Authlogics

Strong Authentication Made Simple

Two-Way Identification Using PINgrid

Solve the customer identification dilemma whilst cutting 50% of the call time

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

Social engineering techniques are growing in sophistication and as a result, customers who are trying to verify themselves to a calling bank or utility provider may be inadvertently giving away their confidential information to scammers posing as legitimate businesses. A two-way identification process is required to give both the caller and recipient of the call certainty of each other's valid identity. Here we discuss the problem and how Authlogics' PINgrid solves this problem.

The Identification Dilemma

Sometimes it is the simplest attacks that cause the most damage.

We are all too familiar with the attacker who uses their technical savvy to infiltrate protected computer systems to compromise sensitive data. This type of hacker is in the news all the time. This in turn motivates those responsible for the protection of sensitive data to invest in new technologies to further arm network defences.

However, there is another breed of attacker who uses their tactics to circumvent our tools and solutions. They are the social engineers who specialize in exploiting the one weakness found in every organization: human psychology. Using phone calls and social media, these attackers trick people into offering them access to sensitive information. While this type of fraud has been around for a long time, attacks of this type have recently increased, as has the associated media interest.

With growing reliance on IT systems, the protection of user data housed within IT systems has become critical. Despite both physical and legislative stringent controls are continuously being introduced and enforced, the fight continues and is evident everywhere.

To conform with data-protection legislation, corporations must take steps to ensure that a client's identity is verified prior to engaging in a communication. We have all experience the following scenario: Your bank or utility provider phones you to discuss a matter. However, before telling you what they want to talk about, one is bombarded with a battery of 'security' questions to prove that you are who you say you are.

Frequently, the questions asked and answers provided were, typically, established a long time ago. These questions tend to follow a similar pattern, such as "state your mother's maiden name", "what is the city of your birth", and so forth. Of course, most of these questions can be answered by studying an individual's social media pages.

Using them for security may not be the best approach, especially when it's pertaining to the security of your phone banking facility which does require a high level of security.

We are conditioned to expect a pattern of answering questions when contacted by banks and utilities. This expectation exposes a client to a ridiculously simple and dangerous attack. While answering questions correctly may well prove the client's identity to the bank, how does the customer know that the person phoning is actually from the bank? Even if the caller works for the bank and has access to all your details, how do you know they won't pass those details onto someone who can use those 'secure' details to impersonate you in future.

Two-Way Identification using PINgrid

The only way to solve this problem is to find a mechanism that allows a client to verify that a caller is actually who they say they are. This verification has to be done in a way that does not allow a simple replay attack at a later time.

Authlogics' PINgrid is an award-winning multi-factor authentication and transaction verification solution, provides an easy solution to this problem when used to as a two-way identification solution.

PINgrid's patented technology is being used in the public and private sector today to transform any mobile device into a soft-token, via a simple offline app, replacing passwords with a memorable pattern that automatically generates a One Time Password (OTP).

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.

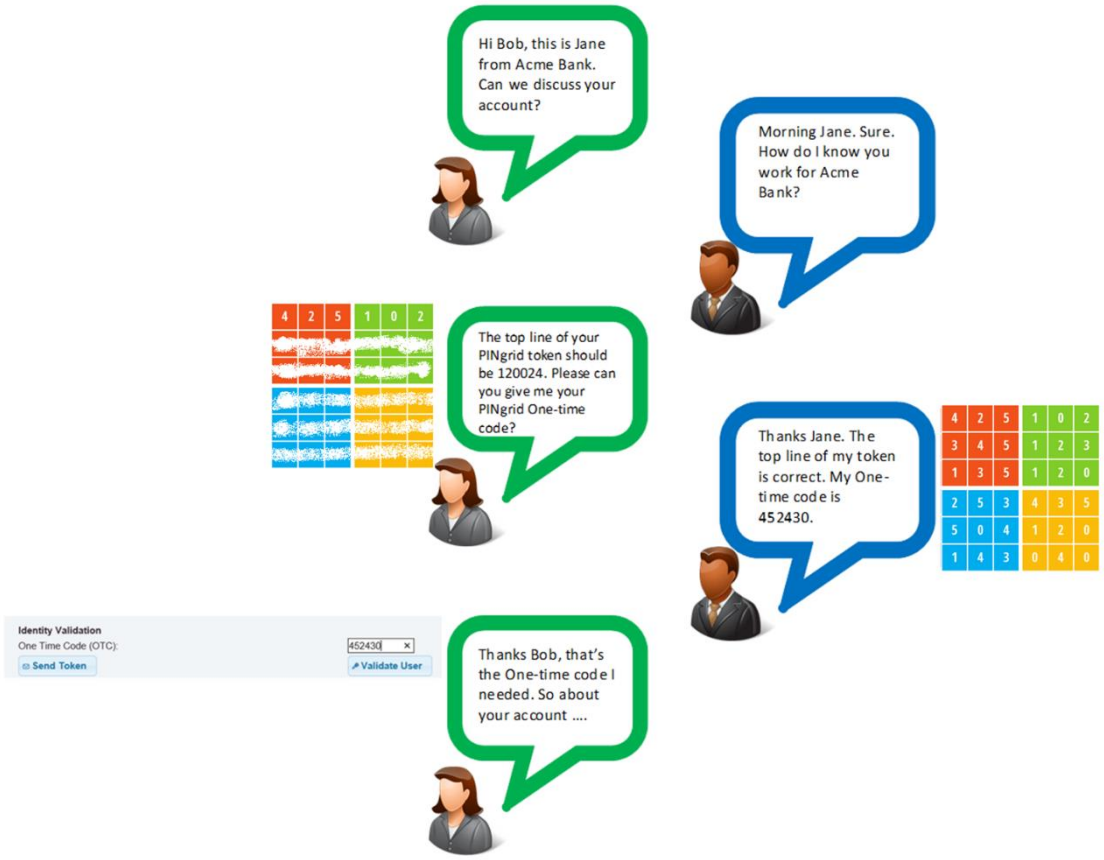
The grid of numbers changes regularly and is random. This means that the numbers entered will differ every time, even though the user's pattern remains the same. Unlike conventional password based solutions, the 'password' is never disclosed.

How PINgrid Achieves This

In this situation, rather than authenticating the user to the organization, the organization authenticates itself to the user. Looking back at the bank / utility scenario described earlier, this is how PINgrid will help. A banking customer called Bob, receives a call from a bank agent called Jane. To continue the call, the bank, Jane, must verify herself to the customer, Bob. And vice versa, Bob must verify himself to Jane.

So Bob receives a phone call from the bank he checks his bank supplied application on his smart-phone. The application will show a fresh PIN grid, just as he might use to login to Internet banking. On her system, Jane can see only the top line of the PINgrid challenge grid visible to Bob within his PINgrid application. Jane reads out these numbers to Bob who, looking at the application, can verify these numbers. If they match, Bob will know for certain that Jane is indeed an agent calling from his bank.

Now that Bob trusts Jane, Jane can ask Bob for his PINgrid one-time code which he then supplies. Jane enters this code into her system. Once the system accepts this code as being correct, Jane can be sure that Bob is indeed Bob.



By using PINgrid for the two-way identification process, two key features have been accomplished. Firstly, Jane and Bob can be certain that the other is who they say they are thus ensuring data-protection legislation, corporate policy and general best practices have all been satisfied. Secondly, none of the information exchanged thus far is of a sensitive nature which might be used maliciously in the future.

Conclusion

While Authlogics' PINgrid is most commonly used to provide multi-factor authentication to secure remote access solutions, desktop login access, web portals and Internet sites, it can easily be configured to securely verify the identity of two parties engaged in sensitive discussions. By configuring PINgrid as outlined, it is easy to both authenticate a customer and assure them you are the business you say you are. Considering the recent increase in social engineering scams, this may be the way forward in securely identifying all parties that are subject to a conversation.

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 banks we web sites.

PINpass

PINpass is a 2 and 3 Factor OATH compliant 6 - 8 digit 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.