The Vulnerabilities of Two-Factor Authentication

Eddie Onsare

ICTN.4040 Term Paper

East Carolina University

Greenville, NC

Abstract - In efforts to secure user data, companies employ two-factor authentication to prevent accounts from unauthorized access. SMS based authentication is the most common and convenient method of authentication and is also the most vulnerable. This paper details and critically analyzes several exploits and vulnerabilities that have arisen since the popularization of the feature. Additionally, it will make recommendations for more secure two-factor authentication methods.

Keywords – 2FA, vulnerabilities, MFA, two-factor authentication, multi-factor authentication, security, U2F, SMS based

INTRODUCTION

Passwords by themselves are no longer a trustworthy token of authentication in this day and age. Enter two-factor authentication; a subset of multi-factor authentication which is the practice of having more than one token of authentication. Be it something you know, have or are, combining two or more of these factors of authentication provides more security than having only one would. “Two-factor authentication requires the prover to provide two distinct factors to the verifier… In two-factor authentication, the verifier won't accept a prover that provides only one factor; both must be provided.” [1] Although no authentication factor is flawless, with the utilization of multi-factor authentication an attacker would have to steal multiple tokens in order for your account to be compromised. If a password is something you know; time or event-based one-time passwords, application-based authentication, and SMS-based authentication methods would be modern day examples of something you have. Previously, companies used expensive, complex solutions such as hardware tokens that were nearly impossible for average consumers to use in securing their own personal accounts. However now that nearly everyone has access to a cellular phone, SMS based verification is the most widely used two-factor authentication method thanks to its convenience. Unfortunately, it also suffers from several security concerns since two-factor authentication does not secure you from certain attacks,

attackers can clone phones, text messages can be intercepted and phones themselves could easily get lost making it the least secure two-factor authentication method.

VULNERABILITY FACTORS

Users should be concerned and aware of the vulnerabilities SMS based authentication poses. Education is extremely important to the average consumer because when new security features such as the one in question start gaining traction people assume that it is foolproof and that as long as they have it they are protected. However, that is not the case as there are a plethora of factors that must be considered before one can ascertain whether or not SMS based authentication would help or harm you.

TYPE OF DEVICE AND TRANSMISSION PROTOCOL

One of the important factors as to whether SMS based two-factor authentication would be a secure option is the type of device you are using. This does not only apply to the operating system you are on; be it Android or Apple's iOS. But with the increase in demand for VoIP communication services companies and consumers must now consider the transmission protocol too as it can be difficult to know whether an SMS is being sent over a secure encrypted cellular network or not. Thinking about the type of device first, it is a well-known phenomenon that Apple operating systems are one for the most secure in the market and this is apparent when compared to Android operating systems. This is mainly due to the restrictive permissions enforced when installing applications on Apple's iOS. Fresh out of the box, Apple phones do not allow installation of applications that are not on the official App store; where applications put up by developers are well vetted to ensure the safety of iPhone users. Although this can be changed through a process known as jailbreaking; we will not consider that in our scenarios since people that do that are well aware of the associated risks. Instead, let us consider a non-jailbroken iPhone with all the latest updates. It would be extremely difficult for a user to mistakenly install some sort of malware on their device that would, for example, clone their phone or install screen capture malware that could be used to intercept or redirect the two-factor authentication code sent via SMS. On the other hand, the same cannot be said for Android systems which allow the user to turn off the setting that allows only official applications being installed making it inordinately simple for a user to mistakenly click on a link that will install a malicious application capable of intercepting a two-factor authentication code. A good example of a malware case that affected Android systems is the "Pincer Trojan, Android.Pincer.2.origin, which infects devices by masquerading as a security certificate and is capable of intercepting and forwarding inbound text messages." [2] This is

the sort of malware that leaves SMS based verification codes sent to Android phones susceptible to interception; ultimately making the two-factor authentication framework vulnerable.

Moving on, it would not matter what device you are on if the transmission protocol you are using is insecure. Thanks to the increase in phone bills US consumers pay year after year, demand for cheaper options have grown; most of which cost in the security department. VoIP has been popular ever since the invention of Skype and others alike; however, there are services that offer free phone numbers for you to send and receive SMS texts online through web applications as well as phone applications and as long as you have a Wi-Fi connection you can use this service. An example of the hundreds of websites that offer this service is Globfone which allows you to send text messages worldwide without registration or payments. A drawback to using such a service is the security and privacy that you give up since a free service such as this will not have the funds capable to securely manage a cellular network when compared to huge companies such as AT&T. Furthermore, for spam protection purposes, anyone can request a log of the text messages sent to and from one of these free numbers. Reasons such as these are why the National Institute of Standards and Technology (NIST), an organization responsible for recommending security best practices to the US government, recommended that the use SMS based verification be depreciated. The NIST Special Publication 800-63B Digital Authentication Guideline states that "if out-of-band verification is to be made using the PSTN (Public Switched Telephone Network), the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device." [3] Meaning that a telephone number must not be associated with a VoIP or other software-based service; but rather a physical mobile device. Since companies do not check where a message is being sent to, and it has become harder to assess whether an SMS message is being tunneled through insecure transmission protocols with varying levels of security or if it is, in fact, being sent over a secure encrypted cellular network users may be putting themselves at risk without knowledge of the fact.

TYPES OF ATTACKS

Although implementing two-factor authentication to secure your account gives u more piece of mind, there are certain attacks this technology is vulnerable against. This is unfortunate since two-factor authentication still does not protect you from attacks we are starting to see more often.

PHISHING ATTACKS

Two-factor authentication does not prevent or secure one from phishing attacks. We see news of servers being hacked and millions of emails and passwords being leaked extremely often. The average user thinks they are still

protected with two-factor authentication even though their password is compromised. Although this is supposed to be how it works; once an attacker has more information about you the ability to craft an attack specifically for you becomes much more feasible. This is known as phishing; where "the attacker creates a fake version of an existing webpage to fool an online user into elicit personal Information… it is the combination of social engineering and technical methods to convince the user to reveal their personal data." [4] Let us use the 2012 LinkedIn hack where the accounts of almost six and a half million users were hacked and leaked to the public as an example for our scenario. Let us assume two-factor authentication was enabled on one of the leaked LinkedIn accounts. The first thing an attacker would do is send a phishing email since they already know your address. This email might be in the form of a connection request as it is most likely to be clicked without second-guessing the sender. In Fig. 1. we can see a convincing phishing sample that is originating from an email with the domain linked.com as opposed to linkedin.com which can be easily missed by an unobservant user. If the email is well crafted, which they usually are, the user would gladly click the malicious link to accept the request which opens their browser and takes them to the LinkedIn website where they can enter their username and password after which the two-factor code will be sent to their phone for them to type in before they can access their account. While all this is going on the attacker would have an active terminal session harvesting all the data. After the user has successfully signed in the attacker will not only have their username and password, but will have obtained the session cookie. The session cookie which is present on a user's computer

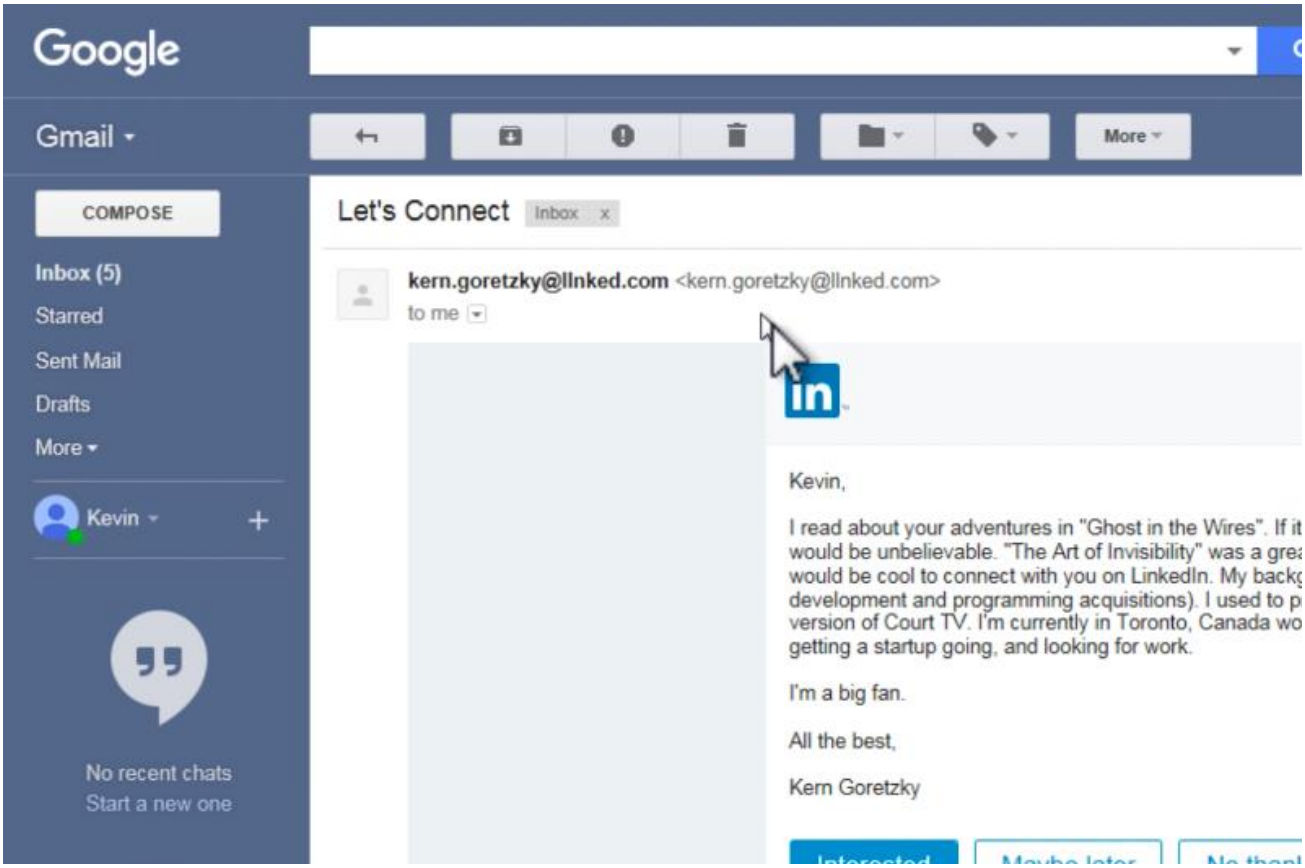

Fig. 1. Phishing email example
Kevin Mitnick, "New Exploit Hacks LinkedIn 2-Factor Authentication." YouTube, YouTube, 5 May 2018, URL: www.youtube.com/watch?v=xaOX8DS-Cto.

essentially identifies and verifies the user on the server-side as well. With this cookie, the attacker can load it into their own web browser and instantly have full access to an account. As we can see the two-factor verification code was not even relevant in this attack since an attacker can piggyback off the real authenticated user.

NUMBER PORTING

Number porting is another way an attacker can access your account even though you have two-factor authentication enabled. This method exploits actual procedure customers and cell phone providers undergo when a user wants to switch providers but keep the same number. “Porting a number to a new provider shuts off the phone of the original user, and forwards all calls to the new device. Once in control of the mobile number, thieves can request any second factor that is sent to the newly activated device, such as a one-time code sent via text message or an automated call that reads the one-time code aloud.” [5] To accomplish this, an attacker would call a customer service representative and either social engineer their way through getting the number ported or provide all the required personally identifiable information of the victim that may have been stolen using other methods. The information required to port a number usually includes the name of the previous service provider, the previous account number, name, address and Social Security number along with the phone number that is to be ported. Surprisingly, most of this information can be found on a victim’s phone bill. Once a number has successfully been ported it would not take long for an attacker to begin requesting the two-factor authentication codes and changing the passwords to those accounts; ultimately kicking the real user off completely while they wonder why they have no cellular service or cannot access their accounts.

RECOMMENDED TWO-FACTOR AUTHENTICATION METHODS

APP-BASED TWO-FACTOR AUTHENTICATION

Instead of having two-factor authentication codes sent via SMS; one can have them on an application on their smartphone ready to be used when the time comes. There are certainly some benefits of using this app-based system compared to an SMS-based system; however, it is still not a flawless method. The application-based system is not susceptible to number porting since it does not rely on the cellular network, and consequently it can work without any cellular service or internet connection. However, it relies heavily on a secret key that is entered during the initial setup and shared with the server. This along with the time is then used to generate a random code that can be used as a second authentication factor. The drawback is “if a crook can crack the app or the server and recover the secret, they can clone your 2FA codes indefinitely.” [6] Another drawback is that the authenticator applications run on the same smartphone one may use on a daily basis and can mistakenly install a malicious application capable of reading

data from your authenticator and relaying it to an attacker. If security is extremely important one could consider purchasing another cheaper smart-phone that can be used solely for authentication; preferably an iPhone, this minimizes the risk of amassing any sort of malicious application.

UNIVERSAL 2ND FACTOR KEYS

The most secure two-factor authentication method available today is the Universal 2nd Factor key (U2F). U2F keys rely on Near Field Communication (NFC) or Universal Serial Bus (USB) standards to work. It is fairly simple to use; during the initial setup, the U2F key will generate a random number known as a nonce. The key is hashed with the website domain to create a code that is unique to one's account. Subsequently, to sign in "the user presents the second factor by simply pressing a button on a USB device or tapping over NFC." [7] The use of U2F keys is supported across several web browsers including Google Chrome, Opera, and Firefox as well as websites such as Facebook, Dropbox and GitHub. There are several drawbacks to this method too; starting from the cost. If one chooses the USB route, it would be ideal to purchase two or more keys, in case one gets lost, which could cost around $15 to $50 each. Secondly, this method of authentication is not as widely accepted as others such as SMS based authentication.

CONCLUSION

After covering the different ways an attacker could get into your account when utilizing the SMS-based two-factor authentication method; these vulnerabilities should serve as a reminder to use something other than SMS based two-factor authentication whenever possible. Users should understand that multi-factor authentication will always be better than one-factor authentication; but that it is not a replacement for good passwords and good password security. Additionally, it would be difficult to use two-factor authentication on every single system as it would require a tremendous amount of patience and the willingness to put up with the inconveniences such as, making sure you always have your phone or USB key on you at all times and understanding that they could get lost and ultimately lock you out of your own account. The app-based alternative is still not infallible in any way but is much more difficult for attackers to intercept; the likelihood of authenticator servers being hacked still needs to be assessed in depth to fully determine the security of this method. Users can use the most secure options on the most important accounts and vice versa but always use two-factor authentication whenever they can.

REFERENCES

1. Dimitri DeFigueiredo, “The Case for Mobile Two-Factor Authentication,” in IEEE Security & Privacy, vol. 9, no. 5, pp. 81-85, Sept.-Oct. 2011. doi: 10.1109/MSP.2011. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6029364&isnumber=6029351

2. Michael Cobb, “Do two-factor authentication vulnerabilities outweigh the benefits?”, unpublished. URL: https://searchsecurity.techtarget.com/answer/Do-two-factor-authentication-vulnerabilities-outweigh-the-benefits

3. Paul A. Grassi, James L. Fenton, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, William E. Burr, Justin P. Richer, “NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management.” URL: https://doi.org/10.6028/NIST.SP.800-63b

4. S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 537-540. doi: 10.1109/CCAA.2016.7813778.* URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7813778&isnumber=7813678

5. Brian Krebs, “How to Fight Mobile Number Port-out Scams”, unpublished. URL: https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/

6. Maria Varmazis, “SMS or authenticator app – which is better for two-factor authentication?”, unpublished. URL: https://nakedsecurity.sophos.com/2016/08/12/sms-or-authenticator-app-which-is-better-for-two-factor-authentication/

7. Kai Fan, Hui Li, Wei Jiang, Chengsheng Xiao, Yintang Yang, “Secure Authentication Protocol for Mobile Payment” in Tsinghua Science and Technology, vol. 23, no. 5, pp 610 - 620, Oct. 2018. doi 10.26599/TST.2018.9010031.* URL: https://ieeexplore.ieee.org/document/8450873