



Faculty of Science



IT-security: User Authentication
 Access control
 Identity and Access Management
 Passwords and SSO
 Biometrics
 Social engineering

Carsten Jørgensen
Department of Computer Science

DIKU 13. september 2021



IAM - ACL

An access control list (ACL) is a list of permissions attached to an object.

An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects

Alice: read,write; Bob: read



IAM

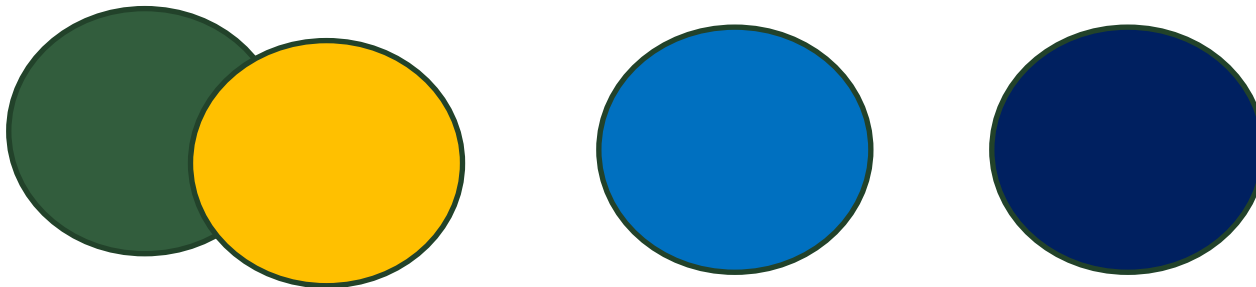
Role Based Access Control (RBAC)

Peter is a current employee, Peter is Administrator

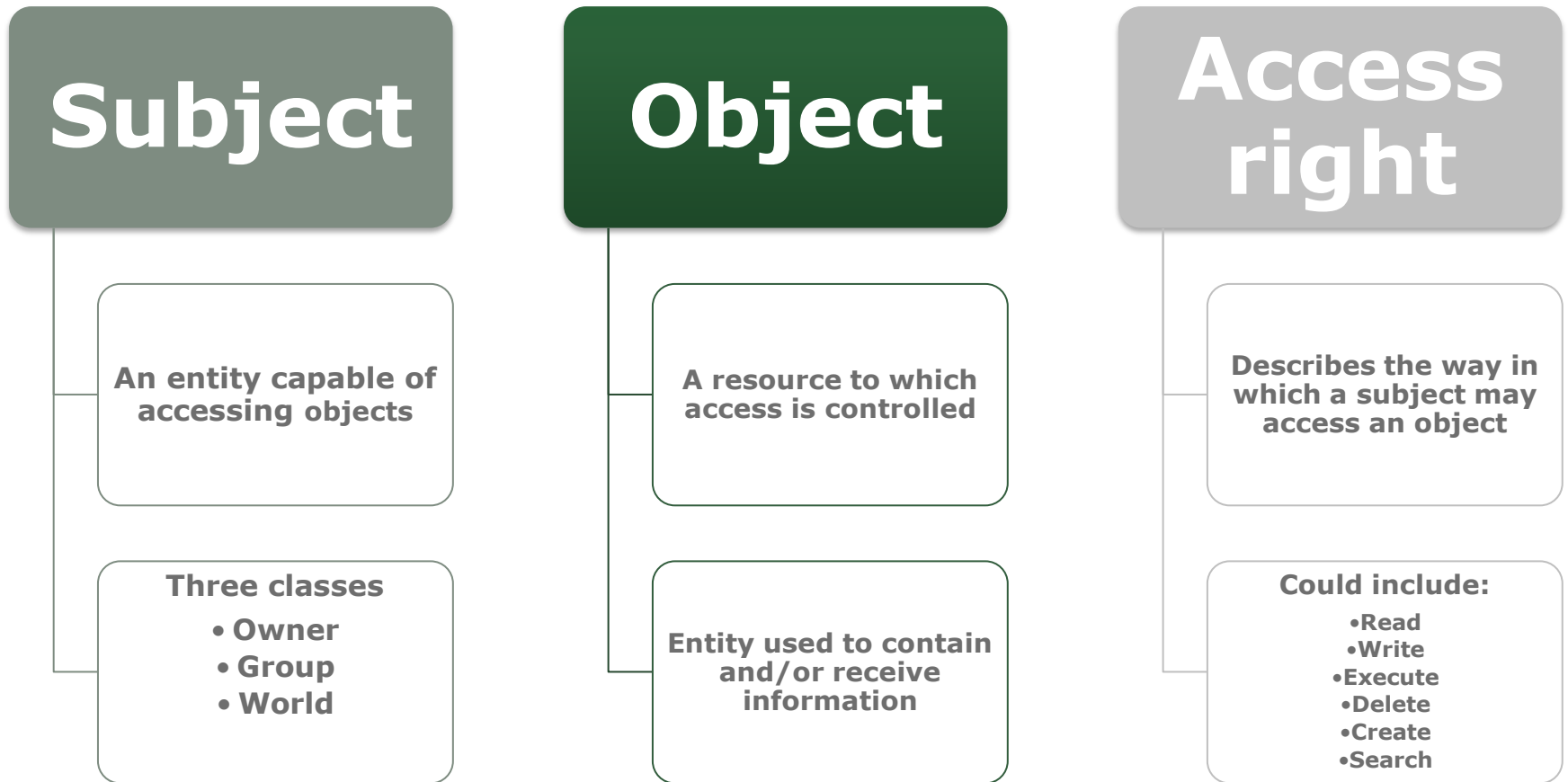
Mia is an employee, Mia has access to SAP

Susan is no longer employee, Susan has Guest-access

Jens has resigned, he was Administrator, does he still have access?



Subjects, Objects, and Access Rights



Access Control Policies

Discretionary access control (DAC)

- Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do

Mandatory access control (MAC)

- Controls access based on comparing security labels with security clearances

Role-based access control (RBAC)

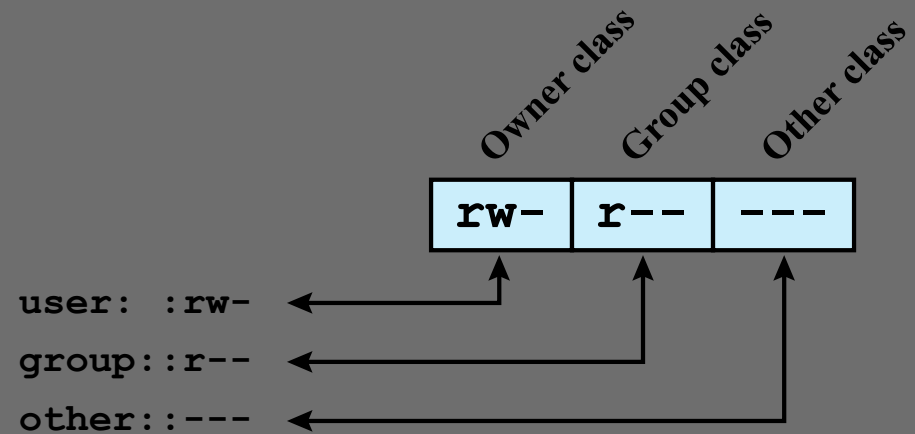
- Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

Attribute-based access control (ABAC)

- Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

UNIX - File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
 - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



(a) Traditional UNIX approach (minimal access control list)

Figure 4.5 UNIX File Access Control

Traditional UNIX - File Access Control

- "Set user ID"(SetUID)
- "Set group ID"(SetGID)
 - System temporarily uses rights of the file owner/group in addition to the real user's rights when making access control decisions
 - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
 - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
 - Is exempt from usual access control restrictions
 - Has system-wide access
- AWS Roles



IAM

An administrative process coupled with a technological solution which validates the identity of individuals and allows owners of data, applications, and systems to either maintain centrally or distribute responsibility for granting access to their respective resources to anyone participating within the IAM framework.

IAM refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources



IAM – Identity Life Cycle Management

Identity, Authentication and Authorization

Principle of Least Access

Groups and Roles

Administration

Auditing, Logging and Reporting

Segregation of Duties/Funktionsadskillelse



IAM

Identity: Who are you (you or a computer):
UserIDs, Certificates, cards...

Authentication: Prove your identity: challenge-response: Passwords, Private keys, PINs...
Your possession of the secret proves you are who you claim to be.

Authorization: the system controls which resources you're allowed to access. Typically through the use of a token or ticket mechanism. Allows you to access only that which the administrators have determined is necessary, thus enforcing the *principle of least privilege*.



IAM

Password

Password is used by another user

	Provided by	Answers	Attributes	Uniqueness
Identity	principal	"Who are you?"	public assertion	yes, locally
Authentication	principal	"OK, how can you prove it?"	secret response	no
Authorization	system	"What can I do?"	token or ticket	(n/a)
			access control	

Netflix, Google, Facebook...

NemID – identities and auth?



Identity, authentication, authorization

Log på Netbank

NEM ID

Basisbank A/S

Bruger-id

?

Adgangskode

?

[Glemt adgangskode?](#)

Næste

Log på uden nøglekort

Log på Portalbank

NEM ID

Hals Sparekasse

Bruger-id

?

Adgangskode

?

[Glemt adgangskode?](#)

Log på

Log på med nøglekort

Service Provider provides access to services
based on their own risk assessment



IAM - Case

Du arbejder på et internt projekt til udvikling af nyt økonomisystem til din virksomhed.

Projektlederne fortæller, at for at overholde tidsplanen skal der ikke bruges bruger-id'er. Systemet skal i stedet have et stærkt hardcodet password (17 tegn incl. specialtegn)
Alle der skal have adgang til økonomisystemet vil få oplyst koden hvis de har brug for adgangen.

Hvad siger du til projektlederen?



IAM - Case

Du arbejder på et internt projekt til udvikling af nyt økonomisystem til din virksomhed.

Projektlederne fortæller, at for at overholde tidsplanen skal der **ikke bruges bruger-id'er**. Systemet skal i stedet have et stærkt **hardcodet password (17 tegn incl. specialtegn)**

Alle der skal have adgang til økonomisystemet vil få oplyst koden hvis de har brug for adgangen.

Hvad siger du til projektlederen?



IAM – Case

Identity, Authentication and Authorization

Principle of Least Access

Groups and Roles

Administration

Auditing, Logging and Reporting

Segregation of Duties/Funktionsadskillelse



IAM – Case

Identity, Authentication and Authorization

Principle of Least Access

Groups and Roles

Administration

Auditing, Logging and Reporting

Segregation of Duties/Funktionsadskillelse



IAM – Case

Identity, Authentication and Authorization

Principle of Least Access

Groups and Roles

Administration

Auditing, Logging and Reporting

Segregation of Duties/Funktionsadskillelse



Tre faktorer+ til autentificering

Noget man **ved**, noget man **har** og
noget man **ér**

Noget man **har glemt**, noget man
har tabt og noget man **har**
været

Noget man **gør**, **hvor** man er



Hvad er et godt password?



Hvad er et godt password?

Brugernes passwords er altid dårlige

Opfylder kun lige akkurat de tekniske krav der stilles

Dvs. password regler styrker passwords, men kun op til den tekniske grænse løsningen tvinger brugerne til

Med mindre vi bliver tvunget - eller undervist - i andet, så vælger vi alle password efter dette mønster:



Hvad er et godt password?

1. Ingen koder

Hvis man giver en bruger frit valg vil alle brugere selvfølgelig, alt andet lige, vælge at ikke bruge passwords, fordi det er det mest brugervenlige (dvs. letteste)

2. Almindelige ord

Hvis systemet tvinger til at bruge et kodeord, er første problem hvordan man selv husker sin kode.

Så man vælger i første omgang sin kode ud fra, om man tror man kan huske den, ikke fordi man tænker på "sikkerhed"

– brugerens risikovurdering



Mental models – “noget man tit tænker på”



You Retweeted



Gene Spafford @TheRealSpaf · 22 Sep 2014

“@shariv67: Had I known I was going to need this many passwords, I would have had a lot more pets.”



19



17



You Retweeted



George Takei @GeorgeTakei · 23 Jul 2014

Every time I change my password, I have to get a new pet.



615



1K



Hvad er et godt password?



I changed all my passwords to 'incorrect'. So my computer just tells me when I forget.



Hvad er et godt password?

Systems:

But we use the same systems – otherwise we cannot remember the passwords:

- If both upper-case and lower-case letters are required people only use one upper-case letter – and it is always first:
The password becomes "PAssword", not "pAssword"
- If numbers are also required, they are always last: "Password12"
- Non-alfabetic are the very last part, if they are required.
So the "super-strong" password would be "Password12!"
- On smartphones we make patterns, such as "1234", "1122", "1111" or years/dates such as "1945", the PIN should be at least 8 characters – and consider biometrics



Two passwords

Password123dec

hY6%%#2873GH/GtAQ?08-dPe2>S

- Guessing the first PW means all future PWs can be guessed
- The user can remember the first password - no.2 will be written down somewhere because of password change rules
- Nr.2 is impossible to break, no.2 is not
- Which password is best now?
- Which password is best next month?



Hvad er et godt password?

"The password must be impossible to remember
and nowhere written down"

Peter Gutmann



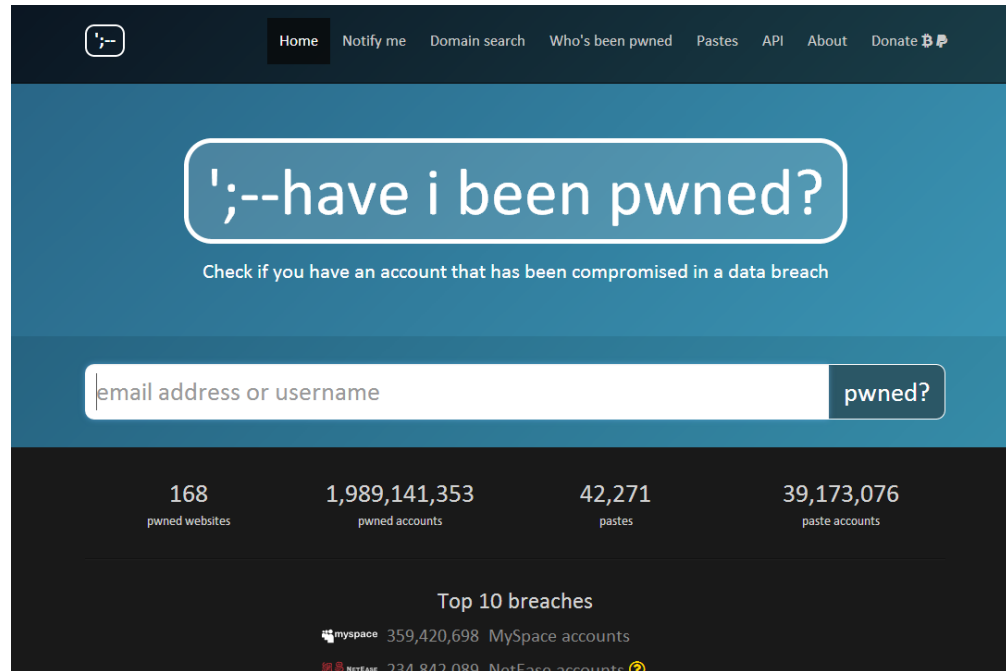
Må man skrive sine passwords ned?

https://www.youtube.com/watch?v=Srh_TV_J144



Password reuse

Model2: samme password på mange sites
Er det et problem?



The screenshot shows the homepage of the 'have i been pwned' website. The header is dark blue with a navigation bar containing links: Home, Notify me, Domain search, Who's been pwned, Pastes, API, About, and Donate. The main content area has a large blue box with the text '';--have i been pwned?' and a subtext 'Check if you have an account that has been compromised in a data breach'. Below this is a search bar with the placeholder 'email address or username' and a 'pwned?' button. The footer is dark blue and displays statistics: 168 pwned websites, 1,989,141,353 pwned accounts, 42,271 pastes, and 39,173,076 paste accounts. It also lists 'Top 10 breaches' with 'myspace' and 'NetEase' as examples.

Category	Count
pwned websites	168
pwned accounts	1,989,141,353
pastes	42,271
paste accounts	39,173,076

Top 10 breaches

- myspace 359,420,698 MySpace accounts
- NetEase 234,842,089 NetEase accounts

Password reuse:
<https://haveibeenpwned.com>



Hvor langt skal et password være?
Hvad med special tegn?

<http://howsecureismypassword.net>



HOW PASSWORD
LENGTH WINS
THE INTERNET

Passwords 102



Hvad er et godt password?

Password huskere

Overvej password managers som [1password](#), [Roboform](#), og [Password Safe](#).

Kan beskytte koderne og kan give adgang til de gemte koder med et "super-password".

Autogenere stærke koder. Genbruger aldrig vigtige passwords på forskellige sider.

Selv stærke passwords kan mistes på sites med sikkerhedsproblemer.



Password managers

Undgår password genbrug
Stærke passwords over det hele

Problemer?

Password manager salt



Angreb imod brugerens passwords

1. Hvad er dit password? (spørge)
2. Gætte / default passwords
3. Dictionary Attack
4. Brute Force (f.eks. imod LanMan hash)
5. Rainbow Tables



Password cracking

Hashcat: <https://hashcat.net>



hashcat
advanced
password
recovery

hashcat

Forum

Wiki

Tools

Events

Converter

Contact

```
HwMon.Dev.#2.....: Temp: 55c Fan: 30% Core:1010Mhz Mem:1250Mhz Lanes:16
HwMon.Dev.#3.....: N/A

Started: Wed Nov 30 10:48:18 2016
Stopped: Wed Nov 30 10:48:43 2016
```

Algorithms

- MD4
- MD5
- Half MD5 (left, mid, right)
- SHA1
- SHA-256
- SHA-384
- SHA-512
- SHA-3 (Keccak)
- SipHash
- RipeMD160
- Whirlpool
- DES (PT = \$salt, key = \$pass)
- 3DES (PT = \$salt, key = \$pass)
- GOST R 34.11-94
- GOST R 34.11-2012 (Streebog) 256-bit
- GOST R 34.11-2012 (Streebog) 512-bit
- Double MD5
- Double SHA1
- md5(\$pass.\$salt)
- md5(\$salt.\$pass)
- md5(unicode(\$pass).\$salt)
- md5(\$salt.unicode(\$pass))
- md5(sha1(\$pass))
- md5(\$salt.md5(\$pass))
- md5(\$salt.\$pass.\$salt)
- md5(strtoupper(md5(\$pass)))
- sha1(\$pass.\$salt)
- sha1(\$salt.\$pass)
- sha1(unicode(\$pass).\$salt)
- sha1(\$salt.unicode(\$pass))
- sha1(md5(\$pass))
- sha1(\$salt.\$pass.\$salt)
- sha1(CX)



Password cracking

2009: “most people aren't going to have access to these sorts of clusters”

2014: AWS G3 1,536-core GPU: \$0.26/time



The screenshot shows the top portion of an Ars Technica web page. The header features the 'ars technica' logo in white on a dark background. Below the logo is a navigation bar with links for 'MAIN MENU', 'MY STORIES: 13', 'FORUMS', 'SUBSCRIBE', and 'JOBS'. The main content area has a section header 'RISK ASSESSMENT / SECURITY & HACKTIVISM' in large, bold, blue letters. Below this is the article title '768-bit RSA cracked, 1024-bit safe (for now)' in a large, bold, black font. The subtitle reads 'Researchers have posted a preprint that describes their method for factoring a ...'. The byline states 'by John Timmer - Jan 8 2010, 12:20am +0100'. A comment count of '39' is visible in a small box. The first paragraph of the article begins with 'With the increasing computing power available to even casual users, the security-conscious have had to move on to increasingly robust encryption, lest they find their information vulnerable to brute-force attacks. The latest milestone to fall is 768-bit RSA; in a paper posted on a cryptography preprint server, academic researchers have now announced that they factored one of these keys in early December.'

ars technica

MAIN MENU MY STORIES: 13 FORUMS SUBSCRIBE JOBS

RISK ASSESSMENT / SECURITY & HACKTIVISM

768-bit RSA cracked, 1024-bit safe (for now)

Researchers have posted a preprint that describes their method for factoring a ...

by John Timmer - Jan 8 2010, 12:20am +0100

39

With the increasing computing power available to even casual users, the security-conscious have had to move on to increasingly robust encryption, lest they find their information vulnerable to brute-force attacks. The latest milestone to fall is 768-bit RSA; in a paper posted on a cryptography preprint server, academic researchers have now announced that they factored one of these keys in early December.



Baggrund

Passwords er den nye firewall
– risikovurdering

Tokens, smart cards,
biometrics

Password hash,
hash og salt,
scrypt/bcrypt



Baggrund

Password hash
hash og salt,
bcrypt/bcrypt

Password Reminder

There was a recent password request from our website.

Here is your login information for your account.
Login Email: **bigbob@mailinator.com**
Login Password: **123456**


Check the "manage account" page to change your password.


[login instantly](#)


[or click here to change your password](#)

No account yet? [Sign up](#)

! We have reinforced your password security. If you can't log in, we invite you to enter your password in lowercase only. If you still can't log in, [choose a new password](#).



 Nickname

 Password

☒ **Keep my session active**

Leave this box unchecked on a public or shared computer.

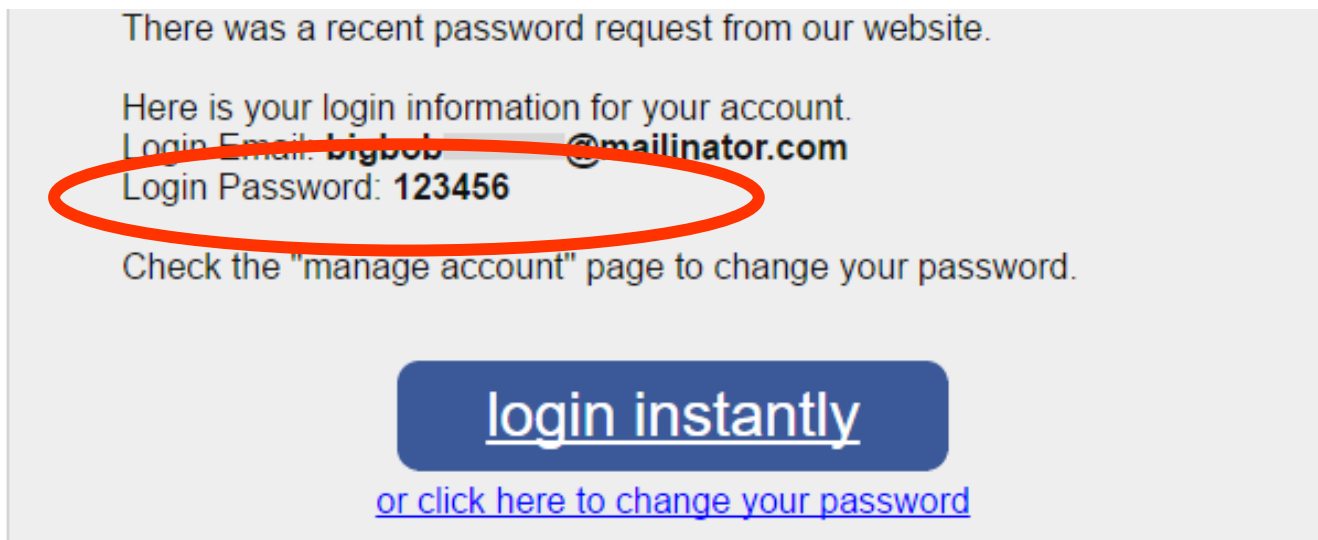
[Login](#)

[Forgot your password?](#)

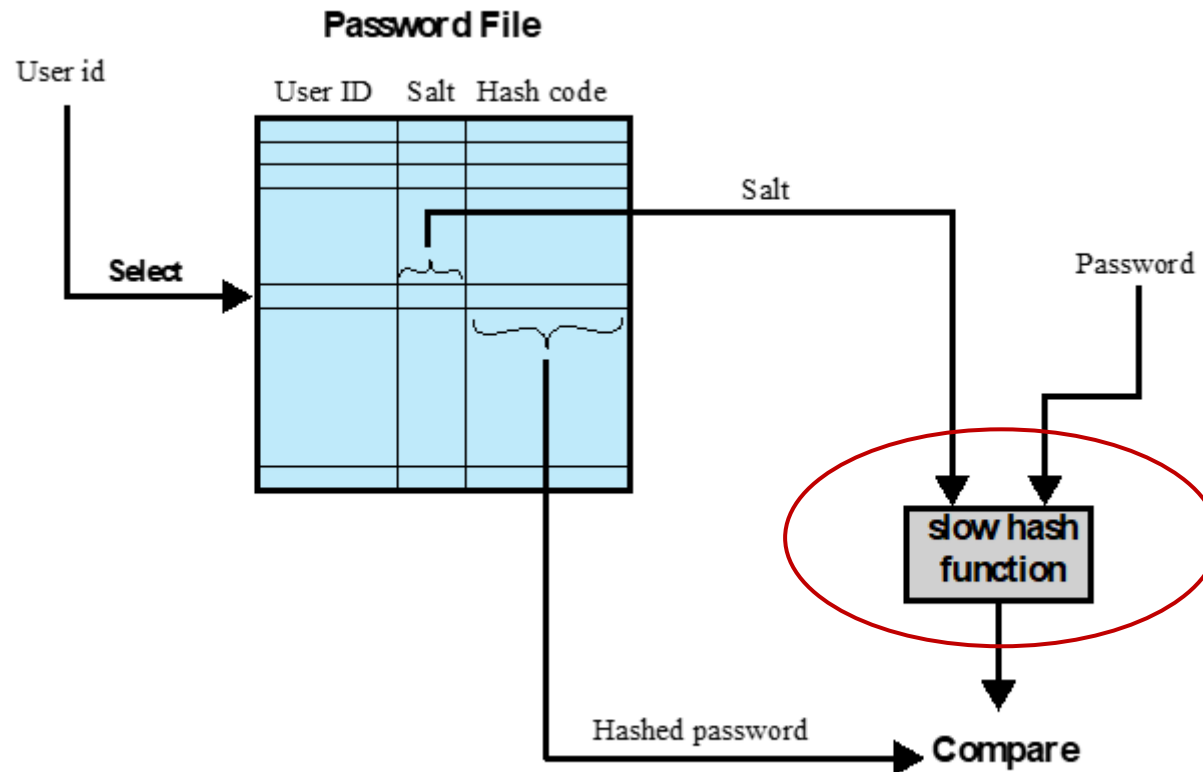
Baggrund

Password hash, hash og salt, scrypt/bcrypt

Don't store the password, store a hash of the password



Salt



(b) Verifying a password

Password hash?

Direkte off-line adgang til password hash
eller

Online - forbinde til serveren hver gang?

- Begrænsninger på antallet af forsøg?
- Time-delay mellem sign-in attempts, brug af penalty period (f.eks. 1 time) hvis forkert password er indtastet for mange gange
 - f.eks. 10 gange



Password hash?

The password "**alpine fun**" can be brute-forced in only 2 months if the server can be attacked 100 times per second. But, with a penalty period and 5 second delay, the same password can suddenly sustain an attack for 1,889 years.

No of attacks	Password	Time	Security level
100 times per sec	alpine fun	2 months	Low risk
1 time every 5 sec	alpine fun	63 years	Secure
1 time every 5 sec with a 1 hour penalty period after 10 attempts	alpine fun	1,889 years	Secure forever

Se f.eks. "The Usability of Passwords"

<http://www.baekdal.com/tips/password-security-usability> og

"The Usability of Passwords FAQ":

<http://www.baekdal.com/tips/the-usability-of-passwords-faq>



Apple

Apple default: 80ms per password attempt delay
Enforced by tamper resistant hardware

Exponential growth:

# characters	[0-9]	[0-9a-z]	[0-9a-zA-Z]
1	0.8 seconds	2.9 seconds	5 seconds
2	8 seconds	1.7 minutes	5.1 minutes
3	1.3 minutes	1 hour	5.3 hours
4	13 minutes	1.6 days	2 weeks
5	2.2 hours	8 weeks	2.3 years
6	22 hours	5.5 years	140 years
7	1.3 weeks	200 years	9 thousand years
8	13 weeks	7 thousand years	550 thousand years
9	2.5 years	260 thousand years	34 million years
10	25 years	9 million years	2 billion years

Pause



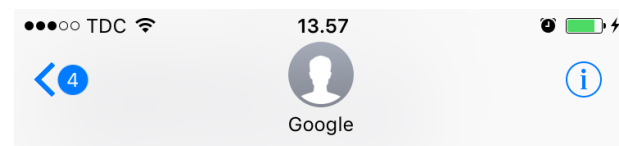
Two Factor Authentication (2FA)



Se f.eks.:

<https://www.yubico.com>

<https://duo.com>



Mon, 8 Feb, 12.00

G-743835 er din bekræftelseskode til Google.

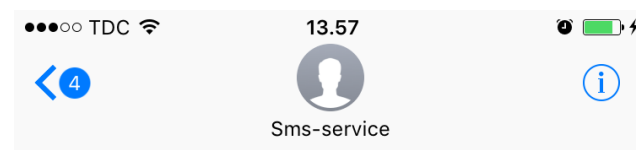
Tue, 9 Feb, 08.47

G-493534 er din bekræftelseskode til Google.

Wed, 10 Feb, 08.22

G-840743 er din bekræftelseskode til Google.

Mon, 20 Jun, 12.15



Text Message
Sat, 26 Nov, 07.36

Din personlige engangskode er: 1527

Bemærk! Engangskoden udløber om 12 timer.

Two Factor Authentication (2FA) – nogle termer

Push notification

Verify identity by approving a push notification, for instance in an app

Phone callback

Require you to pick-up a phone call and for instance press a specific key, or any key, before you are provided access

Challenge-response

Requires you to enter data back to the system to verify a transaction is correct

Token

A hardware device, after pushing a button to generate a code, the code is then typed into the password prompt



Two Factor Authentication (2FA) – nogle termer

SMS passcode

A code is sent to your phone via SMS and must be typed into the two-factor prompt

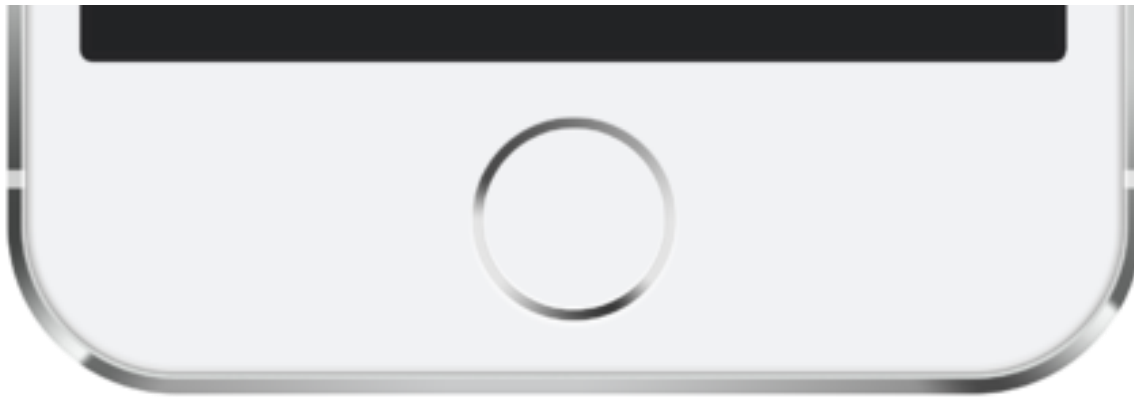
One-Time Password/One-Time Pad (OTP)

Can only be used one time



Hvad er et godt password?

Biometri?



Hvad er et godt password?

Hvor tit skal password skiftes?

Ikke kritisk – afhængig af hvor man indtaster passwords

Krav om skift f.eks. hver 90 dage kan være et problem fordi folk så typisk vælger svage passwords.

=> "Password06" eller "PasswordJuni"



Hvad er et godt password?

Overvej det hvis det er muligt at bruge 2-faktor authentication på en site

Næsten altid en forbedring af sikkerheden

- Support er dyrt

Pas på "secret questions"

Backup systemet for glemte passwords må ikke være svagere end dit password.



Meget lavere sikkerhed

Pick a secure password:

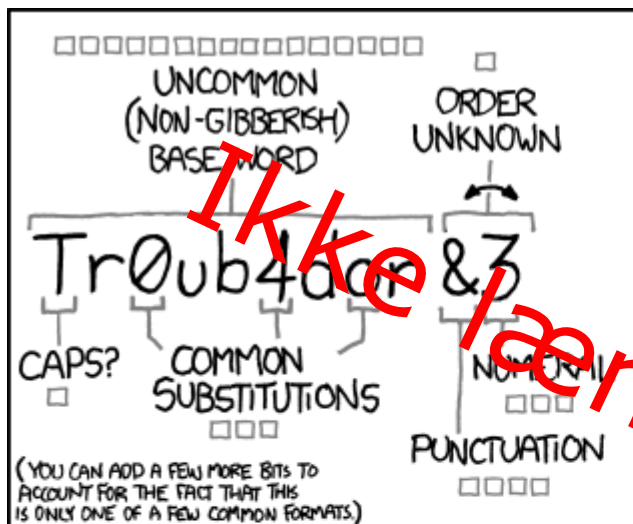
"0k5ijU)=2w8VAiqxozKyB"

**Now, in case you forget it, what's
your favorite color?**

"Blue"



Hvad er et godt password? (længde > kompleksitet)



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

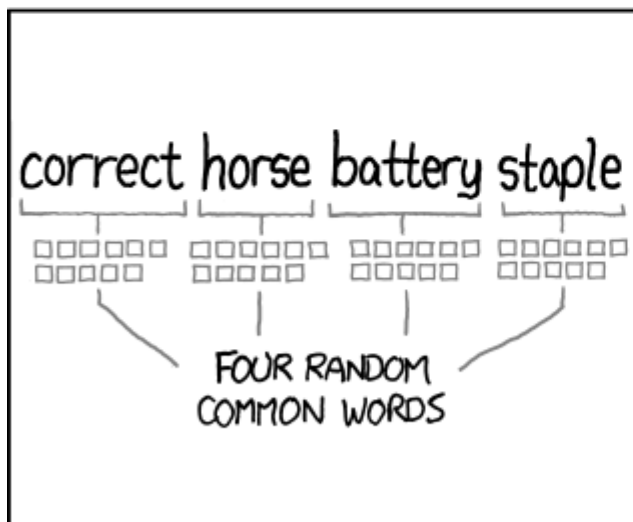
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Default passwords

**Eksempel på dårlige passwords:
Amerikanske Dankort maskiner**



Amerikanske ATM/Dankortmaskiner hacket med default password

ATM hacket, tror indeholder 5\$ sedler i stedet for \$20 => udbetaler 3x for meget

Pre Paid Card

9 dage før kunder rapporterede



Amerikanske ATM/Dankortmaskiner hacket med default password

http://www.youtube.com/watch?v=cmW_4R81jVU

CNN Report: Robber Tricks ATM machine



CNN Report: Robber Tricks ATM machine



Amerikanske ATM/Dankortmaskiner hacket med default password

Minibank 1510 - Mozilla Firefox

Filer Rediger Vis Gå til Bogmærker Funktioner Hjælp

http://www.phoenixcardnet.com/1510.htm

Computer Forensics.DK

Home Up

Merchants
Distributors
Employees
Products
Services
[ATM balancing](#)
Disputes



VISA
MasterCard
STAR
Citizens Bank
Not your typical bank®

PHOENIX CARDNET
Tel: (888) 972-4286

- 5.7" LCD with 320 x 240 resolution
- 8 menu screens
- 7 screen advertising capability (Mono or Color)
- Encrypted Pin Pad (EPP)
- Triple DES compliant
- Removable money box




- Dip-type card reader
- Lock options:
 - Manual dial lock
 - Electronic lock
 - Cencon 2000 lock



Encrypted Pin Pad (EPP)
Triple DES compliant



Amerikanske ATM/Dankortmaskiner hacket med default password

Welcome to Tranax Technologies, Inc. - Mozilla Firefox

Filer Rediger Vis Gå til Bogmærker Funktioner Hjælp

http://www.tranax.com/

Computer Forensics.DK


home Products Industry Channel Partners Service & Support Corporate info

login contact

TRANAX TECHNOLOGIES RECOGNIZED WITH PRESTIGIOUS GROWTH STRATEGY LEADERSHIP AWARD

2006 FROST & SULLIVAN Growth Strategy Leadership Award

More Info




Card Dispensing Self-Service Terminal


Instant Issue Cards a Reality


- ◆ Instant Issue Stored-Value Cards
- ◆ Automate Stored-Value Card Dispensing
- ◆ Increase Revenues


details >>

news:

 **Partnership Delivers Self-Service & Financial Services to Presto Convenience Stores**
TIO & Tranax Partner to Deliver Self-Service Bill Payment and Financial Services to Presto Convenience Stores.

 **Strong Demand in Credit Union Market for Tranax 'Essential Banking' ATMs**
Tranax announced strong demand for its Mini-Bank family of "Essential Banking" ATMs for credit unions and smaller banks.

 **Tranax wants to be first to ride wave of change**
For Dr. Hansup Kwon, change is a good thing. It had better be, for the mild-mannered leader of Tranax Technologies Inc. is banking his company's future on it.

 **Tranax Technologies recognized by Frost & Sullivan**
Tranax, chosen for exceptional growth in the highly competitive North American ATM Marketplace, was

Færdig

Adblock



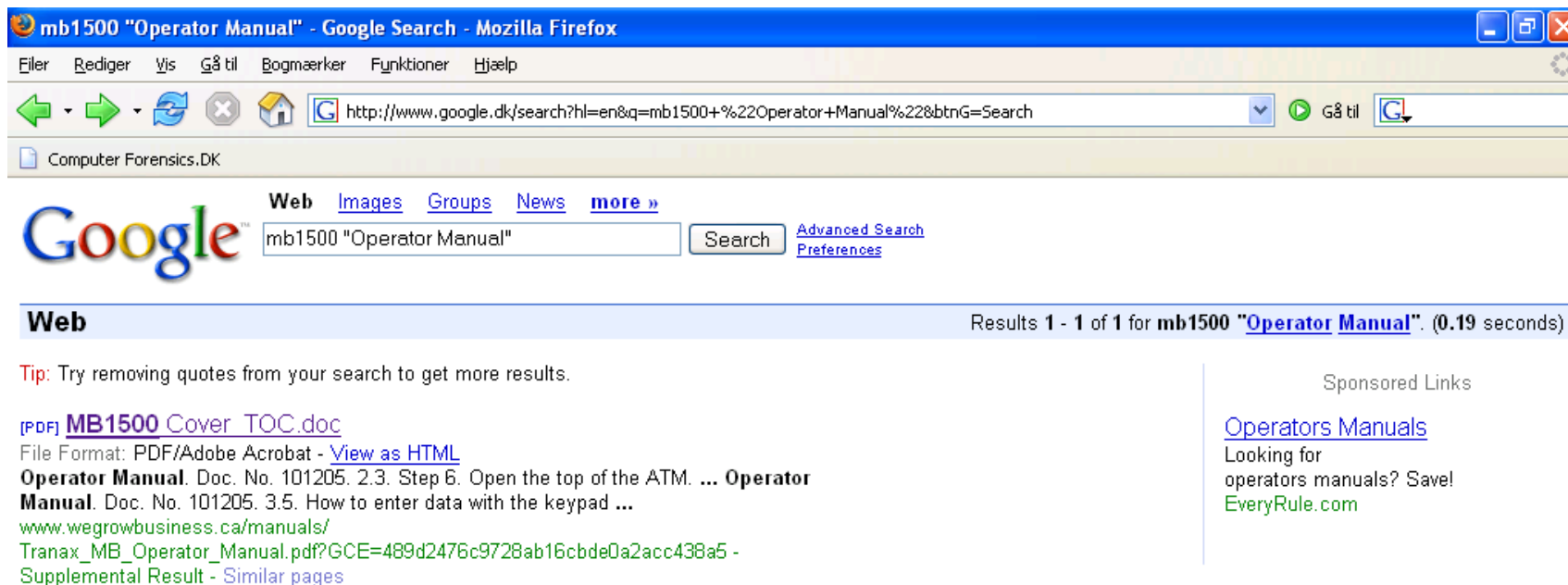
Amerikanske ATM/Dankortmaskiner hacket med default password

Knowledgebase:

The ATM is programmed with the passwords that the distributor requests when the order is placed to program a new ATM. *When special passwords are not requested they are left at the factory default (see your mini-bank operators manual)* Every new ATM that is shipped from Tranax has a copy of the print setup included in the “open me first” box or envelope. The master password is hand written at the top of the print setup for the convenience of the installer.



Amerikanske ATM/Dankortmaskiner hacket med default password



mb1500 "Operator Manual" - Google Search - Mozilla Firefox

File Rediger Vis Gå til Bogmærker Funktioner Hjælp

http://www.google.dk/search?hl=en&q=mb1500+%22Operator+Manual%22&btnG=Search

Computer Forensics.DK

Google Web Images Groups News more »

mb1500 "Operator Manual" Search Advanced Search Preferences

Web Results 1 - 1 of 1 for mb1500 "Operator Manual". (0.19 seconds)

Tip: Try removing quotes from your search to get more results.

[PDF] [MB1500 Cover TOC.doc](#)
File Format: PDF/Adobe Acrobat - [View as HTML](#)
Operator Manual. Doc. No. 101205. 2.3. Step 6. Open the top of the ATM. ... **Operator Manual.** Doc. No. 101205. 3.5. How to enter data with the keypad ...
www.wegrowbusiness.ca/manuals/Tranax_MB_Operator_Manual.pdf?GCE=489d2476c9728ab16cbde0a2acc438a5 - Supplemental Result - [Similar pages](#)

Sponsored Links

[Operators Manuals](#)
Looking for operators manuals? Save! [EveryRule.com](#)

Tranax manual inurl:pdf



Amerikanske ATM/Dankortmaskiner hacket med default password

Thranax:

Master = 555555

Service = 222222

Operator = 111111

Triton:

12345

Lipman:

Merchant = 222222

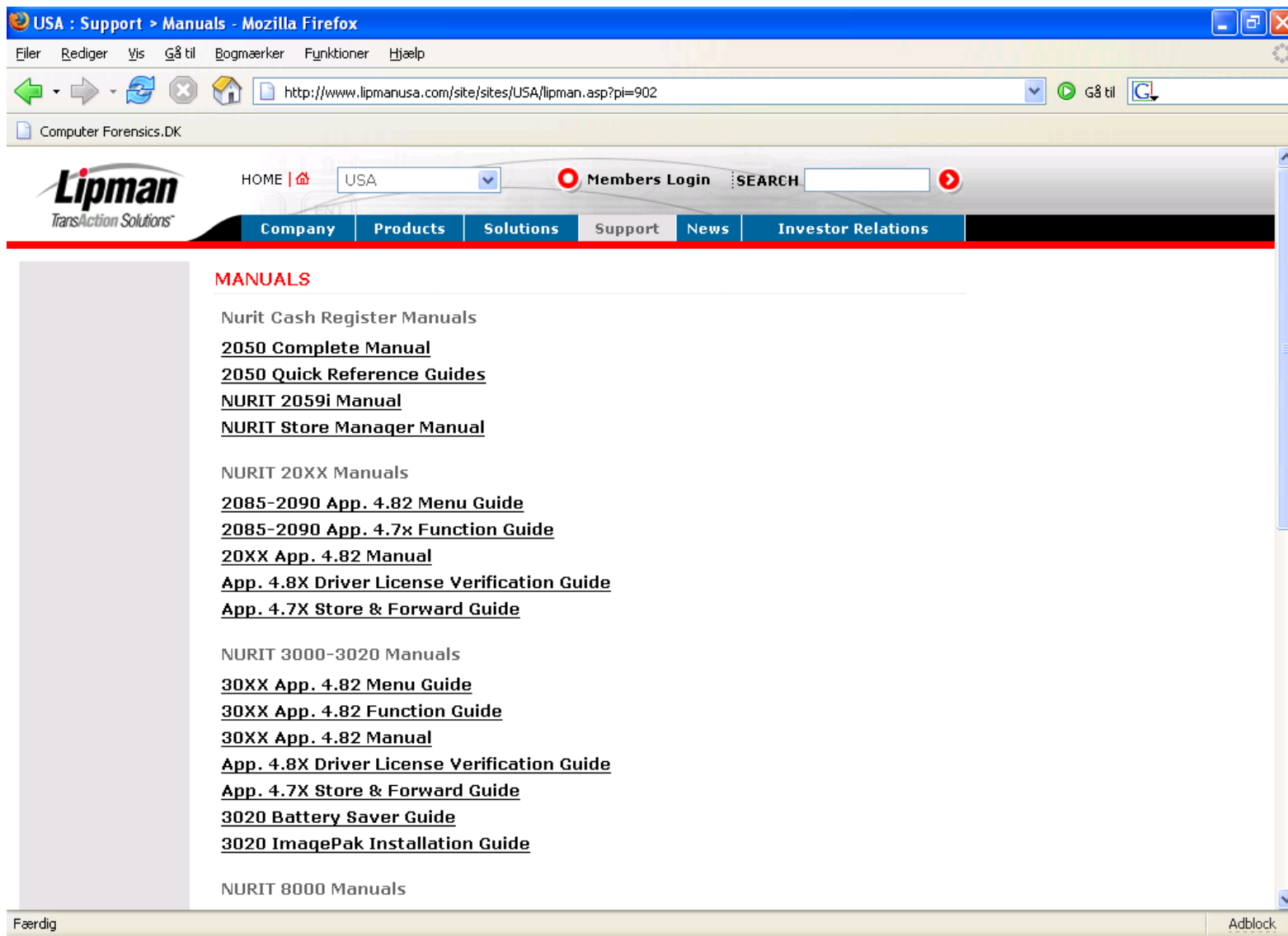
Technician = 111111

GTI:

1234



Amerikanske ATM/Dankortmaskiner hacket med default password



The screenshot shows a Mozilla Firefox browser window displaying the Lipman TransAction Solutions website. The address bar shows the URL <http://www.lipmanusa.com/site/sites/USA/lipman.asp?pi=902>. The website header includes the Lipman logo, navigation links (HOME, USA, Members Login, SEARCH), and a menu bar with links to Company, Products, Solutions, Support, News, and Investor Relations. The main content area is titled "MANUALS" and lists various manuals for different models:

- Nurit Cash Register Manuals
 - [2050 Complete Manual](#)
 - [2050 Quick Reference Guides](#)
 - [NURIT 2059i Manual](#)
 - [NURIT Store Manager Manual](#)
- NURIT 20XX Manuals
 - [2085-2090 App. 4.82 Menu Guide](#)
 - [2085-2090 App. 4.7x Function Guide](#)
 - [20XX App. 4.82 Manual](#)
 - [App. 4.8X Driver License Verification Guide](#)
 - [App. 4.7X Store & Forward Guide](#)
- NURIT 3000-3020 Manuals
 - [30XX App. 4.82 Menu Guide](#)
 - [30XX App. 4.82 Function Guide](#)
 - [30XX App. 4.82 Manual](#)
 - [App. 4.8X Driver License Verification Guide](#)
 - [App. 4.7X Store & Forward Guide](#)
 - [3020 Battery Saver Guide](#)
 - [3020 ImagePak Installation Guide](#)
- NURIT 8000 Manuals

The browser window also shows a status bar at the bottom with "Feerdig" and "Adblock" indicators.



Amerikanske ATM/Dankortmaskiner hacket med default password

Adobe Reader - [1099.pdf]

File Rediger Vis Dokument Værktøjer Vindue Hjælp

Gem en kopi Søg Vælg 118% Søg på nettet Har du behov for at oprette PDF-dokumenter?

Søg efter: Forrige Næste

Accessing the Service Menu

Important!

One of two passwords can be entered. For merchant access please enter the merchant password. For Technician access (including *Money Service*) please enter the Technician password.

The default system passwords are:
 Merchant = 2222222
 Technician = 1111111

Function Description

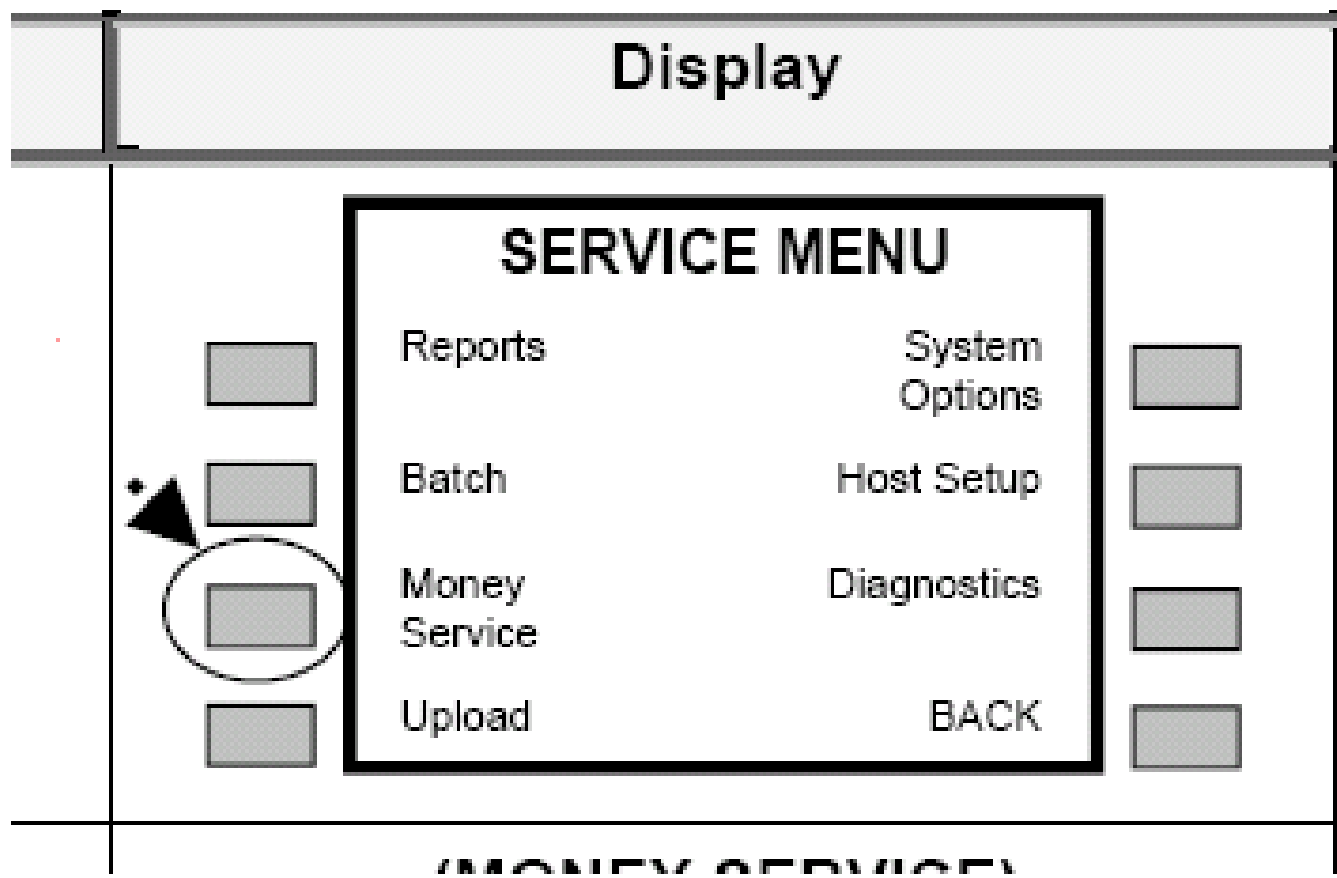
The following Step/Action table will assist you in accessing the Service Menu of the ATM from the idle prompt.

Step	Action	Display
1.	From the Idle Prompt press the following buttons in the following order: [CANCEL], [CLEAR], [ENTER], [1], [2], [3]	ENTER PASSWORD [_ _ _ _ _]
2.	Input the default Password <u>Note:</u> For Merchant Access input the merchant default password. For technician access (Including <i>Money Service</i>) input the technician default password.	ENTER PASSWORD [* * * * *]

10 af 73



Amerikanske ATM/Dankortmaskiner hacket med default password



Amerikanske ATM/Dankortmaskiner hacket med default password

TP-820327-001B * Operating Guide for the Diebold 1075ix Exterior Walk-up Cash Dispenser - Mozilla Firefox

Filer Rediger Vis Gå til Bogmærker Funktioner Hjælp

http://www.diebold.com/ficcdsvdoc/techpubs/ixCustomer/TP-820327-001/TP-820327-001_fram.htm Gå til

Computer Forensics.DK

DIEBOLD
We won't rest.

Operating Guide for the Diebold 1075ix Exterior Walk-up Cash Dispenser

- + 1 Introduction
- + 2 Cash Dispenser Devices
- + 3 Beginning and Ending a Maintenance Session
- + 4 Fluorescent Lamp Replacement Procedures
- 5 Cash Dispenser Device Maintenance
- + Appendix A Entering and Changing the Safe Lock Combination
- Appendix B Related Customer Documents
- + Figures

These steps are required to perform the following steps:

- If continuous availability mode is set up to require a password, the Password Entry screen appears (Figure 3-22). Enter your 6-digit password, using the numeric keys on the keypad.

NOTE

If you are logging on for the first time, the default password is 0-0-0-0-0-0.

As you enter your password, each entry appears as an x. Use the backspace key to correct a mistake. After you enter the sixth digit, your password is verified and the Continuous Availability Mode screen appears (Figure 3-21).

Figure 3-22 Password Entry Screen

Password Entry

Enter Password using keypad
Press Cancel (Esc) to abort logon
Use backspace to correct errors

—

Time Remaining (seconds)
11

M27209A

Logging on to Maintenance Mode

- Go to the Terminal Control Software (TCS) screen (Section 3.7.1).

Find: pas Find Næste Find forrige Fremhæv alt Forskel på store og små bogstaver

Strong passwords

Kort sagt:

2FA er næsten altid bedst (brug det hvis i overhovedet kan)

Brug en password manager

Lange passwords er bedre end komplekse passwords (passphrases over 14 tegn)

Brug mange forskellige passwords (password manager)

Back dine passwords op

Lange passwords er bedre end hyppige skift - med mindre der har været risiko for aflytning



The advice

- Long passwords are – everything else equal – better than complex passwords. But do not just use a single word (for instance "DIKU") or lazy combinations, such as "DIKU12"
- Strong passwords are better than frequent password changes, unless there is a risk the password has been compromised (hotels, airports etc)
- Use many different password, never the same password on different services
- Use a password manager
- 2-factor is almost always better than your password today, use it when you can



Biometrics



Biometri

Noget man ved
Noget man har
Noget man er

Biometri bør altid kombineres med
BrugerID/password

ID samles typisk i en hash



Biometri

Er biometri identity eller authentication ?

Public or private?

Man efterlader biometri-data over alt

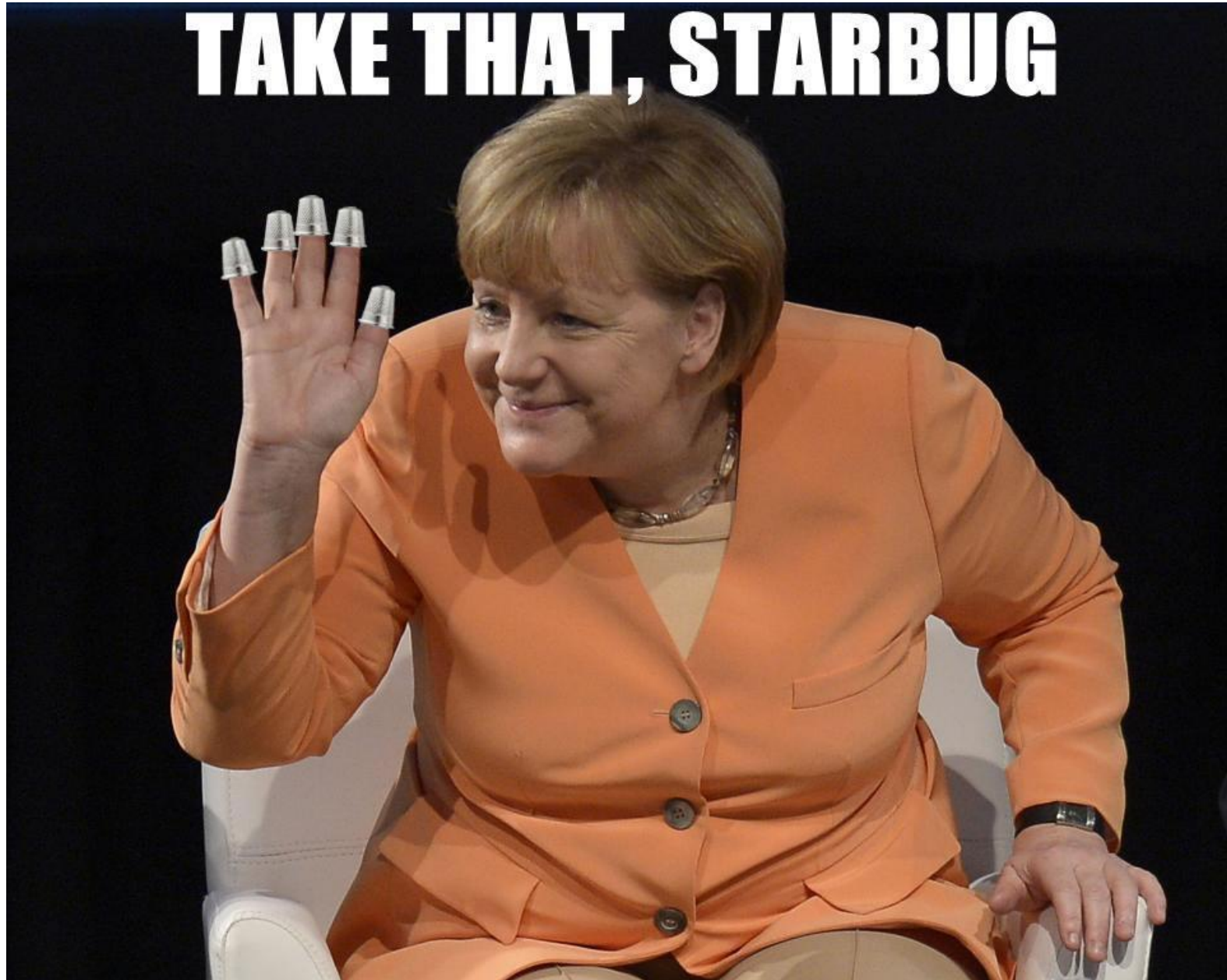
AI/Deep-fakes (stemme, ansigt osv)

Biometri som authentication – uden andre faktorer –
er potentielt et problem
(risiko vurdering!)



Biometri

Husk
threat-
model



Biometri

To biometriske målinger er aldrig helt ens, derfor er der altid element af usikkerhed:

False Acceptance Rate:

Rate at which someone other than the actual person is falsely recognized.

False Rejection Rate:

Rate at which the actual person is not recognized accurately.



Biometri

Fingeraftryk og håndscanner

Optical scanner med lys (klassisk)

Træk fingrene over pladen, ellers efterlades fingeraftrykket

Capacitive (semiconductor), finger bryder delvis isoleringen mellem to ledende materialer, derved tages billedet

Spyt, opvarmet vingummibamse eller ballon med varmt vand



Biometri

Iris scan

Potential for walk by capture
Høj opløsning, HDTV osv.

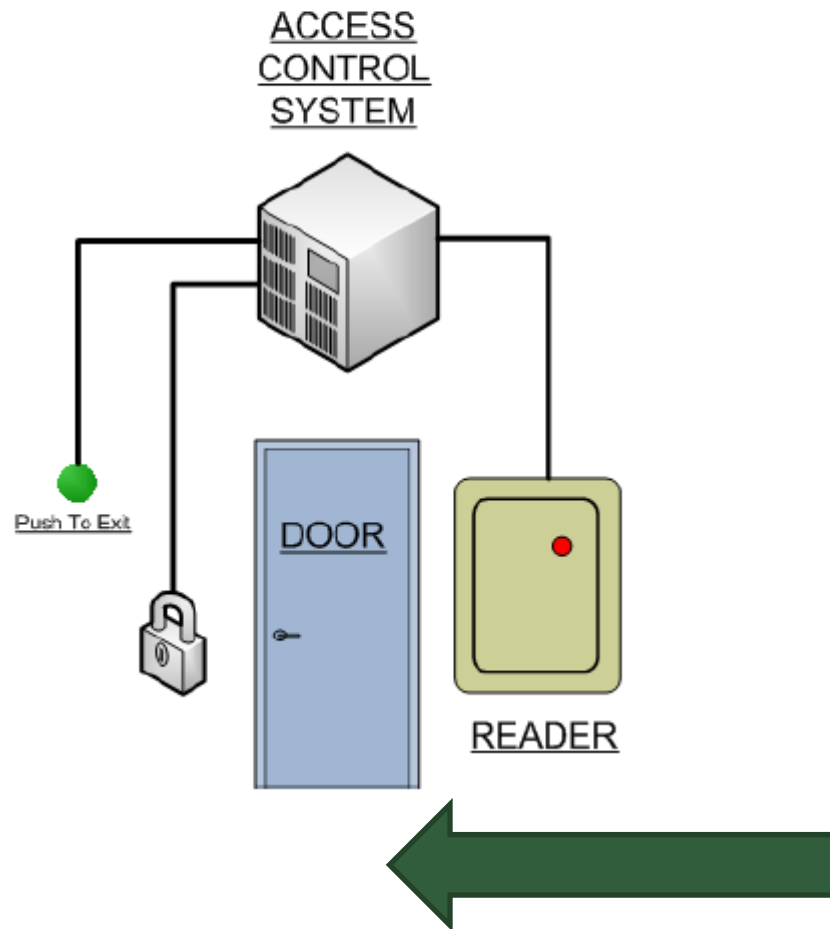
Retina scan

Svært at stjæle - men også svær at bruge
(alignment kræver træning og øvelse)

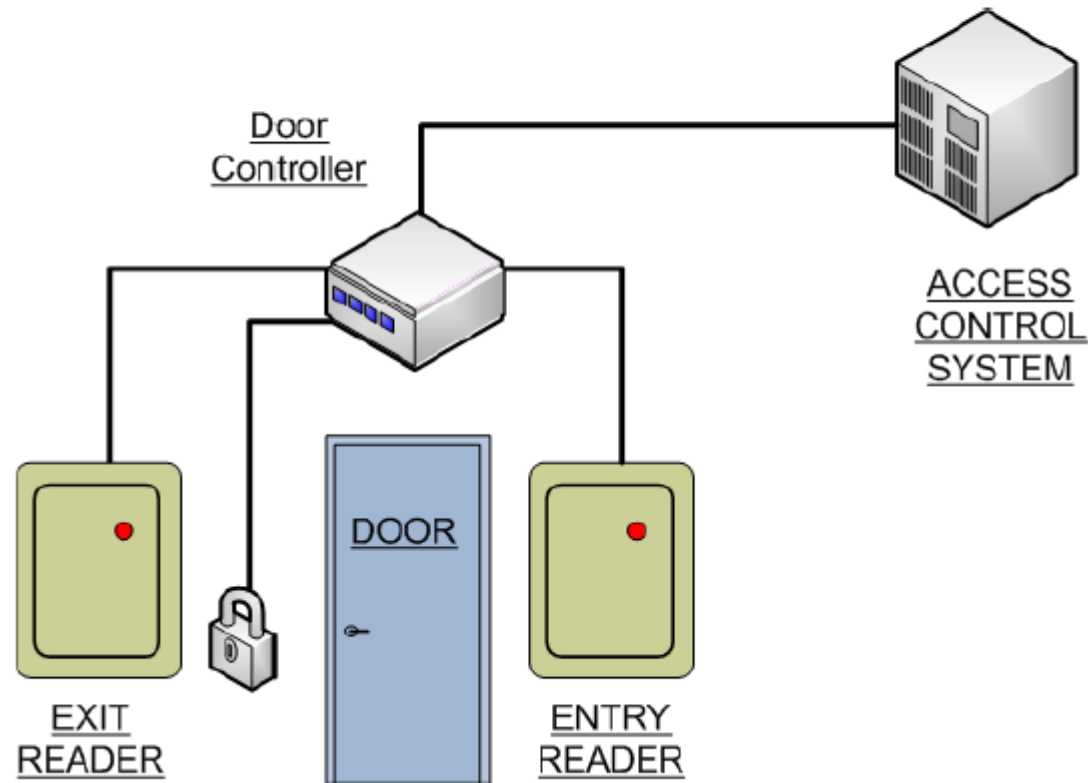


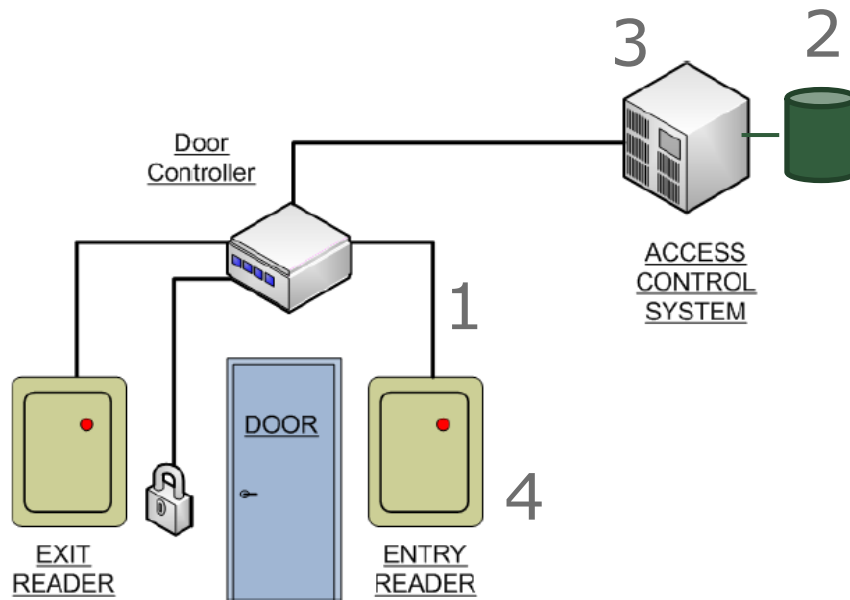
Basic system

Placering af "request to exit" knapper er vigtig, kan de aktiveres ude fra?



Anti-Passback system





1. Angreb imod data og kommunikation
2. Angreb imod templates
3. Angreb imod software
4. Angreb med sensoren

Biometri

TABLE 37.1 Overview of Selected Biometric Technologies

Biometric	Uniqueness	Universality	Permanence	Measurability	Acceptability
DNA	High	High	High	Low	Low
Face geometry	Low	High	Medium	High	High
Fingerprint	High	Medium	High	Medium	Medium
Hand geometry	Medium	Medium	Medium	High	Medium
Iris	High	High	High	Medium	Low
Retina	High	High	Medium	Low	Low
Signature dynamics	Low	Medium	Low	High	High
Voice	Low	Medium	Low	Medium	High

Hvor let er det at stjæle credentials ?



Credential revocation



Fingeraftryk / hånd revokering

Beskyttelse af biometri-data

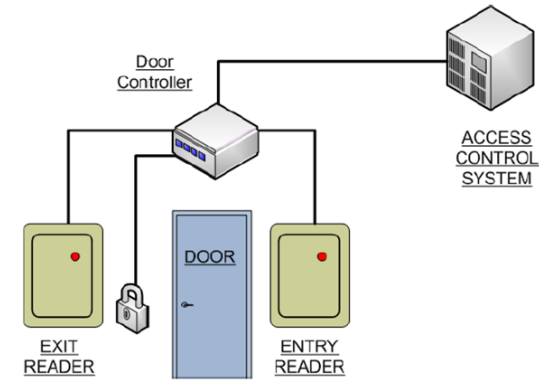
Defeating Facial Recognition Systems doesn't have to be Hi-Tech



facebook.com/OneTruth4Life



Biometri



Der findes også default access nøgler til smart cards.

F.eks. kan en MD5 hash af UID og master nøglen give adgang til smartcardet/administrator kortet

Biometri er også hardware, software og brugervenlighed

Hvor stort er keyspace for hash af template?
Kan man "bare" forsøge at brute-force - eller
sende templates til backend serverne?

Hvor god er match algoritmen, hvem skrev den,
hvad bygger den på?

Hvor stor del af finger aftrykket scannes egentlig
(er det kun center) ?

For meget lys kan ødelægge kameraets billede
(dos/angreb)

Bagud kompatibilitet





Pause



Single Sign On (SSO)



Authentication/authorization

- Huske brugernavn/PW til mange sites
 - Sites skal gemme og administrere id/pw
- Devices, computers, partners, cloud-providers
 - Bruger afgiver alle informationer

SAML

Oauth

OpenID

OpenID Connect

WS-*



Identitet og privacy - termer

Silomodeller – Federation (Føderation)

Identity - Bruger

Identity Provider – Udsteder af akkreditiver

Service Provider – Serviceudbyder

Tokens , assertions eller "billetter"



Traditionel fødereret sikkerhed

Log på Netbank

NEM ID

Basisbank A/S

Bruger-id

?

Adgangskode

?

[Glemt adgangskode?](#)

Næste

Log på uden nøglekort

Log på Portalbank

NEM ID

Hals Sparekasse

Bruger-id

?

Adgangskode

?

[Glemt adgangskode?](#)

Log på

Log på med nøglekort

Akkreditiver: tokens/assertations/billetter (SAML Assertion, x509 certifikater, Kerberos tickets osv)

PKI: certifikatudstedere

SAML: Identity Providers

WS-*: Security Token Service

Attributtjenester



Identitet og privacy

Hvordan får man et tilbud på et lån?

Skat

Bank

NemID



Identitet og privacy – Nemlog-in (SAML) - NemID

The screenshot shows the 'DET OFFENTLIGE LOG-IN-FÆLLESSKAB – NEMLOG-IN' login page. A modal dialog box is open in the center, titled 'Du viderestilles nu til Det Offentlige Log-in Fællesskab'. The dialog contains the following text:

Velkommen til Det Offentlige Log-in Fællesskab - NemLog-in. Her kan du benytte både din personsignatur og din medarbejdersignatur til at logge ind.

Brug din personsignatur, hvis du skal logge ind i privat øjemed.

Med din personsignatur kan du for eksempel logge ind på skat og rette i din selvangivelse eller udføre andre handlinger, der knytter sig til dig som privat person.

Brug din medarbejdersignatur, hvis du skal logge ind i erhvervmæssigt øjemed.

Med din medarbejdersignatur kan du indberette direkte til myndighederne på din virksomheds vegne. Din medarbejdersignatur er personlig og knyttet til den virksomhed, du er ansat i.

☐ Vis ikke denne besked igen

In the background, the login form is visible with the title 'NEM ID NemLog-in'. It includes input fields for 'Bruger-id', 'Cpr-nr., NemID-nr. eller selvalgt bruger-id', and 'Adgangskode'. A 'Næste' button is at the bottom of the form. Below the form, there is a checkbox for 'Husk jeg vil logge ind med nøglekort' and a section titled 'Husk sikkerheden' with a link to 'Læs hvorfor >'.

Identitet og privacy

Hvordan får man et tilbud på et lån?

Skat

Bank

NemLog-In



NemID



Authentication – SAML er mest udbredt i virksomhederne

Security Assertion Markup Language (SAML) is an XML-based open standard protocol for exchanging authentication and authorization data between parties/two security domains, in particular, between an identity provider and a service provider

Federated identity, f.eks. cloud single sign-on (SSO)

“Standard protocol til at kommunikerer identiteter over internettet”



Authentication – SAML er mest udbredt i virksomhederne

Two federation partners can choose to share whatever identity attributes they want in a SAML assertion (message) payload as long as those attributes can be represented in XML.

Enterprise SAML identity federation use cases often sharing identity between an existing IdM system and web applications.



Authentication – SAML er mest udbredt i virksomhederne

Tokens i stedet for passwords.

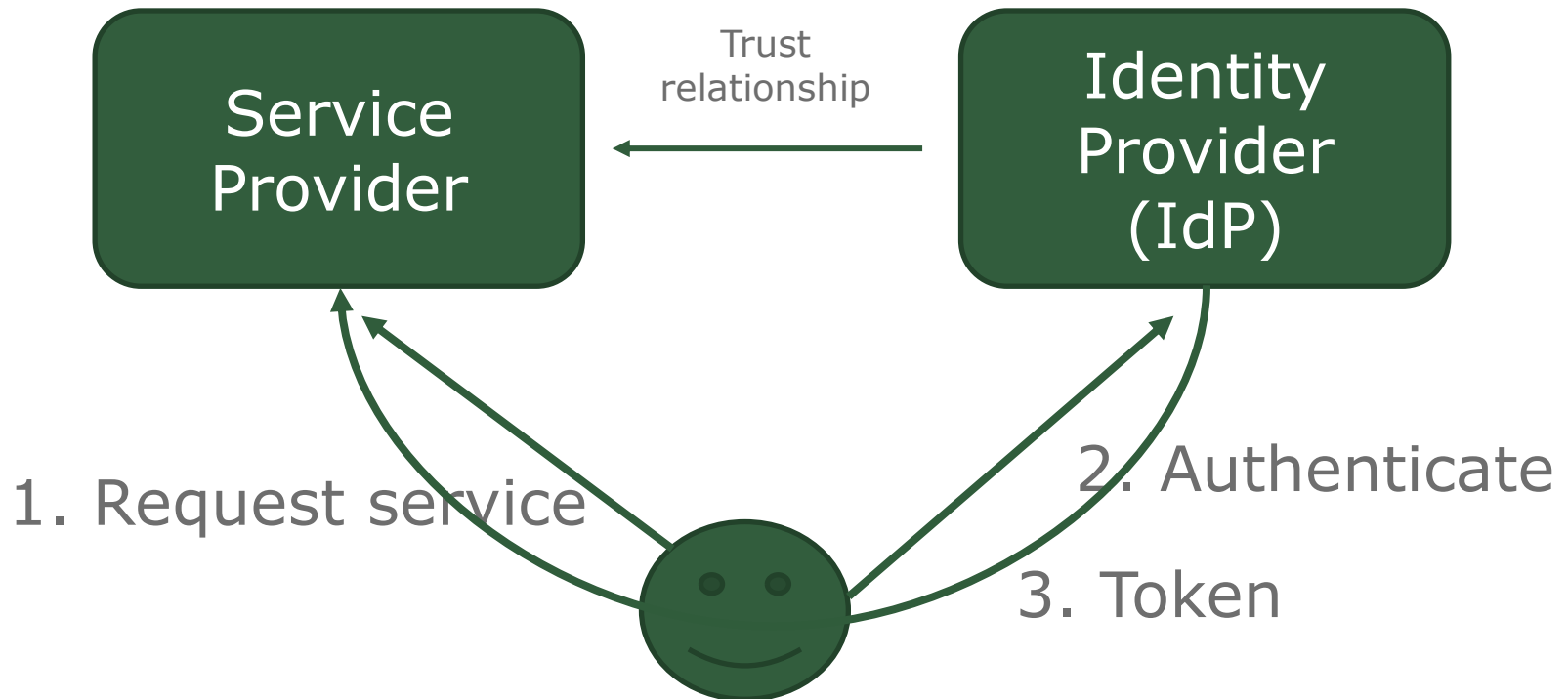
Tre entities:

1. Identity provider
2. Service provider (kan være ekstern, som Salesforce)
3. Brugeren, har en konto hos Identity Provider

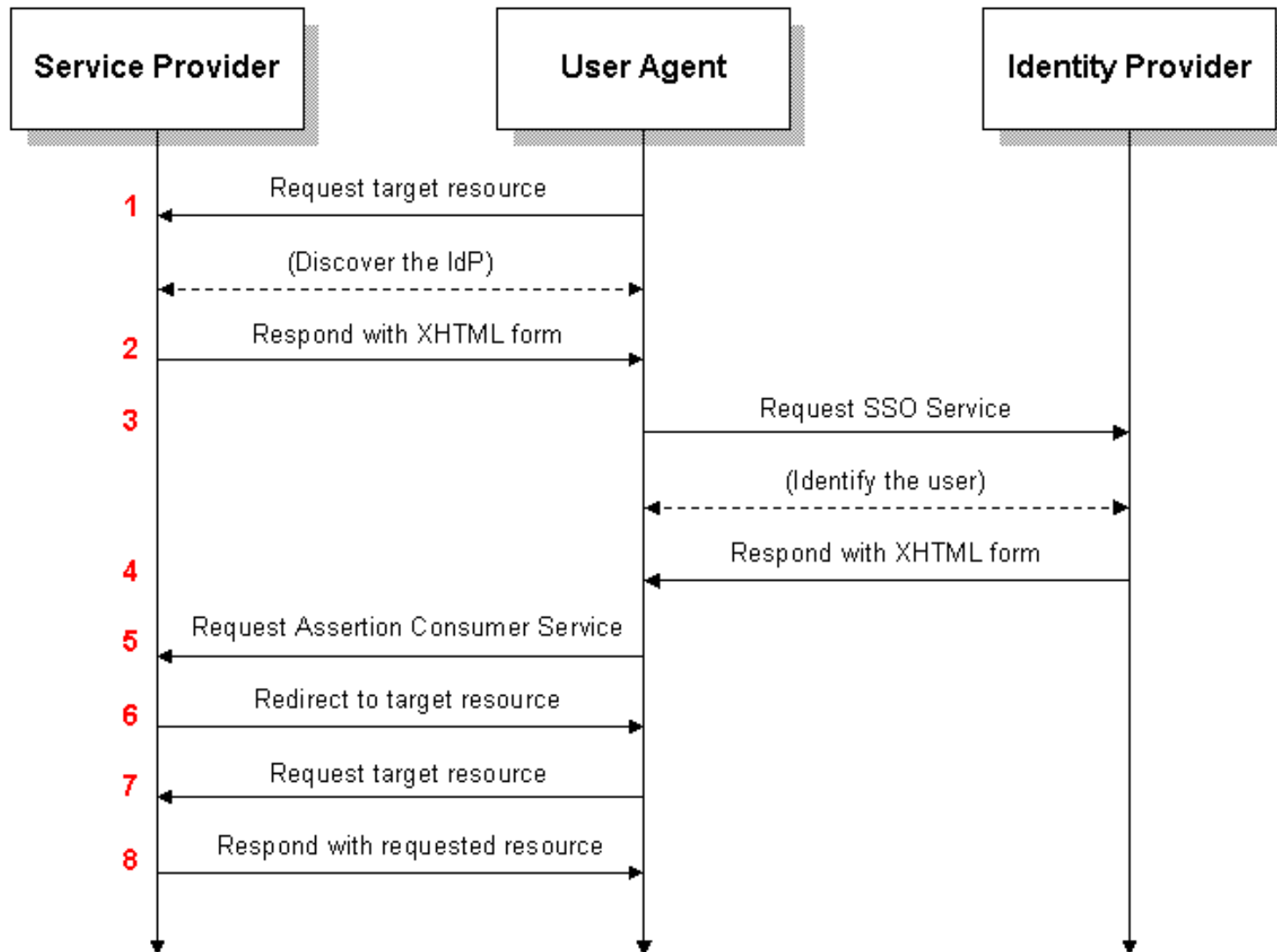
Bruger autentificerer hos Identity Provider, der udsteder en SAML-token, sendes tilbage til brugeren, der sender videre til Service Provider



Authentication – SAML er mest udbredt i virksomhederne



Authentication – SAML er mest udbredt i virksomhederne



Authentication – OAuth 2.0

OAuth (Open Authorization) er en standard for authorization af adgang til ressourcer.

V2.0 dækker både authentication og authorization (Kan outsource authentication til f.eks. Google, Facebook for en applikation (se OpenID Connect))

Standard method for web, mobile and desktop applications

OAuth tokens can be binary, JSON or SAML

HTTP (SSL)



Authentication – OAuth 2.0

OAuth is a framework to allow one application access to one account without giving your account login information.



Brugervenlighed, mindre administration osv...



Social login

Hvad (kan) modtageren få at vide om dig når man laver "social login" via Facebook login:

Facebook

Gender

Get access to the following for users that authenticate with Facebook:

Basic Profile Enterprise Pro Plus Basic

Read access to the users' profile data. Returned by the [auth_info](#) API call.

Address	Birthday	Email	Profile Photo
Verified Email	Display Name	Gender	Homepage
Identifier	Name	Preferred Username	UTC Offset

Extended Profile Enterprise Pro Plus

Read access to the users' extended profile data. Returned by the [auth_info](#) API call.

About Me	Activities	Addresses	Albums
Books	Current Location	Emails	Games
Groups	Interested In M...	Interests	Languages Spoken
Movies	Music	Organizations	Page Likes
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Videos
Friends List	Heroes	Id	Last Updated
Name	Profile URL	Sports	URLs

Contacts Enterprise Pro

Read access to the users' friends. Returned by the [get_contacts](#) API call.

About Me	Activities	Addresses	Birthday
Books	Current Location	Interested In M...	Interests
Languages Spoken	Movies	Music	Organizations
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Display Name
Gender	Heroes	Id	Last Updated
Name	Preferred Username	Profile URL	Sports
URLs			

Oauth 2.0 vs SAML 2.0 – sammenfald i principper

SAML typically used in Enterprise SSO scenarios
(inside the enterprise, enterprise to partner, enterprise to cloud)

Enterprise SSO = SAML

Partner, or Customer app, access to portal = SAML

Centralized identity source = SAML (OpenID Connect)

Oauth designed for use with applications on the internet: Provide access to resources (accounts, pictures, files...) = Oauth

Mobile devices typisk = OAuth



Authentication – OpenID Connect

OpenID Connect is a way to specify one identity for multiple sites so you don't need to register over and over again.

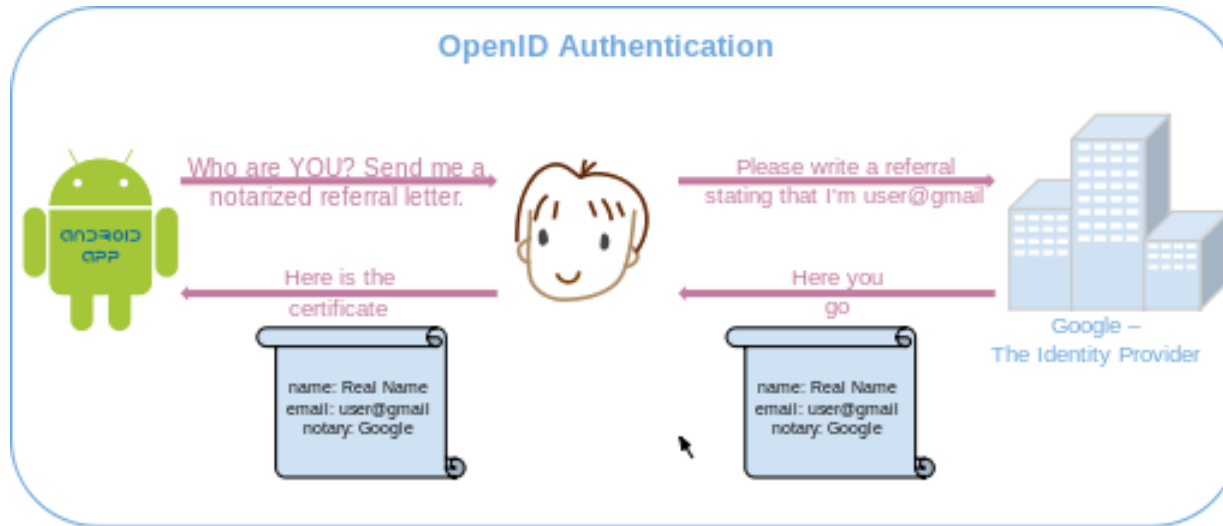
You can log in into multiple websites with a unique account, using OpenID Connect.

Trust the specific OpenID Connect Identity Provider?

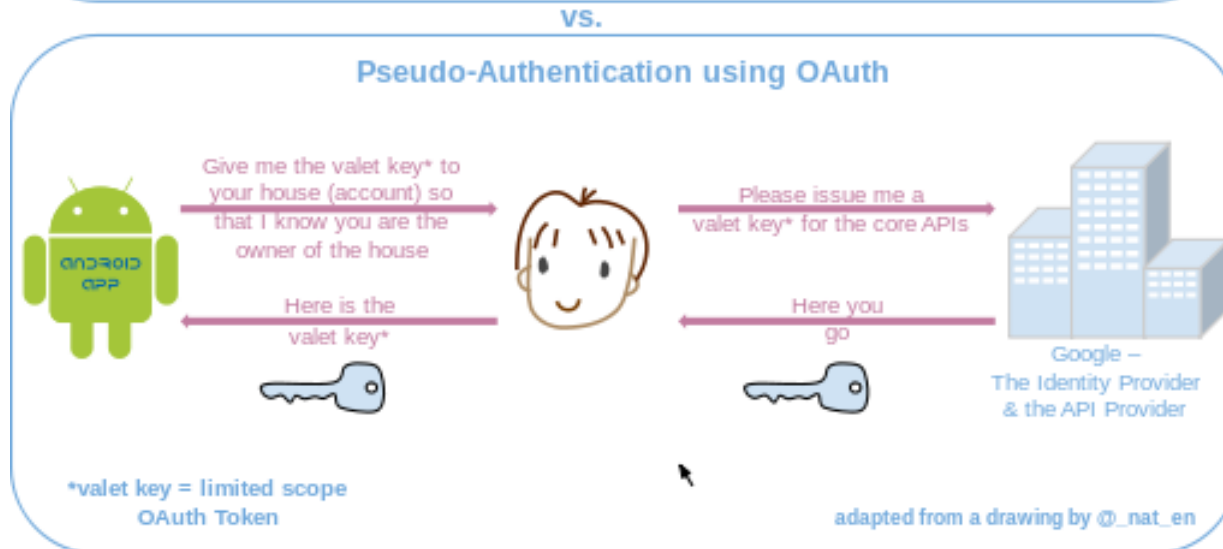
Sometimes OAuth and OpenID together



Authentication – OpenID Connect vs. OAuth 2.0



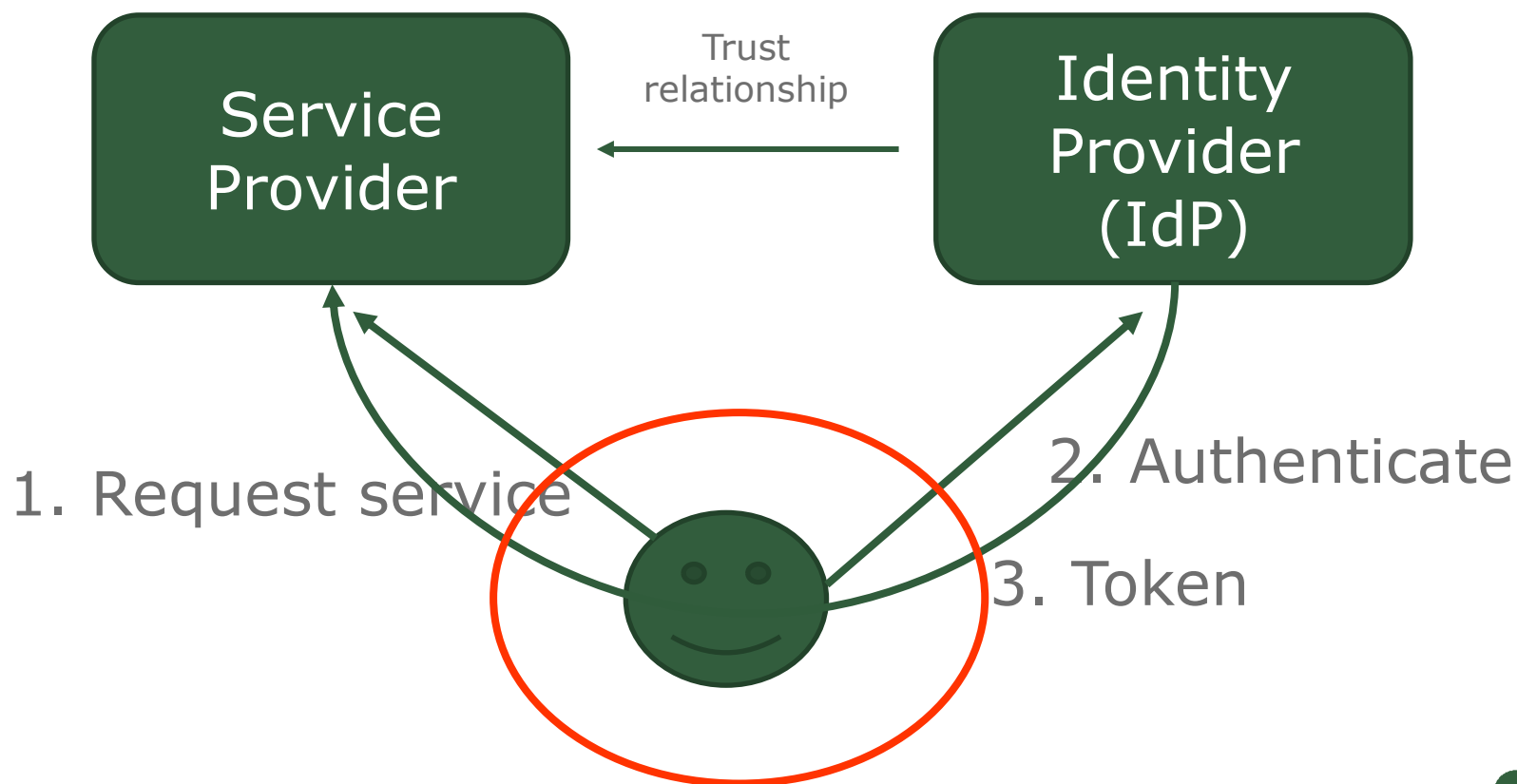
Giver navn og mail til mange sites



Opnår adgang uden nødvendigvis at give sites dine id-oplysninger

Identitet og sikkerhed

Brugeren er i centrum



Identitet og sikkerhed

287

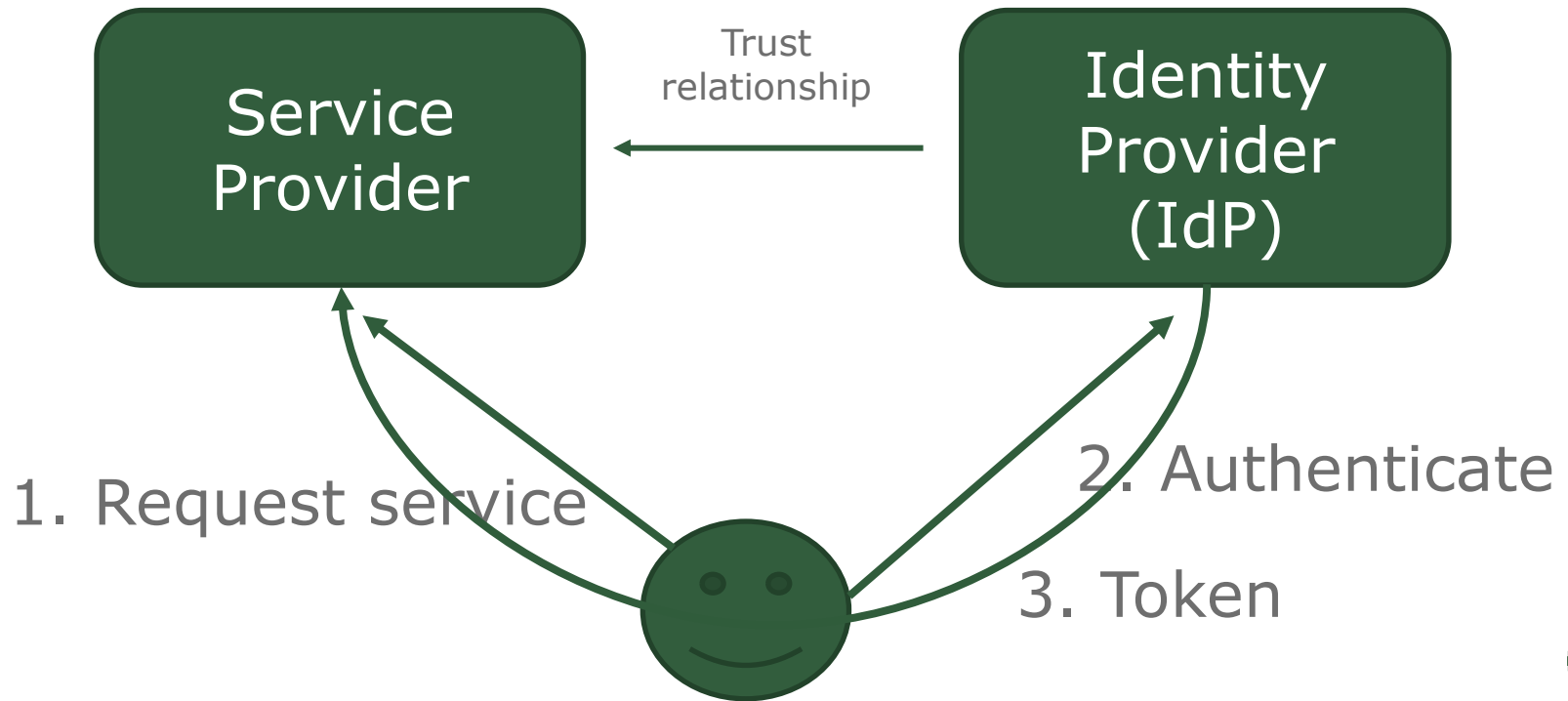
TABLE 17.1 Evaluating identity 2.0 technologies

Requirement	XRI/XDI	ID/WSF	Shibboleth	CardSpace	OpenID	SXIP	Higgins
Empowering total control of users over their privacy							
Usability; users are using the same identity for each identity transaction							
Giving a consistent user experience due to uniformity of identity interface							
Limiting identity attacks such as phishing							
Limiting reachability/disturbances such as spam							
Reviewing policies on both sides when necessary, identity providers and service providers							
Huge scalability advantages because the identity provider does not have to get any prior knowledge about the service provider							
Assuring secure conditions when exchanging data							
Decoupling digital identity from applications							
Pluralism of operators and technologies							

Identitet og sikkerhed

Hvem er det vi vil/skal beskytte – bruger, SP eller IdP?

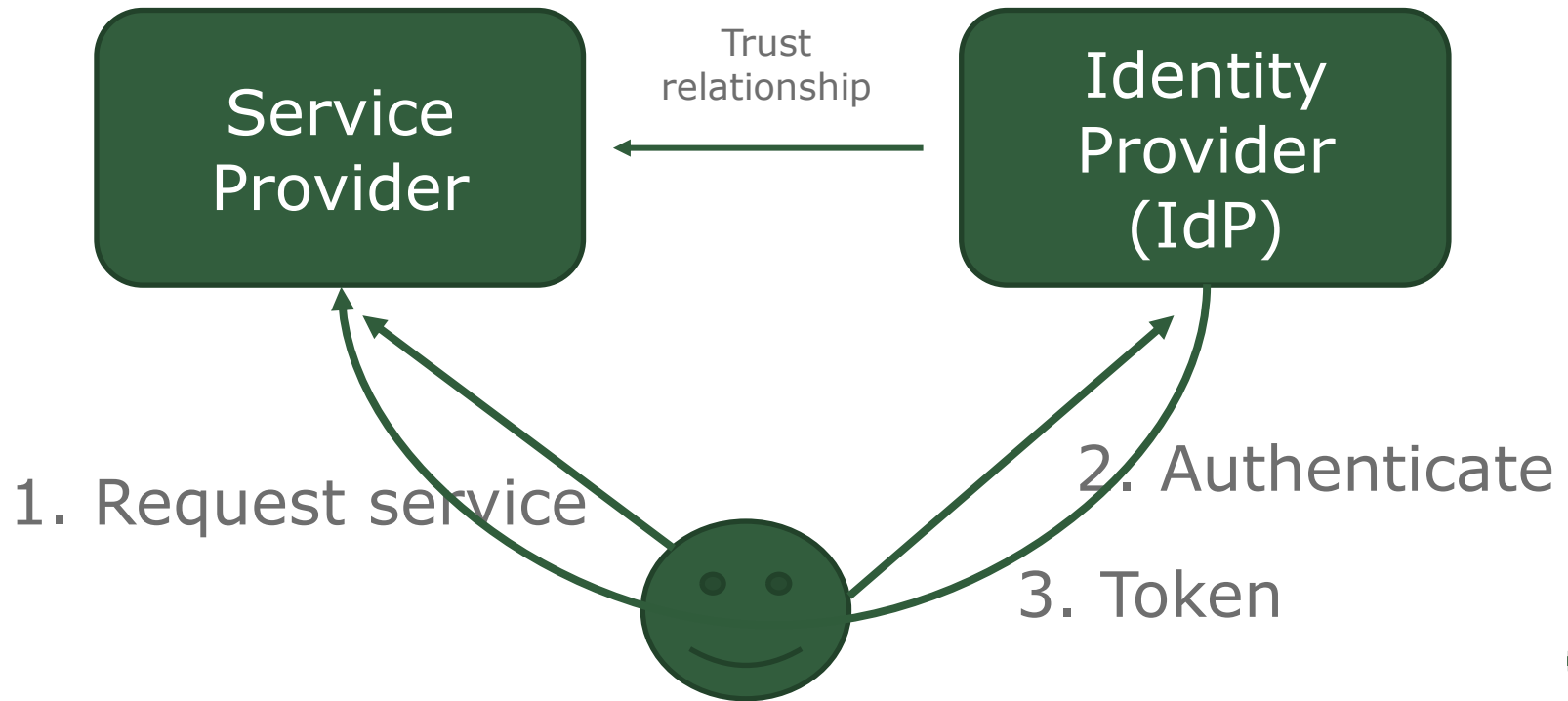
Hvad er NemID's focus?



Identitet og Privacy

Privacy by Design

Identity Provider / OpenID Provider osv ved hvor og hvornår du logger ind hos alle Service Providers



Summary

Digital user authentication principles

- A model for digital user authentication
- Means of authentication
- Risk assessment for user authentication

Password-based authentication

- The vulnerability of passwords
- Password selection strategies
- The use of hashed passwords
- Password cracking of user-chosen passwords
- Password file access control

Token-based authentication

- Memory cards
- Smart cards
- Electronic identity cards

- Biometric authentication
 - Physical characteristics used in biometric applications
 - Operation of a biometric authentication system
 - Biometric accuracy
- Remote user authentication
 - Password protocol
 - Token protocol
 - Static biometric protocol
 - Dynamic biometric protocol
- Security issues for user authentication

"Cheating": Social engineering



IT Security is difficult

Intelligent adversaries



Kompromittering via Social Engineering

- At narre mennesker til at gøre ting de ellers ikke ville gøre eller udlevere fortrolige oplysninger.
- Kan fører til hacking og identitetstyveri.
- F.eks. ved at optræde som insider med afsæt i viden om virksomheden.

Hvordan kan en angriber få viden om en virksomhed?



Hvad sker der ?

Nysgerrighed
Hjælpssomhed
Undgå konflikter
Stress



“No matter how low an opinion you have of your users,
they will figure out a way to disappoint you.”
-Stamos' Law

“We have dumb monkeys who clicks on buttons”
- Chris Hoff



Fremgangsmåden

Informationsindsamling

Opbygning af tillid

Scenariet

Pres for en løsning - "hvad kan vi gøre?"



Bagrundsviden



0. Informationsindsamling

Internet, sociale netværk, dumpster diving, besøg, opsøge medarbejdere, webmail, linkedin, jobannoncer osv, osv.



Hej, hvad er dit password?

1. Opbygning af tillid

Det er sjældent nok at sige
"Hej, hvad er dit password?" eller
"Hallo – det er din chef, giv mig Admin
passwordet eller du er fyret"

En række venlige, trivielle spørgsmål først
(opbygger tillid)



Hej, hvad er dit password?

2. Baggrundsscenariet (pretexting)

Ramme for angreb, kan være en hel identitet (baseret på indledende research)



"Her er mit billede"



Hej, hvad er dit password?

3. Pres

"Hvordan løser vi det her?"

Kropssprog, stemmeføring,
høflig/vred/travl/autoritær osv



Han er "en af vores"

Samme sprog og jargon
Det rigtige tøj

Overbevise folk om man "hører til"



Påklædning er vigtig

Dress as a DJ:

<https://www.youtube.com/watch?v=uoIL2x6sIC8>

Hvad ville have virket i bussen?



Man er usynlig i en neon-vest

<https://www.youtube.com/watch?v=tFur1-i6BpA>



Praktisk eksempel (2019)



"Pre-loading"

Mange, mange teknikker

Påvirke inden faktiske møde/hændelse
Verifikation af identitet



Fysisk adgang

ID-kort

Piggybacking/tailgating

Telefoner, kopper og pakker

Bude, reparatører, revisorer, journalister

Rygere og andre grupper

Pre-loading

Tyveri, informationsindsamling, trådløse
accesspoints, netværksadgang, serverrum

...



Det svageste led i sikkerhedskæden

Telefon, personlig fremmøde,
USB, CD, websider, pdf-filer, hacke
e-mail, vinde gaver, voice beskeder



Don't click it – and don't pick it up either!

**Ah – og hvis du finder en USB-nøgle
på jorden: lad være med at teste den !**



Phishing

A phishing attack usually comes in the form of a message meant to convince you to:

- **click on a link**
- **open a document**
- **install software on your device**
- **enter your username and password into a website that's made to look legitimate.**

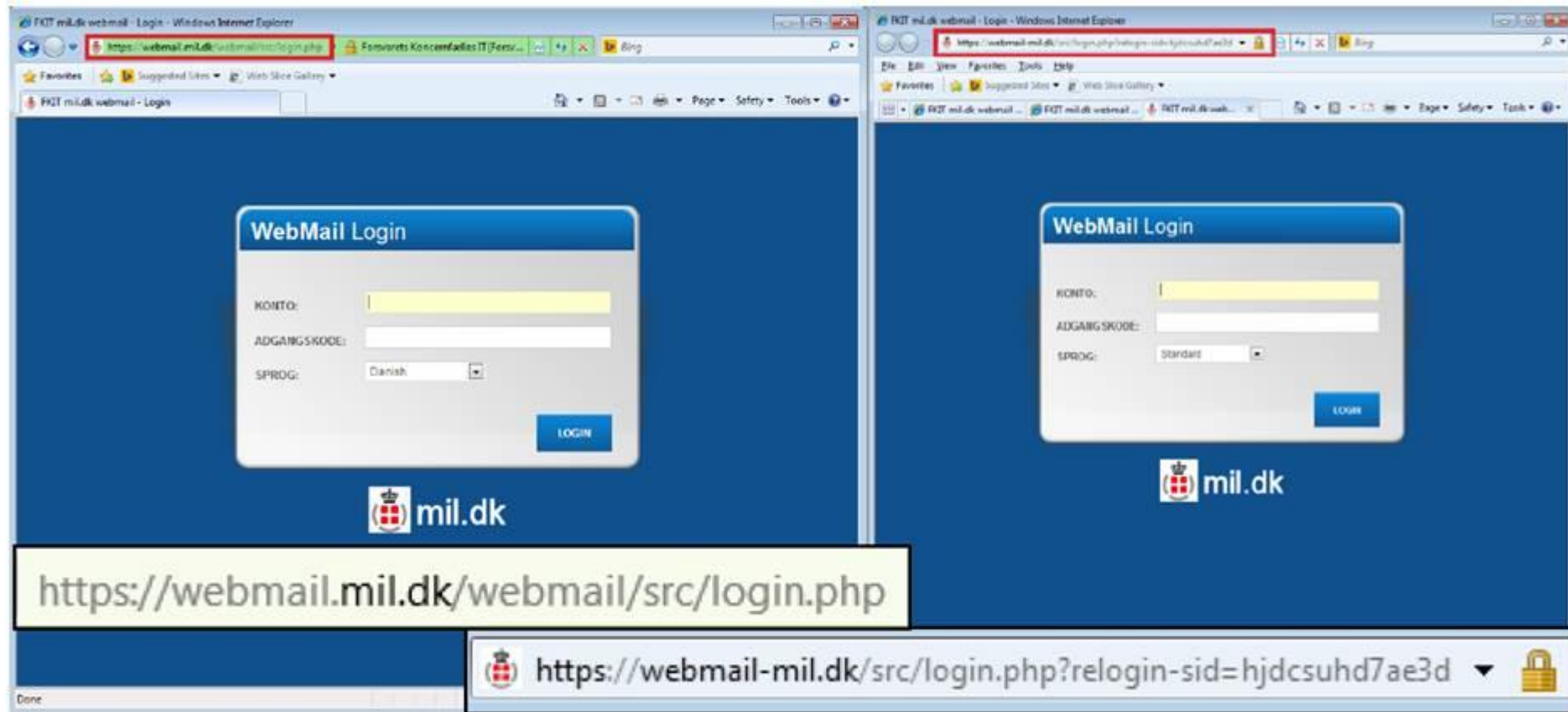


Don't click it



Totally not a
virus. Trust
me...im a
dolphin

Don't click it



Billede 1: Den falske e-mail-login-side sidestillet med den legitime side. De to URL'er er fremhævet nedenunder.

Don't click it



Someone has your password

Hi William

Someone just used your password to try to sign in to your Google Account

@gmail.com.

Details:

Tuesday, 22 March, 14:9:25 UTC

IP Address: 134.249.139.239

Location: Ukraine

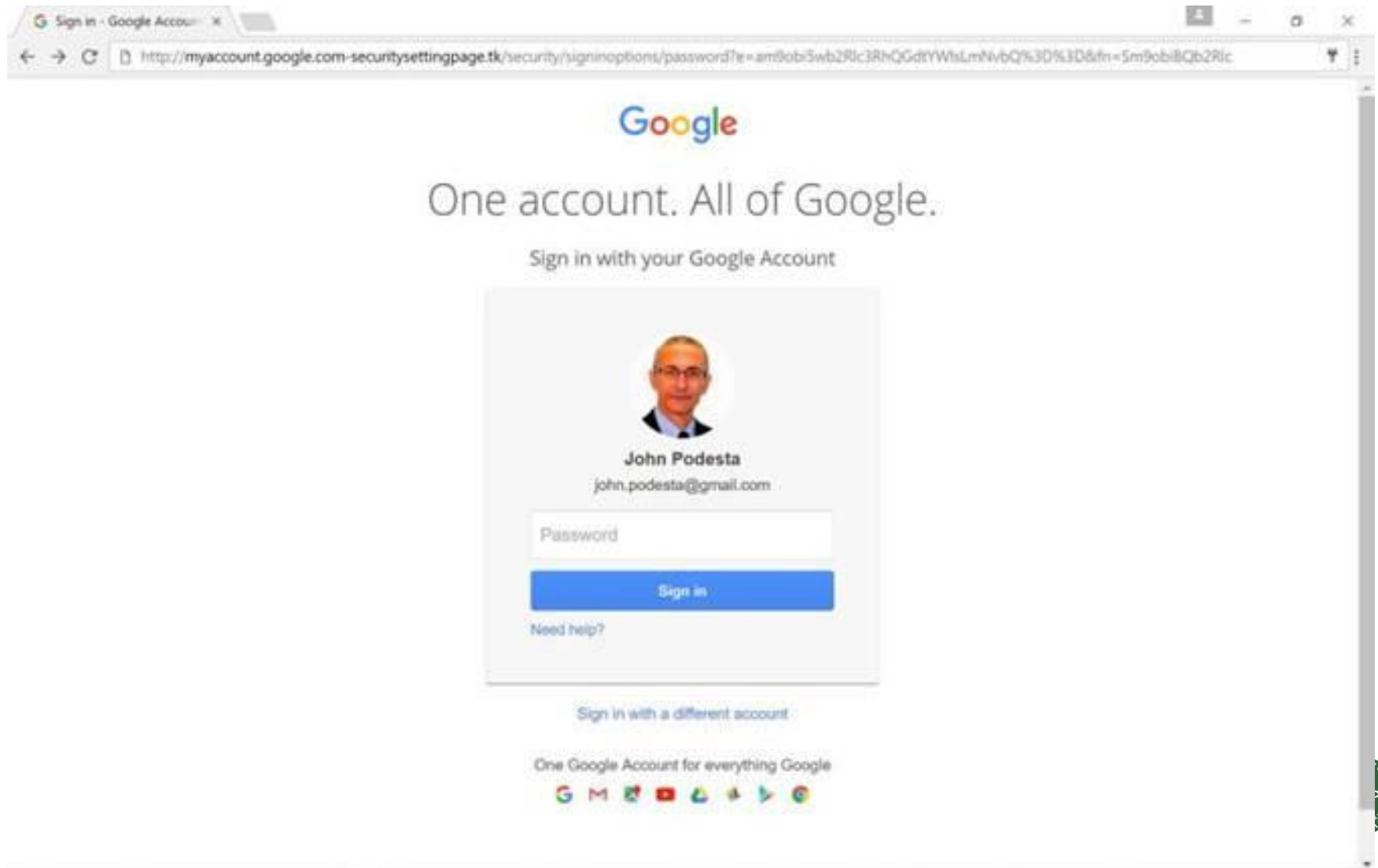
Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team



Don't click it



Don't click it

Be suspicious of all **links** that ask you to log in, regardless of the sender.

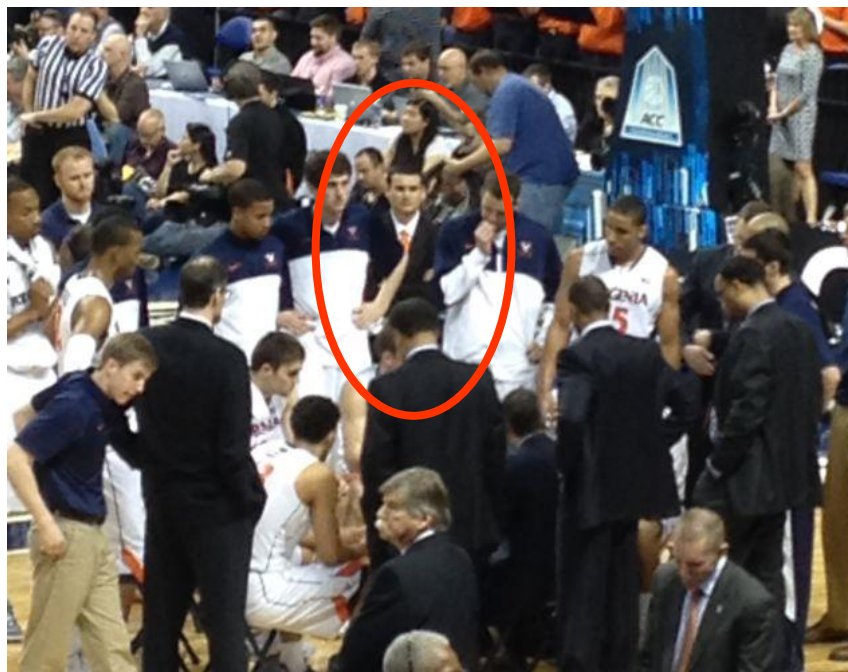
And be very careful of all **attached files** – regardless of the sender



By the way - do not "*enable content*" on documents with macros (.docm)



Er det svært for dem?



<http://deadspin.com/uva-fan-bluffs-his-way-through-the-perfect-acc-title-ga-1547386713>

70 dollars i Walmart...



Hvad gør man imod Social Engineering?

Pain Center



Forstå truslerne

Jo højere sikkerhed, jo mere sandsynlig
er social engineering

Træning og understøttende procedurer
– hvad er advarselssignalerne
-procedure gør det svært for angriber

Ikke kun telefonen - også mail, chat,
hjemmesider og fysisk fremmøde m.m.

"Hvordan kan vi forbedre vores procedurer?"



Ikke det samme for alle

Rette niveau af paranoia !

Hvis man føler sig *usikker* – "der er et eller andet, der ikke føles rigtigt"



Forstå truslerne

O. Informationsindsamling

Makuler dokumenter

Forsigtig i offentlige rum

Information over telefonen, mail o.lign.,
særligt ved uventede henvendelser

1. Opbygge tillid

Meget snakkende

Hvorfor taler han om det?

Spørg ind ved fejl, hvis fejl fortsætter ->
afslut



Forstå truslerne

2. Scenariet

Hvis usikker: gencheck, gencheck, gencheck
Tag dig tid og følg proceduren

3. Pres

Teknikker der benyttes (awareness)

Giv ikke efter

Henvis til politikker og procedurer

Tilkald en leder hvis usikker (overfør risiko),
tag ikke beslutningen selv



Mulige tiltag

Anden kanal til at overdrage info, end den der spørges fra, f.eks.

- telefon til voicemail/SMS
- email til leder
- give fysisk til anden person fra afdelingen

Ring tilbage/send mail tilbage
(men ikke reply-to)



Mulige tiltag

Check og bekræft id, også selvom det er svært
(eller måske særligt hvis det er svært)

Passwordbeskyttelse af information

Fysisk sikring, f.eks imod tail-gating

Kultur, "Hvorfor har du ikke skilt på?"



Mulige tiltag

- **Awareness**
- **Opdateret software**
- **Brug 2FA (og/eller password manager)**
- **Bekræft med afsender (vha andre kanaler)**
- **Åben attachments på en sikker måde**
- **Backup**

A sense of urgency is always the first big clue

Giver pretext'en egentlig mening – ville et firma virkelig ringe til dig, eller bede dig om at ringe til dem?

Ville dét firma virkelig bede om den information?



Social engineering teknikker virker i praksis

Makollig Jezvahted and Levdaroum DeBahzted

My colleague just farted, and left the room, the bastard



(.wav)



Spørgsmål

