Betrachtungen aus der Stille
oder:
Die Kunst ein starkes Paßwort zu finden und zu schützen

Stefan Schumacher

www.net-tex.de
stefan@net-tex.de
PGP:0xB3FBAE33

Id: starke-passwoerter-vortrag.tex,v 1.7 2008/03/01 07:05:54 stefan Exp

9. Chemnitzer Linux-Tage 2008, 2008/03/01

Teil I

Motivation

Wo ist das Problem?

- Paßwort: *das* Authentifizierungsmerkmal schlechthin
- leider häufig unterschätzt
- interessanter Angriffspunkt
  - sowohl technischer Mittel (Wörterbuchangriffe, Tastaturrekorder)
  - als auch sozialer (Social Engineering)

Wo ist das Problem?

- Paßwort: *das* Authentifizierungsmerkmal schlechthin
- 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
- 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

Teil II

Was gefährdet mein Paßwort?

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

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

- Deus Ex Machina? Nein – Ich bin Gott.
- jeder hält sich für unfehlbar und unbetrügbar
- darum funktioniert Betrug so wunderbar
- Social Engineering: Maßnahmen, um Menschen zu hacken, statt Maschinen
- oder schlicht: Trickbetrug
- WarGames mit Matthew Broderick,
  Der Coup mit Robert Redford und Paul Newman
  Kevin Mitnick The Art of Deception

Schutz vor Social Engineering

- Brain v1.0
- Aufklärung (es gibt da wen, der will dir böses tun)
- umfassende Sicherheitsrichtlinie

Teil III

Technische Details und Paßwortgenerierung

Kombinatorik

- fröhliches Paßwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfügbare Buchstaben}^{\textit{Paßwortlänge}}$
- 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

Kombinatorik

- fröhliches Paßwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfügbare Buchstaben}^{\textit{Paßwortlänge}}$
- 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

Kombinatorik

- fröhliches Paßwortraten: alle Kombinationen probieren
- $\textit{Anzahl Kombinationen} = \textit{verfügbare Buchstaben}^{\textit{Paßwortlänge}}$
- 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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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* oder 2*L*2*e*0*s*1*s*1*i*7*n*2*g*9

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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* oder 2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen 1.7 ,
  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* oder 2*L*2*e*0*s*1*s*1*i*7*n*2*g*9
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`

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
OtOknelun
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 -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<
```

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 -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<
```

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 -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<
```

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 -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<
```

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 -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<
```