Detailed Summary of the Introduction Section

User Authentication and Password-Based Authentication (PBA):

User authentication is essential for online services like banking and social media.

PBA is the most common method, where users identify themselves with a password.

However, PBA is known to be insecure for several reasons:

Users choose weak passwords that are easy to guess.

Passwords can be compromised through malware, phishing, and data breaches.

Password reuse across accounts can lead to multiple accounts being compromised if one password is stolen.

Multi-Factor Authentication (MFA) as a Security Improvement:

MFA offers an additional layer of security by requiring a one-time passcode (OTP) along with a password.

This OTP is typically generated by a trusted source, like a mobile app, and sent to a user's device.

By requiring both the password and OTP, MFA makes it harder for attackers to gain access even if they steal the password.

Risk-Based Authentication (RBA) for Balancing Security and Usability:

While MFA enhances security, it can be less user-friendly.

RBA addresses this by adapting to login attempts.

It analyzes factors like location, device, and time of day to assess the risk of a login attempt.

If the risk is high, RBA may request additional information like an OTP for verification.

For low-risk attempts, RBA allows login with just the password.

Limited Research on Availability of MFA and RBA:

Despite their security benefits, the adoption rates of MFA and RBA on websites are not well-understood.

Previous research has focused on a small number of sites.

No studies have analyzed the impact of Single-Sign On (SSO) providers on the availability of MFA and RBA.

Goals of This Research Paper:

This paper presents the most extensive study to date on the availability and characteristics of MFA and RBA on the web.

The researchers will analyze 208 popular websites to understand:

The percentage of sites offering RBA.

What additional information is requested during suspicious login attempts.

The percentage of sites offering MFA.

The devices supported for MFA by these websites.

How login security is affected by using Single-Sign On (SSO) providers.

Expected Contributions:

This research will provide valuable insights into the prevalence of MFA and RBA on popular websites.

The findings will likely show that many websites still lack MFA despite its security benefits.

The study may reveal that while some sites with MFA don't automatically block suspicious logins, they might alert users of such activity.

The research might show that even though most sites lack MFA or RBA, many offer login through SSO providers that do support these features.

The study may also uncover a potential privacy trade-off, as most SSO providers with MFA/RBA are also major third-party trackers.

Detailed Summary of the Related Work Section

This section discusses existing research on measuring the availability of MFA and RBA on websites.

Key Points:

There are few comprehensive studies that measure how prevalent MFA and RBA are on the web.

Existing studies have limitations:

Quermann et al. [29]: Analyzed a small set of services (48) and focused on details rather than widespread availability. Didn't test for RBA.

2fa.directory [1]: Offers a broader picture of MFA availability but lacks entries for many popular sites and information on SSO or RBA.

Wiefling et al. [37]: Focused on understanding RBA in eight popular sites through automated interaction. Didn't analyze prevalence across a larger range of sites or consider SSO impact.

Lin et al. [24]: Tested 300 sites but relied on a limited RBA detection method and focused on identifying RBA for tool evaluation, not prevalence. Their results may not reflect overall RBA availability.

Other studies have analyzed SSO relationships at a similar scale but focused on vulnerabilities and how relying parties inherit them, not the potential benefits of using SSO providers for login security.

Detailed summary of methodology section
Challenges to Large-Scale Studies (Section 3.1) in Even Greater Detail:

1. Unreliable Support Documentation:

Incompleteness: Documentation for Multi-Factor Authentication (MFA) and Risk-Based Authentication (RBA) support might not be available on a website. Researchers cannot rely on its presence to determine if a site offers these features.

Inaccuracy: Even when documentation exists, it cannot be guaranteed to be accurate. The researchers encountered situations where documented MFA factors differed from those actually offered by the website.

2. Challenges with Identifying RBA:

Unobservability: RBA operates by analyzing user login behavior. Unlike MFA, it doesn't have a user-controllable option or readily available documentation explaining its activation criteria.

Simulating Suspicious Logins: To identify RBA presence, researchers need to simulate login attempts that deviate significantly from typical user behavior. This requires knowledge of the specific features used during:

Account Creation: The machine's characteristics (operating system, browser, IP address, etc.) used when creating the account need to be known.

Successful Logins: Any subsequent successful logins to the account also need to be performed using the same machine characteristics to establish a baseline.

Risk of False Negatives: Without knowing the specific features used during account creation and successful logins, researchers risk setting up suspicious login attempts with features too similar to regular behavior. This could lead to RBA remaining undetected, resulting in false negatives (failing to identify a website that actually uses RBA).

3. Limitations of Automated Techniques for Account Creation:

Low Success Rates: Existing automated tools for account creation have a low overall success rate (around 1.59%). This rate drops even further (to 11.83%) for websites with unknown signup form structures.

Unpredictable Signup Forms: Signup forms on websites can have unpredictable layouts and require specific formatting for each field. Creating a single automated tool capable of handling all these variations is practically impossible.

CAPTCHA and Web-Bot Detection: Many websites employ CAPTCHAs and web-bot detection tools specifically designed to hinder automated account creation efforts.

Skewed Results: Focusing solely on websites susceptible to automated account creation would exclude a significant portion of websites, potentially including those with more sophisticated security measures (which might also be the ones employing RBA). These excluded websites wouldn't be part of the study, leading to skewed results.

4. Crowdsourcing Limitations:

Verification Issues: Ensuring that a large number of participants performing audits across numerous websites execute them correctly would be challenging.

Ethical Concerns: Burdening websites chosen for control purposes with a substantial number of unnecessary accounts created by participants raises ethical concerns. These control websites would be subjected to potential disruptions caused by the influx of irrelevant accounts.

Browser Fingerprinting Control Challenges: Providing participants with the ability to manipulate browser fingerprinting during suspicious login attempts presents additional challenges. This manipulation would be necessary to effectively simulate login attempts from different machines. However, enabling such control introduces complexities in managing the crowdsourcing process.

Site Selection and Account Creation (Section 3.2) in Detail:

Focusing on Popular User Experience:

Impracticality of Studying the Entire Web: Analyzing every website on the internet is unrealistic for a large-scale study.

Focus on Popular Sites: Researchers aimed to capture the user experience with MFA and RBA for typical internet users. They reasoned that a significant portion of internet traffic concentrates on popular websites, following a Zipf distribution [23].

Selection Process:

Initial Dataset: The research leveraged a dataset compiled by Innocenti et al. [17] containing 366 account-creation websites of varying popularity. This saved them time identifying websites that support account creation.

Filtering for Popularity: From this dataset, they selected the 161 websites ranked within the top 1000 of the Tranco list [23] (generated on June 21, 2021). This ensured a focus on popular websites.

Adding Broader Coverage: To include a wider range of website popularity, they randomly selected an additional 50 websites from the dataset ranked between 1000 and 5000 on the Tranco list.

Including Single Sign-On (SSO) Providers: For each website chosen, they identified all its Single Sign-On (SSO) providers. They then recursively included the SSO providers for those providers as well (limited to providers within the Tranco top 5000). This ensured they considered websites accessed through SSO logins.

Final Set: Following these steps, the final dataset for analysis consisted of 235 unique websites.

Account Creation Decisions:

Focusing on Most Common Account Type: When a website offered multiple account types (e.g., job seeker vs. employer on Indeed), researchers created an account for the type they perceived to be the most common for that website (e.g., job seeker on Indeed).

Free Accounts Only: The study focused on analyzing functionalities of free accounts, assuming most users wouldn't pay for premium versions with potentially additional security features.

Reporting for Chosen Account Type: In cases with multiple account types, results (MFA availability, RBA behavior, SSO providers) are reported for the chosen account type only.

Handling Sites with SSO Login:

Forced SSO Login: Some websites require account creation through another domain, essentially forcing the use of Single Sign-On (SSO). For example, creating a Slideshare account redirected to LinkedIn for account creation, with all subsequent logins using Linkedin SSO.

SSO Provider Audit: In the three cases where this occurred, the researchers audited the SSO provider (e.g., LinkedIn) and applied the audit data to the relying party website (e.g., Slideshare).

Login Scripting (Section 3.3) Explained:

Challenges of Automated Account Creation vs. Login:

Simpler Login Forms: Compared to account creation forms, login forms typically request only username and password, making them easier for an automated tool to interpret.

Less Frequent CAPTCHAs: Websites are less likely to use CAPTCHAs during login attempts compared to account creation (13.8% vs. 3.9%, according to cited studies [10, 18]). This reduces the hurdles for automation.

Benefits of Login Scripting:

Faster Analysis: Automating logins across websites significantly speeds up the analysis process compared to manual logins.

Enhanced Repeatability: Scripting ensures consistency in login procedures, minimizing the risk of human error and improving the repeatability of the study.

Login Scripting Implementation:

JSON-based Login Instructions:

The researchers developed a system that relies on JSON files to define login procedures for each website.

Each JSON file specifies:

Username and password for the website's account.

Login page URL.

A series of "actions" using CSS selectors. These actions define how to interact with specific elements on the login page, including:

Entering text into input fields (e.g., username and password).

Clicking buttons or other elements.

Hovering over elements (optional interaction).

Waiting for page loads to complete.

Login Automation Tool: They built a tool that parses these JSON files and executes the defined actions in sequence.

HOSIT Browser Automation Framework:

This chosen framework (HOSIT) extends Puppeteer [14] to mimic human-like behavior during login attempts. Here's how HOSIT achieves this:

Randomized Clicks: Instead of clicking on a specific pixel location within an element (e.g., a button), HOSIT clicks at random points within the element's boundaries, replicating slight variations in human clicks.

Keystroke Delays: Similar to human typing, HOSIT introduces delays between key presses to avoid appearing automated.

Mouse Click Delays: Delays are also implemented between mouse clicks to further enhance the realism of the login process.

Headful Mode for Avoiding Bot Detection: Although browser automation tools often operate in headless mode (no visible browser window), the researchers specifically ran HOSIT in headful mode. This bypassed certain bot detection mechanisms that target headless browser instances.

HOSIT Enhancements:

The researchers modified HOSIT to:

Handle errors more gracefully during the login process.

Improve its ability to simultaneously click elements and wait for page loads to complete.

Overall Objective: By employing login scripting with HOSIT's human-like behavior simulation, the researchers aimed to minimize the need for manual logins and enhance the efficiency and reliability of their analysis.

Detecting Risk-Based Authentication (RBA) with Black-Box Testing

This section describes how the researchers conducted black-box testing to identify websites that utilize Risk-Based Authentication (RBA). Unlike Multi-Factor Authentication (MFA), which can be directly detected in account settings, RBA requires a different approach.

Challenges of RBA Detection

RBA relies on analyzing user behavior patterns, not settings displayed to users. There's no direct way to check if a website uses RBA by simply looking at account options.

RBA Detection Strategy

The researchers employed a two-step strategy:

RBA Model Training: They trained a model to associate a specific set of features with a user account on a website. These features essentially create a user "fingerprint" and could include:

IP address

Operating system

Browser

Screen resolution

Triggering RBA Response: After training the model, they attempted to log in from a machine with significantly different features compared to the training machine. This drastic change aimed to trigger the website's RBA system to request additional authentication or react noticeably in some way.

Feature Selection for RBA Detection (Table 1)

The researchers based their feature selection on a prior study by Wiefling et al. [37].

Chosen features:

IP address

Operating system

Browser

Screen resolution

Justification:

The study by Wiefling et al. showed these features triggered RBA on five websites.

Some websites (like Google and Facebook) placed high weight on these features for RBA decisions.

RBA Model Training Process

Each account was trained on a Chrome browser running on a specific IP address in Boston, USA (without a VPN).

Suspicious login attempts were conducted using Firefox on Windows 10 from Bulgaria using a VPN. Bulgaria was chosen due to its distance from the training location and the presence of sophisticated hackers in Eastern Europe.

Stay tuned for the next section where we'll explore how the researchers determined the minimum necessary site interaction required to train the RBA model.

Selecting Features to Detect RBA

This section details the reasoning behind the features chosen to identify websites utilizing Risk-Based Authentication (RBA).

Choosing the Right Fingerprint

The researchers relied on the findings from a previous study by Wiefling et al. [37] to select features that would effectively create a unique user "fingerprint." Here's a breakdown of their choices:

Reference Study: The study by Wiefling et al. demonstrated that training accounts with a specific IP address and then attempting logins from a different country triggered RBA on five websites. This indicated that IP address is a significant factor for RBA.

Additional Informative Features: The study also highlighted the importance of user agent string (combination of browser version and operating system) and screen resolution. Notably, Google and Facebook placed high weightage on these features for their RBA decisions.

Based on these insights, the researchers selected the following features for their analysis:

IP Address

Operating System

Browser

Screen Resolution

Training Details (Table 1)

Training Environment: Each account was trained on Chrome 89.0 running on a Ubuntu 20.04 virtual machine with a specific IP address in Boston, USA (no VPN used).

Suspicious Login Setup: Login attempts were then made using Firefox 91.0 on Windows 10 from Bulgaria via a VPN (NordVPN). Bulgaria was chosen due to its significant geographical distance from the training location and the reported presence of skilled hackers in Eastern Europe.

Table 1 Summary: Table 1 summarizes the specific values used for each feature during both the training phase and the suspicious login attempts.

Replicating Prior Work's Setup

The researchers intentionally mirrored the experimental setup used by Wiefling et al. [37] for two main reasons:

Consistency for HOSIT Integration: They wanted to ensure compatibility with their existing tool (HOSIT) to avoid unforeseen issues.

Proven Effectiveness: The prior study successfully triggered RBA on five websites using this configuration. By replicating it, they aimed to achieve similar results.

Lack of Formal Parameter Evaluation

The researchers acknowledge that neither their study nor the referenced study by Wiefling et al. formally evaluates the specific environmental parameters influencing RBA activation. However, they argue that such an evaluation might be unnecessary.

Their justification is that their suspicious login attempt is deliberately crafted to be a clear sign of potential unauthorized access (logging in from a geographically distant location with a different device). Ideally, any website with a functional RBA system should detect this attempt.

They propose that if a website's RBA implementation fails to respond due to specific details in their experimental setup, it exposes a security weakness. In such cases, the website's RBA might not be effectively protecting user accounts from hijacking.

By potentially misclassifying such websites as lacking RBA, their results would still be valuable. They would essentially be highlighting websites with insecure RBA implementations by focusing only on sites with effective RBA, a metric with greater practical significance for users considering the detailed nature of their study.

Note: The section also mentions how they handled websites that blocked access from non-US IP addresses. We'll cover that in the next section.

Unveiling the Minimum Dance for RBA: Less is More

This section explores how much website interaction is necessary to trigger Risk-Based Authentication (RBA). Prior research by Wiefling et al. [37] involved extensive interaction (20 sessions over two months) before attempting suspicious logins. However, replicating this for all websites would be impractical.

Limited Ground Truth and Our Assumptions

No established benchmark exists to determine the minimum interaction required for RBA activation and model training.

The researchers made two key assumptions about RBA implementations:

RBA models likely train only on successful login data. Extensive post-login fingerprinting is less probable due to performance concerns.

Completing account verification should be sufficient to enable RBA. Waiting periods or interaction thresholds would create vulnerable windows for unauthorized access.

Investigating the Minimum Interaction Sweet Spot

To test their assumptions and establish a reasonable baseline, they conducted the following experiment:

Website Selection: A random sample of 50 websites was chosen from their dataset of 235.

Account Creation and Verification: Two accounts were created for each website, and all verification steps were completed for both.

Login Automation: Login attempts were automated using a tool whenever possible (successful for 35 sites).

Interaction Methods:

Minimal Interaction: One account logged in 10 times consecutively using the automation tool (no further interaction). This mimicked typical user behavior of repeated login attempts in a short period.

Extensive Interaction: The other account underwent 10 manual sessions (15-30 minutes each) over a week, simulating typical user activity (watching videos, browsing products, etc.). Additionally, detailed profiles with fake personal information were created for these accounts.

Suspicious Login Attempt and Observation

One day after completing the interaction sessions, a suspicious login attempt was made for both accounts on each website. The website's response was recorded, including:

Request for additional authentication factors

Email alert sent to the user

The Key Finding: Interaction Doesn't Matter (Much)

The results were intriguing. For all 50 websites, both accounts received the same response to the suspicious login attempt. This implies that 10 consecutive logins might be sufficient to enable and train RBA, and extensive interaction over a week may not be necessary.

Next Steps: Refining the RBA Detection Methodology

Based on these findings, the researchers adopted a new approach for their RBA detection methodology, which will be covered in the next section. This approach incorporates the concept of minimal interaction for efficiency.

Refining the RBA Detection Methodology (Section 3.4.3)

Building upon the findings from the previous section, the researchers established a more efficient methodology for their RBA detection process:

Login Procedure for RBA Model Training

Each account underwent a login and logout sequence 10 times consecutively, right after account creation and verification (when required).

Similar to the initial experiment, each login used a cleared browser cache and cookies to avoid identification through cookies.

The timing of these logins wasn't critical, but they never occurred on the same day as account creation.

Handling Sites Requesting Additional Authentication

Websites that requested additional authentication factors during logins, even from the original machine, were excluded from further testing.

The researchers reasoned that these sites likely relied on a simple RBA implementation that solely checked for a specific cookie to bypass additional authentication. The absence of this cookie triggered a high-risk score.

RBA Response Categorization

Websites that responded to the suspicious login attempt were classified as using RBA and further categorized into two groups:

Blocking Sites: These sites requested additional authentication or completely blocked the login attempt (e.g., displaying a generic error message).

Alerting Sites: These sites allowed the login to proceed without requiring extra information but sent an email alert to the user about the suspicious activity.

Websites that neither blocked the login nor sent an alert were classified as not using RBA.

Second Suspicious Login Attempt (to Account for Delayed Activation)

Acknowledging the possibility of RBA activation only after a longer period or suspicious activity, the researchers conducted a second suspicious login attempt two months after the first one.

This attempt used a machine with significantly different features compared to the training machine:

Operating system: macOS Big Sur

Browser: Safari 15.0

IP address: New Zealand (chosen for extreme distance)

For websites that blocked traffic from Bulgaria (used in the first attempt), the second attempt originated from a US location (Dallas, Texas) farthest from the other US locations used.

Table 2 summarizes the specific features employed during the second suspicious login attempt.

Confirmation with Website Owners

To validate their RBA detection findings, the researchers contacted websites that did not block the second suspicious login attempt through various channels:

Bug bounty programs

Security contacts

Customer support

The goals of this communication were:

Verification of their RBA detection results

Understanding the reason behind not implementing RBA

Gauging their interest in adopting RBA in the future

Investigating Post-Login Security (for Non-Blocking Sites)

A random sample of 50 websites (from those that didn't block the suspicious login) were further investigated for post-login security measures:

After a successful login from the suspicious machine, researchers navigated through all account settings pages.

They observed if personal information could be viewed or modified.

They attempted to change the account password and noted if it was successful and triggered an email alert.

Case Study: Bypassing RBA with Login Machine's Cookies

For websites that blocked the suspicious login attempt, the researchers conducted an additional test:

They logged in from the original training machine (where the account was trained).

Then, they copied all cookies for that website's domain and transferred them to the suspicious machine.

They observed if they could gain access to the account settings using the suspicious machine with copied cookies.

This concludes the explanation of Section 3.4.3 on Audit Methodology. By employing these techniques, the researchers aimed to identify websites that implemented RBA and assess their effectiveness.

Beyond RBA: Additional Data Gathered (Section 3.5)

This section details the additional data the researchers collected alongside their RBA measurements for each website:

Single Sign-On (SSO) Providers:

The researchers identified which SSO providers were supported for logging into the website. This information was usually readily available on the signup or login pages.

They manually noted the domains they were redirected to when selecting each SSO provider.

Multi-Factor Authentication (MFA) Support:

The researchers followed a multi-step process to determine if a website offered MFA:

Account Settings Exploration: They manually searched through all account settings pages, typically focusing on security-related sections.

Enabling MFA Option: If they found the option to enable MFA, they documented all supported devices for multi-factor authentication.

Double-Checking with 2fa.directory: Regardless of the findings in step 1, they cross-referenced their results with a directory of websites supporting MFA (2fa.directory).

Verifying Self-Attestation: If 2fa.directory had no information, they looked for any official statements by the website itself regarding MFA support.

Conclusion Based on Evidence: If none of the above steps provided evidence of MFA support, the researchers concluded the website did not offer MFA.

This additional data collection aimed to provide a more comprehensive picture of the website's overall authentication security posture, going beyond just RBA.

Understanding the Limits of this RBA Detection Study (Section 4)

This section acknowledges the limitations and scope of the research on Risk-Based Authentication (RBA) detection:

Challenges in Proving Absence

The study can definitively identify websites that use RBA, but not conclusively prove its absence.

The researchers cite an example of Facebook potentially enabling RBA only for specific accounts based on social interactions. This highlights the limitations of their methodology.

Their findings represent a minimum threshold for RBA availability, not an exhaustive list.

Other Factors Affecting Authentication

The study doesn't explore how RBA models work internally or assess their security.

It excludes other login security measures like rate limiting or account lockout after failed login attempts.

Dataset Size and Generalizability

While the study is the largest of its kind for MFA and RBA, the dataset size involving 235 websites is still relatively small.

The researchers focused on popular and freely accessible sites. They believe their results provide valuable insights into these commonly used websites, but they acknowledge these findings might not be representative of the entire internet.

The study doesn't investigate the availability of MFA or RBA for other services like online banking, internet-connected devices (IoT), or mobile applications.

Figure 1: Distribution of Analyzed Websites (Informational)

Figure 1 is a histogram (graphical representation of data distribution) showing the ranking of the analyzed websites on the Tranco list (likely a website ranking or popularity list).

The X-axis represents the website rank, and the Y-axis represents the number of websites.

This figure provides context for the type of websites included in the study (likely popular ones).

Overall, the researchers are transparent about the limitations of their work and emphasize the valuable insights it offers into RBA prevalence on popular websites.

RBA Detection Study Results (Section 5)

This section presents the key findings from the researchers' investigation into Risk-Based Authentication (RBA) adoption:

Audit Coverage and Basic Authentication Support

Out of the initial 235 websites, 208 were successfully analyzed (audited).

Interestingly, all audited websites implemented Password-Based Authentication (PBA), a basic authentication method using usernames and passwords.

Reasons for Failed Audits (27 Websites)

The researchers encountered various obstacles that prevented auditing 27 websites:

Paid Subscriptions: Some websites required paid subscriptions for account creation.

Regional Restrictions: Certain websites mandated region-specific identification numbers the researchers didn't possess.

Account Creation Removal: A few websites had discontinued account creation since a previous study (by Innocenti et al.).

Undiagnosed Errors: Other websites displayed errors during account creation that the researchers couldn't troubleshoot.

Figure 1: Tranco Ranking Distribution (Informational)

Figure 1 (mentioned previously) is a histogram illustrating the distribution of audited websites based on their Tranco ranking (likely a website ranking/popularity list). This helps understand the popularity range of the analyzed websites.

Scriptable vs. Manual Logins

The researchers were able to automate login using a tool for 152 (73.08%) of the audited websites. These are classified as "scripted sites."

The remaining 56 websites (26.92%) required manual login due to various challenges and are categorized as "manual sites."

Reasons for Manual Logins

CAPTCHAs: 43 websites employed CAPTCHAs (challenges to distinguish humans from bots) on the login page, hindering automation.

Enforced MFA: Ten websites mandated Multi-Factor Authentication (MFA) on every login attempt, making scripted login impractical.

Web Driver Detection: Three websites identified and blocked the login attempts originating from the researchers' web automation tool.

Login Automation and Website Popularity (Figure 2)

Figure 2 (not shown here) explores the correlation between a website's popularity (Tranco rank) and the feasibility of scripted logins. The x-axis is on a logarithmic scale to accommodate the skewed distribution of website ranks (most websites have lower ranks).

The graph suggests that website popularity has minimal influence on login automation success, except for the most popular websites (Tranco top 50) that might have stricter bot mitigation measures.

The success rate for scripted logins hovered around 67% for the Tranco top 50 and top 100 websites.

Beyond rank 200, the success rate remained above 70% for most websites.

Key Takeaways from this Section

The study achieved a high audit success rate (over 88%).

All audited websites used PBA, but their RBA adoption remained to be investigated (addressed in later sections).

Login automation was successful for a significant portion of websites (over 70%). Website popularity played a minor role in automation feasibility, except for the most popular ones.

Multi-Factor Authentication (MFA) Adoption Rates (Section 5.1)

This section dives into the prevalence of Multi-Factor Authentication (MFA) among the analyzed websites:

Disappointingly, only 42.3% (88 out of 208 websites) offered some form of MFA, highlighting the widespread reliance on Password-Based Authentication (PBA) despite its known security weaknesses.

MFA Availability and Website Popularity

Figure 3 (shown here) explores the correlation between a website's popularity (Tranco rank) and MFA support. The green line represents the percentage of sites with MFA at or below a given rank.

The average website with MFA ranked at 527.75, compared to the overall average rank of 811.09.

Interestingly, MFA adoption was nearly universal for the most popular websites (Tranco top 50) with a rate of 90.48%. Similarly, 70% of websites in the Tranco top 100 offered MFA.

However, beyond rank 334, the percentage of sites supporting MFA dropped significantly below 50% and continued to decline.

Supported MFA Devices (Table 3)

Table 3 summarizes the various devices supported for MFA and the number of websites offering them. Notably, no biometric or passwordless authentication methods were encountered.

SMS and third-party authenticator apps were the most common options, both supported by 61 websites.

The researchers caution against SMS-based MFA (used by 10 websites) due to its lower security compared to other methods.

Email-based MFA (found on 4 websites) also raised concerns as it doesn't necessarily prove possession of the user's device but rather knowledge of their email credentials.

"Unsafe" MFA and Popularity

A total of 18 websites only provided SMS or email-based MFA, categorized as "unsafe" MFA. These websites also tended to be less popular, with the most prominent one ranking at 116 (canva.com).

The average rank for websites with "unsafe" MFA was 859.33, compared to 527.75 for sites with any MFA option.

MFA Adoption by Website Category

Website categories were classified using a URL Ticketing System. Some categories exhibited a higher tendency to support MFA than others.

Among categories with at least three websites, Auctions/Classifieds, Games, Social Networking, and Personal Network Storage had the highest adoption rates (over 75%).

Conversely, none of the websites in General News, Sports, and Fashion/Beauty categories offered MFA.

Secure vs. Insecure MFA by Category

The preference for secure MFA methods also varied by category.

For instance, half of the websites in the Auctions/Classifieds category only offered "unsafe" MFA (SMS or email).

On the other hand, all websites in Personal Network Storage and Finance/Banking categories provided MFA through secure means like authenticator apps, security keys, or proprietary devices.

Appendix A.1 (not shown here) provides a detailed breakdown of MFA adoption and supported methods across different website categories.

MFA Availability and Login Automation

Table 4 (shown here) presents the distribution of MFA availability for websites requiring scripted logins versus manual logins.

One might expect websites with stronger security measures against automated login attempts (manual sites) to be more likely to offer MFA. The results support this assumption: 60.71% of manual sites offered MFA compared to 35.53% of scripted sites.

A statistical test (two-proportion z-test) confirmed this correlation with high significance (p-value much lower than 0.01), indicating that websites with bot protection are more likely to provide MFA.

This section exposes the concerningly low adoption rate of MFA despite its well-established security benefits. The analysis also revealed a connection between website popularity, website category, and the likelihood of offering secure MFA.

Risk-Based Authentication (RBA) Adoption Rates (Section 5.2)

This section explores the prevalence and behavior of Risk-Based Authentication (RBA) among the analyzed websites:

When a suspicious login attempt was initiated, 46 websites (22.1%) responded by blocking it. Table 5 (not shown here) details the additional authentication factors requested by these websites (mostly email OTPs).

Email was the most common channel for these additional authentication requests since email addresses were likely the only identifiers provided during account creation (phone numbers weren't mandatory).

Another 23 websites didn't block the suspicious login but sent an email alert to the user.

The remaining 139 websites (almost two-thirds) showed no response to the suspicious login attempt, suggesting they might not use RBA.

RBA and Website Popularity (Figure 3)

Figure 3 (shown previously) illustrates the correlation between website popularity (Tranco rank) and RBA usage. The blue line represents the percentage of sites using RBA (blocking or alerting) at or below a given rank. The red line shows the percentage of blocking sites only.

Both lines exhibit similar trends: RBA adoption is nearly universal for the most popular sites (Tranco top 50) with a rate exceeding 60%.

However, the percentage of websites using RBA drops sharply around rank 20, remains relatively steady until rank 80, and then steadily declines as website rank (popularity) decreases.

RBA Adoption by Website Category

Website categories were again classified using a URL Ticketing System. Certain categories exhibited a higher tendency to employ RBA than others.

Among well-represented categories (at least 3 websites), Games, Personal Network Storage, Social Networking, and Finance/Banking had the highest RBA adoption rates (over 40% blocking suspicious logins and over 60% blocking or alerting).

Conversely, none of the websites in General News, Education/Reference, and Fashion/Beauty categories displayed any response to suspicious login attempts.

Interestingly, the categories with high and low RBA adoption mirrored those with high and low MFA adoption observed in the previous section.

Table 10 in Appendix A.2 (not shown here) provides a detailed breakdown of RBA behavior across different website categories.

The Relationship Between RBA and MFA

Table 6 (shown here) presents RBA responses for websites with and without MFA.

While 38 out of 88 websites with MFA blocked the suspicious login, 34 didn't respond, indicating room for improvement even among MFA-enabled sites.

Contrary to an initial expectation, 15 websites used RBA without offering MFA. Eight of these blocked the login attempt, while the others only alerted the user.

This highlights a potential concern: some websites might rely solely on RBA without allowing users to leverage MFA for enhanced security.

Interestingly, 17 websites that requested email OTPs upon a suspicious login attempt via RBA did not offer email OTPs as an MFA option. This suggests these sites reserve email OTPs specifically for RBA-triggered scenarios.

RBA and Login Automation

Table 7 (shown here) compares RBA responses for scripted and manual logins.

Similar to the findings with MFA, one might expect websites with stronger security measures against automated login attempts (manual sites) to be more likely to use RBA.

The results support this assumption: 50% of manual sites responded to the suspicious login (blocking or alerting) compared to only 27% of scripted sites.

A statistical test (two-proportion z-test) confirmed this correlation with high significance, suggesting websites with bot protection are more likely to implement RBA.

RBA Prevalence Across Different Popularity Segments

Only 52% of websites in the Tranco top 50 and 42% in the Tranco top 100 blocked the suspicious login attempt, and the rate drops to 22% for the entire dataset.

When considering both blocking and alerting responses, these numbers rise to 62% and 63% for the Tranco top 50 and 100, respectively, but still fall to 33% for the whole dataset.

Limited Post-Login RBA Detection

As mentioned earlier, 50 websites that didn't block the suspicious login attempt were further investigated for post-login RBA.

In all these cases, researchers were able to view and modify user information (name, address, etc.) after logging in from the suspicious machine.

Only two out of these 50 websites required an email OTP to change the account password.

Email or SMS alerts upon password changes were sent by only 1

Impact of Single Sign-On (SSO) on Authentication Security (Section 5.3)

This section analyzes how Single Sign-On (SSO) providers influence the security landscape for user authentication:

While most audited websites lacked Multi-Factor Authentication (MFA) or Risk-Based Authentication (RBA), many utilized SSO providers that offered these features.

If a compromised login attempt occurs, the attacker would need to bypass the SSO provider's security measures (which might include MFA or RBA) to gain access to the user's account.

The researchers investigated how SSO providers affect MFA and RBA availability for websites.

SSO Enhances Authentication Security

The study revealed a significant positive impact of SSO on user authentication security:

167 websites (80.3%) in the sample either supported MFA directly or could inherit it through SSO providers.

Even for sites with only SMS/email-based MFA (considered less secure), 14 out of 19 had an SSO provider offering more robust MFA options.

Similarly, 161 websites (77.4%) either used RBA or could inherit it via SSO.

Among these, 151 websites had or could inherit an RBA mechanism that blocked suspicious login attempts, providing the strongest security.

Interestingly, all websites without inherited MFA or RBA lacked SSO providers altogether. This suggests that at least one SSO provider offers both MFA and blocking-RBA for any website using SSO.

The Role of Major SSO Providers

Google and Facebook were the dominant SSO providers, accounting for 107 and 106 websites respectively.

Both Google and Facebook blocked suspicious login attempts and offered secure MFA options (authenticator apps, hardware keys).

Figures 4 and 5 (not shown here) visualize the widespread influence of Google and Facebook as SSO providers.

Each node represents a website, and edges depict the connection between an SSO provider and the websites it authenticates (relying parties).

The size of a node reflects the number of websites it authenticates.

Light green nodes represent websites with inherited MFA or RBA blocking.

Even though Apple and Twitter were also SSO providers for some websites, all their relying parties were also connected to Facebook or Google.

Beyond Google and Facebook

While Google and Facebook played a major role, SSO's positive impact wasn't solely reliant on them.

Many websites connected to Facebook and Google also relied on other providers with MFA and RBA capabilities.

Even without Google and Facebook, 132 websites (63.5%) could still benefit from inherited MFA, and 109 (52.4%) could inherit blocking-RBA.

Privacy vs. Security Trade-Off

A significant caveat emerged: most SSO providers that offered inherited MFA or RBA were also major website trackers (e.g., Google, Facebook, Twitter).

This implies a privacy trade-off: enhanced security through SSO might come at the cost of increased user tracking, even without traditional third-party tracking cookies.

Disabling SSO providers from known tracking domains (using Disconnect.me's list) would decrease overall availability of inherited MFA and RBA:

MFA availability would drop to 56.8% (from 80.3%) with SSO and increase by only 14.1% compared to no SSO.

RBA blocking would decrease to 45.7% (from 77.4%) with SSO and increase by 23.6% compared to no SSO.

Table 11 in Appendix A.3 (not shown here) details the impact on MFA and RBA availability when excluding specific SSO providers.

Without tracking domains, Apple emerged as the primary provider for inherited MFA (26 websites) and blocking-RBA (44 websites).

Conclusion

SSO plays a significant role in improving user authentication security by enabling websites to inherit MFA and RBA from providers that offer these features. However, this benefit comes with a potential privacy cost as major SSO providers are often also prominent website trackers.

The Current State of User Authentication Security: A Struggle Between Security and Privacy (Section 6)

This section discusses the broader implications of the study's findings on user authentication security.

Low Adoption of MFA and RBA

Despite the well-known weaknesses of passwords alone, only 42.3% of audited websites offered MFA, and a mere 22.1% blocked suspicious login attempts (indicating RBA).

Security improves with website popularity: 90.5% of websites in the Tranco top 50 supported MFA, and 52.4% blocked suspicious logins.

However, both MFA and RBA availability drop sharply for less popular sites, suggesting a trend across the broader internet.

SSO Partially Mitigates the Issue

This highlights the potential value of Single Sign-On (SSO) for enhancing security on less secure websites.

Due to the dominance of Google and Facebook as SSO providers (both offering MFA and blocking suspicious logins), leveraging SSO could significantly improve security:

80.3% of websites could potentially gain access to MFA.

72.6% of websites could inherit RBA that blocks suspicious login attempts.

The Privacy vs. Security Trade-Off with SSO

A major concern arises: most SSO providers that offer inherited MFA or RBA are also notorious website trackers (e.g., Google, Facebook).

Disabling tracking domains for SSO reduces overall security benefits:

MFA availability would drop to 56.8%.

RBA blocking would decrease to 45.7%.

In this scenario, Apple emerges as the primary provider for inherited security measures, but its reach is limited.

Recommendations

The ideal solution would be for websites to implement MFA and RBA themselves, eliminating reliance on SSO providers and the associated privacy concerns.

However, the study reveals a lack of motivation among website owners:

No cited technical or financial hurdles for RBA implementation.

Some believe users are responsible for account security (strong passwords, using available MFA).

Some perceive a lack of user demand for MFA and RBA.

To improve user authentication security, a two-pronged approach is needed:

Security community efforts:

Educate website owners about password limitations and user hesitancy towards MFA.

Advocate for offering MFA for security-conscious users and implementing RBA for automatic protection.

User behavior changes:

A more vocal user base demanding MFA and RBA can incentivize website adoption.

Increased user security awareness can encourage even non-security-conscious users to benefit from these protections.

Conclusion

The current state of user authentication security presents a complex challenge. While SSO offers some improvement through inherited security features, it comes at the cost of user privacy. Ultimately, a combination of website owner behavior changes and a more security-conscious user base is necessary to achieve a balance between strong authentication and user privacy.

Ethical Considerations Regarding Account Creation

This section addresses the ethical considerations surrounding the creation of user accounts during the research:

The researchers acknowledge creating accounts on 208 websites specifically for this study, accounts they never intended to use as typical users.

To minimize potential harm, the researchers limited account creation:

Typically only two accounts were created per site:

One for guiding and testing the automation used for data collection.

One for collecting the final audit data.

In some cases, existing personal accounts were used for automation guidance, requiring only one new data collection account.

For a specific experiment (Section 3.4.2), a maximum of three accounts were created per site involved.

Even during an initial experimentation phase, the maximum number of accounts created for any single site was five.

The researchers opted against creating more accounts to avoid overwhelming the websites with login attempts, which could be considered spamming or misuse of the platforms.

Transparency and Balancing Research Needs with Ethical Practices

This section is a positive example of researchers considering the ethical implications of their methods. They prioritized minimizing any negative impact on the websites they studied while still gathering necessary data.

User Authentication Security: A Web of Insecurity and Privacy Concerns

This study investigated the prevalence of Multi-Factor Authentication (MFA) and Risk-Based Authentication (RBA) on popular websites. Here are the key takeaways:

Low Adoption of Advanced Security Measures: Disappointingly, only 42% of the audited websites offered MFA, and a mere 22% blocked suspicious login attempts (indicating RBA).

Security Improves with Popularity: More prominent websites tended to prioritize security: 90% of the top 50 Tranco-ranked sites offered MFA, and over half blocked suspicious logins.

SSO Partially Rescues the Situation: Single Sign-On (SSO) emerged as a potential solution for less secure websites. By leveraging SSO providers like Google and Facebook (which offer MFA and RBA), a significant portion of websites could benefit from:

Increased MFA availability: Up to 80% of websites could potentially gain access to MFA.

Enhanced RBA protection: Over 72% of websites could inherit RBA that blocks suspicious login attempts.

Privacy vs. Security Trade-Off with SSO: A concerning aspect is that most SSO providers with MFA and RBA are also major website trackers. Disabling tracking domains for SSO reduces the security improvements:

MFA availability would drop to 56.8%.

RBA blocking would decrease to 45.7%.

The Ideal Solution (and Why It's Not Happening): Ideally, websites would implement MFA and RBA themselves, eliminating reliance on privacy-intrusive SSO providers. However, the study reveals a lack of motivation among website owners:

They often cite a belief that users are responsible for their own security (strong passwords, using available MFA).

Some perceive a lack of user demand for these advanced security features.

A Two-Pronged Approach for Improvement: To bridge the security gap, a combined effort is needed:

Security community efforts: Educate website owners about password limitations and user hesitancy towards MFA. Encourage them to offer robust authentication and implement automatic RBA protection.

User behavior changes: A more vocal user base demanding MFA and RBA can incentivize website adoption. Increased user security awareness can encourage even non-security-conscious users to benefit from these protections.

Conclusion

The current state of user authentication security online presents a complex challenge. While SSO offers some improvement, it raises privacy concerns. Ultimately, a shift in attitudes and practices from both website owners and users is necessary to achieve a balance between strong authentication and user privacy.

This appendix provides additional data and analysis related to the main body of the research paper.

A.1 MFA Factors by Category

This section (Table 9) explores Multi-Factor Authentication (MFA) factors offered by various website categories. It shows the number of sites within a category that support different MFA methods, including:

SMS (text message)

Email

Third-party app (e.g., Google Authenticator)

Security key (physical device)

Phone call

First-party app (developed by the website itself)

First-party device (unique to the website)

The table highlights the following:

Business and Software/Hardware categories have the highest overall MFA adoption.

SMS and Email are the most common MFA factors offered, but some sites utilize more secure options like security keys or first-party apps.

The "Unsafe" column identifies sites solely reliant on SMS or Email for MFA, which are considered less secure methods.

A.2 RBA Behavior by Category

This section (Table 10) focuses on Risk-Based Authentication (RBA) behavior observed across website categories. It details how many sites within a category exhibit specific RBA actions, such as:

Requiring additional verification (like an OTP - one-time password) based on factors like login location or device.

Sending alerts upon suspicious login attempts.

The table reveals:

Business and Internet Services categories have the most widespread RBA implementation.

Email OTP and SMS OTP are the most common RBA verification methods used.

Some sites leverage email alerts or phone number confirmations for enhanced security.

A.3 MFA and RBA Availability with Restricted SSO Providers

This section (Table 11) analyzes the impact of limitations on Single Sign-On (SSO) providers on Multi-Factor Authentication (MFA) and Risk-Based Authentication (RBA) availability. It shows the number of sites that:

Offer MFA or could potentially inherit it through SSO.

Exhibit various RBA behaviors.

Block login attempts entirely or send alerts based on SSO restrictions.

The table demonstrates:

Restricting SSO providers generally reduces the number of sites offering MFA or exhibiting RBA behaviors.

Blocking all SSO providers significantly diminishes both MFA and RBA availability.