Authlogics

Strong Authentication Made Simple

The Problem with Passwords

The use of passwords alone to secure access to systems is no longer effective.

Whitepaper

Authlogics, 12th Floor, Ocean House, The Ring, Bracknell, Berkshire, RG12 1AX, United Kingdom
UK Tel: +44 1344 568 900 US Tel: +1 857 214 2174 email: info@authlogics.com web: http://authlogics.com/

Introduction

Authenticating people to computers and services is a classic case of human versus machine interaction, coupled with a security problem. Most existing solutions fail to recognize the human factor and are hence weakened. Here we discuss the problem, common attempts at solutions and how Authlogics' PINgrid solves this problem.

The Problem with Passwords

One of the earliest recorded uses of passwords was by Roman legions who used passwords to identify themselves to remote garrisons, and so gain admittance. Passwords were first used for computers around 1961 and have continued largely unchanged to this day. The world, however, has since changed, making computer passwords inefficient and virtually ineffective.

There are two principal reasons why passwords are now failing:

Firstly, we now access services that are remote and where the network can conceal an attacker. In the case of a Roman legion identifying itself to a garrison, you would not get many guesses before you were in serious trouble. Today's attackers are hidden by the Internet and so can guess for as long as you let them. Even if you limit the number of guesses an attacker can make then users are locked out creating a denial of service attack against yourself.

Secondly, the computing resources to exhaustively (brute force) guess a password is now easily and cheaply available to anybody who might want them.

Common responses have been to suggest using 'strong' passwords. We are told that a strong password is something that has to be long, has to be complicated, and must be something you change regularly. We are told this keeps passwords safe. In reality, we are just making things harder for humans to use and easier for machines to guess and to crack. These days with computing power, breaking through a password is literally done in seconds and without any great difficulty. You can use uppercase, lowercase, numbers and special characters. It really doesn't make a significant difference to a computer trying to crack a password. It is no longer 1961.

Of course, the more complicated we make a password for a machine to break, the harder we make it for a human to remember. There is a tendency in computer security to blame users for being the weakest link when attempting to put in measures to protect an organization from a breach. And sometimes that may be true. But, when forced to pick hard to remember passwords, as well as being required to change these frequently, it is no surprise that users forget passwords or write them on post-it notes as a last-ditch resort at trying to remember them.

A great case in point is the image captured during a photo shoot with Prince William containing login details for a military system on the wall behind him. Even the Ministry of Defence is not exempt from the password challenge. This is the real world and this example shows the extent of the problem. Another problem with hard to remember passwords is that some will use the same password again and again. Every time Adobe gets hacked, Facebook recommends, "Please change your password". This is because they know that people use the same password across multiple sites.

Keeping anything a secret with the Internet these days is pretty difficult to do. Are passwords actually secret? The only way to keep something secret is to never give it away. Like any secret, you can't tell anybody what it is. However, every time you use a password or a PIN code, you're giving it away. Anybody could be watching you type it, could be capturing your keystrokes through keyloggers or could actually watch you do it, such as through hacked cameras in ATM machines. The sheer fact that you are sharing it means it's no longer a secret. It is an oxymoron. As soon as you share something it's no longer secret. There isn't a single silver bullet that is going to solve the problem with passwords in its entirety. Passwords, as we know them, are flawed.

Attempts at finding solutions

Passwords on their own are flawed. But how about adding an additional form of authentication to them? This is referred to as two-factor authentication. Whether this is achieved through the use of a token or app, or in some other way, the basis of 2-Factor Authentication is to add something the user has to something the user knows, i.e. the password. Please note that most such solutions are therefore just a second layer on top of a password. These solutions are sticky tape on top of the problem without actually solving it. Therefore, all of the aforementioned challenges still apply. And generally, most users or consumers dislike this type of solution, as they are inconvenient and expensive.

What about biometrics? A big question exists around who stores the biometric data and can they be trusted. The basic problem is that any biometric information is an unchangeable part of you. If the organizations you trust to store this information are breached, as many organization are these days, there is no way for you to change your biometric information, other than surgery.

What remains is that despite all of these challenges you still need to be able to provide access to your company's intellectual property to your user-base and customers. Users expect to work and be productive pretty much anywhere these days. And restricting your customer's ability to do business with you is a recipe for sending them to your competitors!

And what about providing protected remote access to your mobile workforce or people working from home? As well as your cloud applications and your HR system? Or your customer portals containing sensitive customer data? There are laws and regulations around the protection of data.

But what if there were a password that is easy to remember, and changes every time you use it? At Authlogics we've developed a technology that does just that.

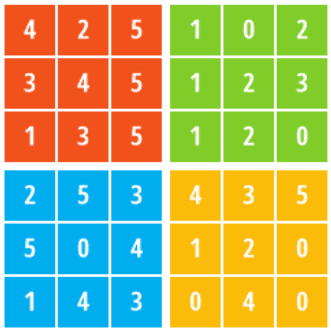
Strong Authentication Made Simple

Authlogics' PINgrid is based on research findings into how people remember. People are far better at remembering shapes than arbitrary text, such as a password. One of the key attributes of PINgrid is that it only expects a user to remember a pattern they have chosen themselves.

To authenticate themselves, users mentally overlay their pattern onto a grid of numbers presented to them. Their passcode is made up of the numbers located under their pattern.

The grid of numbers changes regularly and is random. This means that the numbers entered will differ every time, even though the persons pattern remains the same. As a result, PINgrid allows the user to retain their secret, unlike the disclosure that occurs when dealing with traditional passwords.

These are some of PINgrid's advantages:



1. You have a single user experience whether its used in a browser, on a phone, PC, tablet, ATM machine, etc. PINgrid keeps things simple and consistent.
2. The enrolment process is very fast. You can deploy tens of thousands of users in a matter of minutes.
3. Authlogics can provide 1.5 Factor through to 3 Factor Authentication to match your risk appetite.
4. PINgrid integrates into existing systems and workflows. You can integrate it into the applications you use today. If you need to provide access to the expenses system, great! Add PINgrid to authenticate at that point. It is not a complicated thing to engineer. Choose 1.5, 2 or 3 Factor Authentication as necessary to manage the risk.

Conclusion

There can be little doubt that the use of passwords to secure access to systems is no longer effective. With improved means of attack and users' inability to remember increasing numbers of increasingly complex passwords, the password's time is up. What is needed is a solution that is user-friendly while allowing the organization to manage its risks appropriately.

Authlogics has this solution in PINgrid, a technology that is already in use around the globe and which uses cognitive research to simplify the users' task.

About Authlogics

Authlogics provides IT security professionals with a fresh alternative to legacy authentication and transaction verification methods. We help companies remove the reliance on password-based authentication and hardware tokens, and encourage the use of self-service capabilities. We eliminate costs and administration surrounding card readers and keyring tokens and innovate without the need to implement expensive biometrics.

Whether you want to authenticate to a Web portal, VPN, firewall, or to a multitude of different Cloud providers, Authlogics offers a range of authentication methods to suit your business. Our solution provides 1.5, 2 and 3 Factor Authentication options, via three authentication technologies (PINpass, PINphrase & PINgrid) and can be delivered via the Web, Mobile App, Email or SMS/TEXT. Additionally, we have several integration agents for various 3rd party systems should you need them.

PINgrid

PINgrid is an award-winning and patented multi-factor authentication and transaction signing solution that is being used in the public and private sector today to transform any mobile device into a soft-token, via a simple offline application, replacing passwords with a memorable pattern that automatically generates a One Time Code (OTC).

PINphrase

PINphrase is a memorable word technology where users are asked for random letters from answers they already know to log in, instead of providing a full password. PINphrase is the only off-the-shelf solution that delivers this type of technology used by many banking websites.

PINpass

PINpass is a 2 and 3 Factor OATH compliant 6 - 8 digits random code solution. This standard is widely adopted by many vendors and is well trusted. PINpass turns a mobile device into a token via an App or by sending an OTP via SMS or e-mail. Like most OATH solutions, PINpass works with a fixed PIN code which must be remembered, however, it can also be used with an AD password or work in PIN-less mode.