GNU/Linux/Ubuntu im sicheren Netz

GNU/Linux/Ubuntu im sicheren Netz

- Warum GNU/Linux/Ubuntu?
  - 'to go the Ubuntu Way'
- Verschlüsselung von externen Festplatten
  - Beispiel LUKS
- gemeinsame Daten für die ganze Familie
  - sicheres privates Netz in unsicheren Zeiten
  - Zugriff über das Netz auf den PC zu Hause mit X2GO
  - privates 'Cloud-Computing' :-)
  - Virtualisierung, um einen vorhandenen PC weiter zu nutzen
- Skripte
  - zum Mitnehmen

über mich

- Richard Albrecht
  - Physiker / Uni Halle-Wittenberg, Diplom 1973
  - ab 1988 am MPI für Biochemie Martinsried
    - 3-D Mikroskopie in der Zellbiologie
  - jetzt: Middleware, Datenbanken, .NET, Webanwendungen
  - Linux ist Ausgleich in der Freizeit

- Ubuntu-Karmic, 64 bit, 8 GB RAM
- Migration von PCs für ältere Leute und
  für Leute mit geringen PC-Kenntnissen
  - kein Virenscanner, keine PFW, keine Viren, keine Trojaner
  - Installation wird von mir vorbereitet, einen Abend Einweisung
  - weitere Wartung durch Benutzer, wenig Probleme
  - bisher ältestes Ubuntu-System läuft seit 2005 (Breezy Badger)
  - jetzt 8.04 Hardy, LTS,

Paradigmenwechsel

- PC ist zur Privatsphäre geworden
  - private Sicherheit der Daten wird immer wichtiger
  - Bundesverfassungsgericht in DE, 27. Februar 2008
    - „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“

- Linux hat sich in den letzten 10 Jahren sehr gewandelt
  - 40 Jahre Erfahrung (durch Unix)
  - hohe Sicherheit für den Desktopbenutzer

- KISS – 'Keep It Simple, Stupid'
  - Ockhams Razor
  - möglichst einfache, minimalistische und leicht verständliche Lösung
  - optimale Systeme
  - z.B. Internet, Linux,
    - Bücher: Eric Raymond und Rob W. Landley
    - 'The Art of Unix Programming'
    - 'The Art of Unix Usability'

- … let's go to GNU/Linux/Ubuntu

erste Schritte

"I cannot teach anybody anything, I can only make them think.", Socrates

- täglich damit arbeiten
  - dem allwissenden '*PC-Guru*' kündigen (Nachbar, PC-Freak, ...)
  - nie jemanden an den Linux-PC lassen, der sich '*mit Computern auskennt*'
  - sehr viel '*Computer-Wissen*' bezieht sich auf einen einzigen Software Hersteller
  - Ubuntu ist nicht das,
    was man aus der bisherigen Erfahrung kennt
  - sich auf GNU/Linux/Ubuntu einlassen
    to go the Ubuntu Way
  - im Ubuntuusers-Wiki stöbern: www.ubuntuusers.de, help.ubuntu.com
  - neue Software entdecken (Anwendungen->Softwarezentrum)
  - fast unendlich viele Möglichkeiten
  - Ubuntu ist mehr als jedes 'Ultimate'
- und mit dem Terminal anfreunden
  - es ist sehr effizient und hilft, Linux besser zu verstehen
  - wir werden es gleich benötigen

Vorteile für Sie

- Lernprozess
  - besserer Umgang mit dem Internet
  - bessere Kenntnisse im Umgang mit dem Computer
  - vom 'Klick' zum Wissen
  - keine Limits durch Lizenzen

- Ergebnis
  - sicherer Umgang mit Computern, weil die Hintergründe transparent werden
  - und dann mit Ihren neuen Kenntnissen mit
    jemandem, 'der sich mit Computern auskennt', reden
  - Sie werden staunen, was Sie alles im Umgang mit Ubuntu gelernt haben
- Sicherheit
  - breites Feld
  - hier nur ein Punkt:
    - 'whitelist' Sicherheit durch Prüfung der installierten Software
    - nur mit Open Source Lizenzen in diesem Umfang möglich
- Links
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Main/HomePage
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/CookBooks/Linuxeinstieg

passive Sicherheit durch 'whitelists'

the Ubuntu Way: 'whitelists'

signiertes Repository,
ca. 29000 Pakete
Ubuntu-Server

Beispiel Firefox:
Source: firefox-3.0
MD5sum:
db07d4ab7fba80bcba3c1d7533dfb3af

Programme
auf Echtheit geprüft
nur 'whitelist' Software

herkömmlicher Weg 'blacklists'

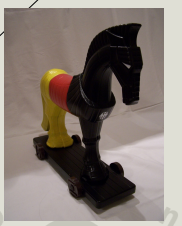
unsichere Webseite

unsichere Webseite

unsichere Webseite

unsichere Webseite

Supertool.exe



PC zu Hause
Daten sind nicht geprüft
Viren und Trojaner müssen
mit 'blacklists' gesucht werden
(kann nie vollständig sein)

Voraussetzungen für die folgenden Abschnitte

- Installieren von Programmen
  - Synaptic od. apt-get
  - Hilfesystem (man, info)
- Terminal
  - Öffnen, einfache Kommandos absenden
  - Arbeiten als root, sudo -s
- Rechteverwaltung
  - Benutzerrechte
  - root Rechte
- Dateisystem (Filesystem Hierarchy Standard)
  - Anlegen von Verzeichnissen
  - Verzeichnisse für Konfigurationsfiles (/etc, ~/.*)
  - Anzeigen dieser Dateien (cat)
  - Editieren von Dateien (vim, gedit)
- Netzwerk
  - Internetadressen, Namensauflösung, DynDNS
  - Dienste, Ports (/etc/services)
  - Router, Modem
  - Provider

Verschlüsselung von Festplatten

- Warum?
  - Grundgesetz, s.o.
- Warum?
  - Diebstahl, Verkauf, Entsorgung, externe HD
- LUKS
  - von Linux favorisiert
- Wie
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/LUKS
  - 'cryptsetup' installieren
  - Partition einrichten
    - 2 x formatieren, a) mit LUKS, b) mit einem Filesystem
  - 'gdecypt' installieren
    - bein Einstecken der HD wird diese autom. eingebunden
  - Vorsicht: Passwort nie verlieren, LUKS ist sehr sicher
  - Vorsicht: lernen, wie in Linux Partitionen aufgelistet werden (fdisk -l)
    - wird die falsche Partition formatiert, dann ...,

gdecrypt

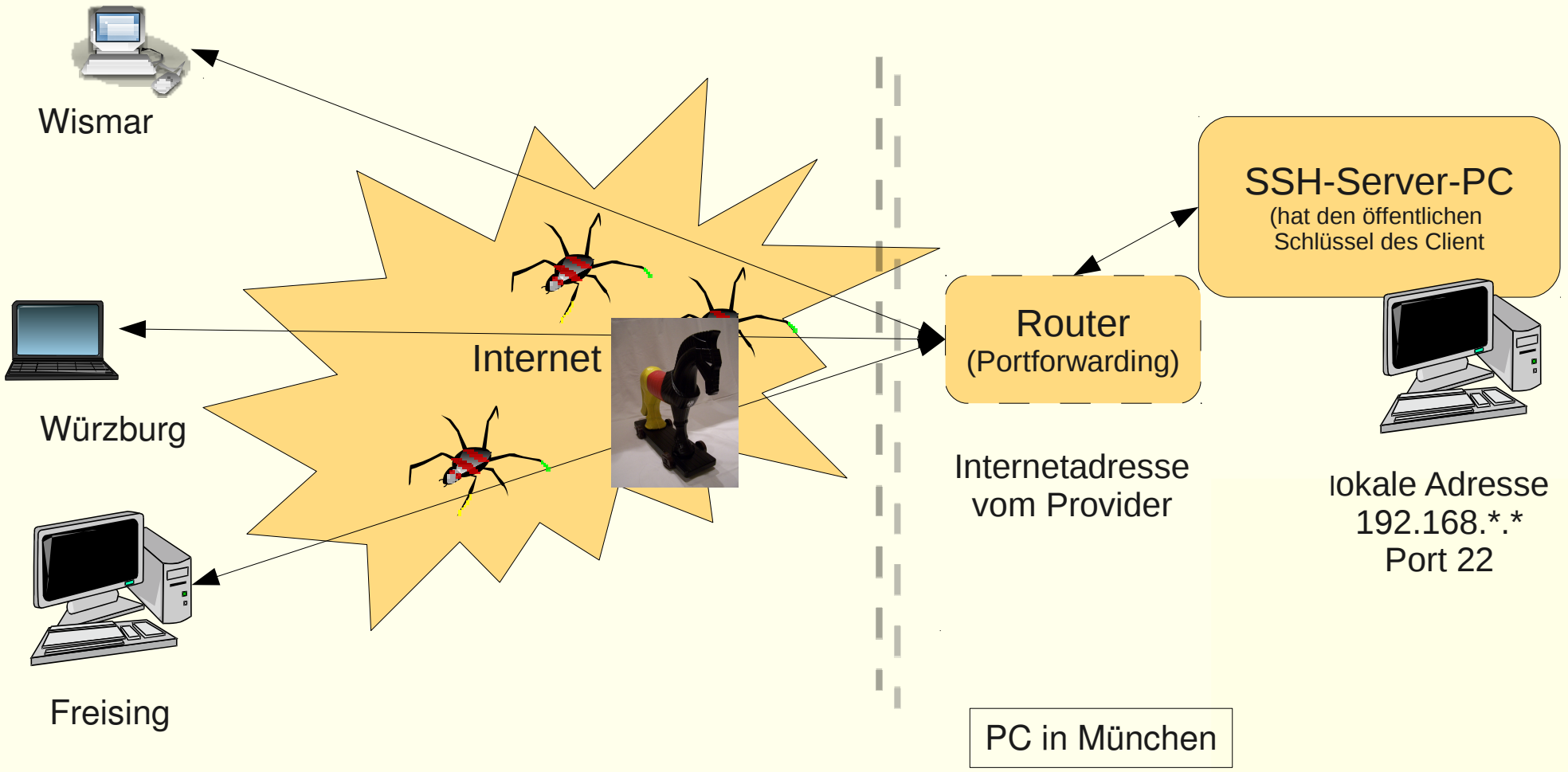
- externe HD/USB-Stick anstecken
  - 'gdecrypt' fragt nach dem Passwort und erledigt den Rest

  - entfernen mit Rechtsclick auf das Icon der HD: 'sicher Entfernen'

sicheres Netz für die Familie

- Warum?
  - Grundgesetz, s.o.
  - Überwachung, DPI wird sehr wahrscheinlich
  - Vergleich mit Postkarte ist falsch
    - die Postkarte liest evtl. der Briefträger
    - unseren Traffic lesen und manipulieren viele (google: **insert coin odem**)
- SSH
  - universelle und sichere
    Verbindung zwischen 2 Ubuntu-PCs
- Remote-Desktop
  - die einfache Variante, aber in der Voreinstellung unsicher
  - wie wird das gesichert?
  - Iptables
    - Sicherung des Remote-Desktops in Zusammenarbeit mit SSH
- Familiennetzwerk mit SSH
  - Netz zwischen Benutzern, die sich gegenseitig vertrauen
  - ohne Zusatzsoftware, ist 'out of the box' vorhanden
- Zugriff auf den eigenen Desktop mit X2GO
  - mit SSH und eigener Session

Wo ist das Problem?



Remote Zugriff mit SSH, Installation

- Installieren, auf allen beteiligten PCs
  - Synaptic: **ssh**
    - Server absichern
    - Passwort-Login für alle Benutzer sperren

PermitRootLogin no
PasswordAuthentication no

  - Schlüsselpaar erzeugen und sichern (key-gen)
    - für jeden Benutzer auf dem Client
  - öffentliche Schlüssel auf die Server verteilen
    - Privater Schlüssel verbleibt auf dem Client
    - Öffentlicher Schlüssel kommt auf den Server (~/.ssh/authorized_keys2

- Router freischalten
  - Port 22 muss zum Server-PC durchgeleitet werden
  - Firewall im Router abschalten, bzw. Port 22 frei schalten

- Link
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/SSH

SSH-Netz

- Client-Server Struktur
  - jeder PC kann gleichzeitig Client und Server sein
  - Client-Benutzer hat beide Schlüssel
  - Server-Benutzer hat den öffentlichen Schlüssel des Client

- Wer → Wohin ?
  - Client initiiert Verbindung zu einem Benutzer auf dem Server
  - *ssh benutzer@server_IP_Adresse*
  - Client bekommt die Rechte von '***benutzer***' auf dem Server
  - d.h. der '***benutzer***' am Server stellt seinen Account dem Benutzer auf dem Client zur Verfügung
  - u.U. für die verschiedenen Clients Accounts mit unterschiedlichen Rechten auf dem Server anlegen
  - Vertrauen untereinander nötig (Familie,Freunde)

SSH Anwendungen, Terminal

- Terminal
  - „*ssh -X -C benutzer@IP-Adresse*„
    - einfaches Terminal, das aber grafische Ausgaben zurück sendet
  - Terminal vom anderen PC
  - Starten von Programmen auf dem anderen PC
  - Ausgabe kommt immer zu mir zurück
  - auch grafische Ausgaben
  - z.B. '*firefox*'
    - started Firefox auf dem anderen PC, wird aber bei mir angezeigt (!)
    - funktioniert mit allen Programmen
    - kann u.U. langsam sein

SSH Anwendungen, Filesystem

- FUSE (Filesystem in Userspace):
  - sshfs login/FolderAufDemServer FolderbeiMir
  - sshfs benutzer@IP-Adresse:/home/benutzer eeepcfuse
  - lösen mit 'fusermount -u eeepcfuse'

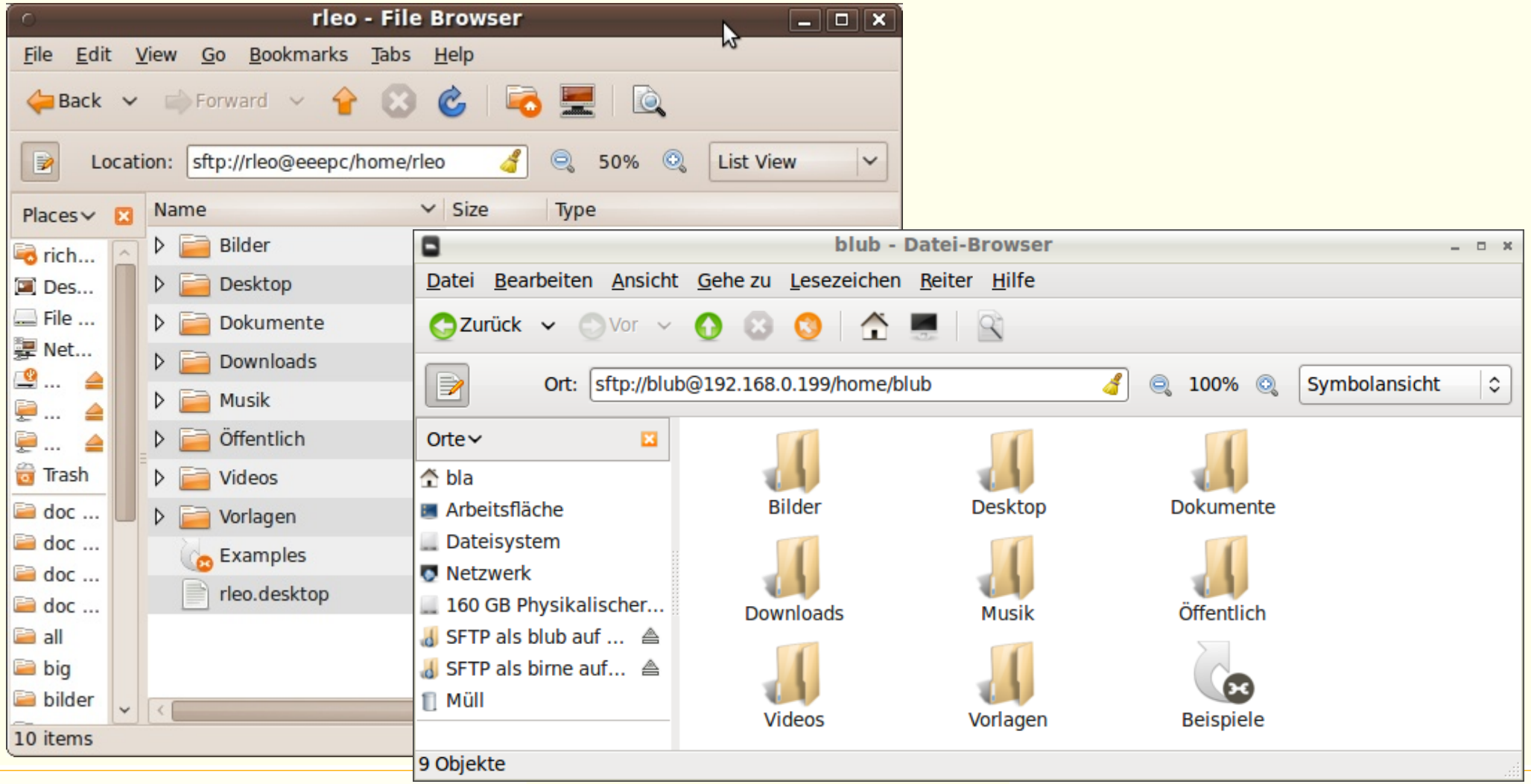
```
File  Edit  View  Terminal  Help
richard@ubuntu64:~/ssh/eeepc$ tree
.
|-- eeepcfuse
|-- fuse.sh
`-- ufuse.sh

1 directory, 2 files
richard@ubuntu64:~/ssh/eeepc$
```

```
File  Edit  View  Terminal  Help
richard@ubuntu64:~/ssh/eeepc$ tree
.
|-- eeepcfuse
|   |-- Bilder
|   |   `-- Webcam
|   |-- Desktop
|   |   `-- DPP0012.JPG
|   |-- Dokumente
|   |   |-- DPP0012.JPG
|   |   |-- DPP0013.JPG
|   |   |-- DPP0189.JPG
|   |   |-- Ubuntu_LinuxDay_2009.pdf
|   |   |-- linuxday09_12.jpg
|   |   |-- linuxday09_13.jpg
|   |   |-- linuxday09_15.jpg
|   |   |-- linuxday09_24.jpg
|   |   |-- linuxday09_35.jpg
|   |   `-- linuxday09_46.jpg
|   |-- Downloads
|   |-- Musik
|   |-- Projects
|   |   `-- all
```

SSH Anwendungen, Filemanager Nautilus

- Im Filemanager: „ssh://benutzer@IP-Adresse/home/benutzer



SSH Anwendungen, Remote Desktop

- Remote Desktop
  - "System -> Einstellungen -> Entfernter Desktop"
  - Freigabe auf dem Server durch Benutzer am Server
  - Zugriff vom Client
  - einfach, unsicher, Daten werden nicht verschlüsselt
- Lösung
  - SSH-Tunnel
    - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/SSH#SSH_Tunnel
    - ssh -L 590**6**:localhost:5900 benutzer@IP-Adresse
    - leitet Daten über den SSH Kanal zu den Ports der Anwendung
    - die Anwendung bemerkt davon nichts
  - Iptables
    - offenen Port 5900 des Remote-Desktop schliessen
    - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/Iptables
  - vncviewer am Client aufrufen
    - vncviewer :Screennummer aus dem Tunnel, siehe Anleitung
    - vncviewer :**6**
- Nachteil/Vorteil
  - der Benutzer am anderen PC muss eingeloggt sein
  - Maus und PC sind gekoppelt, ideal für Hilfeleistung

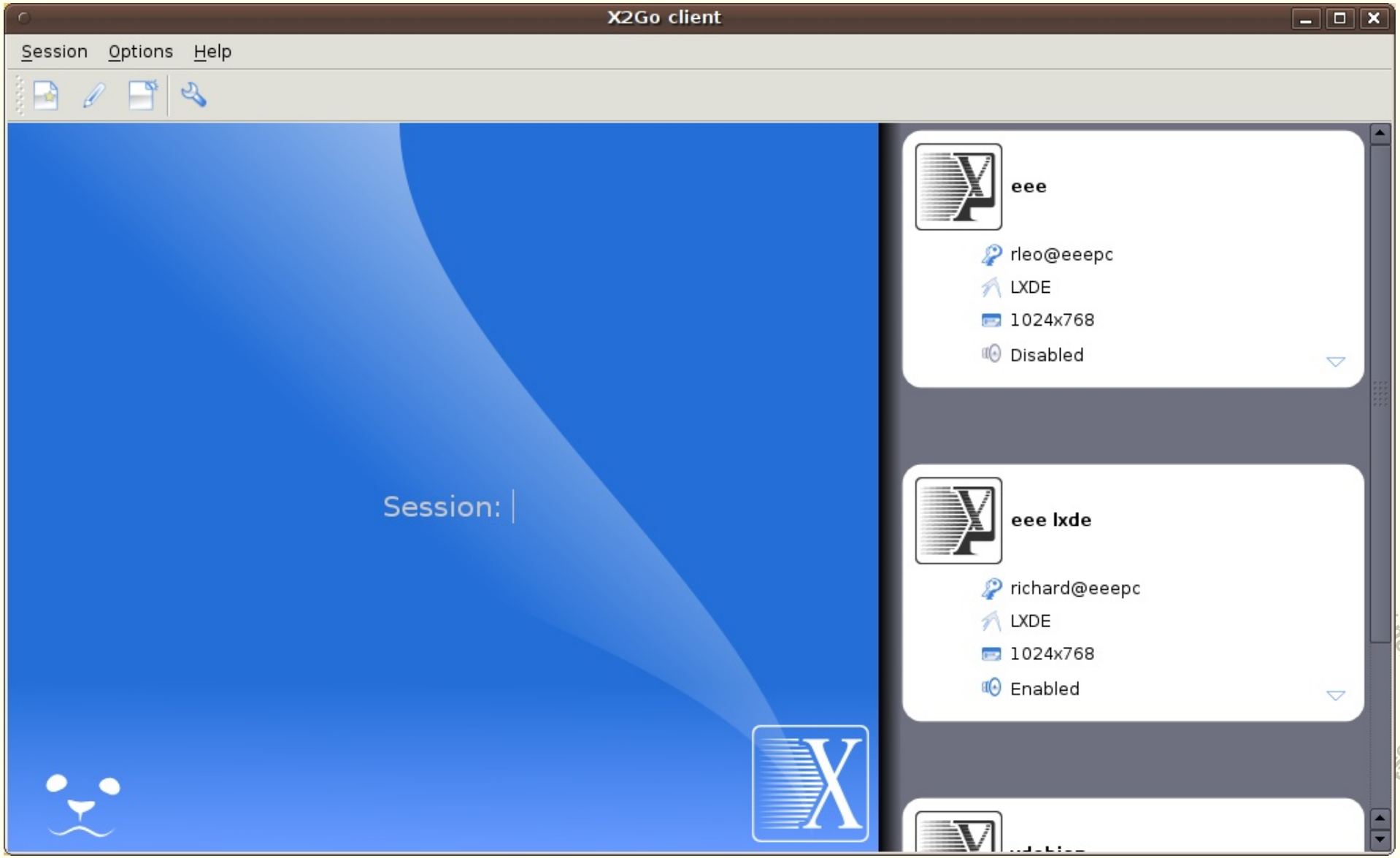
SSH Anwendungen: Remote Desktop mit X2GO

- X2GO
  - www.x2go.org
  - z.B. für den mobilen Einsatz
  - Server zu Hause installieren, keine Konfiguration, siehe:
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/X2GO
  - Client auf portablen PC installieren und SSH Parameter konfigurieren

  - jetzt benötigt man nur noch ein Stück Internet, egal, wie unsicher
  - und man hat 'seinen' PC zu Hause, als wäre er vor Ort
  - Sicherheit des Netzes entsteht durch SSH

- Vorteile/Nachteile
  - eigene Session
  - Benutzer am Server muss nicht eingeloggt sein
  - ideal für unterwegs
  - keine 'Fernsteuerung' des Desktops des Benutzers am Server

Remote Desktop mit X2GO



'Cloud Computing Hype'

- Cloud Computing
  - Daten und Proramme sind in der 'Cloud'
  - Zugriff über 'light' Clients
  - Sicherheit?
  - Wer vertraut wem?
  - Medienhype?
- http://de.wikipedia.org/wiki/Cloud_Computing

- Wollen wir das wirklich?
  - Vertrauen wir einem Provider, z.B google?
  - Oder geht es auch sicherer?

Wir machen privates 'Cloud Computing'

- mit normalen Linux Mitteln
- ohne Tricks und 'Hypes'
- frei nach Ockham: KISS

- Daten und Programme sind auf meinem PC zu Hause
- Sicherheit des Transportnetzes wird unwichtig
- Sicherheit entsteht durch privates SSH
- Zugriff über SSH
  - Terminal
  - grafische Programme (firefox, openoffice, gimp, ...)
  - Filebrowser (nautilus, dolphin, ...)
  - X2GO, ...

- Voraussetzung
  - stabiler, stromsparender PC zu Hause, der immer läuft
  - gute Internetanbindung mit ausreichend Upload (DSL, Kabel)
  - Notebook, Netbook, USB-Stick

- sehr sicher, Sie haben die Kontrolle

Virtualisierung für jeden

- KVM, Kernel based Virtuelle Maschine
  - ab 2006 im Linux-Kernel
  - von Ubuntu unterstützt
  - http://www.linux-kvm.org/page/Main_Page
  - benötigt spezielle CPU, Pacifica, Vanderpool (ist in fast allen neuen PCs enthalten)
  - benötigt viel RAM (64bit Ubuntu, 8GB)
  - benötigt zuverlässigen PC mit ausreichend CPU-Leistung
  - nicht teurer als ein normaler PC, beim Kauf beachten

- Verwendung
  - Aufbau eines lokalen Netzes ohne weitere Hardware
  - jeder hat 'seinen' PC in der Familie (virtuell)
  - Umzug vorhandener PCs ('Physical To Virtual')
  - 'Turnkey Appliances': http://www.turnkeylinux.org/
    - ca. 40 Ubuntu-Server, komplett installiert, mit je einer Applikation
    - Webserver, DB-Server, usw.

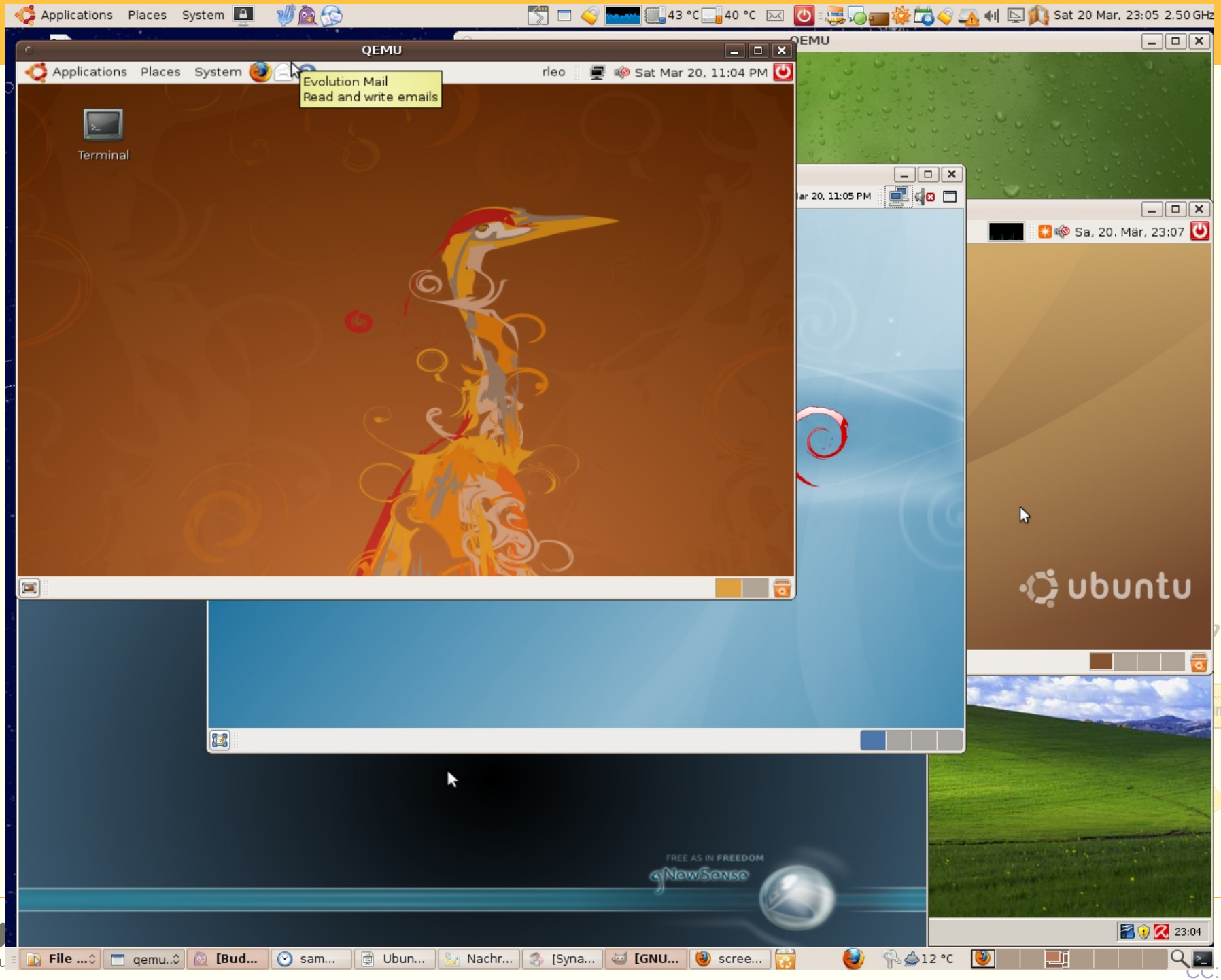
- Link
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Linuxeinstieg/KVM

KVM in Aktion

- 1 Host mit 8GB RAM und 6 VM

- Debian
- Dapper Drake (6.06)
- Hardy Heron (8.04)
- Mint
- gNewSense
- Microsoft Windows XP

KVM in Aktion



Skripte (zum Download)

http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/CookBooks/Linuxeinstieg

- SSH
  - Basis für sichere Netze
- Iptables, für Remote-Desktop
  - den Remote-Desktop auch über unsichere Netze hinweg verwenden
- Backup
  - bitte wirklich machen, es dauert mit diesem Script nicht lange
- X2GO
  - Remote Desktop von überall nach Hause
- KVM
  - der 'alte' PC bekommt eine 2. Chance als virtueller PC
- Repository downloaden
  - wenn man eine unzureichenden Internetanbindung hat

Ende ...

- 'to go the GNU/Linux/Ubuntu Way'

- Lernprozess
  - besserer Umgang mit dem Internet
  - bessere Kenntnisse im Umgang mit dem Computer
- Ergebnis
  - Sie werden staunen, was Sie alles im Umgang mit Ubuntu gelernt haben
- sicheres privates Netz
  - einfach, transparent, sicher
  - KISS (Ockham)

- Links
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/Main/HomePage
  - http://www.lug-ottobrunn.de/pmwiki/pmwiki.php/CookBooks/Linuxeinstieg

Vielen Dank für Ihre Aufmerksamkeit
und ein schönes Wochenende


THE HIGHWAY TO
FREEDOM IS NOW
OPEN FOR
EVERYONE
it's your turn to go ...