Vylepšení stávajících forem autentizace a možné alternativy

Dominik Nop, prezentace do KIB

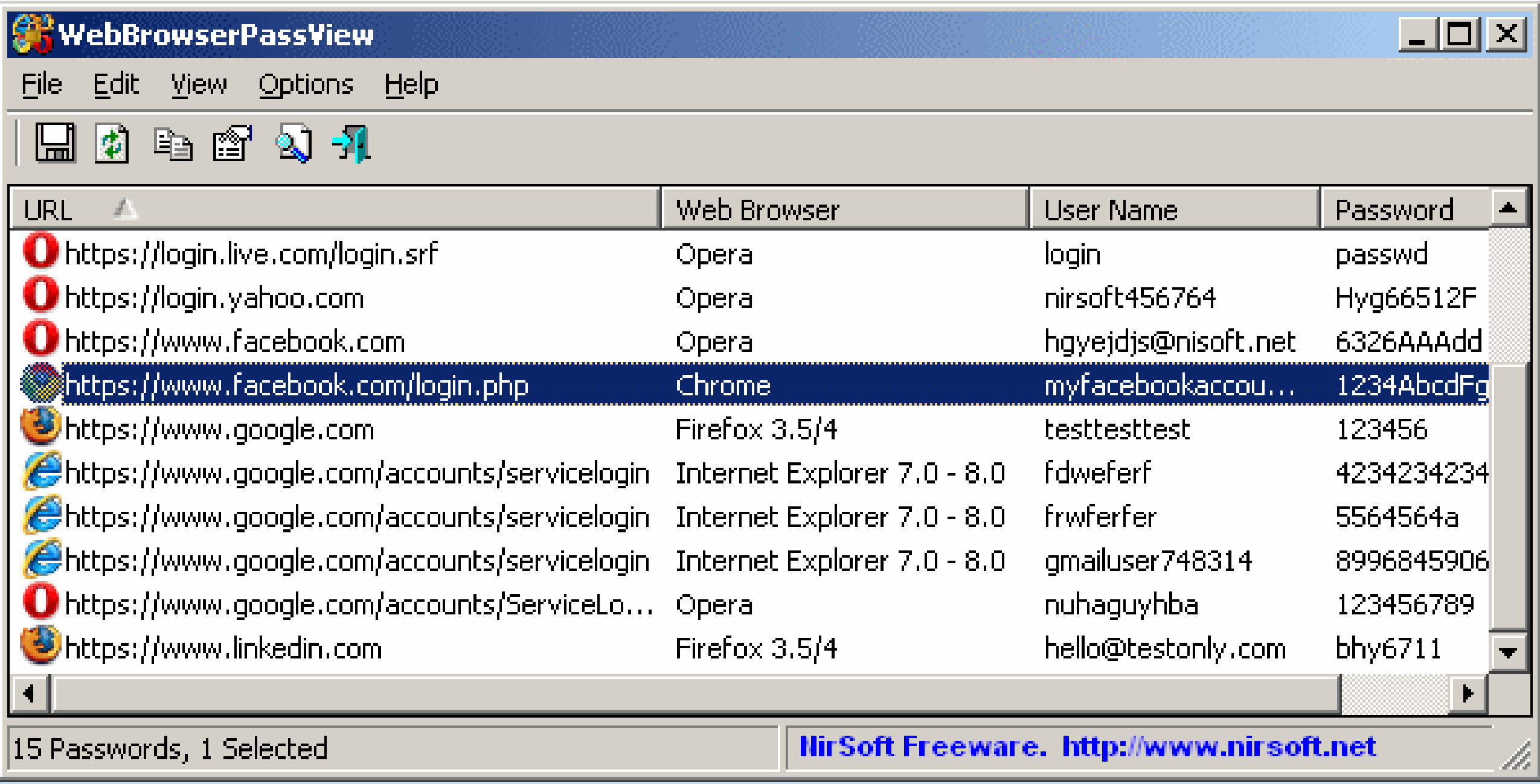
Důvod hledání alternativ a vylepšení

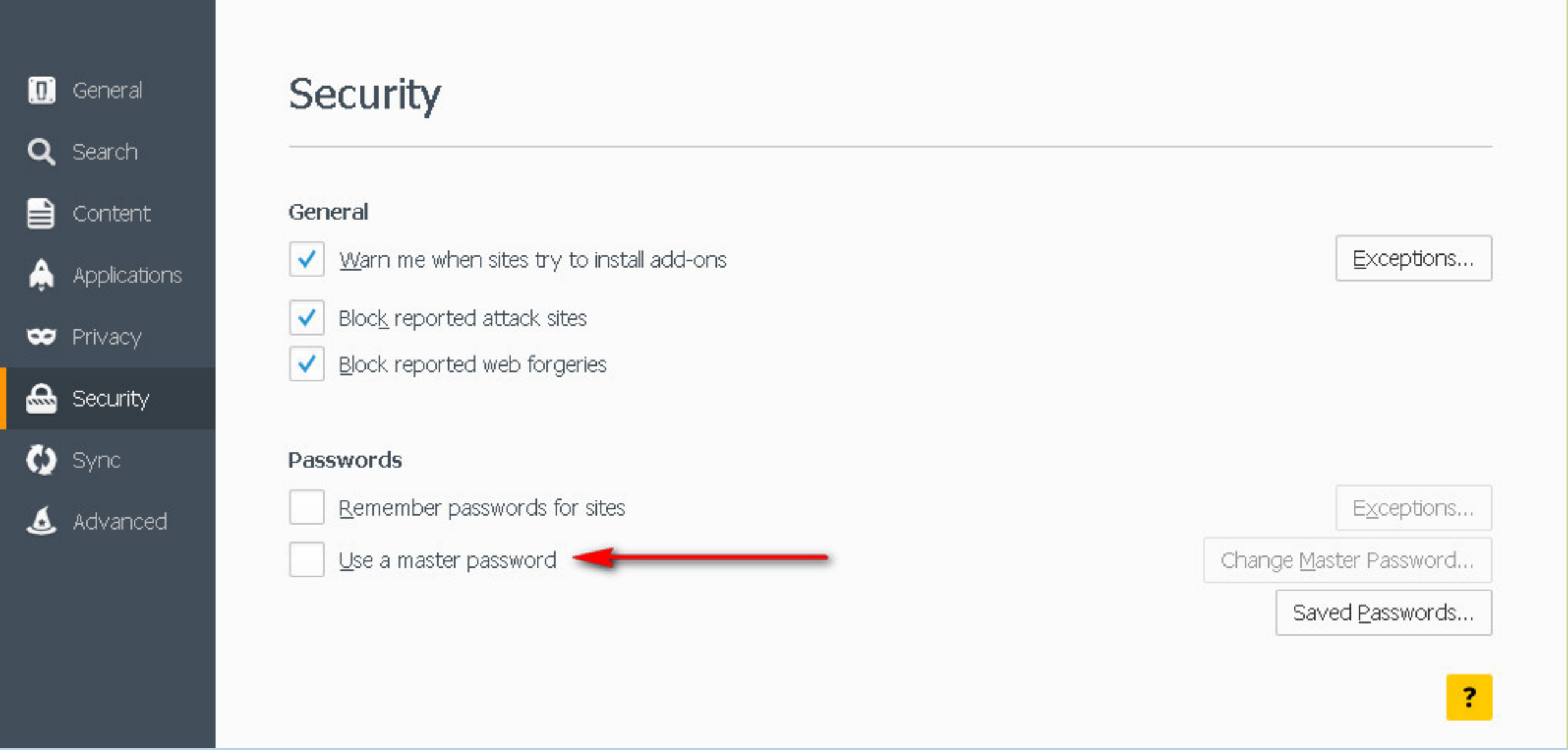
- Uživatelé si nepamatují složitější hesla, nebo PIN kódy
- Někdy ani nechtějí
- O užívání většího množství hesel ani nemluvě
- Následky
  - Oblíbená hesla = velká úspěšnost slovníkových útoků
  - Kratší hesla = menší prostor klíčů = snazší útok hrubou silou
  - Zapisování PIN kódů na papír = Krádeže, shoulder surfing

- Hlavní zdroj: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Správa hesel - prohlížeče

- Snaha usnadnit uživatelům užívání více složitějších hesel
- Chrome, IE
  - žádné zvláštní zabezpečení uložených hesel, stačí znát heslo k přihlášení do PC
  - WebBrowserPassWiew
- Firefox
  - Master password (MP) – heslo hesel
  - signons.sqlite – zašifrovaná databáze se jmény a hesly
  - šifrování uložených dat pomocí 3DES v CBC módu
  - key3.db – obsahuje SDR klíč + sůl (klíč k šifrování databáze), a také „global salt“
  - SDR klíč také zašifrován s pomocí 3DES, klíč = Hash(MP + global salt)

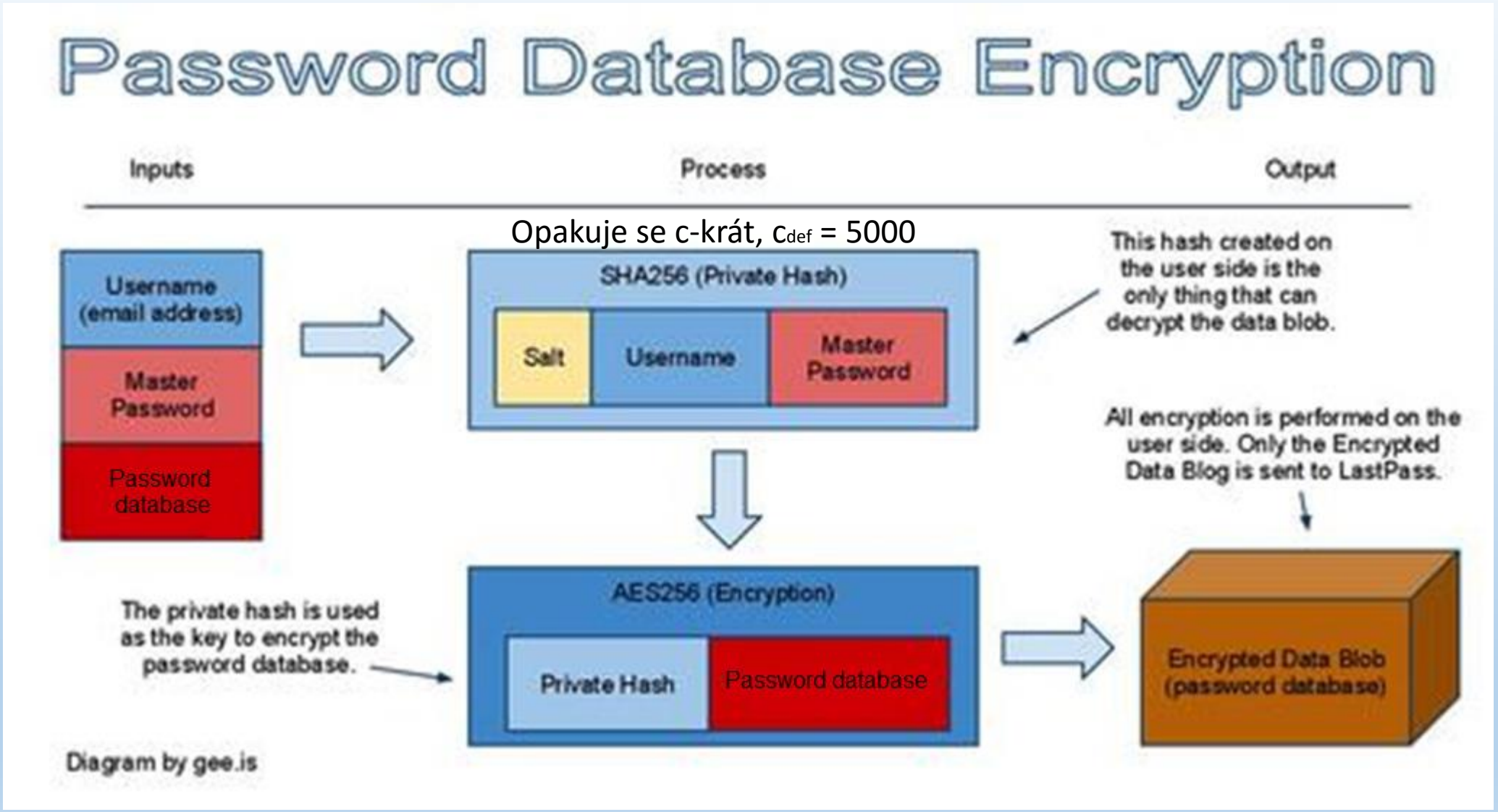

WebBrowserPassView
File Edit View Options Help
URL
Web Browser
User Name
Password
https://login.live.com/login.srf
Opera
login
passwd
https://login.yahoo.com
Opera
nirsoft456764
Hyg66512F
https://www.facebook.com
Opera
hgyejdjs@nisoft.net
6326AAAAdd
https://www.facebook.com/login.php
Chrome
myfacebookaccou...
1234AbcdFg
https://www.google.com
Firefox 3.5/4
testtesttest
123456
https://www.google.com/accounts/servicelogin
Internet Explorer 7.0 - 8.0
fdweferf
4234234234
https://www.google.com/accounts/servicelogin
Internet Explorer 7.0 - 8.0
frwferfer
5564564a
https://www.google.com/accounts/servicelogin
Internet Explorer 7.0 - 8.0
gmailuser748314
8996845906
https://www.google.com/accounts/ServiceLo...
Opera
nuhaguyhba
123456789
https://www.linkedin.com
Firefox 3.5/4
hello@testonly.com
bhy6711
15 Passwords, 1 Selected
NirSoft Freeware. http://www.nirsoft.net



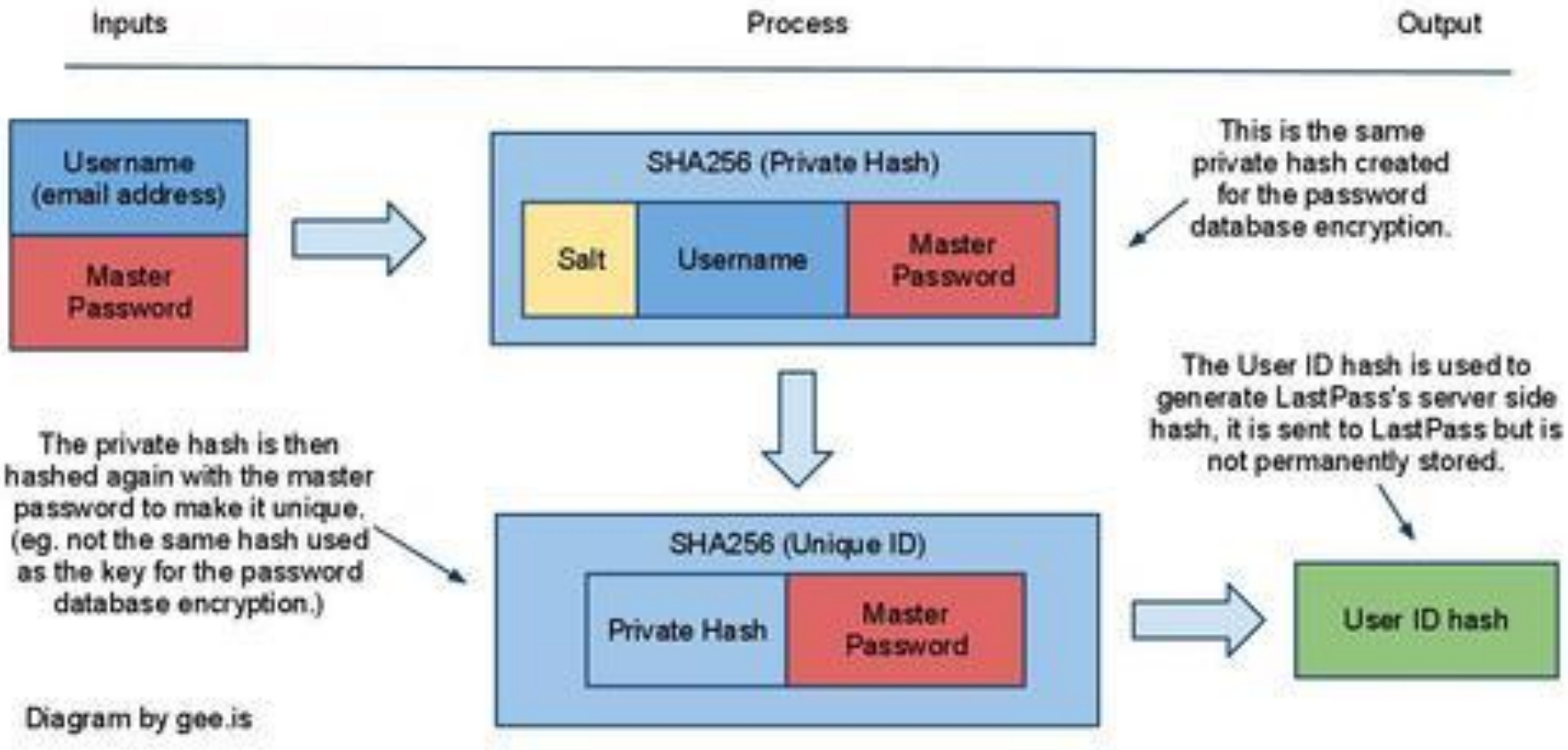
Není – li používáno, je zabezpečení uložených hesel prakticky nulové!!!

Správa hesel - Lastpass

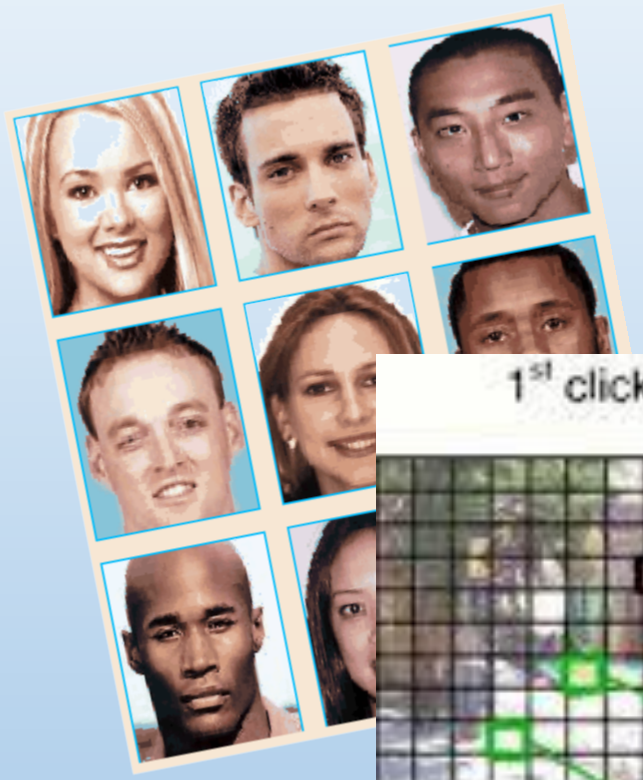
- Ukládání, zabezpečení i generování hesel
- Pro veškerou komunikaci se serverem Lastpass je užíván SSL, všechna data jsou navíc šifrována 256 b. AES
- Šifrování vždy na straně uživatele
- Klíč pro šifrování dat vytvářen pomocí PBKDF2, který užívá SHA-256,
- počet opakování lze nastavit (přednastaveno na 5000 opakování)
- Některé služby a možnosti zlepšení bezpečnosti jsou placené
- 2011 – únik dat???
- 2015 – už zase???

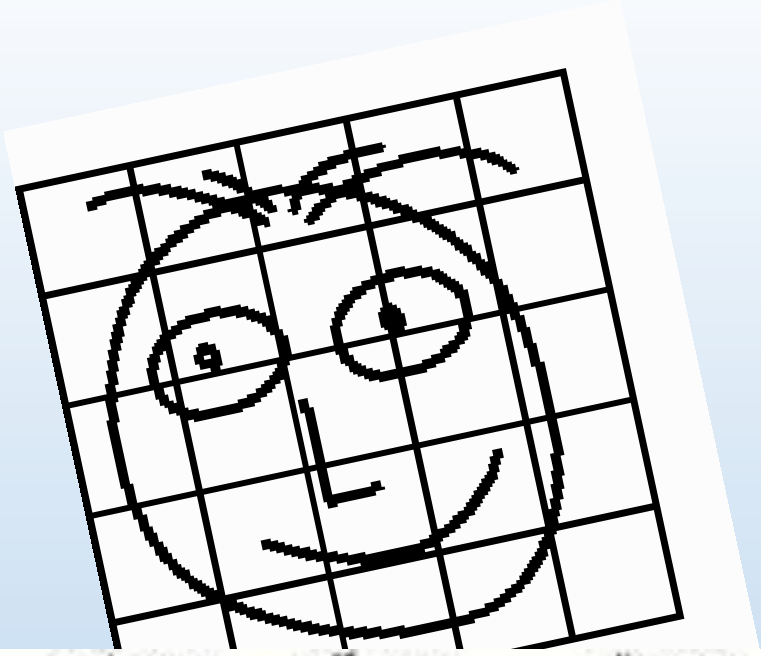

Password Database Encryption
Inputs
Process
Output
Opakuje se c-krát, c_{def} = 5000
Username (email address)
Master Password
Password database
SHA256 (Private Hash)
Salt
Username
Master Password
This hash created on the user side is the only thing that can decrypt the data blob.
All encryption is performed on the user side. Only the Encrypted Data Blog is sent to LastPass.
AES256 (Encryption)
Private Hash
Password database
The private hash is used as the key to encrypt the password database.
Encrypted Data Blob (password database)
Diagram by gee.is

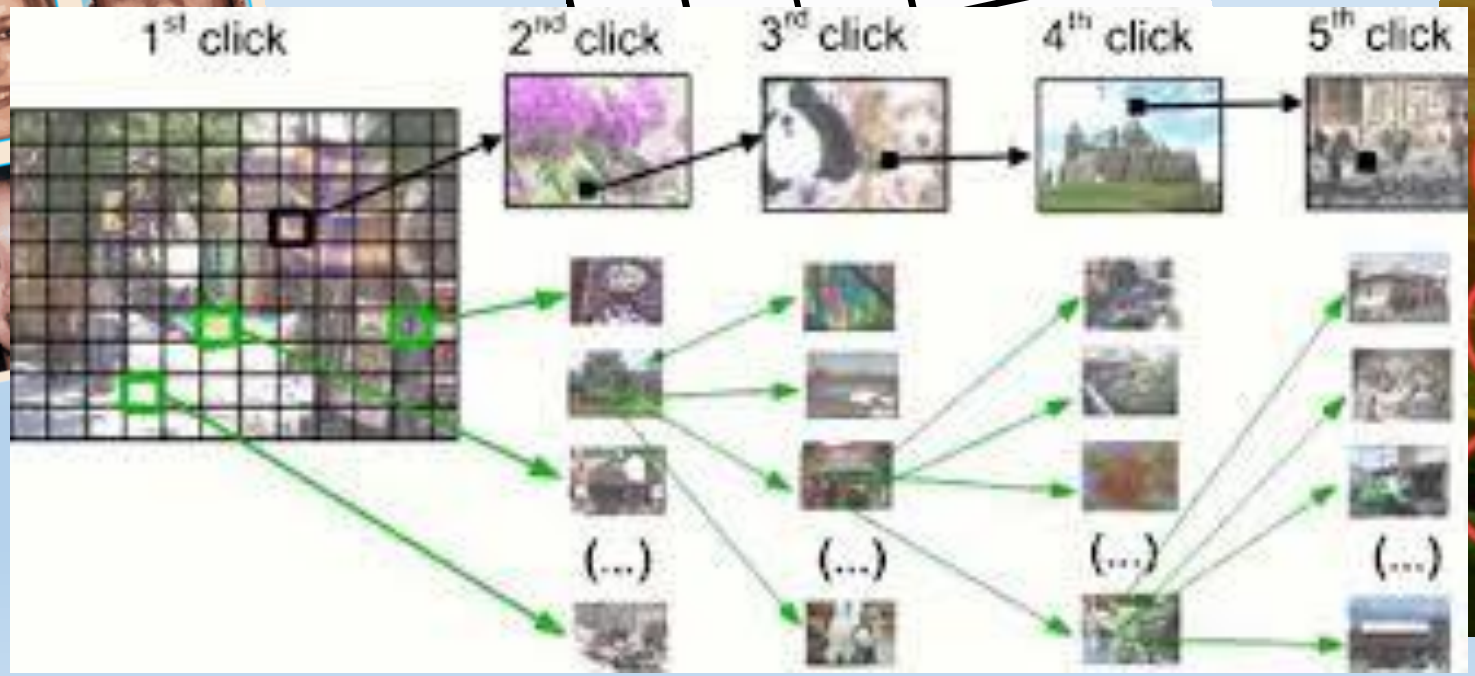
User Authentication Hash

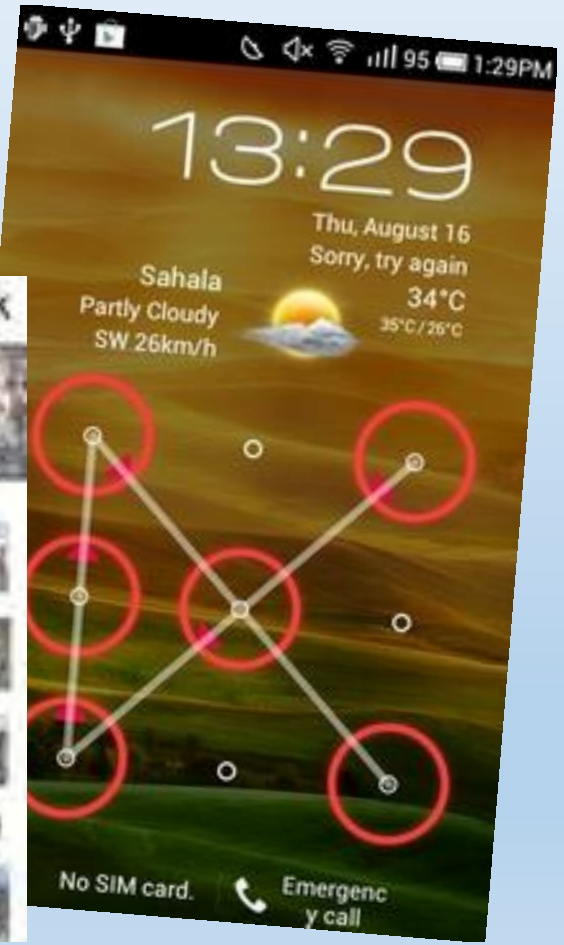


Grafická hesla





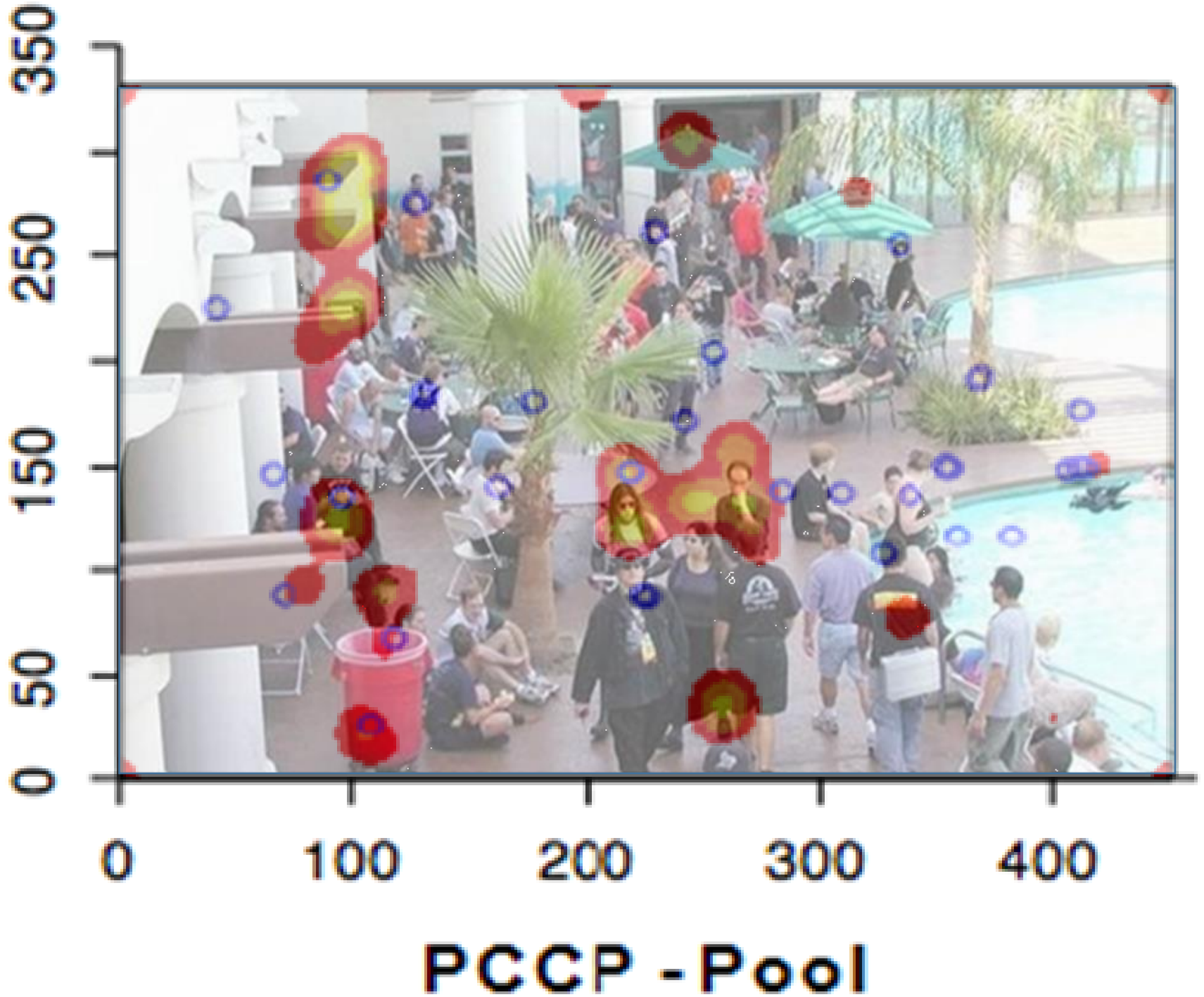




Grafická hesla

- PassFaces – heslo = 3 obličeje, každý je zobrazen společně s 8 dalšími
- Android‘s Pattern Lock – gesto, zamykání obrazovky
- Persuasive Cued Clickpoints – uživatel zvolí v určitém poli 5 bodů
  - různě zvolené body zobrazí různé obrázky
  - výměna obrázků = odolnost proti tzv. hotspotům
  - pole o velikosti 800x600 pixelů s 5 body = 8-místné heslo
  - nejvíce zvětšuje prostor klíčů počet bodů
  - Prostor klíčů = $((w * h)/t^2)^c$

  ($w*h$ = velikost obrázku, t^2 = povolená odchylka, c = počet bodů)

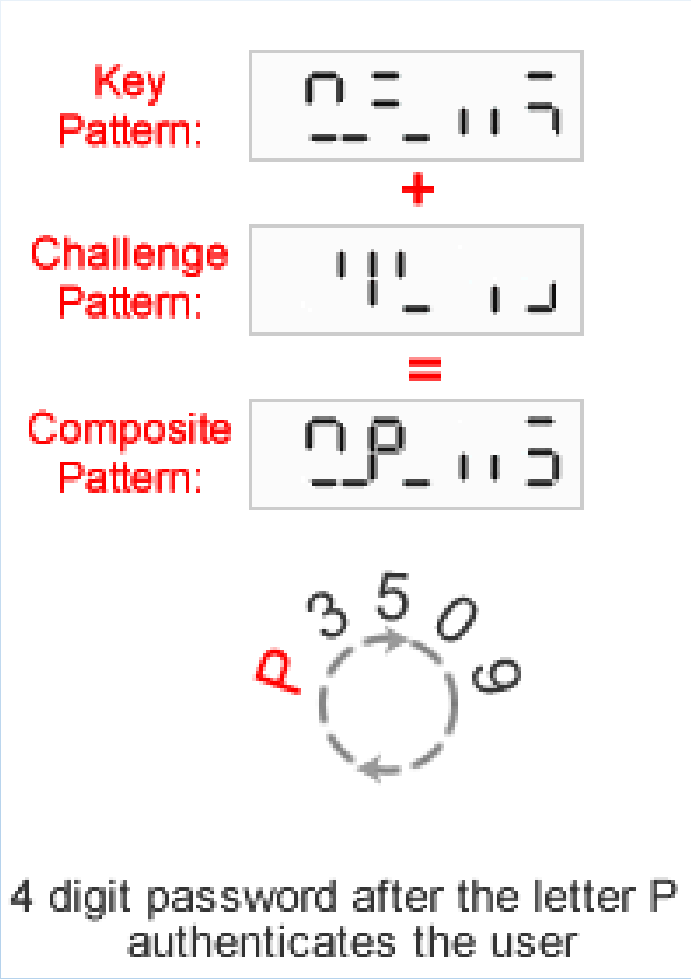

350
250
150
50
0
0
100
200
300
400
PCCP -Pool

Problém:

PassWindow

http://www.passwindow.com/

- Princip výzva-odpověď
- Např. pro bezpečnější online banking
- Odolnost proti malware
- Nepoužitelné pro lidi se špatným zrakem



4 digit password after the letter P authenticates the user

Další možnosti zabezpečení

- PIN + TAN, TAN – dodatečný kód, zasílán e-mailem (Německo, Rakousko)
- RSA SecurID – generátor kódů, nutno přepisovat
- Word association – výzva-odpověď, na slovo-výzvu reakce uživatelem určeným slovem-odpovědí (výzva: „Yellow,“ odpověď „Submarine“)
- Biometrická identifikace – čtečky otisků, skener duhovky, hlasu,…
- A mnoho dalších

Vlastní řešení

Závěr

- Nahrazením, nebo vylepšením hesel zpravidla něco obětujeme
- V lepším případě čas, nebo pohodlí (PassWindow, TAN)
- Peníze (rozšířená verze Lastpass, RSA securID)
- V horším případě zakrytím jedné slabiny odhalíme jinou (grafická hesla)
- LastPass – zajímavé řešení, potřeba zapamatovat si 1 složitější heslo
- Největší slabinou vždy bude uživatel

Zdroje:

- http://raidersec.blogspot.cz/2013/06/how-browsers-store-your-passwords-and.html
- http://www.svethardware.cz/ukladame-hesla-do-cloudu/37531-3
- https://helpdesk.lastpass.com/account-settings/general/password-iterations-pbkdf2/
- http://www.graemenoble.id.au/post/49072807017/lastpass-password-database-explanation
- https://www.internetsafetyproject.org/wiki/graphical-passwords

Děkuji za pozornost