Fachhochschule Nordwestschweiz
Hochschule für Technik

Modul Systemadministration (sysad)

Feedback aus der Hausaufgabe

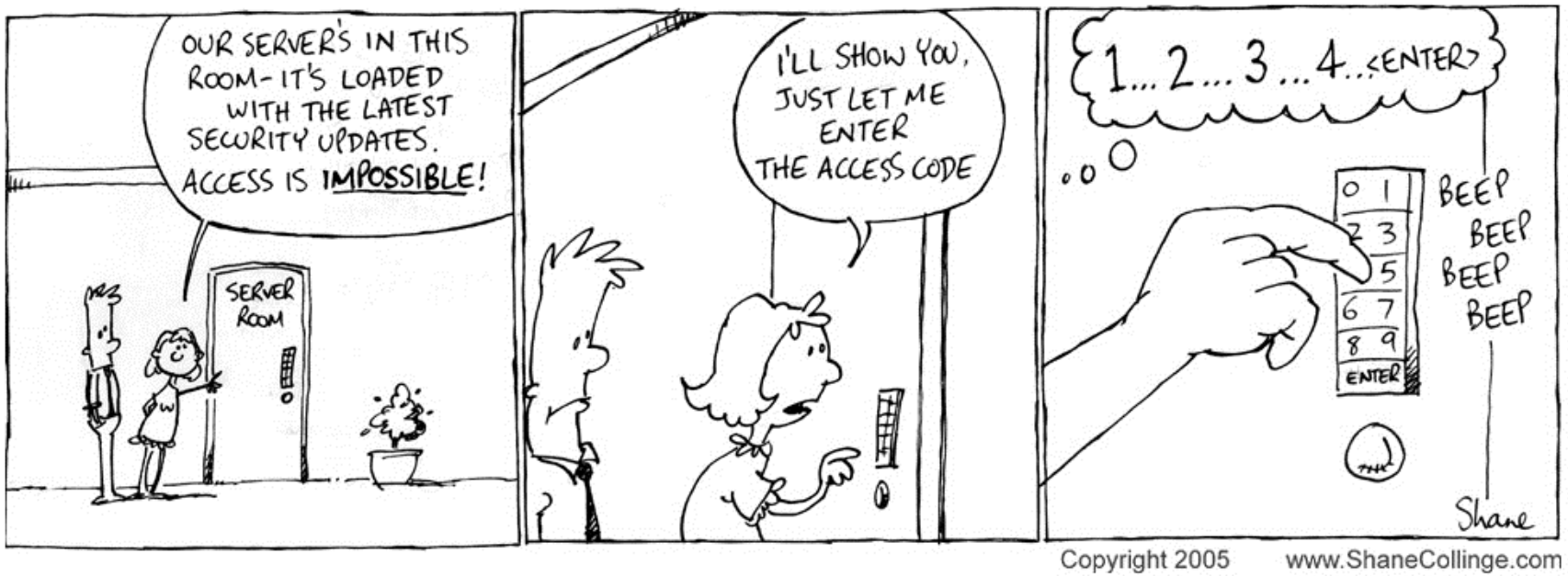
- Wie weit sind Sie gekommen?
- Welche Probleme gab / gibt es?
- Wie viel Zeit haben Sie aufgewendet?

Lektion 5: Benutzer, Passworte, Zugriffsrechte

Inhalt

- 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

Motivation


OUR SERVER'S IN THIS ROOM- IT'S LOADED WITH THE LATEST SECURITY UPDATES. ACCESS IS IMPOSSIBLE!
SERVER ROOM
I'LL SHOW YOU, JUST LET ME ENTER THE ACCESS CODE
1... 2... 3... 4..<ENTER>
0 1
2 3
5
6 7
8 9
ENTER
BEEP
BEEP
BEEP
BEEP
Shane
Copyright 2005
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 Benutzer-gruppen, 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 Grupenmitglieder 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:

wer \ was	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 Mnemnonics “g+x” (man chmod).
Die Kommandos “chown” und “chgrp” ändern Besitzer und Gruppe.

Systemrollen und Umgang mit hochprivilegierten Rollen I

- Der Systemadministrator hat traditionell denBenutzernamen „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 Sotwarepaketen
  - 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).

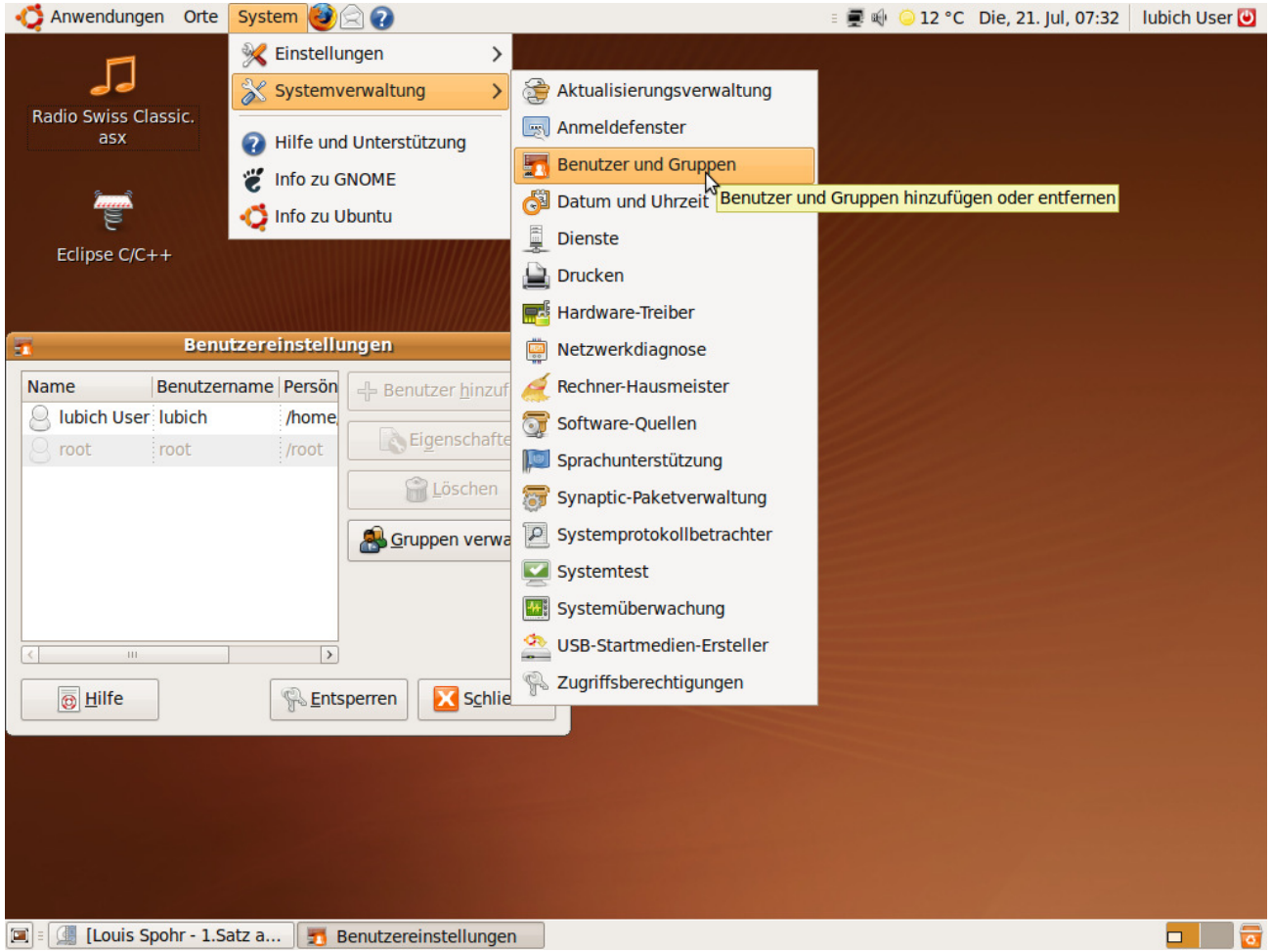
Benutzerverwaltung in Linux

- „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

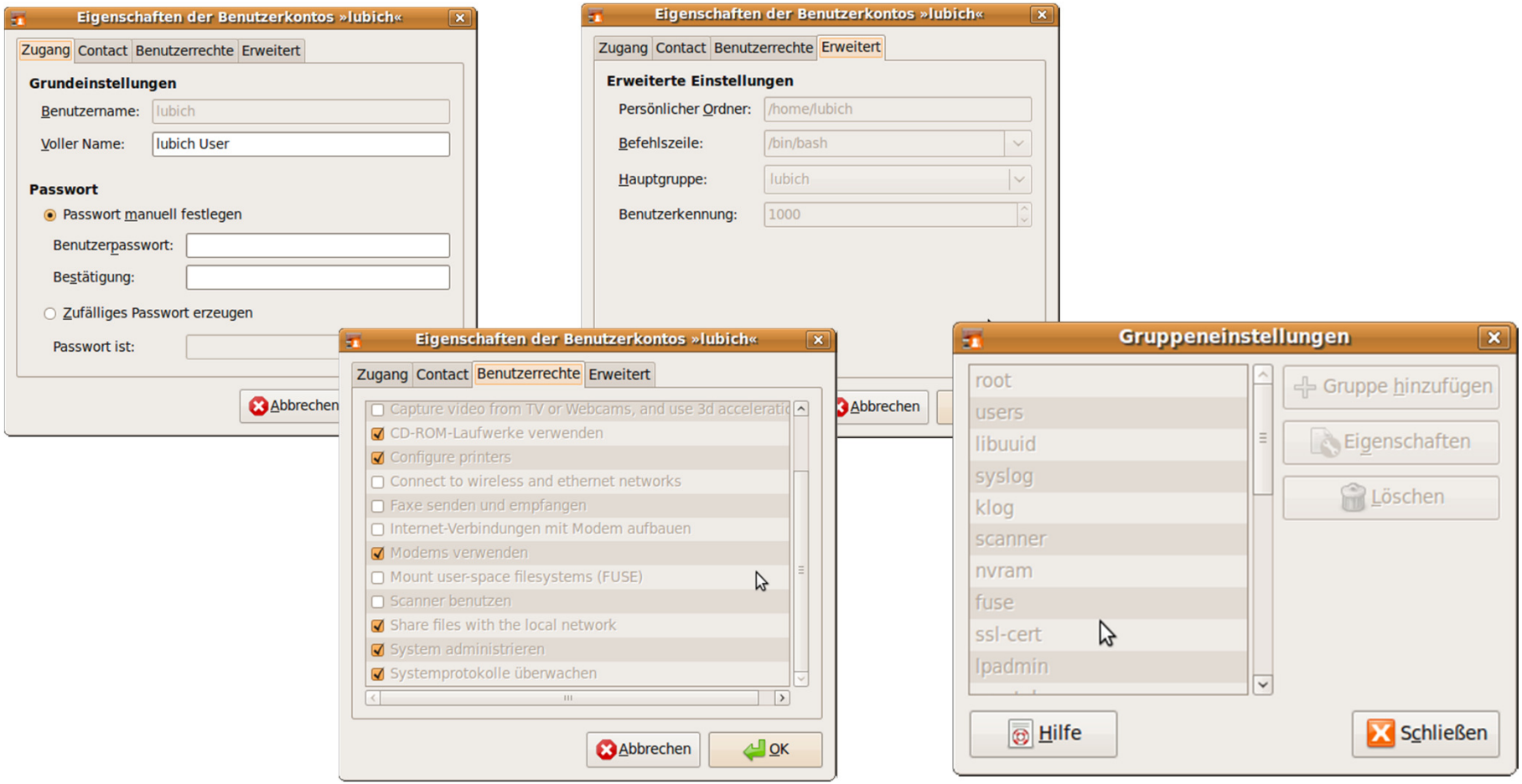
Fachhochschule Nordwestschweiz
Hochschule für Technik

Benutzerverwaltung in Ubuntu-Linux I

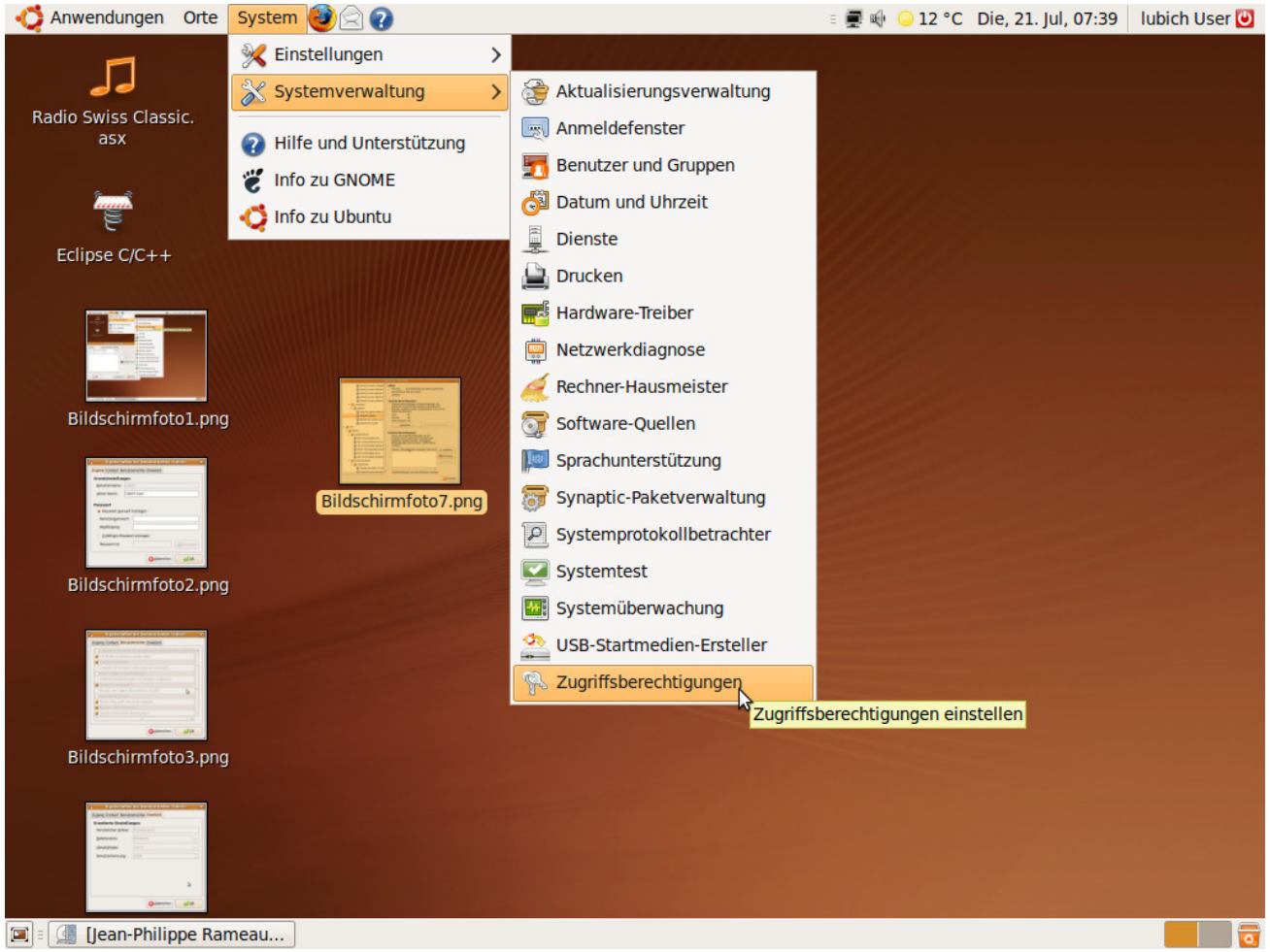


Fachhochschule Nordwestschweiz
Hochschule für Technik

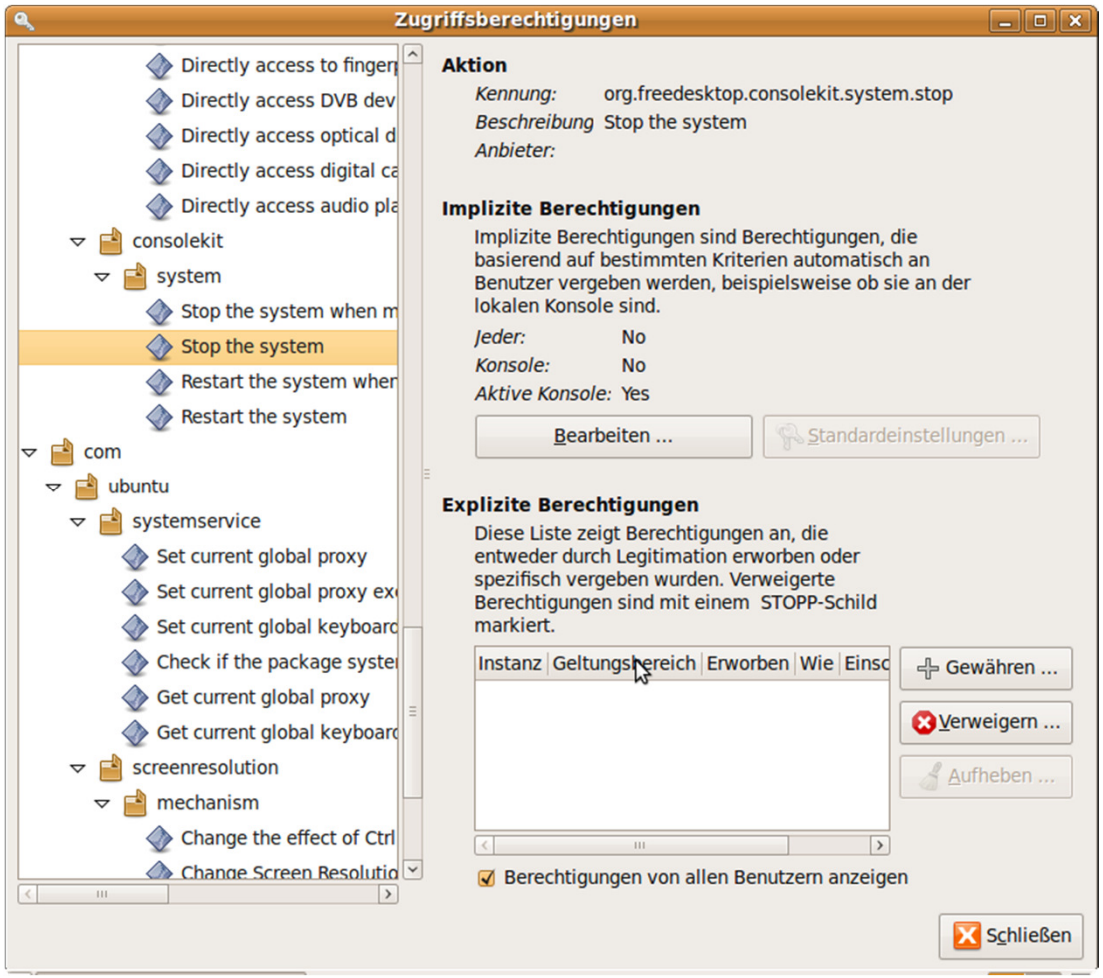
Benutzerverwaltung in Ubuntu-Linux II



Serviceverwaltung in Ubuntu-Linux I



Serviceverwaltung in Ubuntu-Linux II



Pause

Übung

- Aufgabenstellung: gemäss separatem Aufgaben-blatt
- 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)

Pause

Übungsbesprechung (15 min)

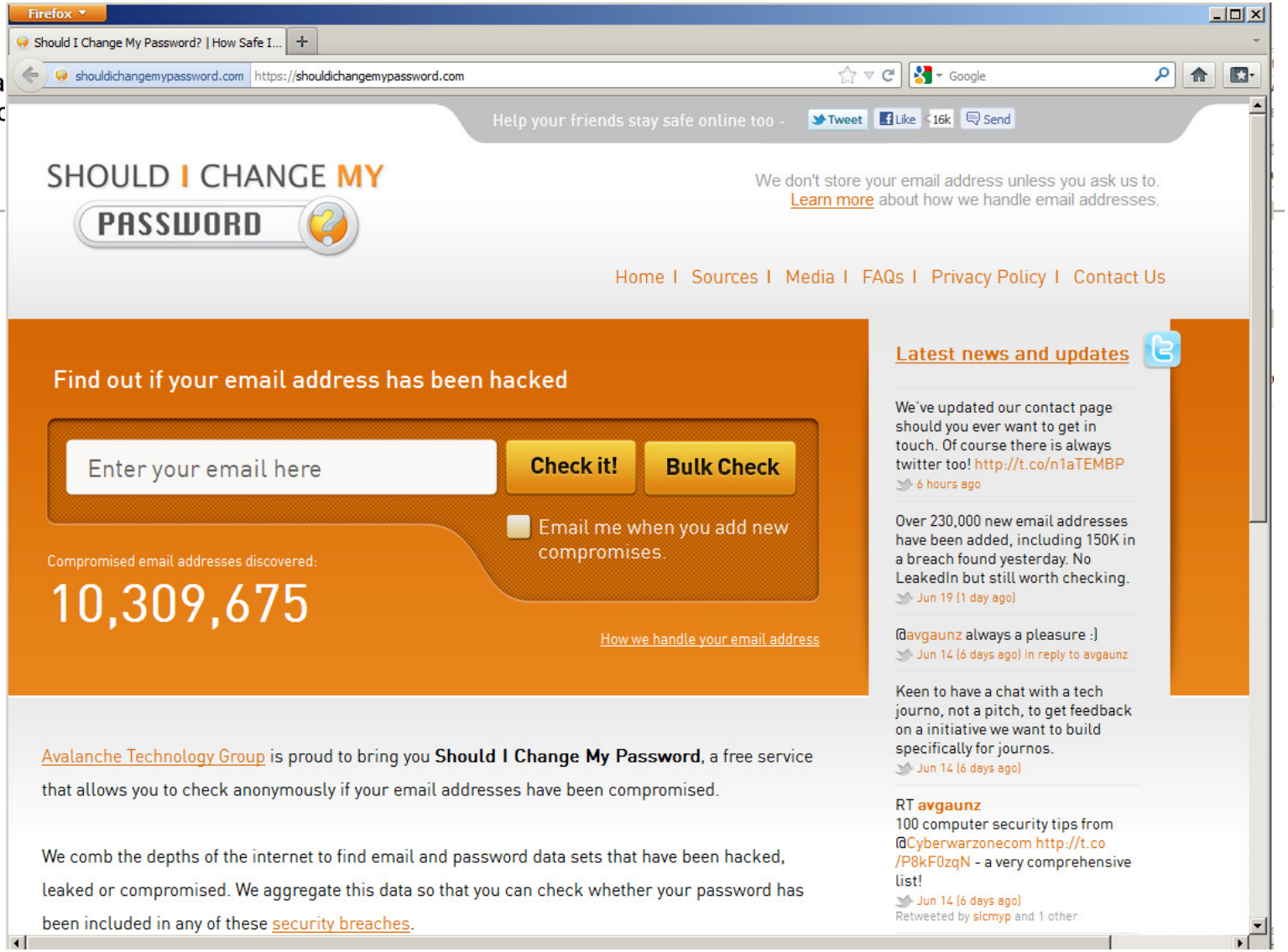
- Stellen Sie Ihre jeweilige Lösung der Klasse vor.
- Zeigen Sie auf, warum ihre Lösung korrekt, vollständig und effizient ist.
- Diskutieren Sie ggf. Design-Entscheide, Alternativen oder abweichende Lösungsansätze.
- Gibt es Unklarheiten? Stellen Sie Fragen.

Passwortwahl

- 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 Sonder-zeichen (z.B. „1“ statt „l“, „0“ statt „O“ etc.) wenn zulässig.
- https://review.datenschutz.ch/passwortcheck/check.php

Passwortwechsel

- 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.



https://shouldichangemypassword.com/

Aufbewahrung von Passworten I

- 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, dass 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.

Angriffe auf Passworte

- 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.

Shadow Passwords

- 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.

Aber …

- 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).

setuid / setgid

- 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.

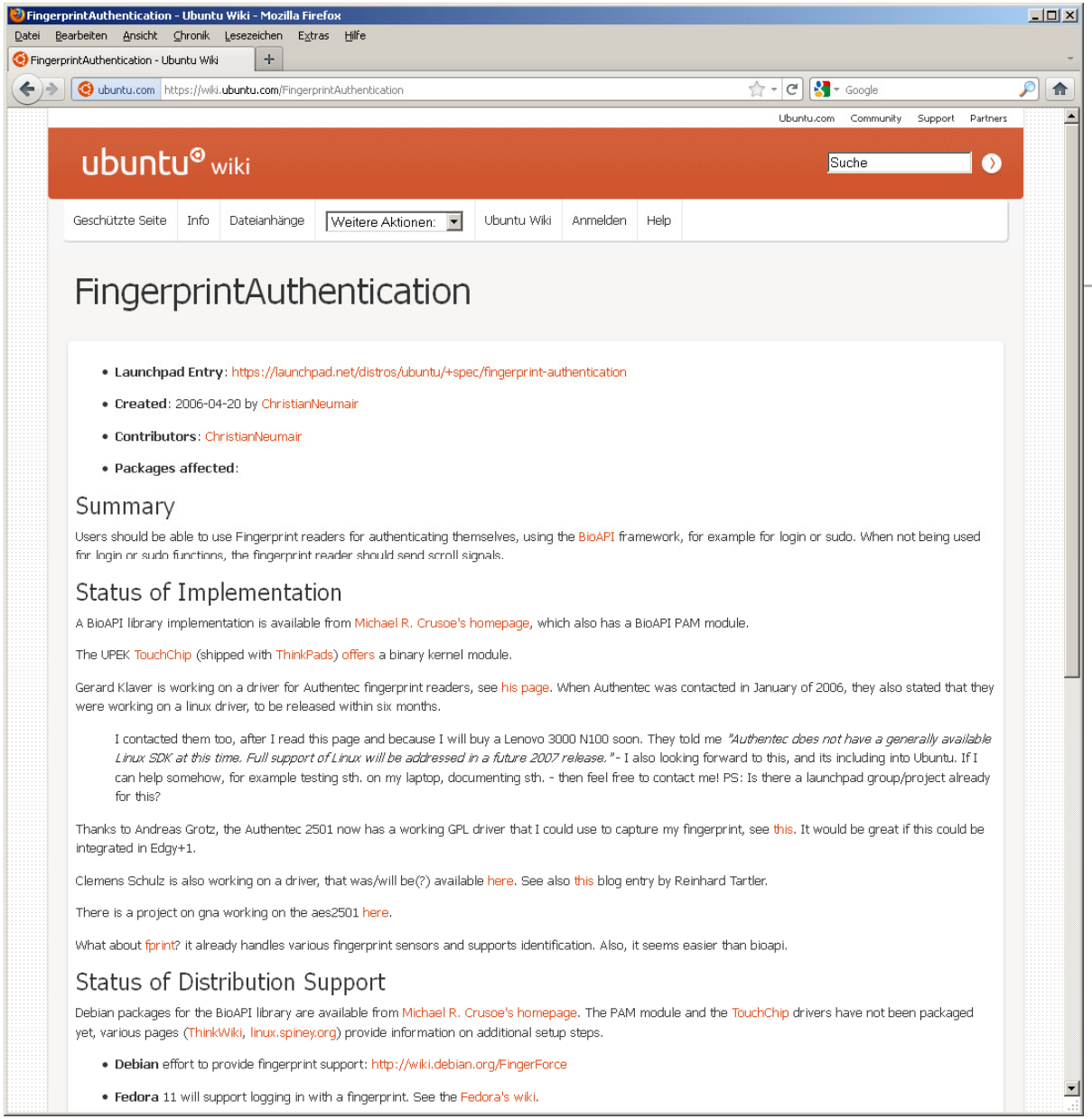
setuid / setgid auf Directories

- 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

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.