User, Gruppen, Rechte & sicheres System

Computerlabor im KuZeB
Ubuntu-Workshop

6.4.2009

Kire
www.kire.ch

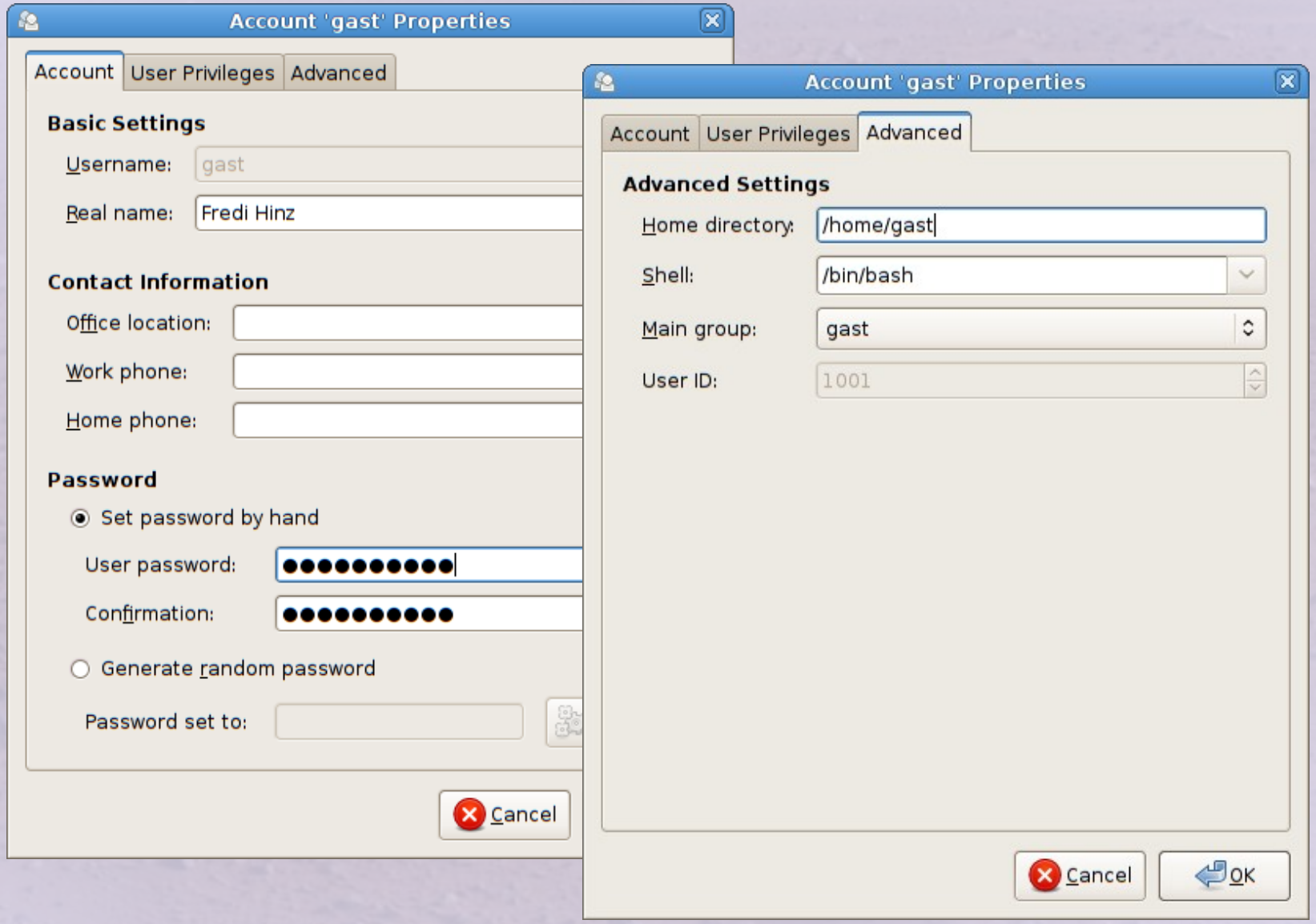
Template von Chih-Hao Tsai (chtsai.org)

Inhaltsverzeichnis

User, Gruppen und Berechtigungen

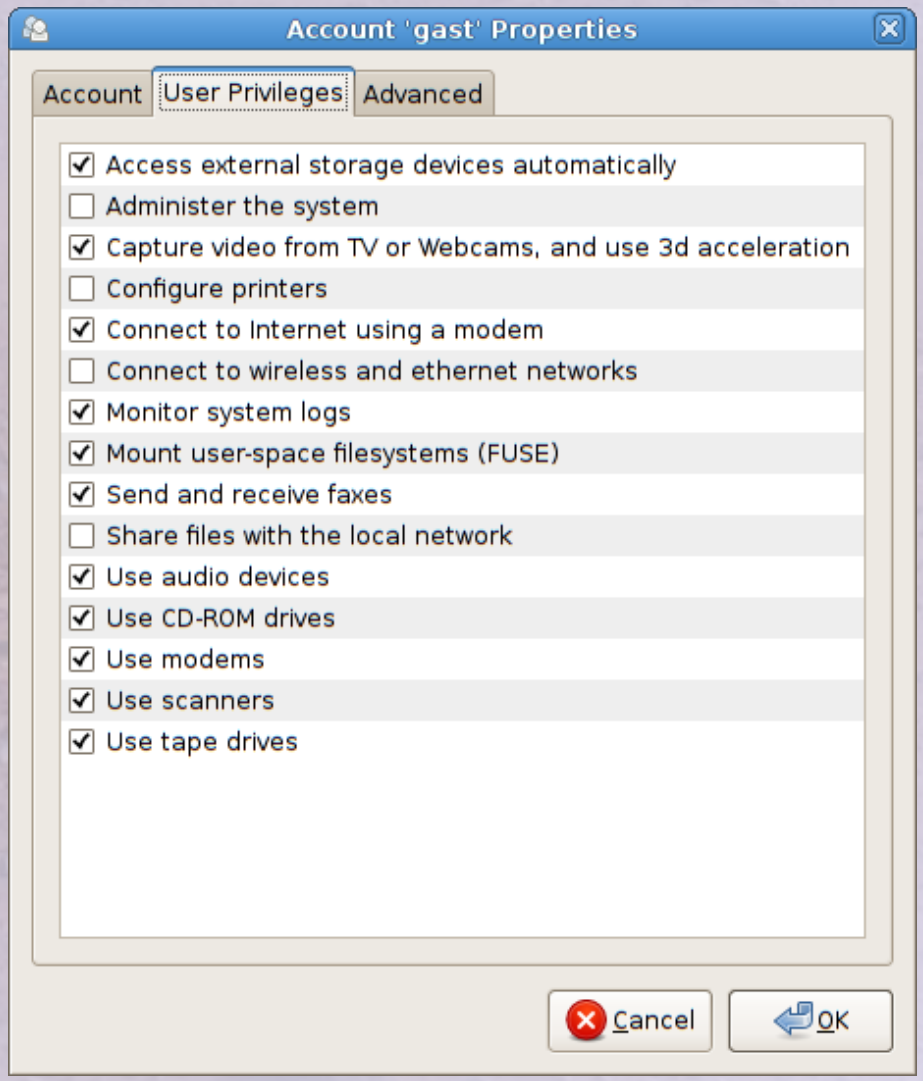
- User
  - root (darf alles)
  - persönliche(r) User
  - Service-User
- Speicherort
  - `/etc/passwd`
    - Namen, IDs, Hauptgruppen-ID, Home-Verzeichnis, Shell
  - `/etc/shadow`
    - nur für Benutzer Root & Gruppe Shadow einsehbar
    - verschlüsselte Passwörter

User, Gruppen und Berechtigungen



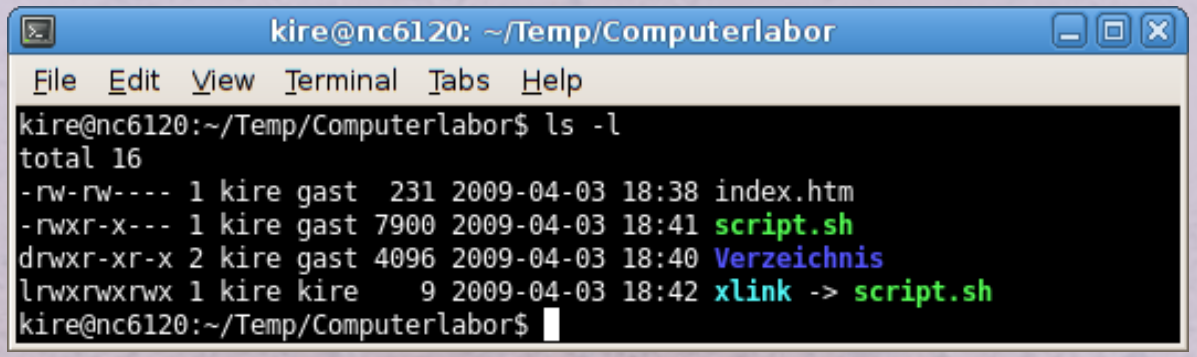
User, Gruppen und Berechtigungen

- Gruppen
  - Zuordnung von User zu Gruppen
  - und Zuordnung von Berechtigungen (für eine Tätigkeit) zu Gruppen
    - Systemadministration (sudo-Recht)
- Speicherort
  - `/etc/group`
    - Name, ID, zugeordnete User



User, Gruppen und Berechtigungen

- Berechtigungen
  - UNIX-Grundsatz: alles ist ein "File"
  - Anzeigen:



    - 1. Name: User (Besitzer)
    - 2. Name: Group
      - (wer weder dieser Gruppe angehört noch Besitzer ist, gehört zu "Other")
    - 1. Zeichen: Datei (-), Directory (d), Link (l)
    - 2.-4. Zeichen: User -> read, write, execute-Recht
    - 5.-7. Zeichen: Group -> read, write, execute-Recht
    - 8.-10. Zeichen: Other -> read, write, execute-Recht

User, Gruppen und Berechtigungen

- Berechtigungen
  - Anzeigen: (Fortsetzung)
    - Bei Verzeichnissen bedeutet "x" das Recht, hineinwechseln zu dürfen
    - Bei Links ziehen die Rechte der Original-Datei
  - Ändern:
    - `chown [neuer User]:[neue Gruppe] [Datei]`
      - `chown root:www-data index.htm`
    - `chmod [ugo][+-][rwx] [Datei]`
      - `chmod g-w index.htm`
  - Passwort ändern:
    - `passwd [User]`
      - Root/sudo darf auch für andere und ohne Abfrage des aktuellen Passworts

User, Gruppen und Berechtigungen

- System mit Gast- resp. mehreren Usern
  - User mit Profile "Desktop User" einrichten
  - Rechte der eigenen und Gast-Daten prüfen/anpassen
    - `/home/[User]/.profile: umask 027`
      - „#“ am Zeilenanfang entfernen
      - setzt neue Dateien, die dieser User anlegt, auf
        - `-rw-r-----` (Neuanmeldung nötig)
        - anstatt: `-rw-r--r--`
    - `chmod -R g-wx,o-rwx /home/gast`
      - rekursiv im Homeverzeichnis:
        - Gruppen: `-wx` & Other: `-rwx`
    - `find /home/gast -type d -perm -g+r -exec chmod g+x {} \;`
      - rekursiv im Homeverzeichnis für Verzeichnisse mit bereits Gruppen-Recht `+r`:
        - Gruppen: `+x`

User, Gruppen und Berechtigungen

- Gast-Session
  - über "User Switcher“ Applet
  - User kriegt ein temporäres Home-Verzeichnis
    - Dateien/Einstellungen sind nach dem Abmelden weg
  - und nur sehr wenige Rechte

(Personal-)Firewall und Antiviren-Software?

- keine bekannten Viren
  - klare Trennung zwischen System- & Userrechten
  - jede Distribution ist etwas anders, keine Monokultur
- Wenn kein Programm ins Netz hört, kann auch nichts eindringen
  - Erst Programme aus Zusatzinstallationen, wie z.B. Webserver, Mailserver etc., öffnen/brauchen Ports
  - oder auch spezielle Clients, wie Vuze (BitTorrent) etc.
    - `sudo netstat -lnpt |grep -i listen |grep -v 127.0.0.1`

(Personal-)Firewall und Antiviren-Software?

- Programme, welche auf das Netz zugreifen
  - Webbrowser, Mailclient etc.
- oder unbekannte Daten öffnen und ausführen
  - OpenOffice.org etc.
- sind potenziell gefährdet
  - aber auch mit Firewall

- Grundsätzlich
  - Updates immer gleich ausführen
  - möglichst nur Open Source-Programme
  - und aus „offiziellen“ Ubuntu-Repositories installieren

Datei- & Festplattenverschlüsselung

- ab Alternate-CD installieren
  - „gesamte Platte mit verschlüsseltem LVM”
  - gutes und langes Passwort wählen
    - komplette Harddisk, ausser /boot, wird mit LUKS/dm-crypt verschlüsselt
    - beim Booten wird nun nach dem Passwort gefragt
- Soll die Festplatte nach eigenen Vorstellungen partitioniert werden, wird es ziemlich kompliziert
  - helfe aber gerne

Datei- & Festplattenverschlüsselung

- Verschlüsseln einer externen Harddisk
  - `sudo bash`
  - `fdisk -l`
    - Wichtig ist, sich sicher zu sein, welches die externe Harddisk-Partition ist
      - Annahme hier: /dev/sdb1
      - Alle Daten auf dieser Partition gehen verloren!
  - `dd if=/dev/urandom of=/dev/sdb1 bs=1M count=2`
    - Alle Bereiche der Partition müssen einmal überschrieben werden; hier der Anfang aus /dev/urandom
  - `cryptsetup luksFormat -c aes-cbc-essiv:sha256 -s 256 -y /dev/sdb1`
    - Verschlüsselung wird mit abgefragtem Passwort angelegt

Datei- & Festplattenverschlüsselung

- Verschlüsseln einer externen Harddisk (Fortsetzung)
  - **`cryptsetup luksOpen /dev/sdb1 cryptedusbhd`**
    - Verschlüsselte Partition öffnen
  - **`cryptsetup status cryptedusbhd`**
    - Status zur Überprüfung abfragen
  - **`dd if=/dev/zero of=/dev/mapper/cryptedusbhd`**
    - Rest der Partition aus /dev/zero überschreiben
      - dauert!
  - **`mkfs.ext3 /dev/mapper/cryptedusbhd`**
    - Partition mit Linux-Filesystem formatieren
  - **`cryptsetup luksClose cryptedusbhd`**
    - Partition schliessen
      - Disk abziehen, neu einstecken: Passwort wird abgefragt

Datei- & Festplattenverschlüsselung

- Angriffsszenarien
  - bei nicht ausgeschalteten Systemen
    - auch Suspend-to-RAM
  - Passwort für Verschlüsselung aus dem RAM auslesen
  - Direct Memory Access (DMA)
    - Hotplug-PCI-Karte (Server)
    - Firewire, spezielle PC-Card, Firewire-PC-Card
    - Lösung (nicht für Hotplug-PCI)
      - ergänzen `/etc/rc.local`:
      - `# Kernelmodul fuer Firewire ohne DMA laden`
      - `rmmod ohci1394`
      - `modprobe ohci1394 phys_dma=0`
      - `# Kernelmodul fuer PC-Cards entladen`
      - `rmmod pcmcia`

Datei- & Festplattenverschlüsselung

- Angriffsszenarien (Fortsetzung)
  - Residentes Memory (bis 30s)
    - BIOS-Passwort
    - Hauptspeicherprüfung bei Neustart
    - Gegen Kühlung und Transfer des Hauptspeicher-Bausteines in einen anderen Rechner ist (noch) kein Kraut gewachsen; ausser Rechner ausschalten
  - `www.kire.ch/datenschutz/keyrecovery.htm`

Datei- & Festplattenverschlüsselung

- einzelne Files oder Verzeichnisse verschlüsseln
  - verschiedene Möglichkeiten
    - GnuPG (für Dateiaustausch mit anderen)
    - TrueCrypt (kennt auch Hidden Volumes für glaubhafte Abstreitbarkeit)
    - Ubuntu Encrypted Private Directory
  - sind aber nicht unbedingt zu empfehlen
    - Ein in einen verschlüsselten Container verschobenes File ist nicht automatisch spurenfrei (also noch unverschlüsselte Datei) gelöscht
    - Temporäre Dateien: /tmp, ~/tmp
    - Druckdateien: /var/spool/cups, /var/spool/cups-pdf
    - Hauptspeicher-Auslagerungs-Partition