```
CentOS release 5.5 (Final)
Kernel 2.6.18-194.32.1.el5 on an i686

tuxbox login: root
Password: _
```

Mario Lorenz

mario.lorenz@guug.de

Chemnitzer Linux-Tage 2011

Inhalt

- Benutzer-Authentifizierung: Grundlagen
- Passwörter: Verfahren, Stärken, Schwächen
- Einmal-Passwörter (OTP)
- Tokens
- Einrichtung und Verwendung unter Linux

- Zusammenfassung

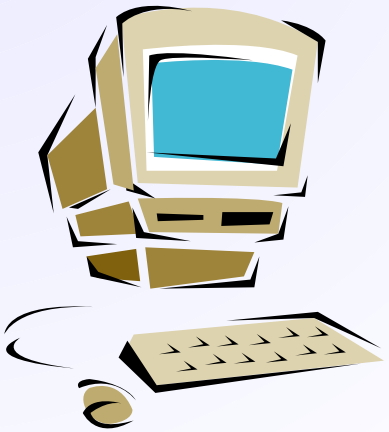
Aufgaben für Andere ausführen

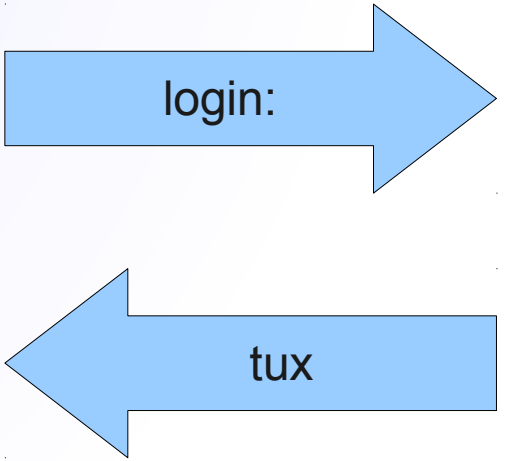
Vor Ausführung der Tätigkeit prüfen:

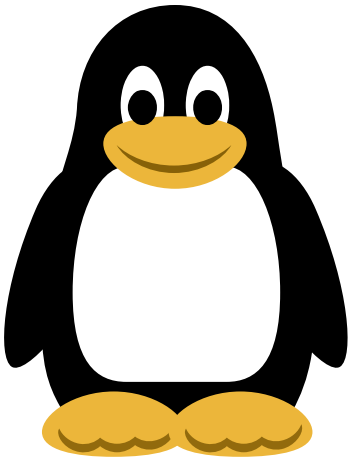
- Identifizierung (Wer?)
- Authentifizierung (Ist er es wirklich)?
- Authorisierung (Darf er das?)

- Davor/danach: Accounting (Protokollierung)

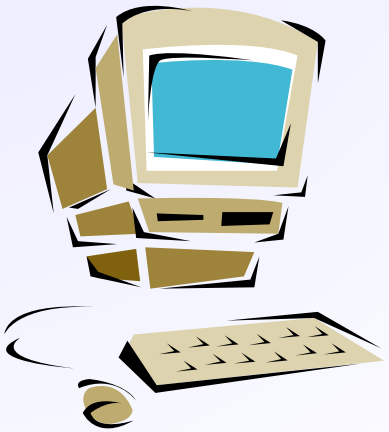
Identifizierung





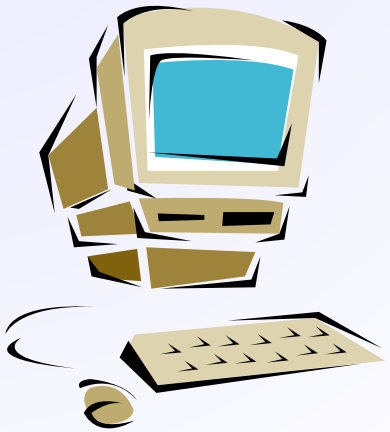


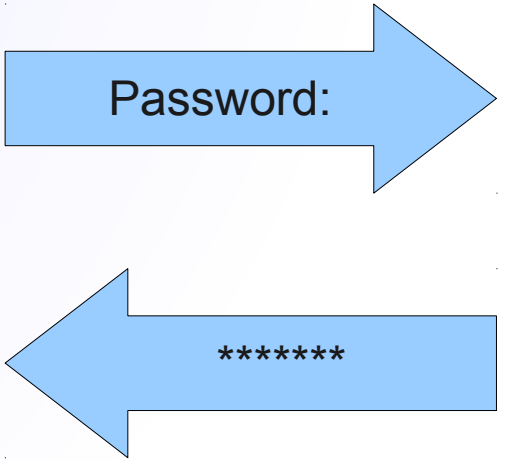
Authentifizierung

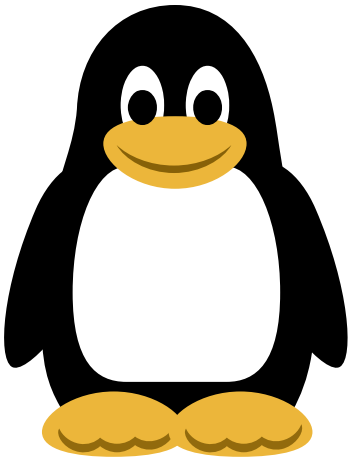


tux

Authentifizierung







Authorisierung

```
[tux@tuxbox /projects]$ ls -l
drwx------   2 beastie beastie  4096 Mar 12 08:33 world_domination_plans
[tux@tuxbox /projects]$ ls -l wold_domintion_plans
ls: world_domination_plans: Permission denied
[tux@tuxbox /projects]$
```

Accounting

(aus http://xkcd.com/838/)

Methoden der Authentifizierung

- Direkte Authentifizierung („Erkennen“)
- Indirekte Authentifizierung: Trusted Third Party
- Fordern eines Identitätsbeweises
  - Beweis durch Können
  - Beweis durch Besitz
  - Beweis durch Wissen
  - Beweis durch biometrisches Merkmal

Probleme

- Unzuverlässigkeit der Methode
- Spezielle Eingabegeräte oder Schnittstellen
- Spezielle Software
- Vertrauen in entfernte Terminals

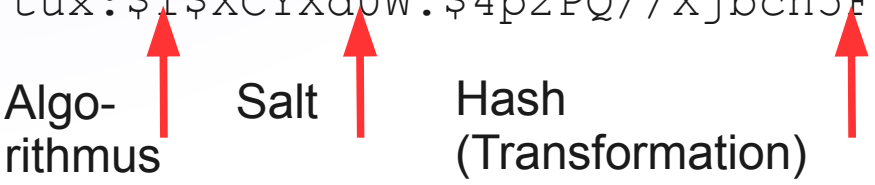
Passwörter

- Beweis durch Wissen
- Einfache Eingabemöglichkeit
- Protokoll:
  Nutzer gibt geheime Zeichenfolge ein
  a) Rechner vergleicht Zeichenfolge mit gespeicherter Kopie
  b) Rechner vergleicht Transformation der Zeichenfolge mit gespeicherter Transformation
- Variante: Challenge-Response

Passwörter unter Linux

/etc/shadow

```
ntp:!!:14315:0:99999:7:::
nscd:!!:14315:0:99999:7:::
vcsa:!!:14315:0:99999:7:::
rpc:!!:14315:0:99999:7:::
rpcuser:!!:14315:0:99999:7:::
nfsnobody:!!:14315:0:99999:7:::
named:!!:14315:0:99999:7:::
sshd:!!:14315:0:99999:7:::
dovecot:!!:14315:0:99999:7:::
webalizer:!!:14315:0:99999:7:::
squid:!!:14315:0:99999:7:::
pcap:!!:14315:0:99999:7:::
haldaemon:!!:14315:0:99999:7:::
xfs:!!:14315:0:99999:7:::
tux:$1$XCYXd0W.$4p2PQ//Xjbcn5FP2qtS/60:15047:0:99999:7:::
```



Ideale Passwörter

- einfach zu merken / nicht zu vergessen
- nicht zu erraten (hinreichend komplex)
- einzigartig (nicht mehrmals verwendet)
- regelmäßig geändert
- geheim

Grenzen

- Anzahl der Passwörter pro Person ?
- … nicht aufgeschrieben ?
- … nicht im Browser gespeichert ?
- … nicht mehrmals verwendet ?

- Sichere Client-Umgebung ?
- Abhörsichere Verbindung ?

Fallback-Anforderungen

- Compromize-Evident
- Leicht änderbar

Einmalpasswörter

- Passwort nur einmal gültig
- Nächster Authentifizierungsvorgang erfordert neues Passwort
- Passwörter sind auf Liste aufgeschrieben

  → Beweis durch Besitz
- Liste muss geheim bleiben
  - Sicher aufbewahren
  - Nicht in Rechner (oder Web-Dienste) eingeben
- Ergänzung durch herkömmliches Passwort („PIN“)

Stand der Technik

- Generierung mit Hilfe von Tokens

Bild: Mateusz Adamowski/WikiMedia

Tokens

- Kleine Scheckkarten/Schlüsselanhänger
- Vertrauenswürdiges Rechnersystem
- Schlüsselmaterial in Token gespeichert
- Token berechnet gültiges Passwort
- Unmöglich auszulesen („Tamper-Proof“)
- Vergossen („Tamper-Evident“)

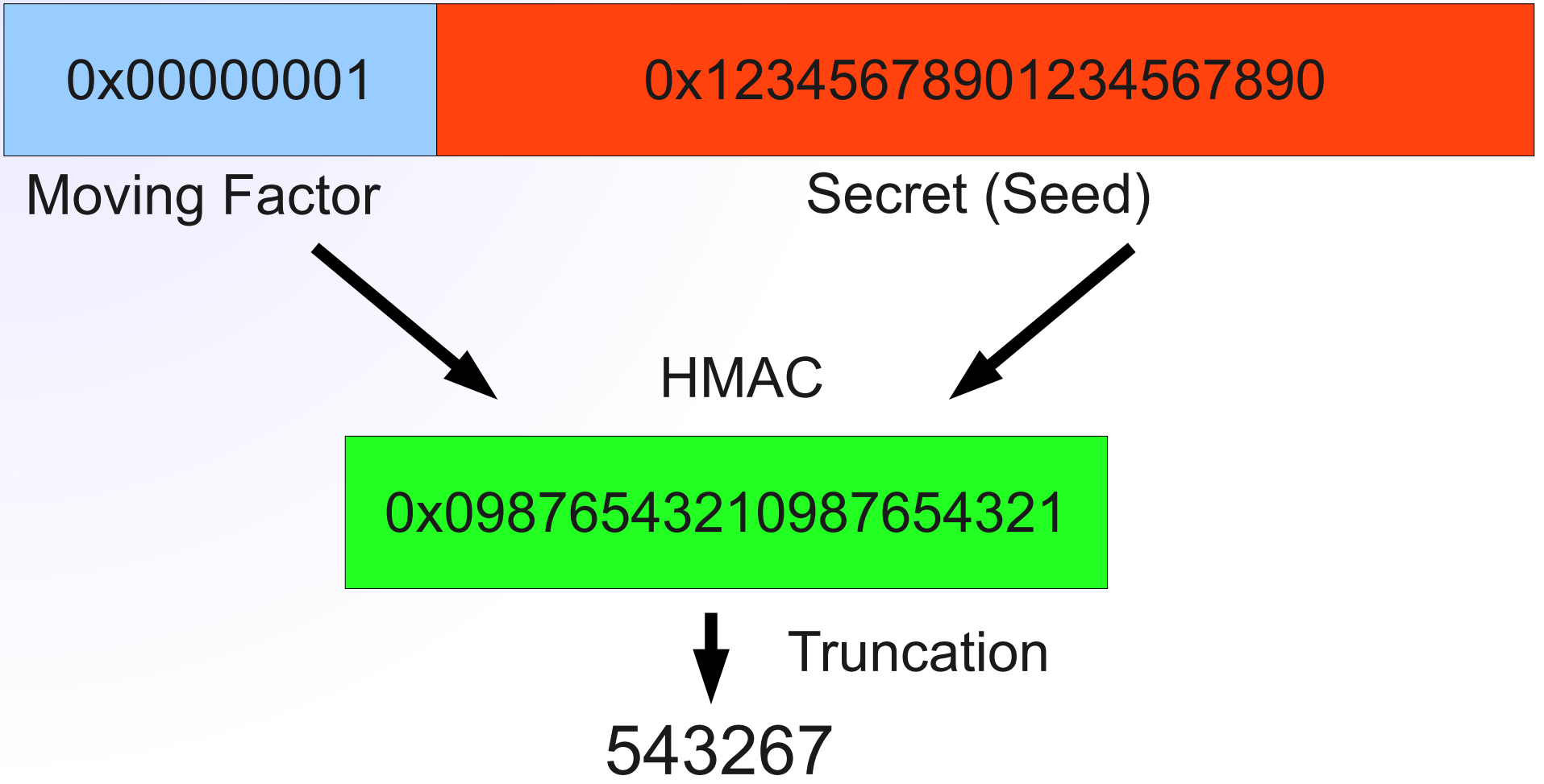
Software-Tokens

- Rechner, PDA oder Handy
- ~~Vertrauenswürdiges Rechnersystem~~
- ~~Schlüsselmaterial in Token gespeichert~~
- Token berechnet gültiges Passwort
- ~~Unmöglich auszulesen („Tamper-Proof“)~~
- ~~Vergossen („Tamper-Evident“)~~

Entwicklung

- Bellcore S/Key, OPIE
- Proprietäre Algorithmen (RSA SecurID, mOTP)
- OATH: www.openauthentication.org

OTP-Funktionsweise



Moving Factor

- Ereignis-Basiert (HOTP)
- Zeit-Basiert (TOTP)
- Challenge-Response (OCRA)

Praxis

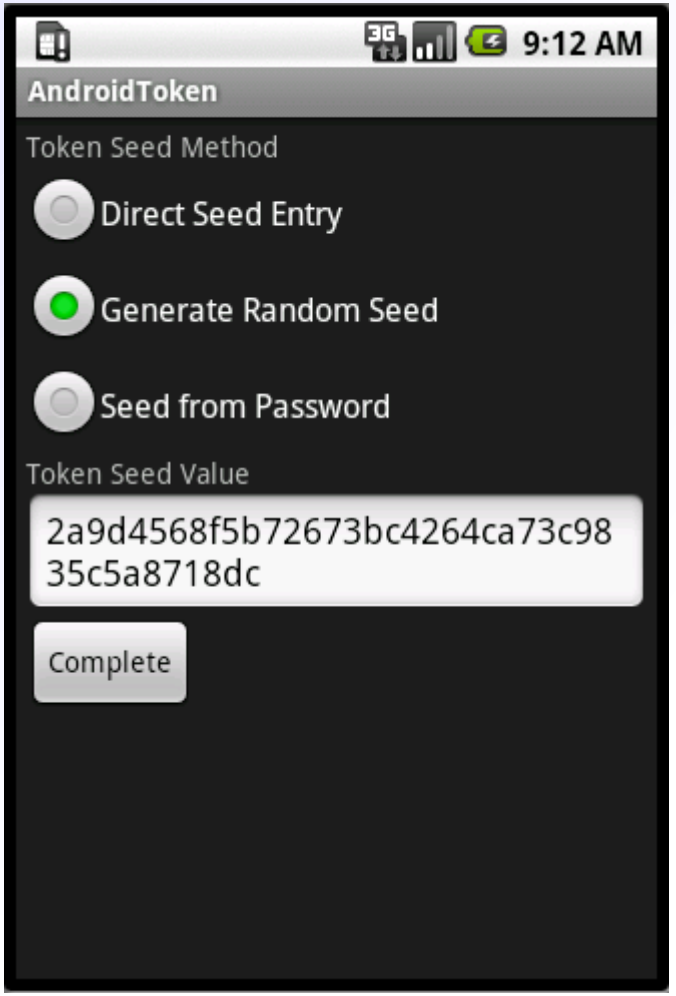
OTP mit Linux

Schritt 1: Tokens beschaffen

- HOTP/TOTP-Kompatibel
- Lieferant liefert Schlüsseldaten
- Lieferantenkette bis Hersteller wird vertraut
- z.B Feitian, Zyxel,...

- z.B. Feitian C-100 / C-200,
  Preis ca. EUR 10,- / Stück, bei www.gooze.eu
  Disclaimer: Ich kann nichts zur Vertrauenswürdigkeit sagen – weder positiv noch negativ...

Software-Tokens



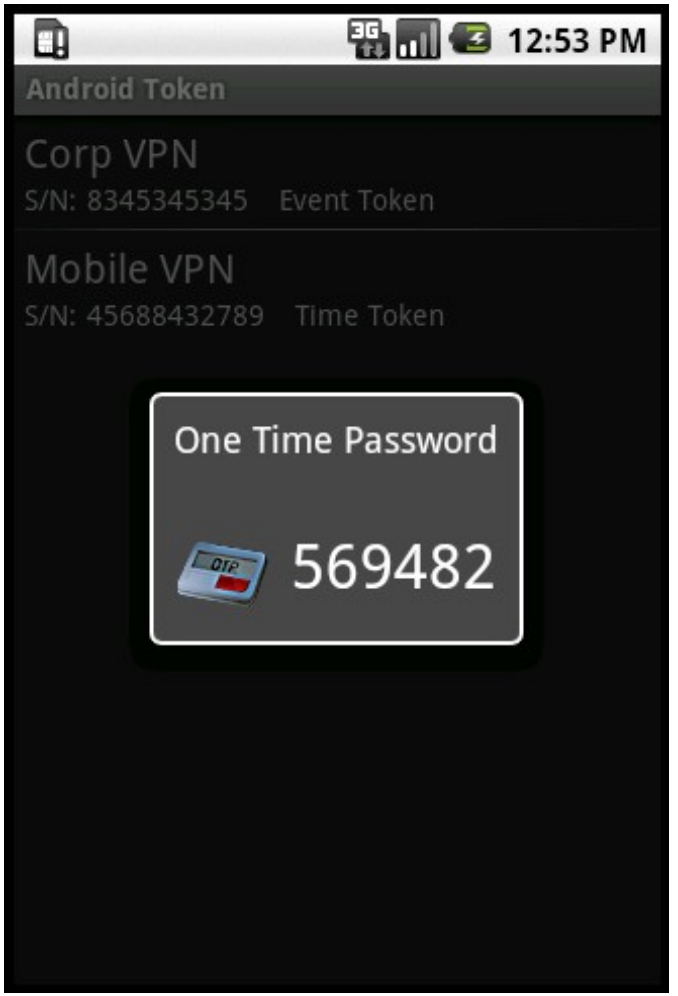


Abbildung: Androidtoken

Software-Token für Phones

- IPhone
  http://code.google.com/oathtoken/
- Android
  http://code.google.com/p/androidtoken/
- Java MIDP (praktisch alle besseren Telefone)
  http://www.ds3global.com/index.php?option=com_content&task=view&id=71

Schritt 2: Software beschaffen

- Hersteller-Software (teuer...)
- OATH-Toolkit (HOTP, TOTP comming soon)

http://www.nongnu.org/oath-toolkit/

```
sudo apt-get libpam-dev
./configure –prefix=/
make
sudo make install
```

Schritt 3: PAM konfigurieren

```
[root@tuxbox etc]# cat /etc/pam.d/sshd
#%PAM-1.0
auth sufficient pam_oath.so usersfile=/etc/users.oath window=10 digits=6
auth       include      system-auth
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    required     pam_loginuid.so

…
```

Schritt 4: Secrets konfigurieren

```
[root@tuxbox etc]#
oathtool --hotp -w 1000 -d 6 258AAFBC7B4FC97AF639A655AB05AF8AF476A726 755639
42
[root@tuxbox etc]# cat ls -l users.oath
-rw------- 1 root root 89 2011-03-18 22:29 users.oath
[root@tuxbox etc]# cat ls -l users.oath
HOTP    ml  test    258AAFBC7B4FC97AF639A655AB05AF8AF476A726  42 755639 \
                                                    2011-01-19T00:06:13L
```

- Dieser Key ist jetzt fast wertlos...

Schritt 5: Ausprobieren

- ChallengeResponseAuthentication=yes in /etc/ssh/sshd_config
- sshd neu starten
- Login versuchen

Komplexere Setups

- Apache: http://code.google.com/p/mod-authn-otp/
- Web-Auth mit OTPs nicht trivial..
- Konsistenz des Moving-Factors: Schreibzugriff.

Komplexere Setups

- Anbindung von Diensten:
  - Windows-Auth
  - Radius
  - Web-Authentifizierung
- Rechnercluster
- Moving-Factor-Konsistenz

- In OpenSource nur begrenzt verfügbar

Zusammenfassung

- Authentifizierung = Identitätsbeweis
- Passwörter alleine sind (relativ) unsicher
- Multi-Faktor-Authentifizierung sinnvoll
- z.B. Wissen + Besitz
- Besitz-Faktor: Vertrauenswürdige Tokens
- Preiswert verfügbar
- Für Linux in kleinen Setups einfach einsetzbar

Vielen Dank für Ihre Aufmerksamkeit.

Fragen ?

URLs

- SoftTokens:
  http://code.google.com/oathtoken/
  http://code.google.com/p/androidtoken/
  http://www.ds3global.com/index.php?option=com_content&task=view&id=71

- Software:
  http://www.nongnu.org/oath-toolkit/

- Tokens:
  http://www.gooze.eu

Backup Slides

Reflections on Trusting Trust

- Ken Thompson:
  http://cm.bell-labs.com/who/ken/trust.html

- Wie weit geht Vertrauen ?