Authlogics

WHITEPAPER

Pattern-based Authentication

Solving the Password Problem

www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Authlogics may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Authlogics, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Authlogics on the issues discussed as of the date of publication. Because Authlogics must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Authlogics, and Authlogics cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. AUTHLOGICS LTD MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Copyright © 2021 Authlogics Ltd. All rights reserved.

CONTENTS

SYNOPSIS

Every day Fortune 500 companies with "sophisticated" password policies are being hacked. Users are overwhelmed by password requirements and the businesses that are forcing them to increase password complexity are beginning to find that this tactic has the opposite effect; users weakening their passwords simply so that they can remember them. Passwords are becoming more complex for humans to use and easier for machines to crack.

In the following pages, we will delve into the password problem, how this method is today doing more harm than good, and how pattern-based authentication can eliminate the problem.

Mitigate Risk &
Password Reliance

Regulate
Compliance

Go Passwordless
Secure & Replace Passwords

INTRODUCTION

Think of the last time you unlocked a mobile device or entered a PIN at an ATM, how often do you look at the keypad to complete the password? Do you find your fingers follow an automatic pattern without you actually thinking about it? That is the case for most of us. Passwords have become an unavoidable part of our lives. As our engagement with computers, mobile devices, cloud-based applications, and websites grows, so does the list of passwords we have to manage. They have become more expansive and at the same time, less effective as an authentication mechanism. If we are all hard-wired to remember patterns and shapes, what would it mean to use this psychology to create a better login system?

By utilizing the mind's preference for thinking in patterns and shapes, rather than letters, numbers and words, we can create a solution that provides improved security over passwords and provides a better user experience.

Simple & Memorable Login

Reduce Helpdesk Calls

Increase Employee Productivity

THE PASSWORD PROBLEM

Passwords came into existence to keep systems and their users safe, from banking through to internal business systems where IP and user data need to be protected to save from hacking, identity theft, and the safekeeping of private intellectual property.

First used for computers in 1961, passwords have remained relatively unchanged until today. But the world has changed, and the humble password is failing to protect us.

Fortune 500 companies are being attacked and hacked every single week. Traditional password policies are failing. Considering the regularity of breaches, it seems wise that most businesses force users to regularly change passwords, as well as setting requirements for length and complexity. However, with passwords now requested by every app, system, and log-in that users interact with on a daily basis (all requiring different, unique passwords), the ability for users to follow the advised guidelines has become near impossible. As a result, users have begun to work around the set guidelines, reproducing the same passwords for multiple systems, reducing their strength, and risking the security of the users and organizations whose system they're interacting with.

Existing solutions are no longer working for us. They are making things harder for users and easier for machines to crack. With computing power as it is today, breaking through a password can literally be done in a matter of seconds with barely any effort.

Continuing in a direction that makes this process more difficult for users will only lead to more workarounds that put businesses at greater risk of a breach. Passwords need to go.

80% OF CYBERATTACKS ARE DIRECTED AT PASSWORDS COSTING THE GLOBAL ECONOMY ON AVERAGE $2.9 BILLION PER MINUTE

Source: World Economic Forum

PATTERN-BASED SECURITY SOLUTIONS

From significant research in the field of Cognitive Neuroscience, a popular theory called dual coding (Paivio, 1969, 1983, 1986) has emerged which shows us that graphical objects such as pictures, images, or shapes are better remembered than words or number sequences. This is because this method gives the brain more stimuli, and ultimately leads to better short-term and long-term memory recall.

Building onto the Paivio theory, Weldon and Roediger (1987) claimed that the more data was encoded with conceptual processing, the better it would be recalled. Pictures and shapes have more conceptual encoding than words and numbers and therefore are easier to remember(1).

Additional studies within the Neuroscience community show that people both think and read in shapes, not letters and words. It is for **tihs vrey raeosn taht you sohlud hvae no prlboem redaing tihs snteence dsetpie the dielebarte eorrrs**. The premise of this belief is that our thoughts and language are broken down into shapes/patterns and stored and recalled as such. When reading the earlier sentence, despite many apparent flaws, provided the first letter and the last letter within the word are correct, the rest of the word's shape is what the mind expects and therefore can be decoded (read) accordingly. Even experienced journalists and proof-readers make errors, as mixed up letters in words can be hard to consciously spot.

As a result of these studies, popular memory improvement techniques such as Graphical and Textual mnemonics have become well-proven aids to assist people with memory recall and are particularly popular with students the world over.

REAL WORLD PATTERN RECALL

Without consciously understanding why, many people regularly realise that they have a greater recall of patterns over words and numbers. We can all identify with the real-world scenario where we withdraw cash from an Automated Teller Machine (ATM).

Typically, ATMs require a 4-digit PIN to prove who you are. A 4-digit PIN should be simple to remember, however, faced with infrequent usage of the PIN, or large numbers of PINs to remember, people often enter a pattern sequence on the keypad instead of thinking about the actual PIN number - because it's far easier to remember the pattern, than it is to remember a random 4-digit number.

The same can be said for mobile phone lock screens, burglar alarm control pads or any system requiring pin entry on a numerical keypad. The examples below show how a user remembers their PIN code; visualising the keypad and "drawing" the pattern by entering the numbers in the correct sequence to make the same shape as the pattern in their memory.

A square pattern = PIN 1793

Linear zig-zag pattern = PIN 1570

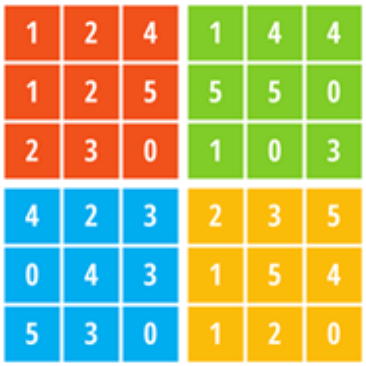
UTILISING PATTERN-BASED RECALL FOR AUTHENTICATION

When banks tried to deter “shoulder surfing” attacks by moving numbers around on the keypad, this broke customer’s pattern-based recall process and led to many failed ATM transactions, resulting in the system being abandoned.

By turning this concept on its head and separating the idea of the pattern away from the PIN, we can create a unique authentication method with a number of interesting benefits. If one were to capture a user’s pattern, one would use the numbers entered only to verify that the correct pattern had been entered. In the previous example, we know the user has a square pattern because of the numbers entered – 1793 – and the sequence in which they were entered. But once we know the pattern, we can use any series of numbers or letters to determine if the user has entered the correct pattern, and change this sequence on a regular basis. Unlike passwords, the pattern is never transmitted between the user and server, only the one-time code that is generated for as long as that sequence of numbers is valid.

The following steps show how a user would set their pattern and log into an application or device:

A user chooses a pattern on a grid. The grid should be large enough to create enough variation in possible pattern combinations, and small enough not to overwhelm them with options, especially during the pattern recall.



When a user logs onto a device, they are presented with a grid of numbers. This can be on the same device, or the grid generation can take place separately, to add multiple factors to the authentication process.

The user combines the position and sequence of the pattern they memorized with the unique grid that is displayed to them, to create a one-time code that is centered in place of a password.

ADVANTAGES OF A PATTERN-BASED AUTHENTICATION APPROACH

Introducing pattern-based authentication comes with a range of obvious benefits-improved security for both users and businesses being the number one, but let's explore some of the other advantages:

Patterns Are Not Divulged

When users enter a password, this password is divulged to the system so that it can confirm the password is correct. This leaves a footprint of the password and opens up room for potential breaches. Unlike passwords, patterns are not transmitted between the user and the server, meaning that hackers cannot access the pattern.

Shoulder Surfing Risk is Reduced

When someone is spying over a user's shoulder, they are looking out for the numbers or letters of the password, rather than the pattern. With pattern-based authentication, learning the code means nothing for the thief, as the code will change from minute to minute - only the pattern remains the same.

Avoid the effort and expense of Multi-Factor

Pattern-based authentication can be used with efficacy in isolation to allow users to login with a one-time code, without the need for a second physical device. This makes for a quick and low-cost deployment and is a drop-in replacement for a password login.

Step up to Multi-Factor when needed

Where stronger authentication is required, the user can enrol a device as a second factor - a mobile phone or tablet, for example. This adds an additional layer of security, as the challenge grid is physically separate to the logon. The user would have to have control of the device and know the pattern to logon. This step up in security is seamless to the user as the logon experience is the same.

Easy Integration

Pattern-based authentication can be easily integrated into networks and applications via standards-based methods such as SAML and RADIUS, which require no developer interaction.

CONCLUSION

Endless cases of major corporation password breaches tell us unequivocally that this security method is failing. In 2018 alone over 5 billion data records(2) -- corporate passwords and email addresses-- were exposed and compromised. 81 percent of these were the result of a stolen or weak password.

Putting stricter policies in place to increase the complexity of passwords and make it more difficult for users to remember is a useless endeavor that is merely making matters worse.

With the sophistication of hackers today, and the accessibility of password hacking programs, no amount of increased complexity is going to solve the password problem. The password has to go.

Pattern-based authentication eradicates the password problem by creating a one-time code from a pattern that only the user knows. Tapping into user's hard-wired ability to remember patterns and shapes, pattern-based authentication guarantees organizations a level of security that the password has long been unable to provide, whilst also reducing lock-outs and calls to the help desk

Separating the pattern from the PIN, pattern-based authentication is familiar to users, therefore easy to adopt, with no possible workarounds that could threaten the security of the system or the user.

ABOUT AUTHLOGICS

Award-winning(3) authentication experts Authlogics are committed to assisting IT managers improve security while making it easier for users to access their information. Authlogics focuses on helping your business transition from password-driven environments, while increasing your security posture and compliance to policy.

PINgrid pattern-based authentication is included as part of Authlogics Authentication Server, one of the core components of the Authlogics product suite. PINgrid is an enterprise-ready authentication solution designed for risk-appropriate authentication situations such as Internet Banking or workflow accountability. To find out more about Authlogics and our products and technologies, please visit our website at www.authlogics.com or contact us:

APPENDIX

(1) Altering retrieval demands reverses the picture superiority effect. Authors: Mary Susan Weldon & Henry L. Roediger, ©Springer Nature Switzerland AG: https://www.researchgate.net/publication/19491984_Altering_retrieval_demands_reverses_the_picture_superiority_effect

(2) The Year-End 2018 Data Breach Report. Authors: © Risk Based Security Inc. https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report

(3) Authlogics were awarded Best Password Compliance & Replacement Specialists for two consecutive years 2019/2020, Cyber Security Awards and SC award for Best Secure Transaction Solution, PINgrid (Winfrasoft) 2013, https://www.scmagazineuk.com/article/1481951

PATTERN-BASED AUTHENTICATION WHITEPAPER

CALL

UK/MEA +44 1344 568900

US +1 408 706 2866

EMAIL

sales@authlogics.com

CORRESPOND

329 Doncastle Road,

Bracknell, Berks

RG12 8PE, UK

Authlogics