



# Feedback aus der Hausaufgabe

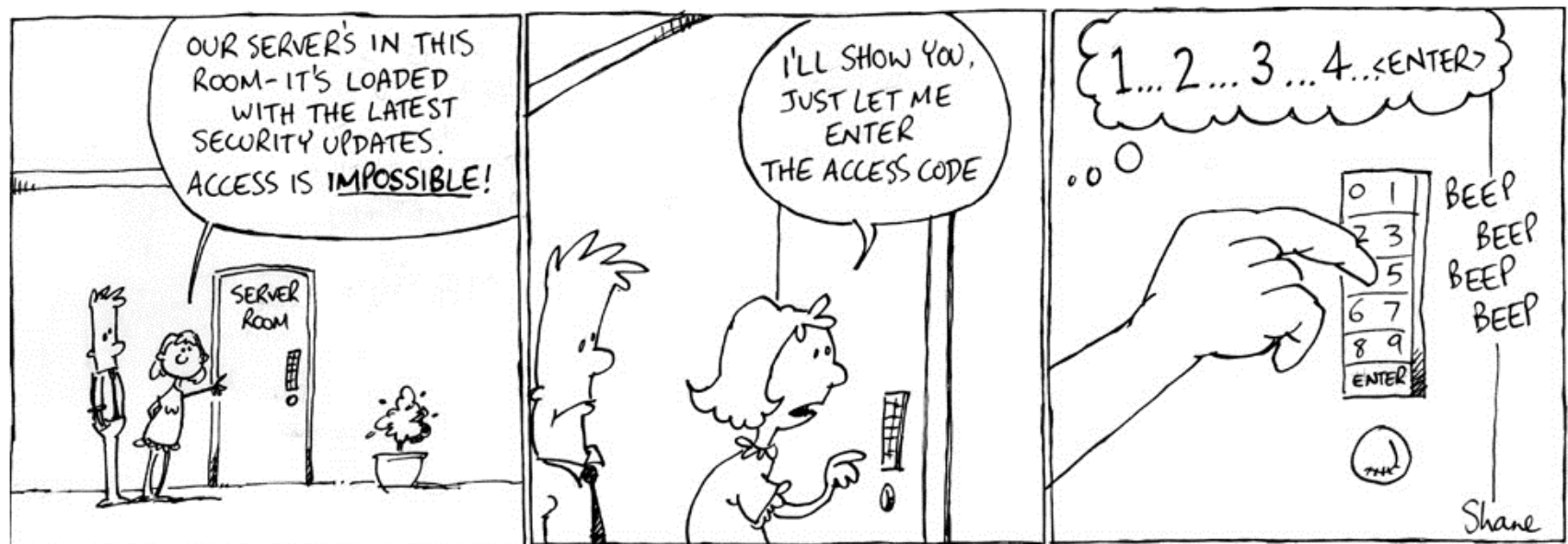
---

- Wie weit sind Sie gekommen?
- Welche Probleme gab / gibt es?
- Wie viel Zeit haben Sie aufgewendet?

## Lektion 5: Benutzer, Passworte, Zugriffsrechte



- User-ID's in Linux und zugehörige Privilegien
- Systemrollen und Umgang mit hochprivilegierten Rollen (root)
- Permanenter/temporärer User-ID-Wechsel (su, sudo)
- Passwortwahl, Passwortwechsel
- Shadow Passwords



Copyright 2005

[www.ShaneCollinge.com](http://www.ShaneCollinge.com)

# User-ID's in Linux und zugehörige Privilegien I

---

- Unix/Linux unterscheidet verschiedene Benutzer und kann diesen Zugriffs- und Ausführungsrechte zuordnen.
- User-ID's sind numerisch, werden aber als Gründen der Benutzerfreundlichkeit auf Benutzernamen abgebildet.
- Zusätzlich verwaltet Unix/Linux Benutzergruppen, denen ebenfalls Zugriffs- und Ausführungsrechte zugeordnet werden.

# User-ID's in Linux und zugehörige Privilegien II

- Die zentrale Datenbank für User-IDs, Benutzernamen und andere Information für den Benutzer ist die Datei `/etc/passwd`.
- Jede Zeile in `/etc/passwd` beschreibt einen Benutzer und seine Attribute:

```
root:asd%sZsd:0:1:Super-User:/root:/sbin/sh
daemon:x:1:1::/
bin:x:2:2::/usr/bin:
lubich:Hx&wrt%d:20:10:Hannes Lubich, FHNW, 4.317:/usr/lubich:/bin/csh
nobody:x:60001:60001:Nobody:/
```

- Jede Zeile in `/etc/group` beschreibt eine Gruppe und nennt ihre Mitglieder:

```
root::0:root
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
usr::10:lubich
```

# User-ID's in Linux und zugehörige Privilegien III

---

- Benutzerrechte sind an die Attribute von Dateien geknüpft. Diese Rechte entscheiden, welche Benutzer oder Gruppenmitglieder eine Datei lesen, verändern oder ausführen können.
- Loggt sich ein Benutzer ein, läuft die Start-Shell mit der User-ID des Benutzers ab – alle weiter durch den Benutzer gestarteten Prozesse haben die gleiche User-ID.
- Wird eine Datei ausgeführt (d.h. es wird ein Prozess erstellt), läuft dieser mit den Rechten des Benutzers/Aufrufers, nicht des Besitzers.



# User-ID's in Linux und zugehörige Privilegien IV

---

- Jeder Benutzer ist selbst verantwortlich für die Zuteilung von Zugriffsrechten für seine oder ihre Dateien (discretionary access control, DAC) – eine Shell-Variable (die „umask“) legt einen vom Benutzer veränderbaren Defaultwert fest.
- Manche hochsicheren Unix/Linux-Varianten erzwingen stattdessen eine Daten-Klassifikation, aus der dann die Zugriffsrechte automatisch abgeleitet werden (mandatory access control, MAC).

# User-ID's in Linux und zugehörige Privilegien V

- Dateizugriffsrechte:

was \ wer	read	write	execute
owner	✓	✓	✓
group	✓	—	✓
world	—	—	✓

`/usr/users/lubich/bin/test`      `lubich staff`      `-rwxr-x--x`

Rechte werden oktal notiert: read = 4, write = 2, execute = 1, z.B. "751",  
Das Kommando "chmod" unterstützt auch Mnemonics "g+x" (man chmod).  
Die Kommandos "chown" und "chgrp" ändern Besitzer und Gruppe.

- Der Systemadministrator hat traditionell den Benutzernamen „root“, entscheidend ist aber die User-ID „0“.
- Für „root“ gelten keine Einschränkungen bezüglich Zugriffs- und Ausführungsrecht.
- Unter „root“ laufende Prozesse werden bevorzugt und können bessere Prioritäten erhalten.

## Systemrollen und Umgang mit hochprivilegierten Rollen II

---

- Benutzer von Desktop-Unix/Linux-Systemen sind oft versucht, immer als „root“ zu arbeiten, da sie die einzigen interaktiven Benutzer sind (jedoch sind viele andere ID's aktiv).
- Dies ist gefährlich, da Fehlmanipulationen (z.B. „`rm -r -f / bla`“) leicht möglich sind und Unix/Linux dies ohne Rückfragen ausführt.
- Das „root“ Passwort oder eine offene „root“-Shell sind zudem Geschenke für Hacker.

## Systemrollen und Umgang mit hochprivilegierten Rollen III

---

- Unix/Linux Systeme umfassen zudem oft eine Anzahl „technischer Benutzer“, die für die Verwaltung von Zugriffsrechten für Subsysteme oder Applikationen benötigt werden:
  - Ohne interaktive Login-Shell: adm, lpr usw.
  - Mit dediziertem Login-Programm
  - Mit interaktiver Login-Shell, z.B. bei nachinstallierten Softwarepaketen
  - Mit oder ohne Passwort bzw. Wartungs-Passwort
- Diese Accounts sollten zyklisch überprüft werden.

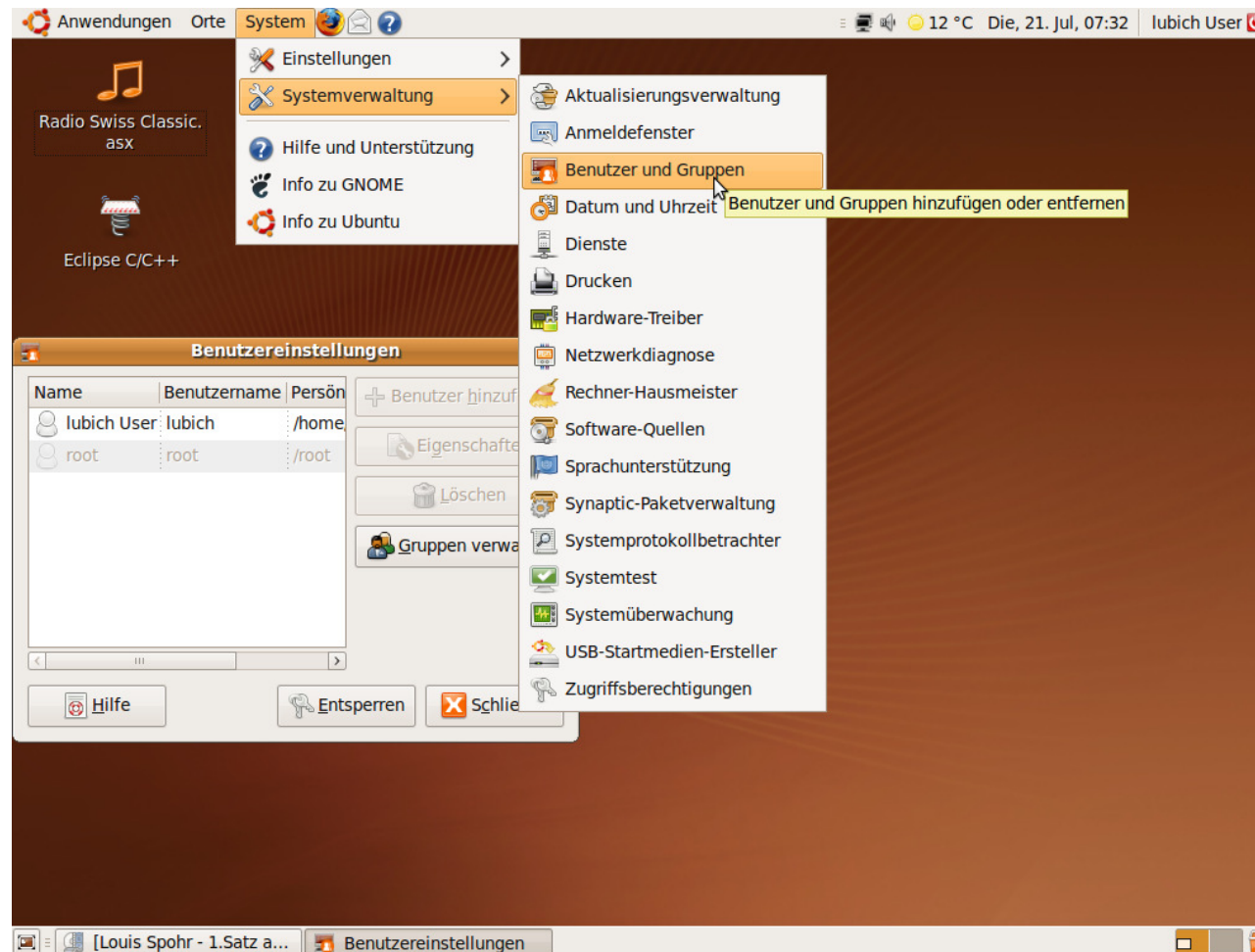
# Permanenter/temporärer User-ID- Wechsel

---

- Es ist sinnvoll, grundsätzlich auch als Besitzer einer Desktop Linux-Installation mit der normalen User-ID zu arbeiten und nur bei Bedarf in den „root“ Modus zu wechseln:
  - `su <Benutzername>`: permanenter Wechsel der Shell auf diese User-ID, Default ist der „root“ Benutzer, dieses Kommando ist auf vielen Systemen für „root“ nicht anwendbar.
  - `sudo <Kommando>`: Wechsel auf „root“ für dieses Kommando (aber „`sudo /bin/bash`“ wäre auch möglich und würde eine „root“-Shell erzeugen).

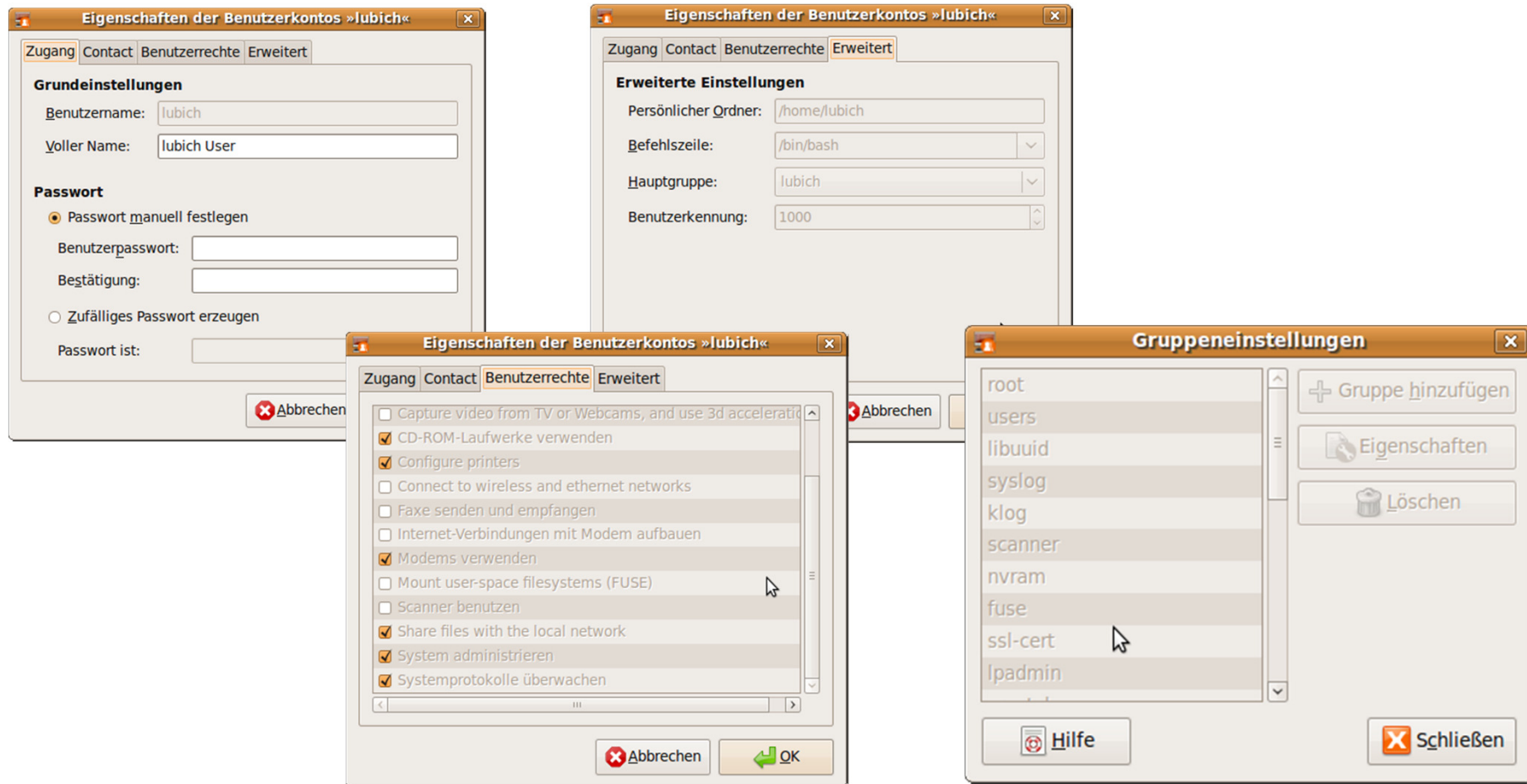
- „vi /etc/passwd“ „/etc/group“
- vipw, vigr
- adduser, addgroup, deluser, delgroup (basiert auf Default-Konfigurationsfile)
- useradd, groupadd, groupmod, usermod, userdel, groupdel (basiert auf Default-Konfigurationsfile)
- Grafische Benutzerschnittstelle
- ConsoleKit (neu ersetzt durch systemd)
- Selbstverwaltung durch Benutzer: passwd, chfn, chsh

# Benutzerverwaltung in Ubuntu-Linux I

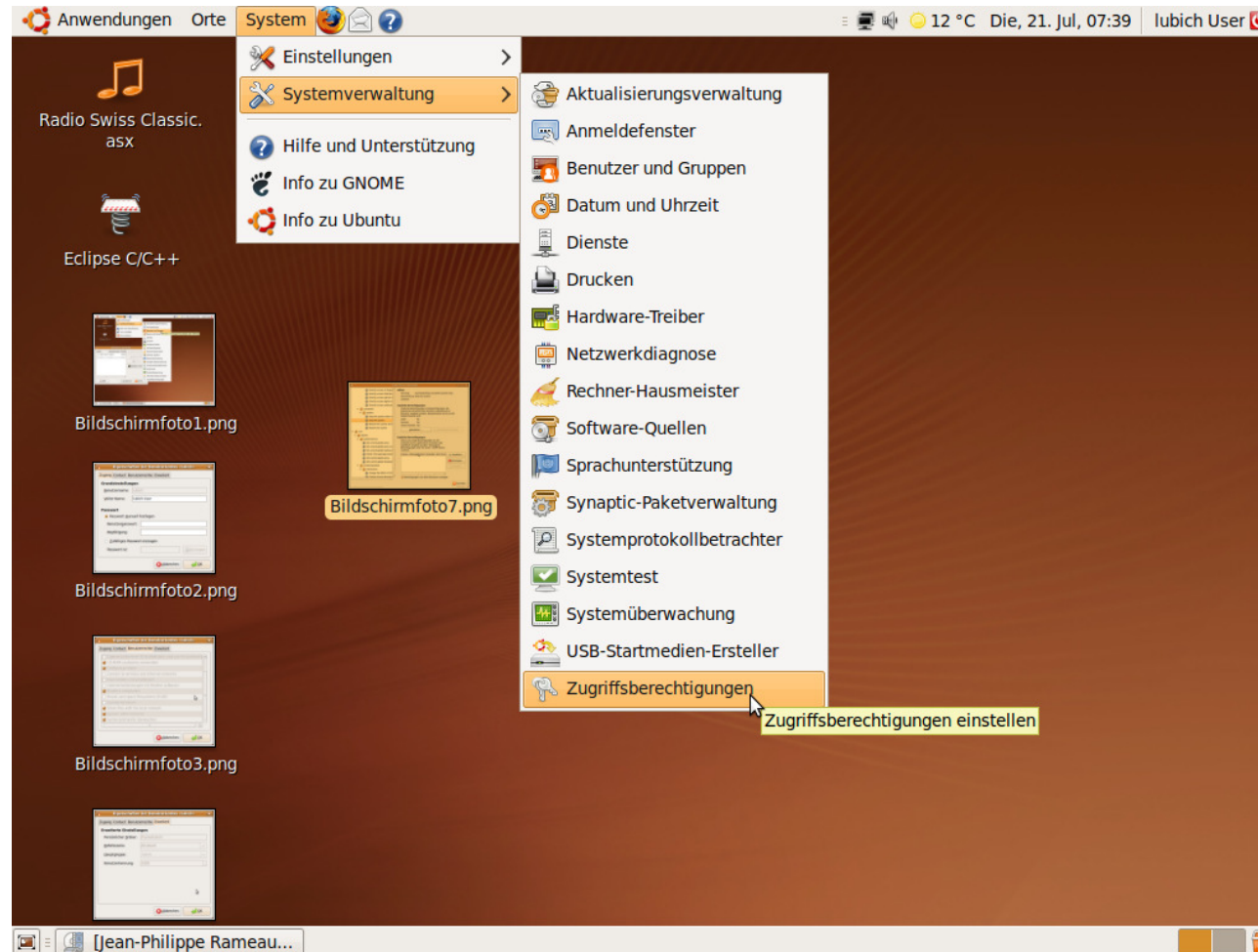




# Benutzerverwaltung in Ubuntu-Linux II



# Serviceverwaltung in Ubuntu-Linux I



# Serviceverwaltung in Ubuntu-Linux II





- Aufgabenstellung: gemäss separatem Aufgabenblatt
- Dauer: 45 Minuten
- Lösungsansatz: Einzelarbeit oder Gruppen von max. 2 Personen
- Hilfsmittel: beliebig
- Besprechung möglicher Lösungen direkt nach dem Ende der Übung
- Bei Interesse Detailkorrektur ihrer Lösung bis ca. nächste Woche (Abgabe bis Heute Abend per e-mail)



# Übungsbesprechung (15 min)

---

- Stellen Sie Ihre jeweilige Lösung der Klasse vor.
- Zeigen Sie auf, warum ihre Lösung korrekt, vollständig und effizient ist.
- Diskutieren Sie ggf. Design-Entscheide, Alternativen oder abweichende Lösungsansätze.
- Gibt es Unklarheiten? Stellen Sie Fragen.

- Nicht erratbar („Linux“)
- Nicht der Person zuzuordnen („Hannes“)
- Nicht in einem Lexikon enthalten („Test“)
- Nicht durch einfache Kombinatorik erzeugt („Test1“, „1tseT“, „TestTest“ usw.)
- 6 bis 8 Zeichen lang (Unix unterstützt nur eine maximale Passwortlänge von 8 Zeichen).
- Enthält Gross- und Kleinbuchstaben, Ziffern und (wenn erlaubt) Sonderzeichen.
- Leicht merkbar / konstruierbar, z.B. zweiter Buchstabe jedes Wortes eines merkbaren Satzes.
- Substitution von Zeichen durch Ziffern oder Sonderzeichen (z.B. „1“ statt „l“, „0“ statt „O“ etc.) wenn zulässig.
- <https://review.datenschut.ch/passwortcheck/check.php>



- Sofort nach der ersten Verwendung des Initial-Passwortes (manchmal auch erzwungen).
- Zahnbürsten-Regel: regelmässig verwenden, regelmässig erneuern, nicht weitergeben
- Wann sollte ein Passwort gewechselt werden?
  - Wenn es kompromittiert wurde.
  - Wenn der Verdacht besteht, es könnte kompromittiert worden sein.
  - Wenn es zu einfach ist.
  - Wenn es weitergegeben wurde.
  - Wenn es zu alt ist (manche Systeme unterstützen oder forcieren Passwort-Aging und Passwort-Generationen) – das „richtige“ Alter und die Anzahl gesperrter Passwort-Generationen ist sehr umstritten.

Firefox

Should I Change My Password? | How Safe I... +

shouldichangemypassword.com https://shouldichangemypassword.com

Help your friends stay safe online too - Tweet Like 16k Send

# SHOULD I CHANGE MY PASSWORD

We don't store your email address unless you ask us to. [Learn more](#) about how we handle email addresses.

Home | Sources | Media | FAQs | Privacy Policy | Contact Us

## Find out if your email address has been hacked

Enter your email here **Check it!** **Bulk Check**

☐ Email me when you add new compromises.

Compromised email addresses discovered:  
**10,309,675**

[How we handle your email address](#)

[Avalanche Technology Group](#) is proud to bring you **Should I Change My Password**, a free service that allows you to check anonymously if your email addresses have been compromised.

We comb the depths of the internet to find email and password data sets that have been hacked, leaked or compromised. We aggregate this data so that you can check whether your password has been included in any of these [security breaches](#).

### Latest news and updates

We've updated our contact page should you ever want to get in touch. Of course there is always twitter too! <http://t.co/n1aTEMBP>  
6 hours ago

Over 230,000 new email addresses have been added, including 150K in a breach found yesterday. No LeakedIn but still worth checking.  
Jun 19 (1 day ago)

@avgaunz always a pleasure :)  
Jun 14 (6 days ago) in reply to avgaunz

Keen to have a chat with a tech journo, not a pitch, to get feedback on a initiative we want to build specifically for journos.  
Jun 14 (6 days ago)

RT **avgaunz**  
100 computer security tips from @Cyberwarzonecom <http://t.co/P8kF0zqN> - a very comprehensive list!  
Jun 14 (6 days ago)  
Retweeted by sicmy and 1 other

<https://shouldichangemypassword.com/>

- Benutzer-seitig:
  - Sichere Ablage, z.B. PGP chiffrierte Datei oder Applikation, z.B. <http://keepass.info/>
- System-seitig:
  - /etc/passwd in chiffrierter Form
  - Bei der Übermittlung (meist Klartext!)
  - Im Speicher einer Applikation (meist Klartext!)

# Aufbewahrung von Passworten II

---

- Die Datei /etc/passwd enthält die chiffrierten Passworte aller Benutzer.
- Die Chiffrierung erfolgt mit einer Einweg-Funktion (d.h. nur Chiffrieren ist möglich).
- Beim Einloggen wird das Klartext-Passwort, das der Benutzer eingibt, mit der Einweg-Funktion chiffriert und das Ergebnis mit der gespeicherten Kopie verglichen.
- Die ersten Buchstaben des chiffriert abgelegten Passwortes werden vom System gewählt und bei der Chiffrierung als zufälliger Initialwert („salt“) verwendet. Dies verhindert mit einer gewissen Wahrscheinlichkeit, dass zwei gleiche Passworte verschiedener Benutzer als identisch erkennbar sind.

- Diebstahl beim Benutzer: abhören, zusehen, „social engineering“, usw.
- Versehentliche Publikation durch eine Search Engine, die das System indexiert hat (z.B. Google-Suche: "Index of /" +passwd )
- Erraten. Aber: nach mehrmaligen Fehlversuchen beim Einloggen wird je nach Systemkonfiguration:
  - die Verbindung getrennt,
  - die Wartezeit für den nächsten Login-Prompt verdoppelt oder
  - Der Benutzer-Account gesperrt.
- Dennoch ist bei Diebstahl der Passwort-Datei ein „brute force“ Angriff durch Erraten möglich.

- Um den Diebstahl von Passwort-Dateien zu verhindern, wurde in modernen Unix- und Linux-Systemen die Passwort-Datei aufgeteilt.
  - /etc/passwd enthält alle Daten ausser den Passworten und ist für alle Benutzer lesbar.
  - /etc/shadow enthält die den User-IDs zugeordneten verschlüsselten Passworte und ist nur mit „root“ Privilegien lesbar.

- Wie kann ein nicht-privilegierter Benutzer sein Passwort oder seine Start-Shell ändern (also /etc/passwd und ggf. die Shadow Passwort Datei beschreiben)?
- → setuid / setgid Mechanismus (ursprünglich als einfache Hardware-Schaltung patentiert, da Software früher nicht patentierbar war).

- Der Ersatz des „x“ Bits einer Datei zur Kennzeichnung (chmod) von Ausführungsrechten durch ein „s“ signalisiert dem Kernel, dass bei der Ausführung die User-ID (bzw. Group-ID) des ausführenden Prozesses für die Ausführungsdauer auf die User-ID (bzw. Group-ID) des Dateibesitzers geändert werden soll und die zugehörigen Rechte gelten (es muss also nicht „root“ sein).

```
40 -rwsr-xr-x 1 root 37084 2009-04-04 07:49 /usr/bin/passwd
```

- Risiko: setuid/setgid-Programme mit unerwünschten Nebeneffekten, z.B. Escape Shell, sowie bei ausführbaren Dateien, welche Scripte enthalten (manche Systeme ignorieren das „s“-Bit auf Script-Dateien).



## setuid / setgid auf Directories

---

- Das Setzen des setuid-Bits auf Directories hat keine Wirkung.
- Das Setzen des setgid-Bits auf Directories bewirkt, dass alle neu erstellten Dateien oder Subdirectories in diesem Directory die Gruppen-ID des Directories erhalten, und nicht die Gruppen-ID des Erzeugers der Datei oder des Subdirectories.

# Single-SignOn in Ubuntu

The screenshot shows a web browser window displaying the 'SingleSignOn' page on the 'Community Ubuntu Documentation' website. The page has a search bar at the top right and a navigation breadcrumb: 'Ubuntu Documentation > Community Documentation > SingleSignOn'. The main heading is 'SingleSignOn'. Below it, the '1. Introduction' section is visible, explaining that the page describes how to set up network-connected Ubuntu machines to support Single Sign-On (SSO). It mentions that SSO is a collection of technologies allowing network users to provide a single set of credentials. A bulleted list follows, detailing the services centralized by this SSO solution: Authentication (using Kerberos), Account Management (using OpenLDAP), Shared File Systems (with options like NFS, Samba, and SSHFS), and (Limited) Authorization (combining LDAP directory and local file system permissions). A table of contents on the right side lists the sections and their sub-topics. The '3. Authentication' section is partially visible at the bottom, mentioning Kerberos as an authentication protocol.

ubuntu documentation

Community Documentation

Ubuntu Documentation > Community Documentation > SingleSignOn

## SingleSignOn

### 1. Introduction

This page describes how to set up network-connected Ubuntu machines to support **Single Sign-On** (SSO). SSO is a name for a collection of technologies that allows network users to provide a single set of credentials for all network services. In a properly configured SSO environment, a user's desktop environment can migrate seamlessly between computers, and access to shared resources such as file systems and printers can be managed with ease.

This SSO solution centralizes the following services:

- Authentication: Verification that a user or server is who they claim to be and providing a mechanism for passing this information to hosts on the network. Kerberos is used for this purpose.
- Account Management: Information about the user such as username and group membership. OpenLDAP is used.
- Shared File Systems: several options are available. Auto-mounting is effected by `pass_mount`.
- (Limited) Authorization: authorization information is a combination of group membership information held in the LDAP directory and local file system permissions.

This guide is divided into several sections that describe installation of required server software, testing, and installation of software on the client.

### 2. Audience

This guide is written for system administrators looking for a Single Sign-On solution. To properly implement the practical steps found in this guide, the reader should be comfortable with the use command-line applications, using the Bourne Again Shell (bash) environment, and editing system configuration files with their preferred text editor application. While previous familiarity with OpenLDAP or Kerberos is not required for this guide, the reader is advised to pursue further learning from the resources listed in the Resources section to broaden their understanding of the technologies involved in SSO.

### 3. Authentication

Kerberos is an authentication protocol using a combination of secret-key cryptography and trusted third parties to allow secure authentication to network services over untrusted networks. This guide uses the MIT implementation of Kerberos as the **authentication** function of SSO.

See the [Kerberos](#) wiki page for instructions on deploying MIT Kerberos.

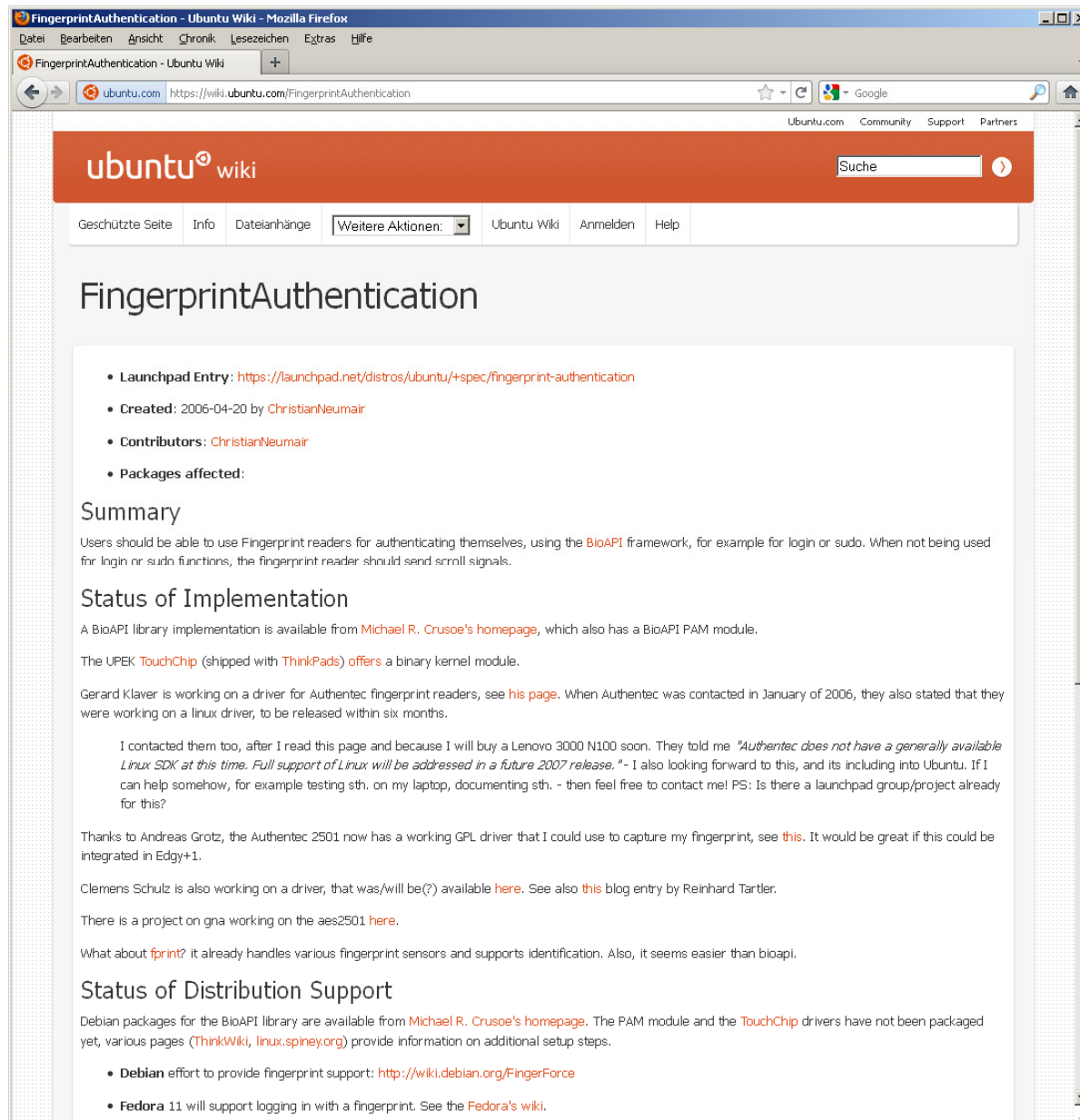
### 4. Account Management

Inhaltsverzeichnis

1. [Introduction](#)
2. [Audience](#)
3. [Authentication](#)
4. [Account Management](#)
  1. [Securing Access](#)
    1. [Anonymous Access](#)
5. [Shared File Systems](#)
  1. [NFS](#)
  2. [Samba](#)
  3. [SSHFS](#)
6. [Client Configuration](#)
  1. [Authentication](#)
  2. [Accounts](#)
  3. [Shared Files](#)
  4. [Testing and Validation](#)
7. [Caching](#)
  1. [Hostnames](#)
  2. [Credentials](#)
8. [LDAP Authentication](#)
  1. [Installing required packages](#)
    1. [Configuring LDAP](#)
    2. [Configuring Kerberos](#)
    3. [Configuring PAM and NSS](#)
  2. [Reverting](#)
9. [Troubleshooting](#)
  1. [Common Error Messages](#)
  2. [Kerberos](#)
  3. [OpenLDAP](#)
10. [Service Configuration](#)
  1. [SSH](#)
  2. [Apache](#)
  3. [NFS](#)

<https://help.ubuntu.com/community/SingleSignOn>

# Biometrik in Ubuntu



<https://wiki.ubuntu.com/FingerprintAuthentication>

# Zusammenfassung der Lektion 5 und Hausaufgabe

---

- Methoden zur Anlage, Administration und Benutzung von Benutzerrollen in Linux.
- Methoden zur Auswahl, Registration und Änderung von Benutzer-Passworten.
- Methoden und die Verwendung der Zuteilung von Benutzerrechten und deren praktische Anwendung.
- Hausaufgabe:
  - Repetieren Sie den Stoff dieser Lektion.
  - Finden Sie mittels „find“ heraus, wie viele und welche Dateien auf Ihrem System setuid oder setgid gesetzt sind. Finden Sie im zweiten Schritt heraus, was diese Dateien tun und warum das „s“-Bit nötig ist.