Towards Supporting a Diverse Ecosystem of Authentication Schemes

Alain Forget
Carnegie Mellon University
aforget@cmu.edu

Sonia Chiasson
Carleton University
chiasson@scs.carleton.ca

Robert Biddle
Carleton University
robert_biddle@carleton.ca

ABSTRACT

Many authentication schemes have been proposed, each with strengths and weaknesses. We introduce Choose Your Own Authentication (CYOA); a novel authentication architecture that enables users to choose a scheme that best suits their preferences, abilities, and usage context. CYOA could easily replace existing text password systems. There are numerous benefits to CYOA, including a three-party architecture would enable delegating the management of authentication systems to trusted-third parties.

1. INTRODUCTION

Despite text passwords' problems, it seems unlikely any single novel authentication scheme will replace text, since no one scheme outperforms text passwords by all measures [2]. Perhaps users should authenticate with whichever scheme offers the security, usability, and accessibility appropriate for the given user, account, and threat model.

A selection of authentication methods was first proposed as administrator-selectable Pluggable Authentication Modules (PAMs) [3] for UNIX-based systems. OpenID [4] proposed that users could choose between identity providers based on which authentication scheme they offered. Google Android users may unlock their mobile devices with text passwords, PINs, swipe patterns, or facial recognition, or download and install third-party authentication schemes.

These architectures could give provide a vast choice in authentication schemes, but there are challenges to address. First, PAM and Android's schemes are system-dependent unless completely re-implemented. OpenID is more generalised, but it is mainly intended as a single sign-on protocol, rather than supporting multiple authentication schemes. Second, people may have no reason to trust third-party authentication applications as there is no assurance they are securely implemented. Third, there is little published research on either how users select authentication schemes or how to architect and maintain systems to support multiple authentication schemes.

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

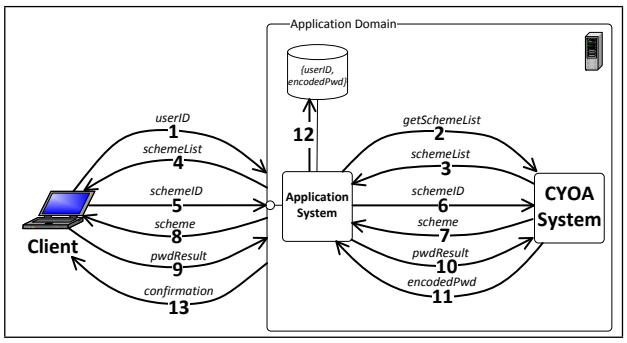

Figure 1: Basic two-party CYOA architecture where the application server and CYOA module are managed by the same organisation.

2. CYOA PROTOCOL

We introduce Choose Your Own Authentication (CYOA); an architecture that provides several authentication alternatives to users. In all cases, three main entities are involved in the encrypted protocol: The user remotely authenticates with their ***client*** machine, the ***application server*** hosts the resources requiring authentication, and the ***CYOA module*** that stores and manages the data and code necessary for the CYOA architecture to function. In its simplest form, the CYOA module can simply be part of the application server as any typical authentication scheme.

We will illustrate how CYOA would work on the current Internet infrastructure, where the application is an arbitrary web-based service or resource for authenticated clients. In this scenario, the user would navigate to the application website's registration or login page and proceed as illustrated in Figure 1: (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 sends a list of schemes and relevant data as a web form 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 confirm their password. Any necessary communication between the chosen scheme and the CYOA server during password creation or entry would occur between this step and the previous one. (10) The application server sends the password string to the CYOA module. (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 given username. (13) If the user is registering a new password, the user is sent confirmation of the successful registration. If logging in and the encoded passwords match, the user is granted access. Otherwise, access is denied.

2.1 Discussion

CYOA provides numerous technical and usability benefits:

Easy adoption for existing systems. Since CYOA authentication schemes also return encoded passwords as strings, as do modern password systems as hashed password strings, integrating a CYOA module into an existing password system requires only minor modifications.

Supports most knowledge-based authentication (KBA) schemes. Most KBA schemes already encode passwords as a string, and thus are supported by CYOA.

Modular architecture. The CYOA module itself is designed modularly, so system administrators can add, modify, or remove 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.

Third-party expert-certified authentication security. We envision a network of third-party authentication experts and certification authorities. Researchers and developers may implement and submit novel schemes to these authorities who independently analyse, review, certify, and serve approved schemes for application administrators to download and plug-in to their CYOA module. We could extend the role of the trusted third-parties, whereby applications could redirect users wishing to register or login to the trusted third-party, who serves the authentication scheme directly to the client, and returns the authentication result to the application server for storage or verification. A third-party CYOA service would relieve application administrators of the burden of maintaining an authentication system.

Resistance against password guessing attacks. System-wide password guessing attacks against CYOA 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).

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 select schemes with greater password strength for accounts of higher personal value or risk, or more memorable (but possibly less secure) schemes for low-value accounts.

Educates about authentication concerns. The CYOA scheme selection interface should provide a description, tutorial, and various ratings [2] for each scheme to help users make their choice. The ratings may be available at multiple levels of granularity. These interface elements provide numerous opportunities to teach users how to behave securely.

Supports accessibility. Current text password systems may pose barriers to people with special needs (e.g. people with dyslexia or fine motor-control impairments). Dyslexic users could select a graphical password scheme. Users with visual impairments could choose some form of audio-based authentication scheme. CYOA could easily offer authentication schemes that use alternative input methods (e.g., speech, eye tracking) which may better support users with special needs. To our knowledge, supporting multiple authentication methods is currently the only solution to accessible authentication problems.

There are also a number of open questions to be explored:

How can CYOA support challenge-response and biometrics? To minimise required modifications to the application server's existing authentication process, CYOA may not support challenge-response schemes or many biometrics, because they require scheme-specific verification functions (rather than a simple comparison of hashes).

How should legacy systems with password restriction policies be accommodated? There may be conflicts between the encoded passwords generated by CYOA schemes and legacy systems' password restriction policies that limit password contents.

How could CYOA automatically determine each user's preferences and requirements? Belk et al. [1] recently proposed providing users either a text or graphical password, depending on their cognitive abilities, as determined by controlled in-lab psychometric tests. It would be ideal if CYOA could automatically determine users' abilities and usage context, and suggest the most appropriate scheme.

How can trust in CYOA be provided to all authentication stakeholders? For everyone to fully benefit from CYOA, reputable organisations of authentication experts must be willing to support a third-party CYOA service. User and application administrators must have confidence in said organisations' expertise to review and certify authentication schemes. Users also must have confidence they are entering their password to the correct third-party.

We must address these and other issues for everyone to benefit from the diverse ecosystem of authentication schemes.

3. REFERENCES

[1] 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.

[2] 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 *IEEE Symposium on Security and Privacy*, 2012.

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

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