**ABSTRACT**

Passwords remain the most common form of user authentication that we use in our everyday lives. As attackers use ever more sophisticated methods and techniques in an endeavor to crack passwords, it is imperative that users are able to formulate passwords which are strong and secure. The most common tool to assist with this is the strength meter, prevalent in a large number of websites. However, the exact implementation of these password meters can vary greatly, potentially confuse the user, and may not effectively evaluate how secure a password might really be. We will be attempting to examine if these password meters are in fact truly effective in their goals of helping users to select a password that is secure.

**1 PROBLEM**

We use passwords to protect the information we store on various web services, ranging from our social media accounts to the sensitive data found in our bank accounts. However, users of such websites may not always be aware of what a strong password may be, or may have no motivation to create one as long as they are able to immediately access these services. It then becomes the task of these websites to aid such users in formulating secure passwords to help protect them against possible threats to their information stored online. They commonly use password strength meters to do so. These are often the coloured bars that provide visual feedback to a user where in the range of “weak” to “strong” their proposed password lies. They are often accompanied by a set of guidelines of what a password should be comprised of. A number of studies have been conducted in the past to assess the integrity and efficacy of these password meters. In 2014, de Carnavalet and Mannan conducted a large-scale analysis of the password meters of high-profile websites, they concluded that such meters are “highly inconsistent, fail to provide coherent feedback, and sometimes provide strength measurements that are blatantly misleading.” [1] Wang and Wang in 2015 conducted a similar empirical analysis of the password policies of 50 leading web services, and found that they provide “highly inconsistent outcomes” under identical testing, and that they “largely fail to withstand online guessing attacks.” [2] Moreover, in a paper by Ur *et al*., while they found that these meters do affect user behaviour, they state that “the resulting passwords were only marginally more resistant to password cracking attacks.” [3] It is therefore apparent that there is a serious problem among these password strength meters, in that they vary greatly in their implementation, provide incoherent or confusing feedback, and that they may not actually be correctly assessing the strength of a password. These findings weaken the purpose of these password meters. This poses an alarming security risk, as this can allow individuals to have the wrong perception of what a secure password is, and thus, with the ever growing number of threats and attacks happening among various websites today [4], individuals may therefore be more susceptible to password cracking and guessing attacks, and leaks of personal information may become more prevalent. Therefore, with a constantly growing online world, it is relevant to analyze and reassess these password meters to see if there have been changes made in increasing their integrity and security, and if they are indeed the effective tools they ought to be.

**2 APPROACH AND ANTICIPATED RESULTS**

**2.1 Proposed Approach**

We will repeat and extend upon the empirical analyses and studies on the password strength meters of many popular websites, as found in the cited papers and research studies above. To perform our analysis, we will first choose a number of popular, high-profile websites to work with (as based on their rankings from *Alexa Internet*, which ranks web pages according to their web traffic over three-month periods). We aim to select a diverse list of websites, encompassing different areas ranging from social networks to online retailers, so that our study will be representative enough of the large number of web services available today. We will utilize pre-existing leaked passwords to conduct our tests (such as those released by Mark Burnett from 2015 [5]). This will allow us to use real passwords from real individuals, and in doing so, we can ensure that the tests we are performing are emulating real-world scenarios and real user behaviour as much as possible. To conduct our tests and analyses, we will build upon and use the techniques and tools used by de Carnavalet and Mannan, Wang and Wang, and Ur *et al*. on the password meters of our selected websites. These may include: the analysis and comparison of the password meters’ outward-facing characteristics, policies and guidelines, a test to verify if they use any blacklists, an analysis of the algorithms they use, or even emulating online guessing attacks, among several. Then, as an extension of these studies, we will propose and formulate our own technique or tool to assess the efficacy and integrity of these password strength meters. We will also make sure to use any regulations produced by the National Institute of Standards and Technology (NIST), such as those found in the *Guide to Enterprise Password Management*, which published recommendations for the protection and confidentiality of passwords [6], so that our tests and analyses will abide by the standards set by the security industry. Finally, we will compare our results to those of the original studies.

**2.2 Anticipated Results**

By the end of our study, we expect to be able to verify if the password strength meters among many high-profile web services are indeed effective tools in providing security (i.e., if they are actually helping users in creating more secure passwords). We also expect to be able to list any vulnerabilities or threats that are present in their implementations, as well as any notable weaknesses they may possess, and the possible inconsistencies in the resulting assessments they provide of an individual’s desired password. Furthermore, with our findings, we aim produce a list of standard but minimal list of requirements of what is needed to be able to create an effective password strength meter, which these websites can use. However, despite this, it should be noted that every password meter should still have some distinction from other meters, as having one set of rules or requirements of how these meters should operate will only make the lives of attackers easier. In the end, we expect that our findings will aid in further improving the integrity and security of these existing password meters, and thus allow them to be the effective tools that they are required to be.

**3 RELEVANCE TO THE COURSE**

This project is relevant to the course as it falls under the scope of: (1) *software security*, since, through this, we will be able to pinpoint any vulnerabilities that password meters may possess as a result of poor implementation and development choices, or if any tools or algorithms were improperly utilized, and thus be aware of any exploits attackers may use to compromise the security of various websites; and (2) *authentication* (and, in a way, *access control*), since the use of passwords is very common in regulating the access of various resources. With this project, we expect to learn what constitutes a good password, and thus be able to properly study and critique the tools and techniques used in assessing the efficacy of password meters. To do so, we will have the chance to use common security evaluation standards, such as those promulgated by NIST, and thus use them to review the security standards followed by the password meters we will be analyzing. Thus, we will also be made aware of the current techniques that attacks may be using today to compromise the security of various systems. Indeed, these aforementioned goals match those found in the learning objectives for this course.

The proposal shall address the following questions:

* **What is the context of your project? (In other words, describe enough background to help the instructor understand the project topic.)**
  + Use same intro from proposal
    - We use passwords everyday for everything
    - Attackers consistently using more advanced techniques to crack passwords and do online guessing attacks of passwords/databases
    - Password meters and policies are prevalent among many websites
    - Should help guide users into creating stronger passwords, BUT this may not be true according to research (insert research here):
      * Password meters are highly inconsistent—provide incoherent feedback that may confuse users
      * Not well implemented
      * . . .
* **What is the (research/technical) problem the project attempts to address? Why is it significant?**
  + *The password meters, policies or guidelines of popular, high-profile, high-traffic websites are highly inconsistent, give incoherent feedback and/or are not well-implemented*. This poses a great security risk for the many users of these web services since: (1) this can lead to users creating weak, unsecure passwords, or (2) it may give users the wrong perception that the passwords they are creating are strong or secure enough, and, most importantly, (3) it becomes easier for attackers to guess and crack these users’ passwords. It would therefore be pertinent to re-analyze and scrutinize the efficacy of password meters deployed by a few selected popular websites, as there has been noteworthy growth in the online world, with the massive growth of social media and online businesses.
* **What approach is proposed to address this problem?**
  + Choose *n* websites to work with, as based on their Alexa rankings and web traffic, choosing a variation of websites that encompasses different fields (?) (e.g., email, social network, online retailer, messaging, etc.)
  + Use pre-existing lists of leaked passwords, dictionaries of common passwords, etc.
  + Use techniques/analyses from other papers to test and analyze efficacy of pw meters and compile them together in a new empirical analysis
    - Analysis of algorithms they use?
    - How prone they are to online guessing?
    - Comparison of characteristics/policies/guidelines
    - Test against blacklists?
  + Formulate our own way of testing and comparing pw meters
* **What are the anticipated results?**
  + Be able to tell how effective pw meters are, if there inconsistencies among them that could lead to vulnerabilities and threats to the system they're protecting (e.g., highly inconsistent strength outcomes for the same password in different meters), and that our findings may help in improving existing meters, and possibly make them an effective tool in the long run.
  + Produce a standard list of minimal requirements for creating an effective password meter and their accompanying set of policies/guidelines based on our findings
  + However, we want to assume that every pw meter should have some distinction from other meters, since a uniform pw meter would have great security risks.
* **Why is the project topic relevant to this course? Do so by identifying the expected learning experiences generated by the project, and arguing that they match the learning objectives of the course.**
  + Software Security: **The vulnerabilities (and corresponding exploits that are due to the poor construction of a piece of software.** Such vulnerabilities may be due to deficiencies in the development process, programming practices, programming languages, tools and compilers, or software design and architecture. Also relevant will be tools or practices that can prevent the injection of vulnerabilities into a software in the first place.
    - If algorithms of pw meters are designed properly (what we are testing)
    - If there's some vulnerability in the tools and algorithms used in the construction of password meters, it could lead to potential attacks
    - Also relates to how the software interface of pw meters are designed that could lead to potential vulnerabilities (e.g., showing too much guidelines in pw creation)
  + Access Control: One of the core issue in application-level security is access control: the articulation of policies for regulating the access of resources, and the design and implementation of mechanisms for the enforcement and articulation of such policies.
    - Relates to authentication and access control—use of passwords is very common in regulating the access of various resources
* arguing that they match the learning objectives of the course.
  + By the end of the course, the student should demonstrate the operation of common access control mechanisms in operating systems, among others
  + students should be able to critique an arrangement of protection mechanisms, or a system, or program logic
  + **By the end of the course, students should be able to list common static analysis techniques and tools and demonstrate the ability to run such tools on real, large software code Students should also be able to list common (e.g., NIST) security evaluation standards; the advanced student will be able to list specific evaluation criteria from the appropriate model.**
  + **By the end of the course, students should be able to use their knowledge of evaluation standards**, the Security Mindset, and **analysis tools to produce a security review of a product**, protection technique, or security mechanism.