LUG Ottobrunn - München Südost

GNU/Linux/Ubuntu im sicheren und virtuellen Netz

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/C++ Entwicklung
  - bis 2011: Middleware, Datenbanken, .NET, Webanwendungen
  - jetzt: Software für CCD Kameras bei SVS-Vistek in Seefeld

  - Linux ist seit 2006 Hobby Nr.1
  - Vorträge, Linuxtage

- Hilfe bei der Umstellung von PCs nach Linux
  - **keine** Viren**, keine** Trojaner**, kein** Virenscanner, **keine** Firewall
  - Installation wird von mir vorbereitet
    - eine kurze Einweisung
    - weitere Wartung durch den Benutzer
    - 'Altlasten' umlagern nach Windows 7 mit KVM
  - www.rleofield.de

Themen

- Warum Sicherheit der privaten Daten?
  - Grundrecht
  - Privatsphäre
  - Unabhängigkeit
- Sicherheit ist 'out of the box' vorhanden
  - unkompliziert, mit Linux für alle einsetzbar
- gemeinsame Rechnerwelt für die ganze Familie
  - sicheres privates Netz in unsicheren Zeiten
  - Einsatz von SSH zum Aufbau eines sicheren Netzes unter Freunden
  - Ressourcen bleiben zu Hause und sind von überall her erreichbar
- Virtualisierung für alle mit Linux
  - Was ist Virtualisierung?
  - Warum brauchen wir virtuelle PCs?
    - 'Altlasten', Linux Varianten testen, Surfstation, Mini-Server, uvam.
- Was zeige ich nicht?
  - komplizierte Rezepte und Anleitungen
- Was zeige ich?
  - was möglich ist und wo Sie das finden
  - http://www.lug-ottobrunn.de

Zeitenwechsel

- 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“
- Sicherheit ist anders geworden
  - Bundestrojaner entdeckt
    - Bericht CCC, FAZ 8.10.2011
    - Super GAU der Computersicherheit
    - es werden kommerziell Trojaner hergestellt
    - man verliert die Kontrolle darüber
    - Websperren, Vorratsdatenspeicherung
  - Stuxnet
  - 'drohender Cyberwar' (in den Medien und bei Politikern)
- Unsicherheit am PC ist Alltag, 3 Beispiele der letzten Woche
  - „GVU-Trojaner bittet Raubkopierer zur Kasse“ Heise online 20.03.2012 16:40
  - „Werbe-Trojaner mit Schweizer Segen“ (Trojaner mit Zertifikat!) Heise online 19.03.2012 11:22
  - „Exploit für Windows-RDP-Lücke im Umlauf“ Heise online 16.03.2012 17:55

Fragen

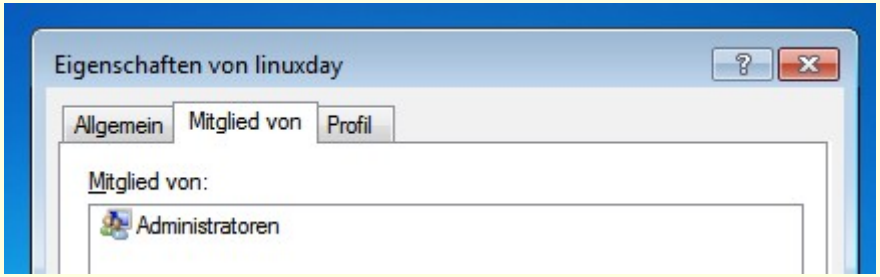
- Sind wir davon betroffen?
  - nein, Linuxviren gibt es nicht
  - ja, wenn wir mit Linux so umgehen, wie wir das mit Windows gewohnt waren

- Lösung:
  - sich auf Linux einlassen und **selbst** lernen
    - Wikis lesen (z.B. ubuntuusers.de)
    - Community kennenlernen (LUG vor Ort, Linuxtage)
  - Linux ist nicht wie der bisherige PC
    - Erfahrungen aus der bisherigen PC Welt werden gegenstandslos
    - Vorsicht! Sie können 'Freunde' verlieren (und den Job)
    - ein Windows-Nutzer mit langer Erfahrung muss erkennen,
      dass er wieder ein Anfänger geworden ist
  - dem ***'allwissenden PC-Guru'*** kündigen *(Nachbar, PC-Freak, 'guter Freund' ...)*
  - niemanden an den Linux-PC lassen, der sich '***mit PCs auskennt***'

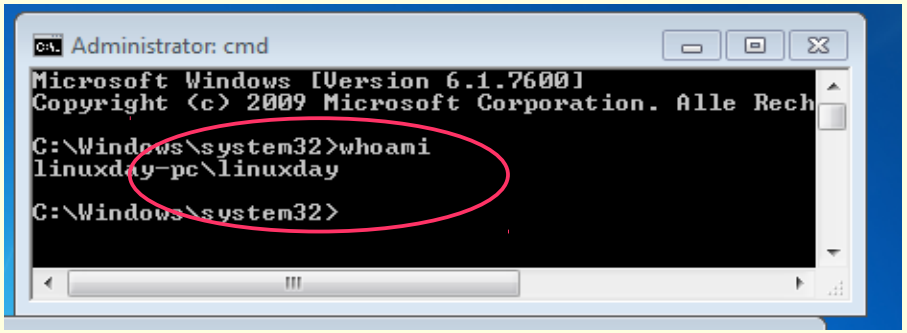
es ist Ihre Entscheidung . . .

Default Sicherheit, Beispiele aus Windows 7 und Ubuntu

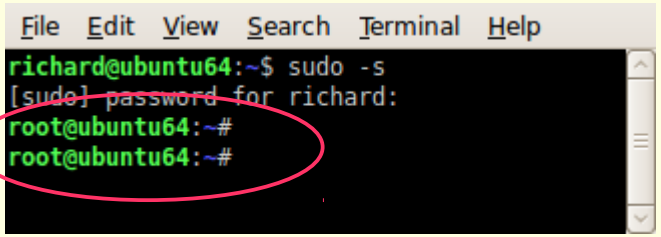
Benutzer nach Installation ist Admin, kein Hinweis darauf
(sehr viele Nutzer wissen es nicht)



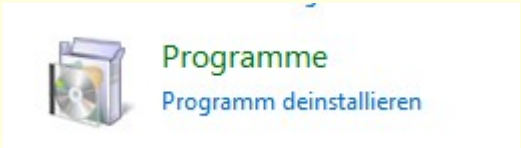
User ***linuxday*** bekommt mit UAC ***Administrator-Rechte***
(ohne PW, nur mit Klick, Zustand ist nicht gut sichtbar)



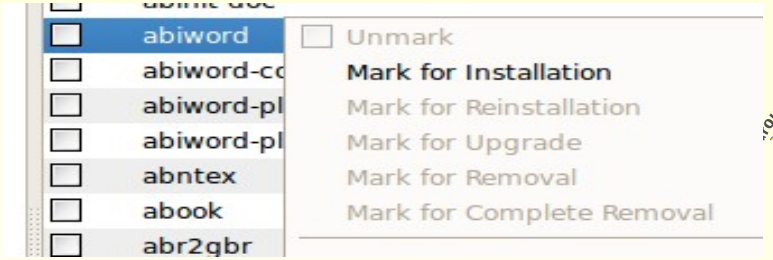
User ***richard*** bekommt keine ***Administrator-Rechte***
richard wird mit 'sudo' für ein Programm ***root***
(nur mit Passwort, Zustand ist gut sichtbar '#',
alle Linux-Benutzer kennen den Unterschied)



Programme, nur deinstallieren, nicht installieren
(Systemsteuerung, nur mit GUI)



in **Ubuntu** installieren und deinstallieren
(viele Möglichkeiten)



Sicherheit im Netz (für Windows und Linux)

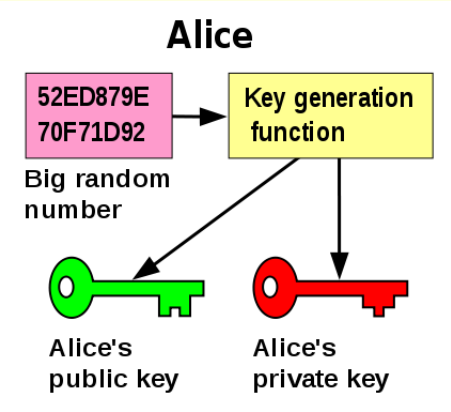
- PGP für Mails
  - *Schlüssel unter voller Kontrolle*
  - Mails müssen dabei unter eigener Kontrolle sein
  - in Linux: GPG = Gnu Privacy Guard

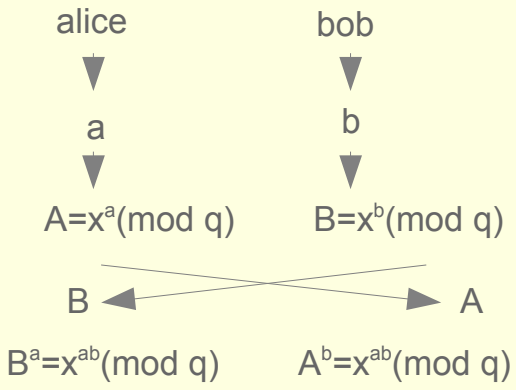
- HTTPS gegen 'abhören'
  - *Schlüssel über CA, der man vertrauen muss* (?)
  - CA = Certificate Authority
  - Surfen über unsichere Netze,
  - Authentifizierung der Webseite (eBanking, Shops)

- SSH zur privaten Kommunikation unter Freunden
  - *Schlüssel unter voller Kontrolle*
  - sicherer Tunnel zum Zugriff auf andere Rechner
  - Erlaubnis des Besitzers nötig
  - SSH bei Windows nicht dabei, es gibt aber OpenSSH

Public-Private Key Verschlüsselung

- http://de.wikipedia.org/wiki/Public-Key-Verschlüsselungsverfahren
  - Basis ist Produkt von sehr großen Primzahlen (z.B. 3 * 5 = 15)





-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBE9bsgQBCACknQnvfkisPVZ9EtxLsvlZdq5flz22hXeWbhsb59K7hgG/Sr2E
SFmVyL+RvDlFAl+quuRf1xl0R5EzhzXgvab8mbJVoSeHjCmjfMV9llzoiK5q1hON
xofESkQ98wMe5CdE5jj96qK/LrLlvVX7Mpndy7gx28766i1SjNvJnx7YDwzvtPwO
cYCdHgd2kuXFX3bsodkUu4HesQpTiYOTAaudLmaKwDyOqcpWwc/LnfSgFtmCFwmR
OeaqE0/V8wnHX4aJkmLVgBGFKOyqHUkdoIb4l/rU39RnlEPEqieaUC6b2UH4LmZc
hB6HF7soLUR1vwevzgwDzuxScgXfRqNIjeSxABEBAAG0ImFsaWNlIChhbGljZSkg
PGFsaWNlQHJsZW9maWVsZC5kZT6JATgEEwECACIFAk9bsgQCGwMGCwkIBwMCBh
UI
AgkKCwQWAgMBAh4BAheAAAoJEHIDBu3RqBNwi8QH/iirqP+dSj9op1unn/ooMZHy
pABd7IFGUXrdjjEY2/2O1T3zei+DGCyJITDcoBbAHucPikPo7kBxGHlz8GTzIRpn
8kivCe9XlQ1+PWKs28ujSV4hPHe4rvlfT+Pj7SOeyVXTFxWf9+B7bxCL7N395UWW
CN7EaSwxI1Wr398+zXHxGyPytrsPF/Dyt75z1az9eatBtmoLReYYx9q02VBxLHTN
Bn+zcQwZNVNKbqUO7ByTdDuYpmUS9JxEp91+DfLSbcRdd2y0zaKJyf+gl6n7j2nn
cuGlYBw5dzWuI5XdrKgdWxS0Usm7DscnHfgpxmlP43EVYGYy0XBvVsSdKBqPos2J
ARwEEAECAAYFAk9eT0sACgkQ7oQvcWqaLQ1yYwgAgQYCL7U6EaicMledrRL5I9+8
WoL8UQNT93yBv6REXdEsBX6uSgnwC1AJkk1TzgKJxAabIqJMJAf1LutBQ9eO6az1
Dl9Up0duWEZukR7TZJln/jJdKXazbtMorirrtEOXseLcpInveDTYbaN89x3i1xly
hrMYKD12iZoDbkSlWEvMD9Lai2Aasvnqi0k6Hzu0eKUy1quahKlb1YejgrqDcvsF
iLpS3CKvXpqk/Kn8Kf8nc/XGgOjeSj5vkVqUmk38mMRMeRC/KkH4J54wR7wn2V9k
qjhozt5pQkWKc4MII7qLbdOV1afPQQyPntlI5EGLJOzgUY71abNdhKnqmEbTyLkB
DQRPW7IEAQgAuG6wPfxseliLzO9MG9+HqpeRJ8QS6wuUNMFjWc6oljLeiPmCWVOK
MSlC1i2+msOuL/nccu8QUowDmXeB5vHUla1Hdh8Jsz8azptf6eHxYW7fB1hhjtml
7Kt/XUO+e0bv5Vf6B10/XfudROMNakQEncObjghuiyYozuBkh6wK9R9mKjcBtMI+
x3zeVUVNST4WMRo2zAHpgi4C1YD+sZIT1pAC84HmuFh+JRXdU1I51V9gs5zqlowC
O3NjOdNVI2WDw0e0comv3sVqcLlizu74Zwzyzm4iTQI9I5BdMGczk5dpz1jySp4h
aPLXmGVvHUHaru3dcfo6gjWRwhVTcOhU1QARAQABiQEfBBgBAgAJBQJPW7IEAhsM
AAoJEHIDBu3RqBNwpH0H/RAt/UAC5eATuxBEXzVWMK1dyYY0/fVTEXzX8hu5lgeq
/Puh0XHP1eGkSfpkJNjIlkrUOyCx72LEJxkj7WbISKO9rRg9IORXlM3ZO596L8CW
jZ0zd3BimGoN2oXl/xCvYxER/JIF7PEF62wtWWTH+U0WB2cSs9Fgn9OJM39hwEZ7
GgS6Elnph7gsP78kLY0ay44Xl44nJwXIsYC0Wf8NXVP6pCfDSf+rqVjcYzQlBj4Q
QHV8OtQlesK3w1KKUHG0FANyIHbaeYle7UYL80yk6fU5YUNo7JMiKDndlYbGMPeI
hKYfQxTyuZtl6hTqmmPdF4mmfKScj4qBjqjosXUCx8g=
=yCO4
-----END PGP PUBLIC KEY BLOCK-----

Fingerprint zur Verfizierung:

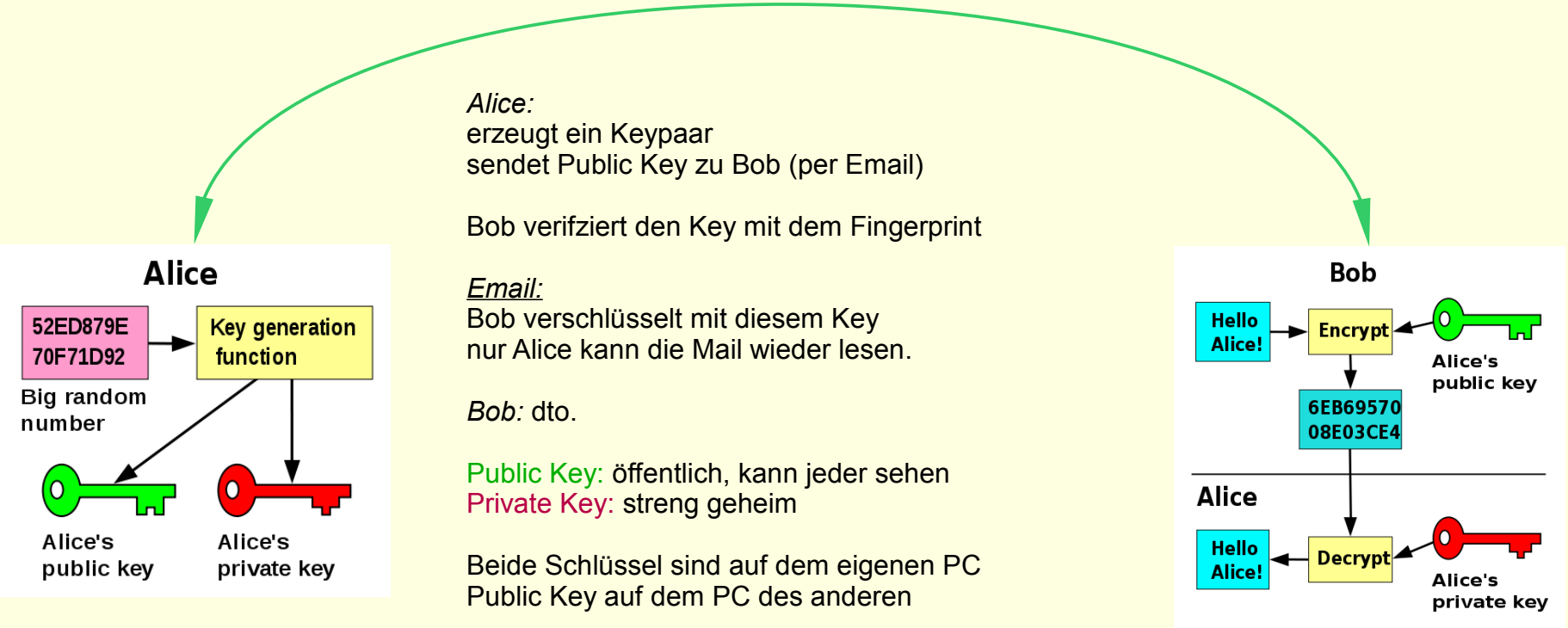
697C 7375 A84C 4597 D0A9
3143 7943 06ED D1A8 1370

-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

lQO+BE9bsgQBCACknQnvfkisPVZ9EtxLsvlZdq5flz22hXeWbhsb59K7hgG/Sr2E
SFmVyL+RvDlFAl+quuRf1xl0R5EzhzXgvab8mbJVoSeHjCmjfMV9llzoiK5q1hON
xofESkQ98wMe5CdE5jj96qK/LrLlvVX7Mpndy7gx28766i1SjNvJnx7YDwzvtPwO
cYCdHgd2kuXFX3bsodkUu4HesQpTiYOTAaudLmaKwDyOqcpWwc/LnfSgFtmCFwmR
OeaqE0/V8wnHX4aJkmLVgBGFKOyqHUkdoIb4l/rU39RnlEPEqieaUC6b2UH4LmZc
hB6HF7soLUR1vwevzgwDzuxScgXfRqNIjeSxABEBAAH+AwMCIc+AzIyv6TVgHZa1
ggqLnI0rY96ezT/1vVWPQTAo+j8PpJcNbJLO0S+PRGqYD2FfjId4aHcTCYOXDjnVW
p5VXQiJAzEXEC/5q6PTcRnsdkjyHs7rpUABxYjYn4ZhNtWeslptOg7tTuwjYyV+h
AMxjylC7DB0PPRuG/cZQdx+vYYI1fyahTOaJOZMvXUEDRU+j3fX2K7GT8xkwmZFf
upAwXGziAcW78E8PF7yJ7XAIICx/RY6iemzy8dbvbFTKPPL4BJ+tT03IWxxoZf+A
k6AC9wOXWyBl2MR1Xls4REl9CKQpszFVr5pH6vwVLS0Lk+1L1orLuy0RNNuFI7G2
WwnDEigqc3hIo4ONcDP/KrbBIM5vE//DIPAFTisxoz7eq6CKlQOwG+yVlMdaA8Bv
GFrNoZP2kfA5HNX7tQNp78tO2V4Tt6vrN+7lTaSHMncAzdBF650F+P4yKMA9tjwl
+mx+OSGnkV7iz+TnFpxRhSUmAfE91wFO0hoGM1mtZqkTucSyuPYbcq7pvVtSa/NP
XtGtlhIWWLxW6hkzB8Nkf41Gg4LpsOGtiX9TfW4cFN2WCKh/0mUdnygtlJ1T2U16
+E+YDr3B+P4373i5WUsgmnGRLjuzXxkslGdHLJ4JJjkHnOVSHtOBNX+HLVWcNNR5
rAH9bDOJbyYRACO8Y14z1rLvLGjGWAXalc9Bh8YmqVXpRs98SbQqANNAwAD/LoVJ
9tteCHEu2HBf9WBPHT2qhtuj3RNcH9SEa+8UZAZfGgwaCJFwH8Q8UKglHyTe11BM
IWPEFbq62WSMDMpW4yP1b/0ox8huqr/6J4DEqobeDT6GAz1cObaqnLKYSqsj7qK6
Q1urARAIvP68xK4zip7fLptTd483S+3ofuky3u2c+FKkrCcFVy3hIIUMwrYP2wFX
qLQiYWxpY2UgKGFsaWNlKSA8YWxpY2VAcmxlb2ZpZWxkLmRlPokBOAQTAQIAIgUC
T1uyBAIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQeUMG7dGoE3CLxAf+
KKuo/51KP2inW6ef+igxkfKkAF3uUUZRet2OMRjb/Y7VPfN6L4MYLIkhMNygFsAe
5w+KQ+juQHEYeXPwZPMhGmfySK8J71eVDX49Yqzby6NJXiE8d7iu8h9P4+Ptl57J
VdMXFZ/34HtvElvs3f3lRZYI3sRpLDEjVavf3z7NcfEbl/K2uw8X8PK3vnPVrP15
q0G2agtF5hjH2rTZUHEsdM0Gf7NxDBk1U0pupQ7sHJN0O5imZRL0nESn3X4N8tJt
xF13bLTNoonJ/6CXqfuPaedy4aVgHDl3Na4jld2sqB1bFLRSybsOxycd+CnGaU/j
cRVgZjLRcG9WxJ0oGo+izZ0DvgRPW7IEAQgAuG6wPfxseliLzO9MG9+HqpeRJ8QS
6wuUNMFjWc6oljLeiPmCWVOKMSlC1i2+msOuL/nccu8QUowDmXeB5vHUla1Hdh8J
sz8azptf6eHxYW7fB1hhjtml7Kt/XUO+e0bv5Vf6B10/XfudROMNakQEncObjghu
iyYozuBkh6wK9R9mKjcBtMI+x3zeVUVNST4WMRo2zAHpgi4C1YD+sZIT1pAC84Hm
uFh+JRXdU1I51V9gs5zqlowCO3NjOdNVI2WDw0e0comv3sVqcLlizu74Zwzyzm4i
TQI9I5BdMGczk5dpz1jySp4haPLXmGVvHUHaru3dcfo6gjWRwhVTcOhU1QARAQAB
/gMDApXPgMyMr+k1YCeTxfWu+79//lsQXnn15eYZa1PSDWNH2bKCxGvdtD+ZW6Tv
gnjTZHwIbeUIdjTY0eHSYe5uasCowjwo++D4CjrMxszV4qf85YdXvvgG6bG8x4Qk
UMCSkDEilajpYDSmG9LOZUbjofx07wT3l0/FIPoWwnyWasugPC++psrpTC5oDvWm
kNmj8vIzZrdoO5+9p3uurN3a5yMojsuvloeiM8UkPcMk9o1YU5CeHC0JBYYDkDOM
L0fArftVwLf2/bnn393dsCtFByU7cK6JIQ7UNR5JFzhRb722VgjxsqehYU5YrJvo
mW0ft474JS3lJXZHA7ekMvOftMhwG30Chp1uuQ5tag1sxGxlfBG9s6Nufg0xztcx
0MVXGFXCzBSp8VIRXfkVPdcfdlynHTP2Y1kOMIj9lYHhfIz3mlGfGomG3AOxrPY7
KVYsEeQScd+BR9ZQeNiNXNApWvjAb88mfT5u0E6dONTh+B7ax6j/G7Os5vR7zf2C
YFR5jKNJon7/97pf6AifksenortKTX5aoK6eCZwAd5/HgBmP/6qFgb4HXR89tz75
/wNhRKgudsm0M7zoGU7kpwqUWGMkal5Ht4771usEFd82JXjaOn5Gtew6LKBLiyQa
qxq1DAVJm6EppYxwd+TieL1a5qsJM6yIQJn8se8osn/2mVD04UBUKctnCPqK7O8i
RVzPWIcEsZe4D4I1bsdvIgIJHKndWqhaCCRR2pLPkg8jzLT67uizYwnoxdiXmiCa
71oTFW7s1HpW7io1MG3WTqRNW5rC6BD+cHtGCr8zh52TYmfh3uYoVWmMV8OCl91E
VUHJn/tpLE+ofQMEsnUfodE8oTG5NKXr/sAfUewKr43DJ+l5i0nTQSRP5nctRS0Z
NTieofgN6iQVxl31eaokVrmJAR8EGAECAAkFAk9bsgQCGwwACgkQeUMG7dGoE3Ck
fQf9EC39QALl4BO7EERfNVYwrV3JhjT99VMRfNfyG7mWB6r8+6HRcc/V4aRJ+mQk
2MiWStQ7ILHvYsQnGSPtZuVIo72tGD2U5FeUzdk7n3ovwJaNnTN3cGKYag3aheX/
EK9jERH8mUXs8QXrbC1ZZMf5TRYHZxKz0WCf04kzf2HARnsaBLoSWemHuCw/vyQt
jRrLjhcjjicnBcixgLRZ/w1dU/qkJ8NJ/6upWNxjNCUGPhBAdXw61CV6wrfDUopQ
cbQUA3lgdtp5gh7tRgvzTKTp9TlhQ2jskyIoOd2VhsYw94iEph9DFPK5m2XtPOqa
Y90XiaZ8pJyPioGOqOixdQLHyA==
=EYDr
-----END PGP PRIVATE KEY BLOCK-----

Quelle:
http://de.wikipedia.org/wiki/Public-Key-Verschl%C3%BCsselungsverfahren
http://upload.wikimedia.org/wikipedia/commons/3/3f/Public_key_making.svg

Gnu Privacy Guard, GPG



Alice:
erzeugt ein Keypaar
sendet Public Key zu Bob (per Email)

Bob verifziert den Key mit dem Fingerprint

Email:
Bob verschlüsselt mit diesem Key
nur Alice kann die Mail wieder lesen.

Bob: dto.

Public Key: öffentlich, kann jeder sehen
Private Key: streng geheim

Beide Schlüssel sind auf dem eigenen PC
Public Key auf dem PC des anderen

Signieren:
Bob signiert mit seinem Private Key
Mail muss nicht verschlüsselt sein
Alice kann mit dem Public Key von Bob prüfen, ob die Mail von Alice ist (Authorisierung)
Und Alice kann prüfen, ob der Inhalt verändert wurde.

kombinierbar, Verschlüsselung und Signieren

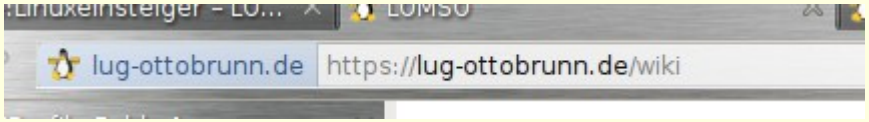
Quelle:
http://de.wikipedia.org/wiki/Public-Key-Verschl%C3%BCsselungsverfahren
http://upload.wikimedia.org/wikipedia/commons/3/3f/Public_key_making.svg
http://upload.wikimedia.org/wikipedia/commons/f/f9/Public_key_encryption.svg

HTTPS (im Browser)

- HTTP ist Protokoll für Webseiten
- HTTPS ist das gleiche Protokoll, aber mit Verschlüsselung
  - http://en.wikipedia.org/wiki/HTTP_Secure
- Einsatz im Webbrowser
  - Verschlüsselung des Datenstroms beim Zugriff auf Webseiten
  - Authentifizierung der Webseite (bin ich auf der Webseite der Bank?)
  - Schutz gegen Veränderung der Inhalte beim Transport
  - Public Key ist im Browser und von einer CA signiert
    - Sicherheit hängt vom Vertrauen in die CA ab
    - eigene Schlüssel über CAcert (http://www.cacert.org/)
- Demo einer Manipulation der Inhalte
  - http://odem.org/insert_coin/
  - „Zwei Personen kontrollieren 250 Personen“
    - Diplomarbeit, Hochschule für Gestaltung, Stuttgart

HTTPS (Demo)

LUG-Ottobrunn



General | Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	*.lug-ottobrunn.de
Organisation (O)	<Not Part Of Certificate>
Organisational Unit (OU)	<Not Part Of Certificate>
Serial Number	00:D1:D6

Issued By

Common Name (CN)	CAcert Class 3 Root
Organisation (O)	CAcert Inc.
Organisational Unit (OU)	http://www.CAcert.org

Validity

Issued On	21/05/11
Expires On	20/05/13

Fingerprints

SHA1 Fingerprint	24:14:1E:C9:EE:8C:E3:F4:55:3E:AF:1E:20:BD:3B:C2:17:EE:7E:6C
MD5 Fingerprint	99:16:CC:E9:E3:17:B9:74:08:EF:7F:3E:1B:9D:4F:19

Viren

- 'Computer**viren**' ?
  - 'Computer**viren**' gibt es nicht, es sind immer Programme, die Fehler ausnutzen
    - Computerviren sind kein ***medizinisches*** Problem
      - diese Begriffe findet man bei 'Sicherheitsexperten'
    - Computerviren sind kein ***militärisches*** Problem
      - diese Begriffe findet man bei Politikern (Cyberwar, Abschreckung, milit. Gleichgewicht)
    - Computerviren sind ein Hinweis, dass das System *defekt* ist (Konzept, Design,...)

- Firewall ist überflüssig
  - Programme, die 'nach Hause' telefonieren, abwehren?
    - löschen oder gar nicht erst installieren, ist besser als Firewall
    - in Windows nur schwer möglich
  - Ubuntu hat **keine** Programme mit 'Heimweh'
  - Ubuntu hat **keine** offenen Ports
    - Serverinstallationen sind ein anderes Thema
  - ***Linux ist nicht sicher, aber anders gesichert.***

  (Sehen Sie bitte nach, was Ihnen Ihre Sicherheitsfirma empfiehlt.)

Sicherheit erhalten

- keine **Voreinstellungen** ändern
  - genau wissen, was man macht
- 'root' login nicht freischalten (ist in Ubuntu gesperrt)
  - zur eigenen Sicherheit
- sichere Passwörter für alle Benutzer
  - mit 'pwgen' erzeugen
- keine Software aus **Fremdquellen** installieren
  - Ausnahmen bestätigen die Regel, X2GO
- **Updates** täglich durchführen
- **Backups** mit 'rsync', täglich
  - ist mit Linux einfach und schnell
- sei nicht zu clever …
  - ein modernes Linux pflegt sich selbst

passive Sicherheit durch 'whitelists'

the Ubuntu Way: '**whitelists**'

signiertes Repository,
ca. 30.000 Pakete
von Ubuntu-Server

Beispiel Firefox:
Source: firefox-3.0
MD5sum:
db07d4ab7fba80bcba3c1d7533dfb3af

download, update:
ein sicherer Weg

Programme
auf Echtheit geprüft
nur '**whitelist**' Software

herkömmlicher Weg '**blacklists**'

unsichere Webseite

download update:
mehrere und unsichere
Wege

unsichere Webseite

unsichere Webseite

unsichere Webseite

Supertool.exe

PC zu Hause:
Daten sind nicht auf Echtheit geprüft
Viren und Trojaner müssen nach
*dem Download mit '**blacklists**' gesucht werden*
(kann nie vollständig sein)

passive Sicherheit, Linux intern

- Sicherheit durch strenge Trennung der Rechte
- root
  - darf fast alles
  - streng vom Benutzer getrennt
  - es gibt immer 'root' und mind. einen Benutzer
  - einem Benutzer kann das Recht verliehen werden, kurzfristig 'root' zu werden
  - Wechsel der Identität und nicht nur des Kontextes
- Benutzer
  - darf Programme nutzen, nicht installieren
  - hat 'seinen' Bereich und seine Konfiguration unter '/home/benutzer'
  - kann versch. Rollen bekommen
  - ein Trojaner kann u.U. nur die Daten des Benutzers ändern, aber niemals einen Schaden am System erzeugen

Ergebnis

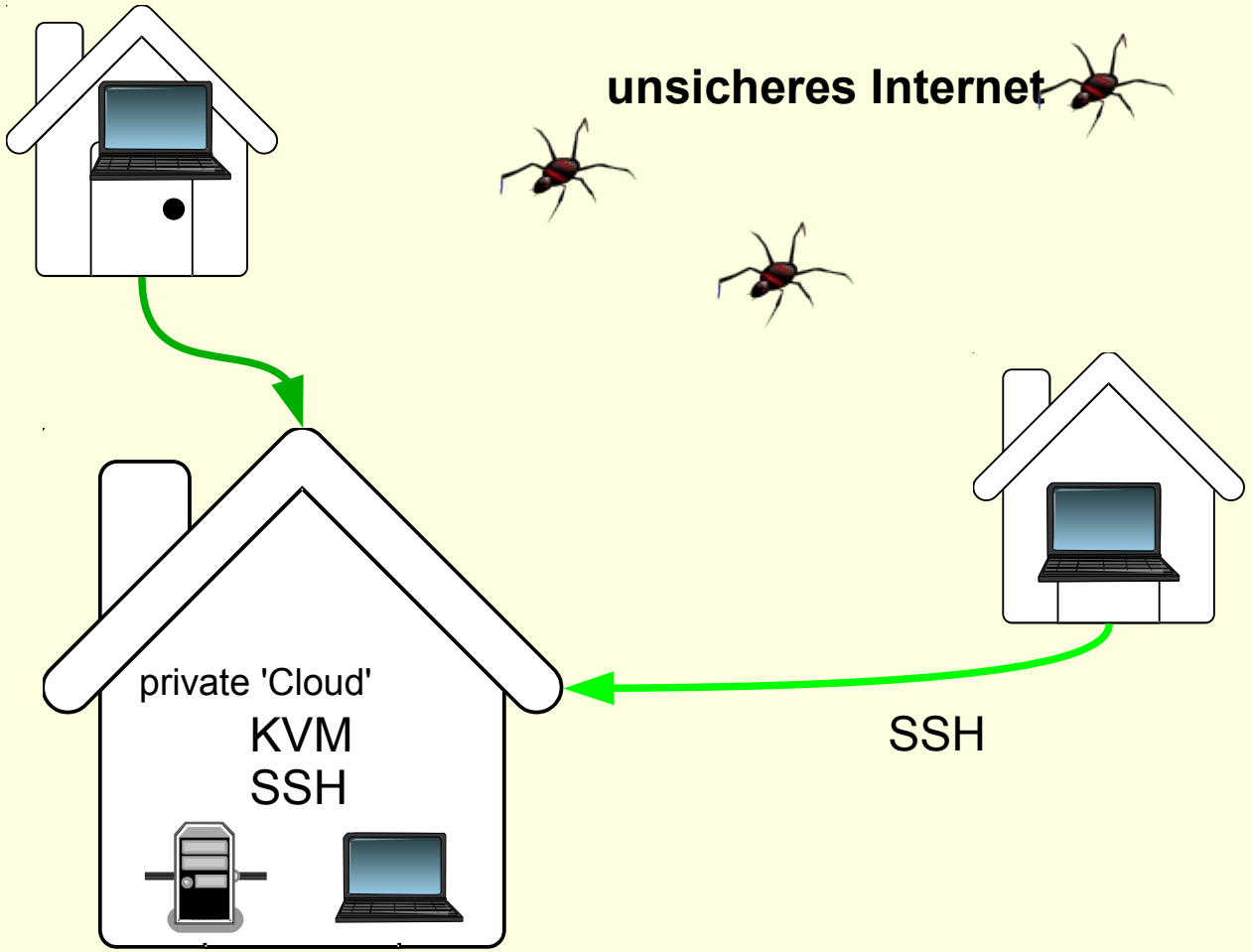
- 'Cyberwar' findet ohne uns statt
  - Computer-Unsicherheit hat politische Folgen
  - Cyberabwehrzentrum der Bundesregierung (?)
    - 'Frühwarnung gegen sogenannte **Cyber-Angriffe**'
  - http://de.wikipedia.org/wiki/Cyberwar
    - Krieg als 'Computerspiel'
  - „stell Dir vor, es ist Cyberwar und wir gehen nicht hin“ ;-)
  - das ist Linux

Vorteile für Sie

- Lernprozess
  - besserer Umgang mit dem Internet
  - bessere Kenntnisse im Umgang mit dem Computer
  - der Weg geht vom 'Klick' zum Wissen
    - nicht nur 'Häkchen setzen', sondern wissen, was man konfiguriert, einstellt ...
- Ergebnis
  - Besserer und 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 Linux/**Ubuntu** gelernt haben
- Links
  - http://lug-ottobrunn.de
  - http://www.lug-ottobrunn.de/wiki/Kategorie:Linuxeinsteiger

GNU/Linux/Ubuntu im sicheren Netz

privates sicheres Netz, Sie haben die Kontrolle und die Sicherheit



sicheres Netz für die Familie

- Warum?
  - Überwachung des Datenstroms nimmt zu
  - 'Deep Paket Inspection' ist sehr wahrscheinlich
  - „Das Arsenal der digitalen Überwachung“, 19.11.2011
    - http://netzpolitik.org/2011/das-arsenal-der-digitalen-uberwachung/
  - Inhalte können vom Provider im Auftrag kontrolliert werden
  - Sendung „Die Tücken der Überwachungstechnik“
    ARD FAKT , 25.10.2011 21:45 Uhr
    http://www.mdr.de/fakt/ueberwachungssoftware100.html
- SSH
  - universelle sichere Verbindung (verschlüsselt)
  - Peer to Peer
- Was kann ich damit tun?
  - einfache Terminal Verbindung
  - Ausgabe von grafischen Programmen umleiten
  - Filemanager verteilt verwenden
  - Ausgabe beliebiger Programme sicher durch das Netz bringen (Tunnel)
- Familiennetzwerk mit SSH
  - Netz zwischen Benutzern, die sich gegenseitig vertrauen
  - in Linux ohne Zusatzsoftware, '*out of the box*'
  - Zugriff auf den eigenen Desktop mit X2GO
  - stromsparender Server (z.B. invis)

Sicherheit von SSH

- SSH installieren (auf allen beteiligten PCs)
  - # apt-get install **ssh**
  - Schlüsselpaar erzeugen und sichern ($ ssh-keygen)
    - 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)
- Passwort Login sperren
  - **Server absichern**
  - **/etc/ssh/sshd_config editieren**
  - Passwort-Login für alle Benutzer sperren

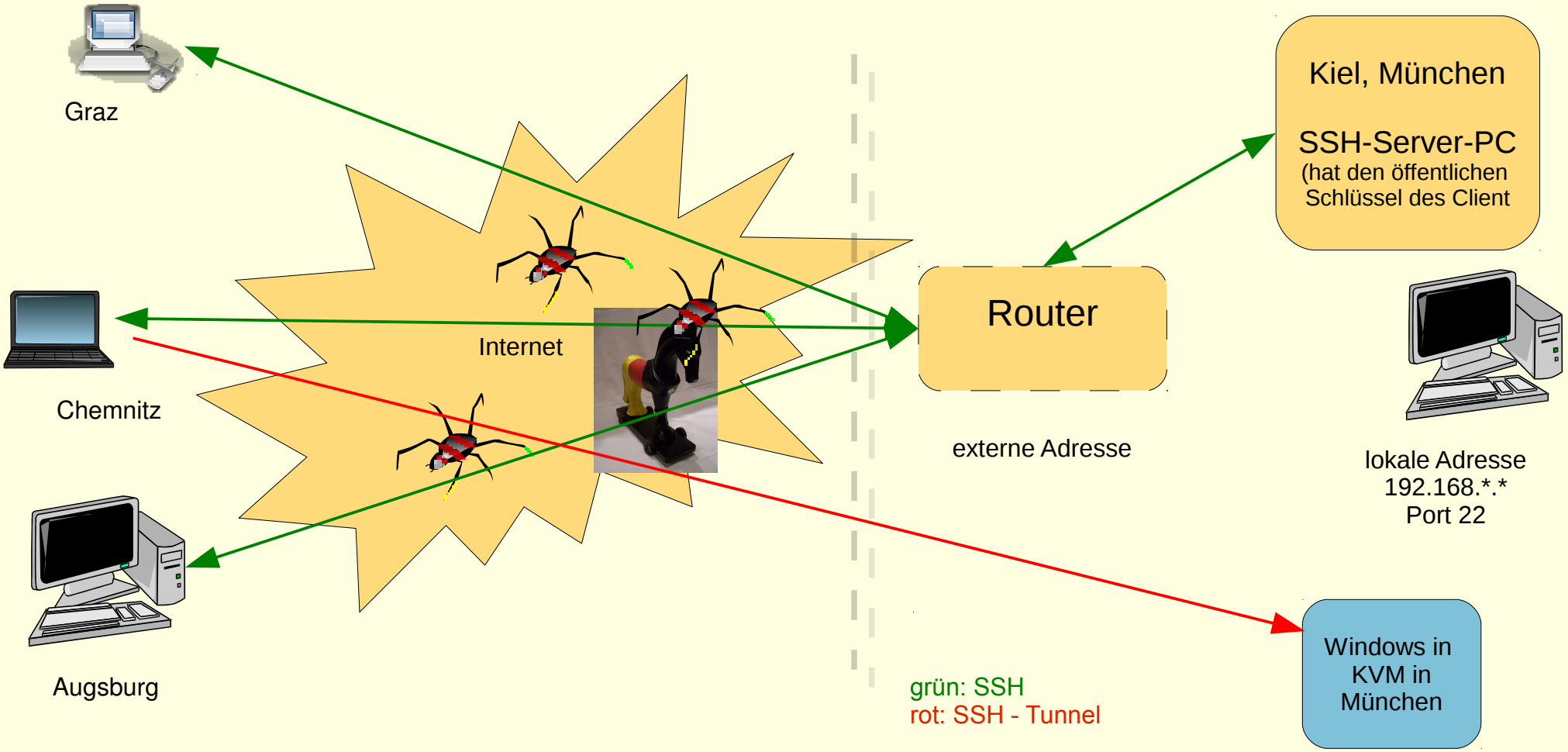
PermitRootLogin no
PasswordAuthentication no

- Router freischalten, nach dem Sperren des Logins
  - Port 22 muss zum Server-PC weitergeleitet werden
  - Firewall im Router abschalten, bzw. den SSH Port freischalten
    in Doku des Routers nachlesen

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 -X -C 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)
  - oder sicheren Account anlegen
- Links bei der LUG-Ottobrunn
  - http://www.lug-ottobrunn.de/wiki/SSH_Simple
  - http://www.lug-ottobrunn.de/wiki/SSH_Spickzettel

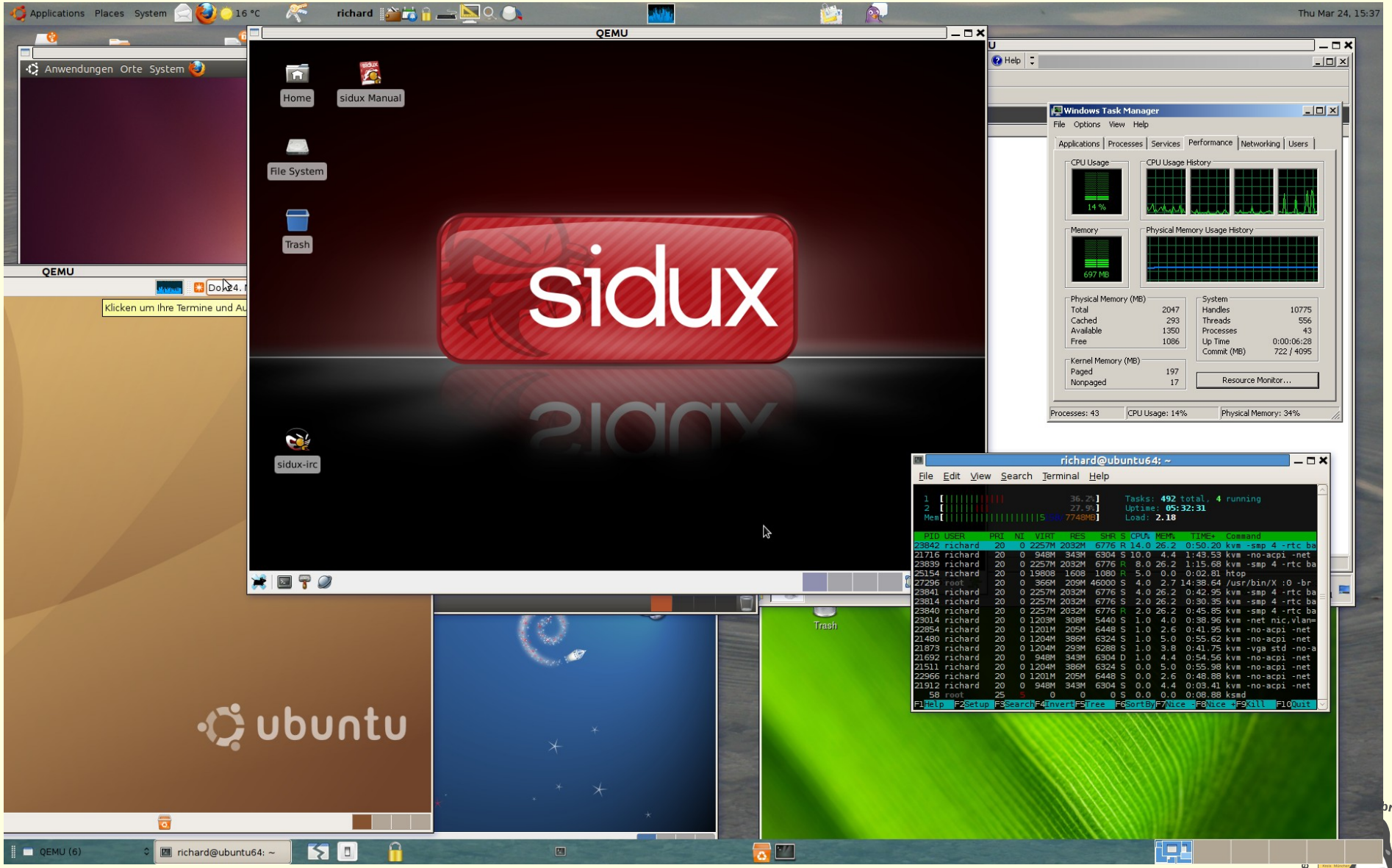
so sieht es aus



SSH Anwendungen

- Terminal
  - ssh -X -C richard@kiel.ath.cx
- Filemanager
  - ssh://richard@kiel.ath.cx/home/richard
  - Demo Liste der Bookmarks in Nautilus
- X Forward
  - in Kiel, cd boids, ./boids
- X2GO
  - Remote Desktop nach Kiel, bzw. nach München

Virtualisierung mit KVM



Installation von KVM unter Ubuntu

- Kernel Based Virtual Machine
  - von Ubuntu favorisiert
  -
  - PC Altlasten weiter betreiben (Lizenzen beachten)
  - In KVM
  - z.B. Finanzbuchhaltung,
  - Steuererklärung
  - Branchensoftware
  -
- Siehe Webseiten von 'ubuntuusers.de' und 'ubuntu.com'
  - http://wiki.ubuntuusers.de/KVM
  - http://wiki.ubuntuusers.de/QEMU
  - https://help.ubuntu.com/community/KVM
  - http://www.linux-kvm.org/page/Management_Tools

  - Install **qemu-kvm** und testen
    - # apt-get install kvm
    - $ **kvm-ok**

      INFO: Your CPU supports KVM extensions

      INFO: /dev/kvm exists

      KVM acceleration can be used

  - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

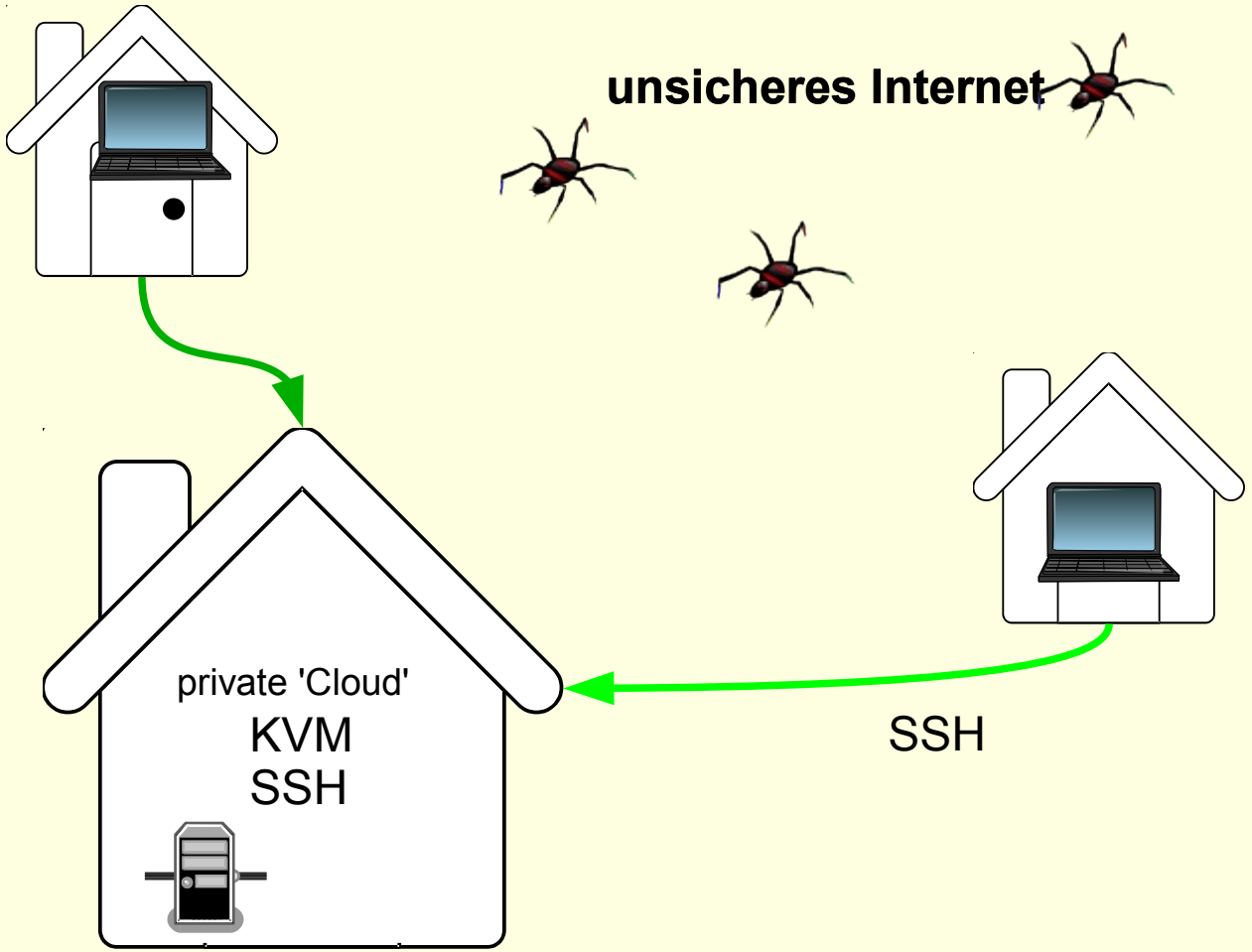
Einbinden in das lokale Netz

- *bridge utils* für Einbindung in das lokale Netz (192.168.*.*)
  - default ist 10.2.0.2, d.h. die VM ist 'unsichtbar'
  - https://help.ubuntu.com/community/KVM/Networking
  - nicht ganz einfach, aber gut dokumentiert
  - http://lug-ottobrunn.de/wiki/Virtualisierung_mit_KVM

- Demos
  - Windows 2008 Server, in KVM im lokalen Netz zu Hause
  - Zugriff mit Remote Desktop
  - Windows kann kein SSH, Ubuntu schon
  - **ssh -L 10022:vwin2008:3389 lugdemo@meinPC.dyndns.org**
  - Zugriff mit Remote-Desktop, localhost
  - **rdesktop -x l -g 1100x720 -a 16 -k de -u Administrator -p xxxxxxx localhost:10022**

  - Demo 2: Windows 7 lokal
  - **kvm win7fibu.ovl -m 2048 -smp 2 -net nic -net user,hostfwd=tcp::3389-:3389**
  - Zugriff zum Remote-Desktop mit localhost
  - **rdesktop -x l -g 1200x720 -a 16 -k de -u rleo localhost**

privates sicheres Netz, Sie haben die Kontrolle



Ende des Vortrages, kein Ende mit Linux ;-)

- 'to go the Ubuntu/Linux Way'
  - ist der Weg zu einem sichern, einfachen und stabilen System
- Lernprozess
  - bessere Kenntnisse im Umgang mit dem Computer
  - bessere Sicherheit des eigenen PC
- Ergebnis
  - **Sie** werden staunen, was **Sie** alles im Umgang mit Linux gelernt haben
- sicheres privates Netz
  - einfach, transparent, sicher
- KVM
  - alter PC lebt virtuell weiter
  - jedem sein PC, egal, wo man sich aufhält
  - besonders gesicherter PC in einer VM

Vielen Dank für Ihre Aufmerksamkeit
und einen schönen Linux-Infotag


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