novoxs

White Paper

See the related patent: # WO2019236530A1

Table of Contents

Introduction

All over the world, people use some kind of authentication to prove their identity.

The importance of protecting your identity is undeniable; otherwise other people could use it at your expense.

The biggest risk for your security is the threat of stolen information and identity theft.

Why is it important to have a robust security on your system?

As a company, with a breached security, unauthorized people have the power to steal money or confidential information from your company, or to mess up your configuration to distract your business.

As an individual, others can destroy your reputation by exposing your privacy. In some cases, you can even loose close acquaintances if personal information or conversations leak out.

How can you protect your identity?

So far, all of our partners and customers have agreed with us, that the current authentication standards - like PIN numbers and passwords - are outdated and the new, more secure methods are inconvenient.

We built a convenient way to protect your business, your customers and your life.

What kind of verifications do we have on the market?

These are the main authentication factors:

“Something you know”: Information that only the authorized person knows. (like a password or a PIN number) This is something that you have to remember.

“Something you have”: A physical device or a mailbox / other kind of address that only the authorized person has access to. (like an employee card, email address or a hardware token device)

“Something you are”: Any kind of biometric authentication belongs to this category. (fingerprint, voice recognition, eye scanning, etc.)

As you will see, novoxs has it's own category. It's a combination of the first two. We call it "Something only you can do".

What is the problem with the current standards?

None of these 3 factors guarantee 100% accuracy, because the authentication secret can be intercepted. The possessed device can be stolen and/or duplicated (like biometrics) and there is a chance for the external device to be compromised, etc. This is why security companies emphasize combining these factors together (multi-factor authentication).

Are passwords inconvenient?

According to a Centrify survey that was completed by IT security professionals:

- They were asked if they were suffering from 'password rage,' and admitted that they are sometimes driven to crying, screaming and swearing.

- In their poll, a quarter of the workers admitted to forgetting their password at least once a day. While 5% said they can never remember their password.

- One in six of the people confessed to screaming or shouting in the office when they forget their password. Some even resort to running off and slamming the door; even banging their head on the desk.

- Passwords are no longer fit for purpose we have too many of them, we tend to use the same ones time and time again, and we don't change them often enough. Even when we do make them hard to remember there is someone out there ready to crack them.

https://blog.centrify.com/password-rage-centrify-survey/

Are passwords unsecure?

Here is just one example of leaked passwords:

According to The New York Times:

- Yahoo announced in September, 2016 that the account information of at least 500 million users was stolen by hackers two years ago, in the biggest known intrusion of one company's computer network. In a statement, Yahoo said user information — including names, email addresses, telephone numbers, birth dates, encrypted passwords and, in some cases, security questions — was compromised in 2014 by what it believed was a "state-sponsored actor."

https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html

Is 2FA (Two Factor Authentication) good enough?

According to Fortune magazine (2017):

- Only 28% of people are using 2FA at all
- More than half of the respondents (56%) **had not even heard of 2FA** in the first place

http://fortune.com/2017/11/07/cybersecurity-2fa-two-factor-authentication/

According to The Verge (2018):

- A Google engineer revealed that more than 90 percent of active Gmail accounts don't use two-factor authentication (2FA).
- Though 2FA provides meaningful protection and most sites offer 2FA, it does have limits, and methods like SMS authentication are easier to hack than something like a hardware token.

https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google

According to The Verge (2017):

- Nearly all major web services now provide some form of two-factor authentication, but they vary greatly in how well they protect accounts. Dedicated hackers have little problem bypassing through the weaker implementations, either by intercepting codes or exploiting account-recovery systems. We talk about two-factor like aspirin — a uniform, all-purpose fix that's straightforward to apply — but the reality is far more complex. The general framework still offers meaningful protection, but it's time to be honest about its limits. In 2017, just having two-factor is no longer enough.

https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

Also, two factor authentication slows down the login process, which can cause serious problems when we need to log in quickly. There is another drawback of using 2FA. When you don't have your phone with you (or the battery dies), it's very irritating that you cannot log in.

What about hardware tokens?

Using physical tokens are very expensive, since they are easy to steal, you can loose them and you have to replace them after they die. In a SaaS scenario, you don't have the ability to give every customer a physical token, especially in case of a free service.

According to LoginTC:

- They're not scalable. To secure access to important digital assets (e.g. VPN), large enterprises, such as a banks or government departments and agencies need to deploy 2FA to hundreds of thousands of employees and/or customers. With hard tokens, that means buying, supplying and managing a physical token for each individual.

- They're easy to lose. Not only are hard tokens uncomfortable in your pocket and bulky on your keychain, they are also easy to forget at home, misplace, drop down an elevator shaft, drop into a puddle.

- They're expensive. The prevalence of lost tokens has forced most administrators to keep extra token inventory in stock to serve as replacement tokens. However, this problem goes beyond being an administrative headache because hard tokens are extremely pricey. A 10-pack of RSA tokens on TokenGuard.com goes for over $3,000 which equates to $300 a pop. Then there's the software license and eventual expiry to consider, at which point you would need to renew. Now apply this to the hundreds of thousands of users we discussed earlier.

- They're limiting. There is only so much you can do with a hard token, as there's not room for much else besides an OTP-type (one time password) code to appear on its screen. This means that as multifactor technology progresses toward widespread incorporation of biometrics (like fingerprint and iris scanning), wearables and contextual information (such as geolocation) hard tokens will fall short.

https://www.logintc.com/blog/2015-03-16-problem-with-hard-tokens.html

What is the problem with biometric authentication?

According to Tata Cyber Security Community:

- Privacy is one of the biggest concerns of the biometric solution. If the servers storing biometric information is hacked, it could have extremely serious consequences for individuals. An example of the breach is the U.S. Office of Personnel Management (OPM), which was hacked resulting in the theft of 5.6 million fingerprints. The biometrics were stolen along with a lot of data of each person.

- Another major drawback is the high cost which is involved in getting the systems up and running and also storing and maintaining the biometrics.

- Apart from these, there are various other challenges like one cannot change the retina or facial scan (which is very specific to the type of solution in place) in case one thinks that his security has been compromised at any point. Also, it is not in favor for a physically challenged person.

https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/01/05/15-important-pros-and-cons-biometric-authentication

How is novoxs different from the other procedures?

If you want to have proof of somebody's identity, you would like it to be dynamically changing, otherwise the proof could be replicated and reused by unauthorized parties. How would you feel if somebody would show up at your door with your friend's photo printed on his face? In person, we could easily detect the trick, because our brain can check things dynamically. We can draw conclusions from the interactions of others. Novoxs is an interaction based method.

Although, there is an illusion of "dynamically changing access codes" when you use a number generating token device or a text-message, it is easy to admit that the device you use or the place where you receive the secret code is still static, so it can be stolen, faked, etc. These procedures depend on a static factor that is independent of you, including the fingerprint, because if it's copied, you can't control it anymore.

Using novoxs, there is only one static part of the authentication: a graphical pattern that you never have to enter anywhere. The method that novoxs uses is the first real dynamic access code generator.

Novoxs is a "what you know" type of verification, but the secret key that you "know" never leaves your head. It is interaction based, it is "what you can do" that matters. In this case it means you can solve a "challenge".

What is the method?

Novoxs requires you to register a 2 dimensional pattern on a 3*3 to 10*10 grid (user chooses the grid size). At the authentication, we fill in this grid with random numbers that change at each login. This way, a random pin code can be retrieved from the presented numbers by using the pre-registered pattern every time you log in. Since you don't share your pattern with anybody, nobody can reverse the secret from the access code.

What makes novoxs secure?

Our team has worked hard to meet a different number of security requirements. There are dozens of security enhancements in our algorithms that protect the user from their pattern being reverse-engineered.

You can read more about the security features below. For a detailed description of the security features, read out patent here: # WO2019236530A1.

How can you make your novoxs configuration more secure?

If you like, you can choose multiple cells from the grid and perform some mathematical operation on them before you put your number into the password field. In addition, you can change the actual value of the presented numbers, so to confuse your audience.

Novoxs also has a “dynamic mode” option, which makes your procedure even more dynamic by refreshing the random grid of numbers at every keystroke, when you input your login code. Use this feature to allow more security on generally weaker configurations too.

Optionally, you can have the ability to require the user to authenticate multiple times in case of unsuccessful login trial. (This feature is not yet available).

How secure is the novoxs method?

The security of this method is measured on 3 levels.

1 – Brute forceability of the login code: The strength is the same of a PIN code.

2 - Brute forceability of the pattern: The strength depends on the configuration. See below.

Example 1:

Grid size: 4*4 (16 cells)

No complications

Access code length: 4

You have 16*16*16*16 different patterns.

Example 2:

Grid size: 4*4 (16 cells)

3 cell operations for each digit.

Access code length: 4

You have (16*16*16)*(16*16*16)*(16*16*16)*(16*16*16) different patterns.

Example 3:

Grid size: 6*6 (36 cells)

No complications.

Access code length: 4

You have 36*36*36*36 different patterns.

3 – Reverse engineering the pattern form dozens of captured grids and login codes: It depends on the complexity of the pattern setup.

Example 1:

Grid size: 4*4 (16 cells)

No complications

No dynamic mode

Access code length: 4

Each digit appears approximately 2 times in the grid.

So, you have to try: 2*2*2*2 combinations with one captured keypair.

Example 2:

Grid size 6*6 (36 cells)

Add 2 cells at each digit (4*2 cells)

No dynamic mode

Access code length: 4

There are approximately 15 combinations to get each digit as the sum.

So, you have to try: 15*15*15*15 combinations with one captured keypair.

Example 3:

Grid size 4*4 (16 cells)

Some numbers' value has been changed

Access code length: 4

Because of the changed values, you have to capture approximately 5 authentications to recover the pattern.

So, you have to try approximately 4*4*4*4 combinations for all of the captured keypairs.

In the examples above, we knew the specific configuration of the grids, but in real life, we don't know if the user uses mathematical operations or changed the numbers' values.

Without this information, the number of the intercepted grid - solution pairs that are required for the attack can vary from 50 to 120.

An additional brute forcing point could be the datafile, where we store the generated keypairs in an encrypted format. We made sure to use hashing algorithms that slow down the brute forcing process. We always recommend to use hardware encryption on the disk, where novoxs is stored, so the datafile can only be accessed after unlocking the computer.

Example 1 - Using novoxs for logging in to a Windows laptop

John has a Windows laptop. He used to log in to his laptop with his password, before he installed novoxs.

Back than, when he used the password, a curious colleague saw him typing in the password. After a while the colleague used that password to unlock his laptop and read his emails.

When John figured it out, he installed novoxs. Now, when he logs in to his laptop, the Windows requires new access code each time so other people cannot use the captured passwords anymore.

Example 2 - Using novoxs to protect POS software settings

Eric has a retail store. His employees always pocket some cash when he doesn't look. It is only possible, because the employees saw his pin code when he logged in to the POS system. With that password they can remove invoices from the system, so Eric cannot see that the money is missing.

Since Eric changed his password and installed novoxs, the employees could not catch his password anymore to manipulate the system.

When he wants to log in to the POS software, he does not enter his password, he uses novoxs. (This feature is not yet available).

Example 3 - Using novoxs on a debit card

The banking industry has a lot of issues with PIN cameras that attackers install to pry on customers when they enter the PIN.

Eastern Merchant Bank (fictional) decided to give the customers novoxs credit card, the customers are prompted to log in with a new access code every time when they use the ATM.

The customers can see their random grid on the card or on the ATM machine and they can log in with their new access code. This way, the attackers cannot reuse the intercepted pin codes. (This feature is not yet available).

Example 4 - Using novoxs in a company system

Katy works in an office, where the employees use desktop computers. The computers are connected to a company domain, which means they can log in with the same password (per user) to any domain connected computer and to the intranet portal.

Rob also works in the office and he wants to spy for confidential information that only Katy has access to. Rob decides to watch Katy's password and he manages to successfully copy Katy's password and use it to log on to the intranet where the company's confidential information is stored.

Once, Tom, the boss figured out this issue, he decided to upgrade the user directory and integrate it with novoxs. From now on, the employees are requested for new access code every time, so other employees cannot pry on each others password anymore.

Example 5 - Using novoxs on a web portal

Paynet (fictional) is an online payment company who wants to protect their customers from hackers. They want to secure their website with novoxs. Paynet decided to integrate our solution as a third-party login, like "Login with Google". When the users log in to their portal, they see an alert to upgrade the password to novoxs. When they proceed, they are redirected to the company's novoxs portal to create their access code.

In the future, when the users want to log in, they enter their username. The software detects, that the user has novoxs set up and redirects them to the novoxs portal. After the authentication, they are logged in to the website. This way, the customers can use different access code every time they log in.

Where other places can novoxs be useful?

Any place where passwords or pin codes are present, authentication takes place for a good reason. Novoxs is useful everywhere where authentication is used.

Summary

There are thousands of articles about the latest and greatest authentication technologies, but they all suffer from some problems and setbacks. One is unsecure, while the other one is too complicated.

Our procedure is a really convenient and affordable way to make a secure and efficient verification happen.

Contact information

If you have any questions, please don't hesitate to contact us on https://novoxs.com/. Our email address is info@alphadev.hu.