

Homework: Passwords

Jackson Mowry

Tue Oct 28 13:55:46 2025

Offline vs Online Chasm

The most interesting takeaway from the paper for me was the chasm that exists between online and offline attacks. I was already familiar with the different modality of each attack, but this chasm is a new concept to me. I found it interesting how the researchers suggested that no effort need be spent to improve a password's guess resistance unless it can be improved above the offline guess rate. This fact suggests that as long as the most basic of passwords can be eliminated there is a strong argument that most passwords should be secure. In addition, this also suggests to me that the actual length of a password need not be incredibly long, as long as the relatively short password is sufficiently strong.

Reducing User Burden

Blacklisting passwords was not a concept that I was familiar with. The process sounds both frustrating as a user and cumbersome as a site administrator. On the other hand, as I stated in the previous point, if we can eliminate the most basic of password we can cross the line of online attack resistance, leading to far fewer passwords being crackable in an iterative attack. The same concept seems to apply to arbitrary restrictions being placed on password composition, which Dr. Ruoti covered previously in Introduction to Cybersecurity. While it may seem at first glance that each user now possessed a more complex password, we have actually just narrowed the search space for a potential attacker. This paper taught me that reducing the ability for a user to pick a "bad" password should be placed as one of the highest priorities.

Password Reuse

Along the same lines as my closing sentence in the previous paragraph, we should seek to make picking strong passwords as easy as possible for our users. The authors call out multiple times that many Tier-1 services allow simple 6-8 digits

pins as the primary authentication method for their platforms. Obviously this puts more burden on the service itself to identify a potentially malicious user and lock them out, but also makes the average user much happier. I've thought many times about a similar concept when it comes to a password manager. If platforms like Windows or macOS were to fully expose access to the cryptographic hardware present on many modern computers more elegant password management systems would be possible. For example having auto generated password that are locked behind other vectors such as biometrics or otherwise. While the passwords themselves are still only as safe as the service they are being used within, we could eliminate that burden from users allowing them seamless access to various services. I believe this is the major selling point behind passkeys as the modern form of authentication.

Question

1. With many more password databases having been leaked since this paper was written, Have any trends been identified when it comes to password composition? What guidance from various authorities has actually been observed in the wild? For example passphrases are commonly suggested, yet has there been an actual rise in their adoption?
2. With the future adoption of passkeys does the problem of password security become less or more of a concern?