A Cue is worth a 1000 resets: Using Google Assistant to Remember Passwords

Ann-Marie Horcher, Ph. D.

Central Michigan University
horch1a@cmich.edu

ABSTRACT

In-home voice-activated Internet appliances provide an interface to technology not ruled by a keyboard and mouse. For sections of the population lacking in technology expertise and/or equipment these appliances provide a channel to knowledge previously reserved to the tech-savvy. The low cost of these devices provides an avenue for those who are on the wrong side of the digital divide based on race, income, gender, and educational attainment. The voice-activated nature of these device makes them accessible to a population with limited vision and physical dexterity. The simplicity of the interfaces make this channel also accessible to individuals with diminished mental acuity caused by exhaustion, excessive multi-tasking, technology over-use, or many other common situations.

The average user manages 25 or more passwords because basic authentication is still the lingua franca of online access. Strong password rules require these passwords to be not word-based, longer than eight characters, contain alphanumeric characters and symbols, and secret. These passwords should also all be different from each other and not follow a pattern. Since the human brain can remember 3-5 pieces of unrelated information, like these passwords, forgetting a password is not a matter of "if" but "when" and even how often.

This research examines the use of voice-activated smart home appliances to assist individuals of diminished capacity in income, technology-expertise, physical capabilities, and mental acuity to remember the passwords required by government, finance, and social networks to remain in contact with the world on the internet.

1. INTRODUCTION

Access to digital information is no longer reserved to an elite minority of scholars and businesses—the Internet has put access in hands of the general public [36]. From environmental information to e-government services to phone directories, information delivery and interaction has shifted from print to exclusively electronic [20]. The accelerated movement of service to e-only delivery makes technology a necessity for all instead of a non-essential luxury item [19]. As reported in a recent study of Detroit neighborhoods without Internet access, the absence of Internet access puts these citizens on the wrong side of a digital divide separating them from on jobs, utilities, and public emergencies as well resources to educate the children in the household [29]. The lack of affordable, easy-to-use equipment reinforces the barrier.

Speech-only interfaces in the form of controlled dialogs with voice menus were noted for frustrating users and unsuccessful data retrieval [37]. Conversational User Interfaces (CUI) married with Artificial Intelligence (AI) produce a more natural dialog with the user through chatterbots [21] and Intelligent Personal Assistants (IPAs) such as Apple's Siri and Microsoft's Cortana, and the Google Now [6] which were typically invoked on smartphones, and occasionally tablets and laptops. The most recent step in the evolution of speech interfaces has been the smart speaker in the home implemented as an Internet-connected device like the Amazon Alexa and Google Assistant [39]. The simplicity of the smart speaker interface, the quality of voice recognition, and the accuracy of the information delivery has opened the Internet to individuals who had difficulty using the traditional Internet browsers [18].

In addition to being a gateway to information on the Internet by pulling news, weather, and answers to trivia questions, the Virtual Personal Assistants (VPAs) provided by Google and Amazon can also serve as a conduit to third-party provided capabilities such texting, booking a restaurant table, or listening to podcasts [39]. This research looks at combining a VPA with an application that helps users remember passwords. The average user has 25 or more user identifier (userid) and password combinations to manage [9]. In most cases the user is expected to recall the passwords and userids from memory. Though users are encouraged to use unique passwords for each account [8], four to five is the number of unrelated, regularly used passwords that users can be expected to successfully manipulate [1].

Authentication schemes are based on what a user knows, what a user has, and/or what a user is [2]. The artifact stores password hints instead of the passwords. When the actual password is not stored, the user must still bring something they know to authenticate. The user must decode the hint into a password. Using cued recall to perform the memory task of password retrieval allows previously inaccessible information in a pure recall situation to be retrieved with a retrieval clue [33]. In this case with the voice interface, someone may overhear the hint. However, a well-chosen hint will only assist the authorized user. Recalling a password from a cue is much more efficient than going through a password recovery and reset [5].

2. BACKGROUND

Because most people find it difficult to remember alphanumeric passwords [8], they adopt various strategies, usually unsafe, to

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.

manage them [7]. The gap between passwords to manage, and the number that can be remembered dooms the effort to failure if the user relies upon the normal capabilities of human memory recall [16]. As a result, the accumulation of more accounts normally means the reuse of more passwords, not the creation of new ones [10]. Password safe software to store groups of passwords securely behind a single key [23] or external password storage in a hardware token such as Pico [32] are options for managing multiple passwords. Using a paper notebook to organize the insecure practice of writing [30] can be better from the user perspective than being denied access to accounts.

Remembering a password can also be more difficult in many common situations that diminish normal acuity. This diminished state can be caused by lack of sleep, which is reaching epidemic levels [34]. Over-use of technology [24] and excessive multi-tasking of any kind [25] are also all too common situations that reduce cognitive ability.

From a security perspective, an application that stores hints instead of actual passwords has less risk of compromise. But the nature of security is such that users are reluctant to trust the research and researcher [3]. The participants in the studies must typically have a trust relationship with the researcher, and are reluctant to reveal their actual activities related to security [22]. In addition users are reluctant to try new security techniques because of the potential risks and their uncertainty about safety [31].

Risk assessment of the use of technology shows locations are not equal in security risk. Internet Protocol (IP) addresses of a device are used as a means to identify risk [26]. GPS can also be used to identify location to determine a potenial risk level. The VPA by its nature sits in the home, which is typically a "safe" area for the potential user when accessing equipment such as smartphones and laptops. In the tradeoff between vulnerability and the likelihood of compromise, the risk within the perimeter of the home should be lower. The security challenge to unlock to view current time should be less than that needed to access a bank account [38]. Similarly requiring the same security effort inside the home as in public may not be valid.

Concerns about how efficiently a password hint can be converted to a password by an unfriendly party mirror the issues raised when using security questions. Like a well-formed security question and answer pair [28], the password hint must not be a matter of public record and reveal the correct solution only to the valid user. Dynamic security questions based on recent behaviors, or logs of activities stored on a mobile device have also shown success in correctly blocking an adversary, but admitting a valid user [14].

Computer equipment within the home typically remains viable because of informal technical support [27]. The VPAs have the advantage of providing an Internet interface with low setup cost and fairly low ongoing maintenance. This is critical to individuals lacking in technology expertise. Previous studies by Blackwell and Poole have shown burden of domestic programming can weigh so heavy on the techno-neophyte that they abandon the equipment [4].

3. Study Design

To assess the usability of a CUI to retrieve and store password clues, this study collects a measures for each dimension of usability as defined by ISO [17]. The Common Industry Format (CIF) for usability testing uses the ISO 9241-11 definition of usability which is how well a product used by specified users achieves specified goals for effectiveness, efficiency, and user satisfaction [17].The following hypotheses explore these dimensions of usability.

H1: Users successfully recall passwords based on cues delivered by the VPA artifact.

H2: VPA artifact accurately retrieves password clues based on voice input

H3: A conversational UI will accurately store password clues based on voice input

H4: Users find VPA artifact for password hints acceptable

H5: Users will feel safe recalling passwords from a VPA artifact.

In Table 1, the data collected in the study is mapped to the hypotheses and the appropriate dimension of usability in the ISO definition.

Hypothesis	Data	ISO Dimension
H1	successful recall of password	effectiveness
H2	Desired password hint retrieved using CUI only	efficiency
H3	Password hint stored using CUI only	efficiency
H4	Acceptable rating from Standardized Usability Scale (SUS)	User satisfaction
H5	Post-study survey	User Satisfaction

Table 1 Study Measures Mapped to ISO usability

The methodology being used is design science research (DSR). Design research (DR) is research into or about design. DSR is research using design as a research method or technique [15]. DSR methodology has a series of steps that result in specific outputs. It can be an iterative process, as information from an evaluation influences the design of another element [35]. Based on the feedback from the initial stages, the design is iteratively adjusted and improved.

An application (called an *Action* by Google) was created using the Dialogflow AI interface. The Dialogflow provides a framework to have a conversation with the application user [13] The designer provides typical responses, and the natural language processing from Dialogflow extracts key variables to drive appropriate responses (Figure 1). In the example shown

the designer anticipates some of the most probable applications the user may have, and need to set/retrieve a password clue. The prompts can be hard-coded or "slot-filled" from a database in the background.

The variables extracted by Dialogflow are passed to a web service written in JavaScript (webhook) which connects to a Firebase database. The backend uses Google's Firebase platform for data storage, and authenticates using the authorized user's Google account [12]. Using Firebase authentication ensures a secure and stable authentication protocol with minimal code for integration.

The Firebase platform also provides a no-SQL database for data collection in the cloud [11]. A data console allows a developer to interact with the data directly, as well as through Application Programming Interface (API).

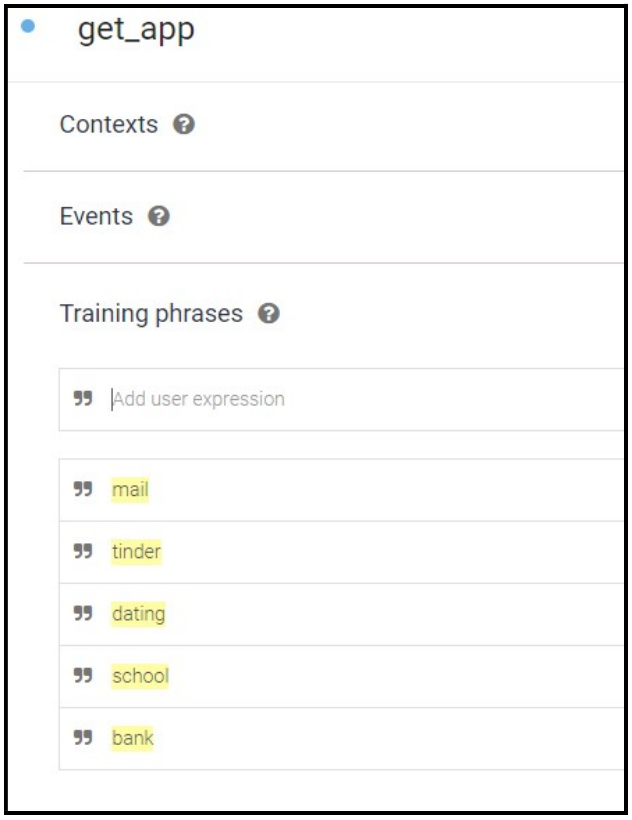

Figure 1- Dialog Flow for defining most common apps

The subjects will be a convenience sample of attendees at a code camp in mid-June of 2018. The subjects first fill out a pre-study questionnaire to establish existing security attitudes and experience with smart home appliances. The subjects are then asked to perform a series of tasks to interact with the Google Assistant to recall and set password clues. After completing the interaction, the participants respond to the SUS questionnaire about the application with additional questions related to attitudes towards safety of a new security interface.

4. Future Work

The next phase of the study will address the group nature of authentication needs for VPAs. In the case of a disabled individual, or elderly person, there may a caregiver interactions on behalf of the individual.

5. REFERENCES

[1] Adams, A., and Sasse, M. A., "Users are not the enemy," *Communications of the ACM,* vol. 42, no. 12, pp. 40-46, 1999.

[2] Almuairfi, S., Veeraraghavan, P., and Chilamkurti, N., "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices," *Mathematical and Computer Modelling,* vol. 58, no. 1, pp. 108-116, 2013.

[3] Baskerville, R., "Information systems security design methods: implications for information systems development," *ACM Comput. Surv.,* vol. 25, no. 4, pp. 375-414, 1993.

[4] Blackwell, A. F., Rode, J. A., and Toye, E. F., "How do we program the home? Gender, attention investment, and the psychology of programming at home," *International Journal of Human-Computer Studies,* vol. 67, no. 4, pp. 324-341, 2009.

[5] Denning, T., Bowers, K., Dijk, M. v., and Juels, A., "Exploring implicit memory for painless password recovery," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2615-2618, 2011.

[6] Ehrenbrink, P., Osman, S., and Moller, S., "Google now is for the extraverted, cortana for the introverted: investigating the influence of personality on IPA preference," *Proceedings of the 29th Australian Conference on Computer-Human Interaction*, pp. 257-265, 2017.

[7] Everitt, K. M., Bragin, T., Fogarty, J., and Kohno, T., "A comprehensive study of frequency, interference, and training of multiple graphical passwords," *Proceedings of the 27th international conference on Human factors in computing systems*, pp. 889-898, 2009.

[8] Florencio, D., and Herley, C., "A large-scale study of web password habits," *Proceedings of the 16th international conference on World Wide Web*, pp. 657-666, 2007.

[9] Gao, H., Ma, L., Jia, W., and Ye, F., "Multiple password interference in graphical passwords," *Int. J. Inf. Comput. Secur.,* vol. 5, no. 1, pp. 11-27, 2012.

[10] Gaw, S., and Felten, E. W., "Password management strategies for online accounts," *Proceedings of the second symposium on Usable privacy and security*, pp. 44-55, 2006.

[11] Google. "Firebase Realtime Database," March 12, 2017; https://firebase.google.com/docs/database/.
[12] Google. "Firebase Authentication," March 3, 2017; https://firebase.google.com/docs/auth/.
[13] Google. "Basics of Dialogflow," May 18, 2018; https://dialogflow.com/docs/.
[14] Hang, A., Luca, A. D., and Hussmann, H., "I Know What You Did Last Week! Do You?: Dynamic Security Questions for Fallback Authentication on Smartphones," *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 1383-1392, 2015.
[15] Hevner, A. R., March, S. T., Park, J., and Ram, S., "Design Science in Information Systems Research," *Management Information Systems Quarterly,* vol. 28, no. 1, 2004.
[16] Horcher, A.-M., and Tejay, G. P., "Building a better password: the role of cognitive load in information security training," *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics* pp. 113-118, 2009.
[17] Jokela, T., Iivari, N., Matero, J., and Karukka, M., "The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11," *Proceedings of the Latin American conference on Human-computer interaction*, pp. 53-60, 2003.
[18] Kaye, J. J., Fischer, J., Hong, J., Bentley, F. R., Munteanu, C., Hiniker, A., Tsai, J. Y., and Ammari, T., "Panel: Voice Assistants, UX Design and Research," *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1-5, 2018.
[19] Kim, E., Lee, B., and Menon, N. M., "Social welfare implications of the digital divide," *Government Information Quarterly,* vol. 26, no. 2, pp. 377-386, 2009.
[20] Kirk, C. P., Chiagouris, L., and Gopalakrishna, P., "Some people just want to read: The roles of age, interactivity, and perceived usefulness of print in the consumption of digital information products," *Journal of Retailing and Consumer Services,* vol. 19, no. 1, pp. 168-178, 2012.
[21] Klopfenstein, L. C., Delpriori, S., Malatini, S., and Bogliolo, A., "The Rise of Bots: A Survey of Conversational Interfaces, Patterns, and Paradigms," *Proceedings of the 2017 Conference on Designing Interactive Systems*, pp. 555-565, 2017.
[22] Kotulic, A. G., and Clark, J. G., "Why there aren't more information security research studies," *Information & Management,* vol. 41, no. 5, pp. 597-607, 2004.
[23] Lee, K.-W., and Ewe, H.-T., "Passphrase with Semantic Noises and a Proof on Its Higher Information Rate," *Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops*, pp. 652-655, 2007.
[24] Lee, U., Lee, J., Ko, M., Lee, C., Kim, Y., Yang, S., Yatani, K., Gweon, G., Chung, K.-M., and Song, J., "Hooked on smartphones: an exploratory study on smartphone overuse among college students," *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pp. 2327-2336, 2014.
[25] Loh, K. K., and Kanai, R., "Higher Media Multi-Tasking Activity Is Associated with Smaller Gray-Matter Density in the Anterior Cingulate Cortex," *PLOS ONE,* vol. 9, no. 9, pp. e106698, 2014.
[26] Park, H., and Redford, S., "Client certificate and IP address based multi-factor authentication for J2EE web applications," *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, pp. 167-174, 2007.
[27] Poole, E. S., Chetty, M., Morgan, T., Grinter, R. E., and Edwards, W. K., "Computer help at home: methods and motivations for informal technical support," *Proceedings of the 27th international conference on Human factors in computing systems*, pp. 739-748, 2009.
[28] Rabkin, A., "Personal knowledge questions for fallback authentication: security questions in the era of Facebook," *Proceedings of the 4th symposium on Usable privacy and security*, 2008.
[29] Reisdorf, B., Hampton, K., Fernandez, L., and Dutton, W. H., "Broadband to the Neighborhood: Digital Divides in Detroit," 2018.
[30] Roberts, M., *Internet Password Notebook: A pocket-sized Internet address organizer for all of your usernames and passwords (Volume 2)*: CreateSpace, 2010.
[31] Siponen, M. T., and Oinas-Kukkonen, H., "A review of information security issues and respective research contributions," *SIGMIS Database,* vol. 38, no. 1, pp. 60-80, 2007.
[32] Stajano, F., "Pico: no more passwords!," *Proceedings of the 19th international conference on Security Protocols*, pp. 49-81, 2011.
[33] Stobert, E., and Biddle, R., "Memory retrieval and graphical passwords," *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pp. 1-14, 2013.

[34] Theresia, C., Iridiastadi, H., and Pratama, G. B., "Impacts of sleep deprivation on vigilance, fatigue, and performance during simulated train driving," *Proceedings of the 2nd International Conference on High Performance Compilation, Computing and Communications*, pp. 45-50, 2018.

[35] Vaishnavi, V., and Kuechler, B. "Design Science Research in Information Systems," October 3, 2011; http://desrist.org/desrist

[36] Yang, L., and Zhiyong, G. L., "Internet's impact on expert–citizen interactions in public policymaking—A meta analysis," *Government Information Quarterly,* vol. 27, no. 4, pp. 431-441, 2010.

[37] Yin, M., and Zhai, S., "The benefits of augmenting telephone voice menu navigation with visual browsing and search," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 319-328, 2006.

[38] Zezschwitz, E. v., Dunphy, P., and Luca, A. D., "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* pp. 261-270, 2013.

[39] Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., and Qian, F., "Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home," *arXiv preprint arXiv:1805.01525*, 2018.