ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

ФАКУЛЬТЕТ ЦИВІЛЬНОГО ЗАХИСТУ

МАТЕРІАЛИ

круглого столу (вебінару)

«ЗАПОБІГАННЯ ВИНИКНЕННЮ НАДЗВИЧАЙНИХ СИТУАЦІЙ, РЕАГУВАННЯ ТА ЛІКВІДАЦІЯ ЇХ НАСЛІДКІВ»

23 лютого 2023 року
Харків

УДК 35.078

ЩОДО ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ ДСНС

Тарадуда Д.В., к.т.н., доц., НУЦЗ України

На сьогодні актуальною проблемою у сфері захисту інформаційних систем підрозділів ДСНС є низька ефективність підсистеми управління доступом до інформації відомчої інформаційно-телекомунікаційної мережі об'єктів критичної інформаційної інфраструктури.

У роботі [1] описані сучасні методи зламування паролів. Розглядаються проблеми, повзанні з людським фактором, пропонуються методи підвищення захищеності пароля, враховуючи довжину пароля, складність пароля і можливість його запам'ятовування, але не враховувалася стійкість парольної системи протистояти атаці зловмисника, який заволодів базою даних облікових записів для відновлення паролів.

Важливою метою систем аутентифікації є допомога користувачам у виборі кращих паролів. У [2] вивчається складність використання пароля, статистичні проблеми оцінки цього показника за допомогою наборів емісійних даних, які можна змоделювати як випадкову вибірку з основного розподілу ймовірностей. Емпіричні оцінки, представлені дисертаційному дослідженні, показують, що рівень безпеки, що забезпечується сучасними системами, низький. Погоджуємося із висновками, що варто повернутися до вибору машиною паролів для програм, що мають найважливіше значення для безпеки. Тому вдосконалення стійкості парольного захисту є оптимальним для забезпечення автентифікації. Як правило, користувачі схильні віддавати перевагу паролям, що запам'ятовуються, але при цьому легко вгадуються зловмисниками, водночас надійні паролі, призначені системою, важко запам'ятати користувачам.

У [3] увага приділяється комплексній оцінці системи графічних паролів Persuasive Cued Click Points, яка включає оцінку зручності використання і безпеки на трьох різних рівнях, що забезпечується за рахунок посилення ролі ефективного простору паролів, тобто в створенні переконливої графічної системи паролів на основі кліків мишкою. Схема точок кліків мишкою з підказками ефективна для зменшення кількості гарячих точок на області зображення, де користувачі з більшою ймовірністю вибирають правильні точки кліків. Однак, як недолік можна відмітити те, що у графічних паролях, заснованих на кліках, погано обрані паролі призводять до появи гарячих точок (ділянки зображення, на яких користувачі з більшою ймовірністю вибирають точки кліку, що дозволяє зловмисникам проводити більш успішні словникові атаки).

У [4] представлена інтегрована оцінка графічної схеми паролів Persuasive Cued Click-Points, ключова особливість яких полягає в тому, що створення важчого для вгадування пароля забезпечується зведенням до мінімуму формування гарячих точок у користувачів, збільшуючи ефективний простір паролів, використовуючи пам'ять людини для візуалізації. Однак, аналіз досліджень, попри сподівання на людську пам'ять для візуалізації, показує, що дизайн користувальницького інтерфейсу впливає на користувачів і може сприяти як безпечному, так і небезпечному вибору пароля, тому проблема забезпечення стійкості парольного захисту не є вирішеною.

У дослідженні [5] запропоновано декілька можливих показників для вимірювання стійкості індивідуального пароля. На відміну від спеціальних підходів, які спирались на текстові властивості паролів, розглядається проблема без будь-яких знань про структуру паролів, що дає змогу оцінювати стійкість щодо семантики паролів. Порівняно результати загальних показників із результатами метрик NIST та інших метрик «на основі ентропії» для великого набору даних паролів. Проте недоліком даних досліджень

є висока ефективність вгадування зловмисниками паролів на основі мови словника паролів і паролів користувачів, які вибирали їх в наборі даних.

У [6] на основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів інформаційно-телекомунікаційних систем показано, що парольний захист на сьогодні є одним із найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах розподілених систем. Проте без використовування інших механізмів захисту парольний захист не є надійним, оскільки не може забезпечити потрібного захисту, тому вважаємо за необхідне розраховувати стійкість парольної системи за формулою оцінки ентропії, що не висвітлено в даній роботі.

У [7] розглянуті особливості алгоритмів оцінки стійкості паролів до зламів на основі аналізу сучасних методів хакерських атак на системи авторизації, запропоновано алгоритм стійкості паролів для його перевірки на етапі створення, але не проаналізовані статистичні показники для надійності індивідуального пароля.

Таким чином, не вирішеною частиною проблеми захисту інформації відомчої інформаційно-телекомунікаційної мережі є кількісна оцінка стійкості парольних систем.

ЛІТЕРАТУРА

1. Weir M., Aggarwal S., Collins M., Stern H. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords // CCS '10: Proceedings of the 17th ACM conference on Computer and communications security. United States 4 – 8 October 2010. P. 162–175.

2. Bonneau J. Guessing human-chosen secrets // University of Cambridge, Computer Laboratory. 2012. № 819. URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-819.pdf

3. Nayak A., Bansode R. Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points // 7th International Conference on Communication, Computing and Virtualization (ICCCV). 2016. V. 79. P. 553–560.

4. Chiasson S., Stobert E., Forget A., Biddle R., Van Oorschot P. C. Persuasive Cued Click-Points Design, implementation, and evaluation of a knowledge-based authentication mechanism // IEEE Transactions on Dependable and Secure Computing. 2012. V. 9. I. 2. P. 222–235.

5. Bonneau J. Statistical metrics for individual password strength // 20th international conference on Security Protocols. Berlin April 2012.

6. Khorev P. B. User Authentication Based on Knowledge of Their Work on the Internet // Wireless Mesh Networks – Security, Architectures and Protocols. 2019.

7. Kelley P. G., Komanduri S., Mazurek M. L., Shay R., Bauer T. V. L., Christin N., Cranor L. F., Lopez J. Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms // IEEE Symposium on Security and Privacy. Pittsburgh, USA 20–23 May 2012. P. 523–537.