|  |  |
| --- | --- |
|  | |
| Awareness Campaign – Authentication | |
| **Diego Borghgraef** | Bachelor in Information management & Security  Specialization: Cybersecurity |
|  |
| Academic year: 2021-2022  Campus: De Vest |

1

# Foreword

To achieve my Bachelor’s degree in Information Management & Security with a specialization in Cyber Security at Thomas More Mechelen I attended my last year’s internship at EY between February till May 2022. The internship took place during the last semester of my Bachelor’s degree.

During the course of my internship, I had the opportunity to join the Cyber Security team at EY and explore all the fascinating techniques & best practices implemented in an Identity & Access Management business environment. I gained in-depth knowledge about the new authentication methodologies and performed a thorough analysis of user behavior.

Furthermore, I had the opportunity to explore more about Authentication interests by performing an Awareness Campaign on the different user profiles to see which techniques sparks interest to be potentially implemented in the future business environment.

# Summary

During my internship, I will explore and provide more inside information about the upcoming authentication technologies for each user profile by performing an awareness campaign around the different authentication factors. Because of the COVID-19 outbreak, people have been forced to reconsider things as they have been. Corporates have been compelled to review and adapt their requirements to the changing nature of our traditional workspace to prepare their business for the future of offices. More and more people are switching over to a flexible workspace where work-from-home will be the new way of working. For this reason, new security enforcement rules need to be in place to make sure employees can work in a safe environment without any disruption.

In a post-COVID-19 era, Identity & Access Management will therefore become more critical than ever, Businesses will try to cope with the challenges of COVID-19 by adopting new cloud technologies and finding ways to enforce their cloud security.

The problem with the implementation of remote workforce is that the primary source of cyber outbreaks will be more vulnerable than ever. Employees are to this day still the main reason for a disruption in organizations as they get targeted by threat actors in different ways with sole purpose of gathering as much data of a certain company. Therefore sensitising users with the right authentication methodologies is the first line of defence that should be applied in every corporate organization.

# Contents

[1 Foreword 5](#_Toc103946282)

[2 Summary 6](#_Toc103946283)

[1 Contents 7](#_Toc103946284)

[2 Research Question 8](#_Toc103946285)

[3 Introduction to Identity & Access Management 9](#_Toc103946286)

[3.1 Components in Identity & Access Management 10](#_Toc103946287)

[3.2 Importance of Identity & Access Management 11](#_Toc103946288)

[4 Authentication 12](#_Toc103946289)

[4.1 Something you know 12](#_Toc103946290)

[4.1.1 Password Authentication 13](#_Toc103946291)

[4.1.2 Passphrases 16](#_Toc103946292)

[4.1.3 Password Managers 17](#_Toc103946293)

[4.2 Something you have 18](#_Toc103946294)

[4.2.1 Multi-Factor Authentication 18](#_Toc103946295)

[4.2.2 Common types of 2FA 19](#_Toc103946296)

[4.2.3 Token-Based Authentication 19](#_Toc103946297)

[4.3 Something you are 21](#_Toc103946298)

[4.3.1 Biometric Authentication 21](#_Toc103946299)

[5 Interactive web-based awareness campaign 25](#_Toc103946300)

[5.1 Implementation 25](#_Toc103946301)

[5.2 Introduction 25](#_Toc103946302)

[5.3 Learn 25](#_Toc103946303)

[5.3.1 Password Breach – Interactive tool 26](#_Toc103946304)

[5.3.2 Passphrase Generator – Interactive Tool 26](#_Toc103946305)

[5.3.3 2FA Websites – Interactive Tool 27](#_Toc103946306)

[5.3.4 Preferred authentication – Interactive Tool 27](#_Toc103946307)

[5.4 Survey 28](#_Toc103946308)

[5.5 Results 28](#_Toc103946309)

[6 Conclusion 29](#_Toc103946310)

[7 Bibliography 30](#_Toc103946311)

# Research Question

My research question for my internship is as follows:

**“ Awareness Campaign – Which key factors define the authentication methodology of the future?**

Due to the rapid growth of hybrid working, authentication has become significantly more important for each user profile. Applying the right security enforcement tools is becoming a real challenge that needs to be addressed. Therefore an analysis will be done, where users will get a foretaste of what authentication methodologies are available by performing an interactive learning course.

Afterwards, users will have the opportunity to fill in a survey about the authentication methodologies that were discussed during the interactive learning course. The survey will define if user’s behavior goes in line with the new upcoming technologies, to define which techniques bring the best outcome when Security, Ease of use & Cost is on the line.

# Introduction to Identity & Access Management

Identity & Access Management (IAM) is a set of policies, procedures and technology that enables businesses to manage digital identities and allows or restricts certain users to access sensitive corporate information at a certain time. The main goal of IAM systems is to provide a single digital identity for each user in a simplified manner. Once a digital identity has been created, it must be maintained, adjusted, and monitored throughout its whole lifecycle.

Identity & Access Management is built around 2 fundamental ideas:

**Authorization**:

Authorization occurs in IAM when the allocation or delegation of permissions is given to a certain individual or client. These permissions will define what the user can access in a certain organization and which information is restricted for users with higher privileges.

Diagram

Description automatically generated

Figure 1 - https://forum.huawei.com/enterprise/en/the-overview-of-identity-and-access-management-iam-part-02/thread/818685-867

**Authentication**:

As the name implies, Authentication is the phase where entities are verified against a database to see if the person, piece of software/hardware is who they claim to be. This will be done by checking credentials against the database. IAM cloud solutions provide a more robust and versatile authentication system than most traditional alphanumeric password solutions.

Diagram

Description automatically generated

## Components in Identity & Access Management

When we think about Identity & Access Management we can hear 2 important terms. Both terms are related to each other but have a significant other utility and cannot be interchanged between each other.

**Identity** occurs when we need to authenticate an employee, contractor, intern or client to any of the business services of a corporate organization. It gives the possibility for system administrators to identify all users in a simple manner. Furthermore, if Identity was implemented with a cloud solution, users may be able to log in from a variety of devices, like smartphones, laptops & home computers. Under identity we can define the following 3 components:

* **Database Management:**
  + The first step when deploying an IAM system is tracking the user behavior of each employee by defining a unique identity for all users. Their UID and position will then be stored in a database.
* **Provisioning / Deprovisioning:**
  + The next step is the process of creating, updating and deleting users from different applications and systems. Only the necessary applications/tools can be used by a certain user.
* **Authentication**
  + The most important part of IAM is that we will check if the user is the one who he claims to be. Various methods can be implemented. Authentication methods like passwords, tokens, biometrics or one-time password can be used depending on the security levels of the company.

**Access** occurs after an Identity has been established. Afterwards, it is critical to define the access rights of users. Depending on the role inside of the corporate organization, more or less access rights will be assigned to them. Unauthorized access will be reduced to the strict minimum of what an employee, intern… needs to access to fulfill their work. Under access we can define the last 3 components of IAM:

* **Authorization**
  + Once the user has received access to the system and tools of the company it will need authorization to access specific services, drives or folders.
* **Permissions**
  + Once the access rights are given, permissions need to be implemented for each user. Depending on the employee’s roles inside the company **edit, comment, view or share** permissions will be given.
* **Reporting**
  + The final component is essential in an IAM environment. User login history, permission rights and user activities are logged for the system administrator. Thus given the first signal in case unusual behavior occurred on the company’s intranet.

## Importance of Identity & Access Management

In the last few years, the importance of Identity & access management has been growing at a rapid pace. Many businesses have been forced to reinvent themselves online as a result of the ongoing worldwide pandemic. Businesses are changing their way of working by forcing remote work on their employees, therefore a new focus on cybersecurity must be implemented to reinforce their existing infrastructure to meet the urgent risks that the pandemic has caused.

Because of the large-scale work-from-home transition for most employees, cybercriminals have more opportunities to infiltrate and compromise essential systems from em

ployees. Because of the fast-paced action in which the pandemic occurred a lot of businesses were not ready to transition to a new remote workforce which left them vulnerable to a varied amount of cyberthreats.

When we look at the charts below we can see a clear increase in cybercrime since the beginning of the global pandemic. Cybercrime has almost doubled since the start of the pandemic in April. Furthermore, we can see that most cybercrimes occurred during the following months of the global pandemic. Those were the months were most corporate businesses were not prepared to switch over to remote work, thus making them more vulnerable to different cybercrimes.

Chart, bar chart

Description automatically generated

Figure 2 - vpngids.nl

Seeing those results, a focus on cybersecurity and more specifically authentication are more important than ever. By applying a good Identity & Access Management model with the right Awareness Campaign for Authentication, businesses can prevent a large amount of upcoming cybercrimes as the first line of defence is prepared against it.

# Authentication

‘Identification’, ‘Authentication’ & ‘Authorisation’ form the 3 fundamental principles around a secure Identity & Access management environment. They provide a process for identifying a user by authenticating them, using different types of authentication techniques. Depending on the identity of the user, they will be authorized to access certain information on different platforms.

Authentication can be categorized into 3 different groups, depending on how they are implemented and used:

* ***Something you know (Knowledge-Based Authentication):***
  + The most common form of credentials includes passwords, PINs, security questions and any other information which information you know. Every authentication method is based on knowledge.
* ***Something you possess (Token Based Authentication):***
  + When implementing MFA, you can introduce new ways of authentication yourself like objects, apps and devices that you possess to allow yourself to authenticate. Authentication occurs using authenticator apps, SMS codes, smart cards or security keys.
* ***Something you are (Biometric Authentication):***
  + Lastly, new ways of authentication came about with the introduction of Biometrics. Those are elements that are unique to everyone else. Common forms of authentication are Fingerprint, Facematch, Eye scanners and Voice recognition….



## Something you know

The idea behind knowledge-based authentication is that you know a secret, also called a password. The only aspect that differentiates you from other users is that you know a secret different from someone else. An authentication system will simply need to check to see if the person claiming to know the secret.

Unfortunately, the use of secrets is not the perfect solution. When a secret is entered on a keyboard it is vulnerable to shoulder surfing. Furthermore, authentication mechanisms use challenge-response protocols to avoid sending secret keys in plain text over the wire where it could be intercepted by a wiretapper, but humans can’t engage in a challenge/response protocol on their own, which makes them vulnerable to non-encrypted communications.

In addition, people tend to choose passwords that are easy to remember, which usually implies their password is easy to guess. In a business world, people are obliged to change their passwords every 3 months, making it harder and harder to remember their changed passwords. Users will then step down their guard and eventually write down their password or succumb to non-secure passwords.

During the following chapters, we will dive into a more complex explanation of passwords and what better knowledge-based authentications are available for users to implement.

### Password Authentication

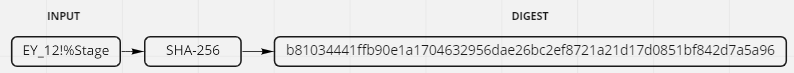
Passwords are the most commonly used type of knowledge-based authentication for most applications and websites. However, it has been known for decades that passwords are the most insecure form of user authentication. Before we dive further in the subject, we will define the baselines of password authentication.

Password authentication is the process in which users input a unique ID & key, which will be compared to previously stored credentials. In normal circumstances only the person who established and set the password will know it and be able to repeat it, thereby confirming their identity and granting access to restricted data and services.

In the early days of computers and mainframes, passwords were stored in a database as plain text. A gatekeeper application would ask you for your password when tried to sign in. It would take anything you wrote in and compare it to what it had saved in its database. If the two texts were identical it would grant you access to the service you were using. Unfortunately, it did not take long for threat actors to find ways to gain unauthorized access to those systems. Techniques like brute force attacks and dictionary attacks made it very simple to gain unauthorized access.

#### Password Hashing

A solution to this problem was the implementation of Password Hashing. Hashing refers to “Chopping something into small pieces” to make it look unrecognizable from its origin. This definition closely refers to what hashing represents in computing. In cryptography, a hash function can be seen as a mathematical algorithm that converts data of arbitrary size to a fixed-length bit string. This fixed-size string function output is known as a hash or the message digest.



An example of a hashing algorithm is the SHA-2 hash Algorithm. It is a set of multiple cryptographic hash functions created by the NSA (National Security Agency) that provide a secure way to store our passwords. Each of the SHA-2 hash functions has its own way of processing information and will provide always the same length of digest for each text input given by a user. Users that create a new account will provide their password and the web application will run it through a hashing algorithm that will store a digested version of their password making it not readable to the human eye. The story unfortunately does not end there. Even if hashes were a breakthrough in security it did not take long to find new ways to get through the systems. Threat actors started to reverse engineer the hashes, by hashing stolen databases of passwords in hashed passwords and then comparing them against each other. When a hacker found two similar hashes, he knows that a password was cracked and only needed to find the matching password in the original database with his newly made hashed password.

Hashcat is a well-known password cracker for hashed passwords. It provides a way to perform dictionary & brute force attacks by guessing passwords. Even if the database consists of hashed passwords. It will compare them in an automated way against a known database of hashed passwords.

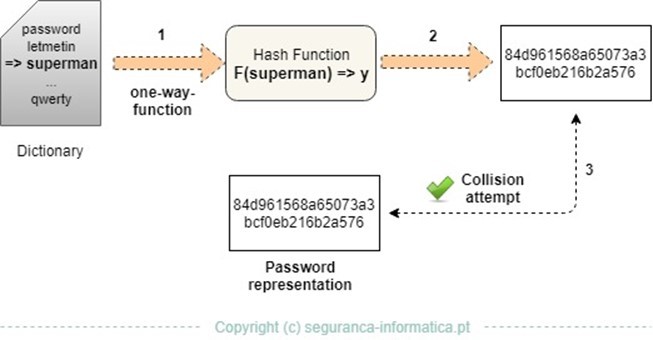


Figure 3 - https://seguranca-informatica.pt/hashcat-tutorial-for-beginners/#.YiXxunqZOUk

One advantage of using hashes is that it takes a few milliseconds to hash each password. So you need very fast computing power to generate all possible passwords. Another option for a threat actor is to have a very large dictionary of all the well-known passwords, generate hashes from all the words and then store those hashed passwords. All you need to do is look for a similar hash in the database, this method is called **Rainbow tables** and are very effective & fast. To protect against those kinds of attacks a new implementation was added.

#### Password Hash Salting

Another key period for authentication occurred in the 1970s, when password salting was invented. Instead of passing the password only inside a hashing algorithm a second security layer is added, called a Salt. A random piece of text is added with the password before it is hashed. This makes the hash unique and almost impossible to crack.

Diagram

Description automatically generated

The salt, or “little piece of text” is saved alongside the hash as plaintext in the database. But it is worth noting that the salt is different for each password, which makes it almost impossible for a threat actor to have dictionaries of passwords with random letters.

Although this technique protects the user from all possible dictionary/rainbow table attacks, it would also need a good server-side implementation by applying a “per-user” salt, which defines a different salt for every user. In case the same salt is used for a whole database it would take the threat actor one good salt guess to gather all database information. Therefore counting on server-side security is never a good idea and personal security best practices should be implemented.

#### Password security requirements

With all these cited concerns about passwords, users must have the right considerations when choosing a password. There are three dimensions, and they interact so that the strengthening in one dimension can be used to offset a weakness in another dimension:

*Length:*

* The first dimension for people to strengthen is Length. It is generally known that longer passwords are better. Considering making a password of at least 8 characters or more is becoming a necessary security requirement. In general passwords of 8 characters will have a “Time to guess” of about 29.190 minutes. In case we increase the number of characters those times can double or even triple the time to guess. [Password length best practices - Specops Software](https://specopssoft.com/blog/password-length-best-practices/?msclkid=b2a24348a8fd11ecae8dc0c1e1768350)

*Character set:*

* The second most important dimension is the character set. Having characters inside a password greatly increased security. As characters exist in a multitude of forms, implementing multiple characters gives any threat actor a lowered chance of accessing personal information.

*Randomness:*

* The biggest point of failure for users are regularities in passwords. When choosing a password that exists in your language a threat actor can leverage regularities in the language, meaning they search for known words in a certain language. Choosing words/phrases that do not make sense a recommended.

While we have mentioned a lot of solutions for traditional passwords, there is still a debate about passwords and how stronger they should be built. Do we need to add extra numbers, symbols or use uncommon words? Using all those best practices makes the user change their password very frequently, making it very complex. The problem is that users are not able to remember a very complex password that needs to be changed every trimester by company rules. They will start to write down their passwords on a sticky note or store their password inside their mobile phone, which makes their personal information more insecure and vulnerable to possible attacks. Therefore a solution to the problem needs to be found.

### Passphrases

A first alternative for insecure password are Passphrases. They both are made of words and mixed up with letters and characters, but the biggest difference is how they are built. A password is known to be one or two words, that are intended to confuse hackers who are attempting to access digital resources. While a passphrase is an entire phrase, sentence or statement that is made out of three to ten words.

Because of the changing nature of security in the last decade passwords are seemingly getting more complex to a point where human memorability not sufficient is to keep memorizing their password. Passphrases bridges this gap between human memorability and sufficient complexity to prevent any hackers.

First of all, they are a good alternative as they are easy to remember. Because of the logical aspect, users will remember them more frequently. Furthermore, passphrases create long complex passcode, while a password is constituted of 8-12 characters and often mixed with very complex characters (numbers & symbols). Passphrases on the other hand are usually 20 characters or more, combined with common words. The biggest difference is that hackers will need to do additional dictionary attacks for each existing word in a passphrase, which is almost impossible to hack.

#### **Passphrase example**

As an example, we will continue working on our initial password: **3Y/St@ge\*(12).** Using the security.org website we can see that it would take a computer 46 million years to crack our password without any extra information (dictionaries, threat actor involvement, etc..)

It is recommended to not compose any phrases that are common to the general public like “Bite the bullet”, and “Better late than never”… as those will be guessed easier. Usage of a general phrase that is only known in your environment is already a preferable alternative. Working further on my initial password it would look something like this:

**“3Y/St@ge\*(12)” => “EY-12-stage-weeks”**

As we can see the passcode is now composed of 17 letters and it provides a way easier passcode than before. Furthermore, when we pass the passphrase into the Security.org password checker we can see the time to guess has dramatically increased to 93 trillion years. Additionally when can make the passphrase even more complex by adding extra interchangeable characters like A, E & I into @, 3 & 1 which is still memorable and very complex. Because of the usage of passphrases, we could also extend the “time to change” of passwords to 6 months because of the complexity.

|  |  |
| --- | --- |
| Password/Passphrase | Time to crack |
| 3Y/St@ge\*(12) | 46.000.000 years |
| 3Y-12-st@g3-w33ks | 96,000,000,000,000 years |

### Password Managers

A second alternative solution of passwords started to occur in the late 1980s when people were confronted with the usage of multiple passwords/passphrases for different applications. As the internet expanded and security became a primary role in our lives users needed to invent a handful of different passwords for each of the applications. A study in 2017 reported that on average, people had to remember 191 different passwords.

While technology promises to make our lives easier, there is still a stumbling block for most users when it comes to having another password for each application we sign up for. A 2019 Security Survey found that **52%** of respondents reused the same password for multiple accounts. This is a big security vulnerability as compromised passwords could be added to giant lists of stolen passwords, also called dumps. Cybercriminals could get access to those lists and start brute forcing applications with password dumps. Making the user not only vulnerable for one application but for all the applications where he used the same passwords.

Fortunately, we do not have to remember all those passwords. As password managers were invented to store all those passwords in a closed and secured vault. Password managers are software tools designed to store and manage internet credentials. The saved passwords are stored in encrypted databases and protected by one master password. This means that the user only has to remember one master password to enter and use all of the account usernames and passwords.

#### **Benefits of password managers**

* Memorization of Passwords:
  + Only 1 master password needs to be remembered to unlock your password vault. Some password managers also provide a cloud solution giving the option to access your vault from anywhere.
* Password Generator
  + In case you have reused multiple passwords on multiple applications the user can generate passwords in a very simple way. Long passwords with alphanumeric characters will be generated that are almost impossible to guess.
* Data Breaches
  + Because complex passwords can easily be generated inside a password manager, data breaches become less frequent.
* Auto-fill
  + Most password managers provide a way for users to fill in their passwords automatically on web applications. Users only need to provide their master password once to get the auto-fill possibility.
* Extra Security Measures:
  + Passwords managers also provide extra security features such as multifactor authentication: Google Authenticator, Microsoft Authenticator, Yubico, Salesforce authenticator and many more

## Something you have

Another factor in authentication that is not based on the principle of something you have is *physical authentication*. Various token/card technologies support this new form were, you will need to have a physical element to be able to authenticate. Often physical authentication is combined with a 2-factor solution, which involves 2 independent means of authentication to access an online identity. This implies that a user not only has to possess a device but also know any kind of knowledge-based authentication (PIN, Password, Passphrase…)

### Multi-Factor Authentication

The problem with previously cited authentications (Something you know) is that each one of them has still one point of failure, meaning that a threat actor only needs 1 crucial piece of information to access their online identity. Therefore, solutions have emerged with the implementation of Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA). They require you to present two or more forms of credentials when logging in.

As we have mentioned above, credentials can generally be broken into three categories:

* Something you know
* Something you possess
* Something you are

This means that a potential compromise of just one of these factors won’t make it possible for threat actors to unlock your account. Even if your password or your phone is lost, the chances of someone having the second-factor information are highly unlikely.

Therefore a multitude of reasons exists for why MFA should be a standard implementation when identifying an application. The most evident reason for implementing it is that it provides an added layer of security on top of your passwords/passphrases. Especially in corporate organizations, MFA is required to be used so implementing it for personal use is highly recommended. MFA also provides practicalities as creating hundreds of passwords is not a necessary implementation anymore. Furthermore, MFA also provides SSO (Single Sign-on) in many corporations giving the users the ease to connect to multiple applications without the need for a password.

The biggest obstacle when using MFA is that there is a multitude of applications that offer MFA solutions. Defining which one fits you the best is a laborious quest as a large number of features are prominent. In general term defining the right authentication tool, are done using 3 of the most predominant factors:

Logo

Description automatically generatedSecurity: Does the authentication mechanism provide enough necessary protection for the user to protect their online identity from possible data breaches?

Usability: Refers to the efficiency and user acceptance of an authentication system. Does it provide a good user experience without compromising to much security?

Cost: Does the price have enough impact on the Usability & Security to make the cost of a certain authentication mechanism valuable?

### Common types of 2FA

Several types of two-factor authentication are in use today. Some may provide a strong and more complex authentication form, while some provide ease of use for users. It all depends on the requirements/needs of a specific user. In general, each MFA option provides better protection than passwords alone.

Examples of MFA authentication technologies that are based on something you possess:

### Token-Based Authentication

#### **Disconnected tokens**

Disconnected tokens also known as soft tokens have neither a physical nor logical connection to a client computer. They don’t require any form of user input device. Instead, it is built around screen displays that generate authentication data, which the user will then manually implement on online platforms by providing a security key. To this day disconnected tokens are the most widely used form of authentication and in combination with a passcode, it forms two-factor authentication for most online identifications. An example of soft tokens are contactless tokens:

Contactless tokens provide a way to connect to devices without the need for access codes. Instead, the tokens/devices will connect to wireless systems based on known connection credentials. Depending on the credentials access will be granted or denied.

Advantages of Disconnected Tokens

1. *Ease of use:* Once the software is installed, disconnected tokens can be used. It works in the same way as SMS OTPs (One Time Password) except the user doesn’t need to wait for an authentication SMS and can immediately use the generated One-Time-Password inside an OTP application.
2. *No extra Cost:* As the product is inside a phone you already possess you don’t need to pay extra to receive OTP passwords.
3. *Availability:* Disconnected tokens are widely available on a multitude of online platforms, whereas other types of Token-Based authentication mechanisms are not that sought-after yet.
4. *Pin code protection*: Allowing protection for OTP password generators from unauthorized access, meaning you need to enter a knowledge-based authentication form before you can access the OTP application.

Disadvantages of Disconnected Tokens

1. Cyber Attack, like most authentication methodologies a plausible attack can occur. In case a system allows a user to authenticate via an untrusted network, the chances exist a man-in-the-middle attack can occur. A threat actor will act as a middle man between the user and the legitimate system to intercept the 2-factor authentication, meaning the password and the generated OTP key.

In conclusion, Disconnected tokens provide a very secure and flexible security infrastructure at a fraction of the cost of other alternatives. Furthermore, it doesn’t require any extra effort from the client-side as it is just an add-on to mobile devices which is a standard object in this day and age.

#### **Connected Tokens**

One of the more advanced technologies in security tokens are the connected tokens (Hardware token), the way they work is that you slide your hardware security token into a USB reader. When you do so, your hardware token will push relevant authentication information to the system, making the user able to connect to their system after input of a second security layer, like PINs, Passwords, Passphrases. Common examples of connected tokens:

Smart Cards, a secure microchip that enables a user to authenticate using cryptographic keys, making it protected in both logical and physical ways, making it hard to be compromised. To authenticate use will need a smart card reader. Whenever a user swipes their card and enters their PIN, 2FA will be applied.

USB Tokens, work in a similar way to smart cards, offering the same functionality but in a convenient more portable format that can be carried on a key ring. Usually, USB tokens are used with Password Managers, Encryption or Two-factor authentication. The main advantage of Smart card is that it provides a way to authenticate with the need of readers for each end-user.

Advantages of Connected Tokens

1. *Confidentiality*: Connected tokens assure users that possession exchange has been done with the verifying mechanism, making it impossible for threat actors to access physical tokens.
2. *Time*: Because no OTP application is required, the process of authentication is accelerated. Plugging the hardware tokens and first authentication mechanism has been confirmed.
3. *Protection*: A common disadvantage, it that physical objects can get lost. Fortunately, the issuer can deactivate the token meanwhile soft tokens generator device will keep on working.

Disadvantages of Connected Tokens

1. *Lost*: Connected tokens can easily be forgotten at home or lost somewhere making it almost impossible to authenticate. You have to always carry it anywhere you go making it also more vulnerable to getting stolen.
2. *Expensive*: Because of the physical nature of the token, there is a price to pay for them. Fortunately, companies started manufacturing alternatives at lower costs, which will be explained later on.
3. *Scalability*: For companies to use connected tokens, a lot of technicalities are involved. Hardware tokens need to be bought, supplied and managed for each individual working, while soft tokens can be controlled from distance.

#### **New age of Hardware Tokens (FIDO2 Security Token)**

* New Passwordless Standard
* How does it work
* Difference with normal USB tokens
* Advantages/Disadvantages
* FIDO2 Implementation

## Something you are

### Biometric Authentication

Following the important considerations when choosing an authentication system we can find Biometrics. Biometrics differ from other authentication in different ways. As biometrics can be classified as physical or behavioral types. The behavioral type is more complex and includes learning movements of a certain user such as signature handwrites keyboard dynamics, but because of the unstable nature, it is recommended to work with more physical biometric types. The physical type includes biometrics based on stable body features, such as fingerprint, face, iris and hand. For the sake of my analysis, I will focus on stable biometrics signals as they provide more accessible results and are generally more accepted and used by users.

|  |  |
| --- | --- |
| **Physiological Identifiers** | **Behavioral Identifiers** |
| Fingerprint, handprint, footprint  Iris & Retina  Face, Ear | Voice  Signature  Gestures, Gait |

#### Fingerprint Scanners

The oldest biometrics identifier that has been used for authentication purposes is fingerprint scanners. They started to be utilized in the 19th century when the FBI funded the first development of a first computerized fingerprint scanner. It brings a unique way to authenticate as it is very difficult to alter and durable over the life as it doesn’t change over time. Therefore fingerprint recognition systems are still widely used to this day as the convenience, security and performance characteristics of fingerprints are optimal. The most common fingerprint sensor to this day are *Optical Scanners, Capacitive Scanners and Ultrasonic Scanners*.

##### ***Optical Scanners***

The oldest way of capturing and comparing fingerprints is with optical fingerprint scanners. This method is based on the capture of an optical picture, which is essentially a photograph of your finger. It will analyze the lightest and darkest portions of the image to discover distinctive patterns on the surface of the finger to find ridges or marks by using algorithms.

The problem with these sensors, like smartphone cameras, is that they have a limited resolution. The finer details the optical sensor can discern the higher the level of security. The biggest difference with optical scanners is that they capture images with far more contrast than a typical camera. This is done using a high number of diodes to capture extremely fine details. Another characteristic of optical scanners is that they incorporate an array of LEDs to light up the picture before a scan as the finger will cover most external natural light.

The main disadvantage of using optical scanners is that they are quite easy to deceive. The sensor captures a 2D image, which means prosthetics or high-quality pictures can be used to fool this particular design, which makes this type of scanner not a secure option anymore and industries have moved on to more secure hybrid solutions.

###### Optical fingerprint scannerHow do optical scanners work?

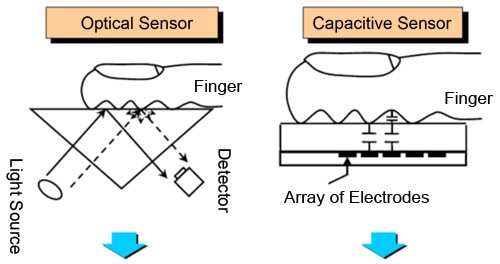
The way optical scanners work is by shining light over your fingerprint using bright LEDs and taking a digital picture. The light-sensitive microchip makes a digital picture by looking at the ridges and valleys of the fingerprint, turning them later into a binary data stream consisting of 1s and 0s that will create a user’s own personal code. This personal code will be encrypted and stored on any device and won’t be available for access.

##### ***Capacitive Scanners***

A first hybrid solution used today are capacitive scanners. This type of scanner can be found on most of the front and rear of smartphones, as well as in cutting-edge in-display models. Because of their added security mechanism capacitive scanners have gained in popularity and are standard implementation for most technological advancements.

Capacitive scanners acquire data using arrays of tiny capacitor circuits. They draw energy from a battery and are used to track the specifics of fingerprints by attaching them to conductive plates on the scanner’s surface. When the ridges of our finger are placed on the conductive plate our stored charge will somewhat alter each time. These changes will be tracked using an op-amp integrator circuit, which can subsequently be recorded to make the necessary changes.

###### How do capacitive scanners work?

After a digital image has been acquired, the digital data will be evaluated for distinguishing and unique fingerprint characteristics. Which makes this sensor very hard to bypass as no image is being made. The only viable attack would be hardware or software security concerns.

Using a large enough array of capacitors makes it possible for a single scanner to create highly detailed representations of ridges and valleys of a fingerprint using only electrical impulses. In conclusion, it provides a high level of security at a more expensive cost to manufacture.

##### Qualcomm 3D Sonic Sensor: ultrasonic security solution I Qualcomm***Ultrasonic Scanners***

Ultrasonic sensors are the most recent fingerprint scanning technology to join the smartphone market. The technology was introduced in 2016 with Qualcomm’s Sense ID technology. It consists of an ultrasonic transmitter and a receiver to actually capture the features of a fingerprint. When a finger is placed over the scanner, an ultrasonic pulse will be transmitted. Depending on the ridges, valleys and pores pulse signals will be bounded back or absorbed. The ultrasonic sensors are able to detect mechanical stress to calculate the intensity of the returning signals. Ultrasonic scanners also provide the option to make 3D reproductions of the scanned finger instead of the 2D images from optical scanners. The 3D nature of those scanners makes them even more secure than capacitive scanners. One major drawback of ultrasonic is that it is not as quick as other scanners. This is because a 3D image needs to be made, which takes a longer time to process than average 2D images. Also because ultrasonic devices relate to 3D, it gives smartphone’s a harder time detecting fingerprints in case we use thick screen protectors.

##### ***Security Concerns***

Unfortunately only using a fingerprint scanner as the main method of authentication is not advised as they have not been foolproof. DeepMasterPrints are like master keys that can match a large number of fingerprints. DeepMasterPrints have a high attack accuracy with the capacity to generate complete images. This was done by training a Generative Adversarial Network (GAN) on a large set of real fingerprint images. Using stochastic implementations are used to search for occurring input variables. Another security concern of fingerprints are small sensors. Because of the small size of those sensors, only partial information of the finger will be recorded and authenticated and because some features among fingerprints are more common than others it becomes highly possible for DeepMasterPrints to obtain true positive results using forged fingerprints. Following a study on DeepMasterPrints, it was found that the generated prints were able to spoof 77% of the subjects at a 1% false match rate

#### Facial Recognition

Since the late 1960s Facial Recognition was a new topic in the industry of biometric authentication. It performed basic analysis on the user’s personal expressions and facial landmarks such as eye centering, mouth placement and head shape. In this day and age, we can identify Facial recognition as a way of identifying and confirming a user’s identity using advanced facial patterns. A computer will analyze image data and look for a specific set of traits in a user’s face. It all begins with a collection of images and videos that will be performed on people’s faces. The computer will then be trained to read the geometry of a face to identify specific facial traits and will gather more than 68 different landmark points of each individual. Regions around the eyes, nose, mouth, chin, jaw and eyebrows will be captured. Furthermore, AI technology will be used to set up enough general rules to include enough user details, but also narrow down facial traits to exclude imaginary users. This is done using different techniques:

##### ***Gradients***

Computer algorithms will compare every image pixel’s brightness to the brightness of pixels around it, creating a map of changing “pixel intensity”. With the created brightness gradient map the AI will analyze & compare them with existing databases to find out if the image consists of real skin. In case the pixel brightness matches a real face when compared with the database then the AI will examine other facial features until every location has been tested.

A good example of this Facial Recognition technique is the Gradient app, which provides an almost identical lookalike picture of someone with the same skin tone. It uses the brightness gradient map of a user’s picture to find a matching celebrity.

##### ***Projection***

Another technique for facial recognition is projection. In this case, a 2D photo will be projected on a 3D model to define a third dimension that can often reveal forms of symmetry characteristics that are difficult to be found in a flat 2D image. Once an image has been 3 scanned, the system will encode the face & compress it with the most distinguishing characteristics and facial patterns to create a smaller and simplified file that will be used to cross-check encoded faces during authentication.

Considering the presented technical attributes used to process facial recognition, several limitations and imperfections can be encountered. Therefore it is important to define the right facial recognition technology that provides a high-security approach for users.

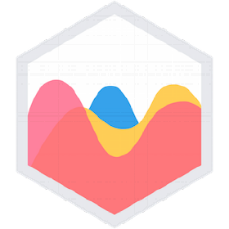
##### ***How accurate is facial recognition?***

Every authentication technology needs to have a very low false-positive ratio as it would break the purpose of security requirements, but fortunately, in recent years we have seen a drastic decrease in error rate when it comes to facial authentication. In 2014 the best facial recognition algorithms had an error rate of 4.1% which is still very significant when security is the primary factor. In 2018 the error rate decreased to 0.5% and in recent report of 2021, the error rates have even decreased to a stunning 0.08%. This proves that accuracy has been on the rise and that Facial recognition can become a primary authentication tool for bigger and more complex platforms if the right support & security measurements are in place.

# Interactive web-based awareness campaign

Now that all means of authentication have been defined with their benefits, disadvantages and method of implementation I established an interactive web-based awareness campaign for users to get to know more about each authentication methodology. The campaign consists of 4 different modules which their own specific purpose. Before we get started, a brief explanation of the implementation.

## Implementation



The awareness campaign was build using the free open-source front-end Javascript library, React JS as it provides single-page application functionalities which makes it very easy to reuse multiple components in a single page without rewriting the code every time. This avoid unnecessary page reloads making webpages fast, scalable and simple to use. In addition, React JS was one of the frameworks I didn’t try yet and as I am eager to learn I decided to take the challenge and make my awareness campaign on it.

Alongside React JS, I used Node.js for all the back-end functionalities as it is really easy to work with. Node.js provides packages for your web application, making it possible to reuse them in your project. An example for this is Firebase.

Firebase Realtime Database was used for my survey analysis to collect all the user responses. It provides a easy implementation with not too much technical knowledge required.

Finally Chart.JS was used for interpreting all the survey responses into different chart types. Furthermore it provides a way for the users to interactively work with each information.

## Introduction

During the first chapter the user will get a quick introduction about the purpose of the awareness campaign as it is meant for users to finally break the barrier of unfamiliarity between all authentication methodologies. Furthermore a brief explanation of each module has been set up.

## Learn

In the second chapter each authentication methodology will be explained, compared and analysed against each other to define their benefits and disadvantages. This was done using the 3 main components that were discussed previously which are: Security, Usability and Cost. Depending on the user preference different authentication factors matter the most, therefore I provided each authentication methodology with different levels in those factors, making the user able to choose which one suits them the best.

Furthermore, each methodology was provided with an interactive tool/game. The reason behind it, was to enable users to actively work with each authentication methodology making them more aware of the benefits and drawbacks.

### Password Breach – Interactive tool

A first tool was designed after the drawbacks of traditional passwords were explained, by providing the user with a tool to analyze their own password breaches. This was done using the API of haveibeenpwned.com. Using the Pwned Passwords API and searching information by range, we can find out if a user password has been previously exposed in a data breach.

A screenshot of a computer

Description automatically generated with medium confidence

<https://awarenesscampaign-authentication.netlify.app/PasswordsBreach>

### Passphrase Generator – Interactive Tool

While passphrase are kind of similar as password, it often gets confused between each other, therefore following the different ways in which they can be implemented, a passphrase generator tool was designed. It helps users transform a chosen phrase into a given passphrase.

Graphical user interface, text, application, website

Description automatically generated

<https://awarenesscampaign-authentication.netlify.app/CreatePassphrase>

### 2FA Websites – Interactive Tool

Given detailed information has been explained about the different 2FA approaches, it is crucial to keep the users interested in the subject. In the 2FA Website tool user are able look through more than 1400 different 2FA enabled websites. Each website domain defines the available 2FA method with their setup documentation. This removes the biggest usability stumbling block of 2FA. Most of time website do not promote the usage of alternative authentication solutions, while there are crucial.

Text

Description automatically generated

<https://awarenesscampaign-authentication.netlify.app/2FA-Directory>

### Preferred authentication – Interactive Tool

Whenever the user has terminated the whole awareness campaign they get a last interactive tool which combines all the previously cited authentication methods with their security, usability and cost level. As users have filled in a survey about their preferences they can finally decide which authentication methodology suits them the most.

Chart, radar chart

Description automatically generated

<https://awarenesscampaign-authentication.netlify.app/Conclusion>

As you can see, a user can choose between their interest point. In case a cost is their primary concern followed by usability and security, we would advise the user to use passphrases, as it provides an average security with a very high usability and at no extra cost.

## Survey

In the 3rd module a survey has been setup for users to see if interest has spiked in the authentication methodologies. Different topics such as password habits, password creation and password breaches are discussed. The purpose of the survey is to get a general overview of authentication practices with different user types. All information about the survey questions can be found back on the awareness campaign.

Graphical user interface, text, application

Description automatically generated

Survey : <https://awarenesscampaign-authentication.netlify.app/Survey>

## Results

In the results tab of the awareness campaign all information can been found back about the questions results. Using the Chart.JS tool user can look through all the results and define which inputs are important for them so that they can make their own opinion the answers. Furthermore I made a survey analysis where I take a in depth look at all the surveys and try to find correlation between them.

Chart, histogram

Description automatically generated

Responses : <https://awarenesscampaign-authentication.netlify.app/SurveyResponses>

Graphical user interface, text, application

Description automatically generated

Analysis : <https://awarenesscampaign-authentication.netlify.app/SurveyAnalysis>

# Conclusion

As a final conclusion of my awareness campaign we can see that campaigns who are crafted around concrete calls to actions, instead of believes or behaviour have a greater impact. Users had the opportunity to interactively work with different upcoming authentication methodologies that could replace their original way of authenticating. By doing so they were actively working with newer authentications.

Proving the effectiveness of the awareness campaign was done by performing a survey, where users that followed the awareness campaign had to answer different questions. From this we could conclude people where more driven to change their way of authenticating when action & interactivity was set in place. Furthermore we found out that more than 40% of users that performed the awareness campaign actually changed their methodology.

From the given results we can comfortably say that it was a successful campaign. All the expectations were fulfilled and concrete information was proven. Different approaches with awareness campaign have shown their results will be applied in the future.

# Bibliography

(2021, July 10). Retrieved from MFA Methods: https://www.rcdevs.com/why-is-the-software-token-the-best-mfa-method/

Batt, S. (2021, 11 24). *MUO*. Retrieved from https://www.makeuseof.com/tag/ways-hackers-bypass-fingerprint-scanner/

Engineer, R. C. (2021, February 25). *Hashing: A Better Way to store Passwords*. Retrieved from https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

HSU, D. S. (2016, 11 3). *Semiconductor*. Retrieved from https://semiengineering.com/fingerprint-senor-technology-and-security-requirements/

Keith, M. J. (2007, January). The usability of Passphrases for authentication: An empirical field study.

Malwarebytes. (n.d.). *Password Manager*. Retrieved from https://www.malwarebytes.com/what-is-password-manager#:~:text=A%20password%20manager%20is%20a,locked%20behind%20a%20master%20password.

Mott, N. (2021, 11 22). *PCMag*. Retrieved from https://uk.pcmag.com/security/137235/hacking-fingerprints-is-actually-pretty-easy-and-cheap

N., S. (2015, July). Authentication Systems: Principles and threats. pp. 3-19.

Nachreiner, C. (2018, 09 22). *Digital Authentication, The pas, the present and uncertain furture of the keys to online identity*. Retrieved from https://www.geekwire.com/2018/digital-authentication-human-beings-history-trust/

*Password Authentication & Passord Cracking*. (2015, June 25). Retrieved from https://www.wordfence.com/learn/how-passwords-work-and-cracking-passwords/

Pearson. (2011, June 6). *pearsonitcertification*. Retrieved from https://www.pearsonitcertification.com/articles/article.aspx?p=1718488

Stieb, A. (2020, July 22). *Shredcube*. Retrieved from https://shredcube.com/passphrases-vs-passwords/

Tavares, P. (2018, May 1). *Hashcat Tutorial for Beginners*. Retrieved from https://seguranca-informatica.pt/hashcat-tutorial-for-beginners/#.YihnsHqZOUl

*Techtarget*. (2021, July). Retrieved from https://www.techtarget.com/searchsecurity/definition/security-token

*The Best Password Managers for 2022*. (2022, February 19). Retrieved from https://www.pcmag.com/picks/the-best-password-managers