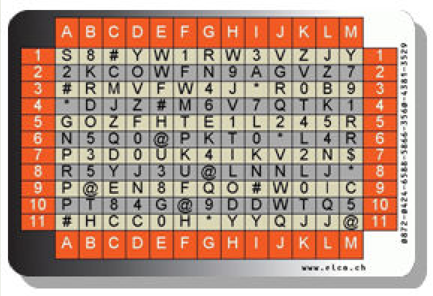
Online auhthentication methods

"Evaluate the strength of online authentication methods"



	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	S	8	#	Y	W	1	R	W	3	V	Z	J	Y	1
2	2	K	C	O	W	F	N	9	A	G	V	Z	7	2
3	#	R	M	V	F	W	4	J	*	R	0	B	9	3
4	*	D	J	Z	#	M	6	V	7	Q	T	K	1	4
5	G	O	Z	F	H	T	E	1	L	2	4	5	R	5
6	N	5	Q	0	@	P	K	T	0	*	L	4	R	6
7	P	3	D	0	U	K	4	I	K	V	2	N	$	7
8	R	5	Y	J	3	U	@	L	N	N	L	J	*	8
9	P	@	E	N	8	F	Q	O	#	W	0	I	C	9
10	P	T	8	4	G	@	9	D	D	W	T	Q	5	10
11	#	H	C	C	0	H	*	Y	Y	Q	J	J	@	11
	A	B	C	D	E	F	G	H	I	J	K	L	M	

www.elca.ch

Introduction

Cornel de Jong

System and Network Engineering

Universiteit van Amsterdam

Spui 21

1012WX Amsterdam

Supervisors:

UvA:

Cees de Laat

Deloitte:

Gijs Hollestelle

Tom Schuurmans

Research Project

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.

Agenda

- Project background
- Authentication methods
- Characteristics
- Attack vectors
- Comparison Matrix
- Scenario

Security.NL maakt Nederland veilig - Windows Internet Explorer provided by Deloitte.
http://www.security.nl/article/17846/1/Trojaans_paard_kraakt_beveiliging_400_internetbanken.html
Google
Security.NL maakt Nederla...
SquirrelMail 1.4.9a - Signout
Risk Management - contro...
Biometrics - Wikipedia, th...
Security.NL maakt Ned...
Page
Tools
SECURITY.nl
maakt nederland veilig
..op het gebied van veilig programmeren?
Home | Forum | Links | Archief | Tip ons! | Contact | Themaweken | Adverteren | RSS
Login @ ANP
mailto:redactie@security.nl
Internet | Protected Mode: On
180%

Poll

Belangrijkste meetpunt voor veilige software:

- ○ Aantal beveiligingslekken
- ○ Impact van beveiligingslekken
- ○ Aantal dagen dat software lek is
- ○ Aantal uitgebrachte patches
- ○ Aantal patchmomenten
- ○ Beschikbare exploits
- ○ Aantal regels broncode
- ○ Gebruikte ontwikkelmethode
- ○ Anders, ...

Trojaans paard kraakt beveiliging 400 internetbanken

Door Redactie op dinsdag 15 januari 2008 16:06

Dat malware in staat is om de twee-factor authenticatie te kraken die banken voor het online bankieren gebruiken is al langer bekend, een nieuw Trojaans paard jaagt zelfs een virusonderzoeker die regelmatig dit soort malware onderzoekt de stuipen op het lijf. "De schaal en complexiteit van deze nieuwe Trojan is zorgwekkend, zelfs voor iemand die op dagelijkse basis banking Trojans ziet", zegt Symantec's Liam OMurchu.

Silentbanker, zoals de malware wordt genoemd, kan de beveiliging van meer dan 400 banken omzeilen, waaronder die in Europese landen. Het Trojaanse paard onderschept transacties die twee-factor authenticatie vereisen, en laat dan de betaling naar de rekening van de crimineel of katvanger, overmaken. Om het slachtoffer niets te laten vermoeden krijgt die een gemanipuleerd afschrift en overzichtspagina te zien. Aangezien de gebruiker niets vermoed, bevestigt die de transactie waarna het geld naar de criminelen wordt overgemaakt. "De

Login

E-mail:

Wachtwoord:

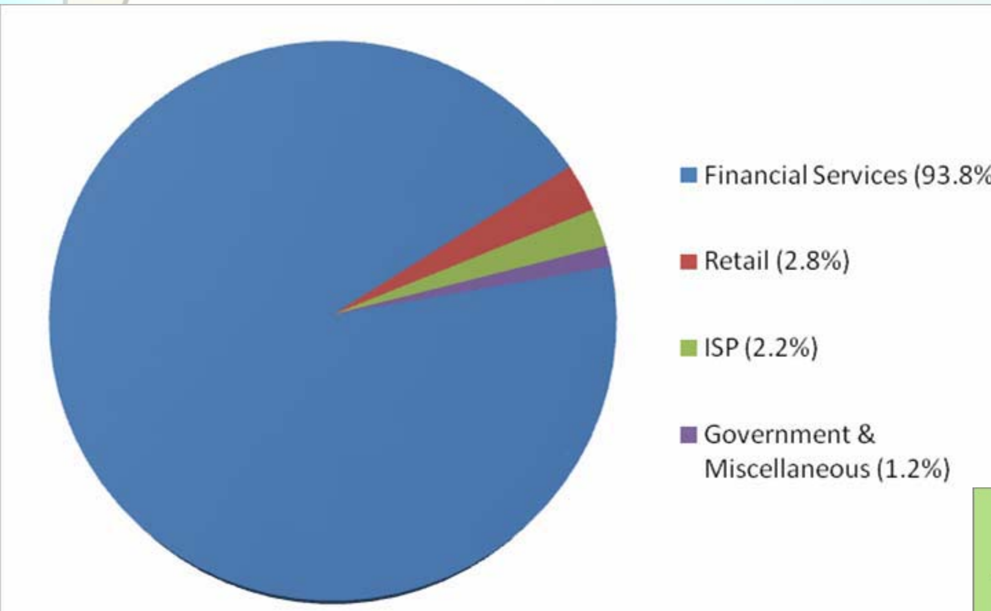
Login of registreer

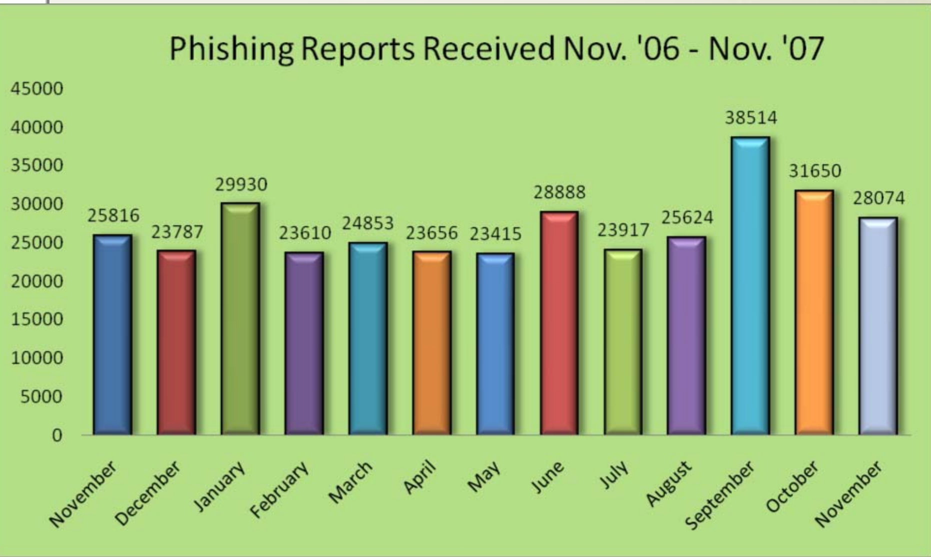
□Stelling

ANP zelf schuldig aan computervredebreuk door Novum

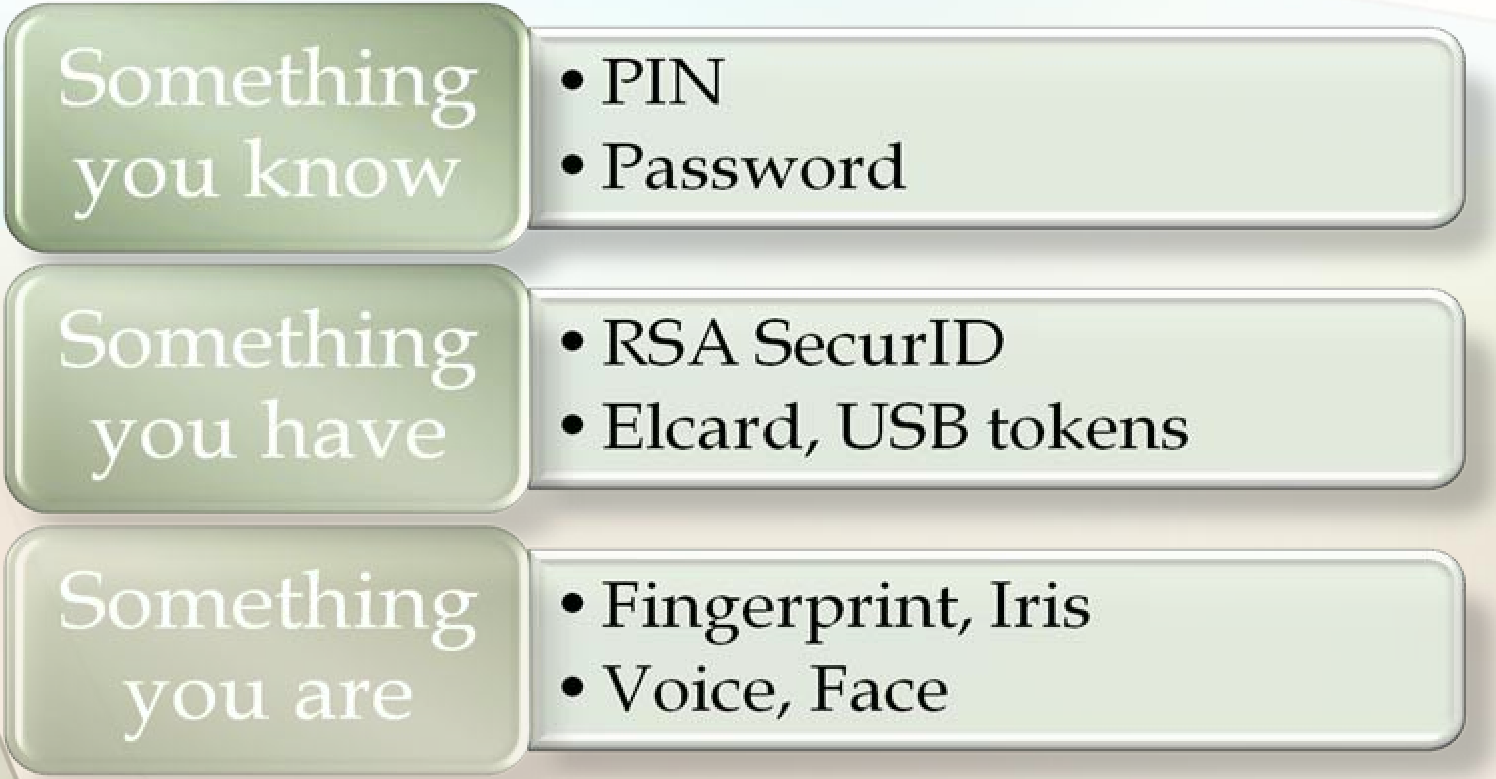
Antiphishing.org

November 2007





Authenticate



Something you know

- PIN
- Password

Something you have

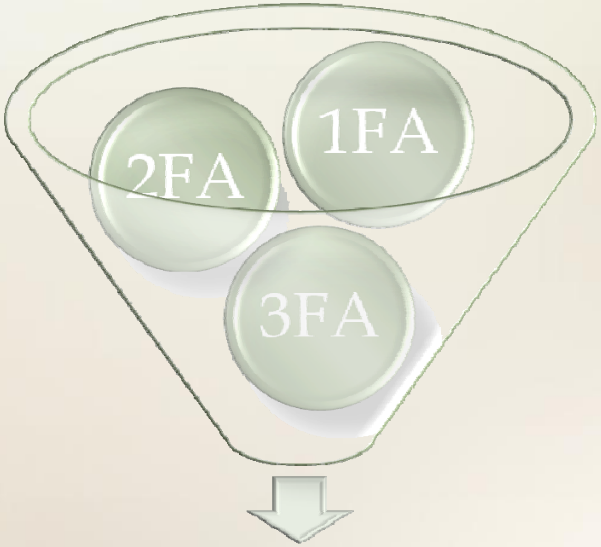
- RSA SecurID
- Elcard, USB tokens

Something you are

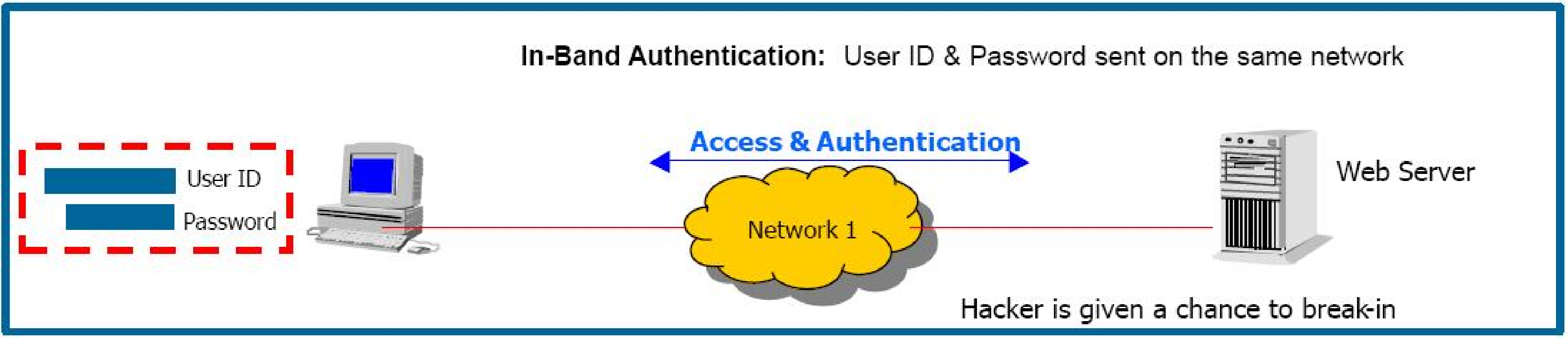
- Fingerprint, Iris
- Voice, Face

Multifactor authentication

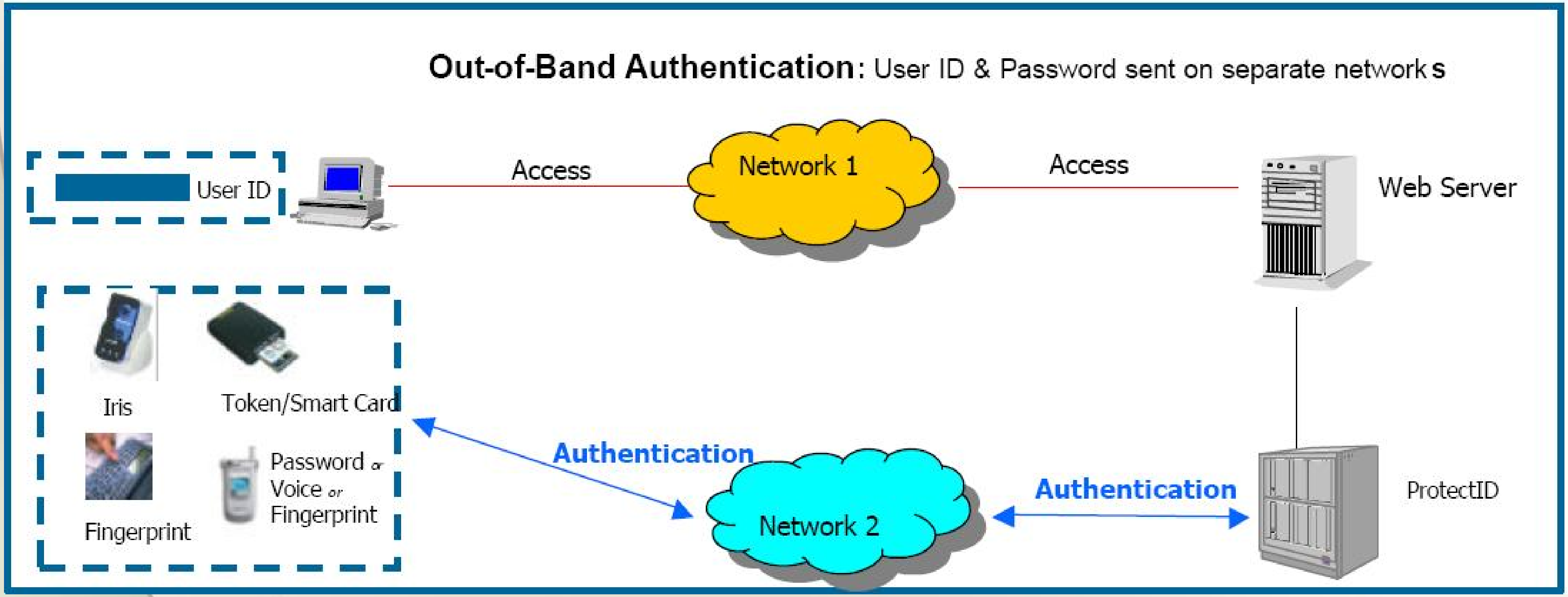
- One-Factor Authentication
- Two-Factor Authentication
- Three-Factor Authentication



In-Band versus Out-Of-Band



In-Band Authentication: User ID & Password sent on the same network



Out-of-Band Authentication: User ID & Password sent on separate network s

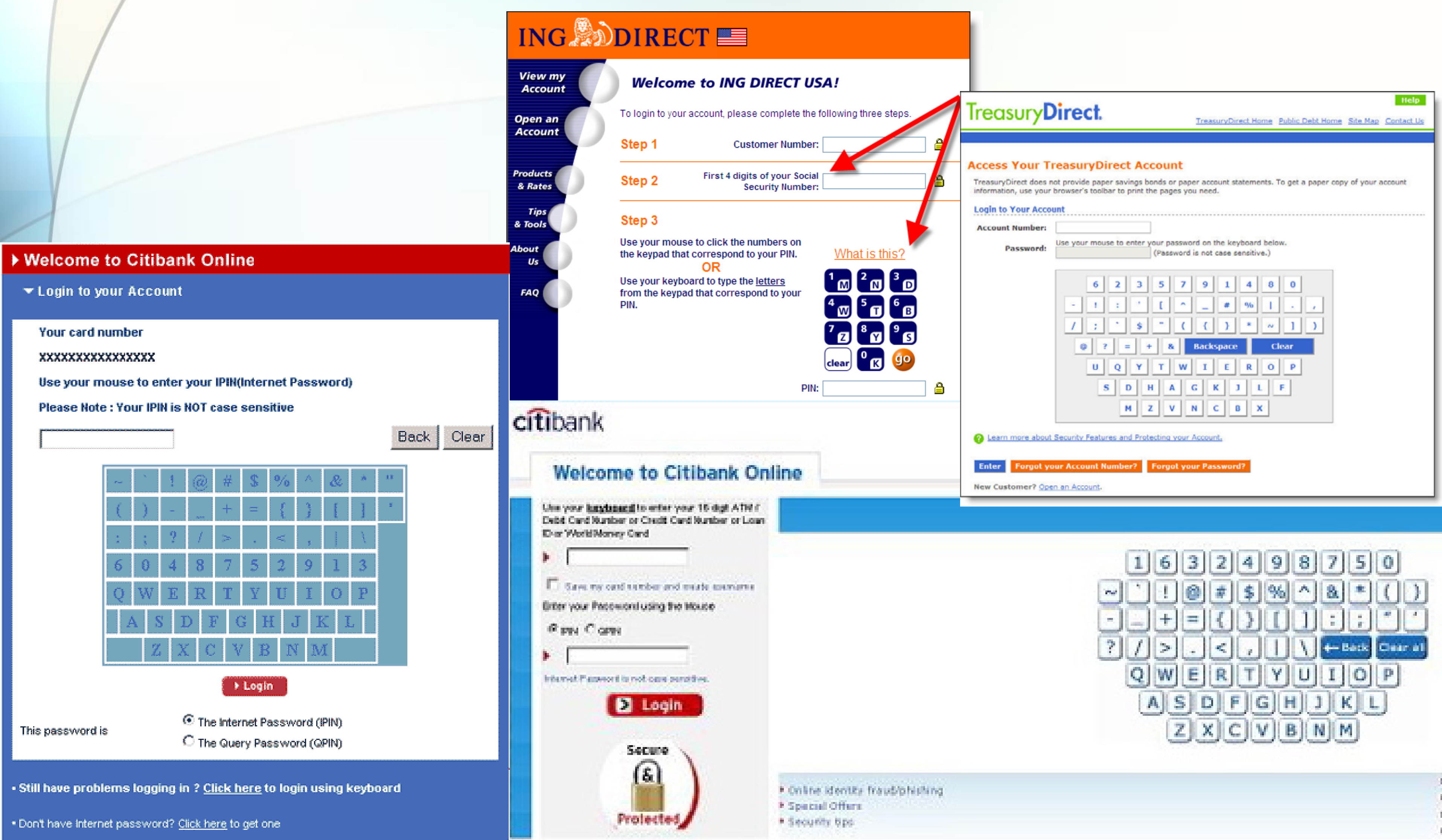
Authentication methods

- Password (only)
- SIM Toolkit
- Hardware Token
- Graphical
- EMV Smartcard
- PKI Smartcard
- One Time Password
- Bookmark

Virtual keyboard

- No hardware keyboard required
- Requires Flash / JavaScript
- Random positioning of the characters
- Prevents keylogger attacks
- But makes it easier for shoulder surfing and screen capturing

Virtual keyboard examples



ING DIRECT

Welcome to ING DIRECT USA!

To login to your account, please complete the following three steps.

Step 1 Customer Number:

Step 2 First 4 digits of your Social Security Number:

Step 3

Use your mouse to click the numbers on the keypad that correspond to your PIN.

OR

Use your keyboard to type the letters from the keypad that correspond to your PIN.

What is this?

PIN:

TreasuryDirect.

Access Your TreasuryDirect Account

TreasuryDirect does not provide paper savings bonds or paper account statements. To get a paper copy of your account information, use your browser's toolbar to print the pages you need.

Login to Your Account

Account Number:

Password: Use your mouse to enter your password on the keyboard below. (Password is not case sensitive.)

Learn more about Security Features and Protecting your Account.

New Customer? Open an Account.

Welcome to Citibank Online

Login to your Account

Your card number

xxxxxxxxxxxxxxxx

Use your mouse to enter your IPIN(Internet Password)

Please Note : Your IPIN is NOT case sensitive

This password is ● The Internet Password (IPIN) ○ The Query Password (QPIN)

• Still have problems logging in ? Click here to login using keyboard

• Don't have Internet password? Click here to get one

citibank

Welcome to Citibank Online

Use your keyboard to enter your 16 digit ATM / Debit Card Number or Credit Card Number or Loan ID or WorldMoney Card

□ Save my card number and make username

Enter your Password using the Mouse

● IPIN ○ QPIN

Internet Password is not case sensitive.

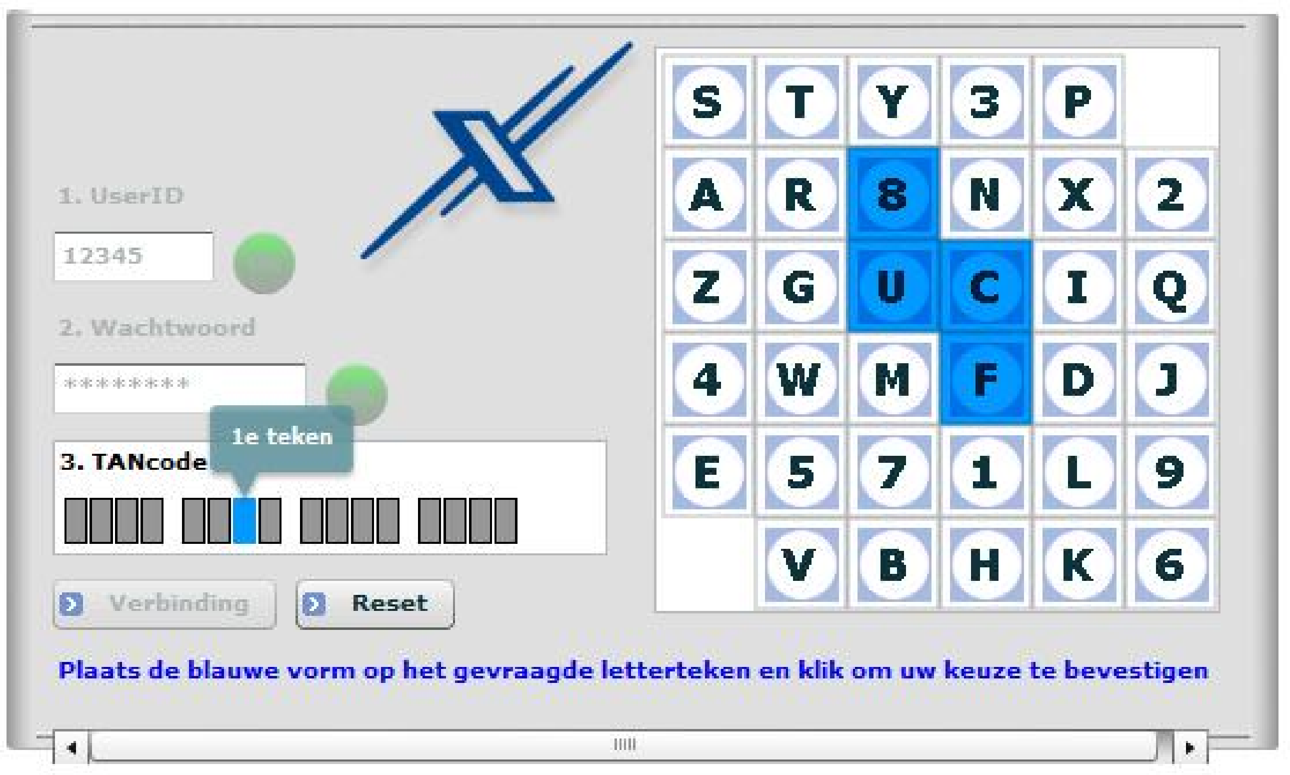
• Online identity fraud/phishing

• Special Offers

• Security tips

Virtual keyboard examples 2

A more sophisticated example of the Dexia bank (Luxembourg)



1. UserID

12345

2. Wachtwoord

****

3. TANcode

S	T	Y	3	P	
A	R	8	N	X	2
Z	G	U	C	I	Q
4	W	M	F	D	J
E	5	7	1	L	9
	V	B	H	K	6

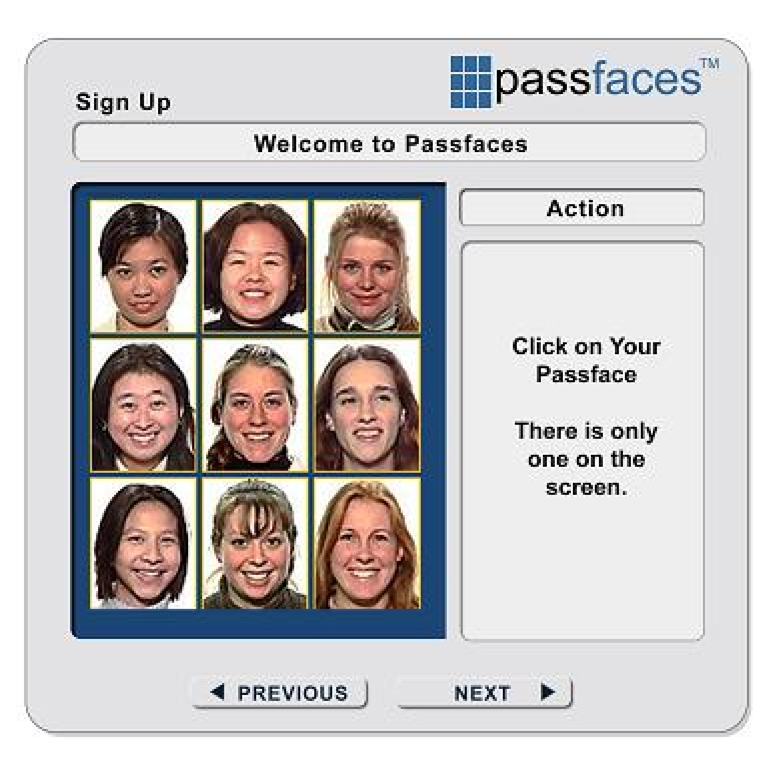
Plaats de blauwe vorm op het gevraagde letterteken en klik om uw keuze te bevestigen

https://secure.dexiapluspro.lu/pro/logon_flash.asp?lang=nl&clifpversion=9&clifpok=true

PassFaces

- Graphical authentication
- JavaScript, ActiveX, Java
- Completely mobile
- User selects a face from each page
- Custom image databases available
- Prevents keylogger attacks

PassFaces 2



Sign Up

Welcome to Passfaces

Action

Click on Your Passface

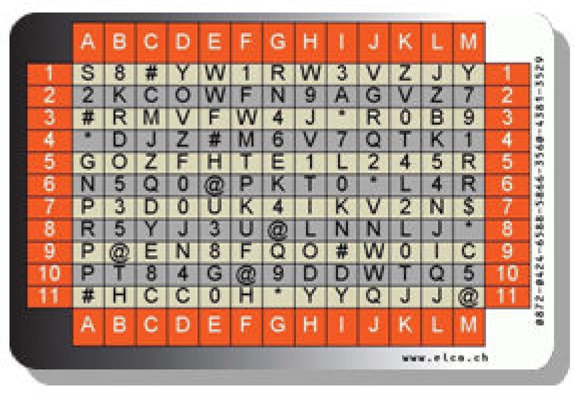
There is only one on the screen.

Passfaces are picked from sets of 9 faces. You determine the number of sets.

http://www.realuser.com/enterprise/demo/try_passfaces.htm

One Time Password manual

- Elcard
- Different layouts
- Different form factors
- A Scratch card adds a little more security



	A	B	C	D	E	F	G	H	I	J	K	L	M	
1	S	8	#	Y	W	1	R	W	3	V	Z	J	Y	1
2	2	K	C	O	W	F	N	9	A	G	V	Z	7	2
3	#	R	M	V	F	W	4	J	*	R	0	B	9	3
4	*	D	J	Z	#	M	6	V	7	Q	T	K	1	4
5	G	O	Z	F	H	T	E	1	L	2	4	5	R	5
6	N	5	Q	0	@	P	K	T	0	*	L	4	R	6
7	P	3	D	0	U	K	4	I	K	V	2	N	$	7
8	R	5	Y	J	3	U	@	L	N	N	L	J	*	8
9	P	@	E	N	8	F	Q	O	#	W	0	I	C	9
10	P	T	8	4	G	@	9	D	D	W	T	Q	5	10
11	#	H	C	C	0	H	*	Y	Y	Q	J	J	@	11
	A	B	C	D	E	F	G	H	I	J	K	L	M	

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

Bookmark authentication

- Use a Bookmark as a “virtual token”
- Token is not send over the network
- JavaScript to read the token
- No Cookies are used

https://site.com/login#[TOKEN]

Examples are:

- BeamAuth
- PhishCops

Characteristics

- Additional hardware
- Additional software
- Complexity
- Scalability
- Portability
- Login time
- System requirements
- Acquisition costs
- Deployment costs
- Operating costs

Comparison Matrix Characteristics

The Comparison Matrix shows the authentication methods and their characteristics, based on a scale from 1 to 5, where higher is better.

- Investigate the available options
- Assign values to the authentication methods

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

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

Attack vectors

- Shoulder surfing
- Keylogger
- Screen capturing
- Brute force (exhaustive search)
- Guess attack (knowing someone)
- Dictionary attack
- Hardware (observation) attack
- Social engineering
- Phishing attack
- Man In The Middle (MITM) attack
- Man In The Browser (MITB) attack
- Network sniffing
- Short access

Attack vectors explained

Guess attack

- Useful for “secret questions” (password forgotten).
- Name of your first pet? / Mothers first name?

- Search information through sites like: Hyves and MySpace.

Hardware (observation) attack

- Vary from copy a TAN code list to an electron microscope.

Attack vectors explained 2

Man In The Browser attack

- Installed by a Trojan Horse
- Similar to MITM
- Works inside the web browser
- No hyperlink to click on
- Activates by typing an URL
- Hard to prevent and disinfect

Attack vectors explained 3

Short access

- Is it possible to do a successful login when an attacker has short physical access to the computer / hardware?

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

Authentication method:	Attack vectors:													
	Shoulder surfing	Keylogger	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	Total score:
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])

Scenario

An online banking site wants to offer customers safe login, even from an internet-cafe abroad. The solution must be highly resistant against:

- Shoulder surfing
- Keyloggers
- Screen capturing

At least 3 or higher is required for these items (higher is preferred)

Scenario 2

Usable in an internet café abroad

This points out 3 important characteristics:

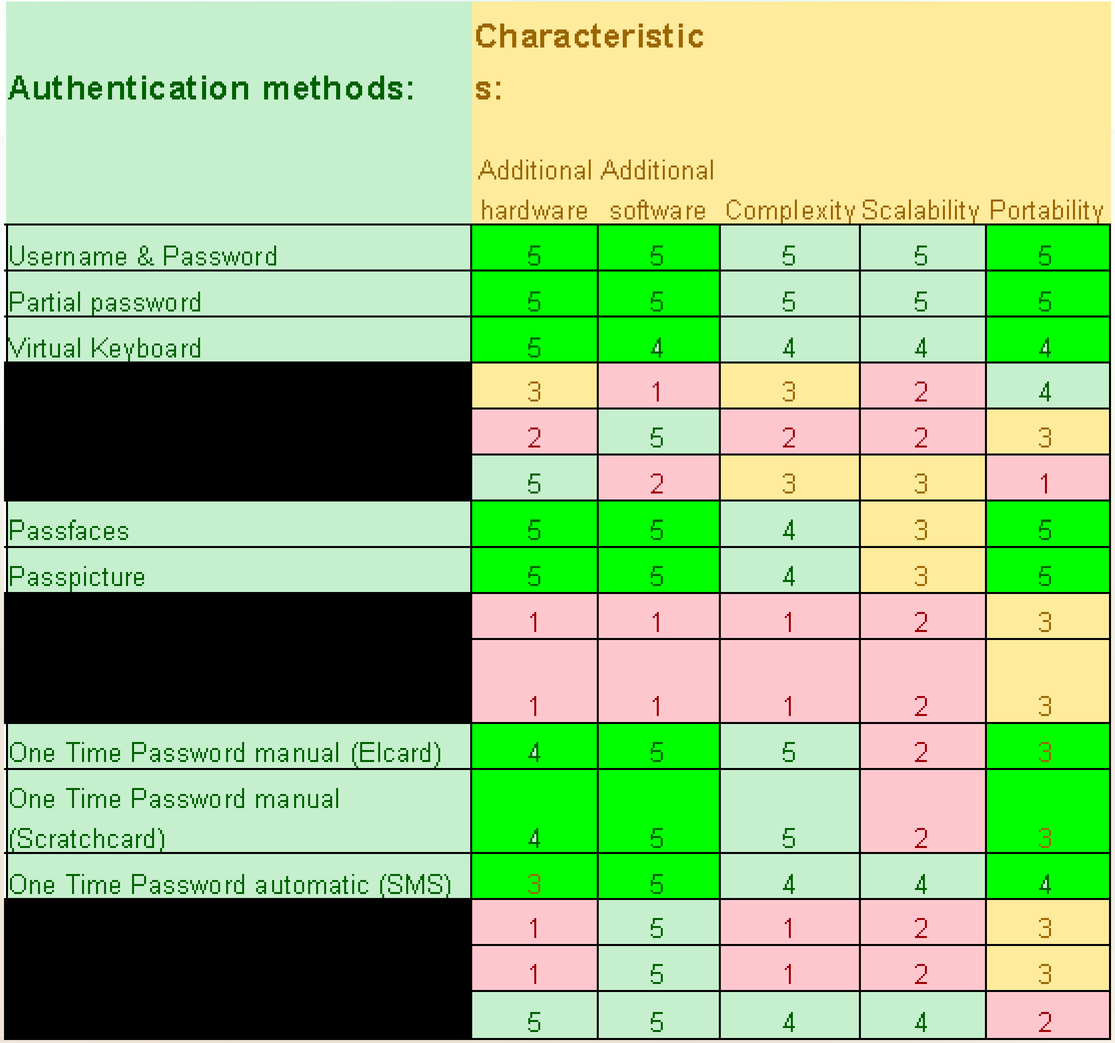
- Additional software
- Additional hardware
- Portability

Scenario 3

When we apply the requirements on the Comparison Matrix Characteristics, this results in the following authentication methods:

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

Shown from the Comp. Matrix



Authentication methods:	Characteristics:				
	Additional hardware	Additional software	Complexity	Scalability	Portability
Username & Password	5	5	5	5	5
Partial password	5	5	5	5	5
Virtual Keyboard	5	4	4	4	4
[redacted]	3	1	3	2	4
[redacted]	2	5	2	2	3
[redacted]	5	2	3	3	1
Passfaces	5	5	4	3	5
Passpicture	5	5	4	3	5
[redacted]	1	1	1	2	3
[redacted]	1	1	1	2	3
One Time Password manual (Elcard)	4	5	5	2	3
One Time Password manual (Scratchcard)	4	5	5	2	3
One Time Password automatic (SMS)	3	5	4	4	4
[redacted]	1	5	1	2	3
[redacted]	1	5	1	2	3
[redacted]	5	5	4	4	2

Scenario 4

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

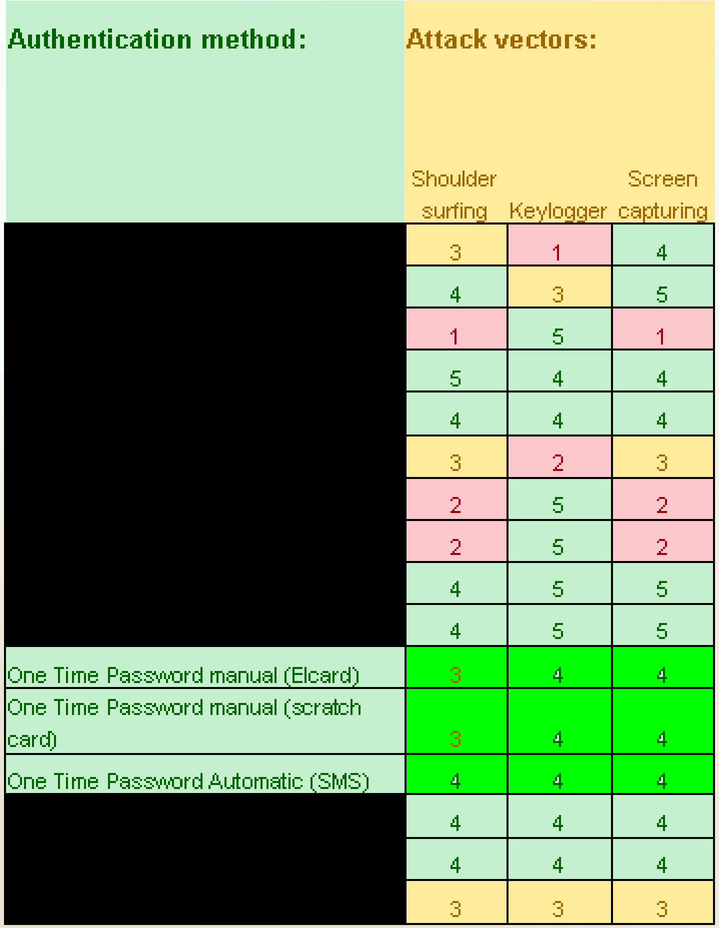
- Shoulder surfing
- Keyloggers
- Screen capturing

Scenario 5

We now apply the selected attacks on the Comparison Matrix Attack vector. Here we select (from the remaining) authentication methods with a 3 or higher, this results in the following authentication methods:

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

Shown from the Comp. Matrix



Authentication method:	**Attack vectors:**		
	Shoulder surfing	Keylogger	Screen capturing
[redacted]	3	1	4
[redacted]	4	3	5
[redacted]	1	5	1
[redacted]	5	4	4
[redacted]	4	4	4
[redacted]	3	2	3
[redacted]	2	5	2
[redacted]	2	5	2
[redacted]	4	5	5
[redacted]	4	5	5
One Time Password manual (Elcard)	3	4	4
One Time Password manual (scratch card)	3	4	4
One Time Password Automatic (SMS)	4	4	4
[redacted]	4	4	4
[redacted]	4	4	4
[redacted]	3	3	3

Questions

?