Open Access License Notice

An Empirical Study of Password Policy Compliance

Robert C. Hall
Computer Science Department
Norfolk State University
Norfolk, Virginia USA
r.c.hall98490@spartans.nsu.edu

Mary Ann Hoppa
Computer Science Department
Norfolk State University
Norfolk, Virginia USA
mahoppa@nsu.edu
0000-0002-6103-7814

Yen-Hung Hu
Computer Science Department
Norfolk State University
Norfolk, Virginia USA
yhu@nsu.edu
0000-0003-0040-4788

***Abstract*—Cybersecurity exploits that take advantage of weak passwords continue to succeed in virtually every industry. This motivates interest in empirically determining the extent to which websites that invite visitors to create new user accounts on them encourage or require users to engage in better password management practices, including strong passwords. This project examined a statistically significant sample of websites to assess how closely they voluntarily adhere to the National Institute of Standards and Technology's authoritative guidance on password policies. Over 100 representative websites were selected from industries that consistently report the most breaches in the Verizon Data Breach Investigation Report. Their respective user account creation processes were assessed via a scorecard approach based on observations collected when following standardized experimental procedures. Scorecard data then were aggregated and analyzed for trends. The research findings highlight potential vulnerabilities that persist in online account password creation practices, leaving many websites susceptible to brute force attacks due to cyber hygiene lapses. Recommendations to help remediate compliance gaps and as paths forward to build upon this work include refining the proposed scorecard, creating and using standardized user registration and profile manager plugins, widely adopting user-friendly password management tools, and enacting tougher legal consequences for website hosts when breaches occur.**

Keywords—password creation, password management, compliance scorecard, NIST SP 800-63-3

I. INTRODUCTION

As technology and computing power increase, so does the ability of threat actors to compromise passwords. At the same time, whether driven by convenience or necessity, people are doing more professional and personal activities online than ever before [1]; and in doing so they share relevant personal information that businesses as well as bad actors can leverage for their own purposes. While news of data breaches should make everyone increasingly wary of how well data they share online is being safeguarded by the companies that house them, users continue to create weak passwords. According to an online study published by YouGov, over half of all online users are using the same passwords for most of their accounts [4].

In short, left to their own choices, users' passwords are not secure despite well-publicized breach incidents and clearly defined best practices from reputable bodies like the National Institute of Standards and Technology (NIST). When websites invite visitors to create online accounts, but then do not enforce compliance with authoritative password guidance, this effectively results in a virtually endless vulnerable attack surface for cyber criminals who seek to breach, then exfiltrate and exploit personal and financial information.

The goal of this project was to empirically investigate the extent to which website hosts try to foster strong passwords during online account creation. This research is important because it highlights potential vulnerabilities that persist in online account creation. In addition, it proposes a scorecard approach for rating how closely sites follow authoritative guidance regarding strong passwords. Together this builds a foundation for suggesting specific ways both end users and online hosts still may need to close the gap between being aware of simple cybersecurity hygiene and actually putting it into practice.

The remainder of this paper is organized as follows. Section II presents background information regarding the prevalence of weak password use and authoritative password guidance. Section III explains methodologies used for the experiment. Section IV discusses findings from data analysis. Section V suggests some recommendations for remedying password compliance gaps. Section VI summarizes the paper and suggests ways to build upon this work.

II. BACKGROUND

A. Problem Scope

Several studies have shown how a random sample of dictionary attacks alone was able to break up to 24 percent of tested passwords [4][5][6]. There are between 12 and 24 million ecommerce sites across all business segments [2]. Extrapolating such historical findings across every ecommerce account ever created implies virtually every internet user is highly likely to have data at risk via credential breaches.

A survey of over 1000 individuals conducted by the security giant Avast concluded that 83 percent of all users are using weak passwords [7]. Troy Hunt, a world-renowned

expert on security and data breaches, hosts a website where he has collected over half a billion passwords that have appeared in known data breaches. Among his most alarming discoveries: in just one breach involving 6.8 million records, 71 percent of those passwords were already in the database of compromised passwords he had compiled [8].

According to a recent Verizon Data Breach Investigation Reports (DBIR), every industry category they track has experienced an incident in which password cracking via brute force attack enabled the breach. In fact, the DBIR has cited stolen or compromised credentials as the top cause of all data breaches for many years [3]. In other words, users continue to create weak, easily cracked passwords.

B. Authoritative Password Guidance

In 2019, the National Institute of Standards and Technology released Special Publication (SP) 800-63-3 which outlines new recommendations for authenticating users to combat this significant vulnerability in the account creation process. The SP builds on findings over several years to overturn previously accepted best practices, replacing them with a new gold standard. As shown in Table I, it lays out nine main points that should be considered when creating password policies with an eye toward security and robust authentication [11].

TABLE I. NIST PASSWORD GUIDANCE

Attribute	***Criteria***
Length	Minimum of 8 when selected by a human; 6 when assigned by a system or service; maximum of 64 should be allowed.
Character types	All ASCII characters, including spaces, should be allowed.
Truncation	Shortening of passwords should never be implemented.
Screening	Checking proposed passwords against dictionaries of commonly used, easy-to-guess passwords is recommended.
Complexity	Requiring complexity criteria must be met is not recommended.
Lockout	Locking the account after a set number (e.g., 10) of failed login attempts is recommended.
Expiration	Requiring users to change their passwords with high frequency is not recommended.
Knowledge-based authentication	Hints and security questions to retrieve or reset forgotten passwords are not recommended.
Two-factor authentication (2FA)	Short Message Service (SMS)-based approaches are not recommended; one-time rotating password applications are acceptable.

C. Motivation for Study

Despite an abundance of authoritative password guidance, users continue to compose weak passwords and to reuse passwords across multiple online accounts, offering a ubiquitous attack surface for cyber criminals. This observation motivated interest in empirically determining the extent to which websites that invite users to create accounts encourage or require them to create strong passwords or to engage in better password management practices in alignment with NIST guidance.

III. METHODOLOGY

This project inspected the account creation process for a statistically significant number of websites that invite visitors to create password-protected accounts. The overall experiment included the following five procedural elements.

A. Sample Population Selection

The DBIR rank-orders 21 industries according to the number of reported data breaches, malware attacks, and other cybersecurity incidents [3]. From that list, nine (9) of the most frequently breached industries were selected: Accommodation, Education, Finance, Healthcare, Information, Manufacturing, Professional, Public, Retail. Then, based on industry definitions, keywords were chosen and used in the Google and Bing search engines to discover industry-relevant websites that feature an account creation process. It should be noted for the Manufacturing industry, the existence of a process for creating an account to apply for a job was deemed acceptable, based on the assumption that the password policies used by human resources (HR) would be consistent with the password policies of the company at large.

By choosing 10 to 15 websites in each of these nine categories, data ultimately were collected from 108 sites. Since the number of websites on the internet is extremely large, this sample size supported statistical calculations accurate to within 10 to 12 percent of the overall population statistics with high confidence.

B. Volunteer Recruitment

Due to time constraints, four student volunteers were recruited from the Computer Science Department at Norfolk State University to help with data collection..

C. Script and Video Creation

A script was created to standardize the collection of experimental observations in comparison with NIST guidance. To the maximum extent practicable, the script focused on data collectors responding to a series of yes/no questions while they created a user account on each selected website, with just a few “fill-in-the-blank” answers. The resulting script is shown in Fig.1. In addition, two instructional videos were created to explain the data collection process and the use of the script to student volunteers.

Step	Finding the Account Setup	
1	Navigate to _____ website.	
2	Search for method to sign in / create account.	
3	Fill out all required information except for the password. Continue to the password data collection portion.	
	Password Data Collection	
4	Are you given guidance on the requirements for a password before entering one?	Yes / No
5	Enter "1 " as a password (no quotations with a space after). Are you now given the requirements for a new password?	Yes / No
6	Is there a minimum character length? If so, what is it?	*Insert min character length*
7	Does the password require a mix of upper and lower case characters?	Yes / No
8	Does the password require special characters?	Yes / No
9	Are the special characters that are allowed listed?	Yes / No
10	If so, what special characters are allowed?	"Insert special characters*
11	Try to use a space as the password. Are spaces allowed?	Yes / No
12	Enter in the password "um1234" (no quotation marks). Does it let you continue?	Yes / No
13	Enter in the password "P@ssw0rd" (no quotation marks). Are you allowed to continue?	Yes / No
14	If you are not allowed to continue, enter in any robust password that meets the criteria required.	
15	Are you required to prove you are human? (Captcha?)	Yes / No
16	Were you at any point prompted to create security questions?	Yes / No
17	Where you at any point prompted to create a password hint?	Yes / No
18	Where you at any point prompted to sign up for two factor authentication (e.x. receiving a code on your phone)?	Yes / No
19	Proceed to Lockout Policy portion.	
	Lockout Policy	
20	Log out of the account you created and return to the login screen.	
21	Attempt to login with the incorrect password.	
22	Are you given a message that your account will be locked out after "X" number of attempts?	Yes / No
23	If so, how many attempts? Skip to #25.	*Enter number of attempts until account is locked out*
24	Attempt to login with the incorrect password a total of 10 times. Were you at any point told that the account was locked out?	Yes / No
25	Click forgot password / reset password. Does it require you to answer an email to reset?	Yes / No
	How does the site require you to reset the password?	*Insert Description*
	End of Questionnaire	

Fig. 1. Data Collection Script

D. Data Collection and Validation

Each volunteer was provided a unique subset of websites drawn from the sample, and instructed to watch the two instructional videos before collecting data. Data collection involved visiting each site to create an account while following and answering the script questions. Sample data sheets were spot checked later to ensure collection procedures had been followed. Minor inaccuracies were found on just two sheets, informally validating the repeatability of the data collection process and the accuracy of the volunteers' efforts.

E. Calculations and Inferences

Collected data were consolidated and summarized to support analysis, comparing results across industries, and to highlight significant trends. These findings and insights are discussed in the next section.

IV. ANALYSIS AND FINDINGS

The analysis goal for this project was to make inferences from the collected data, with a confidence interval of 95 percent, and a margin of error of about 10 percent. This means, the figures calculated based on the sample of websites should deviate no more than +/- 0.1 from those of the entire population of similar websites on the internet.

A. Scorecard Development

An objective method for assessing websites based on their adherence to NIST standards was required for analysis. The data collection script and NIST SP 800-6-3 were used as the basis for creating a scorecard that measures the extent to which each website's respective password policies comply with the standard. The resulting scorecard is shown in Table II. Adding together the scores earned for each variable produces the overall "compliance" score for a website, where a higher score indicates the website follows the NIST standard more closely.

TABLE II. SCORECARD VARIABLES AND MEANINGS

Variable	*Policy Category*	*How to Score*
Char Min	Minimum length enforced	0: < 8 characters allowed 1: otherwise
Char Type	All ASCII characters plus space allowed	0.5: Spaces allowed (Char Type1) 0.5: Allowed special characters not listed (Char Type2)
Passcheck	Easy-to-guess passwords excluded	0: Neither easy password allowed 0.5: "um1234" allowed (Passcheck1) 0.5: "P@ssw0rd" allowed (Passcheck2) 1: otherwise
Complexity	Complexity ignored	0.5: Upper/lower case mix required (Complexity1) 0.5: Special characters not required (Complexity2)

Variable	*Policy Category*	*How to Score*
Acct Lockout	Lockout enforced	0: No lockout 0.5: < 10 attempts before lockout 1: 10 attempts before lockout
Pass Hint	Password hints excluded	0: Yes 1: No
Sec Quest	Knowledge-based authentication excluded	0: Yes 1: No
2FA	SMS-based two-factor authentication excluded	0: No 1: Yes

Inspecting the "How to Score" column reveals that scorecard categories can earn a score ranging from 0 to 1. The net minimum score for a website is 0, meaning the website follows none of the corresponding criteria. The net maximum score is 8, meaning the website follows all criteria perfectly. The complexity, character types and password checking facets were inspected via two questions and therefore were tracked using dual variables: Complexity1, Complexity2; Char Type1, Char Type2; and Passcheck1, Passcheck2. This was done to account for situations where NIST requirements might be only partially met, with each facet in a pair contributing up to 0.5 towards the total category score.

B. Data Aggregation

The first step in analysis was to group together scorecard data for all websites within a given industry category. This produced nine tables, one for each industry. (NOTE: These individual industry tables are not included in the paper due to space constraints.) Each table had columns for the website name, its overall compliance score, and the scores earned for each of the inspected variables (compliance facets). In other words, each row in each such table summarized the compliance scores for one inspected website.

Per-category scores were then averaged and summarized in a chart as shown in the Fig. 2, then finally interpreted into percentages as shown in Fig. 3. The relationship between these two charts is easiest to understand by looking at an Accommodation industry example (first row in both figures).

- In Fig. 2, the Total Score within that row is 5.96, or 75 percent of the maximum possible score of 8 (that is, 5.96 / 8.0 * 100.0) as recorded in the corresponding Fig 3 chart position.
- For two-part criteria, the value pairs for component variables are combined first. Reading from Fig. 2, the sum of Complexity1 and Complexity2 (0.29 and 0.34) yields 0.63, or 63 percent of the potential maximum of 1 as shown in the corresponding Fig. 3 entry.

Site Industry	Total Score	Char Min	Complexity 1	Complexity 2	Char Type 1	Char Type 2	Passcheck 1	Passcheck 2	Sec Quest	2FA	Acct. Lockout
Accomodation	5.96	0.79	0.29	0.34	0.46	0.21	0.39	0.08	0.95	1.00	0.45
Education	5.89	0.42	0.50	0.47	0.50	0.47	0.21	0.08	1.00	1.00	0.24
Finance	6.03	0.70	0.30	0.40	0.48	0.40	0.40	0.15	1.00	0.70	0.50
Healthcare	5.70	1.00	0.20	0.10	0.50	0.10	0.50	0.00	0.80	1.00	0.50
Information	6.13	0.60	0.40	0.45	0.48	0.45	0.30	0.10	1.00	1.00	0.35
Manufacturing	5.88	0.90	0.20	0.20	0.43	0.10	0.45	0.15	0.80	1.00	0.65
Professional	5.98	0.43	0.43	0.46	0.48	0.46	0.21	0.11	1.00	1.00	0.39
Public	6.19	0.75	0.38	0.38	0.44	0.38	0.38	0.13	1.00	0.75	0.63
Retail	5.88	0.41	0.41	0.47	0.50	0.29	0.29	0.06	0.94	1.00	0.50
Total	**5.949**	**0.611**	**0.366**	**0.394**	**0.477**	**0.333**	**0.324**	**0.093**	**0.954**	**0.963**	**0.435**

Fig. 2. Average Compliance Scores

Site Industry	Total Score	Char Min	Complexity	Char Type	Passcheck	Sec Quest	Pass Hint	2FA	Acct. Lockout
Accomodation	75%	79%	63%	67%	47%	95%	100%	100%	45%
Education	74%	42%	97%	97%	29%	100%	100%	100%	24%
Finance	75%	70%	70%	88%	55%	100%	100%	70%	50%
Healthcare	71%	100%	30%	60%	50%	80%	100%	100%	50%
Information	77%	60%	85%	93%	40%	100%	100%	100%	35%
Manufacturing	73%	90%	40%	53%	60%	80%	100%	100%	65%
Professional	75%	43%	89%	95%	32%	100%	100%	100%	39%
Public	77%	75%	75%	81%	50%	100%	100%	75%	63%
Retail	74%	41%	88%	79%	35%	94%	100%	100%	50%
Total	**74%**	**61%**	**76%**	**81%**	**42%**	**95%**	**100%**	**96%**	**44%**

Fig. 3. Percent Compliance Scores

C. *"Internet-wide" Observations*

Keep in mind the statistical assumption that the overall compliance scores observed for the sample in this experiment – shown in the last or "Total" row in the Fig. 3 chart – are indicative of what can be expected for typical similar websites on the internet. Key observations are summarized in the next section. A few quick examples will help understand how to scrutinize and reason from the tabularized data to the trends noted there.

The Acct Lockout variable (column) shows a Total compliance score of just 44 percent in Fig. 3. This means that nearly half the time a randomly selected website that supports the creation of user accounts will not feature account lockout. On the other hand, a perfect score of 100 percent in a compliance variable, such as Pass Hint in Fig. 3, means no sampled website asked the user to create a password hint; therefore, statistically, it is reasonable to expect typical websites on the internet will not do so either. By contrast, while the overall average Passcheck variable in Fig. 3 implies that nearly half of all websites (42 percent) can be expected to comply with NIST, the tiny Passcheck2 score shown in Fig. 2 indicates very few of the sample sites – and by statistical extension many internet sites at large – reject a password like "P@ssw0rd" as being too weak.

When averaged across all variable categories, all selected industries performed similarly, scoring around 70 percent. The best performing industries were Information and Public, while the worst was Healthcare; but even these verticals differed from averages by only a few percentage points.

D. *"Per-industry" Observations*

While drawing conclusions about websites in general is statistically reasonable, recall the sample sizes for individual industries (generally 10 or fewer) are too small to draw statistically significant conclusions about their respective vertical's password policy trends. Still within industries it is interesting to note which compliance scores dominate within or stand out in a remarkable way compared to others. These details are summarized in Table III as food for thought and to suggest possible future investigations.

TABLE III. PER-INDUSTRY OBSERVATIONS

Industry	***Anecdotal Observations***
Accommodation	**Best:** Char Min (79%), Sec Quest (95%), 2FA (100%) **Worst:** Acct Lockout (45%), Passcheck (47%) **Comments:** Concerning due to financial information likely stored on such websites.
Education	**Best:** Complexity (97%), Sec Quest (100%), 2FA (100%) **Worst:** Char Min (42%), Acct Lockout (24%), Passcheck (29%) **Comments:** Susceptibility to brute force attacks puts learner and employee personally identifiable information (PII) at risk.

Industry	*Anecdotal Observations*
Finance	**Best:** Char Type (88%), Sec Quest (100%) **Worst:** Acct Lockout (50%), Passcheck (55%) **Comments:** Trending toward 2FA adoption industry-wide, despite this being contrary to NIST guidance.
Healthcare	**Best:** Char Min (100%), Sec Quest (100%) **Worst:** Complexity (30%), Acct Lockout (50%), Passcheck (50%) **Comments:** Prevalence of weak passwords and absence of lockout are worrisome for healthcare information security.
Information	**Best:** Char Type (93%), 2FA (100%), Sec Quest (100%) **Worst:** Acct Lockout (35%) and Passcheck (40%) **Comments:** Susceptible to brute force attacks.
Manufacturing	**Best:** Char Min (90%), 2FA (100%) **Worst:** Char Type (53%), Complexity (40%), Passcheck (60%) **Comments:** Potential industrial espionage may drive more stringent password policies
Professional	**Best:** Char Type (95%), 2FA (100%), Sec Quest (100%) **Worst:** Char Min (43%), Acct Lockout (39%), Passcheck (32%) **Comments:** Low compliance in key categories may indicate brute-force susceptibility.
Public	**Best:** Sec Quest (100%) **Worst:** Passcheck (50%) **Comments:** No obvious trends due to small sample.
Retail	**Best:** Complexity (88%), Sec Quest (94%), 2FA (100%) **Worst:** Acct Lockout (50%), Char Min (41%) Comments: Desire to encourage "frictionless" online sales may drive weaker compliance choices.

E. Limitations

There were a number of limitations on the execution of this research that are important to keep in mind. The first limitation was a general lack of current research on the password policies of websites that feature account creation. Most research around password policy is based on the human element, such as trying to crack a random sample of passwords, or looking at users' behavior when choosing passwords. While this is helpful, it does not provide the sort of insights this study sought regarding the extent to which websites implement robust password policies. Just one research abstract was uncovered that looks at the password policies of different online retailers over a 10 year period [12]. The lack of published literature on this topic makes it difficult to compare this work to that of past researchers except to say this particular angle appears to be largely unexplored.

A second limitation was the number of websites analyzed. There are millions of websites on the internet today. To make investigating password policies practicable requires relying on the power of statistics. The sample size in this research (just over 100) – while sufficient to make holistic inferences across the totality of industries examined – is insufficient to draw any definitive conclusions about individual industries (which would require around 100 samples per each industry).

A third limitation was the selection of sample websites. The selection methodology used is best described as "pseudo-random." Using a search engine guided by keywords introduces some bias, such as popularity or other proprietary factors imposed by the search algorithm that may prioritize some matches over and above proximity to search terms.

V. SUMMARY AND RECOMMENDATIONS

There are a number of notable observations when looking at the collected and analyzed data through the lens of NIST password policy compliance, which in turn suggests many opportunities for improvement.

A. Summary of Observations

- Nearly all websites (greater than 95 percent) followed the modified NIST guidance for avoiding the use of security questions and SMS-based 2FA.
- The majority of websites (76 percent) have adopted NIST guidance regarding password complexity and allowed character types.
- More than half of websites (61 percent) enforced minimum length in password creation.
- More than half of websites (59 percent) had an account lockout policy.
- Relatively few websites (19 percent) forbade the use of a naïve value like "P@ssw0rd" as an account password.

While most of these statements sound positive, each one must be compared to its complement. That is, based on these findings we can expect:

- Around half of all websites do not enforce minimum password length and do not have an account lockout policy.
- About one in every three websites is not following NIST's complexity or character type guidance.
- Many websites (greater than 80 percent) still deem "P@ssw0rd" an acceptable password.

- A few websites still cling to security questions and SMS-based 2FA.

Remedying these NIST compliance gaps should be a focus for future improvements.

Sample sizes were too small to draw any statistically significant conclusions about websites' password policies within individual industry categories. However, the per-industry observations offered earlier may suggest interesting angles for future in-vertical investigations.

B. Recommendations

Based on the findings of this investigation, significant weaknesses remain within account creation practices on many websites with respect to requiring hard-to-crack passwords. One technical solution is to create a NIST-compliant user registration and profile manager plugin that developers can use seamlessly across websites. A plugin approach creates consistency and takes the guesswork out of adopting secure password policies. WordPress already has several plugins that do something similar to this; however, they are not fully compliant with NIST guidelines [13].

The wide adoption of password manager tools has been hindered by user-friendliness challenges [9]; however, such technology has the potential to encourage stronger password use on all websites. It is incumbent upon the producers of this technology to routinely perform usability tests to make it easier for average users to navigate. Such tools themselves also must enforce strong password policies, since the master key represents a single point of failure in most password managers [10].

A final recommendation is to enforce tougher legal consequences for the owners of breached sites or tool vendors that contribute to the compromise of users' personal information and consequent damages. As one example, Brassring's weak password policies despite its broad adoption in many industries is an example of this careless behavior. If there is no potential for repeated or potential breaches to negatively impact their profits, there is no incentive for responsible parties in any industry to purposefully harden their account creation processes, nor to invest in eliminating other vulnerabilities in their infrastructures.

Presently, a U.S. company that has suffered a data breach – whether the root cause is weak password policy or some other vulnerability – is required to: notify all affected individuals as soon as possible; act upon their security incident response plan; and may incur penalties depending on the severity of the breach. There is no U.S. federal law in place yet, and various jurisdictions have different expectations and fines. So leveling legal consequences nationwide and enacting federal legislation to hold organizations accountable – with stiff fines for infractions – appear to be next logical steps.

VI. CONCLUSION AND FUTURE DIRECTIONS

This research sought to provides insights about the state of password policy creation and enforcement with respect to prevailing "best practices" from an authoritative source (i.e., NIST) across many industries' websites internet-wide. This section summarizes conclusions and suggests some ways to build upon findings.

A. Conclusions

This project used the Verizon DBIR as a starting point to identify industries with the largest number of cybersecurity incidents. Data were collected from 108 randomly selected websites within nine industries known to exhibit a high frequency of cybersecurity incidents. A few volunteer graduate students "crowd sourced" data collection efforts, guided by instructional videos and a step-wise script. Eight variables were created to represent specific aspects of NIST SP 800-63-3 guidance on credentials (passwords), along with a scorecard for assessing each site's compliance with them. Scores were aggregated to glean statistical insights about websites internet-wide. Some potential trends were remarked within industry verticals; however these sample sizes were too small to have statistical significance.

Generalizing from the analysis, many websites that allow users to create accounts on them still do not enforce a minimum password length; nor do they forbid common, easily hacked passwords; nor do they have any account lockout policy. That is, these sites remain susceptible to brute force attacks. Industries with the lowest levels of compliance to NIST password policies were Healthcare, Retail, and Manufacturing. It was noted, however, that all industries scored in the 70 to 80 percent range overall, meaning "on average" they are complying with most NIST password policy guidance.

B. Future Directions

To build upon this work, more extensive data collection would be needed. In particular, to draw conclusions within specific industry categories requires a sample size of 100 or more per vertical. The experiment also should be repeated with multiple randomly selected website data sets to confirm repeatability. Because this study focused on choosing websites from industries with a high historical incidence of breaches, a complementary investigation might instead choose low-reporting industries to determine whether results correlate to higher compliance with NIST guidance.

Observing additional credential attributes based on NIST standards and factoring them into the scorecard and analysis could reveal more insights too. For example, a variable "Allow Paste" could inspect whether users are able to copy/paste a value into the password bar, since some password managers rely on this behavior for logging into accounts on behalf of the user. NIST guidance also states that a password must be between 8 and 64 characters long [11]. This project only scrutinized the minimum length requirement, since shorter passwords are easier to crack. So adding a "Char Max" variable to the scorecard to check for maximum length compliance could yield interesting new results.

REFERENCES

[1] Salesforce, "Trends in Customer Trust," 2018, https://www.salesforce.com/content/dam/web/en_us/www/documents/briefs/customer-trust-trends-salesforce-research.pdf

[2] Branka Vuleta, "Ecommerce Statistics," 2021, https://99firms.com/blog/ecommerce-statistics/

[3] Verizon Enterprise Solutions, "Data Breach Investigation Report," 2020, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[4] Matteo Dell'Amico, P. Michiardi and Y. Roudier, "Password Strength: An Empirical Analysis," 2010 IEEE International Conference on Computer Communications, 15-19 March, 2010, San Diego, California, doi: 10.1109/INFCOM.2010.5461951

[5] R. Staff, "Hackers attack 20 million accounts on Alibaba's Taobao shopping site," 2020, https://www.reuters.com/article/us-alibaba-cyber-idUSKCN0VD14X/

[6] PCRisk, "2,000 Magento Stores Hacked in one Weekend," 2020, https://www.pcrisk.com/internet-threat-news/18842-2000-magento-stores-hacked-in-one-weekend/

[7] Avast, "83% of Americans are Using Weak Passwords," 2019, https://press.avast.com/83-of-americans-are-using-weak-passwords/

[8] Troy Hunt, "86% of Passwords are Terrible (and Other Statistics)," 2020, https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/

[9] Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. "A Usability Study and Critique of Two Password Managers," 15th USENIX Security Symposium, July 2016, https://www.usenix.org/conference/15th-usenix-security-symposium/usability-study-and-critique-two-password-managers/

[10] Jeff Mlakar, "Why You Should Use a Password Manager - The Pros and Cons of Password Management Systems," 2019, https://www.mlakartechtalk.com/why-you-should-use-password-manager-pros-cons-password-management-systems/

[11] National Institute of Standards and Technology, Special Publication 800- 63-3: Digital Identity Guidelines, March 2020, https://doi.org/10.6028/NIST.SP.800-63-3

[12] Steven Furnell, "Assessing website password practices – over a decade of progress?," Computer Fraud & Security, Volume 2018, Issue 7, 2018, Pages 6-13, https://doi.org/10.1016/S1361-3723(18)30063-0

[13] CozmosLabs, "User Registration & User Profile – Profile Builder," 2021, https://wordpress.org/plugins/profile-builder/