عنوان الرسالة :

A Building Model for Enhancing Information Systems Security

بناء نموذج لتعزيز أمن نظم المعلومات

مقدمة إلى قسم علوم الحاسوب كلية الحاسوب وتقنية المعلومات
جامعة صنعاء
كجزء من متطلبات نيل درجة ماجستير العلوم في
علوم الحاسوب

عمل الباحثة:

نوال حمود أحمد حسين هادي

اشراف

أ.د.م عبدالماجد الخليدي

Abstract

In the digital age, password-based authentication serves as a critical safeguard to protect sensitive electronic information systems. However, the challenge is creating strong, easy-to-remember passwords for multiple accounts. Passwords are necessary to protect our personal accounts and sensitive data. As the number of accounts we use increases, it becomes more difficult to remember strong, unique passwords for each account. Researchers have published various methods based on salting, hashing, symmetric encryption, and key splitting methods. The research "Generate a secret key with easy saving and remembering" describes the idea of generating a suitable secret key that is easy to remember and remember, as he succeeded in generating a strong password but difficult to remember and save. This research presents a new model and mechanism for creating the secret key (password) by balancing security and memorability. Based on existing research on key generation and user experience, the proposed model uses a new approach to password generation. The model creates secure passwords that are easy for users to remember and store in their memory with a specific mechanism, reducing the risk of forgetting the password and the difficulty of memorizing it. The research addresses the details of the proposed model and identifies its basic mechanism and implementation. Furthermore, it presents the methodology used to evaluate the model's effectiveness, including user studies and security analysis. The results showed that the percentage of ease of memorization and recall was 7% and 8% out of 10%, respectively, compared to the previous study in which the percentage of ease of memorization and recall was 3% and 4% out of 10%, respectively. The results also showed that the security strength of the secret key generated from the proposed model, in which the number of symbols is

40, requires 87.4 years to break since the Key field is $104^{\wedge 40}$. Thus, the key space is equal to 6.362171 x $10^{\wedge 80}$ bits. The results show that the proposed model significantly improves password recall while maintaining strong security. The model's ease of use and enhanced security features promise contributions to the user experience and information security practices.

الملخص بالعربي

في العصر الرقمي، تعمل المصادقة المستندة إلى كلمة المرور بمثابة ضمانة حاسمة لحماية أنظمة المعلومات الإلكترونية الحساسة. ومع ذلك، يتمثل التحدي في إنشاء كلمات مرور قوية وسهلة التذكر لحسابات متعددة. كلمات المرور ضرورية لحماية حساباتنا الشخصية وبياناتنا الحساسة. مع زيادة عدد الحسابات التي نستخدمها، يصبح من الصعب تذكر كلمات مرور قوية وفريدة لكل حساب. لقد نشر الباحثون طرقًا مختلفة تعتمد على التمليح والتجزئة والتشفير المتماثل وطرق تقسيم المفاتيح. ويصف البحث "إنشاء مفتاح سري يسهل حفظه وتذكره" فكرة توليد مفتاح سري مناسب يسهل حفظه وتذكره، حيث نجح في توليد كلمة مرور قوية ولكن يصعب تذكرها وحفظها.، حيث نجح في توليد كلمة مرور قوية ولكن يصعب تذكرها وحفظها. يقدم هذا البحث نموذج وآلية جديدة لإنشاء المفتاح السري (كلمة المرور) من خلال الموازنة بين الأمان وقابلية التذكر. استنادًا إلى الأبحاث الحالية حول إنشاء المفاتيح وتجربة المستخدم، يستخدم النموذج المقترح أسلوبًا جديدًا لإنشاء كلمات المرور. يقوم النموذج بإنشاء كلمات مرور آمنة يسهل على المستخدمين تذكرها وتخزينها في ذاكرتهم بآلية محددة، مما يقلل من خطر نسيان كلمة المرور وصعوبة حفظها. ويتناول البحث تفاصيل النموذج المقترح ويحدد آليته الأساسية وتنفيذه. علاوة على ذلك، فإنه يعرض المنهجية المستخدمة لتقييم فعالية النموذج، بما في ذلك دراسات المستخدم والتحليل الأمني. وأظهرت النتائج أن نسبة سهولة الحفظ والتذكر بلغت ٧% و٨% من ١٠% على التوالي، مقارنة بالدراسة السابقة التي بلغت فيها نسبة سهولة الحفظ والتذكر ٣% و٤% من ١٠ % على التوالي. كما أظهرت النتائج أن القوة الأمنية للمفتاح السري المتولدة من النموذج المقترح والذي يبلغ عدد الرموز فيه ٤٠ رمزاً، تتطلب ٨٧,٤ سنة لكسرها حيث أن حقل المفتاح هو ١٠٤^40. وبالتالي، فإن مساحة المفتاح تساوي ٦,٣٦٢١٧١ × 10^80 بت. أظهرت النتائج أن النموذج المقترح يحسن بشكل كبير استدعاء كلمة المرور مع الحفاظ على أمان قوي. تعد

سهولة استخدام النموذج وميزات الأمان المحسنة بمساهمات في تجربة المستخدم وممارسات أمن المعلومات.