**Reviewer Report of Rethinking Passwords, by William Cheswick**

**Summary:**

Authentication is needed for all types of accounts with a multitude of service providers, with the most widely used type of authentication being passwords. For password based authentication the U.S. Governemnt produced a book of guidelines in 1985 called The Password Management Guideline—commonly referred to as *The Green Book*—which is the basis for current password rules. Cheswick refers to these rules as *eye-of-newt* password rules. At the time of publishing the rules were solid but have since grown dated with the lack of revisions, some rules hold up, others do not. *The Green Book* was written under multiple old assumptions that do not apply to the modern internet. This is why Cheswick’s article is significant, it brings attention to the dated standards of old. One of the most egregious examples of this is the assumption that users will have few accounts that require authentication, while its common in the modern internet to have multiple dozens.

Some of *The Green Book*’sadvice holds up. This advice includes: users should have the ability to change their passwords; users should have access to authentication audit reports; users should enter their password at authentication time—though this rule should be updated to include 2-factor authentication; and that the best passwords are machine generated. *The Green Book* also includes a plethora of bad advice such as: the user should remember their passwords—which is just not reasonable considering the number of accounts the average user has; users should periodically change their passwords—most users can not create and remember good passwords when it has to be periodically changed; and that the way to recover from a compromised password is to just change it, which is just not the case anymore. Once that password is compromised any other account that uses the same password is also considered compromised.

Cheswick utilizes a table of root processes to show that once a password is compromised any one root process could lead to a compromise of an entire system, giving attacks access to anything on that system. Another graphic Cheswick uses is a table measuring how long a password would take to crack through a dictionary attack with common password lengths, alphanumeric and *eye-of-newt* style, at 7 billion guesses/second and 10 million guesses/second. The purpose of the table is to show that the most important element of a password is its length, not a utilization of the *eye-of-newt* rules. The goal of Cheswick’s article is to demonstrate that password standards do not hold up on the modern internet. Overall the article is well done. The structure and organization is good but needs some work on clarity in the section about dictionary attacks. The conclusion that *eye-of-newt* standards are dated and ought be improved is properly supported by outlining old assumptions that do not apply to the modern internet.

**Comments:**

1. Under the suggestions section Cheswick states that their should be more authentication options but does not provide any. Cheswick should provide an alternative to strengthen the point.

2. The article is well structured, the transitions between points are smooth and build off eachother.

3. There needs to be more clarity surrounding the point of addressing dictionary attacks. The article should clearly state that the point of the table is to show that the most important aspect of a password is its length, not if it follows *eye-of-newt* rules. Currently the point in the article is up to unneeded interpretation and some clarity would be helpful to the broader point.

4. The tables have a nice style, but the resolution is too low. If the graphics were displayed on a larger screen or were zoomed on they would be pixelated.

**Recommendation:**

I recommend this article be publihed after minor changes outlined in the comments to improve clarity and readability.