IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

Application of Honeywords

Mrs. Tejal. S. Sonawane Mrs. Mayuri. U. Ighe Mrs. Jayshree. M. Khairnar
Guru Gobind Singh Polytechnic Nashik, Maharashtra, India
tejal.sonawane@ggsf.edu.in, mayuri.ighe@ggsf.edu.in, jayshree.khairnar@ggsf.edu.in

Abstract: *This is a digital era, most of the activities happen online where all the information is shared on the internet. The use of internet has brought the world closer while making it faster at the same time. the sharing of information has so many advantages but on the other hand it has severe security risk of unauthorized access by hackers. Even though the users are well equipped with the unique and strong usernames and passwords, the hackers, with the help of several software's and programs are able break the passwords and gain the access. To overcome this problem "Honeywords" are used. The Honeyword System creates multiple false passwords and stores them along with the actual passwords. When the hacker or illegitimate user tries to hack in the system by using a honeyword, the attempt is flagged. At the same time the real user doesn't need to know the honeywords related to their password. The honeyword system produces multiple honeywords which are stored along with the actual passwords. Whenever the honeyword is used to gain unauthorized access, the system starts alarm and the notification is sent to the respective user to alert them. The unauthorized user will also get an automatically generated decoy document on their system. This provides the security and decreases the chances of hacking.*

Keywords: Password, Honeywords, hash breach Detection technique, Authentication, Security

REFERENCES

[1]. A. Evans, Jr., W. Kantrowitz, and E. Weiss. A user authentication scheme not requiring secrecy in the computer. Commun. ACM, 17(8):437–442, August 1974.
[2]. R. J. Anderson and T.M.A. Lomas. On fortifying key negotiation schemes with poorly chosen passwords. Electronics Letters, 30(13):1040–1041, 1994.
[3]. M. Bakker and R. van der Jagt. GPU-based password cracking. Technical report, Univ. of Amsterdam, 2010.
[4]. T. A. Berson, L. Gong, and T.M.A. Lomas. Secure, keyed, and collisionful hash functions. Technical Report SRI-CSL-94-08, SRI International Laboratory, 1993 (revised 2 Sept. 1994).
[5]. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In WWW, pages 551–560, 2009.
[6]. H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh. Kamouflage: loss-resistant password management. In ESORICS, pages 286–302, 2010.
[7]. J. Bonneau. Guessing human-chosen secrets. PhD thesis, University of Cambridge, May 2012.
[8]. J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In IEEE Symposium on Security and Privacy, pages 538–552, 2012.
[9]. J. Bonneau and S. Preibusch. The password thicket: technical and market failures in human authentication on the web. In Workshop on the Economics of Information Security (WEIS), 2010.
[10]. B. M. Bowen, S. Hershkop, A. D. Keromytis, and S. J. Stolfo. Baiting inside attackers using decoy documents. In SecureComm, pages 51–70, 2009.
[11]. J. Brainard, A. Juels, B. Kaliski, and M. Szydlo. A new two-server approach for authentication with short secrets. In USENIX Security, pages 201–214, 2003.
[12]. J. Camenisch, A. Lysyanskaya, and G. Neven. Practical yet universally composable two-server password-authenticated secret sharing. In ACM CCS, pages 525–536, 2012.
[13]. William Cheswick. Rethinking passwords. Comm. ACM, 56(2):40–44, Feb. 2013.
[14]. F. Cohen. The use of deception techniques: Honeypots and decoys. In H. Bidgoli, editor, Handbook of Information Security, volume 3, pages 646–655. Wiley and Sons, 2006.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, February 2022
Impact Factor: 6.252

[15]. EMC Corp. RSA Distributed Credential Protection. http://www.emc.com/security/rsa-distributed-credential-protection.htm, 2013.

[16]. A. Czeskis, M. Dietz, T. Kohno, D. Wallach, and Balfanz. Strengthening user authentication through opportunistic cryptographic identity assertions. In ACM CCS, pages 404–414, 2012.

[17]. Defense Information Systems Agency (DISA) for the Department of Defense (DoD). Application security and development: Security technical implementation guide (STIG), version 3 release 4, 28 October 2011.

[18]. A. Forget, S. Chiasson, P. C. van Oorschot, and Biddle. Improving text passwords through persuasion. In SOUPS, pages 1–12, 2008.

[19]. C. Gaylord. LinkedIn, Last.fm, now Yahoo? don't ignore news of a password breach. Christian Science Monitor, 13 July 2012.

[20]. D. Gross. 50 million compromised in Evernote hack. CNN, 4 March 2013.

[21]. C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. IEEE Security & Privacy, 10(1):28–36, 2012.

[22]. S. Houshmand and S. Aggarwal. Building better passwords using probabilistic techniques. In ACSAC, pages 109–118, 2012.

[23]. P.G. Kelley, S. Komanduri, M.L. Mazurek, R. Shay, Vidas, L. Bauer, N. Christin, L.F. Cranor, and J. Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In IEEE Symposium on Security and Privacy (SP), pages 523–537, 2012.

[24]. O. Kharif. Innovator: Ramesh Kesanupalli's biometric passwords stored on devices. Bloomberg Businessweek, 28 March 2013.

[25]. Microsoft TechNet Library. Password must meet complexity requirements. Referenced March 2012 at http://bit.ly/YAsGiZ.

[26]. R. Morris and K. Thompson. Password security: a case history. Commun. ACM, 22(11):594–597, November 1979.

[27]. A. Narayanan and V. Shmatikov. De-anonymizing social networks. In IEEE Symposium on Security and Privacy (SP), pages 173–187, 2009.

[28]. U.S. House of Representatives. H.R. 624: The Cyber Intelligence Sharing and Protection Act of 2013. 113th Cong., 2013.

[29]. B.-A. Parnell. LinkedIn admits site hack, adds pinch of salt to passwords. The Register, 7 June 2012.

[30]. I. Paul. Update: LinkedIn confirms account passwords hacked. PC World, 6 June 2012.

[31]. D. Perito, C. Castelluccia, M. A. Kaafar, and P. Manils. How unique and traceable are usernames? In Privacy Enhancing Technologies, pages 1–17, 2011.

[32]. N. Perlroth. Hackers in China attacked The Times for last 4 months. New York Times, page A1, 31 January 2013.

[33]. G. B. Purdy. A high security log-in procedure. Commun. ACM, 17(8):442–445, August 1974.

[34]. Shrisha Rao. Data and system security with failwords. U.S. Patent Application US2006/0161786A1, U.S. Patent Office, July 20, 2006. http://www.google.com/patents/US20060161786.

[35]. B. Ross, C. Jackson, N. Miyake, D. Boneh, and J.C. Mitchell. Stronger password authentication using browser extensions. In USENIX Security, 2005.