A BIO-key® Solution.

White Paper

6 Unique Techniques for Simplified Web Access

Table of Contents

Introduction 3

Summary 3

Death of the Password - The Debate 3

The Sci-Fi Paradigm 4

Authentication Pain Points 5

Advances in Simplified Web Access 5

6 Unique Techniques 6

A No Password Approach 6

A Hot Key Is All It Takes 7

One Time Personal Password Generator 8

Transparent Logins 10

Kerberos Throughput 10

True Challenge Question Authentication 11

Static and Dynamic KBA 11

Conclusion 13

Modern Marvels 13

Resources 14

Introduction

Summary

Modern web access is a loaded gun – finding the right balance of usability and security often leads to a heavy weight being placed on one side or the other without any real progress being made. With constant debates over the relevance and impact of current web access scenarios, finding a solution to provide the best possible choice can be difficult at the best of times.

This paper serves to address the current state of web access, as well as provide a series of techniques that we believe can address legitimate end-user concerns and problematic web-access scenarios in a secure, yet convenient manner.

Death of the Password - The Debate

In 2004, Bill Gates famously declared, "…the password is dead."[i] In a way, he may very well have been right – just not in the sense that most people understand it. Here we are, more than a decade into the future from a bold claim made by a major player in the digital community, and the password is still the source of such a strong, opinionated debate.

Two Sides of the Same Coin - A Double-Edged Sword

Without even meaning to, most users fall on either one side of the fence or the other in terms of the password debate, and they argue vehemently from their own experience.

On the one hand, we have users and authentication experts who agree with Bill Gates that the password is dead, or that, at the very least, we need a better alternative for our day-to-day authentication[ii]. From that side of the debate, citations and references are made to the increasing amount of data breaches that occur due to weak credentials, or lack of secure password policies – basically the standard weaknesses that one might think of when the question is posed. It comes down to risk – the password is viewed as antiquated, vulnerable and too high-risk to associate with anything of real value anymore. For that reason, many authentication experts and typical users see the password as a remnant of old days with no place in modern authentication.

On the other hand, many users and authentication experts still see the benefit of the password – especially in collaboration with additional credentials. The old adage 'if it ain't broke, don't fix it' might not apply in full, but fixing the password is much easier than removing it altogether. In some ways, it may also be more effective. Often, the debate comes to rest on the shoulders of the end-users, for whom usability remains king. In that regard, the password has remained stalwart on the throne.

The Sci-Fi Paradigm

The password debate is a similar type of situation as illustrated by the various popular science fiction books that have flooded the market throughout the last decade or two – or even the last century for that matter: when it comes to technological advancements as a society, we are never where we think we should be.

Think of popular science fiction such as the works of H.G. Wells or Stanley Kubrick's 2001: a Space Odyssey, and compare the various predictions from these works to the world of today. Of course, some things actually managed to hit the mark, but there are still a wide variety of technological assumptions from sci-fi that never hit the mark.

Technology that Never Took

- Time Machine
- Antigravity
- Complex Artificial Intelligence
- Manned Deep-Space Travel
- Flying Cars
- Teleportation

What this illustrates is the tendency that we have as a society to dream big, even if we don't always hit the mark. Authentication has followed a similar trajectory – predicting the complete eradication of the password, which has clung to life for an additional decade and then some beyond its projected term of life.

In a word, the invention of new, innovative technology comes down to need. Take the idea of flying cars for example – it is interesting and fun to think of, but the need for flying cars has never been of the dire sort. We ask ourselves, "Will this make my life better," and "Will this make life simpler" and the realistic answers to those questions don't always reflect the size and depth of our dreams and aspirations.

Of course, that does not make the results of such strides in innovation any less impressive or important.

Will this make my life better?

Will this make my life simpler?

Authentication Pain Points

Modern authentication has developed at a rapid rate in order to combat realistic pain points stemming from individual, actual end-user problems. Regardless of where a user falls on the debate of the utility of the password, various pain points are common in just about any authentication situation - indeed, issues with the password have even led to various innovations for combatting these pain points.

Common Authentication Pain Points

- Managing Multiple Passwords
  - Remembering Multiple Password
  - Choosing Unique Passwords for Each Account
- Password Policy Compliance
- Cumbersome Multifactor Requirements
- Account Lockouts/Forgotten Password
- Repetitive
- Time-consuming

The bigger we dream, and the more we advance, it seems like we sacrifice convenience for the sake of security. However, despite these many pain points, various advances in web access have come about to provide creative, simple to use web access for end-users.

Advances in Simplified Web Access

We may not have killed the password yet, but as a society we have certainly tried. With the release of new operating systems and end-user devices, authentication has been turned on its head so often that following the trends is a veritable nightmare.

Throughout the last decade alone, end-users have been introduced to:

- Protocol-based Single Sign-On
- Detailed Self-Service
- Secret picture verification
- Photo authentication
- Handwriting recognition
- Typing style confirmation
- Voice recognition
- Fingerprint reading
  - Mobile Authentication
  - Banking Access

6 Unique Techniques

One of most influential pain points stems from issues of convenience: end-users want to have access to various applications and accounts without the hassle associated with memorizing and managing multiple passwords or additional factors. Authentication solutions that build upon convenience without sacrificing security offer a variety of simple and usable web access scenarios based on this user-driven feedback.

Here are six unique ways to implement simplified web access to improve usability and convenience for end-user authentication.

A No Password Approach

In recent years, the digital world has seen a major uptick of Multifactor Authentication (MFA) solutions – the prime purpose of which is to add an extra layer of security to the password during a user login request. Initially, Multifactor Authentication (also known simply as Two-Factor Authentication or 2FA) involved the use of a bulky, somewhat expensive hardware token to provide a unique code that would be entered alongside the initial password. For the most part, the process itself hasn't changed much in recent years – though it has become more streamlined, and more delivery methods for the unique code (typically referred to as a One-Time Password) have been developed to help instill a sense of convenience and usability to the process.

The biggest issue for most people, however, is the continued presence of a password throughout the Multifactor Authentication process. While most agree that MFA significantly bolsters the strength of the login, the combination is still seen as an inconvenience by many. In answer to that worry, a new, innovative idea for simplifying web access has arisen: a no password approach.

In order to provide a higher level of convenience and usability without detracting too much from the increased security of MFA, an Identity Provider (IdP) can be configured to accept the One-Time Password as the standard password for the login. This no password approach makes use of a fluid, constantly changing passcode to login, without relying on the proposed security of a static password that can be lost, forgotten, stolen, or otherwise compromised.

As an additional level of interest, this innovation for web access provides additional benefits for many users who have issues with the standard login process that may be seen as outside of the norm. In scenarios where access needs to be quick and seamless without the possibility of forgetting a password or being locked out, or where users may be even be unable to remember a simple password – there are two methods for end-users to consider: typing in a dynamic OTP, or connecting a token directly to the machine.

Typing in a Dynamic OTP

Devices such the RSA SecurID Token and software solutions such as the Google Authenticator provide a legible, constantly changing OTP that is compatible with most IdPs. In order to login, the end-user need only type in the OTP in the required field – which replaces the standard password input – to gain access to his/her account.

Connecting the Token to the Machine

Some tokens, such as the YubiKey[iii] will plugin to the machine directly via an open USB port. Once connected, a YubiKey generates a constantly changing password with each login request, and even finalizes the login process for the end-user. This functionality will remove the hazards and hassle from standard authentication situations, and provide end-users with a much higher level of convenience during logins.

Audience to Benefit from a No Password Approach

- K-12 Students
- Individuals with Special Needs
- Warehouse Workers
- Police Officers
- Doctors & Nurses

A Hot Key Is All It Takes

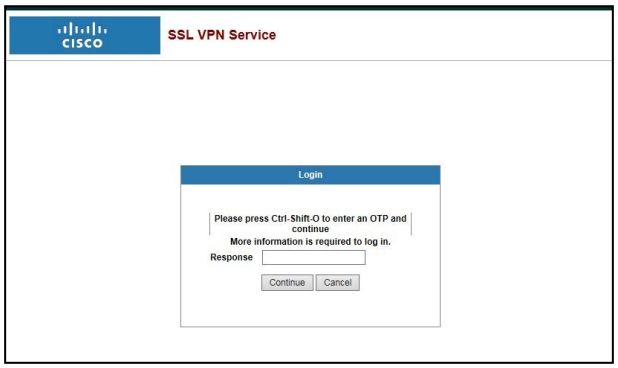
A hot key is a short series of key presses (either simultaneously or in a specific order) that result in a definitive action occurring on the computer in question. In terms of simplified web access, OTP delivery can now be enacted by something reminiscent of bringing up the task manager with the CTRL-ALT-DEL shortcut.

In this instance, the end-user attempts to login directly as he/she normally would, and the IdP will prompt the user for an OTP to verify identity. At this point, the user need only key in a pre-determined hot key combination to gain access to the secured account.

For many users, entering an OTP by hand is obtrusive and inconvenient even at the best of times. Enabling hot key OTP delivery circumvents this hurdle to authentication, providing usability for users who absolutely must enact Multifactor Authentication.

Audience to Benefit from Hot Key to OTP Delivery

- Remote Access Employees
- VPN Network Administrators
- ETC.



One Time Personal Password Generator

It almost goes without saying that those of us who still use a static password have a hard time remembering even one good one, let alone ten or twelve.[iv] In order to keep up with our many accounts, while still adhering to authentication best practices, it is a nightmare of memory to try and make dozens of strong, unique and complex passwords to satisfy various password policy requirements.

Putting that much strain on and end-user, even if it doesn't weigh heavily on the surface, is never a good thing. End-user frustration accounts for a large portion of unsecure authentication practices, and is a problematic issue that has seen several innovative solutions come about in recent years. In terms of simplifying the requirements on end-users to recall dozens of different passwords a day, a daily password generator could be just the right combination of simplicity and complexity that an end-user needs. (Image of the PG Mobile Generator in line)

A unique, daily password generator typically manifests as a mobile application (though some work just fine in a web browser) which points to a central directory or user repository. The software would require an end-user to enroll by answering various personal questions about him/herself. Ideally, an administrator can configure these questions in order to step away from typical questions that may be easy to bypass through social engineering. While the password can be used within a standard password policy (I.E. Expire after a set number of days, etc.), an administrator can also configure the policy at the user, group, or other organizational unit level in the user repository in order to make the password valid for one-time only. This increases the security of the login, and provides end-users with a simple, quick method of logging in without any extra password fatigue.

The Process for Generating a Unique Daily Password:

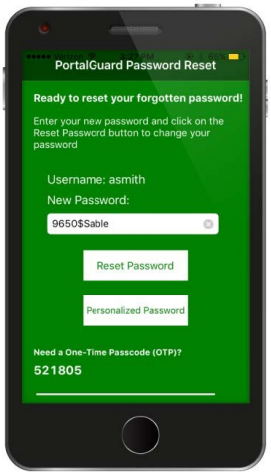
- Open the application
  - Enroll if needed
- Tap Personalized Password
- Continue to Tap Personalized Password until you approve your new Password
  - Tap Set Password
- Revel in your New Familiar Password

The familiar, daily password generator will become the new password immediately once it is set, and can go a long way towards taking the weight of password fatigue from the shoulders of the end-user.

For additional convenience without sacrificing security, a daily password generator can be used in combination with an IdP that provides Single Sign-On to eliminate the need to remember other passwords alongside the daily generated one.

Audience to Benefit from a Unique Daily Password

- Mobile Access Users
- Employees that require Infrequent Access
- Forgetful Individuals
- ETC.



The PortalGuard Mobile Password Generator

Transparent Logins

With the commercial use of Single Sign-On came a new wave of convenient application access throughout a wide range of verticals. Users typically have upwards of 15 accounts to access on a daily basis, and the increasing number of login prompts and passwords that are required to be entered takes an additional toll on daily activities – reducing end-user productivity and compliance with corporate standards.

However, by using Single Sign-On, an IdP can be configured to accept the initial login of a workstation (typically the Windows Login) as leverage for the reset of the applications needed by a specific end-user. This transparent login simplifies web access by eliminating login prompts and password fields altogether – simply providing the end-user with unfettered access to each web application necessary to complete various day-to-day activities.

This innovation requires administration to configure web-applications for SAML access through the chosen Identity Provider. Once this is accomplished, access can be specified to specific applications at the User, Group or even Domain levels in the user repository

Audience to Benefit from Transparent Logins

- Students
- Faculty
- Staff
- Standard Employees
- Hospital Staff
- Individuals who require access to multiple web applications throughout the day

Kerberos Throughput

Unfortunately for some organizations, not all necessary web applications support SAML authentication for Single Sign-On (SSO) using Transparent Logins. However, end-users still deserve convenient methods of achieving web access, and thankfully there are other options to enable SSO.

Kerberos Authentication[v] is nothing new to the web access game – having been designed and released as an Internet Engineering Task Force (IETF) Standard in 1993 – and works with many different applications to provide SSO through a trusted IdP. In order to achieve transparent, convenient authentication to multiple web applications that do not support SAML or other SSO protocols, a server-based proxy can be configured and used by an IdP to streamline the authentication process.

Additionally, the proxy server also supports forms-based authentication to prevent end-users from having to enter passwords in multiple times for legacy applications that were not built to support SAML, Kerberos, or other SSO protocols.

Audience to Benefit from Transparent Logins

- Organizations with Applications that do not support SAML
- Users that rely heavily on Legacy Applications
- Hybrid organizations currently moving to an updated system
- ETC.

True Challenge Question Authentication

Challenge Question Authentication is typically referred to as Knowledge-based Authentication (KBA). Whether we realize it or not, just about every person who uses a digital account today has been exposed to KBA – at least in the simplest form. Think about any time that you have forgotten a password and been asked to provide the correct e-mail that is on file for that account, or the color of your first car, or your mother's maiden name; these types of question and answer scenarios are examples of classic knowledge-based authentication.

Over the years, KBA itself has seen a drastic change both in function as well as public opinion. When the Internet first began and records were hard to come by, KBA was a strong method of securing information without requiring too much of the end-user. Now that much information is readily available online, the benefits of KBA are often undercut as a security weakness – an authentication tactic that has not kept up with the times. Which brings to mind a misunderstanding of just what exactly KBA is and what it can do.

Static and Dynamic KBA

Knowledge-based authentication comes in two forms: static and dynamic. Both forms have their own benefits, but most individuals do not realize the true value of detailed KBA.

- *Static KBA*

Static KBA is the most typical form of KBA: it involves a service provider asking predetermined questions of the user, who provides answers that are stored with the service provider to be used during authentication at a later time. Static KBA is typically used as a fail-safe for account recovery or forgotten password resets – and is widely viewed as an exhibition of poor security.

Additionally, end-users often find Static KBA to be hindrance to convenience, as they often cannot remember the answer that was provided during initial enrollment. Such scenarios lead to weaker, more typical answers being provided, which serves to defeat the purpose. Audience to Benefit from Transparent Logins

With an appropriate authentication solution, an IdP can provide administrators with the ability to fully customize static KBA questions – reducing the likelihood of standard, expected questions by asking end-users relevant, unique questions known only to them.

- *Dynamic KBA*

Dynamic KBA involves the use of challenge questions that are generated on the fly in real time. These questions are typically comprised of information compiled from public and private data that the service provider has access to – sometimes this involves information that is only present in the user repository. As the name would suggest, the dynamic nature of this form of KBA provides an additional layer of security that can help deter social engineering attacks and researched information from granting unauthorized access to an end-user account.

True challenge answer authentication takes the best aspects of KBA – the dynamic capabilities, true customization and variability, etc. – and provides end-users with the option to use a series of questions alone in order to gain access to their accounts. If done correctly, users can gain access to their accounts without ever needed to remember another password to login – they simply need to be able to answer questions specific to their own identity.

Of course, some might associate this with the walled gardenvi issue: the idea that using only a form of KBA for a login actually increases the risk of account compromise. If an attacker manages to breach the wall and enter the garden, they would have full range of access from within.

However, administrators are given full access to customize and configure questions alongside true dynamic KBA in order to put a huge burden on attackers trying to gain access. Also, the benefits of challenge answer authentication come down to an assessment of risk: accounts that require access to less sensitive materials would benefit from this form of authentication, as it would help to streamline access without impeding usability, while administrators and users with access to more sensitive data would be required to proceed with additional authentication methods.

Audience to Benefit from True Challenge Answer Authentication

- Low-risk user accounts
- Infrequently accessed accounts
- Temporary Workers
- Contractor's
- Etc

Conclusion

Modern Marvels

With the amount of end-users that make constant use of various applications and services throughout the day, truly simplified web access without sacrificing necessary security is a modern marvel in its own right. Authentication is one of those common activities that we all face on a daily basis but take for granted – so much so that when a truly beneficial solution is presented to us, it has an instantaneous, far-reaching impact on the rest of our daily lives.

Truly advantageous authentication techniques may not impact the world on an immediately apparent scale, but the impact of simplified web access on the lives of the individual cannot be overstated. Providing sustainable, simplified web access and a uniquely improved end-user experience will change the lives of your users, and those users can change the world.

Resources

[i] http://www.zdnet.com/article/gates-the-password-is-dead/

[ii] https://securityintelligence.com/passwords-are-dead-we-need-a-better-system-now/

[iii] https://www.yubico.com/products/why-yubikey-wins/

[iv] https://nakedsecurity.sophos.com/2014/10/17/average-person-has-19-passwords-but1-in-3-dont-make-them-strong-enough/

[v] http://www.faqs.org/faqs/kerberos-faq/general/

[vi] https://en.wikipedia.org/wiki/Closed_platform

