Measuring NIST Authentication Standards Compliance by Higher Education Institutions

Noah Apthorpe, Boen Beavers, Yan Shvartzshnaider, Brett Frischmann

COLGATE UNIVERSITY

YORK UNIVERSITÉ UNIVERSITY

VILLANOVA UNIVERSITY

Motivation

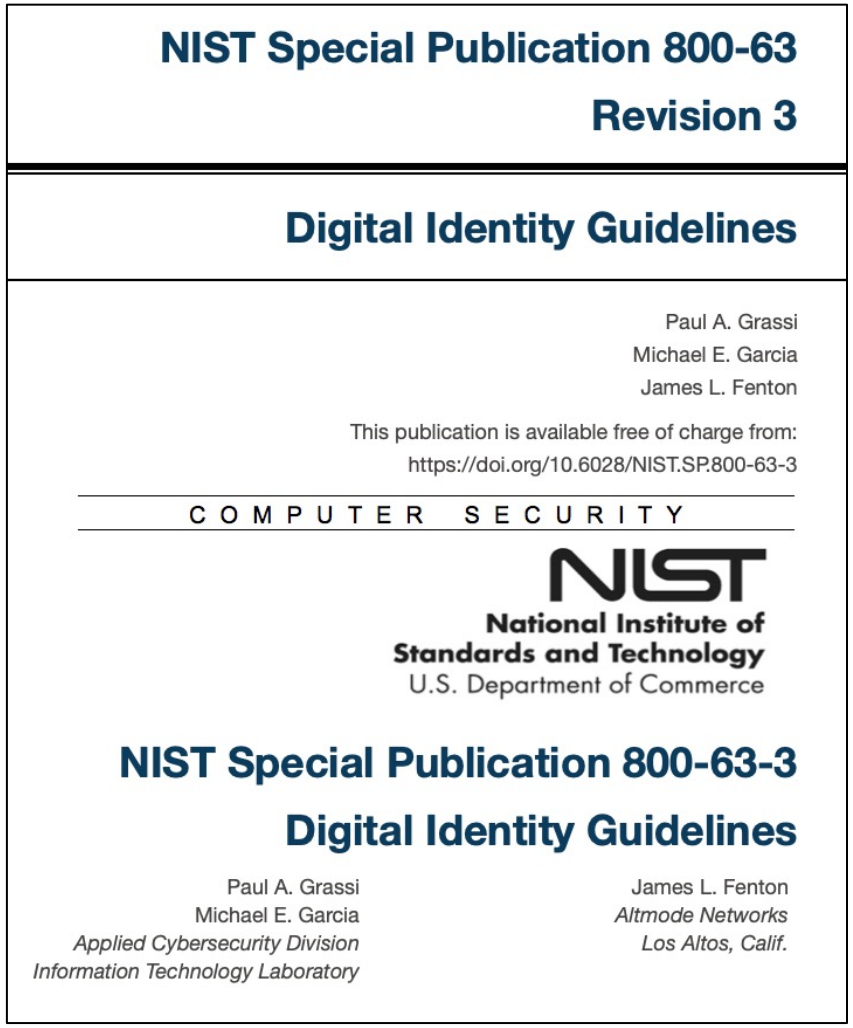

...about digital authentication...
How well is expert cybersecurity advice diffusing to practitioners?
...espoused in standards documents...
...in higher education

Research Question

- How well do higher education institutions' digital authentication ***policies*** align with NIST standards for
  - Multifactor authentication
  - Password expiration
  - Password composition requirements
  - Knowledge-based authentication

NIST SP 800-63 *Digital Identity Guidelines*

- Originally published in 2004
  - Major updates in 2011, 2013, and 2017
- "An overview of identity frameworks; using authenticators, credentials, and assertions in a digital system; and a risk-based process to select assurance levels"
- Higher education institutions can use these standards as non-binding technical guidance for authentication policies


NIST Special Publication 800-63
Revision 3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63-3

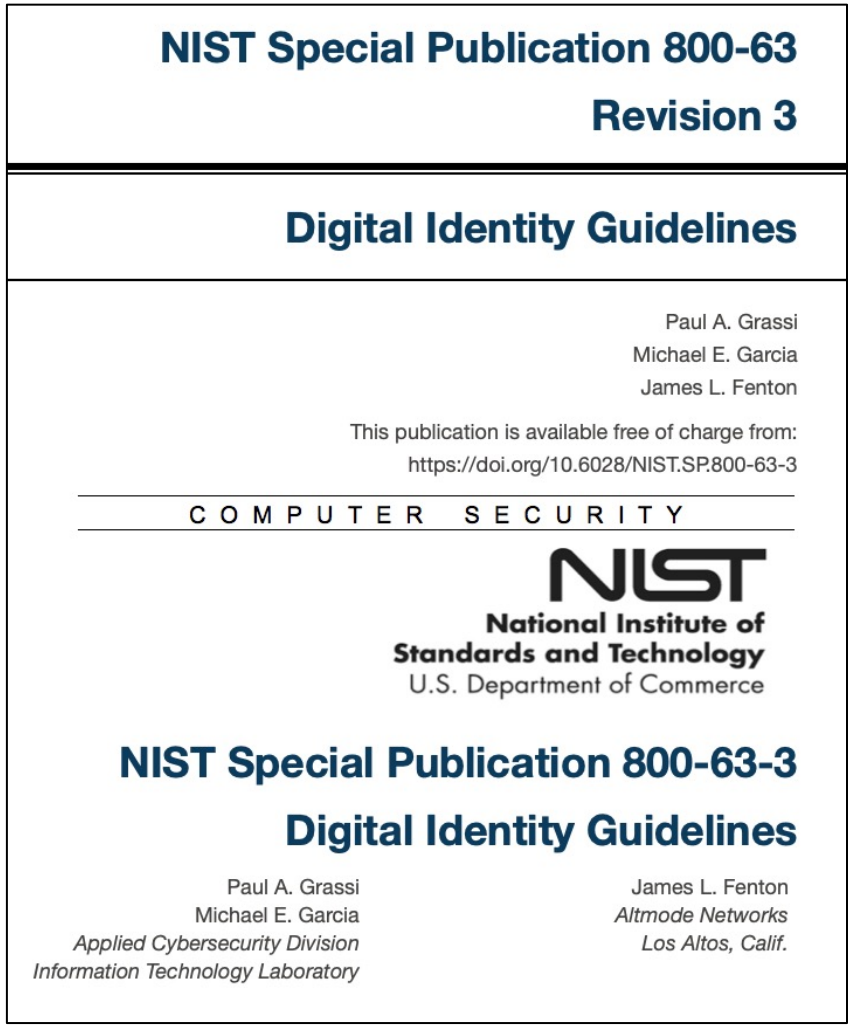
Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

NIST SP 800-63 *Digital Identity Guidelines*

- Ideal case study for our RQ
  - Current standards in place since 2017
  - Clear differences between current and previous versions
  - Widely supported by academic research and other government bodies



NIST Special Publication 800-63
Revision 3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

Institution Selection

- U.S. News & World Report “Top” Institutions 2023
  - 20 Canadian Global Universities
  - 20 US National Universities
  - 20 US Public Colleges & Universities
  - 20 US Liberal Arts Colleges
  - 10 US Historically Black Colleges & Universities
  - US Regional Colleges
    - 10 North region
    - 10 South region
    - 10 Midwest region
    - 10 West region
- 135 institutions total*

* Including ties

Policy Identification & Coding

- Identified publicly-available authentication policies on institutions' websites
  - Search engines with site-specific queries ("site:[institution].edu")
  - Search bars on institutions' websites
  - Manual navigation of institutions' websites

- Preferred newer, institution-wide policies
- Excluded policies over 10 years old

- Policies coded by subset of authors and student RAs for each standard
  - *Required, required for specific affiliates, recommended, discouraged, disallowed, N/A*
- Disagreements resolved by first author

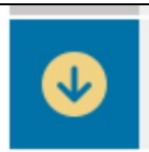
Example Policies

MFA Required

Multi-factor authentication is required for all Colgate students, faculty, and staff for both Colgate network/SSO accounts and Colgate email/Gmail accounts. Enrolling is easy, and provides you a significant new layer of security.

Step-by-step Duo instructions »

Enroll in Google 2-Step now »



Challenge Questions

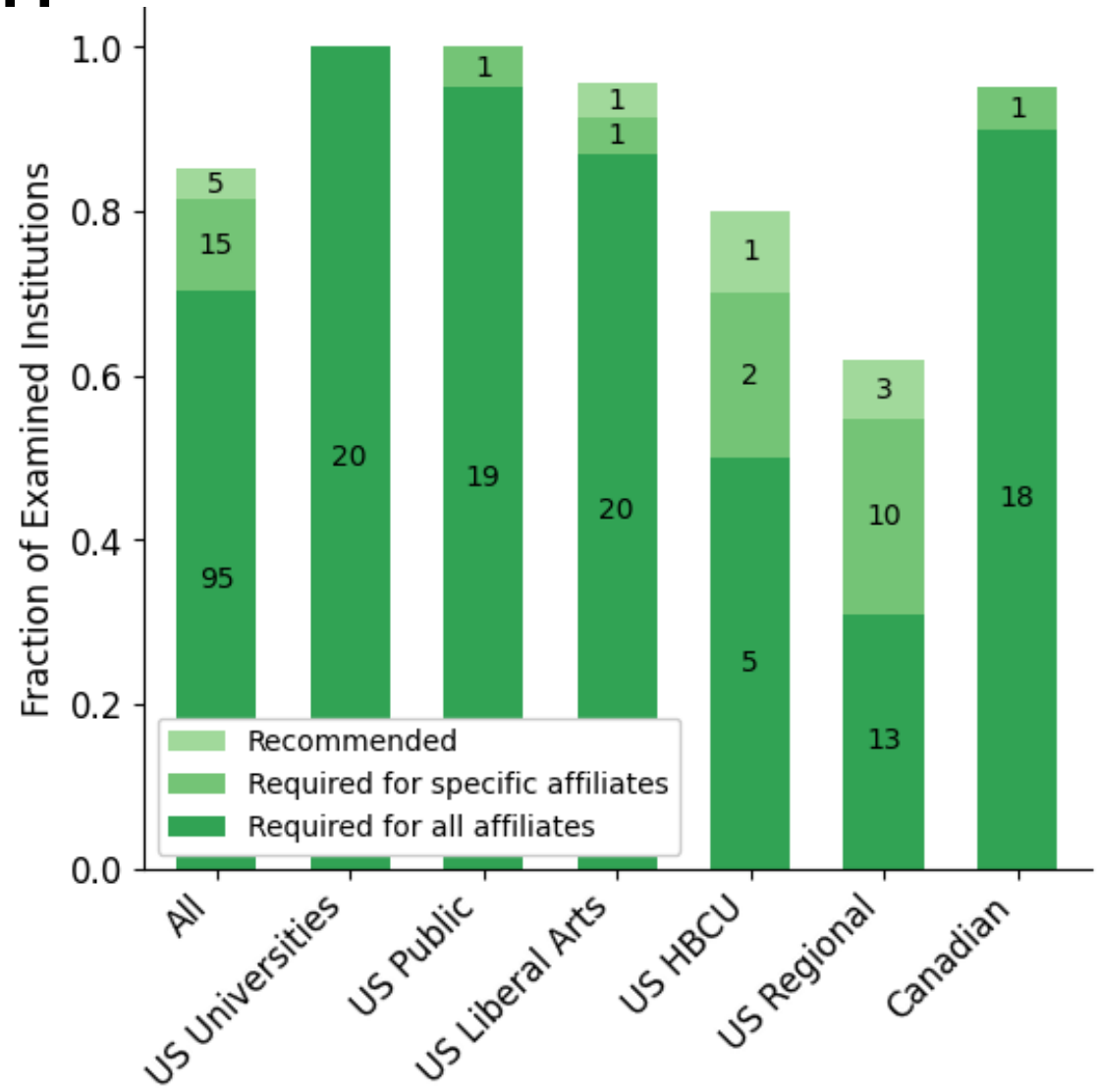
Setting Your Challenge Questions

KBA Recommended

Once you have logged into the access.caltech application, we strongly recommend that you set up your challenge questions. Setting up challenge questions will allow you to use the "Forgot Your Password" feature of access.caltech if you ever forget your password in the future.

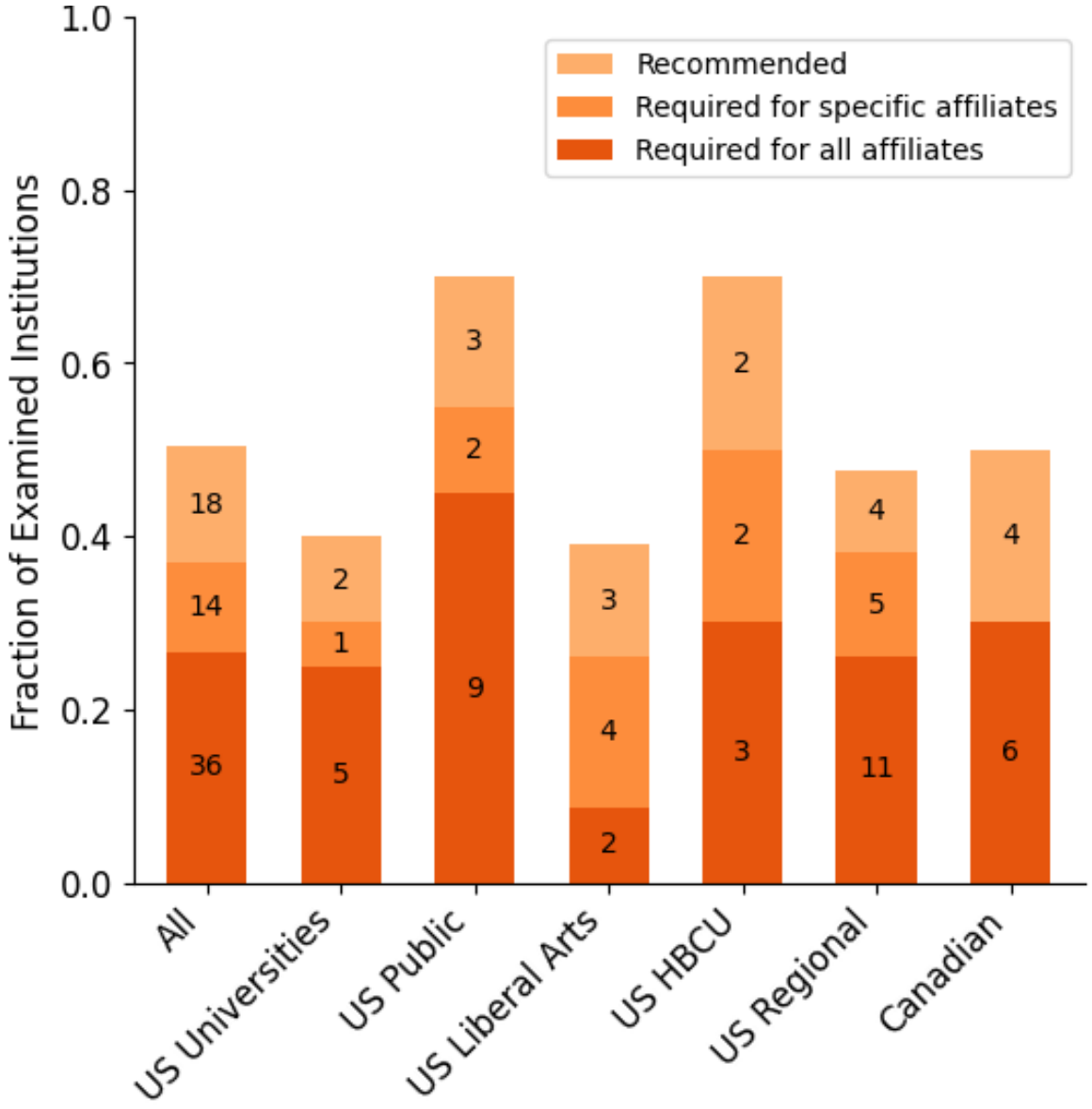
Multifactor Authentication

- Pre-2017
  - LOA 2 (moderate risk)
  - MFA recommended, but not required
- 2017
  - AAL 2 (moderate risk)
  - “Authentication SHALL occur by the use of either a multi-factor authenticator or a combination of two single-factor authenticators.”



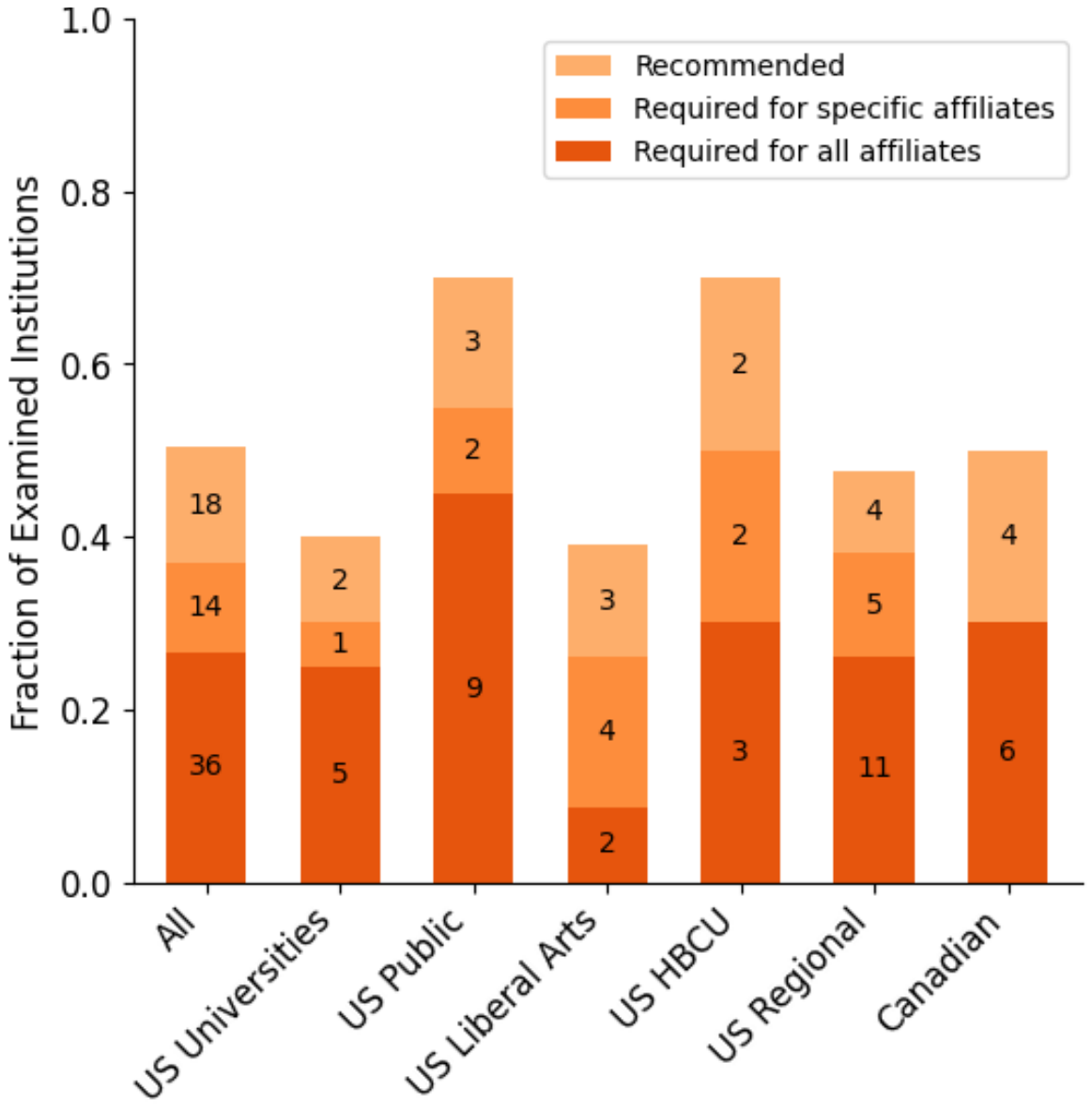
Password Expiration

- Pre-2017
  - Regular password expiration or cycling is best practice
- 2017
  - “Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically).”



Password Expiration

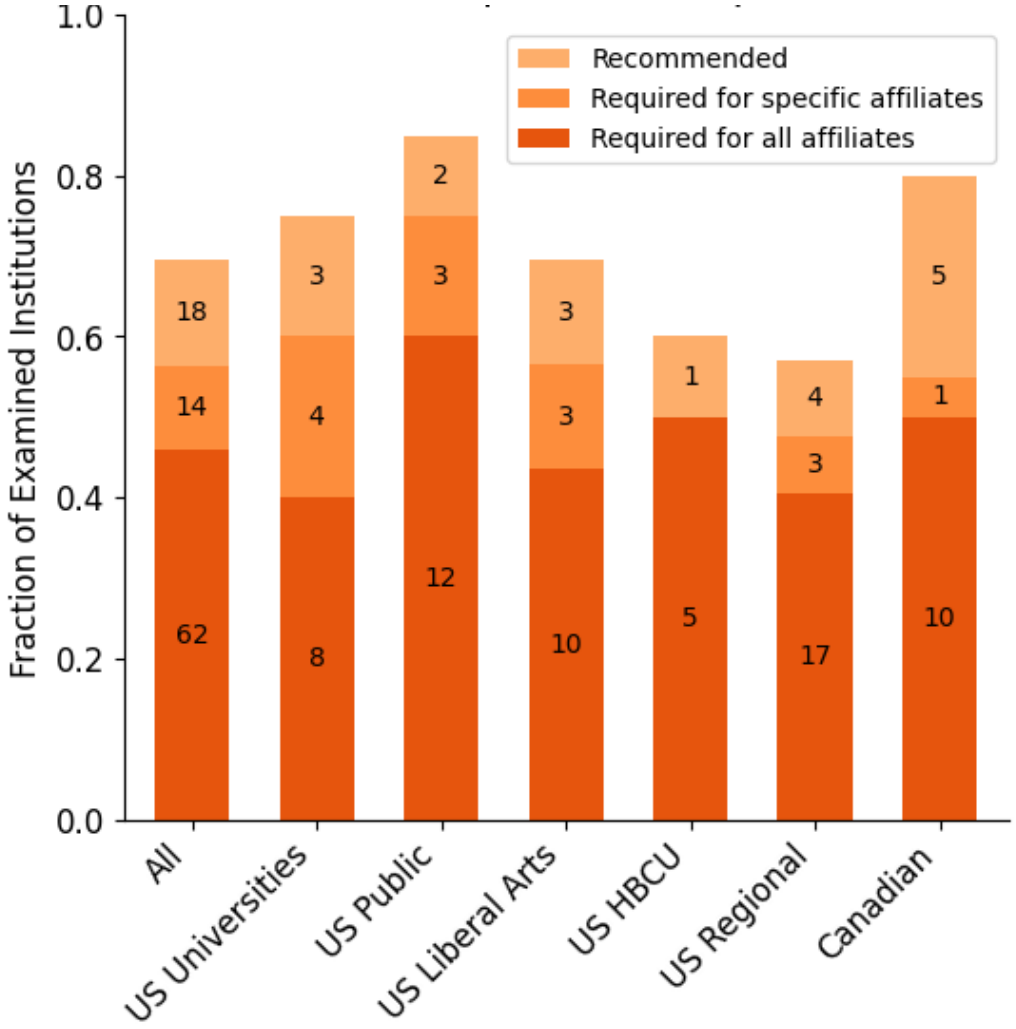
Password Expiration Frequency	Count
1 year (annually, 365 days, etc.)	32
180 days	6
90 days	6
6 months	5
Periodically	5
60 days	2
Often	2
1 year (user), 180 days (admin)	1
1 year (with MFA), 180 days (without MFA)	1
1 year (with MFA), 120 days (without MFA)	1
180 days (user), 90 days (admin)	1
126 days	1
120 days	1
30 days	1
30 days (sensitive data), 90 days (other data)	1
Once or twice a year	1
Frequently	1



Password Composition Rules

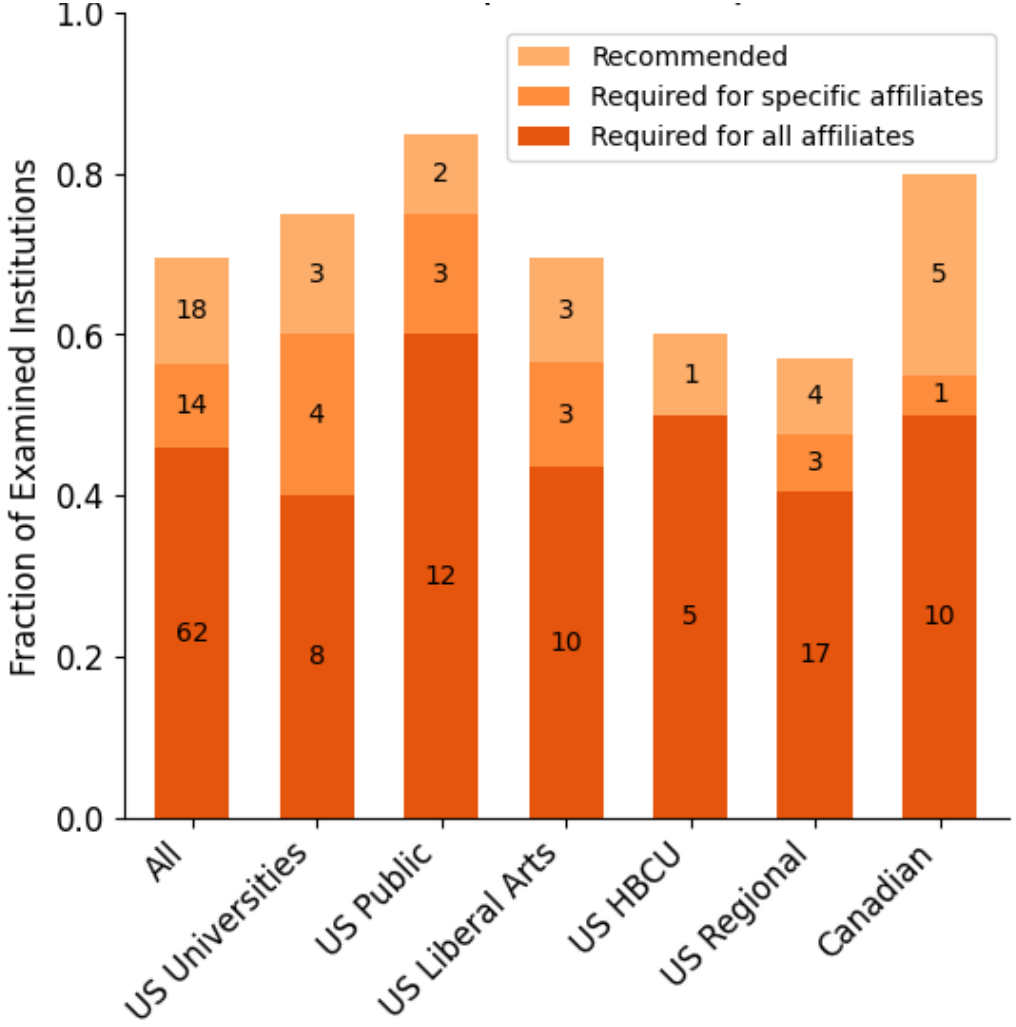
- Pre-2017
  - Password composition rules should be enforced during account creation

- Your password must be between **8 and 16** characters long.
- Your password must contain ***ALL*** of the following:
  - at least **one UPPERCASE letter**
  - at least **one number**
  - at least **one special character**, such as: !, $, #, %, etc.



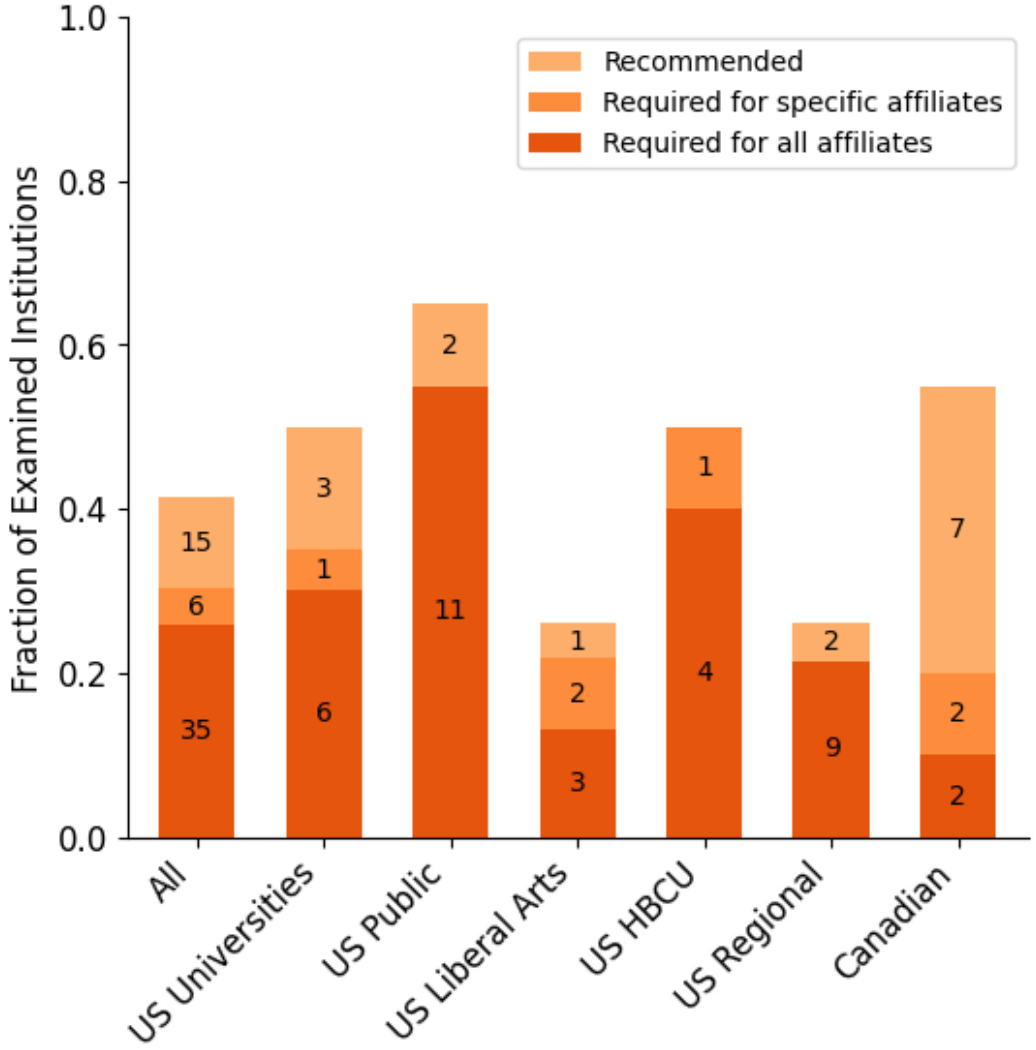
Password Composition Rules

- Pre-2017
  - Password composition rules should be enforced during account creation
- 2017
  - “Verifiers SHOULD NOT impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets.”



Knowledge-Based Authentication

- Pre-2017
  - KBA permitted and referred to as a “pre-registered knowledge token”
- 2017
  - “Knowledge-based authentication (KBA), sometimes referred to as ‘security questions’, is no longer recognized as an acceptable authenticator”



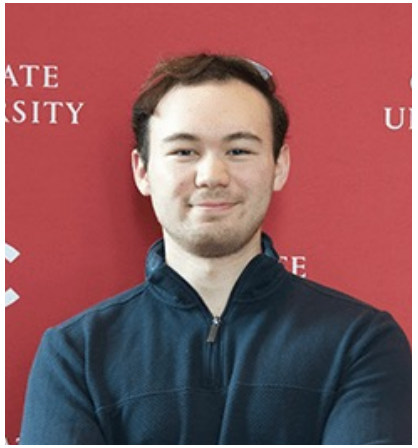
Implications

- The compliance rates we observed were worse than previously measured across a variety of other industries[1]
- Difficult to determine whether policies match actual practices
- Incentives for noncompliance
  - Resource constraints, entrenched legacy systems, difficult to configure third-party software (e.g., single sign-on platforms), institutional prioritization of non-cybersecurity features
- Barriers to knowledge diffusion
  - Insufficient outreach/education, overconfident practitioners, conflicting messages
  - See SOUPS literature about software patches…

[1]Robert C. Hall, Mary Ann Hoppa, and Yen-Hung Hu. An empirical study of password policy compliance. *Journal of The Colloquium for Information Systems Security Education,* 10(1):8–8, 2023.

Contact Information

Noah Apthorpe
Department of Computer Science
Colgate University
napthorpe@colgate.edu



Boen Beavers
Department of Computer Science
Colgate University
bbeavers@colgate.edu

Yan Shvartzshnaider
Department of Electrical Engineering
and Computer Science
Lassonde School of Engineering
York University
yansh@yorku.ca

Brett Frischmann
Charles Widger School of Law
Villanova University
brett.frischmann@law.villanova.edu