Research Seminar: CSC 4112 - Individual Critical review

SC/2020/11691 W S M Fernando

Critical Review: User-Centric Adaptive Password Policies to Combat Password Fatigue

1. Introduction

Despite rapid technological progress, human factors remain a major vulnerability in cybersecurity. Studies show that over 90% of data breaches arise from weak or default passwords [11]. Modern users manage roughly 25 password-protected accounts but only 6-7 unique passwords on average, creating **password fatigue**, plus the **cognitive strain** of recalling multiple complex credentials [33]. The paper by **Al-Slais and El-Medany** [5] introduces the **User-Centric Adaptive Password Policy (UCAPP)** framework to address password fatigue by adapting password complexity to user capability. This review evaluates the framework's conceptual basis, relation to prior work, methodology, and key findings.

2. Summary

2.1. Literature review

Most password policies are rigid, enforcing uniform rules that ignore differences in memory and cognition [4], [16]. UCAPP shifts focus from static enforcement to **cognitive adaptiveness**, using an agent-based model [17] to adjust password difficulty according to the user's cognitive capacity.

Earlier research inspired this approach. Castelluccia et al. [6] and Segreti et al. [22] proposed adaptive password meters, yet these often-frustrated users by limiting freedom. Guo et al. [10] created personality-based recommendations, while Huh et al. [12] improved memorability by letting users modify system-generated passwords. UCAPP advances these ideas by basing

adaptation on measured cognitive factors, **forget rate**, **recall**, and **write thresholds** rather than personality or user preference.

This perspective redefines security as a personalized process that balances strength and memorability.

2.2. Methodology

The UCAPP framework integrates three modules:

1. **PassPAST** gathers demographic data (age, education, literacy) and runs short recall tests to assess memory behavior. Entropy is computed using Shannon's formula [23].
2. **Cognitive Burden Scale (CBS)** combines social and cognitive scores to classify users as **Critical (CU)**, **Typical (TU)**, or **Expert (EU)**. A Naïve Bayes classifier updates profiles as users reset passwords [5].
3. **PassGEN** generates **System-Generated Passwords (SGPs)** suited to each tier. CU receives simpler mnemonic passwords, while TU and EU obtain longer, more complex variants.

This modular design links psychological measurement with adaptive password creation.

2.3. Findings

Preliminary testing showed that UCAPP improved password entropy by 30–40 % for Critical Users and produced high-entropy results for Typical and Expert profiles [5]. For instance, one CU's entropy rose from 37.6 bits to 52.4 bits. Mnemonic passwords were recalled more accurately and imposed a lower cognitive burden than random ones.

These results confirm that user-centric adaptation can strengthen security without sacrificing usability.

3. Critical Evaluation

3.1. Strengths

UCAPP's greatest strength is its explicit inclusion of human factors. The cognitive-behavioral model [17] **targets the underlying cause of weak passwords, memory overload rather than adding arbitrary complexity**. The three-tier profiling ensures inclusivity across ability levels, and the Naïve Bayes learning process maintains adaptiveness over time.

Such personalization could reduce organizational costs tied to password resets and improve compliance [9].

3.2. Weaknesses

However, the framework has notable limitations. The **PassPAST** test can be **gamed**: users may underperform to receive easier passwords [5]. Entropy estimation via Shannon's model [23] may exaggerate actual security, as it ignores social-engineering and dictionary attacks [11].

Moreover, the weighting of social factors (age, education, literacy) is overly broad, relying on self-reporting that may not reflect real cognitive differences [20], [21]. Finally, Critical Users' passwords, though stronger, may still **fall below recommended entropy thresholds**, indicating a **usability-security trade-off**.

4. Conclusion

The **User-Centric Adaptive Password Policy (UCAPP)** framework presents a significant advancement in aligning cybersecurity mechanisms with human cognitive limits. By tailoring password policies through behavioral profiling and adaptive generation, it effectively mitigates ***password fatigue***, the primary usability challenge in authentication systems [33].

However, frameworks such as UCAPP still depend on user participation in cognitive testing and classification, introducing potential manipulation risks and usability overhead. To overcome this reliance, our methodology introduces a **novel pre-hash transformation layer** within the

password hashing pipeline. This **additional layer** mathematically **transforms user passwords into secure, high-entropy representations** before cryptographic hashing. By embedding complexity and unpredictability at the algorithmic level, rather than requiring users to recall or generate complex passwords, the system preserves usability while significantly strengthening resistance to brute-force, dictionary, and rainbow-table attacks.

This approach redefines the usability-security balance. Users can **retain simple, memorable inputs**, while the transformation hashing process ensures cryptographic robustness. In contrast to adaptive frameworks that adjust policy based on human performance, the proposed method **automates adaptation within the cryptographic process itself**, minimizing human dependency and error.

Overall, while UCAPP marks an important step toward human-aligned security design, integrating transformation-based password hashing can provide an additional, system-level defense, achieving both high usability and strong resistance to modern password attacks. This synergy represents a forward path toward sustainable, user-transparent cybersecurity.

References

[1] A. Adams and M. Sasse, "Users Are Not the Enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[4] J. Campbell, D. Kleeman, and W. Ma, "Password Composition Policy: Does Enforcement Lead to Better Password Choices?," *Proc. 17th Australasian Conf. Information Systems*, 2006.

[5] Y. Al-Slais and W. El-Medany, "User-Centric Adaptive Password Policies to Combat Password Fatigue," *Int. Arab J. Inf. Technol.*, vol. 19, no. 1, pp. 55–62, 2022.

[6] C. Castelluccia, M. Dürmuth, and D. Perito, "Adaptive Password-Strength Meters from Markov Models," *Proc. NDSS*, 2012.

[9] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating Human Traits and Cyber Security Behavior Intentions," *Computers and Security*, vol. 73, pp. 345–358, 2018.

[10] Y. Guo, Z. Zhang, Y. Guo, and X. Guo, "Nudging Personalized Password Policies by Understanding Users' Personality," *Computers and Security*, vol. 94, 2020.

[11] T. Halevi et al., “Cultural and Psychological Factors in Cyber-Security,” *J. Mobile Multimedia*, vol. 13, no. 1–2, pp. 43–56, 2017.

[12] J. Huh et al., “Surpass: System-Initiated User-Replaceable Passwords,” *Proc. ACM CCS*, pp. 170–181, 2015.

[16] B. Korbar et al., “Validating an Agent-Based Model of Human Password Behavior,” *AAAI Workshops*, pp. 167–174, 2016.

[17] V. Kothari et al., “Measuring the Security Impacts of Password Policies Using Cognitive Behavioral Agent-Based Modeling,” *Proc. Science of Security Symp.*, 2015.

[20] D. Pilar et al., “Passwords Usage and Human Memory Limitations,” *PLoS ONE*, vol. 7, no. 12, 2012.

[21] C. Rinn et al., “Password Creation Strategies Across High- and Low-Literacy Web Users,” *Proc. ASIS&T Annual Meeting*, 2015.

[22] S. Segreti et al., “Diversify to Survive: Making Passwords Stronger with Adaptive Policies,” *Proc. SOUPS*, 2017.

[23] C. E. Shannon, “A Mathematical Theory of Communication,” *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.

[33] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot, “Revisiting Password Rules,” *Proc. APWG Symp. Electronic Crime Research*, 2016.