GNU/Linux/Ubuntu im sicheren und virtuellen Netz

GNU/Linux/Ubuntu im sicheren Netz

- Warum GNU/Linux/Ubuntu?
  - 'to go the Ubuntu Way'
  - Sicherheit
  - Unabhängigkeit
- gemeinsame Rechnerwelt für die ganze Familie
  - sicheres privates Netz in unsicheren Zeiten
  - Einsatz von SSH zum Aufbau eines sicheren Netzes unter Freunden
  - sicherer Zugriff über das unsichere Internet auf den PC zu Hause mit X2GO
  - Ressourcen bleiben zu Hause und sind von überall erreichbar
- Virtualisierung für alle mit Linux 'out of the box'
  - Was ist Virtualisierung?
  - Warum brauchen wir virtuelle PCs?
    - vorheriges BS, Netzwerk lokal testen, Distro testen
  - Installation und Betrieb mit einfachsten Linux Werkzeugen (KVM)

über mich

- Richard Albrecht, Jahrgang 49
  - Physiker / Uni Halle-Wittenberg
  - Fernstudium Theologie (in der DDR)
  - 1988 - 2000 am MPI für Biochemie Martinsried
    - 3-D Licht-Mikroskopie in der Zellbiologie
    - Bildverarbeitung, C Entwicklung
  - jetzt: Middleware, Datenbanken, .NET, Webanwendungen
  - Linux ist Ausgleich in der Freizeit

- Ubuntu 10.10, 64 bit, 8 GB RAM (für Virtualisierung)
- EeePC 901A

- Migration von PCs für ältere Leute
  - kein Virenscanner, keine Firewall, keine Viren, keine Trojaner
  - Installation wird von mir vorbereitet
    - einen Abend Einweisung
    - weitere Wartung durch Benutzer, kaum Probleme
  - bisher ältestes Ubuntu-System läuft seit 2005 (Breezy Badger)

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)
  - vom Uni-System zum ausgereiften Desktop
  - hohe Sicherheit für den Desktopbenutzer
  - in allen Sprachen verfügbar
  - sehr gute Hardwareunterstützung
  - sehr einheitlich, trotz der Vielfalt

Paradigmenwechsel

- KISS – 'Keep It Simple, Stupid'
  - Ockhams Rasiermesser
  - möglichst einfache, minimalistische und leicht verständliche Lösung
  - optimale Systeme
  - z.B. Internet, Linux,
    - Bücher von Eric Raymond und Rob W. Landley
    - 'The Art of Unix Programming'
    - 'The Art of Unix Usability'
- … let's go to GNU/Linux/Ubuntu

Warum Ubuntu?

- keine Fremdbestimmung durch Herstellerfirma oder deren Marketing
- gleiches System auf dem Netbook, Notebook, Desktop, Server
- kein Unterschied Home, Professional, Ultimate, Enterprise …
- immer aktuell, nie älter als wenige Tage
- hohe lokale Sicherheit, kein Virenscanner, keine Firewall nötig
- sicherer Zugang zu Software
- keine Lizenzprobleme
- ...

Warum Ubuntu?

- Cyberwar
  - stell Dir vor, es ist Cyberwar und wir gehen nicht hin …

- mehr Ökologie,
  - weil es nicht immer der neueste Rechner sein muss

- Filmhinweis:
  - 'Kaufen für die Müllhalde', ARTE Mediathek
  - „ein Artikel, der nicht verschleisst, ist eine Tragödie fürs Geschäft“
    - Zitat von Printers Ink, New York, 1928 (aus dem Film)
  - Geplante Obsoleszenz http://de.wikipedia.org/wiki/Obsoleszenz
    - Drucker, Software, Hardware → künstlich 'alt' gemacht?

Warum sollten wir Ubuntu verwenden?

- und, da fehlt noch etwas?

  - herkömmlicher PC ist Ursache für Bluthochdruck ;-)
  - Ubuntu senkt den Blutdruck!
  - Ubuntu verbessert die Gesundheit ...
  - … denn Ubuntu ist stressfrei

Unsicherheit und eine verblüffende Lösung

- O-Ton MS (Übersetzung bei Heise)
  - **„Um die wachsenden Probleme mit Botnetzen unter Kontrolle zu bekommen, sollen infizierte PCs vom Internet isoliert werden. „**
  - Microsofts Vizepräsident für Trustworthy Computing, Scott Charney
  - http://go.microsoft.com/?linkid=9746317
  - Quelle: Heise, 8.10.2010

- Configuring a Windows PC For a Senior Citizen
  - http://tech.slashdot.org/article.pl?sid=08/12/24/0138213
  - Google Suche: 'slashdot Senior Citizen'
  - Ergebnis der langen Diskussion: **nimm Ubuntu** …

erste Schritte, to go the Ubuntu Way

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

- einfach nur benutzen
  - es geht alles wie von selbst
- täglich damit arbeiten
  - dem allwissenden '*PC-Guru*' kündigen *(Nachbar, PC-Freak, 'guter Freund'...)*
  - nie jemanden an den Linux-PC lassen, der sich '*mit Computern auskennt*'
  - Ubuntu ist nicht das,

    was 'man' so aus der bisherigen Erfahrung kennt
  - sich auf GNU/Linux/Ubuntu einlassen und selbst lernen
- 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

- Links
  - http://lug-ottobrunn.de
  - http://www.lug-ottobrunn.de/wiki/Kategorie:Linuxeinsteiger


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

GNU/Linux/Ubuntu im sicheren Netz

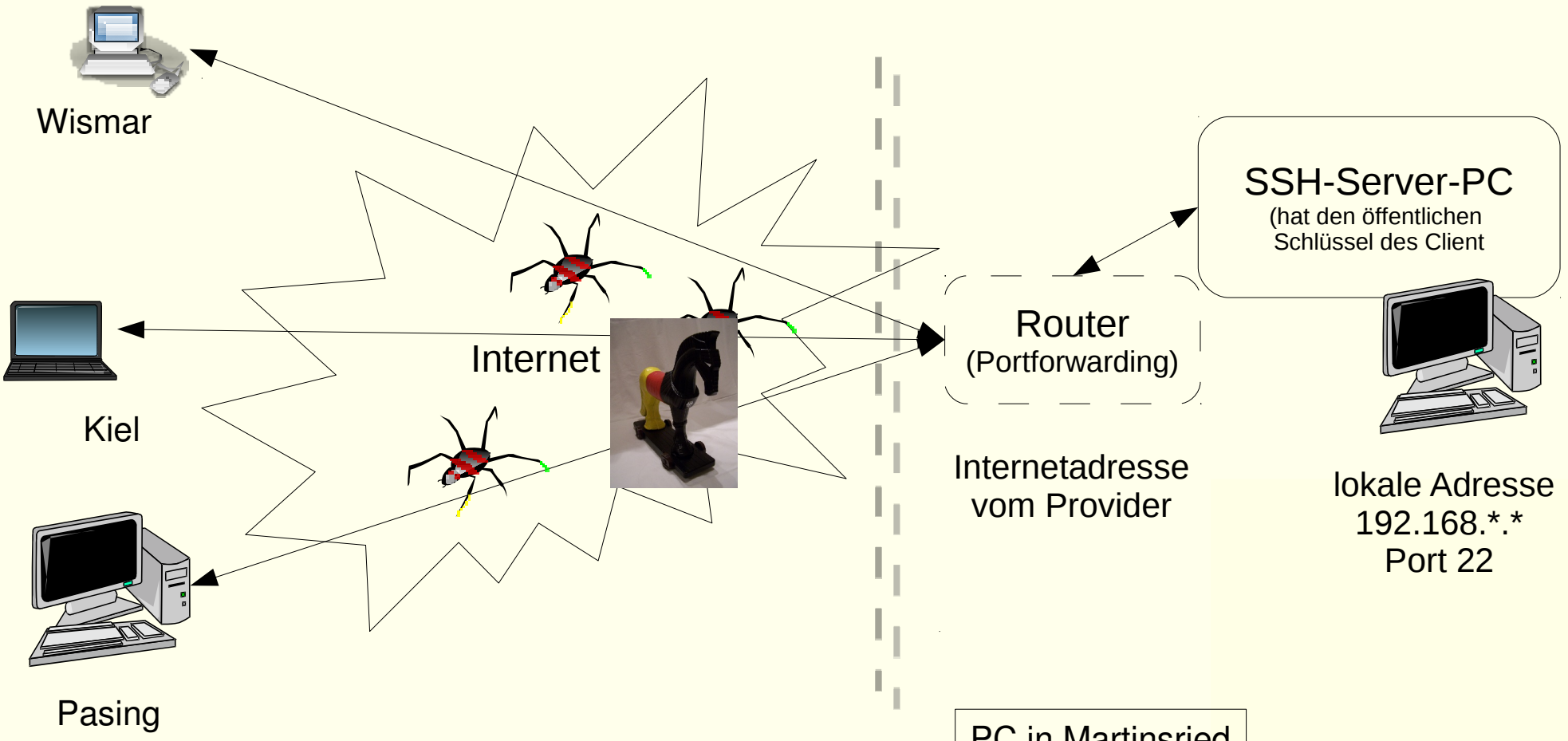
sicheres Netz für die Familie

- Warum?
  - Grundgesetz, s.o.
  - Überwachung des Traffic nimmt zu (z.B. De-Mail, keine vollst. Verschlüsselung)
  - 'Deep Paket Inspection' ist sehr wahrscheinlich (siehe MS Paper oben)
  - Alvar Freude: Zwei Personen kontrollieren 250 Personen http://odem.org/insert_coin/

- SSH
  - universelle sichere Verbindung (verschlüsselt)
- Was kann ich damit tun
  - sichere Terminal Verbindung
  - Ausgabe von Programmen umleiten
  - Filemanager verteilt verwenden
  - mit Tunnel beliebige Programme sicher ins Netz beringen

- Familiennetzwerk mit SSH
  - Netz zwischen Benutzern, die sich gegenseitig vertrauen
  - ohne Zusatzsoftware, in Linux '*out of the box*'
  - Zugriff auf den eigenen Desktop mit X2GO

sicheres Netz in unsicheren Zeiten ….



http://de.wikipedia.org/wiki/Datei:Bundestrojaner.jpg, CC:by-sa

Voraussetzungen für die folgenden Abschnitte

- Installieren von Programmen
  - Synaptic, apt-get
  - Hilfesystem (man, info)

- Terminal
  - öffnen, einfache Kommandos absenden
  - arbeiten als root, sudo -s

- Netzwerk
  - Internetadressen, Namensauflösung, DynDNS
  - Dienste, Ports (steht in /etc/services)
  - Router, Modem
  - Rolle des Providers

Remote Zugriff mit SSH, Installation

- SSH installieren (auf allen beteiligten PCs)
  - # apt-get install **ssh**
    - **Server absichern**
    - Passwort-Login für alle Benutzer sperren
    - steht alles in den Links unten

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 (bzw. der für SSH gewählte Port) muss zum Server-PC weitergeleitet werden
  - Firewall im Router abschalten, bzw. den SSH Port freischalten

- Links
  - http://www.lug-ottobrunn.de/wiki/SSH_Simple
  - http://www.lug-ottobrunn.de/wiki/SSH_Spickzettel

SSH-Netz

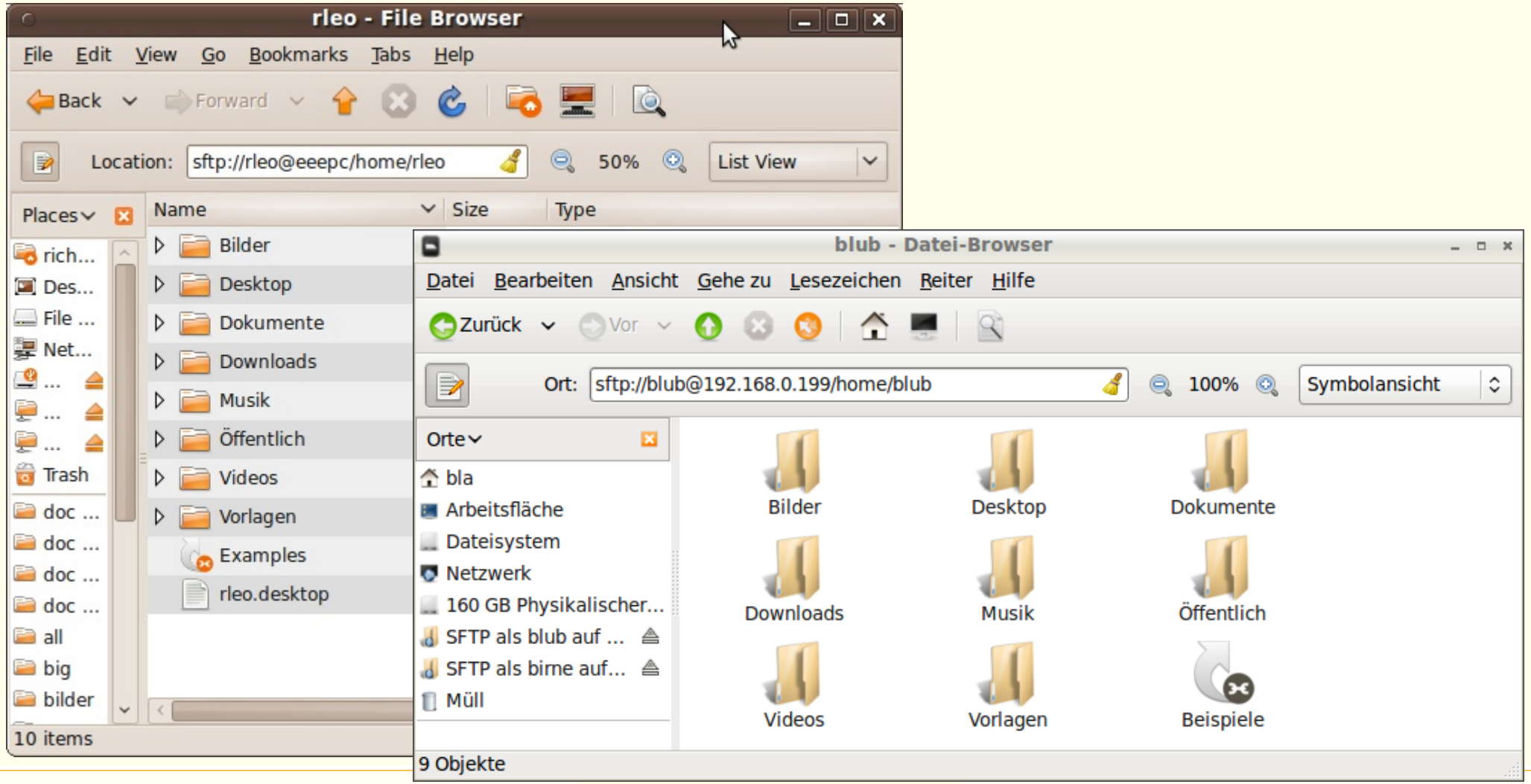
- Client-Server Struktur
  - jeder PC kann gleichzeitig Client und Server sein
  - Client-Benutzer hat beide Schlüssel
  - Server-Benutzer hat den öffentlichen Schlüssel des Client

- 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 zur Verfügung
  - Vertrauen untereinander nötig (Familie,Freunde)

- Anwendungen
  - Terminal, Filemanager, Desktop, Tunnel

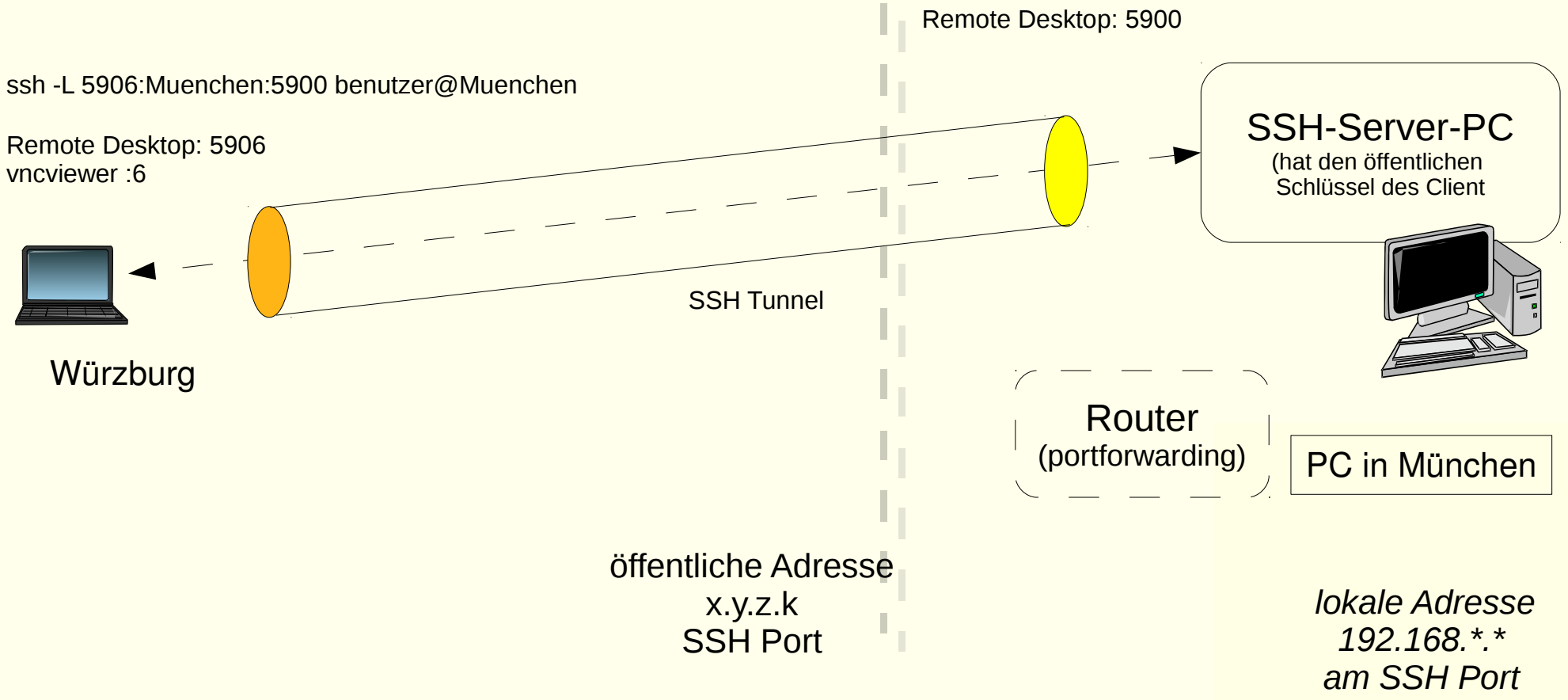
SSH Anwendungen, Beispiel Filemanager Nautilus

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



SSH Tunnel, Beispiel Remote Desktop (VNC)

- Remote Desktop sendet auf Port 5900 + Offset
- Offset erlaubt es, mehrere Desktops zu verwalten
- der VNC Betrachter muss nur den Offset 'wissen'



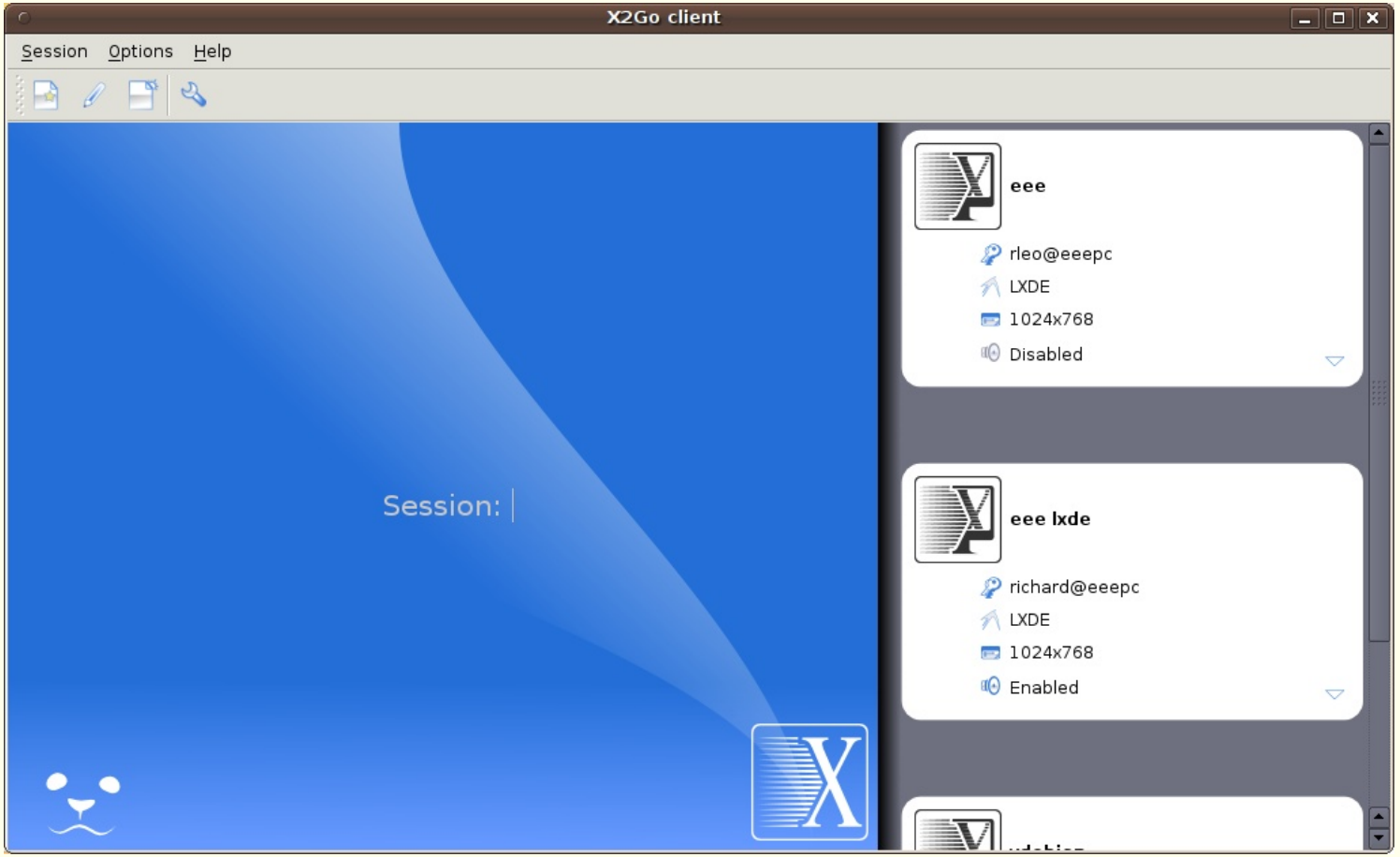
SSH Anwendungen: Remote Desktop mit X2GO

- X2GO
  - www.x2go.org
  - z.B. für den mobilen Einsatz
  - Server zu Hause installieren, keine Konfiguration
  - # apt-get install x2goserver-home
  - http://www.lug-ottobrunn.de/wiki/Remote_Desktop_mit_X2GO
  - Client auf portablen PC installieren und SSH Parameter konfigurieren

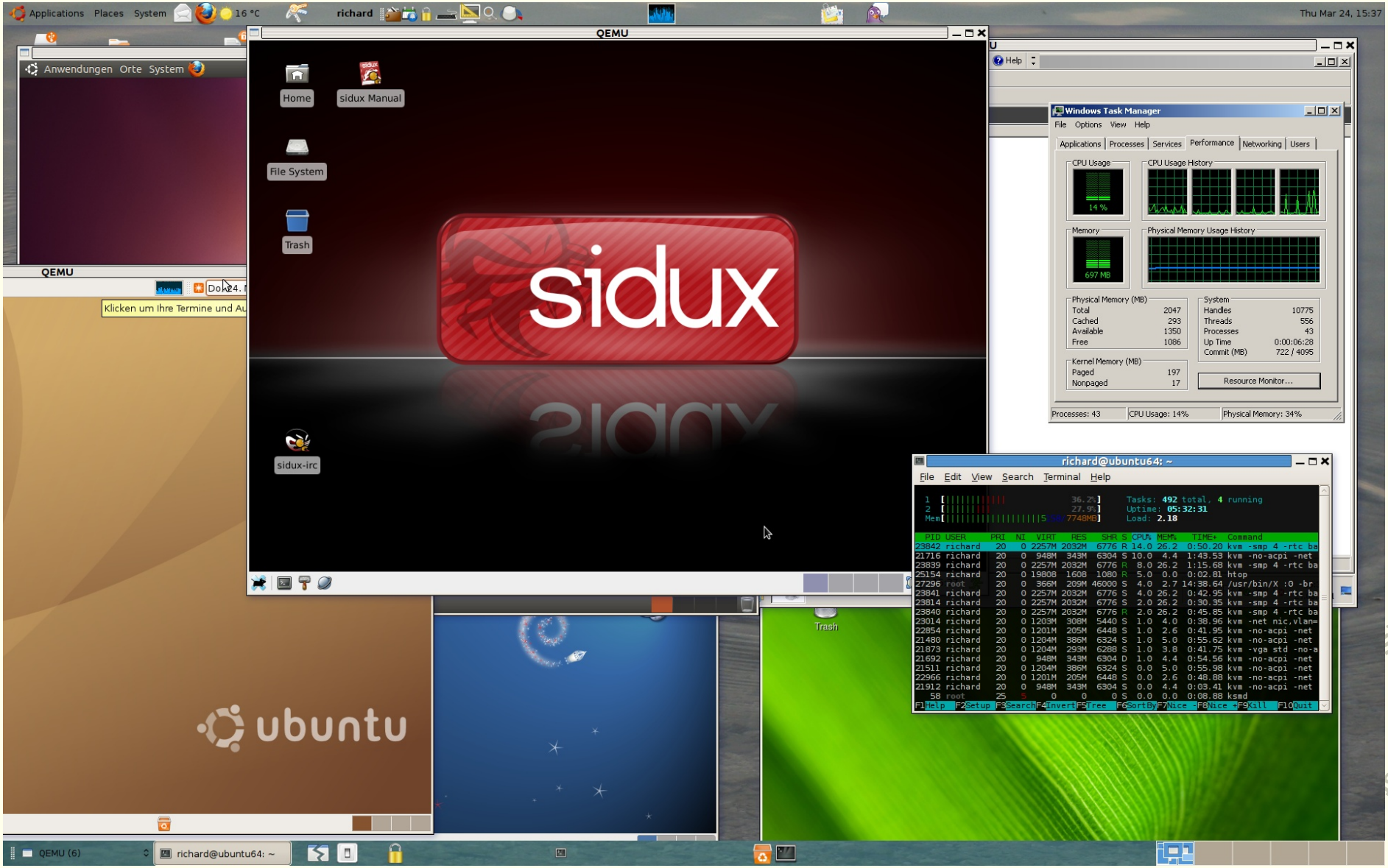
  - jetzt benötigt man nur noch ein Stück Internet, egal, wie unsicher
  - und man hat 'seinen' PC zu Hause, als wäre er vor Ort
  - Sicherheit des Netzes entsteht durch SSH

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

X2GO, so sieht es aus



Virtualisierung mit KVM



Was ist KVM ?

- Kernel Based Virtual Machine
  - Seit 2006 im Kernel, basiert auf QEMU
  - von Ubuntu favorisiert
  - KVM Buch http://qemu-buch.de/de/index.php/Hauptseite
  - http://www.lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

- PC im PC
  - alle Teile eines PC werden über Software simuliert
    - Festplatten, Maus, Netzwerk, Grafik usw.
- Voraussetzung
  - moderner PC, mit Virtualisierungserweiterung in der CPU

- Performance (Beispiel aus der Praxis)
  - 36000 XSL Transformationen (XML nach XML umwandeln)
  - **Vista**, native CPU, Intel Q9550, Quadcore, **4 GB RAM**, 32 bit
    - Laufzeit: 13m:12s
  - **XP** in KVM, 1 GB RAM, 32 bit
    - Laufzeit: 12m:52s
  - **Host**: Ubuntu, 64 bit, AMD 4850e, Dualcore, **8 Gig RAM**

Installation von KVM

- Siehe Webseiten von 'ubuntuusers.de' und 'ubuntu.com'
  - http://wiki.ubuntuusers.de/KVM
  - http://wiki.ubuntuusers.de/QEMU
  - https://help.ubuntu.com/community/KVM
  - Install **qemu-kvm** und testen
    - $ **kvm-ok**
    - INFO: Your CPU supports KVM extensions
    - INFO: /dev/kvm exists
    - KVM acceleration can be used
  - Details auf den Webseiten

- KSM Intervall erhöhen
  - 'Kernel same page merging' ist oft zu knapp eingestellt (alle 20 msec)
  - http://www.linux-kvm.com/content/using-ksm-kernel-samepage-merging-kvm
  - in /sys/kernel/mm/ksm
  - in File: sleep_millisecs 200 eintragen

Einbinden in das lokale Netz

- per default hat KVM ein eigenes Netz hinter einem Router
  - Sicherheit durch Firewall im Router
  - VM kann Internet erreichen, aber nicht den Host
  - Host kann VM nicht erreichen

- bridge utils
  - https://help.ubuntu.com/community/KVM/Networking
  - '*Creating a network bridge on the host*'
  - $ sudo apt-get install bridge-utils

- Networkmanager deinstallieren
  - Netzwerk in */etc/network/interfaces* einrichten

```
auto br0
iface br0 inet static
        address 192.168.0.10
        network 192.168.0.0
        netmask 255.255.255.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
        bridge_ports eth0
        bridge_stp off
        bridge_fd 0
        bridge_maxwait 0
```

Setzen der Rechte, KVM benötigt für das Netz 'sudo'

- # chmod 660 /dev/kvm, von Hand oder in in 'rc.local' eintragen
  - KVM Device ist damit für die Gruppe 'kvm' benutzbar

- Netzwerk über File 'sudoers' ermöglichen
  - /etc/qemuif-up.sh usw. benötigen 'sudo'
  - mit 'visudo' in File 'sudoers' eintragen
  - so sieht es aus:

```
%kvm   ALL=NOPASSWD: /usr/sbin/tunctl, /usr/sbin/brctl, /sbin/ifconfig, /sbin/ifup, /sbin/ifdown
```

Meine Skripte zur Verwaltung (kommentierte Skripte am Stand)

- MAC Adressenliste

```
test        192.168.10.31  DE:AD:BE:EF:E0:01 vtest
maverick    192.168.10.36  DE:AD:BE:EF:E0:06 vmaverick

winw2k      192.168.10.62  DE:AD:BE:EF:F0:02 vw2k
winxp       192.168.10.63  DE:AD:BE:EF:F0:03 vwinxp
win7en      192.168.10.64  DE:AD:BE:EF:F0:04 vwin7en
```

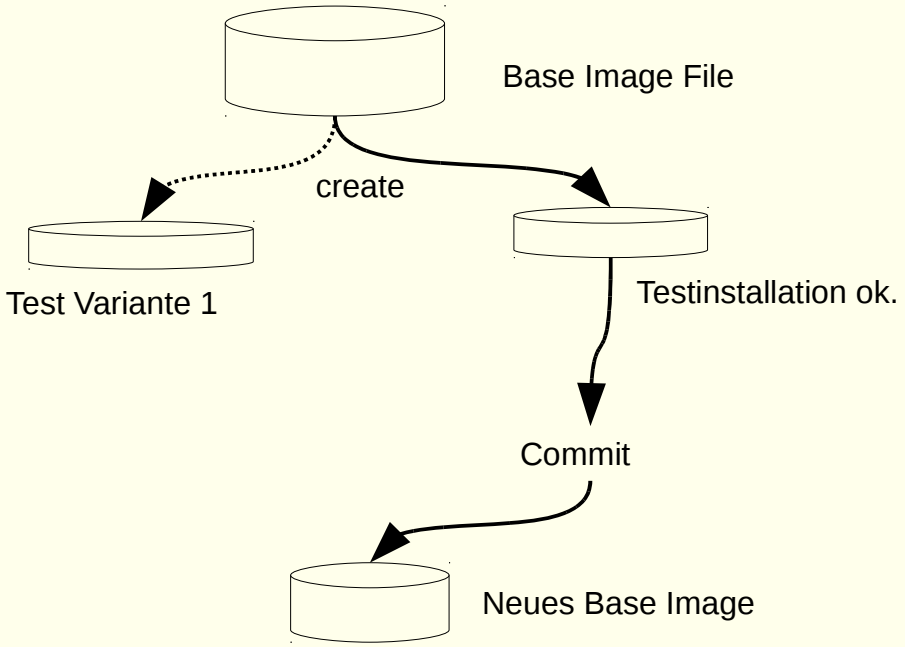
- Startfiles mit den Parametern

```
#!/usr/bin/env bash
SYSTEM=winxp
MAC=`grep $SYSTEM ../../config.txt | awk '{ print $3 }'`
USERID=`whoami`
iface=`sudo tunctl -b -u $USERID`
model=rtl8139
RAM=768
nohup kvm -rtc base=localtime -net nic,vlan=0,macaddr=$MAC -net tap,vlan=0,ifname=$iface \
        -m $RAM -hda $SYSTEM.ovl $@
sudo tunctl -d $iface &> /dev/null
```

- Statische IP oder eigener DHCP und DNS Server im lokalen Netz
  - # apt-get install **bind9**
  - # apt-get install **dhcp3-server**

COW – copy on write

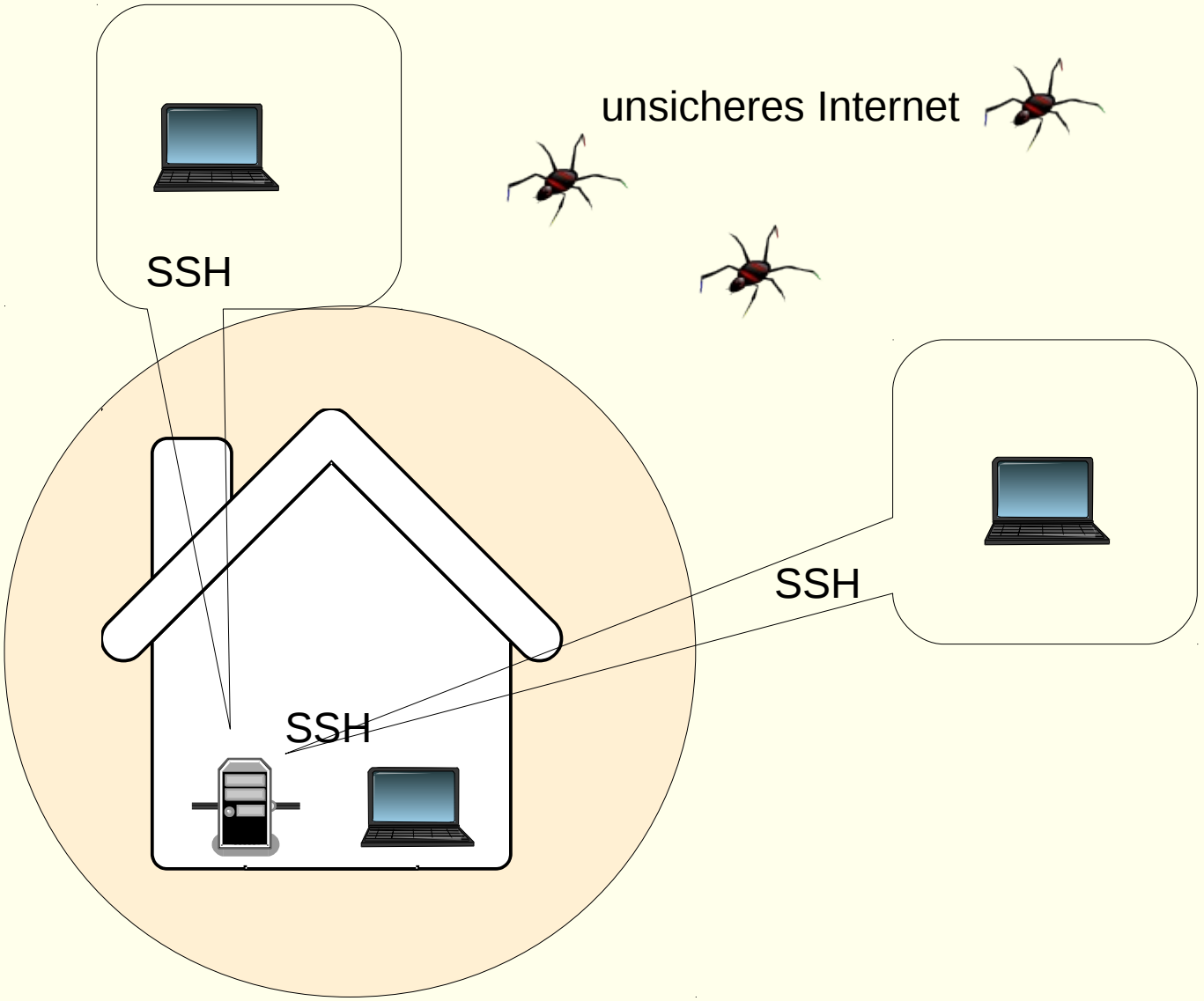
- Copy On Write
  - geänderte Blöcke werden nicht überschrieben
  - in „Overlay“ abgelegt
- Kommandos
  - $ qemu-img **create** -b base.raw -f qcow2 overlay.ovl
  - statt base.img jetzt overlay.ovl starten
  - $ qemu-img **commit** overlay.ovl



Was kann man jetzt alles machen

- Live CDs testen, Mini Demo
  - $ kvm -hda test.img -cdrom file -boot d
- Umzug eines alten PC
  - http://www.lug-ottobrunn.de/wiki/Umzug_eines_PC_nach_KVM
- Overlays
- Snapshots
- QEMU Monitor (ctrl-alt-2)
- Demos am Stand *maverick, dapper, debian, arch, sidux uvam.*
- Demo mit 64 bit win2008 und 4 CPUs
  - SSH Tunnel zum Remote Desktop einrichten
  - Gast kann kein SSH, ist aber durch SSH erreichbar (!)
  - SSH -L 10025:vwinxp:3389 lug1@example.com
  - mit „grdesktop“ sich mit dem Gast verbinden
  - gezeigte VM hat 4 virtuelle CPUs (!) und 2 GB RAM

privates sicheres Netz
sie haben die Kontrolle



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)

- KVM
  - alter PC lebt weiter
  - jedem sein PC, egal, wo man sich aufhält

Vielen Dank für Ihre Aufmerksamkeit
und einen schönen Linux-Infotag