ISSN 2320 - 2602
Volume 13 No. 10, October 2024
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst0113102024.pdf
https://doi.org/10.30534/ijacst/2024/0113102024

Attacks against Multi-factor Authentication

Anastasios Liveretos[1], Prof. Milena Lazarova[2]
[1]Techical University of Sofia, Bulgaria, Anastasis.liveretos@cchellenic.com
[2]Technical University of Sofia, Bulgaria, milaz@tu-sofia.bg

Received Date : August 28 , 2024 Accepted Date : September 29, 2024 Published Date : October 07, 2024

ABSTRACT

There is no such thing as bulletproof authentication, and multi-factor authentication (MFA) is not bulletproof either. There are attacks against MFA. In this paper, we not only present a historical outline of the most significant MFA attacks but also review the available taxonomy tools. Our aim is to equip enterprises with a clear understanding of how MFA attacks may occur and how these are classified. More importantly, we provide proactive considerations on how MFA attacks may be prevented, empowering enterprises to take action.

Key words: Access management, identity management, multifactor authentication, multifactor authentication taxonomy

1. INTRODUCTION

In 2012, a significant event shook the European banking sector-the emergence of the Eurograbber banking Trojan [1]. This attack, which began with banking malware, escalated after the attackers compromised user IDs and passwords. They then sent a link via an SMS message to the victim, purportedly for device protection. However, clicking on the link led to the installation of mobile malware, capable of stealing the second factor, SMS-delivered OTPs. This allowed the attacker to gain control over both factors, potentially causing significant financial losses and reputational damage.

In 2017, a similar attack against German banking institutions took place [2]. The first factor was compromised using malware, and the second factor was compromised using Signaling System 7. This is the underlying infrastructure behind all mobile message and call delivery. It was a rather old system with several security gaps. The attackers were able to contact a rogue mobile network operator, and mobile network operators in the system could access each other's databases and change information there, including routing information. Consequently, the attackers could change routing information and route those SMS-delivered OTPs to themselves.

In 2021, the advent of OTP interception bots, essentially automation of attacks, came up. These OTP interception bots automated the following process: the attacker compromises somebody's first credentials, such as their password, and then they reach out to their victim and tell them they called on their bank's behalf [3]. They then ask their victim to provide the next value generated by Google Authenticator, attributing it to security purposes. Their system is compromised once users respond positively to this and give out the value.

In 2022, the Lapsus$ hacking group perpetrated the infamous attack against Uber [4]. This bold, innovative group allegedly comprised primarily of teenage hackers. This was an MFA fatigue attack. It was a push bombing attack. Essentially, they inundated the victim with push notification messages. The victim was too slow to respond, so they contacted them through another channel and said this was normal. All they needed the victim to do was to push the accept button. Most victims complied, therefore creating an MFA session for the attacker.

In 2022, one of a series of attacks against identity security company Okta also took place [5]. This was an attack against the support staff at Okta. The attackers compromised passwords out of the band. Then, they learned that Okta uses Twilio as a delivery service for SMS-delivered OTPs and that Twilio logs every OTP value. Thus, administrative accounts at Twilio were compromised, and access was gained to administrative consoles and those OTP values. This brought into attackers possession both factors.

In 2023, a new version of a well-known adversary-in-the-middle tool called Evilginx was deployed [6]. Adversary-in-the-middle tools support stealing user IDs, passwords, OTPs, and session cookies.

This paper presents the currently available taxonomy tools for categorizing the different kinds of MFA attacks and suggests ways for enterprises to protect themselves against this threat.

2. TAXONOMY TOOLS

Attacks against multi-factor authentication are on the rise, and attackers always find weak spots in the authentication flows and infrastructures. There is a need to build a taxonomy

of MFA so it can be protected in an organized way. Currently, there's no single taxonomy.

2.1 Verizon's Data Breach Investigations Report Taxonomy

One MFA taxonomy comes from Verizon's Data Breach Investigations Report (DBIR) for 2023 [7]. They have seven categories of threat actions or attack vectors: Social, Hacking, Malware, Misuse, Physical, Error, and Environmental. Several MFA attacks can easily map to those categories.

- Social attacks are relatively common. Phishing, smishing, vishing, and MFA fatigue attacks fall into this category.
- The signaling system 7, referred to above, falls under hacking.
- Several attacks mentioned above are malware-based.
- Misuse is anything related to the misuse of resources for sensitive purposes. So, anything related to compromised administrative accounts or insider threats falls into this category.
- Physical attacks involve the physical environment, such as physical authenticators. The BBC published an example a couple of years ago. Several gym-goers in London were deprived of their credit cards and smartphones. Therefore, both credentials were essentially stolen. The idea behind this was that the attacker wanted to register their mobile app, the banking app, on their mobile device, but they wanted it to be attached to the victim's credit card. To do that, they had to complete second-factor authentication using SMSDelivery.tp, which flashes on the victim's device. They didn't know how to unlock the device but held it long enough to see that flashing value and complete authentication to enroll their mobile device.
- Errors are related to misconfiguration. A recent example is an advisory published by the United States Cybersecurity and Incident Security Agency that discussed a particular agency attacked through misconfiguration. In that specific situation, they configured their multi-factor authentication to fail-open. Once the multi-factor authentication server could not be reached, the system pretended that everything was okay and allowed the user to log in just with a password. The attacker did precisely this. First, they compromised the password. Then, they modified the client configuration to say that the multi-factor authentication service was running on the local host, which it was not. Finally, as the multi-factor authentication failed, they were able to get in completely bypassing MFA.
- So far, no clear indication of an environmentally driven MFA compromise exists. Still, natural disasters causing infrastructure or communication malfunctions could fall into this category.

2.2 MITRE ATT&CK Taxonomy

Another taxonomy is the “Credential Access” pilar from the MITRE ATT&CK framework [8]. Credential Access involves 17 techniques for stealing credentials, like account names and passwords. Techniques used to get credentials include:

1. Adversary-in-the-middle: Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access).
2. Brute force: Password guessing involving a systematic repetitive or iterative mechanism.
3. Credentials from Password stores: Identification of common password storage locations, such as Keychain, Securityd Memory, Web Browsers, Windows, Password Managers or Coud secrets management stores.
4. Exploitation for Credential Access.
5. Forced Authentication.
6. Forced Web Credentials through cookies or SAML tokens.
7. Input capture includes keylogging, GUI input, web portal capture, and credentials API hooking.
8. Modify the Authentication process. This technique includes MFA, Network Device authentication, Reversible encryption, and Hybrid Identity.
9. MFA Interception. In 2020, during the SolarWinds incident, the attacker compromised their victim's ADFS servers, took hold of the private key used to sign SAML assertions, and was able to sign arbitrary assertions that eventually were sent to Azure AD. The assertion included the subject they like and the account they want to compromise. They also included multi-factor authentication claims. When the token reached Azure AD, and the organization had some Azure AD conditional access policies requiring MFA, they performed quote-unquote MFA; therefore, no MFA was needed.
10. MFA Request Generation.
11. Network Sniffing. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network or use span ports to capture more data.
12. OS Credential dumping.
13. Steal Application Access Token.
14. Steal or Forge Authentication Certificates.
15. Steal or Forge Kerberos Tickets. Obtain access to a golden or silver ticket in an Active Directory environment.
16. Steal Web Session Cookies
17. Unsecured Credentials.

One concern with this framework is that it's based on public disclosure. Subsequently, there's a gap between when an attack is discovered and when this particular attack or technique enters this framework.

2.3 Roger Grimes’ Hacking Multifactor Authentication Taxonomy

Everything starts with the user because everything we do is to protect users against account takeover attacks. Users are also a component of the infrastructure. A social engineering

attack can compromise the user and the whole MFA flow (see Figure 1).

Devices and hardware are very relevant to conversations about multi-factor authentication. Devices are subdivided into three categories for authentication: Endpoint, Companion, and Dedicated.

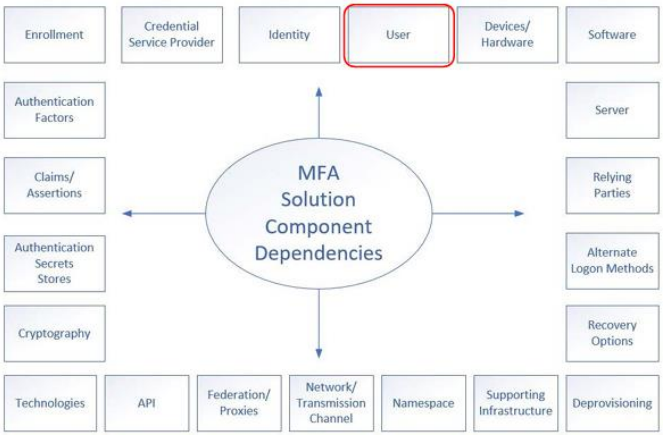

Figure 1: Hacking Multi-Factor Authentication, Roger Grimes [9]

An endpoint device is the device from which the user authenticates or logs in. A companion device is a general-purpose computing device, such as a smartphone, used to complete authentication. Finally, a dedicated device is a hardware token used to complete authentication.

All components and communication amongst them must be secured as required. An example from the SolarWinds incident is very relevant [10]. In that incident, organizations were running Outlook WebX and Outlook Web Access. Those installations were configured to use Duo for multi-factor authentication. The attackers were able to compromise those Duo installations. They stole API keys that Duo typically uses to connect to the Duo cloud service to complete authentication. It also happened that those API keys were used to encrypt local cookies, telling the relying party that multi-factor authentication had occurred. Once these were attacked and compromised, there was no further need to perform MFA. The cookie was presented, and the underlying system concluded that MFA had occurred.

Multi-factor authentication implementations increasingly use infrastructure that is not under the organization's immediate control. SMS delivery is one component. "Bring your own device" and authentication using mobile apps and passkeys are other relevant examples. It is difficult to evaluate those pieces of the infrastructure on which there is no control. On the other hand, one should make certain security decisions about this. It should be adequate to accept that, for example, Apple's infrastructure sufficiently secures passkeys, so using this technology with this device is safe.

This is an extensive model. Yet, one may argue that it takes a static view of MFA. In other words, it doesn't discuss vectors, the dynamic components, or how a particular threat affects things.

2.4 Trust Scale alternatives

All three models may be combined to create a more complete picture for a multi-factor authentication deployment. Introducing a trust scale is a good tool for evaluating the part of the model to be used. Depending on the criticality of the application and the trust level required, different authentication methods may be selected, such as:

1. Very Low Trust: Passwords
2. Low Trust: Desktop, Voice, SMS OTPs
3. Medium Trust: Mobile OTP and Push notifications
4. High: FIDO2 Platform Authenticator, security key, and software roaming
5. Very High: X.509 Hardware token

Furthermore, there is always the option to take a particular authentication method that is generally relatively insecure and implement additional mitigating controls to make it more secure. For example, using number and location matching together increases the protection against brute force for push-bombing attacks.

Different mechanisms exist, which are more fine-grained than this trust scale supports. Based on this risk picture, a decision must be made whether a request is accepted, denied, or even accepted with the simultaneous implementation of a mitigating action.

3. FUTURE CONSIDERATIONS

Many years ago, the initial model was to perform all this before the session started. Look at the credentials, look at the contextual information, and then make a risk evaluation decision.

Then, step-up authentication was introduced. At discrete points in a session, a risk evaluation is performed, and the user requiring additional authentication is stepped up.

Nowadays, we have moved to continuous adaptive trust. The risk is evaluated on every request and even during the same session. The user's device might have gone out of compliance, or the user might have reset their credentials. Maybe they moved the cookie, or somebody else stole it, and it's now running on a completely different device. In such cases, passive behavioral biometrics can be used to determine if the same user is using this cookie.

Implement robust credential management. Ideally, robust end-to-end security needs to be implemented. If the account recovery or the credential enrollment process is very weak, enrolling in a very strong credential is irrelevant. The attacker will move the attack to a different stage.

MFA works with an additional authentication factor. To register one device, another device is used. Although

theoretically, this could work, for most organizations, it doesn't. Most organizations do not want to invest in providing multiple authentication factors for their users, so they look for alternatives.

One of the alternatives is identity proofing or authentication by other means. The most popular way to do identity proofing is document-centric identity proofing. A document issued by a government, such as a driver's license, is presented, followed by a selfie. This completes the authentication. Solutions like this are few and far between. For example, Onfido, recently acquired by Entrust, has a solution for Okta [11]. Okta had other ways to recover accounts, such as identity verification. A third-party vendor stepped in and provided this capability.

Still, if identity proofing is considered too cumbersome and expensive, identity attestation might be the best way around it. The difference between identity attestation and identity verification is that there is no identity-binding step. In other words, there is proof that this identity exists, but not necessarily proof that this identity relates to a specific person. For example, a passwordless company called Trusona allows drivers to register their licenses [12]. There's no selfie, but when account recovery is needed, the driver is requested to present their driver's license to the camera, and then they are allowed in.

Another approach is to use risk and recognition signals or contextual information during registration. Okta, Microsoft Entra ID [13], and others support this setup. When users want to register for a second credential, they are required, for example, to be present on the corporate network or on the corporate VPN.

Finally, the last one is MFA passcodes or bypass codes. When all other options to authenticate are exhausted, a bypass code, as a last resort, can guarantee access for a limited number of days.

However, all these approaches create a dependency that is not supposed to be in multi-factor authentication. The original formula, something you know, something you have, and something you are, was invented to ensure that factors are completely separate. If the attacker compromises one of the factors, they cannot compromise the whole system. They don't get any leg up in compromising the second factor. This cross-pollination between passwords and other authentication factors is not an easy problem to solve. Nevertheless, organizations should consider it, evaluate identity threat detection, and respond accordingly.

In addition to detection and response, thought and effort must be invested in prevention or identity security posture management. When selecting a tool, specific prerequisites, such as MFA configuration, policies, and coverage, need to be satisfied. This can be an attack-based disruption or incident investigation after the fact. These tools typically integrate with the Security Information and Event Management (SIEM) and increasingly with extended detection and response tools.

New processes can also cover the gaps tools leave behind them. Such processes could be penetration testing, threat modeling, application testing, and application integration with multi-factor authentication. For example, OWASP [14], an open web application security project, guides how to integrate multi-factor authentication into applications and how to test that the configuration and integration are correct [14].

Finally, third-party assessments can support mitigating risks. Companies like KnowB4 provide a report showing all possible weaknesses in the MFA implementation [15].

4. CONCLUSION

This paper highlights the importance of understanding and addressing the various attacks against Multi-Factor Authentication (MFA). It emphasizes that while MFA is a crucial security measure, it is not foolproof and can be vulnerable to different types of attacks. The document provides a historical outline of significant MFA attacks and reviews available taxonomy tools to classify these attacks. It also suggests ways for enterprises to protect themselves against MFA attacks, including robust credential management, identity proofing, and using risk and recognition signals.

REFERENCES

[1] E. Kalige, D. Burkey, **A Case Study of Eurograbber: How 36 Million Euros Was Stolen Via Malware**, Versafe.

[2] **SS7 Vulnerabilities And Attack Exposure Report**, Positive Technologies, 2018, available at https://www.gsma.com/get-involved/gsma-membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf

[3] K. Spaeth, **OTP Bots and Crypto: A Tactic to Disrupt**, Cyber Security: A Peer-Reviewed Journal, Henry Stewart Publications, Vol. 6, No. 3, pp. 275-284, 2023.

[4] M. Conklin, B. Elzweig, L.J. Trautman, **Legal Recourse for Victims of Blockchain and Cyber Breach Attacks**, UC Davis Business Law Journal, Vol. 23, pp. 134-180, 2023.

[5] B. Winterford, **The Human Factor in Phishing Resistance**, Octa Security, available at https://sec.okta.com/articles/2022/10/human-factor-phishing-resistance.

[6] S. Mishra, S. Mishra, Y. C. Toh, S. Mishra, P. T. Vi, **Mitigating the Threat of Multi-Factor Authentication (MFA) Bypass Through Man-in-the-Middle Attacks Using EvilGinx2**, in the book "Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society" (Editors: A. Bijalwan, R. Bennett, G. B Jyotsna, S. N. Mohanty), Scrivener Publishing LLC, Chapter 5, pp.59-78, 2024.

[7] **2024 Data Breach Investigations Report**, available at https://www.verizon.com/business/en-nl/resources/reports/dbir.

[8] **Credential Access**, MITRE ATT&CK, available at https://attack.mitre.org/mitigations/M1043.

[9] R. Grimes, Hacking Multifactor Authentication, John Wiley & Sons, 2021.

[10] R. Alkhadra, J. Abuzaid, M. AlShammari, N. Mohammad, **Solar Winds Hack: In-Depth Analysis And Countermeasures**, 2021 IEEE 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1-7, 2021.

[11] P. Jarratt, **Simplifying Digital Access Across Okta's Single Sign-On Ecosystem**, 2022, available at https://onfido.com/press-release/simplifying-digital-access-across-okta-s-single-sign-on-ecosystem.

[12] **Trusona Authentication Cloud**, Trusona, available at https://www.trusona.com/customers/authentication-cloud.

[13] **Microsoft Entra ID**, Micsrosoft, available at https://learn.microsoft.com/en-us/entra/identity.

[14] **OWASP**, available at https://owasp.org.

[15] R. Grimes, **Hacking Multifactor Authentication: An IT Pro's Lessons Learned After Testing 150 MFA Products**, KNOWBE4, available at https://www.knowbe4.com/hubfs/HackingMFA_150Tests_Slides.pdf