Choose Your Own Authentication

Alain Forget
Carnegie Mellon University
Pittsburgh, Pennsylvania, USA
aforget@cmu.edu

Sonia Chiasson, Robert Biddle
Carleton University
Ottawa, Ontario, Canada
chiasson@scs.carleton.ca,
robert.biddle@carleton.ca

ABSTRACT

To solve the long-standing problems users have in creating and remembering text passwords, a wide variety of alternative authentication schemes have been proposed. Some of these schemes outperform others by various metrics in various contexts. However, none unilaterally outperform all others, and so text passwords persist as the main scheme applications depend upon. In this paper, we challenge the long-standing assumption that only one authentication scheme can be offered by an application service. We propose Choose Your Own Authentication (CYOA): a novel authentication architecture that enables users to choose a scheme amongst several available alternatives. CYOA would enable users to select whichever scheme best suits their preferences, abilities, and usage context. Existing text password systems could easily be replaced. Furthermore, the three-party architecture would enable delegating the management of authentication systems to trusted-third parties. The architecture allows rapid deployment and testing of novel authentication technologies. Our two-week usability study suggests that participants were willing to leverage alternative schemes. Participants were confident that CYOA could keep their financial information secure.

CCS Concepts

•**Security and privacy** → **Authentication;** *Usability in security and privacy;* •**Human-centered computing** → Accessibility systems and tools;

Keywords

Authentication; survey; usable security; user study

1. INTRODUCTION

For decades, users have had difficulties creating and remembering secure text passwords [35]. Almost thirty years later, Florêncio and Herley [15] found similar results in a study of online text passwords and remark, "While much has changed since 1979 [...] it is just as true that many users appear to choose the weakest possible password." Industry initiatives [8,13,34] and researchers [3,30,36] have proposed numerous alternative authentication schemes and protocols to address these challenges. Despite the problems with text passwords, it seems unlikely that any single scheme will completely replace them [26], since no one scheme outperforms text passwords by all measures [4].

Perhaps a better approach would be for different schemes to be used in different contexts. Users should be able to authenticate with a scheme that offers sufficient security, usability, and accessibility for the specific user, account, and threat model. But how can an authentication system know every user's preferences and requirements? Users may prefer a scheme with high password memorability for a seldom-accessed account or a high-security scheme for an online bank account. Users' priorities may change yet again for different login circumstances. They may desire a shoulder-surfing resistant scheme for an account they access in public.

In fact, a number of platforms already allow users to choose their authentication method. Android allows users to unlock their mobile devices using text passwords, PINs, swipe patterns, facial recognition, and third-party apps, each catering to different user abilities, preferences, usage contexts, and security requirements. Windows 8 and Apple iOS also offer several authentication choices. However, there is little published research on user-selection of authentication schemes. This gives urgency to our research community to consider how best to support a diverse and dynamic ecosystem of authentication systems, as well as examining users' motivation and behaviour when selecting schemes, to best support users performing this task.

We propose Choose Your Own Authentication (CYOA): an architecture that provides several authentication alternatives to users. In its simplest form (Figure 1), during registration, the user chooses one of several offered schemes and creates a password with said scheme. When later logging in, the user is provided with their chosen scheme and enters their password. CYOA can easily replace text password systems currently used in practice, since it stores passwords as an encoded string, just as current passwords. Users can select a scheme based on their own preferences, abilities, and usage context. CYOA can also support authentication schemes for users with accessibility needs. Administrators can delegate the evaluation, adoption, and support of authentication schemes to a trusted third-party of authentication experts. The authentication schemes are modular such that developers and researchers could implement novel schemes for rapid independent evaluation and adoption by administrators. CYOA thereby should lower the barrier between state-of-the-art authentication research and its adoption in practice, which would benefit all stakeholders.

The remainder of this paper will proceed as follows. We first discuss the relevant background and differences between CYOA and proposals of related intent or scope. We then explore responses from a survey on password choice we conducted to ascertain peo-

NSPW '15, September 08 - 11, 2015, Twente, Netherlands

ISBN 978-1-4503-3754-0/15/09...$15.00

DOI: **http://dx.doi.org/10.1145/2841113.2841114**

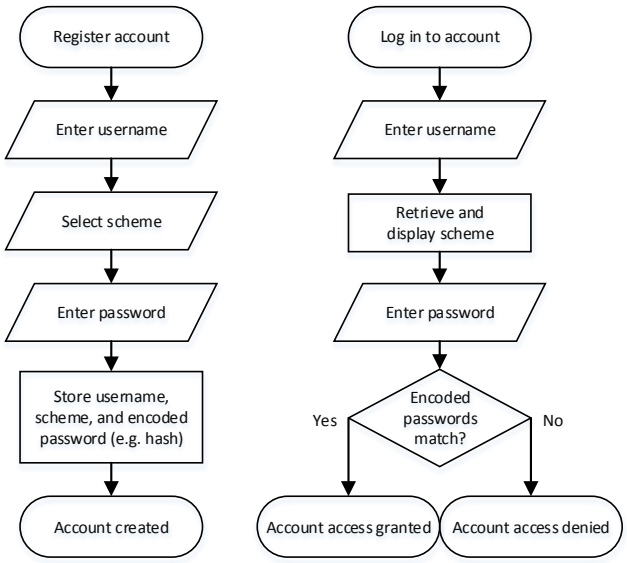


Figure 1: CYOA registration and login flowcharts

ple's desire for different levels of security and memorability for different accounts and passwords. We then elaborate on CYOA's two possible architectural designs, including their benefits and caveats, and the user experience. We then describe the methodology, hypotheses, results, and discussion of our user study to explore people's willingness and ability to choose alternative authentication schemes. Finally, we offer some concluding remarks.

2. BACKGROUND

Users' continuing difficulties to create and remember secure passwords are well-known [15,35,52]. Existing research identifies three primary reasons for the use of insecure passwords [1, 28]. First, choosing unique and random text passwords imposes unreasonable memory demands on users, who cope by reusing, writing down, and sharing predictable passwords. Strict password creation policies are intended to increase security, but they usually result in *less* security [31] due to limits in human memory. Second, secure passwords are difficult to create without substantial computer security knowledge, which end-users lack. Users are often unaware that words and names are the most predictable passwords. It is unreasonable to expect users to be security experts, so security systems should be designed such that the most secure behaviour is the easiest to perform [6]. Third, the security threats to users, their accounts, and the system are largely invisible to users, resulting in little incentive to behave securely. However, when made aware of the security risks, users can become security-conscious and respond appropriately [28]. This challenges the standing assumption that users are never motivated to behave securely. We will discuss how CYOA addresses these issues in user authentication.

Modular authentication schemes were first proposed as Pluggable Authentication Modules (PAMs) [48] for UNIX-based systems. PAMs allow applications to call standardised authentication functions without concern of what scheme or hashing method is in use. Administrators may enable multiple PAMs simultaneously, and may configure them so that users must successfully authenticate with a subset of PAMs (e.g., any one or all of them) to be granted access. However, there is no way for end-users to select which PAM (i.e. authentication scheme) to use. Thus, CYOA differs from PAMs in two important ways. First, CYOA allows end-users to directly select an authentication method. Second, PAMs are restricted to UNIX-based systems, while CYOA's architecture is designed to be implementable at any level, including stand-alone computer applications or multiple Internet services.

Clarke and Furnell [7] surveyed 297 people on their mobile phone authentication attitudes and practices. While two-thirds of respondents used personal identification numbers (PINs), 30% found PINs inconvenient and only 25% were confident in PINs' protection. While 42% of respondents felt PINs provided adequate security, 67% of respondents who reported that their phone had been misused were using PINs to lock their phones. Respondents further suggested that standard mobile locking mechanisms are insufficient, since 85% of respondents desired additional mobile phone security. The authors concluded that, "the need for more advanced authentication mechanisms is predicted due to the increasing functionality and services of mobile devices" and that, "it can confidently be predicted that some [users] will ideally demand protection in excess of the current provision." However, it is clear that different people have different authentication preferences.

Users already have a choice of authentication methods on a number of platforms. For example, recent Apple iPhone users may use fingerprint biometrics to reduce the frequency of PIN or text password entry. Google Android operating system users may unlock their mobile devices with text passwords, PINs, swipe patterns, or facial recognition. Google notes that the different schemes provide different levels of usability and security, as users selecting facial recognition on Android are warned that, "Face Unlock is less secure than a pattern, PIN, or password." Android users may also download and install third-party applications that provide additional authentication options. This gives users a vast choice in authentication schemes for their Android devices, but these applications are not available for other systems (e.g., online services, non-Android operating systems) unless they are completely re-implemented. Furthermore, users have no reason to trust the available authentication applications, since there is no assurance that the schemes are securely implemented. There is little published research on either how users select authentication schemes or how to architect and maintain systems to support multiple authentication schemes.

Single sign-on (SSO) architectures [32], such as OpenID [41], and *password managers* (PMs), such as LastPass [33], allow users to log in to multiple supporting services with a single username and password rather than requiring unique credentials for each service. Their primary advantage is to lower users' memory burdens by reducing the number of passwords users need to remember. This potentially enables users to focus their efforts on remembering fewer, more random (hence more secure) passwords. CYOA is different in that it offers users the choice of several authentication methods for each system, which has its own benefits. CYOA is a complementary solution to SSO and PMs, which could use CYOA to authenticate users, whereby users choose one of many schemes to create a single password used to authenticate to multiple services.

A related proposal named OAuth [22, 23] is an IETF standard for a protocol to allow an entity (the relying party) to access some resource owned by a second-party (the resource owner) and controlled by a third-party (the resource controller), without requiring the resource owners' credentials. For example, a user (as the resource owner) could authorise their social network website (the relying party) to access images on their photo-sharing website (the resource controller). OAuth solves a different problem than CYOA. CYOA is used to authenticate people while OAuth requests user authorisation for third-parties to access users' digital assets.

Belk et al. [2] conducted a study in which participants were randomly assigned either a text or graphical password. After 1.5 months, participants were then required to use the other scheme. After another 1.5 months, participants were given the choice of which scheme they would prefer to use. Throughout the study, participants performed psychometric tests to determine their *cognitive style* (i.e., whether users had stronger visual or lexical cognitive skills). The authors found that cognitively-visual users were significantly faster and less error-prone when using graphical passwords and that they preferred them to text passwords. This demonstrates that different people have different abilities and preferences for different types of authentication schemes and suggests that users would benefit from being given a choice in authentication schemes.

CYOA enables users to choose an authentication scheme not only based upon their preferred cognitive style, but also their physical abilities (or disabilities) and usage context (which may be difficult for an arbitrary system to determine). Although we must rely upon a user's perceived preference for cognitive style, future work should consider how to help users optimise their choice according to their actual cognitive strengths. Furthermore, Belk et al. focused on the correlations between users' cognitive styles and their efficiency, effectiveness, and preference with either text or graphical passwords, while our study primarily aims to gain insight on users' ability to cope with and leverage the power of choice in authentication schemes, particularly if users have little to no experience with the non-text password schemes (as the case would be if CYOA were adopted in practice).

Demographic	# of participants
All	100
Age 21-30	34
Age 31-40	37
Age 41-50	16
Age 51-77	13
Males : Females	42 : 58
No secondary	1
Secondary	14
Some post-secondary	30
Trade	2
Associate's	10
Bachelor's	34
Postgraduate	9
IT	13
Service/Retail	13
Administration	11
Business	10
Arts	9
Homemaker	6
Trades	6
Unemployed	6
Education	5
Various / Other	21

Table 1: Password choice survey respondent demographics.

3. PASSWORD CHOICE SURVEY

Providing a choice of multiple authentication schemes will only be useful to people if they wish different levels of memorability or security for different accounts. We first present a study designed to ascertain if people would benefit from such a system. We surveyed people on various issues regarding the desired security and memorability of the passwords they create. Related questions were grouped into distinct sections. Each section's questions were randomly-ordered for each respondent. We explicitly told respondents to not disclose any of their actual passwords.

We recruited respondents from Amazon Mechanical Turk. Table 1 shows that our respondents varied in age, gender, level of education, and occupation. Most respondents (95%) identified their nationality as "American" or "USA". In analysing each group of responses below, we performed Chi-square goodness-of-fit tests (with the Bonferroni correction) to determine if responses differed significantly from random.

Graphical password schemes try to leverage people's stronger memory for visual stimuli over text [37]. However, we wondered if people also felt visual stimuli was more memorable than text. If so, then their perception may cause them to try alternative graphical authentication options. Table 2 shows the responses to questions regarding people's visual memory (e.g., faces, objects, images) or lexical memory (e.g., names, words, numbers). Respondents felt they were more likely to remember new people's faces over their names ($\chi^2(2) = 82.46, p < .0001$) and had a better memory for objects and images than words and numbers ($\chi^2(2) = 14.18, p < .005$). Despite having expressed a stronger visual over lexical memory, respondents believed that it would be easier to remember ($\chi^2(1) = 5.76, p < .05$) and create secure ($\chi^2(1) = 12.96, p < .001$) text passwords over graphical passwords.

Figure 2 illustrates respondents' importance placed on the memorability or security of their passwords for various types of accounts (e.g., financial, e-mail, social networking, blogs, forums, personal computer) on a 5-point scale from "not at all important" to "very important". The memorability and security questions were each in separate sections whose presentation order was randomised for each participant. Responses regarding the importance of password memorability were not significantly distinguishable from the uniform (random) distribution. However, respondents placed very strong importance in desiring secure passwords for online banking ($\chi^2(4) = 301.1, p < .0001$), non-bank financial (e.g., PayPal, Amazon.com) ($\chi^2(4) = 175.1, p < .0001$), e-mail ($\chi^2(4) = 85.5, p < .0001$), social networking (e.g., Facebook, Twitter, Google+) ($\chi^2(4) = 38.2, p < .0001$), personal computer ($\chi^2(4) = 40.1, p < .0001$), and work computer ($\chi^2(4) = 47.4, p < .0001$) accounts. This suggests that people desire different levels of security for different types of accounts.

We also asked four questions in the form of, "When selecting a password for an account that you [do | do NOT] plan to use frequently, but is [very important and/or contains private information | less important and/or contains NO personal information], which is more important to you?" Table 3 shows that respondents placed a greater importance on selecting secure passwords for important accounts with private information, regardless of whether those accounts were frequently-accessed ($\chi^2(1) = 67.24, p < .0001$) or not ($\chi^2(1) = 51.84, p < .0001$). For less important accounts, password memorability was preferred, also regardless of frequent accesses ($\chi^2(1) = 25.00, p < .0001$) or not ($\chi^2(1) = 29.16, p < .0001$). Thus, when users must choose between creating a password that is easy-to-remember or secure, users want a secure password for important accounts and prefer more memorable passwords for less important accounts.

Overall, these results suggest two findings and possible lines of further inquiry. First, respondents clearly felt that visual stimuli were more memorable than lexical stimuli. However, they still felt more able to remember and create secure text passwords than graphical passwords. This may be because people have more experience with and developed coping mechanisms for text passwords, but little experience with non-text password schemes. It may be dif-

Question	Visual	Lexical	Neither
When you meet someone new, what are you more likely to remember about them?	76	9	15
Which are you generally better at remembering?	51	26	23
Which type of password do you think would be easier for you to remember?	38	62	n/a
Which type of password do you think would be easier for you to create a secure password?	32	68	n/a

Table 2: Responses to questions comparing preferences for visual or lexical stimuli.

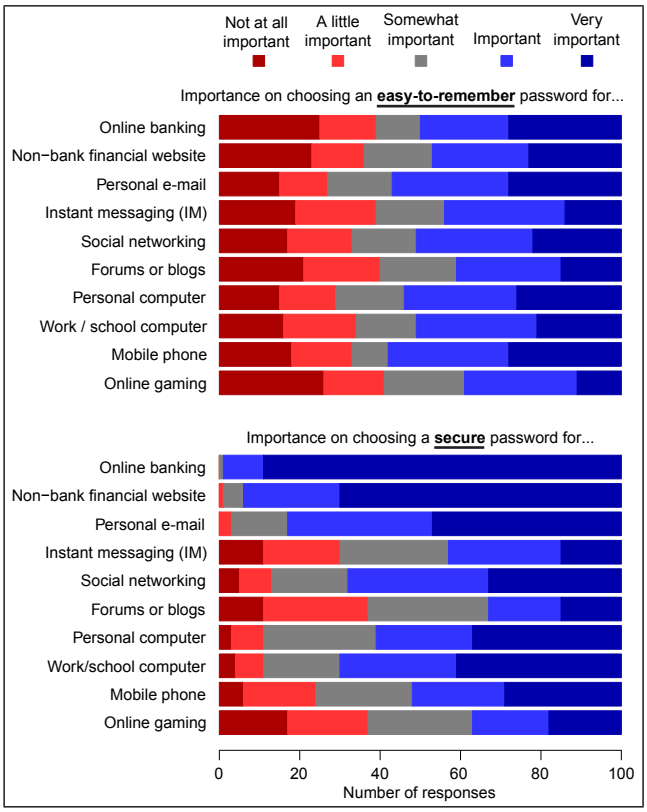


Figure 2: Respondents' importance placed on password memorability or security for various types of accounts.)

ficult for people to make judgements on unfamiliar schemes without the ability to experience them in an authentication context. However, given users' preference towards visual memory, we believe it is worthwhile to test whether users will select unfamiliar authentication schemes if given the opportunity.

Second, respondents clearly emphasised the need for password security for high-value accounts, but not for less important accounts. Furthermore, respondents may be willing to sacrifice password memorability in favour of security for more important accounts. This suggests that people may welcome different methods of authentication, particularly schemes that can assist users in creating more secure passwords for high-risk accounts.

These results suggest some justification for exploring CYOA. To properly test whether people will select more secure authentication schemes for higher-risk accounts, CYOA would need to protect participants' high-value accounts. We decided that for an initial test, it might be imprudent to ask participants to use an untested security mechanism for accounts of high importance. Thus, we chose to instead focus our first user study on evaluating whether or not people would be willing to select unfamiliar authentication schemes at all (Section 6). This would establish a baseline of reactions

	Memorability	Security
Important & frequent	9	91
Important & infrequent	14	86
Unimportant & frequent	75	25
Unimportant & infrequent	77	23

Table 3: Responses to the question, "When selecting a password for an account that you [do | do NOT] plan to use frequently, but is [very important and/or contains private information | less important and/or contains NO personal information], which is more important to you?"

to this new approach. However, before designing and executing a user study, we first had to develop the idea of CYOA into a complete high-level architecture and working prototype, as described in the following sections.

4. TECHNICAL ARCHITECTURE

We begin by describing CYOA's architectural design. We assume that all communications between parties are secure (using SSL, TLS, or other encryption technology). In all cases, three main entities are involved in the protocol:

1. ***Client***: The machine with which the user remotely authenticates to the application. The client's user wishes to register with or log in to the application.

2. ***Application server***: The server hosting the application resources and services which require authentication before access is granted. The application server is responsible for storing and verifying users' passwords. Most other authentication-related tasks are delegated to the CYOA module.

3. ***CYOA module***: The component that stores and manages the data and code necessary for the CYOA architecture to function. This component can either be on its own server or part of the application server. The CYOA module contains the supported authentication schemes, related data, and a database table that stores information keyed to the username and scheme. Users' passwords are never stored in the CYOA module.

In its simplest form, the CYOA module can simply be part of the application server as any typical authentication scheme. Such a CYOA module may reside on the same machine as the application system or on its own server within the application's domain. For clarity, our discussion will treat the application server and CYOA module as separate systems in the same domain.

We will illustrate how CYOA would work on the current Internet infrastructure, where the application is a typical web-based system of any implementation that offers services or resources for authenticated clients. In this scenario, the CYOA user authentication would begin with the user navigating to the application website's registration or login page and proceeding as illustrated in Figure 3:

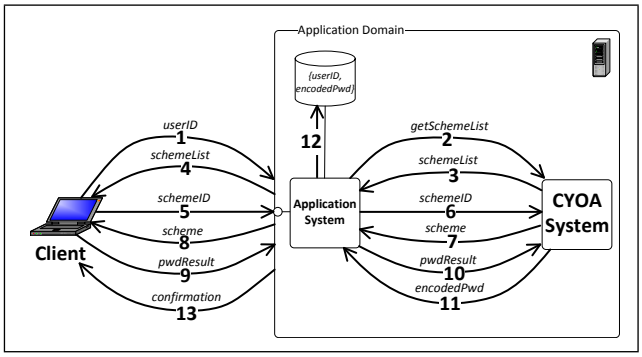


Figure 3: Basic two-party CYOA architecture where one organisation manages both the application server and CYOA module.

1. The user enters their username into the application's login form and submits it to the application server.
2. The application server requests the list of available authentication schemes from the CYOA module.
3. The CYOA module returns a list of available schemes and optional scheme-related data (e.g., descriptions, ratings) to the application server.
4. The application server converts the list of schemes and relevant data into a web form and returns it to the client.
5. On the presented webpage, the user selects the authentication scheme associated with their account and submits a request for the chosen scheme.
6. The application server requests the chosen scheme from the CYOA module.
7. The CYOA module returns the chosen scheme to the application server.
8. The application server adds the chosen scheme to a web form for authentication and returns it to the client.
9. The user enters their password with the selected authentication scheme, which converts it into a text string and submits it to the application server. If registering a new password, the user may need to enter and submit their password a second time for confirmation. If the chosen scheme requires additional communication with the CYOA server during password creation or entry (e.g., fetching images or other resources during password entry), such communication would happen between this step and the previous one.
10. The application server sends the password string to the CYOA module on the server.
11. The CYOA module encodes the password string with the chosen scheme's password encoding function, and returns the encoded password string to the server.
12. If registering a new password, the application server stores the encoded password string keyed to the username. If logging in, the application server compares the encoded password string with the one stored for the corresponding username.
13. If the user is registering a new password, the user is sent confirmation of the successful password registration. If logging in and the compared encoded passwords match, the user is granted access. Otherwise, access is denied.

When resetting their password, users are given the opportunity to select a different scheme. CYOA administrators may require users to select their authentication scheme before logging in. In this case, if the user chooses an incorrect scheme, whatever password the user enters will almost certainly not match their registered password, since different schemes encode passwords differently, and the password entry methods can be completely different. This additional login step provides additional security against password guessing attacks, since the attacker cannot easily determine which user selected which scheme. However, we believe this security gain is not worth increasing users' memory load in remembering not only their password, but also the correct scheme. Thus, we recommend the CYOA module present users with the correct scheme immediately, skipping steps 2 to 5 in Figure 3 for login. Still, the repercussions of either choice should be explored in future work.

4.1 Technical Benefits

Easy adoption for existing systems. Modern password systems already store hashed passwords as strings. Since CYOA authentication schemes also return encoded passwords as strings, integrating a CYOA module into an existing password system requires only minor modifications. Specifically, the CYOA module would replace the existing authentication scheme module, which is most likely a text password system that stores hashed passwords as strings. None of the supporting technology (e.g., database or other infrastructure) needs to be modified, since CYOA can use the same technology as existing text password systems, such as hashing, salting, and key stretching techniques (e.g., PBKDF2, scrypt). Some user interface modifications may be needed to accommodate scheme selection, but no additional software need be installed on the client. Although Figure 3 depicts the CYOA module as a module separate from the application server, CYOA could also be integrated into the application itself. Two simple examples of such an integrated implementation include a WordPress plug-in or the built-in authentication system used by any web application, including an OpenID identity provider.

Supports most knowledge-based authentication (KBA) schemes. Researchers designing novel KBA schemes often strive to require minimal changes to the host application. Thus, many KBA schemes already store an encoded string of the user's password to use when verifying future login attempts. All such schemes are supported by CYOA, since the application server stores encoded passwords as strings and performs a bitwise comparison of stored and entered encoded passwords for verification. However, this precludes CYOA from supporting authentication mechanisms that require a different method of password verification, such as challenge-response schemes (which require that verification vary depending on the challenge) or biometrics (which compare an input biometric to a stored template using heuristics). A simple bitwise comparison is typically impossible for such schemes, but we will discuss in Section 4.2 how this limitation can be overcome.

Modular architecture. The CYOA module itself is designed modularly, so system administrators can "plug-in" novel schemes without any disruption to users. Authentication schemes can be implemented in any language, as long as the executable code can be run by clients. In the modern web infrastructure, this means authentication schemes can be implemented in any format that runs in standard web browsers. New authentication modules can be added to the system, and administrators can choose which are suitable for their particular environment. Administrators can also remove schemes that have a recently-discovered vulnerability or no longer fit their security policy. The administrator may request existing users of removed schemes to select a new scheme and password.

Resistance against password guessing attacks. Despite their ubiquity, the insecurity and lack of usability of user-chosen text passwords and password restriction policies are well-known [15, 31, 35, 52]. There are many alternative schemes that may offer

greater security [3, 4], which are likely to desirable by system administrators. Furthermore, CYOA itself is more resistant to password guessing attacks than any single authentication scheme, since a system-wide password attack must either be prepared to guess passwords for any available scheme or reduce the scope of the attack to the subset of accounts using the targeted scheme(s). However, the security gained by additional schemes is additive, and thus only has a small gain on the number of all possible passwords. Nonetheless, it is still an improvement.

Resistance against phishing. CYOA increases the cost and complexity of launching phishing attacks [10]. A credible phishing site would need to replicate the CYOA module and authentication schemes. This would be particularly difficult for schemes that provide user-dependent cues, like Multitouch Image-Based Authentication [44], Persuasive Cued Click-Points [6], and Use Your Illusion [24]. Without the correct cues, users would most likely be *unable* to enter their actual password, assuming they were not alerted by the incorrect visual cue. This raises the cost of the attack, since the adversary would also have to perform a man-in-the-middle attack, whereby all the user's input on the phishing site are passed to the legitimate site. Alternatively, the attacker could attempt to compromise the legitimate application's CYOA module to obtain the schemes and user-specific pre-authentication information for their own phishing site. However, the CYOA module is no more vulnerable than the application server, since it resides within the application server's domain. Thus, if an attacker breaches the application domain's defences, there is little point in attacking the CYOA module when the application server (which stores all the assets of value) is already compromised.

Expert-certified authentication security. In the simplest form, as discussed above, CYOA could be implemented on the application server as in a typical authentication scheme, but we envision that a network of third-party authentication experts and certification authorities could be organised. The function of this network would be analogous to the academic peer-review or SSL certification processes. Researchers and developers may independently implement novel authentication schemes and submit them to third-party authentication experts who independently analyse, review, certify, and serve these schemes for application administrators to download and plug-in to their CYOA module. Application administrators could subscribe to one or more third-party CYOA scheme certification authorities and thus be relieved from the burden of building or auditing the multitude of possible schemes. However, there is no obligation for application administrators to subscribe to a third-party certifier, so administrators are free to handle the development and/or auditing of schemes if they wish.

Conversely, we could extend the potential role of a trusted third-party. In this three-party architecture, applications subscribe to an authentication authority, and users wishing to register with or log in to the application are redirected to the trusted third-party, who serves the authentication scheme directly to the client. The authentication result is then returned to the application server for storage (at account creation) or verification (at login). Thus, the user performs the password-entry process with a centralised, reputable, and trusted authority, but the hashed password itself is still stored and verified by the application. This decentralised password storage prevents attacks on the third-party CYOA server to obtain users' passwords for subscribing applications, as the authority does not store users' passwords in any form. The third-party authority would be responsible for ensuring the security and integrity of the offered authentication schemes. A third-party CYOA service relieves the burden of maintaining a secure and usable authentication system from the application developers and administrators [12, 16, 21].

4.2 Variations

There are some minor variations that CYOA administrators may consider when integrating CYOA in their applications. First, one of our design goals is to minimise the modifications required to the application server's existing authentication process. As a result, CYOA may not support challenge-response schemes or many biometrics, because they require scheme-specific verification functions. However, CYOA could be adapted to accommodate such schemes by making one of two additions:

- Schemes could be required to include a modular comparison method that CYOA provides to the application server on request. However, this requires the application server to execute code from an external source (i.e, wherever the password verification code originated), which may pose a security risk. Alternatively, the verification function could be executed in a sandbox or virtual machine.
- CYOA schemes could publicly post their verification algorithms for CYOA application administrators to implement themselves. However, this places significant responsibility on the application administrators, particularly if CYOA schemes are added, updated, or removed frequently.

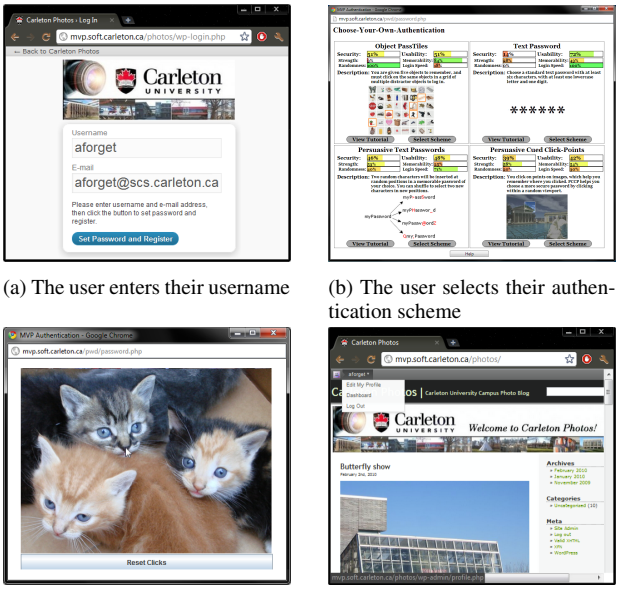
Secondly, many text password systems enforce password restriction policies [21, 31] that constrain passwords' length or character set. Conflicts between the encoded passwords generated by CYOA schemes and the existing restriction policy may occur. We offer two options to resolve this conflict. In most implementations, it should be possible to adapt the restrictions, since CYOA is replacing the text password system. However, some legacy password storage systems may not support arbitrary bit-strings. In this case, the system could convert the scheme-encoded passwords into correctly-formatted bit-strings before storing or validating the passwords. There exist hashing algorithms that output any desired format [43].

Thirdly, CYOA administrators could consider allowing a single user to have multiple passwords to their account, which may be advantageous in some circumstances. For example, users may log in from different locations, some of which may be more vulnerable to particular threats than others (such as in public, where shoulder-surfing is more likely). Thus, the user may wish to log in with a scheme more resistant to their immediate situation's more prevalent threats. Alternatively, CYOA could support multi-factor authentication as well, where the user selects and enters the correct credentials for several chosen schemes, rather than only one.

5. USER EXPERIENCE

The CYOA account creation and login procedure is very similar to the current user authentication process. We illustrate how a user would create a new account for a website using an example web-based implementation of CYOA. The user first navigates to the website's registration page and creates a new account as follows:

1. The user enters their username and submits it to the website (Figure 4a).
2. The user is shown a variety of available authentication schemes (Figure 4b). The user may examine the ratings, descriptions, and tutorials of these schemes. The user chooses an authentication scheme amongst the alternatives.
3. The selected scheme is displayed to the user, who enters and confirms their password (Figure 4c).
4. The user's account is created and may be accessed (Figure 4d).



(a) The user enters their username

(b) The user selects their authentication scheme

(c) The user enters their password (with Persuasive Cued Click-Points [6] in this example)

(d) If the selected scheme and the entered password are both correct, the user is granted access

Figure 4: Example CYOA login user experience.

To log in, users enter their username, are shown their chosen scheme, and enter their password. The user is granted access if the entered password matches the password chosen during registration. If a username for which there is no account is entered, then a random scheme will be displayed and remembered by the system to later be consistently shown for that username, so that potential attackers cannot determine which usernames are valid accounts.

Clients only need a typical web browser to use a web-based implementation of CYOA. Some authentication schemes may use multimedia web technologies (e.g., Flash, Java, Silverlight), requiring an installation. However, we believe most schemes could be implemented with JavaScript, which only requires an up-to-date browser (and most modern browsers automatically update).

This web-based example of CYOA is only one possible implementation. CYOA could also be implemented to specifically target mobile devices, which should only offer authentication schemes appropriate for touch screens and hand-held devices. Another alternative implementation may be across an organisation's workstations, which would enable their administrators to offer only schemes that meet their security and usability requirements.

5.1 Usability Benefits

Accommodates user preference. CYOA allows users to select whichever authentication scheme they wish. Users with better visual memory can choose graphical passwords instead of text, or vice versa. Users may also select schemes offering greater password strength for accounts of higher personal value or risk (e.g., bank accounts). Conversely, users may opt for more memorable (but possibly less secure) schemes for seldom-accessed low-value accounts. Schemes requiring particular hardware (e.g., eye tracker, smart card reader) can be selected when the hardware is available.

Educates about authentication concerns. The CYOA scheme selection interface should provide a description and various ratings for each scheme to help users make their choice. The ratings may be available at multiple levels of granularity. Examples of such ratings include high-level measures of overall security and usability, a list of features supported by the authentication scheme, or more specific measures [4]. Plain-language explanations of the ratings should be available for users to understand their meaning.

Supports accessibility. Current text password systems may pose barriers to people with special needs. For example, people with dyslexia have significantly more difficulty spelling non-words than people without dyslexia [14], which could lead to difficulty with complex text passwords. Users with physical motor-control impairments may use speech recognition software to verbally articulate their passwords. However, users make more errors and are slower when typing with speech recognition software compared to a keyboard [40]. This suggests that speech recognition users require significantly more time to enter text passwords then typists, since text passwords should contain uncommon characters to be secure, and must be 100% accurate for a successful login. CYOA could easily offer authentication schemes that use alternative input methods (e.g., speech, eye tracking) which may better support users with fine-motor control impairments.

Providing an authentication method that is accessible to a newly-registering user, whose abilities are unknown to the system, is a difficult problem [11]. Renaud [42] demonstrates that there is no single authentication solution that can accommodate all users. This highlights the need for CYOA, since supporting multiple authentication methods is currently the only solution to the accessible authentication problem. CYOA could easily accommodate users with accessibility requirements, which have thus far been largely overlooked in authentication research. Newly-developed accessible authentication schemes can easily be added to a CYOA module. CYOA would benefit all users that may have challenges with text passwords. Such users could select a graphical password scheme. Users with visual impairments could choose some form of audio-based scheme. Users with other impairments can similarly select authentication schemes better suited to their abilities.

6. USER STUDY

Given that users typically do not have the opportunity to choose an authentication scheme, our primary research question with respect to CYOA is: *Will users be able to cope with and leverage the power of choice in authentication schemes?* To answer this question, we ran a user study to observe and measure users' behaviour when given a choice of multiple authentication methods:

- ***Text Passwords.*** We included standard text passwords to determine if users would select them over other authentication schemes. Passwords contained at least 6 characters, including at least one lowercase character and one digit.

- ***Persuasive Text Passwords (PTP) [20].*** PTP offers a more secure text-based password scheme than standard text passwords. PTP inserts two random characters at random positions into a user-chosen text password (of at least 6 characters). Users may *shuffle* to have a different random set of characters and positions.

- ***Object PassTiles (OPT) [45].*** OPT is a graphical password scheme where users are assigned five random objects on a 6×8 grid, and select the correct objects to log in. This scheme is an object-based version of the commercial recognition scheme Passfaces [39]. OPT may be more usable than Passfaces because users may have a better memory for distinct objects over faces [27].

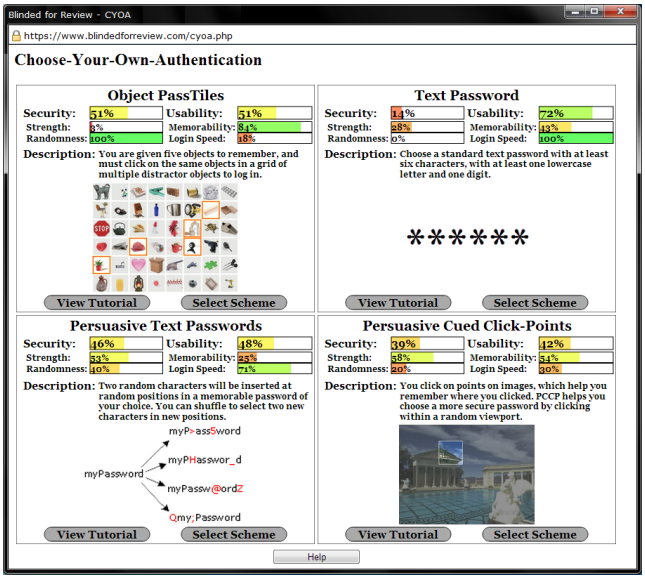


Figure 5: CYOA authentication scheme selection

- ***Persuasive Cued Click-Points (PCCP) [6].*** In PCCP, users are shown five images one at a time and must correctly click on their chosen point on each image. When creating a PCCP password, users must choose their click-points within a randomly-positioned persuasive viewport. Users may *shuffle* to move the viewport to another random position on the image. Comparisons with other graphical password schemes [3] have suggested that PCCP may be one of the more usable and secure graphical schemes currently published.

We specifically chose these schemes for several reasons. First, all of these schemes are well-documented in the literature. Second, these schemes cover the three main memory tasks [38]: Pure recall (PTP), cued recall (PCCP), and recognition (OPT). Third, we believe that each scheme offers unique usability or security advantages. Finally, we felt that offering relatively more complex schemes alongside text passwords would be an effective test of how willing users are to leverage and engage with novel schemes.

The presentation order of the schemes was randomised in a 2×2 grid (Figure 5). It would be an unfair test to require users to select from unfamiliar password schemes without any information about them. To help users choose, we provided a brief description of each scheme, as well as various security and usability ratings based on published authentication research [3, 4, 15, 16, 20, 45, 52]. We acknowledge that these ratings are somewhat subjective and that other rating types and scores are possible. Our intent is not to assess the relative merits of each scheme, but to assess whether users select different schemes when given a choice. Users could mouse-over each rating to see its description. The ratings include:

- ***Security*** is scored as an average of the following measures.
  - ***Password Strength.*** Minimum theoretical password spaces (TPS) [16] were calculated[1]. Schemes with a TPS within a particular range are awarded a proportion of the maximum possible score for this rating. The formula we used to calculate the strength score is $S_{PwdStr} = (TPS - 20) \times 2.5$. TPS values are measured in bits, according to the formula $TPS = log_2(c^n)$, where users' passwords must be at least n selections from c distinct choices [16]. Schemes with a TPS below 20 bits receive a score of 0%, since 20 bits is the bare minimum TPS schemes should support [16]. Schemes with a TPS larger than 60 bits are awarded 100%, since more than 60 bits is considered to provide little additional practical security [3]. To illustrate, text passwords had to contain at least 6 characters, each chosen amongst at least 36 characters (i.e., 26 letters and 10 numbers). Thus, text passwords' strength rating score was $S_{Text} = (log_2(36^6) - 20) \times 2.5 = 27.5\%$
  - ***Randomness.*** Schemes that provide assistance in choosing more secure passwords are scored proportionally to the security increase. Schemes that assign completely randomly-generated passwords are awarded full scores.
- ***Usability*** is scored as an average of the following ratings.
  - ***Memorability.*** Schemes are scored based on available research [6,45] quantifying password recall at least one day after creating the password. This score corresponds to one of two available measures from the longest published user studies: either the login success rate without error [6] or the length of time users could login without error (i.e., *memory time*) divided by the memory time for text passwords from the same study [45].
  - ***Login Speed.*** Login speed is proportional to how fast users entered their password versus text passwords.

[1]Better measures of authentication scheme security [4, 49] were published after this user study was conducted.

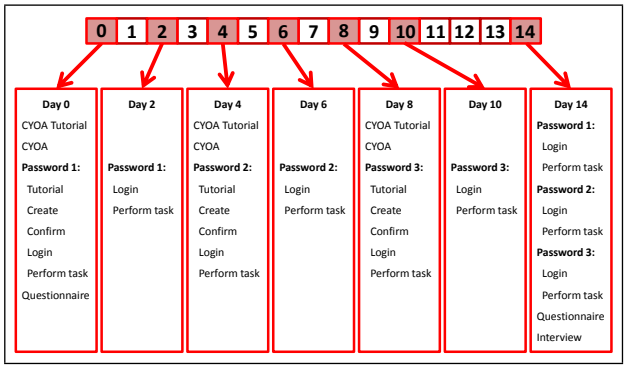


Figure 6: Overview of tasks performed by participants.

Users were offered optional tutorial material to inform their choice of scheme. A tutorial for CYOA itself was shown immediately before selecting a scheme. We also developed hypertext tutorials [19] for each scheme. Users could view a tutorial before making a selection by pressing the *View Tutorial* button for the scheme of interest. When a user selected a scheme, its tutorial was immediately shown.

Over two weeks, participants used CYOA to create and log in to accounts on three websites to perform typical web tasks (e.g., post comments, vote in polls). If users forgot a password, they could reset it by choosing a scheme and creating a new password. Each participant performed the following tasks over two weeks (Figure 6):

Day 0: Participants came to our lab to create an account, log in, and perform a typical web task on the first website. When users were selecting an authentication scheme or creating their password, the experimenter did not provide any additional information. Users also completed a brief questionnaire.

Demographic	# of participants
All	39
Age 19-31	32
Age 34-45	4
Age 60-62	2
Age Not Disclosed	1
Males : Females	22 : 17
Students : Non-students	30 : 9
Undergraduate : Graduate	16 : 23
Engineering and IT	19
Arts or other non-technical	14
Other or unknown	6

Table 4: Demographics summary of participants.

Day 2: Participants were e-mailed a request to log in to their first account and complete a task.
Day 4: Participants were asked by e-mail to visit a second website and create an account (by selecting an authentication scheme and creating a password), login, and perform a task.
Day 6: Participants received an e-mail asking them to log in to their second account and complete a task.
Day 8: Participants were e-mailed a request to visit a third website and create an account (by selecting an authentication scheme and creating a password), login, and perform a task.
Day 10: Participants received an e-mail instructing them to log in to their third account and complete a task.
Day 14: Participants returned to the lab to log in and perform a task on all three websites and complete a final questionnaire.

Since the usability of the available schemes has been assessed elsewhere [3, 4, 6, 45], our study focuses on users' choice of schemes rather than metrics of the particular schemes (e.g., login times, success rates). Thus, we made the following hypotheses:

H1. Scheme selection. For each account password, participants will not select any scheme more often than other schemes.

H2. Informed choice. When first exposed to CYOA, participants who spend more time with the CYOA interface will choose a scheme other than text passwords.

H3. Perception. Participants will rate CYOA positively.

7. USER STUDY RESULTS

We first present the demographics of our sample population, followed by the study's results pertaining to the aforementioned hypotheses. Finally, we present the time participants spent viewing the tutorials and selecting a scheme, as well as scheme re-selection behaviour after password resets.

7.1 Demographics

Table 4 summarises our study's participant demographics. Users were sampled from an online local recruitment system. The mean age was 28 (SD=9.5). All participants used the Internet several times a week. There were slightly more men (22) than women (17). There were more students (30) and people pursuing or holding a graduate degree (23) than expected. However, the study topics and occupations were reasonably varied, including two unemployed and a medical scribe (Other). Although this sample may be more educated than the general population, we believe the diversity is sufficient for this first exploratory study.

Account	Text	PTP	OTP	PCCP
1	14	5	6	14
2	14	2	8	15
3	15	8	9	7

Table 5: Participants' first choice of authentication schemes for each of their three accounts.

1st \ 2nd	Text	PTP	OTP	PCCP
Text	7	0	2	5
PTP	2	2	1	0
OTP	0	0	3	3
PCCP	5	0	2	7

Table 6: Classification of participants according to their scheme selections for their 1st (rows) and 2nd (columns) accounts.

7.2 Hypothesis Testing

H1. Scheme selection. All users' scheme selections for all three account registrations may be found in Appendix A. Table 5 counts how often each scheme was chosen by participants. We performed Chi-square goodness-of-fit tests (against the uniform distribution) to determine if users selected some schemes significantly more often than others. [2] Users showed no significant preference for any schemes when registering their first ($\chi^2(3) = 10, p = .058$) and third account ($\chi^2(3) = 4.0, p = .264$), but did demonstrate significant avoidance of Persuasive Text Passwords (PTP) when registering their second account ($\chi^2(3) = 11.2, p < .05$). We found no clear explanation for this. However, participants showed no significant preference for text passwords.

We also examined how participants' earlier authentication scheme selections may have influenced their later choices. We ran Fisher's Exact Tests [2] on contingency tables counting the number of participants who had chosen each possible pair of schemes for two of their accounts. We found no significant relationship between participants' scheme choices for their 1st and 3rd accounts ($p = .08$) or their 2nd and 3rd accounts ($p = .144$). However, there appeared to be a significant relationship between participants' selections for the 1st and 2nd schemes, which we then examined more closely (Table 6). Coincidentally, five participants switched from PCCP to text passwords, while five others made the opposite switch from text passwords to PCCP. Of greater note, over half (19) of participants chose the same scheme for both accounts, most (12) of which were not text passwords. Table 9 in Appendix A further illustrates that under a third (12) of participants chose the same scheme for all three accounts, under half (5) of which were all text passwords. Overall, our participants appeared willing to adopt and continue using novel and more complex schemes.

H2. Informed choice. We performed a Mann-Whitney U test comparing the total number of seconds spent with the CYOA interface and tutorials between CYOA users creating their first account who chose text passwords and those who chose another scheme. The resulting significant difference ($U = 89, p < .05$) implies that participants who spent more time with the CYOA interface showed a significant preference for schemes other than text passwords. Thus, we accept the informed choice hypothesis. We will more closely examine the time users spent on CYOA in Section 7.3.

[2] We deliberately do *not* apply a correction for families of tests (e.g., Bonferroni) to weaken p-values, since this would favour our hypothesis that we would *not* find evidence.

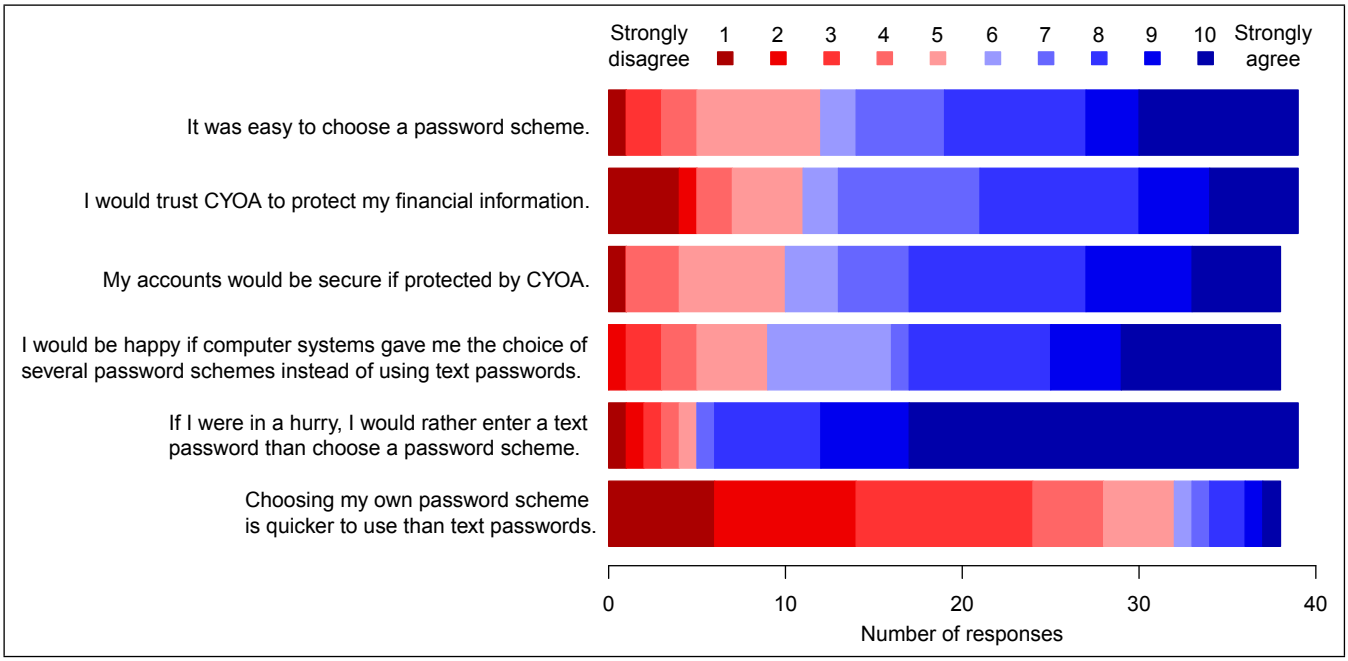


Figure 7: Responses after using CYOA for 2 weeks (1 = "strongly disagree", 10 = "strongly agree", or "prefer not to answer")

H3. Perception. After two weeks using CYOA, participants rated their agreement with various statements, from strongly disagree (1) to strongly agree (10) (or "prefer not to answer"). We report only responses (Figure 7) with significant differences. Participants were generally positive about selecting schemes. They found it easy to choose a scheme ($\chi^2(9) = 22.8, p < .01$), felt it was secure ($\chi^2(9) = 23.1, p < .01$), would trust it to protect their financial information ($\chi^2(9) = 19.2, p < .05$), and would be happy if computer systems gave them a choice of schemes ($\chi^2(9) = 24.1, p < .01$). However, participants preferred to log in with text passwords if they were in a hurry ($\chi^2(9) = 102.3, p < .0001$) and felt scheme selection was not quicker ($\chi^2(9) = 25.2, p < .01$) than text passwords. This is not surprising: scheme selection requires an additional step, and most people have developed rapid text password creation and entry coping strategies, which is not the case for novel schemes.

We also asked participants why and how they chose authentication schemes during their two-week experience. Two researchers independently coded participants' open-answer responses and merged codes into one set of reasons for participants' scheme selections. The bottom row of Table 9 in Appendix A shows that nearly two-thirds of participants (64%) choose schemes they felt would help create a *memorable* password. Under half (46%) of participants chose schemes based on *ease of use*, implying the other half may be willing to tolerate more complex authentication procedures. Only 36% of participants preferred *familiar* schemes, suggesting that almost two-thirds of participants were open to trying unfamiliar schemes. Fortunately, under a fifth (17%) of participants choose new schemes because of *novelty*, suggesting that the observed scheme selection behaviours may persist if our system were widely-deployed. Over one-fifth (21%) of participants mentioned a preference for visual-based passwords. Only 2 participants (5%) specifically stated they favoured text-based passwords. Finally, only 28% of participants chose schemes for security. While this may be cause for concern, we believe there are rational reasons for this result, which we address in Section 7.5.

7.3 Times

Table 7 shows the mean, median, and standard deviation (SD) for time spent with the CYOA tutorial, the scheme selection interface, and the scheme tutorials *before* choosing their first scheme for each of their three accounts. Users spent an average of 86.3 seconds when reviewing the CYOA tutorial for the first time, but only 10.6 when using CYOA for the third time. In all cases, the relatively high standard deviations and lower medians suggest that a most users spent less time than average with the interfaces.

To determine if the decreasing time was a significant trend, we performed a linear mixed-effects regression test on each measure (Table 7). We found an estimated decrease per account of -37.85 seconds for the CYOA tutorial, -18.06 seconds for scheme selection, and -32.21 seconds for scheme tutorials. This confirms that participants took extra time to initially learn to use CYOA, but thereafter only needed a short time to select a scheme.

7.4 Resets

Our 39 participants created 3 different accounts, totalling 117 scheme selections. Throughout the study, users could reset any of their account passwords (if they forgot) and select a different scheme. Despite users initially choosing different schemes for their accounts, we wondered if most users would forget their password and change to text passwords. Table 8 contains the number of accounts where users initially chose one scheme (rows) and either *never* reset their password, or reset at least once and ended the study with another scheme (columns). Summing the Never (reset) column shows that passwords for 61 accounts were never reset, implying that these accounts' users remembered their passwords over two weeks. Just under half (29, 48%) of those were text passwords. Furthermore, summing the rows shows that 74 (63%) of the accounts, users first chose a scheme other than text passwords. Of those 74 accounts, only 23 (31%) of them were changed to a text password. We believe this 31% attrition to text passwords suggests that most users are willing and able to remember passwords from more complex schemes and will *not* flock to text passwords.

Account	CYOA Tutorial (secs)			Scheme Selection (secs)			Scheme Tutorials (secs)		
	Mean	Median	SD	Mean	Median	SD	Mean	Median	SD
1	86.3	78	50.6	52.2	33	39.9	64.4	0	142.6
2	24.1	13	22.9	19.9	14	22.4	0	0	0
3	10.6	6	11.2	16.0	9	20.4	0	0	0
Sig. Test	$SE = 3.92, t = -9.67, p < .0001$			$SE = 3.09, t = -5.85, p < .0001$			$SE = 9.44, t = -3.41, p < .001$		

Table 7: Time spent viewing the CYOA tutorial, scheme selection interface, and scheme tutorials before choosing a scheme.

	Never	Text	PTP + OTP + PCCP
Text	32	10	1 (= 0 + 0 + 1)
PTP	6	4	5 (= 4 + 1 + 0)
OTP	10	6	7 (= 1 + 6 + 0)
PCCP	13	13	10 (= 1 + 4 + 5)

Table 8: Number of accounts where users initially chose one scheme (left, rows) and either *Never* reset their password, or reset at least once and ended the study with either a text or a novel password scheme (top, column).

7.5 Discussion

H1. Scheme selection. We were concerned that users would be unwilling to engage with unfamiliar schemes and would largely default to choosing text passwords, but we found no evidence that this occurred. Participants chose text passwords less than 40% of the time (Table 5). Furthermore, we found no patterns in the schemes users selected across accounts (Table 9). We believe this suggests that users may be willing to choose alternative schemes.

Curiously, participants demonstrated a significant aversion for the Persuasive Text Passwords (PTP) scheme for their second account. Since this seems unlikely to be a random occurrence, the reason for this result should perhaps be more closely examined in future work. We speculate that participants desiring a text password may have felt that this account, a vacation destination discussion forum, did not warrant the additional password strength provided by PTP. This actually seems a rather rational choice [25]. We agree that PTP is better suited for accounts where additional protection is required, such as an online bank account.

H2. Informed choice. As expected, participants that were more willing to engage with the CYOA interface were also more likely to try novel schemes. This suggests that the CYOA interface itself may be a crucial factor in encouraging users to choose different schemes. Clearly, detailed information about CYOA and the schemes should be available for users to make an informed decision. Furthermore, should novel scheme adoption be initially low, adding persuasive elements [17] to the CYOA interface may be particularly effective at encouraging users to select different schemes.

H3. Perception. Likert-scale responses suggested that participants welcomed the ability to choose an authentication scheme and expressed confidence in CYOA's security. However, participants were concerned about the speed and ease of CYOA in comparison to text passwords. This suggests that CYOA may be particularly desirable for applications where the need for security is more obvious. In such situations, users may desire additional authentication choices and be willing to spend a little more time and effort, particularly since less than half of participants chose schemes based on either familiarity or ease of use.

Memorability was the most-frequently cited criteria for selecting authentication schemes. However, most participants did not state security as a factor. We believe this is another rational outcome [25] for the following reasons. First, participants may have trusted the administrators (i.e., researchers) to provide only schemes that were secure. Second, participants may have felt strong passwords were not needed for an account created in the context of a study. Finally, participants may not have felt much risk to the online community-type accounts used in the study.

This suggests two lines for future inquiry. Researchers should examine scheme selection could be simplified by testing different CYOA user interface designs. Furthermore, differences in CYOA user behaviour between high-risk (e.g., online banking) and lower-risk applications (e.g., blogs, forums) should be examined.

7.6 Limitations

Since this level of freedom of user choice in authentication schemes has never been previously examined, we chose to first test users' behaviour in a short-term lab-field hybrid study to determine if CYOA shows any promise before launching more extensive studies. As a result, our user study and results have a number of limitations that should be openly disclosed. First, our participants were mostly well-educated students, which is not representative of the general population. Also, our study's websites were specifically created for authentication scheme experiments [5]. We went to considerable length to create a typical online experience with engaging content. However, users still may not have been intrinsically motivated to perform the tasks and generally behave as they would have for websites and accounts they regularly access and greatly value. Furthermore, we were careful to not influence participants in any way. We told users we were evaluating the websites' usability and not that we were evaluating CYOA specifically, but participants may still have realised the study was focused on the authentication system, since it was inevitably the most unusual aspect. It is currently unclear how users' behaviour would change if they were to choose a scheme for an account they highly value and/or regularly use over a long period of time. To fully address these ecological validity challenges in future work, CYOA would need to be tested in a field study with real accounts that users value highly and must access to accomplish user-motivated (rather than experimentally-requested) primary tasks.

8. WORKSHOP REMARKS

This subsection summarises the three predominant CYOA discussion topics at the 2015 New Security Paradigms Workshop.

8.1 Biometric authentication

The consumerisation of biometrics was posited as rendering knowledge-based authentication (KBA), and thus CYOA, obsolete. As discussed in Section 4.2, CYOA could support biometrics, which we believe could be improved with further research and testing. Another consideration for future work is the implications and practicality of biometric authentication to a local device versus a remote server. Additionally, past work has discussed why KBA (particularly text passwords) will continue to persist for the foreseeable future [26], and that no one single scheme is sufficient for all users and contexts [4]. Thus, we believe the need for research in offering

multiple authentication schemes will increase, particularly as biometrics become less expensive, more accurate, and gain adoption.

While biometric authentication has noteworthy strengths, it can pose new privacy, security, and usability challenges. Firstly, knowledge-based secrets are typically easy to change if they are lost or compromised, while biometrics typically have limits on how easily or frequently they can be changed (i.e., humans only have two eyes, ten fingers, and so on). Knowledge-based secrets can easily be shared between users for account sharing, while biometric systems need to explicitly add this functionality. Apple's Touch ID handles this by allowing several fingerprints to be registered where any one of them will unlock the device. Finally, all accounts for different services that require the same biometric are all personally linked to the same user, which poses very serious privacy risks, since information stored in these different accounts could be linked together without the user's knowledge, let alone informed consent.

8.2 Natural selection of authentication schemes

Some workshop participants commented that CYOA provides a Darwinian approach [9] to authentication schemes. For example, schemes that would be "selected against" include recently-broken schemes that can be quickly and easily deprecated from a CYOA system, as well as schemes that are difficult to use or do not appropriately fit the system's context. Conversely, secure schemes that people find usable across devices and environments would be "selected for" and become increasingly popular, thereby continually improving the overall fitness of the authentication scheme ecosystem (or "market", as a participant remarked). It was also noted that industry-based authentication initiatives (e.g., FIDO alliance [13], Daon [8], maximID [34]) could support CYOA. Password managers could also take an approach similar to CYOA [47].

8.3 To choose or not to choose

Participants in a study comparing Android pattern authentication to PINs [51] felt patterns were quicker and more accurate than PINs, even though the reverse was actually true. This raised the question of whether the community should be designing systems to manage for users' expectations or reality. One's intuition may be to let users choose whatever they like, but psychology research has shown demotivational effects of additional choices [29]. However, our and other recent work [46, 50] has shown that users apply diverse strategies towards authentication, so we believe the community should support users in making informed choices.

9. CONCLUSION

Despite text passwords' long standing as the ubiquitous authentication scheme, users continue to face challenges in creating secure and memorable passwords. Researchers and professionals struggle to replace text passwords despite many proposed alternative schemes. It seems unlikely a single scheme will surpass the convenience of text passwords. Thus, offering users a choice of multiple authentication schemes, each with unique features that cater to different users' preferences, abilities, and usage contexts, may be a promising solution to this long-standing authentication problem.

This paper provides two novel contributions towards solving the authentication problem. Our first contribution is Choose Your Own Authentication (CYOA): a generalised technical architecture to deploy and support a world with many authentication schemes. There are many benefits to our architecture for all primary authentication stakeholders: end-users, administrators, and researchers.

Users benefit from CYOA in numerous ways. CYOA accommodates users' preferences, usage context, and cognitive and physical abilities. CYOA can provide descriptions of the available schemes and expose users to some of the security and usability issues in authentication, which may help users form better mental models and become more proficient in creating secure passwords. CYOA can promote authentication accessibility, since schemes designed to support users with disabilities could easily be added.

System administrators also benefit from our proposed architecture. CYOA can easily replace existing text password systems currently used in practice. Authentication schemes can be easily added, removed, or configured to suit administrators' security and usability requirements. CYOA increases resistance against password guessing and phishing attacks. CYOA also allows the delegation of authentication security management to experts, since administrators may not have the expertise of authentication specialists.

Researchers can also leverage CYOA in many ways. It can be used as a platform for prototyping, testing, and distributing novel authentication schemes. Schemes can easily be implemented as a CYOA authentication module and made available to fellow researchers and CYOA administrators for verification and adoption into their own CYOA systems in practice.

The second contribution is an exploratory user study of how users cope with and leverage the power of choice in authentication schemes. Over two weeks, users interacted with CYOA by choosing a scheme for each of three online accounts and periodically logging in to them. Most participants selected more complex schemes and did not resort to always choosing text passwords. We found no evidence that participants favoured text passwords (or any one scheme) over the other more complex schemes. Participants found it easy to choose a scheme and they were sufficiently confident in CYOA's security that they would trust it to protect their financial accounts. This user study of CYOA focused on users' behaviour and impressions when choosing from previously-unfamiliar authentication schemes, which has not been previously examined. These contributions, the CYOA technical architecture and first exploratory user study, offer a first step towards a world with many secure and usable authentication schemes.

10. ACKNOWLEDGEMENTS

We thank the New Security Paradigms Workshop participants for their insightful comments and discussion during the peer-review process and the workshop itself, particularly Mike Just for his shepherding and clarification of reviewers' helpful comments. We also thank Lorrie Faith Cranor for providing the facilities and personnel for data collection and coding, Saranga Komanduri and Pedro Leon for their statistical consultations, Emily Forney for her data collection assistance, and Sarah Pearman for her proofing and formatting assistance. This work was part of the first author's doctoral thesis [18], which was supported by the Natural Science and Engineering Research Council of Canada (NSERC) and partial funding from the NSERC Internetworked Systems Security Network (ISSNet). The second author holds a Canada Research Chair in Human Oriented Computer Security and acknowledges NSERC for funding her Chair and Discovery Grant.

11. REFERENCES

[1] A. Adams and M. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12), 1999.

[2] M. Belk, C. Fidas, P. Germanakos, and G. Samaras. Security for diversity: Studying the effects of verbal and imagery processes on user authentication mechanisms. In *IFIP TC13 Conference on Human-Computer Interaction (INTERACT)*. Springer, 2013.

[3] R. Biddle, S. Chiasson, and P.C. van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4), 2012.

[4] J. Bonneau, C. Herley, P.C. van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Symposium on Security and Privacy*. IEEE, 2012.

[5] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. F. Machado, A. Forget, N. Wright, G. Chan, and R. Biddle. The MVP web-based authentication framework. In *International Conference on Financial Cryptography and Data Security (FC)*. Springer, 2012.

[6] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P.C. van Oorschot. Persuasive Cued Click-Points: design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 9(2), March/April 2012.

[7] N. Clarke and S. Furnell. Authentication of users on mobile telephones – a survey of attitudes and practices. *Computers & Security*, 24(7), 2005.

[8] Daon. Case study: USAA, October 2015. **http://www.daon.com/identityx/usaa-download/**.

[9] C. Darwin. *On the Origin of Species by Means of Natural Selection, or the Preservation of Favoured Races in the Struggle for Life*. John Murray, 1859.

[10] R. Dhamija, J. Tygar, and M. Hearst. Why phishing works. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2006.

[11] P. Fairweather, V. Hanson, S. Detweiler, and R. Schwerdtfeger. From assistive technology to a web accessibility service. In *International Conference on Assistive Technologies (ASSETS)*. ACM, 2002.

[12] L. Falk, A. Prakash, and K. Borders. Analyzing websites for user-visible security design flaws. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2008.

[13] FIDO alliance, October 2015. **https://fidoalliance.org/**.

[14] R. Fink. Literacy development in successful men and women with dyslexia. *Annals of Dyslexia*, 48(1), 1998.

[15] D. Florêncio and C. Herley. A large-scale study of WWW password habits. In *International World Wide Web Conference (WWW)*. ACM, May 2007.

[16] D. Florêncio and C. Herley. Where do security policies come from? In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, July 2010.

[17] B. Fogg. *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann Publishers, 2003.

[18] A. Forget. *A World with Many Authentication Schemes*. PhD thesis, School of Computer Science, Carleton University, 2012.

[19] A. Forget, S. Chiasson, R. Biddle, and P.C. van Oorschot. Can old dogs learn new password tricks? Supporting learning of novel authentication schemes. In *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (E-Learn)*. AACE, 2012.

[20] A. Forget, S. Chiasson, P.C. van Oorschot, and R. Biddle. Improving text passwords through persuasion. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2008.

[21] S. Furnell. An assessment of website password practices. *Computers & Security*, 26(7-8), 2007.

[22] E. Hammer. Introducing OAuth 2.0, May 2010. **http://hueniverse.com/2010/05/introducing-oauth-2-0/**.

[23] E. Hammer-Lahav, D. Recordon, and D. Hardt. The OAuth 2.0 authorization protocol draft. Technical Report Draft 25, IETF, March 2012. **http://tools.ietf.org/html/draft-ietf-oauth-v2-25**.

[24] E. Hayashi, N. Christin, R. Dhamija, and A. Perrig. Use your illusion: Secure authentication usable anywhere. In *Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, July 2008. ACM.

[25] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *New Security Paradigms Workshop (NSPW)*. ACM, 2009.

[26] C. Herley and P.C. van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, January-February 2012.

[27] M. Hlywa, A. Patrick, and R. Biddle. Facing the facts about image type in recognition-based graphical passwords. In *Annual Computer Security Applications Conference (ACSAC)*. IEEE, 2011.

[28] P. Inglesant and M. Sasse. The true cost of unusable password policies: Password use in the wild. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010.

[29] S. Iyengar and M. Lepper. When choice is demotivating: Can one desire too much of a good thing? *Journal of personality and social psychology*, 79(6), 2000.

[30] A. Jain, A. Ross, and S. Pankanti. Biometrics: A tool for information security. *Transactions on Information Forensics and Security*, 1(2), June 2006.

[31] S. Komanduri, R. Shay, P. Kelley, M. Mazurek, L. Bauer, N. Christin, L. Cranor, and S. Egelman. Of passwords and people: Measuring the effect of password-composition policies. In *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2011.

[32] S. Landau and T. Moore. Economic tussles in federated identity management. *First Monday*, 17(10), 2012.

[33] LastPass, October 2015. **https://lastpass.com/**.

[34] maximID, October 2015. **http://maximid.com/**.

[35] R. Morris and K. Thompson. Password security: A case history. *Communications of the ACM*, 22, 1979.

[36] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, December 2003.

[37] A. Paivio, T. Rogers, and P. Smythe. Why are pictures easier to recall than words? *Psychonomic Science*, 11(4), 1968.

[38] J. Raaijmakers and R. Shiffrin. Models for recall and recognition. *Annual review of psychology*, 43:205–234, 1992.

[39] Real User Corporation. The science behind Passfaces, 2004.

[40] C. Rebman, M. Aiken, and C. Cegielski. Speech recognition in the human-computer interface. *Information and Management*, 40(6), 2003.

[41] D. Recordon and D. Reed. OpenID 2.0: A platform for user-centric identity management. In *Digital Identity Management Workshop*. ACM, 2006.

[42] K. Renaud. Quantification of authentication mechanisms - a usability perspective. *Journal of Web Engineering*, 3(2), 2004.

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

[44] F. Schaub, M. Walch, B. Könings, and M. Weber. Exploring the design space of graphical passwords on smartphones. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.

[45] E. Stobert and R. Biddle. Memory retrieval and graphical passwords. In *Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2013.

[46] E. Stobert and R. Biddle. The password life cycle: user behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2014.

[47] E. Stobert and R. Biddle. A password manager that doesn't remember passwords. In *New Security Paradigms Workshop (NSPW)*. ACM, 2014.

[48] Sun Microsystems. Unified login with pluggable authentication modules (PAM), October 1995. **`http://www.kernel.org/pub/linux/libs/pam/pre/doc/rfc86.0.txt.gz`**.

[49] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Conference on Computer and Communications Security (CCS)*. ACM, 2013.

[50] B. Ur, F. Noma, J. Bees, S. Segreti, R. Shay, L. Bauer, N. Christin, and L.F. Cranor. "I added '!' at the end to make it secure": Observing password creation in the lab. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX, 2015.

[51] E. Von Zezschwitz, P. Dunphy, and A. D. Luca. Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices. In *International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI)*. ACM, 2013.

[52] M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Conference on Computer and Communications Security (CCS)*. ACM, 2010.

APPENDIX

A. SCHEME SELECTIONS

	Scheme selections			Stated reasons for scheme selections					
Participant	Account 1	Account 2	Account 3	Memorability	Ease of Use	Familiarity	Security	Visual	Novelty
P1	PTP	Text	Text		X				
P2	PCCP	PCCP	OPT	X			X		
P3	PCCP	PCCP	PTP	X		X			
P4	Text	Text	Text	X		X	X		
P5	OPT	PCCP	PTP	X	X		X		
P6	PCCP	Text	OPT	X					
P7	Text	Text	PTP			X			
P8	PCCP	PCCP	PCCP	X	X				
P9	Text	Text	Text		X	X			
P10	Text	OPT	OPT	X	X	X	X		
P11	PCCP	PCCP	Text		X		X		X
P12	PCCP	PCCP	PCCP		X		X	X	X
P13	Text	Text	Text	X		X			
P14	PCCP	PCCP	PCCP					X	X
P15	OPT	PCCP	OPT	X					
P16	Text	Text	Text	X		X			
P17	Text	PCCP	Text		X	X			
P18	PTP	PTP	PTP						X
P19	PCCP	Text	Text		X	X			
P20	OPT	OPT	Text			X			X
P21	PTP	PTP	PTP				X		
P22	PTP	Text	Text	X					
P23	PCCP	Text	OPT	X	X				
P24	Text	Text	Text	X		X			
P25	Text	PCCP	Text	X	X				
P26	OPT	PCCP	Text	X		X	X		
P27	Text	Text	PTP		X	X			
P28	Text	OPT	PCCP		X				
P29	OPT	OPT	OPT	X			X		X
P30	PCCP	OPT	PCCP	X				X	
P31	PCCP	PCCP	PCCP	X				X	
P32	PCCP	Text	PTP	X			X	X	
P33	PTP	OPT	OPT		X				X
P34	Text	PCCP	Text	X	X				
P35	PCCP	OPT	PTP	X			X		
P36	Text	PCCP	OPT	X	X			X	
P37	OPT	OPT	OPT	X				X	
P38	Text	PCCP	Text	X	X	X			
P39	PCCP	Text	PCCP	X	X			X	
Sums (and percentages) of stated reasons				25 (64%)	18 (46%)	14 (36%)	11 (28%)	8 (21%)	7 (18%)

Table 9: Users' scheme selections when registering for their three accounts, and their stated reasons for said selections. Schemes are distinguished by colours:

(Text on red): Standard text passwords

(PTP on yellow): Persuasive Text Passwords

(OPT on green): Object PassTiles

(PCCP on blue): Persuasive Cued Click-Points