Authlogics

Deviceless OTP

Technology Drilldown: Issues and merits of Deviceless OTP technology

White Paper

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Introduction

A key feature of any secure environment is being able to ensure that only the people that should have access to it do and those that shouldn't, don't. This truism applies to IT environments as much as, if not more so, to offices, buildings and army bases etc. The first step of any security solution is proper identification and authentication of the person ensuring that they are actually who they claim to be. Initial computer systems relied upon the simple username and password to authenticate the user to the system. This identification and authentication technology has proven to be very weak as it is simply "something you know" but there is little or nothing to stop multiple people knowing the same thing. Sometimes this information is shared deliberately, other times it is shared accidentally or maliciously. In any event, when a system requires a password for authentication, the user is replaying the full unabridged "secret" information which could be and often is intercepted. Effectively, a single attack will reveal the "secret" information permanently.

The following are examples of attacks levied against single Factor Authentication solutions:

- Shoulder surfing
- Keylogging
- Screen scraping
- Replay
- Reverse engineering
- Brute force attacks
- Crenedial spraying
- Man in the middle

It is for the above-mentioned reasons, additional layers or factors have been introduced to mitigate the inherent security limitations of the ubiquitous username and password combination. As the years have progressed, the number of multi-factor solutions have increased exponentially with a whole host of companies providing various forms of authentication technologies ranging from physical key-fob tokens and SMS text messages to fingerprint and retinal scans. These diverse technologies are broken down into sub-sections called factors with each factor having its own specific functionality. The 1st factor as (discussed above with passwords) is "something you know"; 2nd factors are typically "something you have", such as a mobile phone or key fob, "something you are" such as a fingerprint or retinal scan which is unique to every individual or "something you are doing".

This white-paper has been created to discuss the merits and susceptibility of attacks levied against Deviceless OTP (aka 1.5 Factor Authentication) technologies available on the market. Deviceless OTP provides the flexibility of single-factor authentication while thwarting many of the weaknesses of username + password instead of having to depend on multi-factor authentication.

Deviceless OTP Authentication

Deviceless OTP Authentication is a technology class unique to a small group of companies which technically relies on a single factor for authentication, " something you know", however for the most part limits or mitigates the attacks that traditional passwords are susceptible to. Deviceless OTP technology requires no additional physical devices, software tokens or biometric scanners which significantly keeps costs down and lowers user friction.

Where Deviceless OTP Authentication technologies differ from the traditional 1 FA technologies is in the fact that the "secret" information is never replayed in its entirety and the same information is not entered during each login. In essence, when prompted, a user will use the "something they know" in combination with another element provided to them at login to determine a One Time Passcode required for that authentication session. If either part of the combination is incorrect then authentication will fail. The power of Deviceless OTP Authentication is that deployment is both cost-effective and rapid as no additional devices are required and the challenge prompts can be displayed directly on the login page.

In essence, Deviceless OTP produces a One Time Code similar to traditional multi-factor solutions, but with the portability of a password. However, to satisfy high-security requirements, Multi-Factor Authentication is still recommended.

Deviceless OTP Authentication Solutions and Characteristics

The following three solutions provide Deviceless OTP authentication where the authentication prompts/challenges are displayed on the same login page used for authenticating a user to a system. In all cases, no additional hardware devices or scanners are required. In this section, we will evaluate the technologies, describing how they operate and assess their susceptibility to standard attacks.

Swivel Secure – TURing Image

Authenticating using Swivel Secure's PINsafe, a TURing image displays the user's security string. The user then combines this security string with their PIN to derive a one-time code. They then use this one-time code to authenticate themselves. The user needs both the security string and their PIN to authenticate, yet the PIN is never entered as part of the authentication process. The one-time code extraction protocol is simple to use, the PIN determines which characters are to be used and in which order, for the one-time code.

As an example, using the TURing image above, if the user's PIN is 1, 3, 5, 7 then the one-time-code will be 8 4 7 9.

Susceptibility to Attack

Unfortunately, the issue with a TURing technology is an attacker will only require a single successful login to decipher the user's PIN as the numbers displayed in the TURing image are unique. Using the example above, 8 is only found in position 1, 4 is only on position 3, 7 in 5 and 9 at position 7. The simplicity of the PIN (usually 4 digits) coupled to the displayed TURing image means that a single shoulder-surf attack is often enough to compromise the system. This solution turns out to be less secure than a complex password.

Additional Limitations

PINsafe does have a 2-factor configuration where the equivalent of the TURing image is emailed or sent via an SMS Text message to the user. As with the TURing image, the user uses a combination of the PIN and character string to determine the One Time code. However, the TURing image is displayed in a CAPTCHA format to try and obfuscate the numbers against Optical Character Recognition attacks, whereas the 2-factor deployment doesn't use this feature. As such, the user experience differs between 1 and 2-factor deployments.

The CAPTCHA style of the TURing image also causes other issues for users as the symbols are often difficult to read which results in multiple failed logins and frustrated users.

Gemalto (pka SafeNet, CRYPTOCard & GrIDsure)

GrIDsure presents the end-user with a grid of cells containing random characters from which the end-user selects their 'personal identification pattern' (PIP). Each time the end-user needs to authenticate a grid will be displayed containing a random set of characters. The end-user then just needs to remember their PIP and provide the specific characters within those cells that make up their One Time Code to securely authenticate to the protected resource.

3	0	9	7	4
0	4	6	9	6
7	2	0	8	2
1	5	5	5	8
3	2	8	1	1

The size of GrIDsure grid can be increased (e.g. 6x6 or 7x7), however, its default size is a 5x5 grid consisting of 25 cells with a user's pattern being configurable from a minimum 3 characters. Naturally, the longer the minimum lengths, the harder it is to compromise the pattern.

Susceptibility to Attack

To compromise a GrIDsure logon, an attacker will most likely only be required to capture a maximum of 3 valid logons (in most cases 2 logons will suffice) if the length of the pattern is 6 digits. If the user's pattern is 3 or 4 characters then a single logon most likely will be sufficient. The reason for this is that GrIDsure utilises 10 unique numbers/characters/symbols when populating a challenge grid. So in a 5x5 grid comprising of 25 cells, there will be 5 characters repeated 3 times and 5 of the characters repeated only twice. Using the grid above as an example, characters 0, 1, 2, 5 & 6 appear 3 times and 3, 4, 7, 8 & 9 twice. By overlaying 2 grids with their valid login information, an attacker will very likely be able to determine the cells in the grid the user has selected for the pattern as the character re-occurrence is small.

Other Issues

GrIDsure does not have a 2-factor option so users can only be provisioned for Deviceless OTP Authentication. GrIDsure does include the functionality of restricting trivial patterns to disallow the selection of diagonal lines, straight lines and four corner selections however the complexity does not enforce gaps between cells and limiting of using the same cell for almost the entire pattern so trivial patterns can always be selected.

Authlogics PINgrid

A user is presented with a unique challenge grid (Similar to GrIDsure), however, the digits within the grid are repeated equally throughout. This repetition ensures that any attempt to shoulder-surf or capture of the user's entered OTP will be useless as there would be no way of reversing this back to the original pattern.

Susceptibility to Attack

A single vector attack, e.g. a screen-scrape on its own or a key log, will not reveal the secret pattern. With PINgrid authentication, the attacker would need to have a multi-vector attack on multiple occasions. This means that in conjunction with a screen scrape of the area where the challenge grid is displayed, the attacker must also, at the same time key-log the user's valid OTP. This process would need to be repeated 4 or 5 times on average (max 6 times) to be able to reverse engineer the pattern when the minimum of a 6 digit pattern is required. The longer the pattern, the more captured logins would be required to launch an attack. In all cases, the screen-scrape and key-log operations will need to be synchronised, marrying up what is required for a valid login which can be a fairly complicated process and requires moderate to high-level hacker skills.

Additional Considerations

PINgrid includes pattern complexity enforcement which ensures that patterns cannot be comprised of a single cell repeated an excessive number of times (controls can limit a single cell to be used 2 or 3 times maximum), straight lines whether they are vertical, horizontal or diagonal as well as ensuring that patterns use cells that do not touch previously used cells. This complexity increases security significantly.

Unlike other technologies, the PINgrid user experience in a Deviceless OTP or Multi-Factor implementation does not vary as the challenge grids are identical in all scenarios; the only difference is where the grid is displayed. As such, usage is consistent across factors.

PINgrid utilises a combination of FIPS-compliant and standards-based algorithms and patent approved methodologies to generate the numbers in the grid complying industry best practices.

Summary

The three technologies described in this document attempt to provide a mid-way solution between passwords and traditional Multi-Factor Authentication. As this type of authentication is based only on a single factor, i.e. "*something you know*", for it to be more secure than a password it must provide an effective way of protecting the secret.

	PINgrid	GrIDsure	Swivel Secure
Successful logon captures required to reverse engineer secret	6 attempts	2 attempts	1 attempt
Number of available patterns	2.1 billion	390 thousand	10 thousand
Character repetition in challenge	6 times	2.5 times (average)	0 times
Possibility of guessing an OTP	1 : 46,656	1 : 10,000	1 : 10,000

Data based on each product using default settings.

Each solution provides slightly different methods and benefits, however, PINgrid is statistically and mathematically proven to provide the highest level of protection again reverse-engineering the "*something you know*" information and thwarting theoretical attacks.

Conclusion

PINgrid utilises proven techniques to generate the numbers in the grid and, for flexibility, provides numerous methods of deployment. Based on use case scenarios, convenience and cost, adopters have a variant of choices of how to implement PINgrid.

Multi-Factor Authentication is more secure and addresses the few theoretical vulnerabilities associated with Deviceless OTP Authentication. Once a PINgrid Deviceless OTP Authentication solution is in place it can be changed to, or co-exist with, a Multi-Factor PINgrid solution with no back-end application changes thus preserving the initial Deviceless OTP investment.