

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

Anthony Gavazzi¹, Ryan Williams¹, Engin Kirda¹, Long Lu¹,
Andre King², Andy Davis², Tim Leek²

¹Northeastern University, ²MIT Lincoln Laboratory



**Northeastern
University**

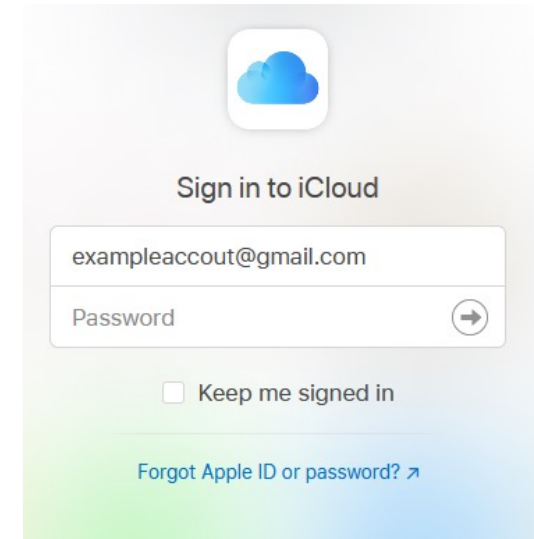


LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Methods of User Authentication

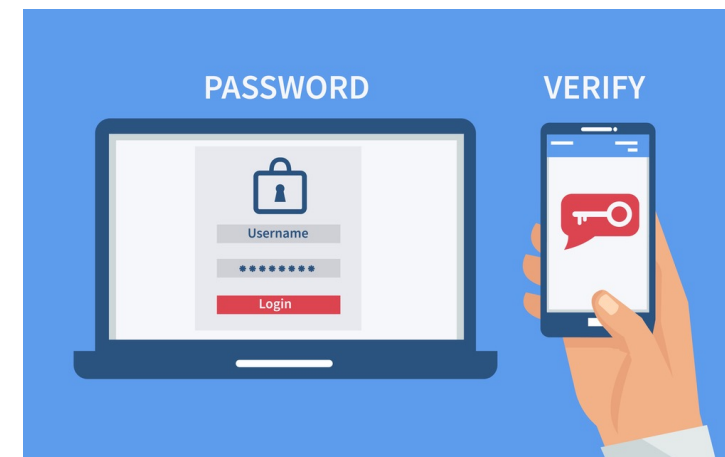
Password-Based Authentication (PBA)

- Authenticate with a username and password
- Simple and intuitive
- Passwords are guessable, leakable, and prone to reuse



Multi-Factor Authentication (MFA)

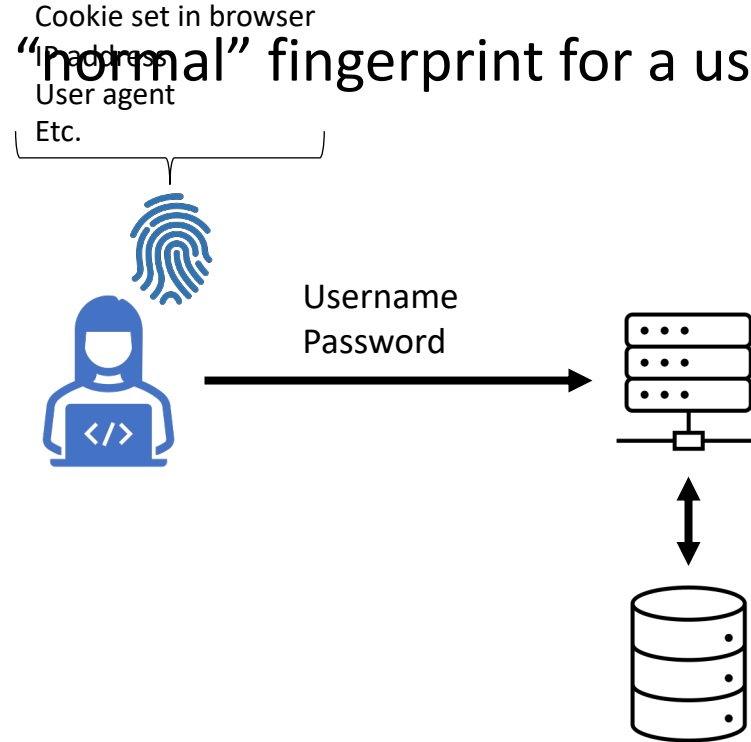
- Present two or more factors
- Raises the bar to compromise an account
- Substantial usability issues



Risk-Based Authentication (RBA)

Transparently observe various implicit features while a user logs in

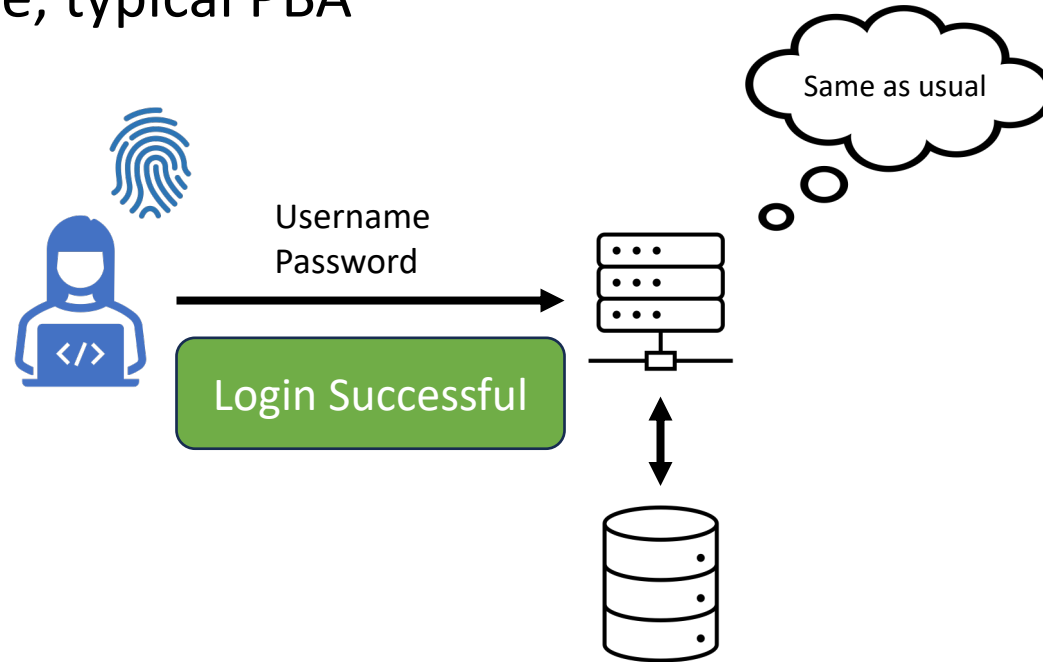
Develop a notion of a “normal” fingerprint for a user



Risk-Based Authentication (RBA)

Features match what is typically observed: allow login as normal

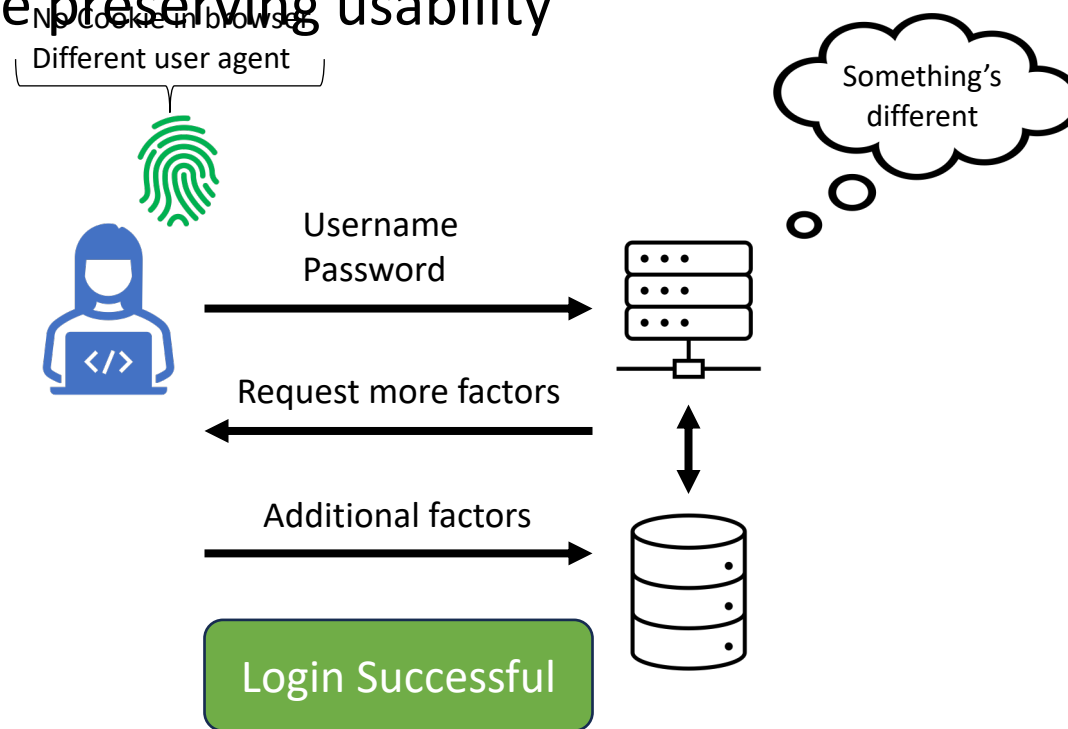
From user's perspective, typical PBA



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?

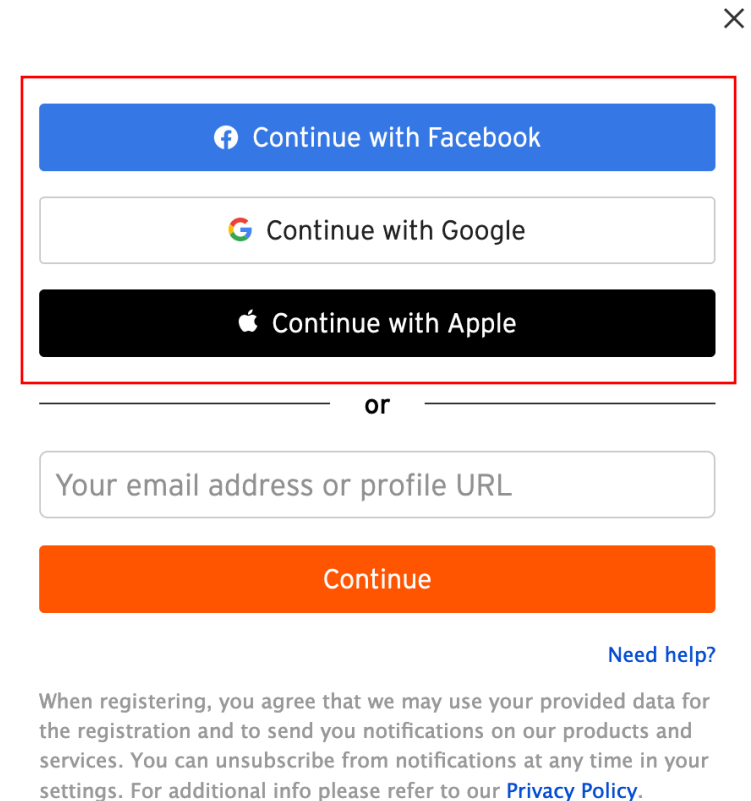
- SMS susceptible to SIM swapping attacks
- Email codes are not MFA, but two-step verification

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



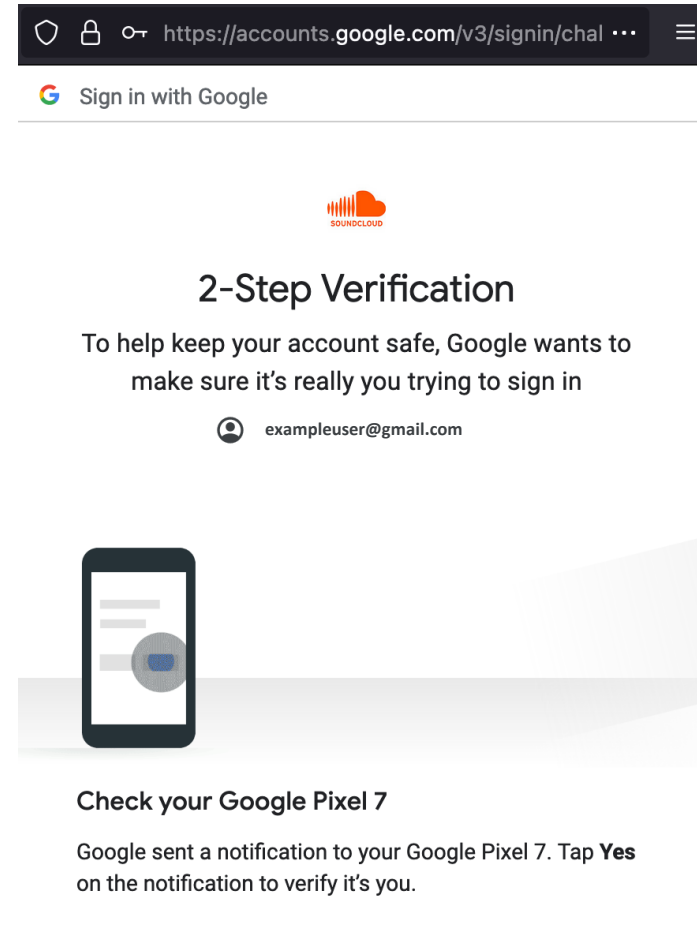
A screenshot of a user interface for registration or login. At the top right is a close button (X). Below it, three social media login buttons are stacked vertically and enclosed in a red rectangular box: 'Continue with Facebook' (blue), 'Continue with Google' (white with Google logo), and 'Continue with Apple' (black with Apple logo). Below these is the word 'or' centered between two horizontal lines. Underneath is a text input field with the placeholder text 'Your email address or profile URL'. Below the input field is an orange 'Continue' button. At the bottom right is a blue link 'Need help?'. At the bottom is a paragraph of text: 'When registering, you agree that we may use your provided data for the registration and to send you notifications on our products and services. You can unsubscribe from notifications at any time in your settings. For additional info please refer to our [Privacy Policy](#).'

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

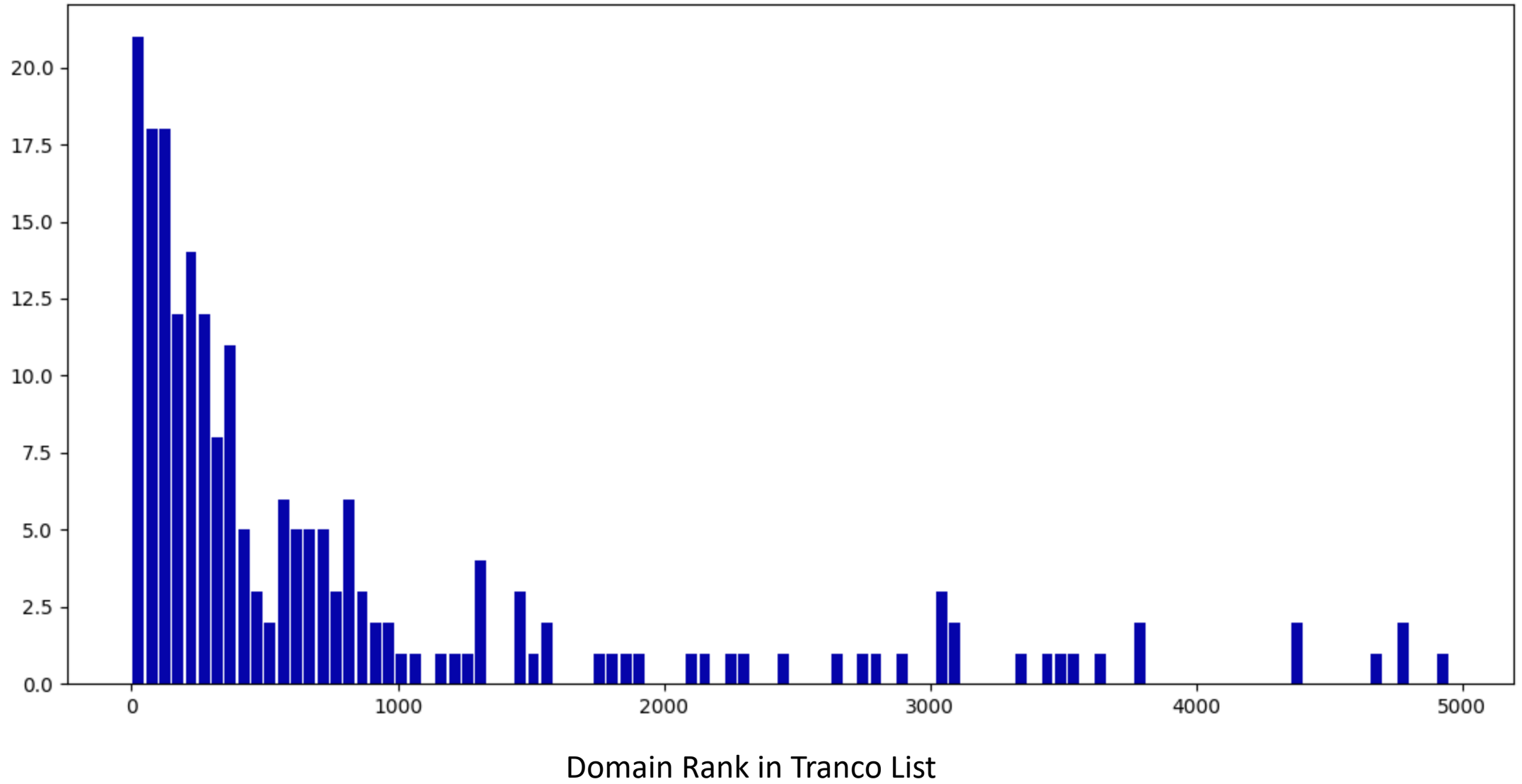
- Self-attestation not guaranteed
- Need new accounts for each site that we control
- Automation and crowdsourcing introduce significant limitations

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



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

Sign in and security

Password	Create a password or modify your existing one.	Edit
Secret questions	Give yourself another secure way to recover your account.	Edit
2 step verification	Protect your account by adding an extra layer of security.	Edit

Hello

Sign in to eBay or [create an account](#)

Email or username

Continue

or



Continue with Facebook



Continue with Google



Continue with Apple

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

Parameter	Training	Suspicious
IP Address	Boston, MA	Sofia, Bulgaria
OS	Ubuntu 20.04	Windows 10
Browser	Chrome 89.0	Firefox 91.0
Resolution	1920 x 1080	1488 x 878

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

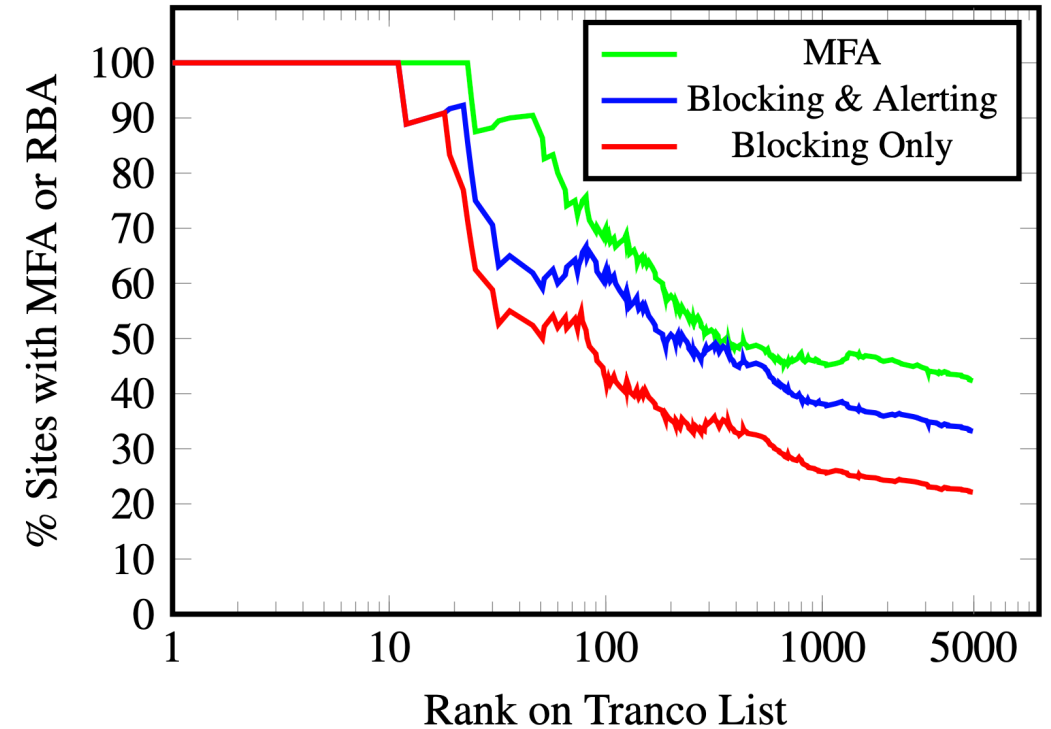


Figure 3: Percentage of sites at or below a given Tranco rank that support MFA or use RBA.

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

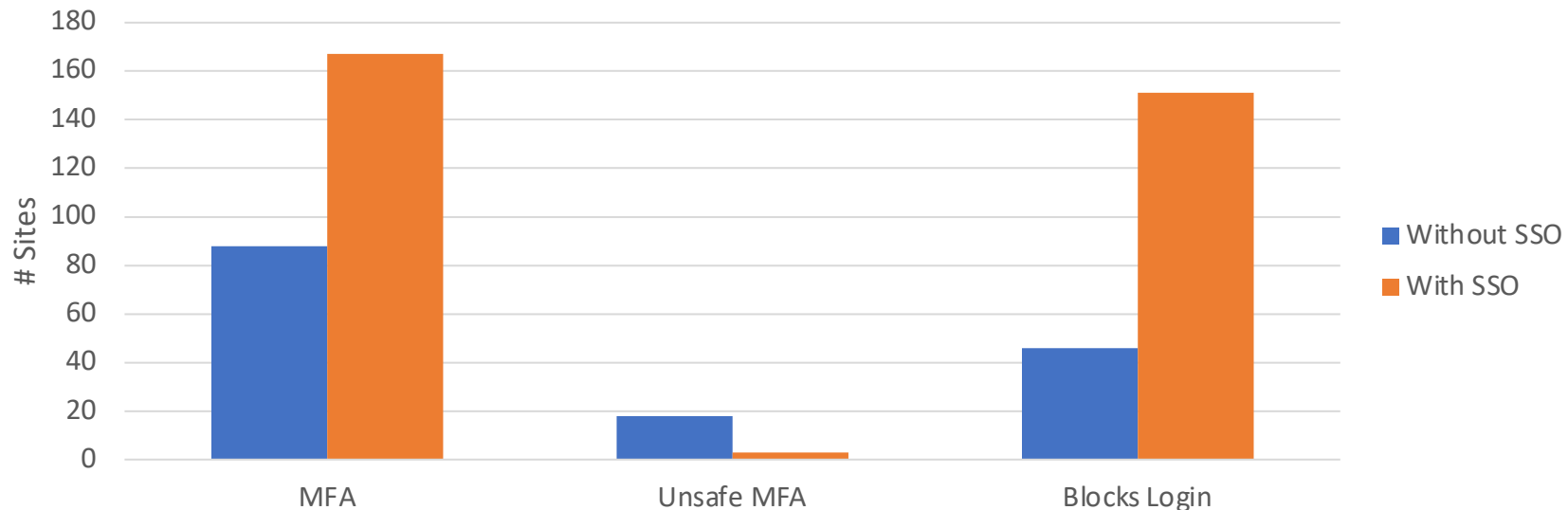
For RBA, email and SMS OTPs nearly universal

- Requested by 82.5% of sites with RBA

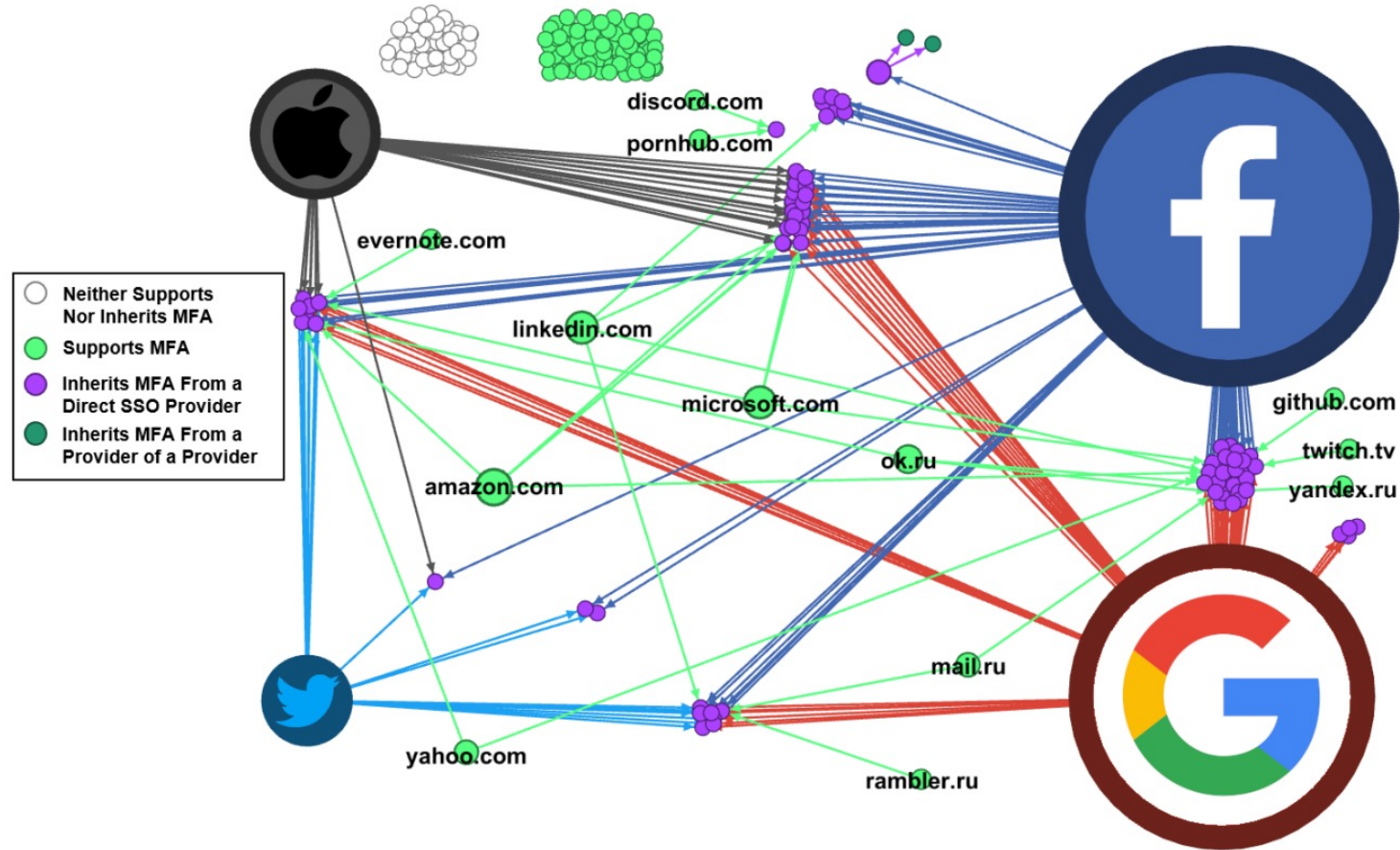
The Impact of SSO

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

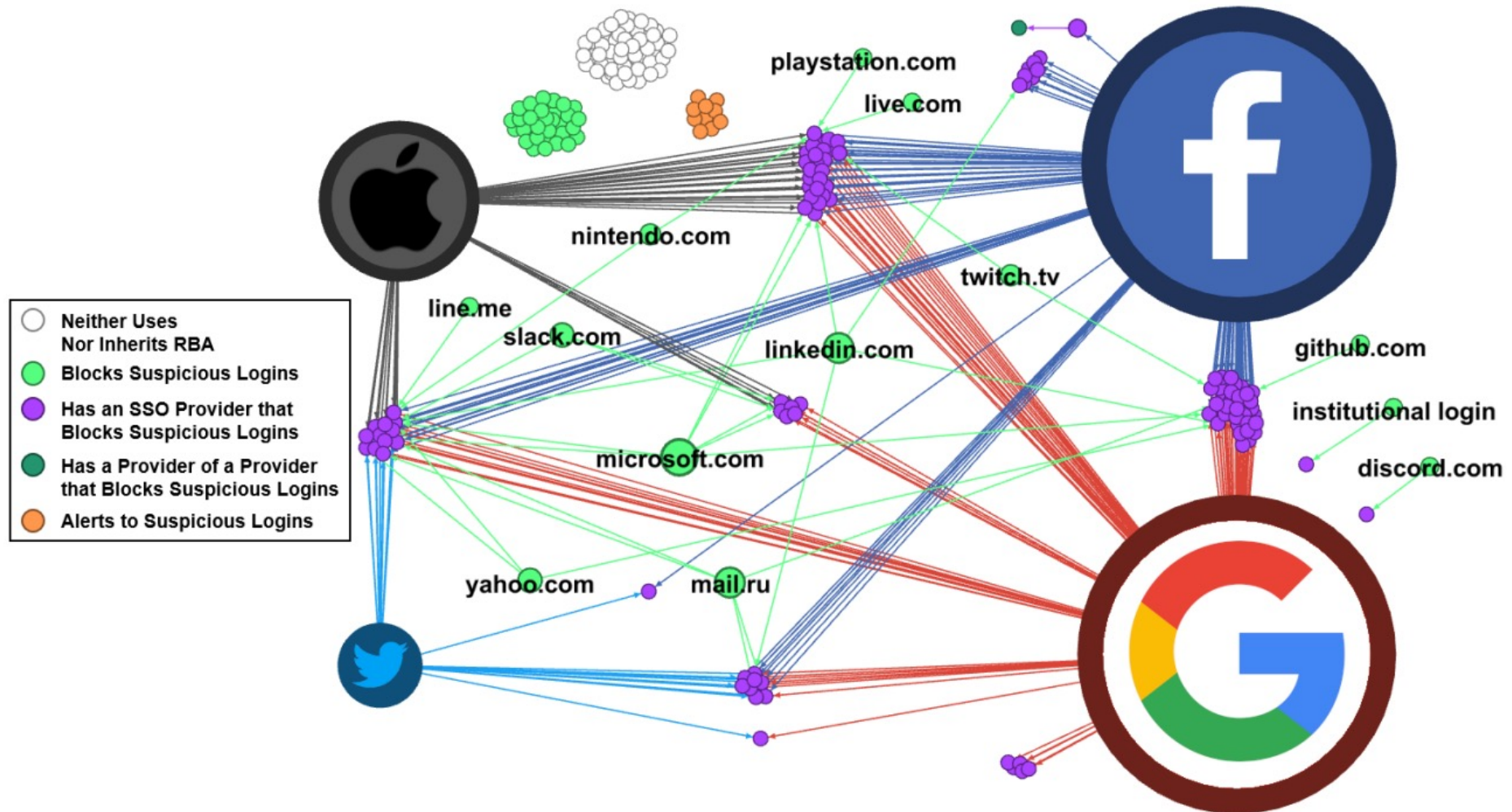
- 80.3% of sites would have access to MFA
- Just 1.4% would have access to only unsafe factors for MFA
- 72.6% would block a suspicious login attempt



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?

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

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