

Online authentication methods

Evaluate the strength of online authentication methods



UNIVERSITEIT VAN AMSTERDAM

Cornel de Jong
System and Network Engineering
Universiteit van Amsterdam
Spui 21
1012WX Amsterdam
Cornel.dejong@os3.nl

Supervisors:

Cees de Laat (UvA)

Gijs Hollestelle (Deloitte)
Tom Schuurmans (Deloitte)

Abstract

This project was initiated because Deloitte¹ was looking for a comparison method of online authentication methods, including the level of protection they offer and other relevant aspects. This has resulted in a "Comparison Matrix" which contains the characteristics and attack vectors of several existing and new online authentication methods.

Because of the short timeframe, it was not possible to actually test the authentication methods in practice. Through the layout of the Comparison Matrix it is easily to extend with more authentication methods and / or attack vectors. At the end of this report there is a scenario which will explain the use of the Comparison Matrix.

Basic knowledge of authentication methods and attacks is supposed.

Contents

INTRODUCTION	2
1. BACKGROUND	4
1.1 STRONG AUTHENTICATION	4
1.2 FACTORS	4
1.3 OUT-OF-BAND	5
1.4 CHALLENGE-RESPONSE	5
1.5 REVERSE AUTHENTICATION	5
1.6 ADDITIONAL MEASURES THAT CAN BE APPLIED ON ALL AUTH. METHODS	6
1.6.1 LOCKOUT (DENIAL OF SERVICE).....	6
1.6.2 VIRTUALATM.....	6
1.6.3 ENCRYPTION.....	6
2. AUTHENTICATION METHODS	7
2.1 AUTHENTICATION METHODS EXPLAINED	7
2.1.1 Password (only) based	7
2.1.2 Virtual keyboard	8
2.1.3 Partial password.....	9
2.1.4 SIM Toolkit.....	9
2.1.4.1 STK in 3G Networks	9
2.1.5 HandyID	10
2.1.6 Graphical.....	10
2.1.6.1 Passmark Sitekey (now RSA)	10
2.1.6.2 PassFaces	11
2.1.6.3 PASSpicture	11
2.1.7 RSA SecurID (SD520).....	12
2.1.8 EMV Smartcard	12
2.1.9 Public Key Infrastructure Smartcard.....	12
2.1.10 One Time Passwords	13
2.1.11 Bookmark authentication	14
2.2 COMPARISON MATRIX CHARACTERISTICS	15
2.2.1 Assumptions.....	15
3. ATTACK VECTORS	17
3.1 ATTACK VECTORS EXPLAINED	17
3.1.1 Shoulder surfing	17
3.1.2 Keylogger.....	17
3.1.3 Screen capturing.....	17
3.1.4 Brute force (exhaustive search).....	17
3.1.5 Guess attack	17
3.1.6 Dictionary attack.....	17
3.1.7 Hardware (observation) attack.....	18
3.1.8 Social engineering.....	18
3.1.9 Phishing attack	18
3.1.10 Man In The Middle attack	18
3.1.11 Man In The Browser attack	18
3.1.12 Network sniffing.....	18
3.1.13 Short access.....	19
3.2 COMPARISON MATRIX ATTACK VECTORS	19
3.2.1 Assumptions.....	19
4. USER ACCEPTANCE	21
5. SCENARIO	22
5.1 SCENARIO ONLINE BANKING	22
5.2 COMPARISON MATRIX CHARACTERISTICS	22
5.3 COMPARISON ATTACK VECTORS.....	23
TO CONCLUDE	24

APPENDIX 1, VASCO DIGIPASS COMPARISON.....	25
APPENDIX 2, READERS USED BY DUTCH BANKS.....	26
LITERATURE	28

Introduction

About Deloitte

Deloitte is the largest provider of audit, tax, consulting and financial advisory services in the Netherlands with around 6,000 staff, and offices throughout the country. It is an independent member firm of the international organization Deloitte Touche Tohmatsu. With offices in over 140 countries, they all work under the same name as autonomous member firms.

All 150,000 staff apply the same code of professional conduct in all service lines. They apply globally uniform client service standards. And apply shared values and ethical principles that unite the member firms.

Enterprise Risk Services

The Enterprise Risk Services (ERS, or Risk Consulting) practices at Deloitte member firms worldwide help clients manage risk and uncertainty, from the boardroom to the network. Through these member firms, Deloitte professionals provide a broad array of services that allow clients around the globe to better measure, manage and control risk to enhance the reliability of systems and processes throughout the enterprise.

Research question

Review new and existing online authentication methods in such a way that it is possible to create a "Comparison Matrix" which contains the authentication methods, characteristics and protection against attack vectors.

Research goal

The goal is to define a method to make a well-funded choice for an online authentication method in a customer specific situation, based on the Comparison Matrix.

Scope

The scope of this project is more wide, instead of going deep into one specific authentication method. This is because the Comparison Matrix needs to be reflection of the authentication methods that are available, otherwise the Comparison Matrix has no additional value.

There are three primary subjects to define:

1. Characteristics
2. Attack vectors
3. User acceptance

Characteristics

Create an overview of the characteristics of the different authentication methods. Use values (1 – 5) to point out the strengths and weaknesses.

Attack vectors

Create an overview of known attack vectors on online authentication methods used by hackers. Use values (1 – 5) to point out the resistance against the attack.

User acceptance

User acceptance is based on multiple factors and strongly dependant of the targeted users. Consider aspects like: additional hardware / software, complexity, login-time etc.

Biometric authentication methods are outside the scope of this project. Because there are a lot of different types: fingerprint, voice, iris etc. and other drawbacks like: costs, distribution, privacy, compromised systems.

1. Background

In an earlier research (Customer Authentication²) results were dramatic considering “strong” authentication methods. Several banks in the investigated countries (The Netherlands, America, Japan and several other European countries) only use username and password to authenticate customers! In America the Federal Financial Institutions Examination Council's (FFIEC) advises banks to use “strong” authentication methods.

The authentication of customers on (banking) websites should be adequate protected against existing attacks and new threats. For many years authentication existed only of a username & password. This is nowadays considered as a weak method, due to its vulnerability to many attacks. This requires stronger authentication.

1.1 Strong authentication

If basic authentication isn't good enough, you need strong authentication. The definition of strong authentication isn't common. Below are some examples of the definition found on the internet:

...”**Strong authentication**³ is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network.”...

...”**strong authentication**⁴

Strong authentication, also called two-factor authentication, is defined as two out of the following three proofs:

- something known, like a password,
- something possessed, like your ATM card, and
- something unique about your appearance or person, like a fingerprint.

Using strong authentication provides more protection for sensitive information than a simple username and password can provide. Strong authentication, especially when combined with other practices like mutual authentication and non-repudiation offers a strong assurance that financial transactions are conducted by two known and trusted parties.”...

...”An authentication factor is a piece of information and process used to authenticate or verify a person's identity for security purposes. Two-factor authentication is a system wherein two different methods are used to authenticate. Using two factors as opposed to one delivers a higher level of authentication assurance. Using more than one factor is sometimes called **strong authentication**⁵”...

1.2 Factors

Documentation on authentication often discusses different ways to authenticate a user and relates this to factors. This section shortly explains these terms.

There are multiple ways through which a user can identify himself:

- Something you know (for example a PIN or password)
- Something you have (for example a hardware token)
- Something you are (for example fingerprint, iris, voice)
- Somebody you know (like the “web of trust” from PGP)

The authentication itself can be divided into different factors, the number of the factor indicates how many of the above mentioned ways are used:

- One-factor (1FA)
- Two-factor (2FA)
- Three-factor (3FA)
- Fourth-factor (4FA)

The first three factors are considered well-known, but the Fourth-Factor⁶ is a paper written by RSA and might be useful for future use. Sometimes the use of two or more factors is mentioned as “multifactor authentication”.

1.3 Out-Of-Band

Out-Of-Band⁷ authentication is the opposite of In-Band. In-Band uses only one communication channel to handle the complete authentication. On the other hand Out-Of-Band authentication uses multiple communication channels (for example internet and SMS) to achieve the authentication. The risk of both communication channels getting compromised is relatively low.

The picture below shows the difference between In-Band and Out-Of-Band authentication:

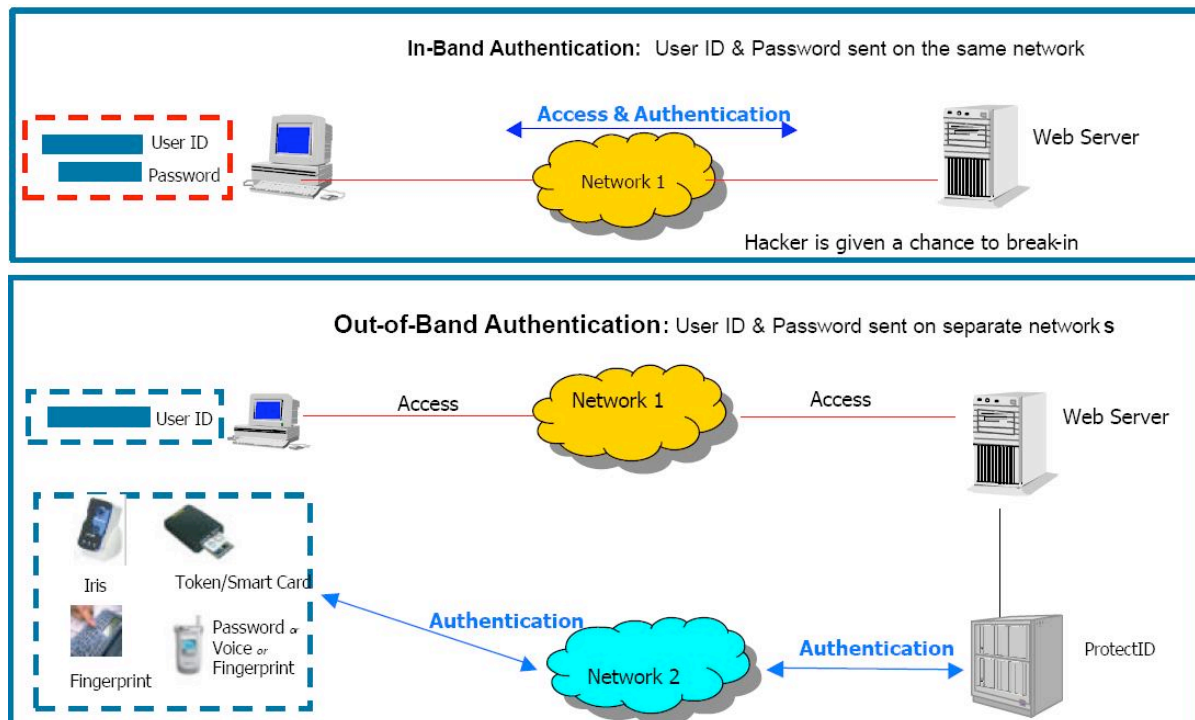


Fig. 1 In Band vs Out Of Band, source: “Out of Band Methodology, StrikeForce Technologies Inc, Monday, June 28th 2004.” (<http://www.sftnj.com/pdf/OutofBandMethodology.pdf>)

1.4 Challenge-Response

This authentication technique⁸ sends a “challenge” (question) to the other party, which on their turn must provide a valid “response” (answer). This technique is commonly used in smartcard based systems. Where the website shows the customer a code (challenge), the customer types this code into the smartcard and the smartcard will return a code (response) which the customer then uses to login to the website.

1.5 Reverse authentication

Reverse authentication⁹ means that the website first authenticates itself to the customer, before the customer proceeds to login and enter their username, password and other methods. When successful the customer knows that it is the original website and not a phishing site. One way of achieving this, is through the use of Out-Of-Band channels (for example through a cell phone).

1.6 Additional measures that can be applied on all auth. methods

Besides the authentication methods itself, there are additional measures that can be taken to improve the level of security. These measures all require different technological skills and may be expensive to implement.

1.6.1 Lockout (Denial of Service)

The lockout procedure is a part of the implementation and often adjustable. Setting the lockout to tight might frustrate users and will increase helpdesk calls. Often the lockout will activate after 3 – 5 failed login attempts. In most situations this feature offers a timer reset option, in which the counter will reset itself. This reset time shouldn't be set very short, this might weaken the authentication method because more login attempts can be made.

Failed login attempts should always be logged, if possible (due to local restrictions and laws) with as much information known. Make sure the time is Network Time Protocol (NTP) synchronized, so it can be used to track and sentence the attacker.

1.6.2 VirtualATM

The VirtualATM¹⁰ (by Authentium¹¹) solution creates a safe environment for online banking. This is done with Virtual Private Network (VPN) solutions. (Implementing VPN can be quite expensive, especially when there are lots of users involved. So this solution is proposed to use in "high security" environments or bank transactions.)

The solution also creates a lockdown of the system, to prevent malicious software of doing an attack. (The lockdown will only allow the VirtualATM to be active, all other applications will be blocked.) This might be frustrating for users who have an e-mail or Word document containing an account number. This solution is compatible with Microsoft Windows 2000 / XP / Vista.

VirtualATM is updated by VERO¹² and provides protection against keyloggers and screen-capture agents for online banking, online stock trading, database operators and Internet payment facilitators.

The VERO toolkit enables financial service providers to choose from a range of security approaches, including session virtualization, secure browsing, secure messaging to the desktop, and in-line anti-malware scanning. The toolkit further automates the process of branding and distributing the VERO secure transaction and communication solution to customers, via both online and offline distribution channels.

1.6.3 Encryption

Through the use of good encryption algorithms for transmitting data over communication channel(s), the risk of intercepting packets is highly reduced. Common used encryption methods for securing communication are: Secure Socket Layer¹³ (SSL) version 3 and Transport Layer Security (TLS) version 1. The use of encryption doesn't prevent Man In The Middle (MITM) attacks. In these attacks the encryption is terminated at the attacker side, who will generate a (fake) certificate real-time to offer to the user. The MITM attack can be noticed through sudden Certificate errors.

2. Authentication methods

In this chapter we discuss several online authentication methods. We have selected some existing (well-known) and new methods. The methods are grouped and shortly explained:

- Password (only)
 - Username & Password
 - Virtual Keyboard
 - Partial password
- SIM Toolkit
 - SIM Toolkit (HandyID)
- Token
 - RSA SecurID (SD 520)
- Graphical
 - Passmark Sitekey (now RSA)
 - PassFaces
 - Passpicture
- EMV
 - EMV Smartcard
- PKI
 - Public Key Infrastructure Smartcard
- OTP
 - One Time Password manual (Elcard / Scratch card)
 - One Time Password automatic (SMS)
 - One Time Password synchronous
 - One Time Password a-synchronous
- Bookmark authentication
 - BeamAuth (In the Comparison Matrix named as Bookmark authentication.)
 - PhishCops (In the Comparison Matrix named as Bookmark authentication.)

2.1 Authentication methods explained

Below is a short description of the different authentication methods.

2.1.1 Password (only) based

Authentication through the use of a username & password has been around for years. Since it does not require additional hardware or software, it is simple to use. In the early years of the internet it was sufficient but nowadays it is considered weak. The username and password can be easily handed over to someone else or be written down. This results in a weaker solution, you will never know who you are dealing with.

Several measures can be taken to increase the security of username & password solutions. Similar to ATM machines there can be a lockout procedure; when the user types in several wrong passwords (generally 3) the user is forbidden to login. Implementing such a solution should be done with care. Consider the length of the lockout (10 minutes, 24 hours or permanently) since this could result in a huge impact on the availability.

Other measures might require a minimum (and maximum) length of the password and show both username and password as asterisks (*). Also complexity requirements; use of letters, numbers and special characters could be considered. Password history is another option, the new password must differ from the last X (adjustable) passwords. Password lifetime defines, how long the password is legitimate. Before a change is required.

2.1.2 Virtual keyboard

Virtual keyboards are very similar to normal password based systems. They only differ in the use of a none hardware based keyboard, instead the keyboard is shown on the screen of the user. (Mostly through the use of Flash or JavaScript.) Some virtual keyboards use random positioning of the characters. These virtual keyboards come in all kinds of different shapes, see some examples below:

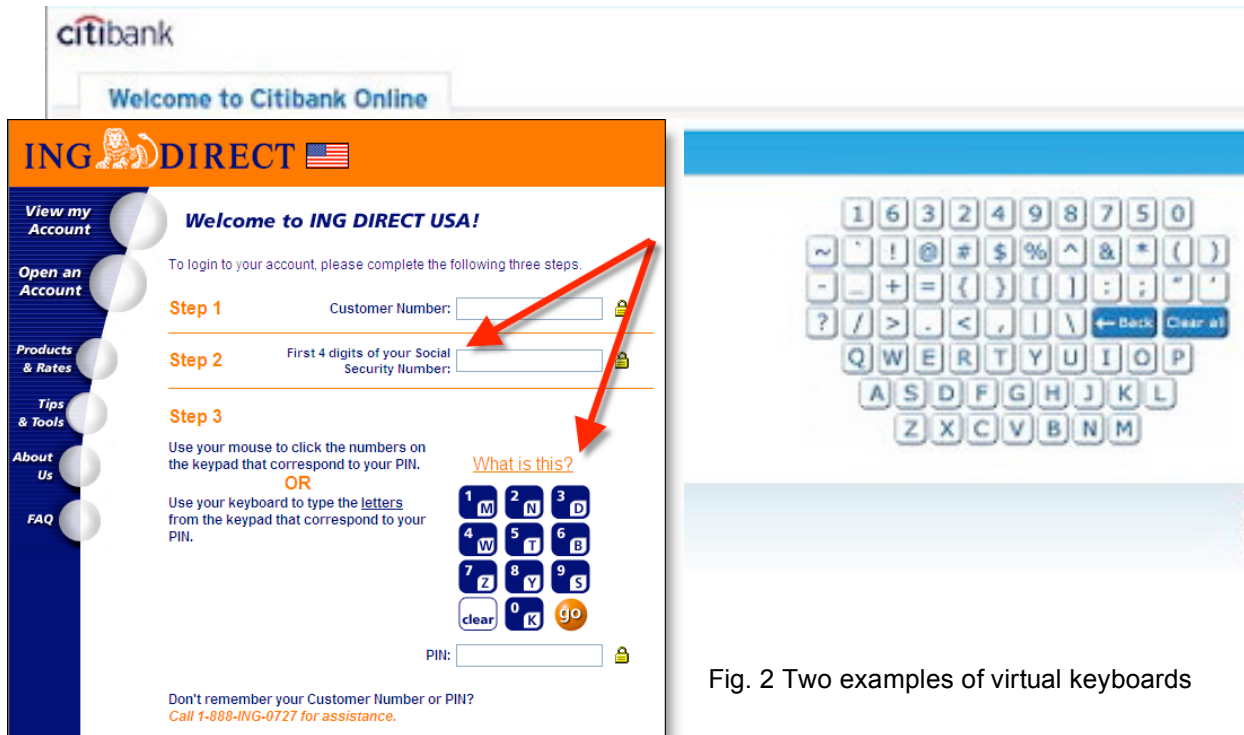


Fig. 2 Two examples of virtual keyboards

Another example is the login of the Dexia Luxembourg bank. Here the user must select the corresponding character using a “Tetris” like figure. This prevent direct recognition of the selected characters, see example below:



Fig. 3 Virtual keyboard used by the Dexia bank

A major bank, the Citibank¹⁴ had implemented a virtual keyboard, but the system was not adequate protected and got hacked¹⁵. This shows us an example of a bad implementation.

2.1.3 Partial password

Partial passwords are similar to normal username & password authentication. But instead of requesting the whole password, it asks some random characters from the password. That makes it harder for an attacker to intercept the whole password; at least it would take several logins to gather all the characters.

2.1.4 SIM Toolkit

SIM Application Toolkit¹⁶ (SAT) (commonly referred to as STK) is a standard of the GSM system which enables the SIM to initiate actions which can be used for Value Added Services (VAS).

The SIM Application Toolkit consists of a set of commands programmed into the SIM card which define how the SIM should interact directly with the outside world and initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access or control access to the network. The SIM also gives commands to the handset, such as display menu and ask for user input.

STK has been deployed by mobile operators around the world for many applications, often where a menu-based approach is required, such as Mobile Banking and content browsing. Designed as a single application environment, STK can be started at the initial power up of the SIM card and is especially suited to low level applications with simple user interfaces. For a schematic overview, see figure 4.

In GSM 2G networks SIM Application Toolkit is defined in the GSM 11.14 standard in 1995.

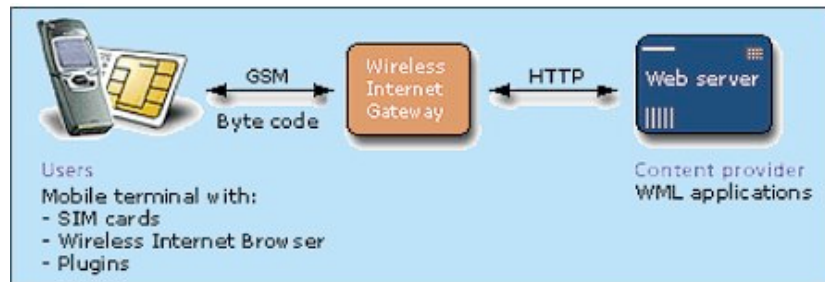


Fig. 4 Schematic overview SIM Toolkit.

Source: [http://www.tdap.co.uk/uk/archive/mobile/mob\(smart_0303\).html](http://www.tdap.co.uk/uk/archive/mobile/mob(smart_0303).html) (also Fig. 5)

2.1.4.1 STK in 3G Networks

USIM Application Toolkit¹⁷ (USAT) is the equivalent of STK for 3G networks. USAT enables the USIM to initiate actions which can be used for various VAS delivered over mobile devices. USAT takes advantage of the multi-application environment of 3G devices by not activating until a specific application has been selected, unlike STK which is activated at startup. Some functions are card related rather than application related. For an example see figure 5.

USAT is defined in standard 3GPP 31.111 for 3G.



Fig 5. illustration of the service

2.1.5 HandyID

HandyID¹⁸ is an mobile authentication method which provides a One Time Password (OTP), token based, two-factor authentication. It's possible to use it on a cell phone, PDA, Blackberry or a smart phone. By using the cell phone as a token, it saves the cost for additional hardware, doesn't provide the customer with additional hardware. This solution works with the ID Control Server¹⁹ (proprietary solution).

HandyID runs as a security application on the cell phone and is capable of generating both synchronous (time based) and a-synchronous (challenge-response) One Time Passwords. This process is protected through a PIN code. The advantage of this solution is that it does not require additional hardware for the customers and most people carry their cell phone around all the time. Example use is shown in figure 6.



Fig. 6 HandyID

2.1.6 Graphical

There are several graphical or partly graphical authentication methods. These methods could be a replacement of the existing username & password. Results of earlier investigations^{20 21} between the recognition of passwords and pictures shows that humans are better in recognizing pictures instead of remembering passwords.

Solutions investigated:

- Passmark Sitekey (now RSA)
- PassFaces
- Passpicture

2.1.6.1 Passmark Sitekey (now RSA)

PassMark²² calls its system a "Two-Factor Two-Way Authentication" system. A two-factor system, according to the PassMark website, is one that relies on two identifying bits of information to authenticate a transaction. One factor might be a traditional password, and the second might be a key fob or even some sort of biometric reader.

A two-way authentication system provides the capability not only for you to prove to the organization you are who you claim to be, but also for the organization to prove to you that it is really the organization sending you that e-mail or presenting you that website page. (commonly named as: Reverse Authentication)

PassMark has bypassed traditional second factors like hardware devices. Instead, the organization takes a look at your computer and creates a unique "fingerprint" of the machine, consisting of things like HTTP headers, the IP-address, software configurations and even its geographic location (based on IP-address). This fingerprint is used when the customer returns to the website of the organization.

For reverse authentication, SiteKey assigns a secret image known, only to the customer and to the organization. Customers logging into the organizations website will see the image and recognize it as a marker that the site is legitimate, and outgoing e-mail from the organization to the customer will also carry the image to mark legitimate e-mail. Figure 7 shows the example use of Sitekey.

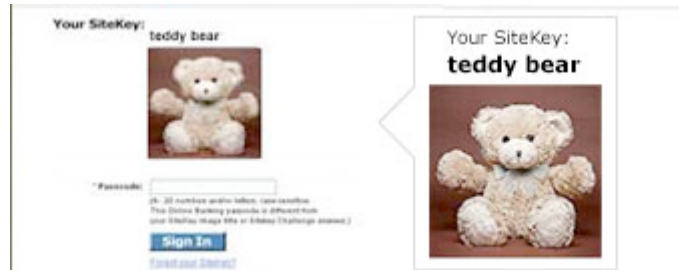


Fig. 7 Sitekey in action. Source <http://www.bankofamerica.com/privacy/sitekey/>

2.1.6.2 PassFaces

Passfaces²³ is an authentication method that uses the brain's natural power to recognize familiar faces. Passfaces authentication is based on a graphical password that provides bidirectional, interactive authentication. It verifies both the site to the user and the user to the site.

Passfaces Web Access is an application developer's kit that provides developers and system integrators everything they need to add Passfaces to customer applications. It includes a Software Developers Kit (SDK) with Server-side Java Class Package, Passfaces Library (database of faces), and the User Interface (client). Figure 8 shows a schematic overview.

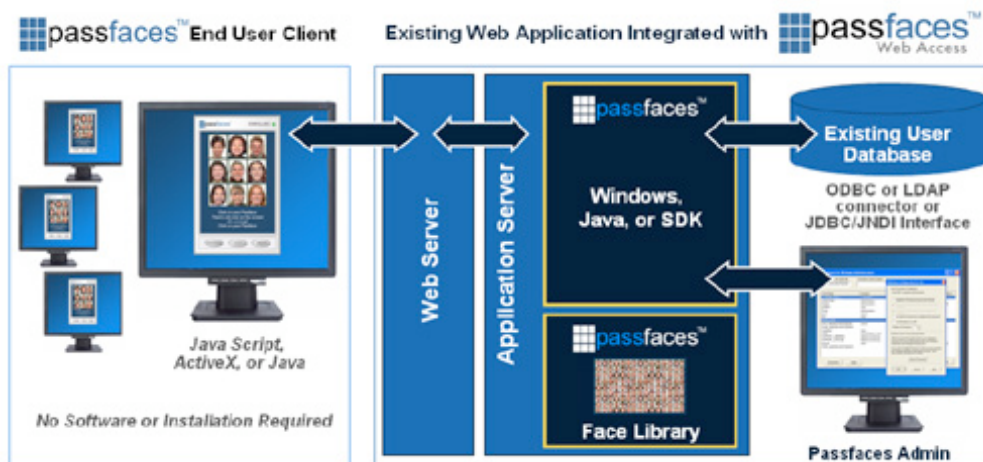


Fig. 8 PassFaces schematic. Source: http://www.passfaces.com/enterprise/products/web_access.htm

2.1.6.3 PASSpicture

This authentication method describes the more commonly known "PassClicks"²⁴. There are several other variants which work similar, or slightly different (for example: Draw a Secret). With PassClicks normal textual passwords are replaced with a sequence of clicks on an image.

New customers must first click on a number of items shown in the picture, and remember them. When the customer returns to login, they have to click on the exact items as they did with the registration process. The accuracy is important, because customers are not accurate enough to click on the exact pixels again. There must be a certain toleration to compensate that behavior.

2.1.7 RSA SecurID (SD520)

SecurID is a product of RSA and comes in different types, as shown in the picture on the right side. Synchronous RSA tokens are simple, based on the time they generate an One Time Password (OTP). In that case it are just “dumb” key generators that just generate OTPs every 30 or 60 seconds. A disadvantages of the tokens without a PIN code are that everyone can use them! Figure 9 shows some different RSA tokens.

The more advanced tokens generate OTPs based on a challenge-response and are protected through a PIN code. For use on a Blackberry or Smart phone there is SecurID software token. Similar to HandyID.



Fig. 9 RSA Tokens

2.1.8 EMV Smartcard

EMV²⁵ stands for Europay, Mastercard and Visa and was formed in 1999. It was funded to manage, maintain and enhance the EMV Integrated Circuit (IC) Card Specifications for Payment Systems. The EMV standard defines the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions.

Due to the use of Integrated Circuits instead of magnetic stripe the protection against copying the card is much better. Now encryption algorithms (DES, 3DES, RSA and SHA) are possible to prove the authentication of the card in the processing terminal and the transaction processing center. The downside is that the processing time is a little longer due to the use of encryption.

2.1.9 Public Key Infrastructure Smartcard

Based on the Public Key Infrastructure (PKI) principle. This means that the PKI solutions are multi purpose; encryption and signing are options that can be used. (Something that not much authentication methods offer.) The private key is embedded in the smartcard itself and not on the computer itself, where it might easily be compromised.

PKI based solutions are also possible in USB hardware tokens.

2.1.10 One Time Passwords

There are many One Time Password²⁶ (OTP) mechanisms, in this section we take a short look at some of them and point out some implementations.

Traditionally passwords can be easily told or handed over to someone else. Using passwords that are only valid for one time use, solves this problem and reduces this risk.

Different types of OTP²⁷:

- OTP manual (Elcard / Scratch card)
- OTP automatic (SMS)
- OTP synchronous (Hardware token)
- OTP a-synchronous (Random Reader)

OTP manual

A paper list or card containing One Time Passwords. It is similar to the TAN code list some banks use. It must be securely printed and mailed to the customer (to prevent copying and intercepting). A scratch card adds a little security because the One Time passwords aren't visible, only when they are scratched.

An example is the Elcard (figure 10), live demo:

http://www.elca.ch/live/3/resources/demo_en/main.html

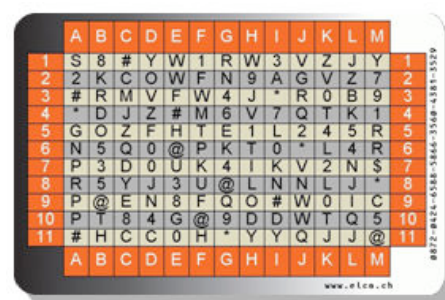


Fig. 10 Elcard

OTP automatic (SMS)

Instead of reading the One Time Password from a card or an (active) reader. The One Time Password is send to the customers cell phone via a Short Message Service (SMS). This is also a good example of Out-Of-Band (OOB) communication. (In this situation two communication channels are used.)

OTP synchronous

The time-synchronized one-time passwords²⁸ are usually related to physical hardware tokens (e.g., each user is given a personal token that generates a one-time password). Inside the token is an accurate clock that has been synchronized with the clock on the authentication server. On these OTP systems, time is an important part of the password algorithm since the generation of new passwords based on the current time rather than the previous password or a secret key.

OTP a-synchronous

This type of token generates a password based on a challenge or nonce from the server that is then combined with a base secret key within the token. The user, in response to the server's challenge, uses the result of this combination as its reply. To begin, the authentication server sends a challenge number to a workstation. This challenge number is entered into the token device. The challenge number is combined with the base secret key to generate the result that is displayed on the token device. The user enters the generated token result. The server, which also knows the token device's secret key, performs a similar function. The server's result is then compared with the result that the user entered.

Vasco is a supplier that is often used in OTP based systems. See appendix 1 for an overview of different Vasco products and characteristics. Appendix 2 shows the use of token devices by Dutch banks, note the use of the Vasco 820 device.

2.1.11 Bookmark authentication

Bookmark authentication relies on a bookmark you create during the registration process. (Often mailed to the new customer, so easy to add). This bookmark embeds a secret token. When clicking (or being direct to) the login page, the customer clicks on the bookmark, which automatically fills in the username and “injects” the secret code into the login page. Now the customer types in the password and submits it.

Example bookmark token:
`https://site.com/login#[TOKEN]`

Solutions investigated:

- BeamAuth²⁹
- PhishCops³⁰

2.2 Comparison Matrix Characteristics

The characteristics are explanatory and will not be discussed in detail. A short explanation is found under the Comparison Matrix itself.

The Comparison Matrix shows the authentication methods and their characteristics, based on a scale from 1 to 5, where higher is better. The use of the scale is shortly explained under the Comparison Matrix because it differs per characteristic, a general description is not possible.

Example: additional hardware.

First we inventory the hardware required by the authentication methods, this results in:

- None
- Cell phone
- Hardware token
- Paper / plastic card
- Card + reader

Now we can assign values to the different methods, based on how much additional hardware is required. We now have the legend for the Comparison Matrix:

- None 5
- Paper / plastic card 4
- Cell phone 3
- Hardware token 2
- Card + reader 1

2.2.1 Assumptions

Several assumptions are made to prevent indistinctness in the Comparison Matrix. These assumptions are discussable, but used to support the chosen values.

Assumptions made:

- The values in this Comparison Matrix should be considered as an average, they might differ per implementation or vendor.
- The values are adjustable, through the scale given in de legend. (Scale depends on the available items, not available is an option here).
- Login times are based on a comparison and thereby estimated values.
- The costs are split-up into 3 different types of cost and based on approximately 20.000 users.

Costs can be divided into: Acquisition-, Deployment-, and Operating-costs. These costs may vary on: developing custom software, amount of tokens, readers, smartcards used, distribution, helpdesk etc. Therefore the costs are an estimate and should always be investigated to a particular implementation.

The Comparison Matrix Characteristics is shown on the next page.

Authentication methods:	Characteristics:											Total score
	Additional hardware	Additional software	Complexity	Scalability	Portability	Login time	System requirements	Acquisition Cost	Deployment Cost	Operating Cost		
Username & Password	5	5	5	5	5	5	5	5	5	2	2	47
Partial password	5	5	5	5	5	3	5	5	4	2	2	44
Virtual Keyboard	5	4	4	4	4	4	4	4	4	2	2	39
SIM Toolkit (HandyID)	3	1	3	2	4	2	2	3	4	4	4	28
RSA SecurID	2	5	2	2	3	3	5	1	1	3	3	27
Passmark Sitekey (now RSA)	5	2	3	3	1	4	5	3	3	4	4	33
Passfaces	5	5	4	3	5	3	5	3	3	4	4	40
Passpicture	5	5	4	3	5	3	5	3	3	4	4	40
EMV Smartcard	1	1	1	2	3	3	1	1	2	3	3	18
Public Key Infrastructure (PKI) Smartcard	1	1	1	2	3	3	1	1	2	3	3	18
One Time Password manual (Elcard)	4	5	5	2	3	4	5	4	4	5	5	41
One Time Password manual (Scratchcard)	4	5	5	2	3	2	5	4	4	5	5	39
One Time Password automatic (SMS)	3	5	4	4	4	1	3	2	3	4	4	33
One Time Password synchronous	1	5	1	2	3	3	1	1	2	3	3	22
One Time Password a-synchronous	1	5	1	2	3	3	1	1	2	3	3	22
Bookmark authentication	5	5	4	4	2	4	5	3	4	5	5	41

(Score based on scale 1 -- 5, higher is better)

Short explanation:

Additional hardware, does the solutions require additional hardware?: [1 = card & reader], [2 = hardware token], [3 = cell phone], [4 = paper or card], [5 = none]

Additional software, does the solution require additional software?: [1 = application, [2 = cookie], [3 = n/a yet], [4 = Flash / Java enabled], [5 = none]

Complexity, how complex is it to implement the solution?: [1 = very difficult], [2 = difficult], [3 = medium], [4 = easy], [5 = very easy]

Scalability, can the solution grow?: [1 = very difficult], [2 = difficult], [3 = medium], [4 = easy], [5 = very easy]

Portability is the solution portable? (in your pocket or to other computers / smart phone): [1 = very difficult], [2 = difficult], [3 = medium], [4 = easy], [5 = very easy]

Login time: [1 = up till 60s or more], [2 = up till 50s], [3 = up till 40s], [4 = up till 30s], [5 = up till 20s]

System requirements: [1 = card + reader], [2 = compatible cell phone], [3 = normal cell phone], [4 = Flash / Java enabled], [5 = normal computer]

Acquisition Cost: [1 = very high], [2 = high], [3 = medium], [4 = low], [5 = very low]

Deployment Cost: [1 = very high], [2 = high], [3 = medium], [4 = low], [5 = very low]

Operating Cost: [1 = very high], [2 = high], [3 = medium], [4 = low], [5 = very low]

Table 1 . Comparison Matrix Characteristics of Authentication Methods

3. Attack vectors

In this chapter we will shortly explain the attacks on online authentication methods and present the Comparison Matrix Attack vectors versus Authentication Methods.

3.1 Attack vectors explained

Below we present short descriptions of the different attack vectors.

3.1.1 Shoulder surfing

Shoulder surfing^{31 32 33} is a method to reveal sensitive (login) information by looking at someone's keyboard or screen while he or she logs in or doing a transaction. This process can be automated, for example by placing cameras at ATM's. In principle it is a very easy way of getting sensitive information, there is not a need to involve any kind of technology. With exception of biometric authentication methods, all other methods are more or less vulnerable.

3.1.2 Keylogger

This attack can be hardware or software based. It simply logs all the keystrokes the user types. Advanced keyloggers³⁴ periodically send a file to the attacker, in that case the process is automatic and the attacker just waits. There are also keyloggers for cell phones (some of them are sold as legitimate parent watching programs).

3.1.3 Screen capturing

Screen capturing³⁵ is often integrated with a keylogger. In that case both keystrokes and visual items (for example virtual keyboards) are captured. This attack is not only useful to detect visual keyboard and other graphical authentication methods. It can also be used to look in confidential files (as they are shown on the screen). The screen capture can take screenshots or just capture the whole screen (small movie).

3.1.4 Brute force (exhaustive search)

Brute force³⁶ attacks simply generates all possible passwords and tries them. This attack is extremely inefficient and time consuming, but in the end it will find the password. This is not a real big risk with online systems due to the use of a lockout mechanisms but it can be a risk in an offline attack. (When the attacker has got a (hashed) password and / or username database.)

3.1.5 Guess attack

Guess attacks³⁷ are often useful for the so-called "secret questions" which are being used for emergency authentication (when someone forgets his password). Often the questions are pre-defined and the customer can select one of them. (For example: What is the name of your first pet? Or What is your favorite team?).

This information might be easy to guess for an attacker who knows his victim or easily being looked up on personal web / profile sites (for example: hyves and myspace). Many people reveal lots of information on these sites.

3.1.6 Dictionary attack

A dictionary attack³⁸ makes use of a dictionary file. People often use names of real things, things that can be easily be looked up as a password. Even if characters are replaced with numbers (e = 3, a = 4 etc.) it is still easy to check variations of the wordlist.

Similar to the brute force attack, the dictionary attack is mostly used in offline attacks. Otherwise there will be a lockout mechanism, and can be easily detected.

3.1.7 Hardware (observation) attack

This attack generally tries to look inside the hardware³⁹. The risk of this attack is determined on the cost and the profit (when successful). To disassemble an advanced hardware token, very specific devices like an electron microscope are necessary (only found in laboratories).

The most simple variant of this attack would be to copy a TAN code list or an OTP list. Other attacks might be on online (smart)card readers.

3.1.8 Social engineering

The success of this social engineering⁴⁰ depends on the readiness of the user to give / tell confidential information to the attacker. It can be summarized as talking to people in such a way that they are willing to give away their authentication information. It is still an underestimated risk, after several campaigns of warning users that usernames and passwords are private and should never be given away or told to other people. It still remains a problem, usernames and password are now considered private by the most customers.

3.1.9 Phishing attack

Phishing is best described as the digital variant of social engineering. Instead of calling people or talking to them, attackers often send e-mails to potential victims. The impact of compromised passwords depends on the authentication method used. In a traditional authentication environment (username & password) the impact is huge, the account can be overtaken.

3.1.10 Man In The Middle attack

All of the authentication methods described in the Comparison Matrix are more or less vulnerable to a Man In The Middle (MITM) attack^{41 42}. (Except PhishCops who are claiming to be not vulnerable to MITM attacks: "... The PhishCops® Website Authentication process is resistant to "man-in-the-middle" attacks and malware...").

The risk of being a victim of this attack depends on the user confidence in a (fake) website. Often a minor loss of attention where the customer clicks on a prepared item will start the attack. From that point on the entire communication is in control of the attacker. An attacker can show the unsuspecting customer just a normal transaction, but this transaction might include an unauthorized other transaction (of course not above a specific amount that must be checked due to banking / government regulations).

Depending on the criminal they might be interested in more personal information to use for identity theft (which is a growing problem on the internet).

3.1.11 Man In The Browser attack

Man In The Browser attacks^{43 44 45} are installed through a Trojan horse on the computer of the victim. This attack is capable of modifying online transactions as they occur in real time and will work on both Internet Explorer and Firefox (certainly on a Windows based Operating System). A MITB attack will activate not by clicking on a hyperlink, but through typing a certain URL in the web browser. Everything looks normal for the customer, but hidden unauthorized action takes place.

The MITB attack is similar to the MITM attack. But where a MITM attacks plays over the network in order to intercept messages in a public key exchange, and retransmit bogus public keys instead of the requested ones. Instead of the MITB attack which takes place in the web browser of the victim and is more difficult to prevent and disinfect.

3.1.12 Network sniffing

Network sniffing^{46 47} is about intercepting packets while they are traveling over the network. (Assumed that there is no encryption used.) The risk of an intercepted username and password are much bigger than the risk of an intercepted OTP. After all an OTP is just once usable (depending on the transaction (challenge-response) or time based and changed every 30 or 60 seconds).

3.1.13 Short access

This attack describes the possibilities of an attacker when there is short access to the computer, TAN code list, Digipass etc. In the situation of an unlocked computer, an attacker might install a software keylogger on the system or look for password post-its. When the computer is locked, there is the risk of installing a hardware keylogger.

Almost all OTP generators use a PIN before the transaction can take place, this reduces the risk to a minimum (especially when combined with a lockout policy) Manual OTP lists and TAN code lists facing the highest risk here, they can be easily copied. (Scratch cards offer the protection against copying)

Modern cell phones face the same risk of installing a keylogger. The lock option some phones offer is rarely used. The cell phone is not a primary risk, because it is mostly used as the secondary factor.

3.2 Comparison Matrix Attack vectors

The Comparison Matrix shows the authentication methods and the attack vectors. Through the use of values which represent the probability to succeed the attack. Based on a scale from 1 to 5 where higher is a better resistance against the attack.

Likely to succeed the attack:

- 1 = very likely
- 2 = likely
- 3 = possible
- 4 = not likely
- 5 = negligible

3.2.1 Assumptions

Several assumptions are made to prevent indistinctness in the Comparison Matrix. This assumptions are discussable, but used to support the chosen values.

Assumptions made:

- Some of the authentication methods might be better protected, depending on the implementation. This Comparison Matrix shows an average.
- Passwords chosen by the user are in general weaker than a generated password.
- Offline readers are not vulnerable to a keylogger, only the response / OTP can be logged. (The password / response is only usable for one specific authentication / transaction)
- There are also keyloggers for cell phones, but their appearance is small. Besides it is not likely that two communication channels are compromised.
- Hardware attack can vary from copying a TAN code list to an electron microscope. The likelihood of such an attack depends on the knowledge and devices required.
- All of the mentioned methods are more or less vulnerable to a MITM attack, however PhishCops (Bookmark authentication) claims not to be vulnerable
- Short access aims at short physical access (the period used here is 10 minutes).

The Comparison Matrix (Attack vectors) is shown on the next page.

Authentication method:	Attack vectors:											Total score:		
	Shoulder surfing	Keylogger capturing	Screen capturing	Brute force (exhaustive search)	Guess attack (knowing someone)	Dictionary attack	Hardware (observation) attack	Social engineering	Phishing attack	Man In The Middle attack	Man In The Browser attack		Network sniffing	Short access
Username & Password	3	1	4	2	2	1	5	3	1	1	2	1	3	29
Partial password	4	3	5	1	3	2	5	3	3	1	2	2	3	37
Virtual Keyboard	1	5	1	2	2	1	5	3	3	1	3	3	3	33
SIM Toolkit (HandyID)	5	4	4	5	5	5	4	5	4	4	5	5	4	59
RSA SecurID	4	4	4	5	5	5	5	5	4	4	4	4	4	57
Passmark Sitekey (now RSA)	3	2	3	3	3	2	5	2	2	3	3	4	3	38
Passfaces	2	5	2	3	1	3	5	3	3	3	3	3	4	40
Passpicture	2	5	2	4	2	3	5	4	3	3	3	3	4	43
EMV Smartcard	4	5	5	5	5	5	5	5	5	4	4	5	4	61
Public Key Infrastructure (PKI) Smartcard	4	5	5	5	5	5	5	5	5	4	4	5	4	61
One Time Password manual (Elcard)	3	4	4	4	5	5	1	3	3	3	3	4	1	43
One Time Password manual (scratch card)	3	4	4	4	5	5	3	3	3	3	3	4	2	46
One Time Password Automatic (SMS)	4	4	4	5	5	5	5	5	4	4	4	4	3	56
One Time Password synchronous	4	4	4	5	5	5	5	5	4	4	4	4	5	58
One Time Password a-synchronous	4	4	4	5	5	5	5	5	5	4	5	4	5	60
Bookmark authentication	3	3	3	3	4	4	5	4	4	4	2	4	3	46
(Likely to succeed the attack: [1 = very likely], [2 = likely], [3 = possible], [4 = not likely], [5 = negligible])														
Short explanation:														
Shoulder surfing, someone is standing behind you and watch your keyboard and monitor.														
Keylogging, piece of software that records each key pressed.														
Screencapturing, captures everything that shows up on the screen.														
Brute force attack, simply try all possibilities, not efficient but finally the password is found.														
Guess attack, by knowing someone's favorite soccer club, wife, pets, children.														
Dictionary attack, use existing dictionaries from languages or known usernames / passwords.														
Hardware (observation) attack. Observe the hardware while performing authentication or transactions.														
Social engineering, try to get confidential information by means of calling or talking to the victim.														
Phishing attack, the digital version of social engineering.														
MITM, attacker is able to read, insert and modify messages on the compromised connection.														
MITB, similar to MITM but the action takes place at the victims browser and not in public space.														
Network sniffing, intercept packets while they are going over the network, without the use of encryption (SSL).														
Short access, is it possible to do a successful login when an attacker has short physical access to the computer / hardware.														

Table 2. Comparison Matrix Attack vectors of Authentication Methods

4. User acceptance

Besides secure authentication itself, user acceptance^{48 49} is another important aspect. The users require a secure login, but without adding much more complexity at the user side. It all starts with awareness of the users. When they are aware of the risks, there is a safe ground to increase security measures. Complexity depends on the user group who is going to use the solution. User acceptance has not always been taken into account (enough), which results in bad user experience or worse; users do not use online services anymore.

When users are forced to use all kinds of complex methods, they are willing to search for a workaround. For example the complexity requirements of passwords: If users are not able to (easily) remember the password, they will write it down or save it in a text file on the computer (this obviously decreases security).

The best way to test the user acceptance is through a “User Acceptance Test” (UAT). This includes different tests than the ones used by the developers, who are focusing their tests on functional requirements.

From the Comparison Matrix the columns below are important to make the distinction between the different authentication methods with regard to user acceptance.

Authentication methods:	Characteristics:			
	Additional hardware	Additional software	Complexity	System requirements
Username & Password	5	5	5	5
Partial password	5	5	5	5
Virtual Keyboard	5	4	4	4
SIM Toolkit (HandyID)	3	1	3	2
RSA SecurID	2	5	2	5
Passmark Sitekey (now RSA)	5	2	3	5
Passfaces	5	5	4	5
Passpicture	5	5	4	5
EMV Smartcard	1	1	1	1
Public Key Infrastructure (PKI) Smartcard	1	1	1	1
One Time Password manual (Elcard)	4	5	5	5
One Time Password manual (Scratchcard)	4	5	5	5
One Time Password automatic (SMS)	3	5	4	3
One Time Password synchronous	1	5	1	1
One Time Password a-synchronous	1	5	1	1
Bookmark authentication	5	5	4	5

5. Scenario

First we will explain how to use the Comparison Matrix. The Matrix is filled with several authentication methods combined with characteristics and attack vectors. First of all the characteristics should be defined: Do you want to use additional hardware and / or software? Do you expect a (huge) increase of users? What is the budget?

Now you have the characteristics and continue to the attack vectors you want to prevent. Do you want to prevent specific attacks? Or prevent all possible attacks at some minimum level?

When the requirements (characteristics and prevention of attacks) are clear, you must select a minimum score. The values in the Comparison Matrix are based on a scale from 1 – 5, where higher is better.

Values are based on some assumptions, which can be changed and with so the values. The total score field is not pointing out the best authentication method, it gives the user a guideline which helps to make a decision in a given situation with specific requirements.

5.1 Scenario online banking

An online banking site wants to offer customers safe login, even from an internet-cafe abroad. The solution must be highly resistant against: (due to the use in an uncontrolled computer environment)

- Shoulder surfing
- Keyloggers
- Screen capturing

At least a “3” or higher is preferred for these items (higher is preferred)

5.2 Comparison Matrix Characteristics

Considering the requirements from the scenario it seems that portability is the important issue here. So the focus should be on:

- Additional hardware
- Additional software
- Portability

Now we are looking for the solution(s) which score a 3 or higher on the selected characteristics.

This results in:

- Username & Password
- Partial password
- Virtual Keyboard
- PassFaces
- Passpictures
- One Time Password manual (Elcard)
- One Time Password manual (Scratchcard)
- One Time Password automatic SMS

5.3 Comparison Attack vectors

The result of the Characteristics is now used in the Comparison Matrix Attack vectors. Here we check how resistant the authentication methods are against the Attacks. In this scenario:

- Shoulder surfing
- Keyloggers
- Screen capturing

Now we look in the Comparison Matrix and we only select the authentication methods with a “3” or higher on the important attacks. The following authentication methods are remaining after the Attack vector is applied.

- One Time Password manual (Elcard)
- One Time Password manual (Scratchcard)
- One Time Password automatic SMS

The results here forms input for an authentication method selection process.

To conclude

The result of this project is a method which allows the user to quickly and easily compare different online authentication methods. This method is specified in an easy to use and extensible Comparison Matrix. At this stage the Comparison Matrix contains several online authentication methods. Through the use of values to make distinction between the authentication methods it can be easily automated in Microsoft Excel for future use.







As shown in the scenario, the Comparison Matrix works fine and is easy to use. The result(s) from the Comparison Matrix can then be further investigated. This will narrow down the range of products that needs to be investigated and forms input for an authentication method selection process.


Appendix 1, Vasco Digipass Comparison

DIGIPASS product overview table

		TIME/EVENT/CHALLENGE BASED ALGORITHMS	CHALLENGE / RESPONSE	RESPONSE ONLY	DES / (3)DES	AES	UNLOCKING VIA CHALLENGE / RESPONSE	UNLOCKING PUK CODE	LANGUAGE SUPPORT	N°OF APPLICATIONS	ACTIVATION METHOD	EXPECTED LIFETIME (IN YEARS)	DESIGNED FOR	SPECIAL FEATURE
	GO 1	TIME EVENT		↔	↔					1	PROG	5	REMOTE ACCESS	EASY
	GO 2	TIME EVENT		↔	↔	↔			↔	± 5	SMART CARD	5	REMOTE ACCESS	BALANCE READER
	PRO 250	TIME EVENT CHAL	↔	↔	↔		↔			3	PROG	7	BANKING	PORTABLE
	PRO 260	TIME EVENT CHAL	↔	↔	↔		↔			3	PROG	7	BANKING	PORTABLE
	PRO 300	TIME EVENT CHAL	↔	↔	↔		↔			3	PROG	10	BANKING	LONG TIME BATTERY
	PRO 550	TIME EVENT CHAL	↔	↔	↔	↔	↔ OR ↔		↔	4 x 2	PROG	5	BANKING	MESSAGES IN OWN LANGUAGE
	PRO 560	TIME EVENT CHAL	↔	↔	↔	↔	↔ OR ↔		↔	4 x 2	PROG	5	BANKING	MESSAGES IN MULTIPLE LANGUAGES
	PRO 700	TIME EVENT CHAL	↔	↔	↔		↔		↔	8	PROG	5	BANKING	COMPLEX SIGNATURES
	PRO 800	TIME EVENT CHAL	↔	↔	↔	↔			↔	± 5	SMART CARD / PROG	5	BANKING	BALANCE READER
	DESK 850	TIME EVENT CHAL	↔	↔	↔	↔			↔	∞ VIA PC	SMART CARD / PROG	5	BANKING / PKI	USB CONNEC- TION
	FOR PALM	TIME EVENT CHAL	↔	↔	↔		SERVER			∞	ONLINE	NOT APPLICABLE	REMOTE ACCESS	MULTI PROFILES
	FOR POCKET PC	TIME EVENT CHAL	↔	↔	↔		SERVER			∞	ONLINE	NOT APPLICABLE	REMOTE ACCESS	MULTI PROFILES
	FOR WIN	TIME EVENT CHAL	↔	↔	↔	↔	SERVER			∞	ONLINE	NOT APPLICABLE	REMOTE ACCESS	MULTI PROFILES
	FOR SIM	TIME EVENT CHAL	↔	↔	↔			↔		8	ONLINE	NOT APPLICABLE	BANKING	MOBILE BANKING
	AUTHENTICATION SERVER	TIME EVENT		↔	↔		SERVER			∞	ONLINE	NOT APPLICABLE	BANKING / E-COM- MERCE	EASY

Appendix 2, Readers used by Dutch banks

Bank	Name of the reader	Picture of the reader
Rabobank	Randomreader / Digipass	
ABNAMRO bank	e.identifier	X
ING bank	Beveiligingscalculator	
SNS bank	Digipas	
Fortis	Access key	
DSB bank	Digi-P	
Friesland bank	Easykey	

Bizner bank	Bizkey	
-------------	--------	------------------------------------------------------------------------------------

Literature

¹ www.deloitte.nl

² Customer Authentication. Lawrence Ong, Deloitte, 2006

³ <http://www.fnal.gov/docs/strongauth/>

⁴ <http://www.rsa.com/glossary/default.asp?id=1080>

⁵ http://en.wikipedia.org/wiki/Two-factor_authentication

⁶ <http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf>

⁷ <http://www.ecommercetimes.com/story/55570.html?welcome=1201687370>

⁸ http://en.wikipedia.org/wiki/Challenge-response_authentication

⁹ <http://www.freshpatents.com/System-and-method-for-security-in-global-computer-transactions-that-enable-reverse-authentication-of-a-server-by-a-client-dt20070104ptan20070006286.php>

¹⁰ <http://authentium.blogspot.com/2007/05/virtualatm-vs-greenborder.html>

¹¹ <http://www.authentium.com/home/>

¹² <http://www.thefreelibrary.com/Authentium+Releases+VERO+Secure+Online+Banking+Solution.-a0169640591>

¹³ http://en.wikipedia.org/wiki/Secure_Sockets_Layer

¹⁴ <http://www.citibank.com/us/index.htm>

¹⁵ <http://www.tracingbug.com/index.php/articles/view/23.html>

¹⁶ http://en.wikipedia.org/wiki/SIM_Application_Toolkit

¹⁷ <http://en.wikipedia.org/wiki/Usat>

¹⁸ http://www.idcontrol.net/index.php?option=com_content&task=category§ionid=6&id=36&Itemid=95

¹⁹ http://www.idcontrol.com/index.php?option=com_content&task=category§ionid=6&id=33&Itemid=54

²⁰ Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice, Susan Wiedenbeck, Jim Waters et-al, College of IST, Drexel University, 2005

²¹ Second Look at the Usability of Click-Based Graphical Passwords, Sonia Chiasson et-al, Human-Oriented Technology Lab & School of Computer Science, Carleton University, 2007

²² <http://www.cafeid.com/art-sitekey.shtml>

²³ http://www.passfaces.com/enterprise/products/web_access.htm

²⁴ <http://labs.mininova.org/passclicks/>

²⁵ <http://en.wikipedia.org/wiki/EMV>

²⁶ http://en.wikipedia.org/wiki/One-time_password

²⁷ E-Banking Authentication. Lawrence Ong, Deloitte, 2006

-
- 29 <http://benlog.com/articles/2007/02/06/beamauth-two-factor-web-authentication-with-a-bookmark/>
- 30 <http://phishcops.com>
- 31 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci802244,00.html#
- 32 http://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29
- 33 <http://hci.stanford.edu/research/GUIDe/publications/SOUPS%202007%20-%20Reducing%20Shoulder-surfing%20by%20Using%20Gaze-based%20Password%20Entry.pdf>
- 34 http://en.wikipedia.org/wiki/Keystroke_logging
- 35 <http://www.zeltser.com/presentations/impersonation-attacks.pdf>
- 36 http://nl.wikipedia.org/wiki/Brute_force
- 37 <http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf>
- 38 http://en.wikipedia.org/wiki/Dictionary_attack
- 39 http://en.wikipedia.org/wiki/Side_channel_attack
- 40 [http://en.wikipedia.org/wiki/Social_engineering_\(computer_security\)](http://en.wikipedia.org/wiki/Social_engineering_(computer_security))
- 41 http://en.wikipedia.org/wiki/Man-in-the-middle_attack
- 42 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci499492,00.html
- 43 <http://www.grenswetenschap.nl/permalink.asp?grens=1655>
- 44 http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1207954,00.html
- 45 <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9049080>
- 46 http://en.wikipedia.org/wiki/Packet_sniffer
- 47 <http://netsecurity.about.com/cs/hackertools/a/aa121403.htm>
- 48 <http://www.prleap.com/pr/86294/>
- 49 http://en.wikipedia.org/wiki/Acceptance_testing#User_acceptance_testing