Unveiling Multi-Factor and Risk-Based Authentication: Critiques and Pathways Forward*

Shivani P. Thakur[1] and Saurabh S. Mishra[1]

International Institute of Information Technology Prof. C R Rao Road Gachibowli,
Hyderabad 500 032 Telangana, INDIA
http://www.iiit.ac.in

Abstract. This research paper embarks on a detailed exploration of the adoption and effectiveness of Multi-Factor Authentication (MFA) and Risk-Based Authentication (RBA) across 208 prominent websites, juxtaposing these advanced security measures against the traditional password-based authentication (PBA) to illuminate the landscape of current authentication practices and pinpoint areas ripe for improvement. Through a rigorous methodology that involves manual account setups and thorough inspections, the study confronts the challenges of detecting RBA and MFA, hindered by sparse documentation and the intrinsic limitations of directly managing RBA. The findings reveal a stark predominance of PBA, with only 42.3% and 22.1% of sites supporting MFA and RBA, respectively, underscoring a significant shortfall in the adoption of robust authentication mechanisms. The investigation further highlights the crucial role of Single-Sign-On (SSO) providers in broadening the implementation of RBA and MFA, albeit at the potential expense of user privacy due to the tracking capabilities of these providers. Critical examination of the study's assumptions and methodological choices points to potential oversights, such as the insufficient consideration of silent security measures and the static analysis approach to dynamic RBA systems, which may have led to an underestimation of these technologies' presence. In response, the paper advocates for an expanded research agenda that encompasses a wider array of account types, delves deeper into technical analyses, prioritizes user experience, and scrutinizes the privacy implications of SSO services. This comprehensive set of recommendations aims to pave the way for more nuanced, secure, and user-friendly authentication strategies in the digital domain, striving for a balance between robust security measures and the preservation of user privacy.

Keywords: Multi-Factor Authentication (MFA) · Risk-Based Authentication (RBA) · Single Sign-On (SSO) · Password-Based Authentication (PBA) · Online Security Protocols · User Privacy · Authentication Techniques · Cybersecurity Measures

* Supported by organization IIIT Hyderabad

1 Summary of the paper

1.1 Introduction

Securing user accounts from attackers is important. Every user wishes to protect their information. The paper emphasizes that despite being insecure and susceptible to attacks, password-based Authentication (PBA) is a popular means of authenticating users. This paper examines 208 websites from the Tranco top 5k list with the aim of investing the availability of other more secure and effective authentication methods such as MFA and RBA. MFA usually requires the user to prove their identity more than once, mostly by means of a one-time password sent to the user's device or email. Whereas RBA authenticates the user based on various parameters such as how and where you are logging in from. It was found out after conducting the study that MFA and RBA are not used predominantly by many sites.

Though most of the sites did not support MFA and/or RBA, many of the websites support SSO login. The SSO providers offer these features to the users. But most SSO providers track user activity.

The key points of the paper are as follows:

- It is by far the broadest study conducted on the availability and features of MFA and RBA on the web. - MFA and RBA adoption is still low despite being more secure. - MFA/RBA do not actively stop malicious login attempts but notify the user. - Most of the sites provide SSO login which in turn provides MFA and/or RBA, but SSO providers are third party trackers which might capture user activity.

To summarize, the paper analyzes the availability of RBA and MFA among 208 sites from Tranco top 5k list. It was concluded that despite being more secure than PBA, RBA and MFA are not used extensively.

1.2 Methodology

The paper also highlights the detailed approach followed to conduct the large-scale availability testing of MFA and RFA across different sites. The study relied on manual account setup and inspection due to the challenges of inadequate documentation on MFA and RBA and the inability of directly managing RBA. Since the efficacy of RBA could only be confirmed by its handling of erroneous login attempts, this procedure was essential for precisely determining the existence of these authentication mechanisms.

A number of well-known websites that facilitate account creation, together with the Single-Sign-On (SSO) providers for each, were selected in order to conduct the study. Notwithstanding roadblocks such as CAPTCHAs, a tool was created to expedite the login procedure, enabling the necessary black-box testing for RBA. Suspicious logins were created for RBA testing by altering some aspects of the account creation process. This showed that only logging in several times was enough to trigger RBA safeguards. Sites lacking RBA answers were contacted to verify findings and learn about their security protocols. The study categorised sites according to how they responded to these tests.

1.3 Scope and Limitations

One of the study's intrinsic limitations is that it can only verify whether RBA is present—not whether it is absent. This is because of things like the possibility that certain websites would permit RBA under particular circumstances, which could result in underreporting. Furthermore, the study concentrates on the availability of these authentication techniques rather than delving into the specifics of RBA models or other login defences like rate limitation. Despite being the largest study of its kind, the results might not accurately reflect the security environment of the whole internet due to the focus on well-known websites, especially in areas like mobile apps, IoT devices, and online banking. As a result, it is best to interpret the results as a conservative estimation of MFA and RBA's online visibility.

1.4 Results

It was discovered that all 208 websites in the survey depended on password-based authentication (PBA). Merely 42.3% of them endorsed multi-factor authentication, indicating a notable deficiency in user account security compared to PBA. Additionally, the analysis showed that sites with higher Tranco list popularity were also more likely to endorse MFA, with MFA support declining as site popularity declined.

Only 22.1% of the sites used RBA, which suggests a poor acceptance rate. Top-ranking sites were more likely to have RBA, and some site categories—such as Social Networking and Finance/Banking—showed a greater propensity to use both MFA and RBA. It's interesting to see that several sites used RBA but not MFA, indicating potential for improved security protocols.

The report emphasized how important Single-Sign-On (SSO) providers are to expanding MFA and RBA's reach. It was discovered that 80.29% of sites could employ RBA through their SSO providers, and 77.40% could enable MFA, which would drastically change the user authentication security landscape. But almost every SSO supplier that provides these security capabilities is also a big third-party tracker, indicating that there is a trade-off between increased security and privacy for the user. This thorough analysis shows how different websites employ MFA and RBA, how site popularity and category affect security procedures, and how SSO providers significantly increase authentication security at the expense of privacy.

2 Major Critiques on Assumptions, Technical Approach, Analysis, and Results

2.1 Assumptions and Methodological Gaps

Limited Detection Techniques The study might have misunderstood when it thought that not seeing Risk-Based Authentication (RBA) and Multi-Factor Authentication (MFA) meant they weren't there at all. This misunderstanding could happen if the study only looked at what's easy to see on websites or did simple tests. Sometimes, security steps work quietly in the background, or websites use different ways to check who's trying to log in. For instance, some websites might add extra security checks after a few wrong password attempts, but you wouldn't know that just by looking quickly or testing in basic ways. Wiefling and colleagues in 2019 talk about how RBA adapts to different situations by noticing things like what device you're using or where you are without making it obvious[2]. This is important because it shows us there's a lot going on with website security that we might not see right away. It tells us we need to look closely at how websites keep things safe, thinking about both the security steps we can see and those we can't.

Analysis of Dynamic RBA Statically Risk-Based Authentication (RBA) changes security based on what it thinks is happening or how users act. But, if researchers only look at it in simple tests, they might not see how well it really works. RBA is smart and looks at lots of things like where you are, what device you're using, and how you use a service. Just testing it once might not show how good RBA is at keeping things safe. Wiefling and his team in 2019 found that RBA can make passwords safer by checking extra stuff, like where you are or what device you're on. This helps protect against common attacks like someone trying to guess your password[2]. Then, in 2020, Wiefling, Patil, Dürmuth, and Lo Iacono looked at different ways to check who you are on RBA. They found ways to make these checks better without making things less safe or harder for users[3].

2.2 Technical Approach

Focus on Specific Account Types The study might have not covered the stronger security steps that some special accounts use. These accounts, like those for companies, app developers, or really important people, have access to more sensitive stuff. So, they use better protection methods to keep their info safe from hackers. This includes checking things more carefully if something seems off, or using several security methods at once to make sure the person trying to get in is supposed to be there. The papers "Modern Authentication Methods: A Comprehensive Survey"[5] and another detailed study on authentication techniques talk about these kinds of extra security measures, showing us how some accounts are like super-secure vaults, not just regular locks.

Limitations on RBA Black-Box Testing Using only black-box testing to check how well Risk-Based Authentication (RBA) works might not show us everything. This kind of testing looks at what happens on the outside when we use RBA, but it doesn't show what's happening inside. For example, Wiefling, Lo Iacono, and Dürmuth in 2019 talked about how RBA helps make passwords safer by looking at extra information like where you are or what device you're using. This helps stop hackers but is hard to see with just black-box testing. Then, Wiefling, Patil, Dürmuth, and Lo Iacono in 2020 studied different ways to make RBA even better, like using links or special codes in emails to check who you are. Their work shows that RBA can be very smart in protecting us, but we might not see all its smart moves with simple tests[2, 3].

SSO Provider Analysis Scope When we study how single sign-on (SSO) providers work, we often look at the big names and might miss out on many other options. Focusing on the big companies can leave out the smaller, unique solutions that are really important for certain groups or industries. For example, a study by Mir, Roland, and Mayrhofer in 2022 talks about a new way to do SSO that's more private and doesn't rely on one big company to handle everything. This shows there are different, possibly better ways to handle sign-ins that the big picture might not show[8].

2.3 Analysis

Unexplored MFA Factor Strengths The study we talked about didn't look closely at how different ways of checking who someone is (like using a code sent to your phone, scanning your fingerprint, or using a special key) are good or bad in terms of keeping things safe and being easy to use. For example, getting a code on your phone is easy but not very safe because others can get this code too. But using your fingerprint or a special key is safer, although it might be harder to use. The paper points out that not looking at these differences can make us think too simply about how these security checks work. It misses out on showing how each method has its own good and bad points in stopping different kinds of online attacks[1].

Inadequate focus on Post-Login Security When we just focus on making sure logins are safe, we might forget to keep an eye on what happens after someone logs into their account. It's really important to keep checking to make sure the person using the account is still the right person and not someone who shouldn't be there. For example, a 2022 study by Papathanasaki, Maglaras, and Ayres mentioned that security shouldn't stop working after you log in[5]. They suggest watching how the account is used and making sure everything looks right, kind of like having a security guard who keeps watching all the time, not just when you enter. Another paper talks about using different ways to check on an account's security even after login, like watching the account's activities or making sure transactions are legit[6]. This means not only worrying about the door's lock but also keeping an eye on everything happening inside the room, making sure everything stays safe the whole time you're there.

Nuanced Privacy Implications of SSO Use The papers we looked at talk about privacy worries when using Single Sign-On (SSO) services, but they don't go deep into the issue. It's really important to think more about how these services make logging in easier but also need to keep user information safe. For example, one paper shares a new way to do SSO that keeps user privacy better by not letting the service that checks your login watch what you do all the time[8]. Another paper points out that we need to understand better how SSO can be both helpful and risky for privacy. This way, SSO can help us log in easily without giving away too much about ourselves[9]. This shows we need to think more about keeping our information safe while enjoying the convenience of quick logins.

2.4 Result

Limited Generalizability If we only look at popular websites to learn about how they check if someone is really who they say they are, we might miss out on a lot of other ways different types of services do this. Big websites might do things one way, but smaller websites or those in special areas might have their own unique methods. By not looking at these, we could end up with a too simple idea that doesn't fit everyone's needs or how they keep things safe.

Stand-Alone RBA Analysis Looking into services that only use Risk-Based Authentication (RBA) without Multi-Factor Authentication (MFA) shows some big security worries. RBA can change its security based on the risk it sees, but this might not be enough to keep everything safe on its own. One of the papers talks about how RBA can adapt and change depending on what dangers it might find, which is a good thing. But, it also says that just using RBA by itself might not stop all types of cyber attacks[2]. Another paper points out that it's really important to use more than one way to check if someone is who they say they are. This means that while RBA is helpful, without adding in the extra checks that MFA provides, there might be some security risks that RBA can't handle alone[3]. This makes it clear that RBA has its strengths, but for the best protection, it's better to use it with other security methods like MFA[4].

Every suggestion points out that we need a better way to look at how safe web services are. They say we should use methods that really understand how modern ways of checking who someone is can change and get complicated. To get a fuller and more true picture of how well these security checks work right now, future studies should try to cover more ways of testing, different kinds of user accounts, and various types of services.

3 Suggestions for Improvements/Extensions

3.1 Broadening the Study Scope

- Expanding the study to look at different types of accounts, like those for businesses, developers, VIPs, or kids, can help us find better ways to keep these accounts safe. By creating tests that act like these different accounts and see how they use the website, we can discover special security steps that work best for each kind of user. This approach helps us understand how to protect everyone on the platform better.

- The feedback about studying Single Sign-On (SSO) services tells us we need to look at more kinds of SSO, not just the big names. It's important to include SSO services that focus on special areas or certain kinds of users. This would help us understand how SSO works for different websites and for people with different needs. For example, a study talks about a new way to do SSO that's safer and doesn't keep track of user info, which could be really good for smaller, privacy-focused services[8].

  Also, asking people from different groups about what they think of SSO services can give us more insights. This way, we can learn how different kinds of users choose and use SSO services, helping us make SSO better for everyone. This idea matches what another paper might say about looking closely at what users need and how they interact with SSO services to make them work better for various types of users[9].

- When we look into how websites check who you are (this is called multi-factor authentication, or MFA), it's good to sort these checks by type: something you know (like a password), something you have (like a phone), or something you are (like your fingerprint). Each type has its own risks, such as someone copying your fingerprint or intercepting a code sent to your phone. The paper "Multi-Factor Authentication: A Survey" by Ometov et al. highlights the evolution of authentication systems towards MFA from simpler forms like Single-Factor Authentication (SFA) and emphasizes the importance of considering the unique challenges and user experience aspects of different MFA methods. This study suggests that by understanding what users like and what stops them from using these security methods, we can make them better and safer for everyone[1].

- Looking into security after someone logs in, like checking what they do on the site or making sure their transactions are safe, is really important. This helps us see if the website keeps user data safe after they log in, by watching for any unusual activities and checking transactions for anything suspicious. The research in " Modern Authentication Methods: A Comprehensive Survey " paper talks about how we need to use many ways to check who someone is (this is called multi-factor authentication) and keep an eye on them even after they log in. This makes sure that the website is safe not just at the door, but inside too [5].

3.2 Deeper Technical Analysis

- Looking into different ways to figure out how websites check if you are who you say you are can really help make things safer online. Sometimes, just using computer programs to check everything might not catch the small, special details. It's also a good idea to manually look at what security steps a website uses by reading their help guides or checking their coding if you can. Talking directly to the people who run websites can also tell us a lot about security steps that aren't obvious just by looking. Plus, using smart computer programs to notice unusual patterns or ways of checking can help find unique security methods that aren't common.

  Research by Wiefling, Lo Iacono, and Dürmuth looked into how some websites keep checking who you are after you log in to keep things safe. This shows why it's important to use different methods to understand security better[2]. Another study they did looked at how these security checks work in real life across different websites. They tried to figure out what makes these checks really work and how they help keep accounts safe[3]. This tells us it's really important to mix and match different ways of checking to really get how secure a website is.

- To really get how well Risk-Based Authentication (RBA) works, it's important to test it like it happens in real life. This means looking at what happens when people do usual things, like using the same computer from the same place, and also when they do something different, like logging in from a new place or with a new phone. By making these tests run on their own for a while, we can collect lots of information on how RBA reacts to different situations. This helps us see how well RBA can spot and react to possible security problems based on what users do.

  The papers we looked at talk about how RBA can change its security levels by noticing different things about how users log in. This could help stop hackers from getting into people's accounts by guessing passwords or using stolen ones [2, 3]. One study even checked out how RBA works when people have to prove who they are again to keep their accounts safe, showing that things like whether you're using a phone or a computer can make a big difference cite3.

- To understand how Risk-Based Authentication (RBA) systems work without knowing everything about their setup, researchers can work with websites for a type of testing called grey-box testing. This way, they can see why and how RBA reacts to certain user actions without needing to know all the system's details. If working directly with websites isn't possible, researchers can use special methods to guess how RBA decides what to do based on what users do on the site.

For example, a study looked at how RBA helps make logging in with a password safer by watching for unusual login attempts, like logging in from a new place. This research shows how partnering with websites for testing can help us understand better when and why RBA asks for extra checks[2].

Another study compared different ways of asking users for extra information if RBA thinks there's a risk. This research tells us that studying RBA's reactions to user actions can show us how to make these extra checks easier for users and still keep accounts safe [3].

3.3 User Experience and Adoption Barriers

- Industry-specific investigations can bring to light particular authentication issues and procedures in various industries, such as the higher security standards in the healthcare and finance industries compared to possibly less strict protocols in the retail or educational sectors. Applying a weighted analysis can improve the applicability and relevance of research findings across various online ecosystems by taking into account variables such as the size of the user base and the unique risk profile of each sector.

- Making sure Risk-Based Authentication (RBA) is used the right way and that people trust it means websites need to be clear about how RBA works and ask users if they're okay with it. This means explaining RBA clearly to users and being open and respectful about their choices. A study [4] by Wiefling, Lo Iacono, and Dürmuth shows that many websites don't share enough information about how they use RBA, which is something they need to do better to build trust with their users.

  Another study[3] looks into how people feel about different ways websites ask them to prove who they are again if there's a concern. This research says it's really important to make sure these RBA methods match what users are comfortable with, which can help people trust these security steps more.

  Lastly, [4] adds more thoughts on making sure RBA is fair, like finding the right balance between keeping things secure and protecting user privacy. By bringing together these ideas, we can work towards RBA methods that not only work well but are also fair and trusted by users, highlighting the importance of talking to users openly and considering their views in the world of online security.

- To make using Multi-Factor Authentication (MFA) easier, we need to study the problems people have when they start using it and while they keep using it. We can make things better by making the setup simpler, giving easy-to-understand instructions, and making sure MFA fits smoothly into using the website or app. A study called ”Multi-Factor Authentication: A Survey” talks about how authentication methods have changed to include MFA. It points out that it’s really important for these methods to be easy for everyone to use and trustworthy. The study says we should look more into how people feel about using these security checks to make them better and easier for everyone[1].

- It is possible to identify areas in which user participation or knowledge may be deficient by assessing the effect of web services’ educational initiatives on encouraging secure authentication methods. Personalized security recommendations based on user behavior, interactive instructional development, and incentives for users to adopt better authentication procedures are some strategies to improve user interaction with security features.

3.4 Privacy-Conscious SSO Solutions

- Improving how we understand and protect privacy in SSO systems is crucial. Looking closely at SSO solutions that focus on protecting privacy, like those that gather very little data about users or use techniques to keep user information anonymous, can offer great insights. For instance, EL PASSO, a system discussed in [9] provides a privacy-preserving SSO solution by using anonymous credentials. This allows users to prove their identity across different services without linking these actions together or revealing more information than needed. EL PASSO shows that it’s possible to have a secure and user-friendly SSO system that respects user privacy, offering a model for developing more private authentication methods .

  Additionally, reviewing the privacy policies of various SSO providers can shed light on how they protect user data. A thorough review can highlight best practices and identify areas needing improvement. This kind of analysis can help create a guide for enhancing privacy protections in SSO systems, making sure user information is kept safe. By integrating these approaches, the analysis can contribute to building SSO systems that better balance convenience, security, and privacy

References

1. A.O. et al.: Multi-Factor Authentication: A Survey. Cryptography 2018, 2(1), 1-31 (2018), https://doi.org/10.3390/cryptography2010001.
2. S. Wiefling, et al.: Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild. In IFIP SEC 2019, LNCS, vol. 11551, pp. 1-16. Springer, Lisbon, Portugal (2019), https://doi.org/10.1007/978-3-030-22312-0_1.
3. S.D. Khan, Y.S. Borse: Geographic Location Based Authentication System. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 8, pp. 16628-16635 (August 2017), https://doi.org/10.15680/IJIRSET.2017.0608288.
4. C. Figueira, R. Matias, H. Gamboa: Body Location Independent Activity Monitoring. In Proceedings of the International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSIGNALS), Rome, Italy, pp. 190-197 (February 2016).
5. M. Papathanasaki, L. Maglaras, N. Ayres: Modern Authentication Methods: A Comprehensive Survey. AI Computer Science and Robotics Technology, 2022(0), pp. 1-24 (2022), https://doi.org/10.5772/acrt.08.
6. G. Austrian Federal Ministry for Digital and Economic Affairs, et al.: Security Evaluation of Biometric Authentication Systems under Real Spoofing Attacks. Security and Communication Networks, 15, pp. 1-15 (2018).
7. Z. Zhang, M. Król, A. Sonnino, L. Zhang, E. Rivière: EL PASSO: Efficient and Lightweight Privacy-preserving Single Sign On. Proceedings on Privacy Enhancing Technologies; 2021(2), pp. 70-87 (2021), https://doi.org/10.2478/popets-2021-0018.
8. M. G.: Anatomy of Account Takeover. In Enigma 2018, pp. 1-6, Colombo, Sri Lanka (August 2015).
9. D. Pointcheval, O. Sanders: Short Randomizable Signatures. In Cryptographers' Track at the RSA Conference, pp. 319-338. Springer (2016), https://doi.org/10.1007/978-3-319-29485-8_18.