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.

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.

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.

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 emphasised 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.