A Study of Multi-Factor and Risk-Based Authentication Availability

Anthony Gavazzi\textsuperscript{1}, Ryan Williams\textsuperscript{1}, Engin Kirda\textsuperscript{1}, Long Lu\textsuperscript{1}, Andre King\textsuperscript{2}, Andy Davis\textsuperscript{2}, Tim Leek\textsuperscript{2}

\textsuperscript{1}Northeastern University, \textsuperscript{2}MIT Lincoln Laboratory
Methods of User Authentication

Password-Based Authentication (PBA)
- Authenticate with a username and password
- Simple and intuitive
- Passwords are guessable, leakable, and prone to reuse

Multi-Factor Authentication (MFA)
- Present two or more factors
- Raises the bar to compromise an account
- Substantial usability issues
Risk-Based Authentication (RBA)

Transparently observe various implicit features while a user logs in

Develop a notion of a “normal” fingerprint for a user
Risk-Based Authentication (RBA)

Features match what is typically observed: allow login as normal

From user’s perspective, typical PBA
Risk-Based Authentication (RBA)

Features differ enough: automatically request more factors

Protects account while preserving usability
What is the State of User Authentication Security?

MFA and RBA recommended by NIST

Several questions not answered by prior work:

Do sites actually support MFA and RBA?

Do those that support them use secure factors?
  • SMS susceptible to SIM swapping attacks
  • Email codes are not MFA, but two-step verification

If sites don’t support them, does Single-Sign-On (SSO) offer a remedy?
MFA/RBA Inheritance Through SSO

Some sites don’t support MFA

Their SSO providers do, though
MFA/RBA Inheritance Through SSO

When logging in through provider...

Additional authentication factors requested

Relying party “inherits” login security
Research Goals and Questions

1. Perform the largest study of MFA and RBA availability on the web

2. What additional factors do sites support for MFA?

3. How do sites respond to a suspicious login attempt?

4. How does SSO change the picture?

5. What are the implications?
Methodology
Scope and Site Selection

Measuring MFA and RBA at full-Internet scale is infeasible
  • Self-attestation not guaranteed
  • Need new accounts for each site that we control
  • Automation and crowdsourcing introduce significant limitations

Instead, focus on a manageably large set of 208 popular sites
  • Obtained from prior work

Perform a systematic, manual analysis of each
Histogram of Domain Ranks of Sites We Audited

Domain Rank in Tranco List
Measuring MFA and SSO

MFA is enabled in account settings
• Simply record what factors we see

SSO plainly visible on login and/or signup page
RBA Challenges

Only way to tell if a site uses RBA is to observe it directly
  • Not under user’s control to turn on/off
  • Can’t be gleaned from login page information

Need to:
  1. Create a new account from one machine
  2. Log in/interact with the site enough to teach it what “normal” is
  3. Attempt to log in from a machine with substantially different features
  4. Observe whether additional factors are requested

Gives rise to two key questions
Which Features to Control For?

Chose a set of features based on prior work

Idea is to set off as many alarms as possible

Account created and all logins from “Training” machine

After teaching site what “normal” is, attempt login from “Suspicious” machine

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Training</th>
<th>Suspicious</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Boston, MA</td>
<td>Sofia, Bulgaria</td>
</tr>
<tr>
<td>OS</td>
<td>Ubuntu 20.04</td>
<td>Windows 10</td>
</tr>
<tr>
<td>Browser</td>
<td>Chrome 89.0</td>
<td>Firefox 91.0</td>
</tr>
<tr>
<td>Resolution</td>
<td>1920 x 1080</td>
<td>1488 x 878</td>
</tr>
</tbody>
</table>
How to Teach Site What “Normal” Is?

How much interaction is necessary to enable and train RBA?
  • How many logins?
  • Any post-login site interaction required?

For each site:
  1. Create and verify a new account from “Training” machine
  2. Log in/out 10x from “Training” machine, scripted whenever possible

This is as good at training RBA as performing lengthy, manual interaction with a site for a week
  • Sites’ response to suspicious login is the same
  • Confirmed through experiment with 50 sites
Results
MFA and RBA Availability

Both MFA and RBA are uncommon in general

• 42.3% supported MFA
• 22.1% blocked the suspicious login
• 11.1% just alerted the user

Popular sites are more likely to support them

Figure 3: Percentage of sites at or below a given Tranco rank that support MFA or use RBA.
Supported Authentication Factors

Most popular MFA factors are SMS OTPs and authenticator apps
  • Each supported by 69.3% of sites with MFA

8.7% of all sites support MFA through *only* unsafe factors
  • Tend to be less popular on average

For RBA, email and SMS OTPs nearly universal
  • Requested by 82.5% of sites with RBA
The Impact of SSO

If one were to sign up through an SSO provider that supports MFA/RBA, whenever available:

- 80.3% of sites would have access to MFA
- Just 1.4% would have access to only unsafe factors for MFA
- 72.6% would block a suspicious login attempt

![Bar chart showing the impact of SSO on MFA and RBA](chart.png)
MFA Inheritance Through SSO
RBA Inheritance Through SSO
SSO Drawbacks

Is SSO the solution, then?

Single point of failure

Nearly all SSO providers with MFA/RBA are major third-party trackers*

May not be amenable to all users to use SSO through these providers
  • Why create manual links between accounts and a tracker?

*as classified by Disconnect’s tracker list
SSO Drawbacks

Excluding third-party trackers* from SSO providers:

• 56.8% have access to MFA
• 45.7% would block a suspicious login attempt
• The only provider with any significant coverage is Apple

SSO is not a silver bullet for improving login security

*as classified by Disconnect’s tracker list
How to Improve this Situation?

Ideally, every site would offer MFA through secure devices and use RBA

We asked all 161 sites without MFA and/or RBA why they did not support it

Heard back from just 4, but the feedback was illuminating

Some said users should choose strong passwords and use password managers instead

Others simply did not see a strong enough user demand for MFA/RBA
Takeaways

Security researchers must work to change prevailing attitudes about relying on passwords

End users benefit from knowing that SSO can provide access to MFA and RBA

But users’ attitudes towards security must also change

Only a preponderance of users requesting security features will encourage developers to support them
Conclusion

Presented the largest study of MFA and RBA characteristics to date

Found low adoption of both in general

A supermajority of sites can access MFA and RBA via SSO providers

SSO is a single point of failure and may pose privacy risks

Prevailing attitudes toward PBA still must change to make the web more secure

Thank you!

gavazzi.a@northeastern.edu