), and indeed all multi-factor authentication, is built on having multiple pieces of evidence as to who you are. Each piece of evidence tends to fall under one of these categories[2]

- what you know
- what you own
- who you are

A password, the most common factor, falls under “what you know”. A credit card falls under “what you own”. Both are insecure because they only use one factor. Some examples of more

secure methods are debit cards, which use the card itself (what you own) and a pin (what you know), or Apply Pay, which uses your iPhone (what you own) and your fingerprint (who you are)[3]. One of the most secure options is a special USB drive that serves as a "what you own" factor on top of a normal password. This drive is $18 and is supported by most major services, so if you aren't prone to losing things this is a good option[4]. Many services use a password (what you know) and a code sent to your phone (what you own) via SMS.

The Faults of Two-Factor Authentication

One reason 2FA is not a solution is that it is not used as often as it could be. In general, organizations are not adopting 2FA because it impedes their employees. In the IS Decisions survey, only 38% of IT managers said their company used multi-factor authentication. In that same survey, 51% agreed that the day-to-day impact of security on employee productivity is increasing.[1] The additional security steps that each user must take to be granted access wears into the time that they are actually accessing the information they need to access, and this decreases how productive these employees are. In an environment where employee productivity is prized above security, the extra steps are not worth the security benefit. In this way, 2FA is ineffective because many don't want to use it. These organizations are not using 2FA also because it is costly and complex for IT to setup and more importantly manage.[1] When 2FA is in use, it is often in the form of SMS texts, which is not an effective security measure. Good practice, as in not using SMS, would greatly improve the security when using 2FA.

When 2FA is in place, attackers can still successfully infiltrate user accounts. The most common form of 2FA is a password and a code sent over SMS, and this code can be intercepted.

Attackers can compromise the wireless carrier and therefore hijack any call or text. Attackers can also exploit account recovery systems to gain access to their victim's texts.[4]

An prime example took place in 2014, when Partap Davis lost $3000 from his bitcoin wallets to an attacker. Davis had set up 2FA for his Gmail account that required inputting a code sent to his phone, and similar authentication for his bitcoin wallets that used an app called Authy on his phone to verify each login. The attacker gained access to Davis's email, and that was the key into gaining access to his other accounts, as she used the email to set up call forwarding from Davis's phone to hers and reset Authy on her phone. From there she could easily gain access to his bitcoin wallets.[5] Despite 2FA, the attacker could still gain access to Davis's accounts, made easier by the fact that the 2FA was based on sending SMS codes to a phone number (said code can also be sent by phone call that would read the code out loud). Similar exploitations have been used to steal bitcoin from other users, all accounts "secured" with SMS based 2FA.[6]

Take Action

One way to increase security is to stop using SMS based 2FA. Other forms of 2FA are more effective, like authenticator apps, without being more of a hassle. Many users don't realize the difference between different types of 2FA, so there is no push to using more secure methods.

The best alternative to 2FA, or even better, another layer of security on top of 2FA is context-based authentication. There are many methods of context-based authentication, and individually they are not invincible, but layered together they increase account security. Notably, these methods are more about detecting anomalous events than preventing them, but detection allows us to catch specific events.

"The problem is that one-size-fits-all doesn't work, so going to a detection-vs.-prevention model is more likely to succeed in the long run." Marc Boroditsky, builds 2FA systems at Twilio [4]

Device registration and fingerprinting

The first time a device is used to log into the account, a fingerprint of the device is registered. Subsequent logins compare the current device's fingerprint to the registered devices to determine the authenticity of the user.

Fingerprint can consist of:[7]

- IP address
- web browser configuration
- language
- installed fonts
- browser plug-ins
- cookie settings
- screen resolution
- time zone

Geo-location

The location of the user's device is accessed to determine authenticity through a number of ways.

1. "Geo-velocity", or how far away are subsequent logins within a certain time period.[4] It's implausible that a user traveled from the East Coast to the West Coast in 30 minutes, so one of the logins is faulty.
2. Implausible remote access, if someone who normally logs in from one area is logging in from across the globe.[4]
3. Access is granted only to users in a certain radius, and anyone outside that radius is denied.[7]

The flaw with using geo-location to authenticate users is that a proxy or VPN will throw off the data. A user with a VPN may be denied access because their IP address shows them as somewhere they're not. Conversely, an attacker can use a VPN to "move" to a plausible location that will allow them access. Another weakness is that geo-location itself is a security flaw, and being able to access a device's location comes with risks.

Behavioral analysis

Normal user activity is recorded and abnormal activity is flagged as suspicious. These activities can include keystroke dynamics, mouse movements, gesture and touch, or motion patterns.[7] Behavior also includes average activity levels and which hours are spent logged in, or what data users normally access. According to the IS Decisions survey, 54% of organizations have implemented alerts on abnormal logon activity as part of their security.[1]

An inherent weakness with behavioral analysis is that some abnormal behavior is still legitimate. For example, a user that is normally online during the day could login in the middle of the night. This would be picked up as suspicious behavior and that user could be denied access, but it was really them. This sort of behavior data sometimes needs to be considered on a case by case basis, and this requires human eyes. Thus, behavioral analysis can take up more resources than whoever is providing the security can give.

Source IP reputation[7]

A user can be blocked if their IP address is on the record with a bad reputation. This involves creating a blacklist of IPs that are not allowed access, which is easily circumvented with proxies, and can never be fully exhaustive.

Conclusion

Overall, two-factor authentication is more secure than a password alone, but is not the grand solution to cyber security issues that is was hailed as. This is especially because a popular form of 2FA is sending codes over SMS, and this is easy for attackers to intercept. The problems with 2FA are not just with how it can be hacked, but also because people are not always going to

use it. It can be a hassle to implement and to deal with at each login. This is a relevant concern because the average user will put ease of use over security. There are alternatives to 2FA that are based on context, and when couple with 2FA they provide even more security. They each have weaknesses and can be circumvented, but are great when layered on top of one another.

References:

[1] “An alternative to complex, costly and disruptive multi-Factor authentication.” IS Decisions, 12 Sept. 2016, www.isdecisions.com/alternative-to-multi-factor-authentication/.

[2] de Borde, Duncan. “Two-factor authentication.” *Siemens Insight Consulting.* 12 Jan. 2012. https://web.archive.org/web/20120112172841/http://www.insight.co.uk/files/whitepapers/Two-factor%20authentication%20(White%20paper).pdf

[3] Team, Editorial. “Beyond Two-Factor Authentication: Minimizing Mobile Payments Fraud.” Finextra Research, Finextra, 16 June 2015, www.finextra.com/blogposting/11130/beyond-two-factor-authentication-minimizing-mobile-payments-fraud.

[4]Brandom, Russell. “Two-Factor authentication is a mess.” The Verge, The Verge, 10 July 2017, www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess.

[5] “Anatomy of a Hack.” TheVerge.com, 4 Mar. 2015, www.theverge.com/a/anatomy-of-a-hack.

[6] Brown, Cody. “How to lose $8k worth of bitcoin in 15 minutes with Verizon and Coinbase.Com.” Medium, Medium, 31 May 2017, medium.com/@CodyBrown/how-to-lose-8k-worth-of-bitcoin-in-15-minutes-with-verizon-and-coinbase-com-ba75fb8d0bac.

[7] “Moving Beyond 2-Factor Authentication With 'Context'.” Dark Reading, 5 Dec. 2014, www.darkreading.com/endpoint/authentication/moving-beyond-2-factor-authentication-with-context/a/d-id/1317911.