Die Kunst ein starkes Passwort zu finden und zu schützen

Stefan Schumacher

Magdeburger Institut für Sicherheitsforschung

Brandenburger Linux-Infotag

Über mich

- Berater für Unternehmenssicherheit mit Schwerpunkt auf Social Engineering, Security Awareness und Counter Intelligence
  `www.Kaishakunin.com`
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  `www.sicherheitsforschung-magdeburg.de`
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung im Meine Verlag
  `www.wissens-werk.de/index.php/mjs`

Übersicht

1. Motivation
2. Was gefährdet mein Passwort?
3. Sicherheitsregeln
4. Passwortgenerierung
5. Zusammenfassung

1 Motivation

2 Was gefährdet mein Passwort?

3 Sicherheitsregeln

4 Passwortgenerierung

5 Zusammenfassung

Wo ist das Problem?

- Passwort: *das* Authentifizierungsmerkmal schlechthin
- *der* Schlüssel zu einem Konto/System
- leider häufig unterschätzt
- interessanter Angriffspunkt
  - sowohl technischer Mittel (Wörterbuchangriffe, Tastaturrekorder)
  - als auch sozialer (Social Engineering)

Wo ist das Problem?

- Passwort: *das* Authentifizierungsmerkmal schlechthin
- *der* Schlüssel zu einem Konto/System
- leider häufig unterschätzt
- interessanter Angriffspunkt
  - sowohl technischer Mittel (Wörterbuchangriffe, Tastaturrekorder)
  - als auch sozialer (Social Engineering)
- Hinweise zur Erzeugung und zum Gebrauch von Passworten
- sowohl sozialer als auch technischer Natur

Wo ist das Problem?

- Passwort: *das* Authentifizierungsmerkmal schlechthin
- *der* Schlüssel zu einem Konto/System
- leider häufig unterschätzt
- interessanter Angriffspunkt
  - sowohl technischer Mittel (Wörterbuchangriffe, Tastaturrekorder)
  - als auch sozialer (Social Engineering)
- Hinweise zur Erzeugung und zum Gebrauch von Passworten
- sowohl sozialer als auch technischer Natur

1 Motivation

2 Was gefährdet mein Passwort?

3 Sicherheitsregeln

4 Passwortgenerierung

5 Zusammenfassung

soziale Ebene? technische Ebene?

- technische Ebene: alles was irgendwie mit Strom zu tun hat und wo man im Idealfall gegentreten kann
- soziale Ebene: Schnittstellen und Protokolle des menschlichen Miteinanders
- leider nicht debugbar

soziale Ebene? technische Ebene?

- technische Ebene: alles was irgendwie mit Strom zu tun hat und wo man im Idealfall gegentreten kann
- soziale Ebene: Schnittstellen und Protokolle des menschlichen Miteinanders
- leider nicht debugbar
- *»If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology« - Bruce Schneier*
- oder: Man kann soziale Probleme nicht mit technischen Mitteln lösen

soziale Ebene? technische Ebene?

- technische Ebene: alles was irgendwie mit Strom zu tun hat und wo man im Idealfall gegentreten kann
- soziale Ebene: Schnittstellen und Protokolle des menschlichen Miteinanders
- leider nicht debugbar
- *»If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology« - Bruce Schneier*
- oder: Man kann soziale Probleme nicht mit technischen Mitteln lösen

http://www.landschaftsmuseum.de/Bilder/Faustkeil_URO-2.jpg

Deus Ex Machina

- Verbindungsübernahme oder Abhörmaßnahmen
  - Kryptographie (SSH, SSL, VPN, GPG ...)
  - vertrauenswürdige Kanäle
- Klartextpasswörter
  - Dienste austauschen (telnet, rsh, ftp $\rightsquigarrow$ ssh)
- Tastaturrekorder, Wanzen, Kameras
  - Rechner und Umgebung prüfen
  - Sichtschutz
- Kompromittierende Strahlung
  - gewollte Strahlung (Wlan, Bluetooth, IrDa) eingrenzen
  - Schirmung (Faradayscher Käfig, Hühnerdraht)
  - Kryptographie

Was ist Social Engineering

- jeder hält sich für unfehlbar und unbetrügbar
- darum funktioniert Betrug so wunderbar
- Social Engineering: Maßnahmen, um Menschen zu hacken, statt Maschinen
- oder schlicht: Trickbetrug
- Stefan Schumacher (2010)
  Psychologische Grundlagen des Social-Engineering
  in: *Die Datenschleuder. Das wissenschaftliche Fachblatt für den Datenreisenden*
  S. 52-59, 2010, Chaos Computer Club Hamburg, ISSN: 0930-1054

Sicherheitsstrategie

- Verteidigung in der Tiefe: Verwundbare Teile des Netzwerkes abschotten und sichern
- Physikalischen Zugriff auf Rechner unterbinden.
- Rechte der Benutzer soweit es geht einschränken, dabei aber natürlich nicht übertreiben. Zu starke Einschränkungen werden gerne umgangen.
- Benutzer unbedingt über Social-Engineering-Angriffe informieren und von Gegenmaßnahmen in Kenntnis setzen.
- Proaktive Passwortprüfungen
- rechtliche Maßnahmen (Abmahnungen, Kündigungen etc.) gegen Verstöße

1 Motivation

2 Was gefährdet mein Passwort?

3 Sicherheitsregeln

4 Passwortgenerierung

5 Zusammenfassung

Feind hört mit!

- Passwörter müssen unbedingt geheimgehalten werden!
- nicht weitersagen
- nicht aufschreiben

Wie werden Passwörter gespeichert?

- Passwörter im Klartext können einfach ausgelesen werden
- Passwörter werden *gehasht*
- Mathematische Einwegfunktion:
  Hash über Passwort bilden ist einfach
  Passwort aus Hash rekonstruieren ist schwer
- Hash kann nicht zurückgerechnet werden
- CRC32, MD5, SHA1, RMD160, Blowfish ...

```
passworttest:$1$Di2VQknM$Vfbi9OkGZKN5Wxi0ypZeT1:
1007:100::0:0::/home/passworttest:/bin/csh
```

Wie werden Passwörter gespeichert?

- Passwörter im Klartext können einfach ausgelesen werden
- Passwörter werden *gehasht*
- Mathematische Einwegfunktion:
  Hash über Passwort bilden ist einfach
  Passwort aus Hash rekonstruieren ist schwer
- Hash kann nicht zurückgerechnet werden
- CRC32, MD5, SHA1, RMD160, Blowfish ...

```
passworttest:$1$Di2VQknM$Vfbi9OkGZKN5Wxi0ypZeT1:
1007:100::0:0::/home/passworttest:/bin/csh
```

Wörterbuchangriffe

- Passworthashes können zwar nicht erraten, aber verglichen werden
- Passwortdatei stehlen
- Hash auf Wörterbuch anwenden
- erzeugte Hashes mit erbeuteter Liste vergleichen
- Treffer heißt, Passwort geknackt
- Rainbowtables mit vorberechneten Hashes
- Thomas Roth: SHA-1-Hash aller 1-6 stelligen Passwörter erstellt, nutzte die GPU in Amazon Cloud Services, Dauer 50 Minuten, Kosten: 2 Euro

Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfuegbare Buchstaben}^{\textit{Passwortlaenge}}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende

Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfuegbare Buchstaben}^{\textit{Passwortlaenge}}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40\ \textit{Minuten}$
- $(99^{10}/432.000.55)/365000 \approx 570$ Tausend Jahrtausende

Wörterbuchangriffe

Kombinatorik

- fröhliches Passwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfuegbare Buchstaben}^{\textit{Passwortlaenge}}$
- 26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$
- 99 Buchstaben, 10 Stellen: $99^{10} = 90.438.207.500.880.449.001$
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40$ *Minuten*
- $(99^{10}/432.000.55)/365000 \approx 570$ Tausend Jahrtausende

Wörterbuchangriffe

Gegenmaßnahme: Passwortwechsel

- zweischneidiges Schwert
- technisch erzwingbar, aber umgehbar (Post-It)
- überhaupt notwendig? (570 Tausend Jahrtausende)
- Wenn Passwort sicher, eigentlich nicht
- Ausspähen (Shoulder Surfing)?

Wörterbuchangriffe

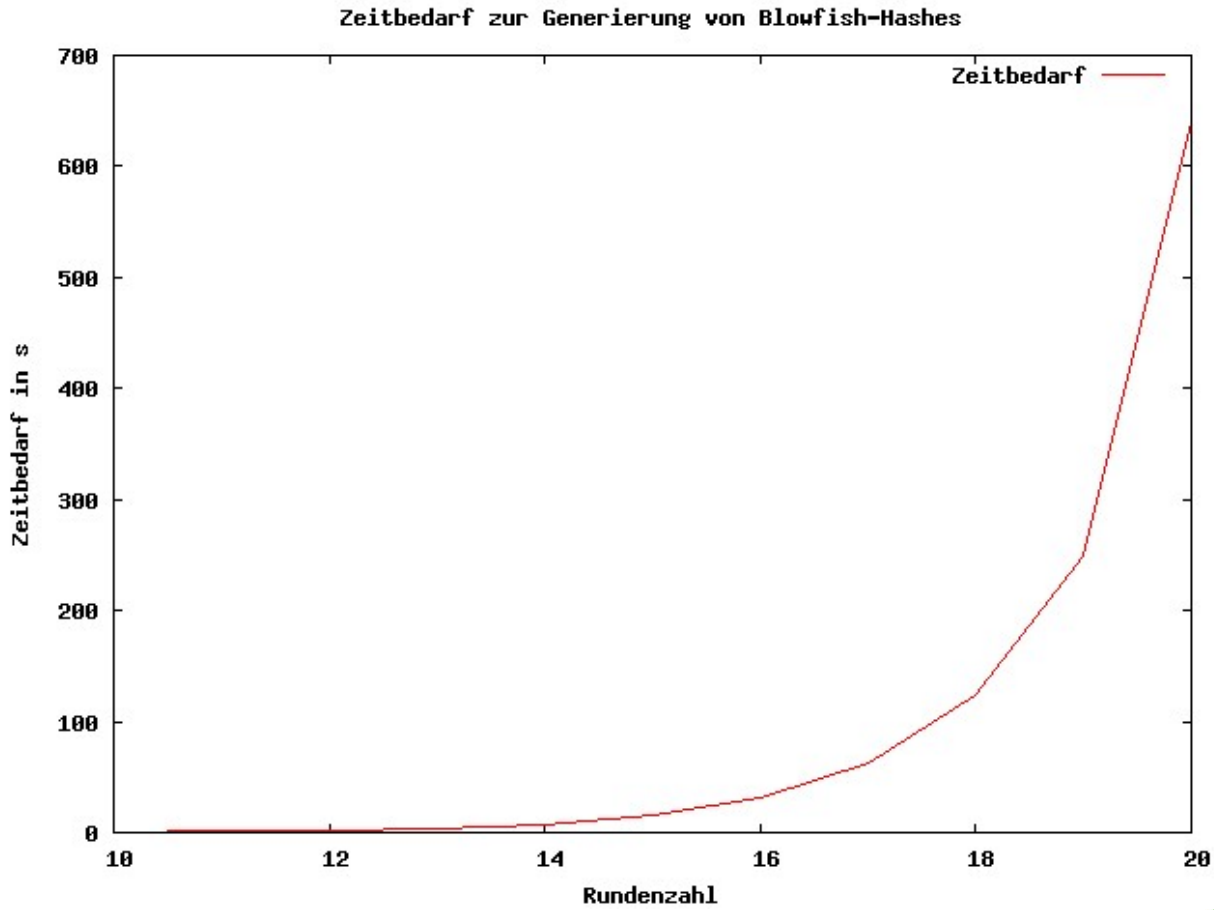
Gegenmaßnahme: Passwortwechsel

- zweischneidiges Schwert
- technisch erzwingbar, aber umgehbar (Post-It)
- überhaupt notwendig? (570 Tausend Jahrtausende)
- Wenn Passwort sicher, eigentlich nicht
- Ausspähen (Shoulder Surfing)?

Wörterbuchangriffe

Gegenmaßnahme: langsamer Hash, hier: Blowfish

Runden	Zeit
10	0.48s
11	0.97s
12	1.92s
13	3.84s
14	7.68s
15	15.36s
16	31.42s
17	61.95s
18	123.06s
19	248.31s
20	639.28s



Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

1 Motivation

2 Was gefährdet mein Passwort?

3 Sicherheitsregeln

4 Passwortgenerierung

5 Zusammenfassung

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ WdgWg,EFFzs.-FS,1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Wörter und Zahlen mischen:
  *R*1*i*2*n*3*g*4*p*5*a*6*r*7*a*8*b*9*e*10*l*
  2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
  GmoitatrhhoplEd

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Wörter und Zahlen mischen:
  *R*1*i*2*n*3*g*4*p*5*a*6*r*7*a*8*b*9*e*10*l*
  2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
  Gmoitatrhhoplled
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Wörter und Zahlen mischen:
  *R*1*i*2*n*3*g*4*p*5*a*6*r*7*a*8*b*9*e*10*l*
  2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
  Gmoitatrhhopled
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Wörter und Zahlen mischen:
  *R*1*i*2*n*3*g*4*p*5*a*6*r*7*a*8*b*9*e*10*l*
  2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
  Gmoitatrhhopled
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen

Passwörter automatisch generieren

- shuffle(1): zufällig permutierte Liste der Argumente
- `$shuffle -0 -p 4 0 1 2 3 4 5 6 7 8 9`
  `6492`
- NIST FIPS PUB 181: Standard for Automated Password Generator (APG)

Passwörter automatisch generieren

- shuffle(1): zufällig permutierte Liste der Argumente
- `$shuffle -0 -p 4 0 1 2 3 4 5 6 7 8 9`
  `6492`
- NIST FIPS PUB 181: Standard for Automated Password Generator (APG)
- apg(1), pkgsrc/security/apg, implementiert den Standard
- generiert zufällige und aussprechbare Passwörter

Passwörter automatisch generieren

- shuffle(1): zufällig permutierte Liste der Argumente
- `$shuffle -0 -p 4 0 1 2 3 4 5 6 7 8 9`
  `6492`
- NIST FIPS PUB 181: Standard for Automated Password Generator (APG)
- apg(1), pkgsrc/security/apg, implementiert den Standard
- generiert zufällige und aussprechbare Passwörter

Apg

10 aussprechbare Passwörter der Länge 8 - 12

```
$ apg -n 10 -a 0 -m 8 -x 12
DahyRijHypjo
wrisEij8
Nuphyeulvuk
itsAcugHyd9
kribazGuc
Ot0knelun
Elon!Quow.
yulWebgie
syflijyujIg
tubemdor
```

Apg

- Zufallspasswörter der Länge 10-14
- aus Ziffern, Sonderzeichen, großen und kleine Buchstaben aber ohne ”0”, ”1”, ”2”, ”3”
- ohne Vorkommen in »verbotenePasswörter«
- mit Zufallszahlen aus shuffle(1) als Initialisierungsvektor

```
$ find /etc/ | xargs md5 > /dev/null &
$ apg -m 10 -x 14 black-M SNCL -E 0123 \
  -r /home/stefan/verbotenePasswörter \
  -c `shuffle -0 -p 8 0 1 ... 8 9 a b c ... X Y Z`
5GapsUrEet=
ral+opeapKawf4
EujOtEpOrp;Om8
8ofCotpyulyuf.
devav5KriWeb<
```

Multifaktor-Authentifikation

1 Motivation

2 Was gefährdet mein Passwort?

3 Sicherheitsregeln

4 Passwortgenerierung

5 Zusammenfassung

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!
- Verwenden Sie nicht überall das selbe Passwort!

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!
- Verwenden Sie nicht überall das selbe Passwort!
- Wechseln Sie Ihre Passwörter!

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!
- Verwenden Sie nicht überall das selbe Passwort!
- Wechseln Sie Ihre Passwörter!

Sicherheitsforschung-Magdeburg.de
youtube.de/sicherheitsforschung

Noch Fragen?

stefan.schumacher@
sicherheitsforschung-magdeburg.de

9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF