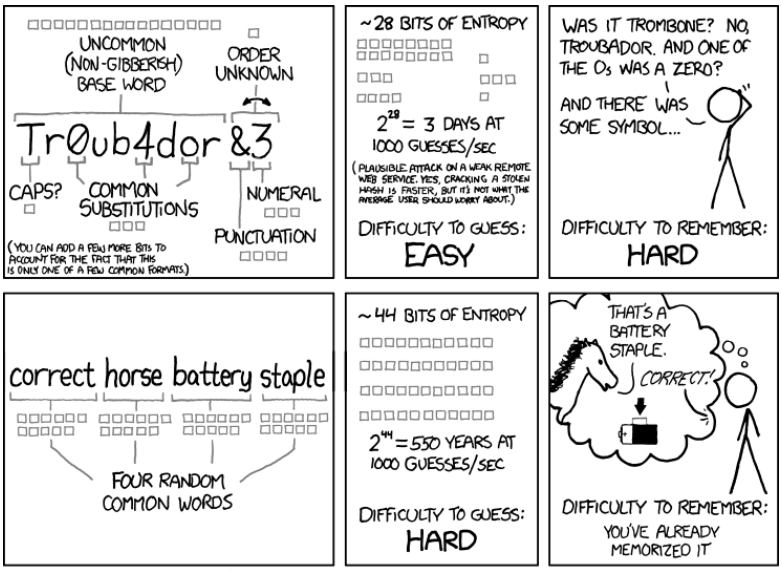
hcc!CompUsers
systemen en applicaties

Sterke wachtwoorden
25 maart 2023
Johan Swenker



https://xkcd.com/936/

Agenda

- Wat is authenticatie
- Wat zijn sterke wachtwoorden
- Echte willekeur ~ entropie
- Wachtwoorden kraken
- Wachtwoorden genereren (1)
- Wachtwoorden onthouden
- Wachtwoorden generen (2)
- Multifactor authenticatie

Wie ben ik

- Johan Swenker
- HCC-lid sinds 1980
- Lid van het Linux platform van CompUsers
- Netwerk en security architect bij een groot internationaal ICT bedrijf

Authenticatie

Bewijzen dat je bent wie je zegt dat je bent

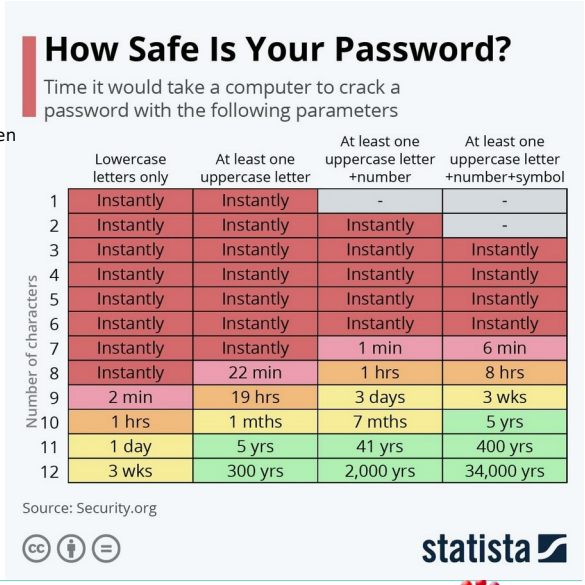
- Twee factor authenticate (2FA) 2 uit de volgende 3
  - Wat je weet ⇒ wachtwoord
  - Wat je hebt ⇒ hardware sleutel
  - Wat je bent ⇒ biometrie

- Slechte wachtwoorden
- Komen voor in de top 500 van de slechtste wachtwoorden allertijden
- http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

URL geeft de 500 meest gebruikre wachtwoorden

Sterke wachtwoorden

- Wachtwoorden die niet te kraken zijn
  - Zoek naar: password crack time
  - https://www.hivesystems.io/blog/are-your-passwords-in-the-green
- Mijn bank:
  - Wachtwoordlengte: 10 tot 20 tekens
  - Minimaal 1 hoofdletter, 1 kleine letter en 1 speciaal teken
  - Cijfers: 0 t/m 9
  - Letters: kleine letters (a t/m z) en hoofdletters (A t/m Z)
  - Speciale tekens: @ ! . $ % – of _
  - 70 verschillende tekens beschikbaar
- Voorbeeld ? : 123qwertyASDFG!
  - Een toetsenbordwandeling is **niet** willekeurig genoeg
- Voorbeeld ? : Tr0ub4dour%
  - Daar kom ik nog op terug



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

hcc!CompUsers systemen en applicaties

Zoeken naar `password crack time` levert vele plaatjes op, vergelijkbaar met het plaatje in de dia.

Wachtwoord Tr0ub4dour% is slecht en niet te onthouden, zie ook dia 14

Échte willekeur / entropie

- Mensen zijn niet willekeurig genoeg
- Computers zijn slechts pseudo willekeurig
- Dobbelstenen zijn perfect

- Berekende complexiteit ~ tijd die nodig is om te kraken
- 70 wachtwoorden van 1 teken ⇒ instantaan
- 70*70=4900 wachtwoorden van 2 tekens ⇒ instantaan
- 70*70*70*70*70*70*70*70*70*70 ~ 3 000 000 000 000 000 000 wachtwoorden van 10 tekens
- Snelheid grafische kaart 70 000 000 000 kraakpogingen per seconde ⇒ 1 jaar
- Wachtwoord van 9 tekens
  - 70 maal zo snel te kraken ⇒ binnen 1 week

- 70 ~ 64 = 2*2*2*2*2*2 ⇒ entropie is 6 bits
- 4900 entropie 12 bits
- 70^10 entropie 61 bits

hcc!CompUsers
systemen en applicaties

Entropie is het aantal factoren 2, dit is een truc om de getallen behapbaar te maken. Deze truc is vergelijkbaar met het aantal nullen in een getal.

Kraken

- Waarom aandacht op kraken?
- Time out bij 3 keer verkeerd wachtwoord
- Gegevenslek (leak)
  - Wachtwoorddatabase wordt publiek
  - Dus ook jouw wachtwoord
- https://en.wikipedia.org/wiki/List_of_data_breaches
- https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/
- https://haveibeenpwned.com/Passwords
  - aapnootmies
  - Genereer wachtwoord met firefox
- Versleuteld opgeslagen wachtwoorden
  - $ echo -n '123qwertyASDFG!' |md5sum
  - 4cf7fffd51034fa6f50dfa0d776c9854 -
  - $ echo -n '123qwertyASDFG!' |sha256sum
  - 7c77744c786b70a5cb0bed15284620eda83332dcc5463d5727560947bc8192c7

hcc!CompUsers
systemen en applicaties

1e URL lijst van datalekken (niet alleen wachtwoordlekken)
2e URL beschrijft een lijst met 8 miljard gelekte wachtwoorden
3e URL geeft aan of jouw wachtwoord al eens gelekt is. Opm. Geef je echte wachtwoord alleen aan deze site als je de site vertrouwt en/of de javascript gecontroleert hebt.
Probeer eens een wachtwoord als aapnootmies, en schrik hoeveel mensen zoiets simpels gebruiken.
md5sum en sha256sum zijn standaard methodes om gegevens te verhusselen.

Kraken met de grafische kaart

- Reden: laat de grafische kaart eens werken
  - watch nvidia-smi
  - /usr/bin/nvidia-settings
- Demo hashcat
  - cat crack2.hash
  - hashcat -m 1800 -a 3 crack2.hash 500_passwords.txt
  - hashcat -m 1800 -a 3 crack2.hash ?l?l?l?l?l -O 6 -w 2

hcc!CompUsers
systemen en applicaties

Linux commando's

watch nvidia-smi
toont continu de processen die op mijn grafische kaart uitgevoerd worden

nvidia-settings
toont continu de temperatuur van mijn grafische kaart

crack2.hash is een bestand met te kraken wachtwoorden (https://samsclass.info/123/proj10/crack2.hash)

hashcat is een wachtwoordkraker

500_passwords.txt is een bestand met 500 meest gebruikte wachtwoorden (https://samsclass.info/123/proj10/500_passwords.txt)

Wachtwoord hygiëne

- Wachtwoordherstelvragen
  - Meisjesnaam van je moeder
  - Naam van je eerste huisdier
- De antwoorden moeten ook sterke wachtwoorden zijn!
- In deze context is liegen verplicht!

- Van een vorige pagina:
  - Gegevenslek (leak)
    - Wachtwoorddatabase wordt publiek
    - Dus ook jouw wachtwoord **voor deze site**
- Aanvaller zal jouw gebruikersnaam met wachtwoord van site 1 proberen op site 2
- Elke website een ander wachtwoord
  - Totaal verschillend
- Hoe doe je dat?

Wachtwoord genereren

- 20 letters en cijfers:
  - $ pwgen -s 20 1
  - TJA31O0W4LvQBICx0SSx
- 20 letters, cijfers en bijzondere tekens
  - $ pwgen -sy 20 1
  - scse><g*|V6E?e(8C4{>
- Probleem 1 (mijn bank): slechts 8 bijzondere tekens @ ! . # $ % – of _
  - ASCII heeft 34 bijzondere tekens
  - Mijn bank verbiedt o.a. alle haakjes () {} [] <>
  - pwgen werkt niet
  - Slechte oplossing
    - pwgen voor 19 willekeurige tekens,
    - Gevolgd door het verplichte uitroepteken
    - 2 tot 6 bits entropie zijn verdwenen
  - Probleem 2: onthouden van TJA31O0W4LvQBICx0SS!

hcc!CompUsers
systemen en applicaties

pwgen is een wachtwoordgenerator (https://github.com/tytso/pwgen)

Wachtwoorden onthouden

- Opschrijven
- https://www.schneier.com/blog/archives/2005/06/write_down_your.html
- Bruce Schneier is een bekende security autoriteit
  - Wij zijn heel goed in het zorgvuldig bewaren van kleine stukjes papier.
  - Dus schrijf je wachtwoord op een klein stukje papier en bewaar dat
  - bij andere kleine maar waardevolle stukje papier: in je portefeuuile

- Wachtwoord-manager
  - Beheert wachtwoorden
  - Slaat wachtwoorden versleuteld op
  - Geeft wachtwoorden door via het klembord (copy/paste)
  - Versleuteling met een primair wachtwoord
  - Voorkomt dat malware bij de wachtwoorden kan
    - Primaire wachtwoord moet je telkens opnieuw intypen
    - Wachtwoord wordt snel weer uit het klembord verwijderd

hcc!CompUsers
systemen en applicaties

URL geeft het opschrijfdadvies van Bruce Schneier

Wachtwoord-manager in de browser

- Kun je de browser vertrouwen?
- Wil je de browser vertrouwen?
- Voor mijn bank niet, voor hccnet misschien wel
- Risico
  - Javascript, van te veel sites
    - Kan javascript bij de wachtwoorden
    - Ook als er een bug in browser zit
  - Vergeten van het primaire wachtwoord
    - Waar zit die knop in firefox?
- Browser ziet verschil mijnbank.nl en mijnbank.nl
  - `Lange ij als i j`
  - `Lange ij als één unicode karakter ij`

hcc!CompUsers
systemen en applicaties

ij is Unicode karakter (U+0132) zie ook https://nl.wikipedia.org/wiki/IJ_(digraaf)#Codering

Wachtwoord-manager als applicatie

- Er zijn heel veel wachtwoord-managers
  - Kosten, licentie, OS, etc op wikipedia
  - https://en.wikipedia.org/wiki/List_of_password_managers
- Losse applicatie beter dan in de browser?
  - Niet alle argumenten zijn steekhoudend
  - Voordeel of nadeel: Firefox kan niet bij de wachtwoorden van Chromium
  - Vaak: wachtwoorden synchroniseren over al je apparaten
    - Via de cloud van de leverancier
    - Dat is voor mij een nadeel

- Voorbeeld KeePassXC
  - Multiplatform
  - Slaat wachtwoorden lokaal op
  - Je moet zelf je KeePass wachtwoord-database synchroniseren
    - In eigen beheer via OwnCloud, NextCloud
    - Via DropBox, Google Drive, OneDrive
  - https://keepassxc.org/docs/#faq-cloudsync
  - Demo: keepassxc

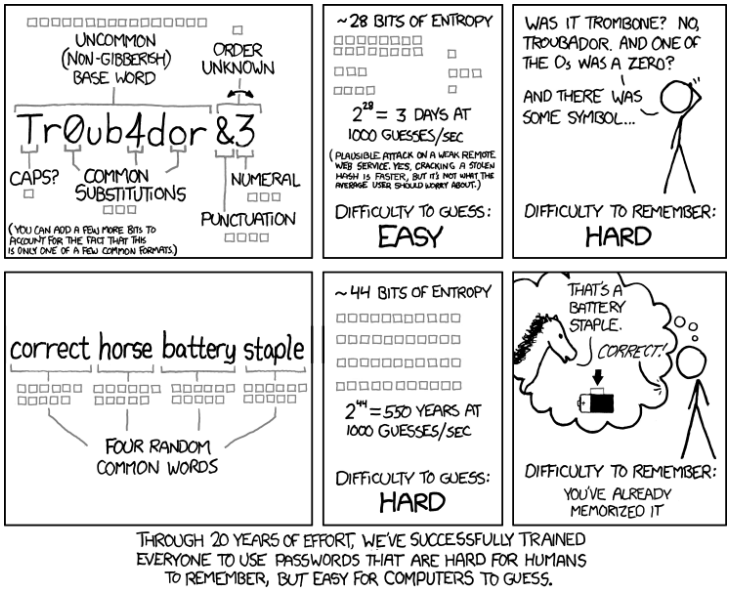
hcc!CompUsers
systemen en applicaties

1e URL geeft lijst met wachtwoordmanagers

2e URL geeft aan dat je KeePassXC met een standaard cloud-opslag-leverancier kunt/moet gebruiken

Wachtwoorden verzinnen XKCD

- Wachtwoord-manager (ook firefox)
- https://xkcd.com/936/ (10 augustus 2011)
- Xkcd is een webcomic over romantiek, sarcasme, wiskunde en taal
- Standaard vervangingen geven weinig entropie Tr0ub4dour% is geen goed wachtwoord
- Neem 6 tot 10 écht willekeurige woorden
  - Uit een lijst van bijvoorbeeld 7776 woorden
- $ xkcdpass
  - backlit devotedly haziness camisole sappiness animator
- 6 woorden uit 7776 is 78 bit entropie
- mijn bank eist minimaal 61 bit (✓)
- Mijn bank eist maximaal 20 tekens ( )



hcc!CompUsers
systemen en applicaties

URL geeft het plaatje op deze dia
Hier wordt het Tr0ub4dour% voorbeeld herhaalt

Wachtwoorden verzinnen diceware

- Dobbelstenen zijn willekeurig
- Neem een woordenlijst met 7776 woorden
  - https://el-tramo.be/diceware/diceware-wordlist-composites-nl.txt
- Gooi 5 keer met één dobbelsteen (7776 mogelijkheden)
  - Neem het woord wat de dobbelsteen aangeeft
  - Een keer gooien met 5 dobbelstenen is toch iets anders
- Doe dat 6 tot 10 keer

- Engelstalige website: https://diceware.dmuth.org/

11111 aai
11112 aaien
11113 aak
11114 aal
...
66663 zwijn
66664 zwik
66665 zwoel
66666 zwoor

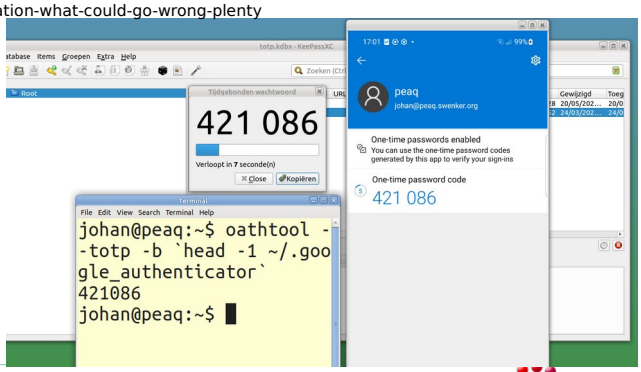
hcc!CompUsers
systemen en applicaties

1e URL geeft een Nederlandstalige woordenlijst voor gebruik met diceware. Een uittreksel van deze woordenlijst staat rechts op de dia.

2e URL toont het gooien van dobbelstenen om een Engelstalige wachtwoordzin te maken.

Multifactor authenticatie

- Gebruik een tweede factor, naast een wachtwoord
- SMS
  - Nooit bedoeld om veilig te zijn
  - Onveilig, gebruik een andere vorm van 2FA
  - Pcmag schrijft: Now if you have a username, cracked password, and phone number, you have a very good chance to get past 2FA.
  - https://www.pcmag.com/news/sms-based-multi-factor-authentication-what-could-go-wrong-plenty
- Authenticator app op de smartphone
  - TOTP: Time-based One Time Password
  - Gestandaardiseerd in internet RFC 6238
  - Veel implementaties beschikbaar
    - https://www.pcmag.com/picks/the-best-authenticator-apps
    - Google authenticator, Microsoft authenticator, ...
    - Ook KeepAssXC
- Demo TOTP
  - $ /snap/bin/scrcpy
  - $ google-authenticator



hcc!CompUsers systemen en applicaties

1e URL geeft artikel van pcmag waarin staat dat SMS geen goede tweede factor is voor 2FA
2e URL geeft review van vele authenticator apps

RFC 6238 is te vinden op https://www.ietf.org/rfc/rfc6238.txt

/snap/bin/scrcpy toont het scherm van een (met USB) aangesloten Android smartphone zie ook https://github.com/Genymobile/scrcpy

google-authenticator genereert en QR-code voor two factor authentication met TOTP

Plaatje:
* rechts (blauw) mijn smartphone via scrcpy.
* midden (grijs) TOTP window van KeePassXC
* links (licht geel) de uitvoer van een TOTP programma op de Linux-commandoregel

```
oathtool --totp -b `head -1 ~/.google_authenticator`
```

Samenvatting

- Goede wachtwoorden zijn
  - Allemaal verschillend
  - Lang
  - Écht willekeurig

- Wachtwoorden onthoud je
  - Met een wachtwoord-manager, desnoods in de browser
  - Een of twee belangrijke wachtwoorden: op papier in je portefeuille
- Maak regelmatig een backup van de wachtwoord-database!

- Wachtwoorden maak je
  - Met je wachtwoord-manager
  - Desnoods met een dobbelsteen
  - Nooit zelf verzinnen (geen standaard verwisselingen E ⇒ 3)