HANDLEIDING BEVEILIGDE PASWOORDEN

Versie 1.0 NL Frédéric Jadoul

een handleiding door

all2all

Moving Art Studio v.z.w.

all2all .beagent RIPE NCC Member

Table of Contents

Beveiligde paswoorden

Een 100% veilig paswoord bestaat niet. Alle paswoorden kennen een zekere graad van zwakte, min of meer in verhouding tot het aantal voorzorgen die genomen zijn door diegene die het gekozen heeft.

In de praktijk

Mensen hebben de neiging om dingen gemakkelijk te vergeten als ze niet direct verbonden zijn aan hun onmiddellijke reatliteit. Dat is misschien waarom er zoveel mensen zijn die gemakkelijk te vindbare paswoorden gebruiken om gegevens te beveiligen die niet verondersteld worden gezien of gebruikt te worden door anderen. De overwegingen die volgen zijn toepasbaar op ieder mogelijk gebruik van een paswoord, onafhankelijk van het feit of het nu gaat om een paswoord voor de tekst in een geheim bestand, een login om zich aan te melden op een discussieforum of op een Unix account, om uw Windows 200x machine op uw kantoor te openen of om geld over te schrijven vanop uw bankrekening.

In al deze gevallen worden de paswoorden gebruikt om toegang te verlenen tot informatie aan bevoegde personen en onbevoegde personen op een afstand te houden. Als uw paswoord wordt gebruikt zonder dat u er weet van hebt kunnen allerlei onaangename dingen gebeuren: financiëel verlies, verlies van gegevens, verlies in termen van merkimago, enz.

Aanvallen van het soort “dictionary attack”

Alle woorden die in een woordenboek staan zijn risico, onafhankelijk van de taal die u gebruikt. Het is wel zeker dat Engelse woorden of woorden in de moedertaal van het slachtoffer (als dat gekend is) gevaarlijker zijn dan bijvoorbeeld woorden in het Swahili. Op het internet kunt u gespecialiseerde woordenboeken vinden om paswoorden te vinden voor een applicatie die op een “brute force”-manier zal alle paswoorden één na één uitproberen.

Ook al kan men een zekere graad van veiligheid bekomen door hoofdletters met kleine letters af te wisselen (als dat mogelijk is), dan is dat nog niet echt een handicap voor dit soort aanval. Ook “paRAPlu” kan na genoeg pogingen in een zekere tijd gevonden worden.

Een Engels woordenboek bevat ongeveer 150 000 woorden. Als u variatie in hoofdletters/kleine letters toevoegt komt u aan ongeveer 15 miljoen woorden. Maar enkele seconden kunnen nodig zijn om het paswoord op “brute-force”-methode te vinden.

In 2002 werd een lijst van 10 000 accounts op een bestaande server geanalyseerd. Na 30 minuten werd 30% van de paswoorden ontdekt (zie Passwords: the weakest link?).

Persoonlijke gegevens

Houd er rekening mee dat paswoorden gebaseerd op persoonlijke gegevens (namen, voornamen, geboortedatum, telefoonnummer, film- of boekpersonnages, vrijetijdsbezigheden of passies van een gebruiker, zijn collega's, zijn familie enz.) nog zwakker zijn dan woorden die uit een woordenboek gekozen worden. Deze woorden kunnen min of meer gemakkelijk geraden worden.

In een studie uitgevoerd in 2001 bij 1200 Engelse werknemers, werd ontdekt dat bijna de helft van de geïnterviewden hun naam, namen van hun huisdieren of namen van familieleden gebruikten als paswoord. De anderen gebruikten namen van fictiehelden zoals Darth Vader of Homer Simpson (zie Homeland Insecurity).

Letterreeksen

Andere veelgebruikte paswoorden zijn letterreeksen van het tyme “azerty”, “qwerty” of “12345”, die makkelijk ingetikt kunnen worden. Deze paswoorden zijn ook zeer kwetsbaar aangezien ze zeer gekend zijn (er bestaan zelfs woordenboeken met enkel dit soort letterreeksen).

“Brute force”-aanvallen

Hedendaagse computers zijn zeer krachtig. Op dit moment zijn er gemakkelijk verkrijgbare systemen die meer dan 10 miljoen sleutelwoorden per seconde kunnen proberen. Bijvoorbeeld het RC5 coderingsalgoritme (die als vrij zwak gezien wordt). Als men dit cijfer vergelijkt met het aantal paswoorden van 6 tekens (inclusief hoofdletters en kleine letters) kunt u gemakkelijk de tijd berekenen die het neemt om een paswoord te vinden op deze manier die men “brute force” noemt.

52 mogelijke karakters tot de 6de macht (lengte paswoord) = ongeveer 20 miljard combinaties

20 miljard / 10 miljoen = 2.000 seconden = ongeveer een halfuur.

We kunnen 2 gevolgen trekken uit deze berekening:

- korte paswoorden zijn zwak
- paswoorden genomen uit een beperkte verzameling van karakters (alleen cijfers of alleen kleine letters) zijn zwakker dan die die genomen zijn uit een grotere verzameling (grote letters, cijfers, kleine letters, speciale karakters).

Conclusie

Samengevat: paswoorden moeten aan volgende voorwaarden voldoen om een acceptabele relatieve veiligheid te bieden:

- De paswoorden moeten lang zijn (minstens 8 karakters)
- De paswoorden moeten verschillende soorten tekens bevatten (letters, cijfers, speciale tekens)
- De paswoorden mogen onzin zijn

De volgende methoden kunnen u helpen om paswoorden te vinden die een adequate veiligheid bieden maar die u toch min of meer gemakkelijk kunt onthouden dan een willekeurige tekenreeks:

- Twee woorden verbinden (door grote en kleine letters dooreen te gebruiken) met een speciaal teken (bijvoorbeeld : "4aT&hOme", "b1G#seCreT", "zEIt+f0rM")
- De eerste letters van een zin gebruiken samen met speciale tekens en cijfers (bijvoorbeeld : "Spau2rP!" voor "Some people are unable to remember passwords!")
- Betekenisloze woorden gebruiken die bestaan uit uitspreekbare stukken gecombineerd met speciale tekens en cijfers

(bijvoorbeeld : "dOsil?Ar0n")

 Gebruik deze voorbeelden niet, vind zelf uw paswoord uit

Waarom zelfs deze voorzorgen niet volstaan

Ingewikkelde paswoorden zijn moeilijker te onthouden dan eenvoudige. Zelfs als het moeilijk te weerstaan is om ze op te schrijven en in uw portefeuille te steken of op uw scherm te kleven, zou het beter zijn om ze alleen in uw geheugen bij te houden. Zelfs als u uw paswoord zeer voorzichtig gekozen hebt zullen anderen zich geen moeite besparen als ze het gewoon kunnen lezen op uw scherm, en veel ongemak kan vermeden worden als uw portefeuille nooit per ongeluk in de handen van iemand onbekend terechtkomt die informatie bekomt om toegang te krijgen tot gegevens van uw organisatie. Maak geen gebruik van uw paswoorden op een niet betrouwbare computer.

Een andere goede manier om paswoorden onveilig te maken is altijd hetzelfde te gebruiken voor verschillende accounts. Als een beheerder van een discussiesite uw paswoord kent, dan kan hij hopen (als hij een beetje van slechte wil is) dat u hetzelfde pasoord gebruikt op het netwerk van uw organisatie. Dit is waarom paswoorden maar een enkele keer mogen gebruikt worden en dikwijls moeten veranderd worden.

Houd er ook rekening mee dat paswoorden soms op een onbeschermde manier over het internet of op het internet netwerk van uw organisatie verstuurd worden. Ze reizen in leesbare tekst en kunnen onderschept worden overal op de communicatielijn. Gebruik nooit die paswoorden een tweede keer.

Het is sterk aangeraden om niemand in deze materie te vertrouwen. Geef dus ook uw niet uw paswoord aan een vriend voor het geval u het zou vergeten of om toegang tot bepaalde gegevens te delen.

Versions

Version number	Modifications	Author
1.0 NL	Original version	Frédéric Jadoul
1.0 FR	Traduction	Frédéric Jadoul
1.0 EN	Translation pdf NL → odt EN	Patrick Brunswyck
1.0 NL	Conversion pdf NL → odt NL	Patrick Brunswyck

page	**Modifications**
first	Added Cover all2all GNU Free Documentation License
last	Versions and Modifications
4	Warning sign in table