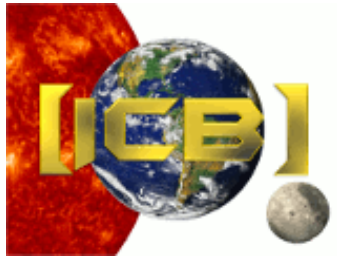
# Linux Anwender-Security

Dr. Markus Tauber

markus.tauber@ait.ac.at

26/04/2013


# Inhalt

- **Benutzer(selbst)Schutz** - für den interessierten Anwender
- Praktische Beispiele und Hintergründe (**Wie & Warum**)
- Basierend auf Ubuntu 12.04 LTS

# Authentifizierung - Tips

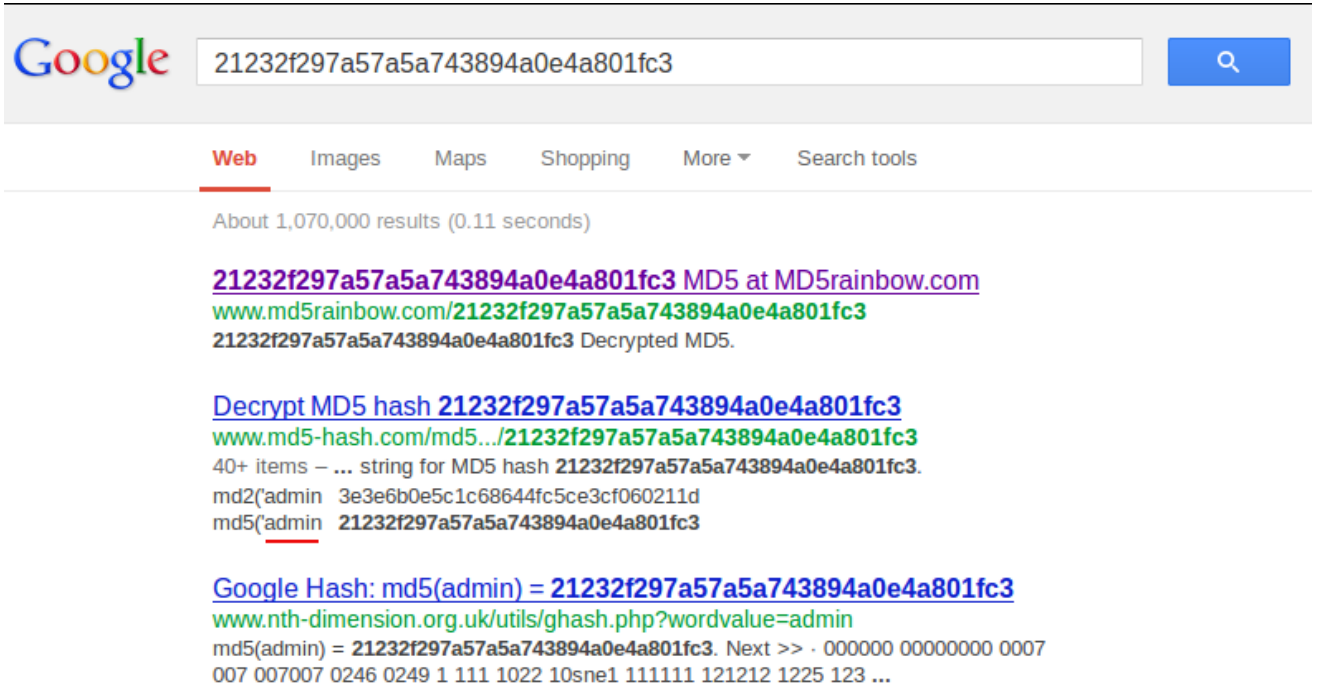
- Sicheres Passwort
  - > 8 Zeichen
  - Buchstaben, Zahlen, Sonderzeichen
- Keine automatische Anmeldung
- Bildschirmschoner

# Warum? - Wie sieht ein Passwort aus?

```
+-----------+-----------------+-------------------------------------------+-
| Host      | User            | Password                                  |
+-----------+-----------------+-------------------------------------------+-
| any       | admin           | 21232f297a57a5a743894a0e4a801fc3 |
```

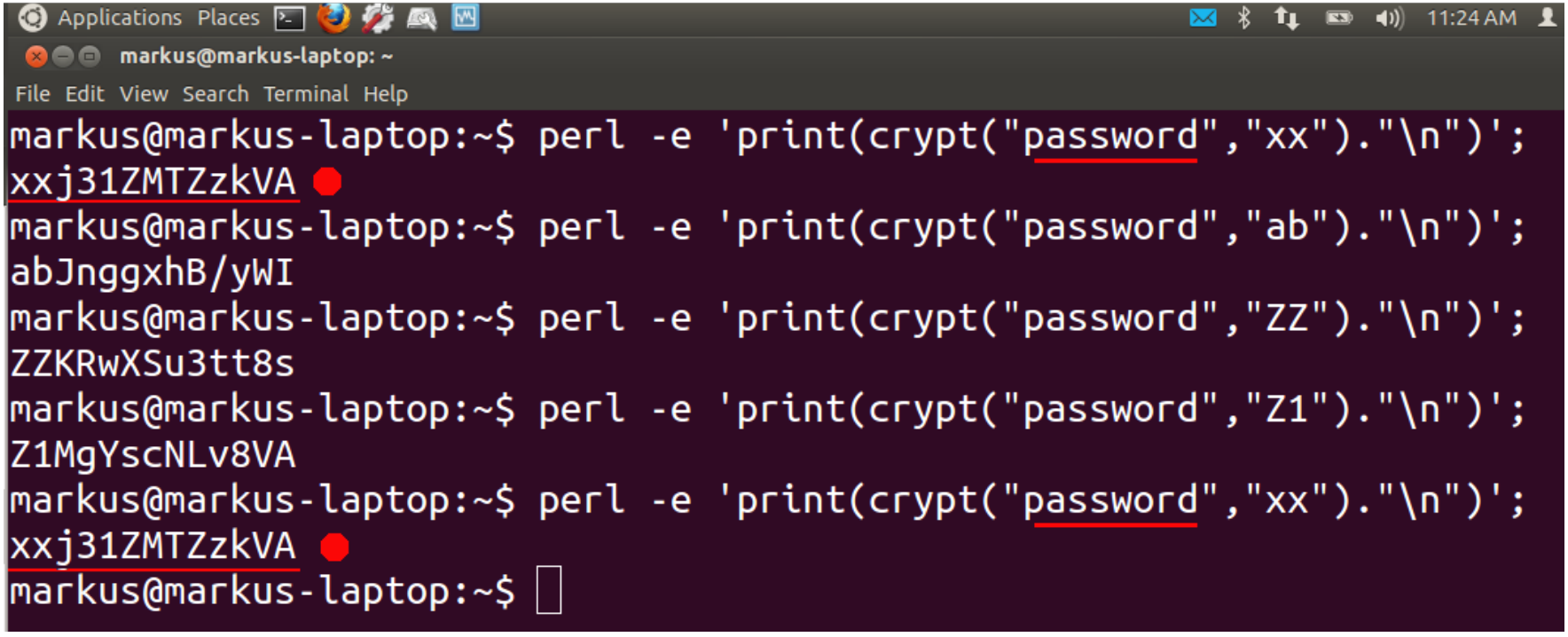
```
+-----------+-----------------+-------------------------------------------+-
| Host      | User            | Password                                  |
+-----------+-----------------+-------------------------------------------+-
| any       | fritz           | xxj31ZMTZzkVA |
```

# "Entschlüsselung" mit Google

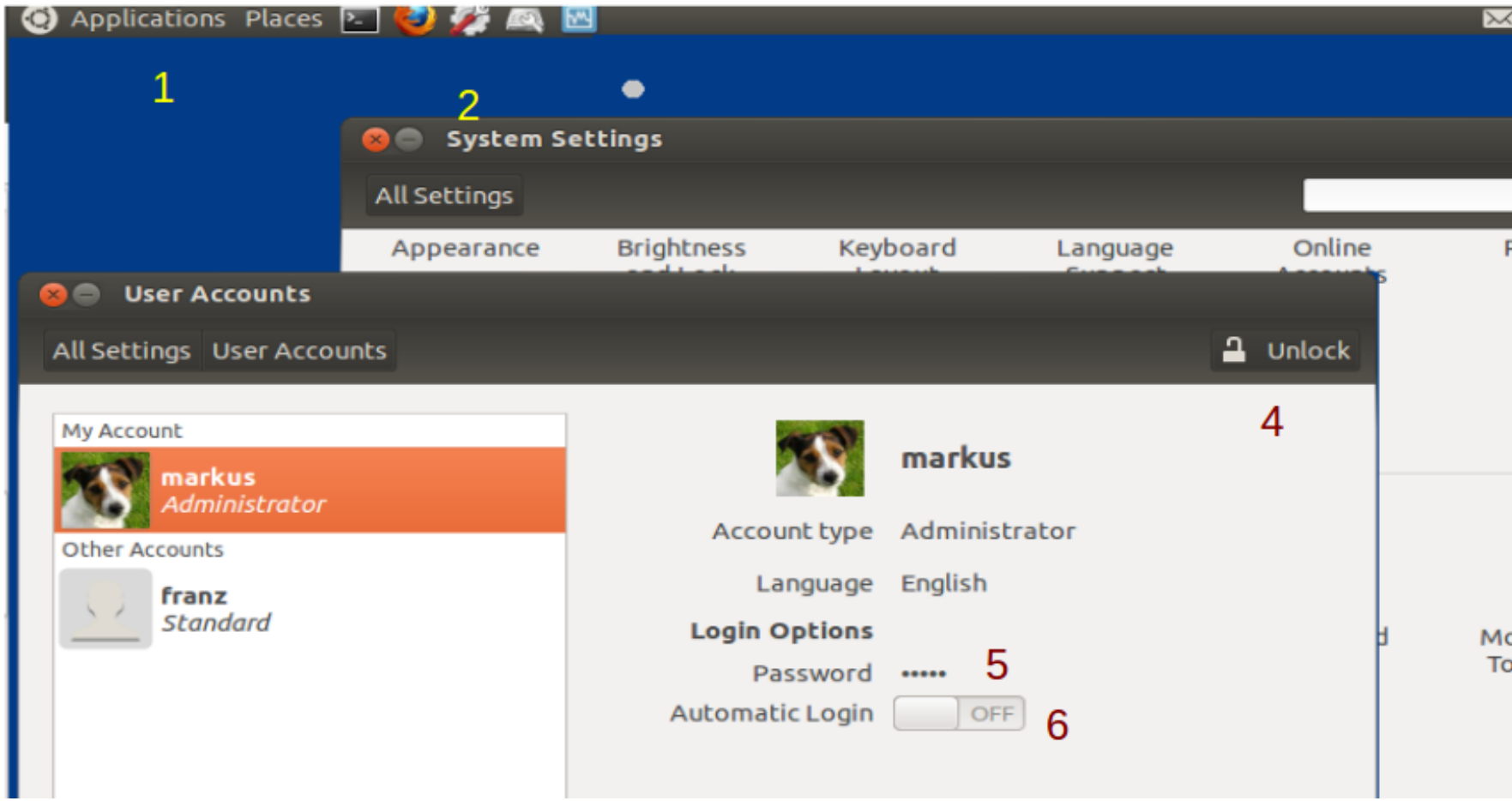


AUSTRIAN INSTITUTE OF TECHNOLOGY

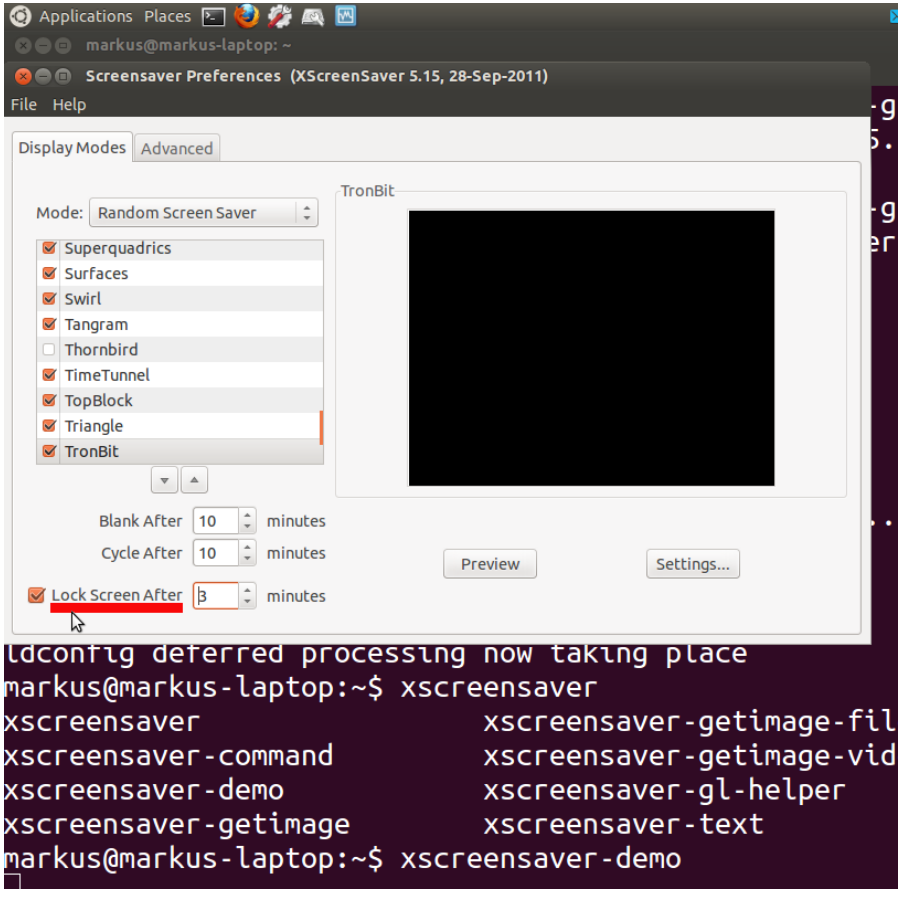
# Wie funktioniert "Entschlüsselung" - Beispiel. crypt()



# Authentifizierung-Konfiguration



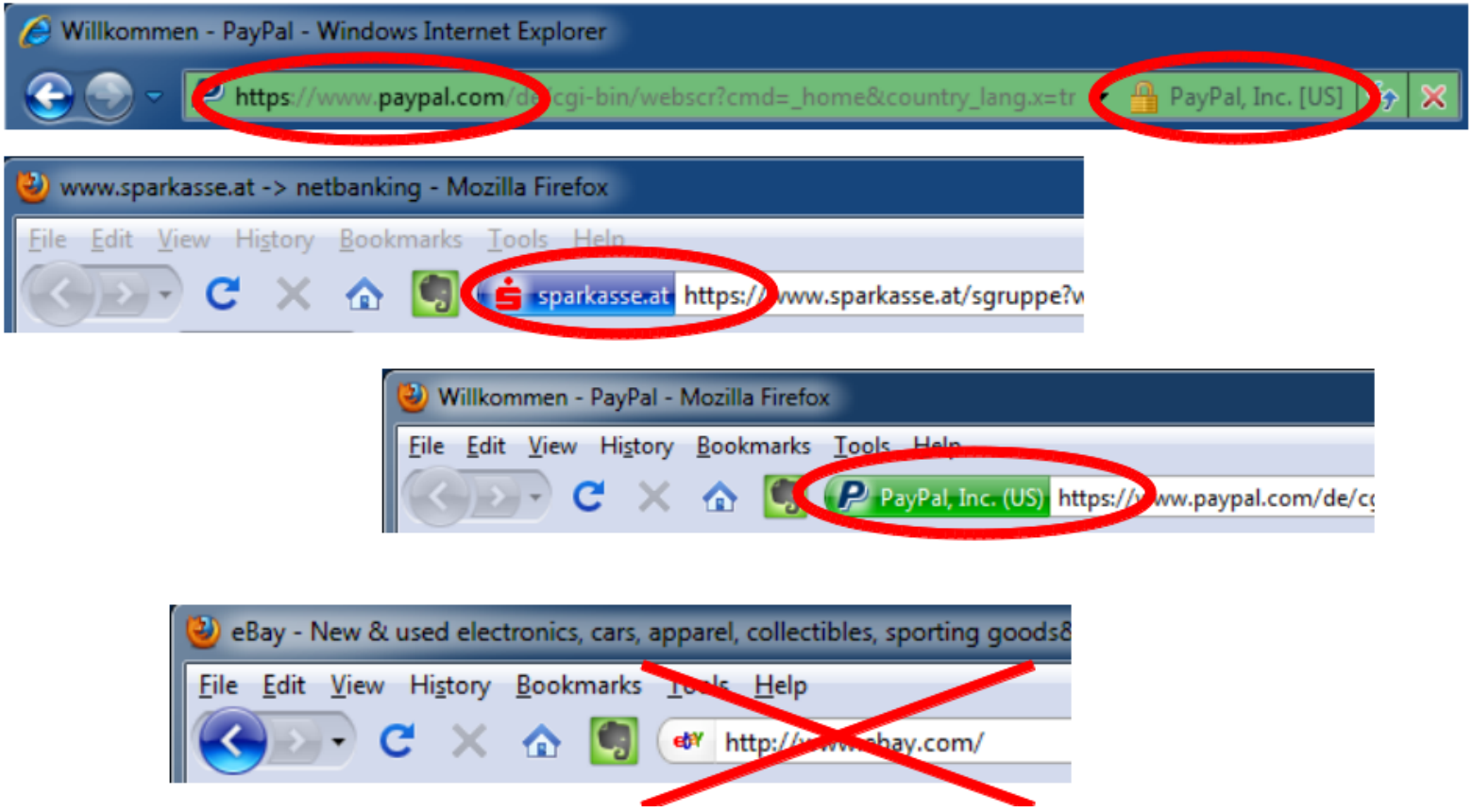
# Bildschrimschoner



# Sichere Websites

- .. haben ein Sicherheits-Zertifikat
- Zertifikat wurde von jemandem ausgefertigt
- Ein vertrauenswürdiger Ausfertiger "ist dem Betriebssystem bekannt"

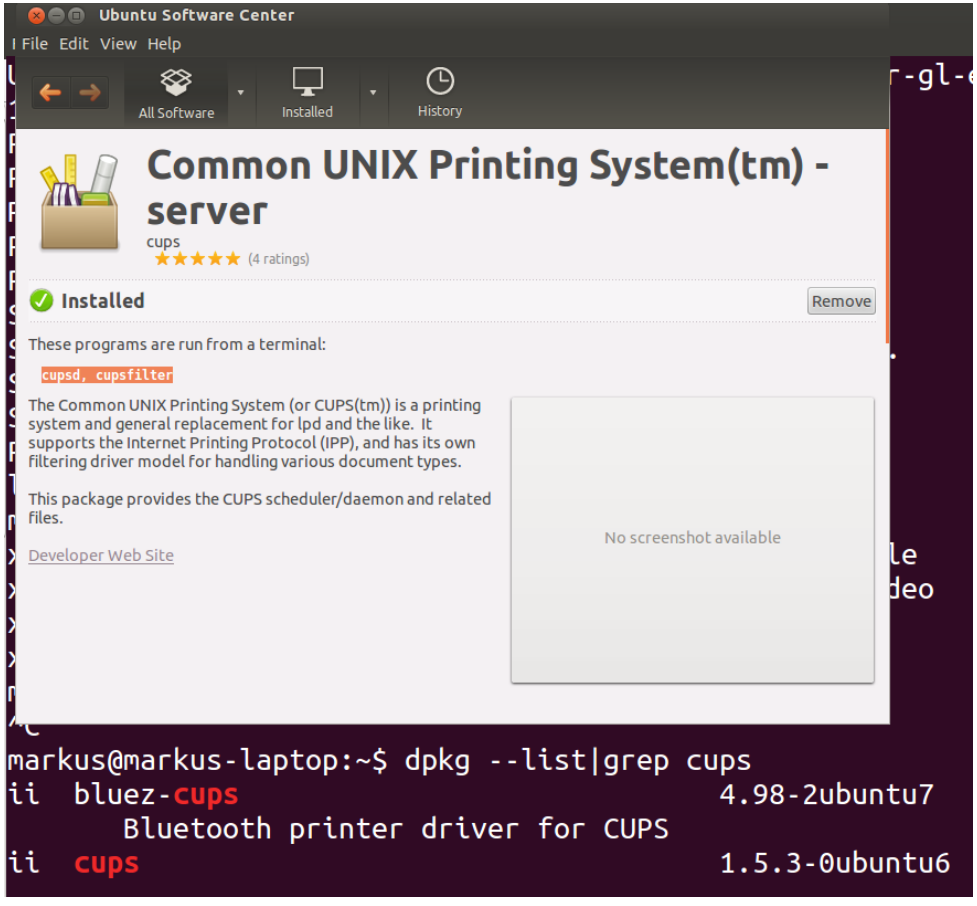
# https Beispiele



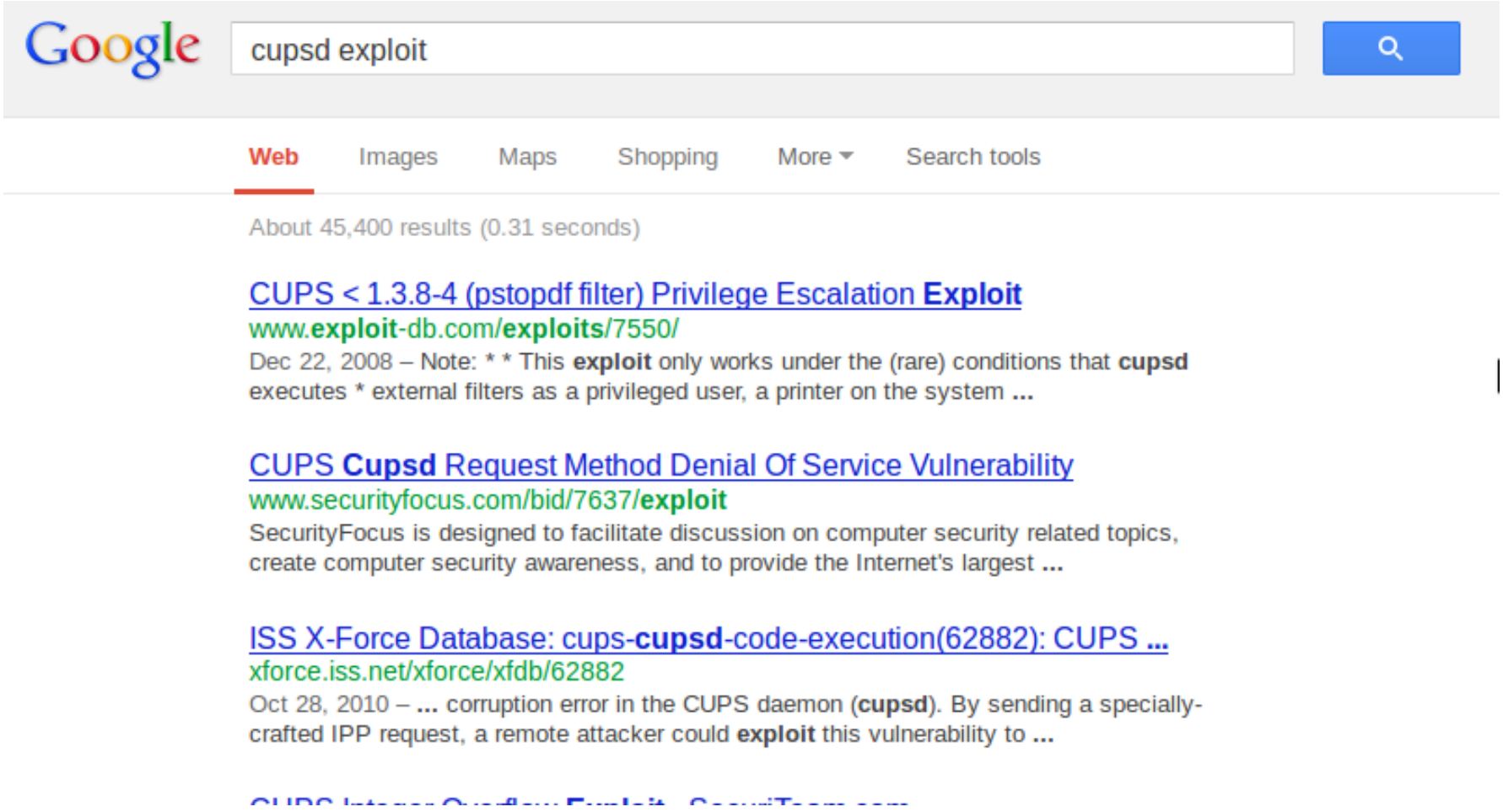
# Welche Software?

- Nur die nötigste Software
- Services stoppen
- Update, update, update, ...

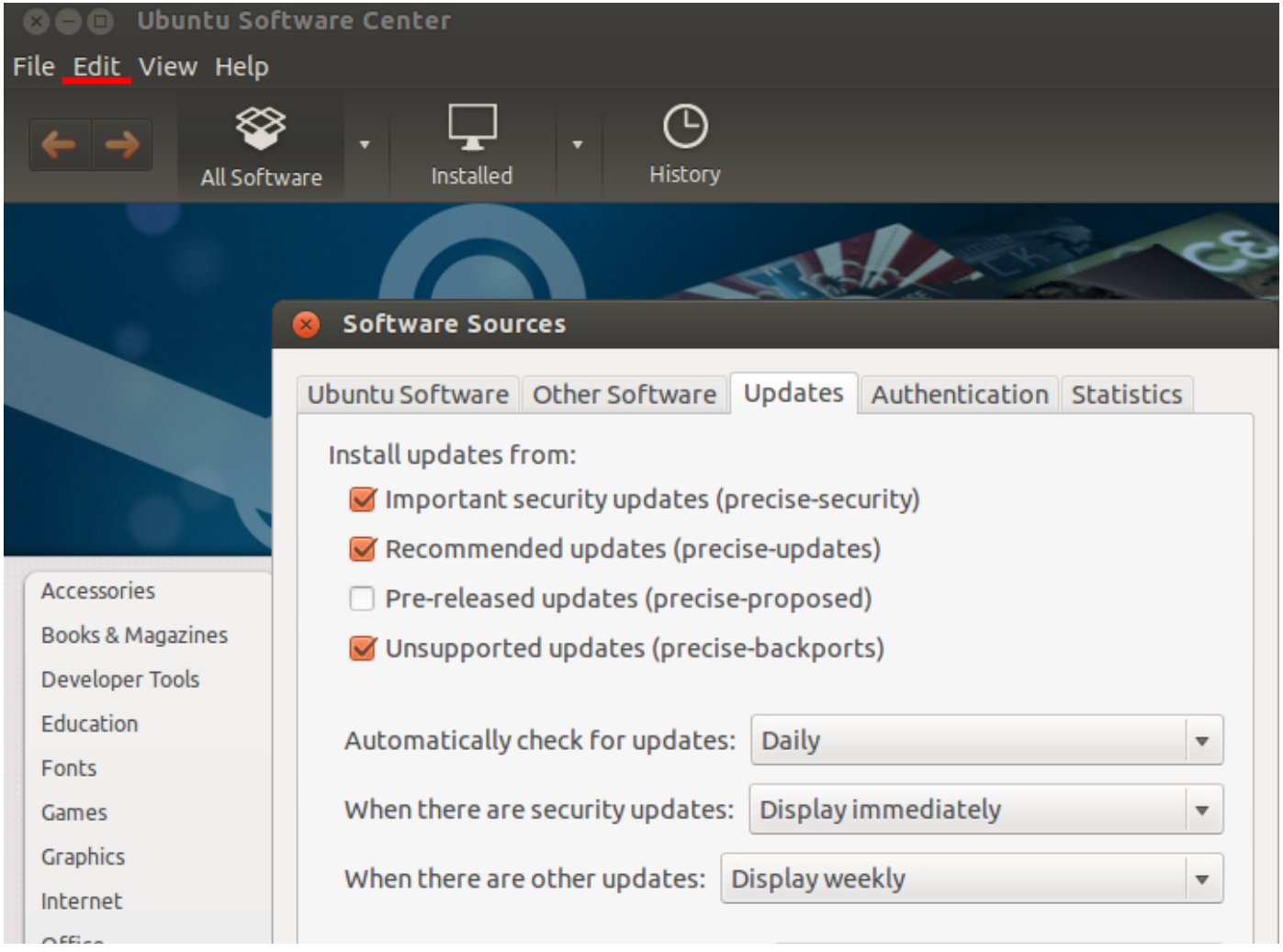
# Was ist cups und welche version version verwende ich?



# Ist meine Version gefährdet?



# Software Updates - HowTo

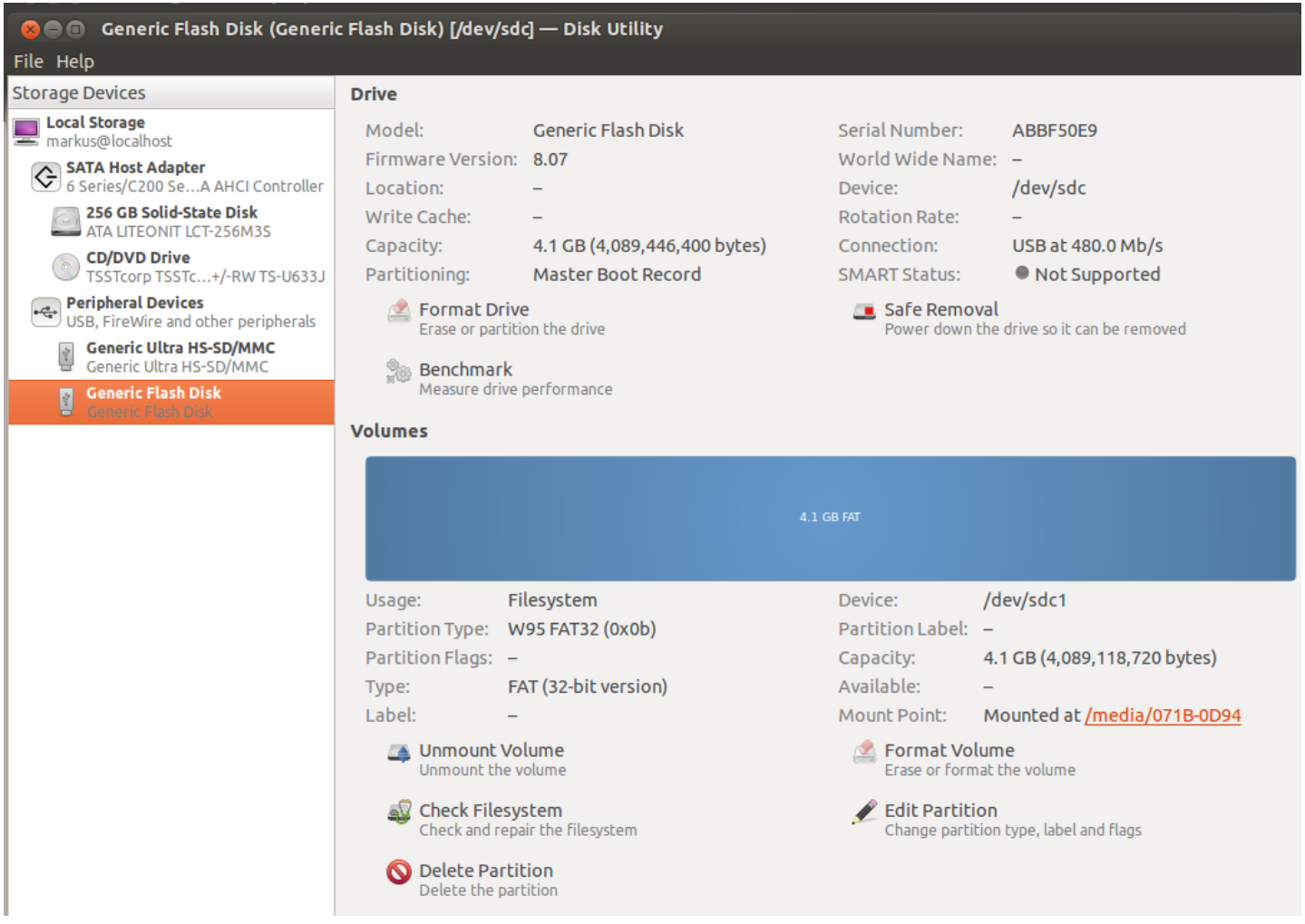


# Festplatten Verschlüsselung

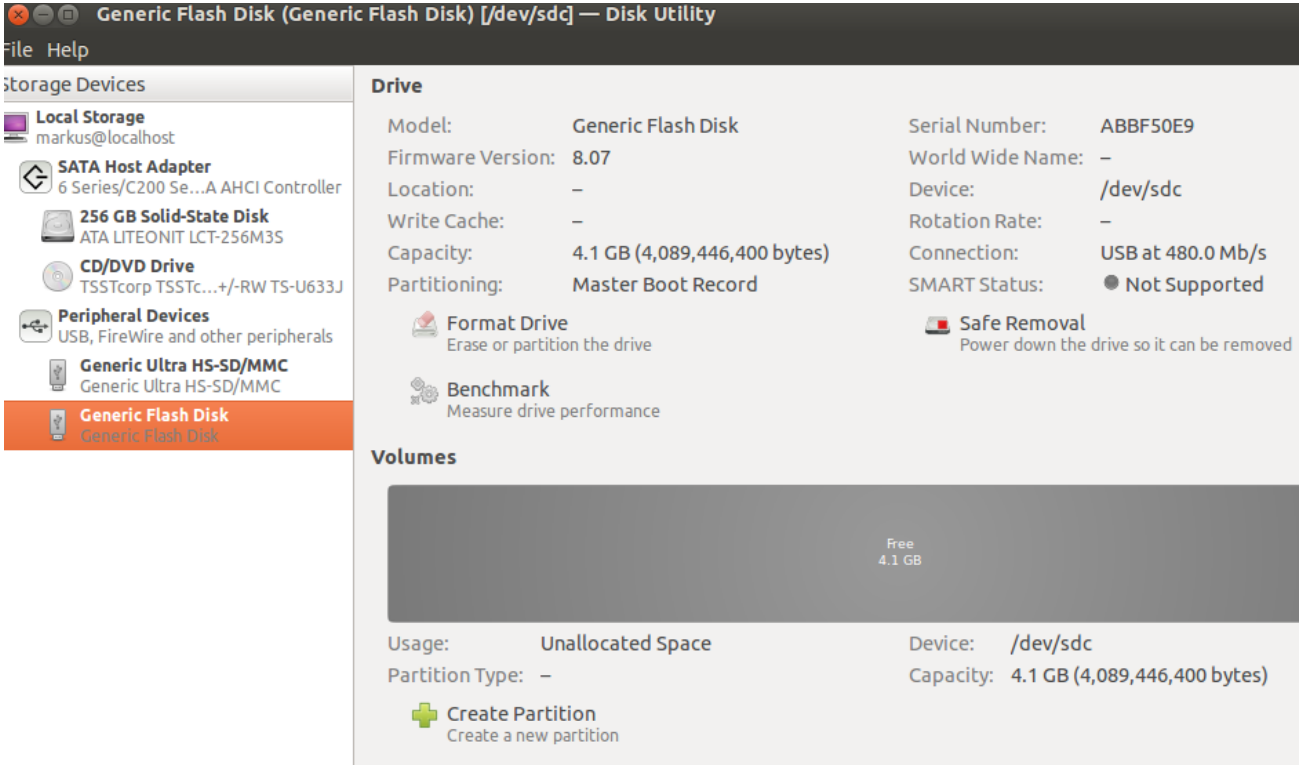
- /home auf eigner partition ermöglicht Verschlüsselung und "verstecken" der Daten
- USB Stick - kann mit sensitiven daten versehen verloren gehen.
- Ubuntu standard tool: Disk Utility

AUSTRIAN INSTITUTE OF TECHNOLOGY

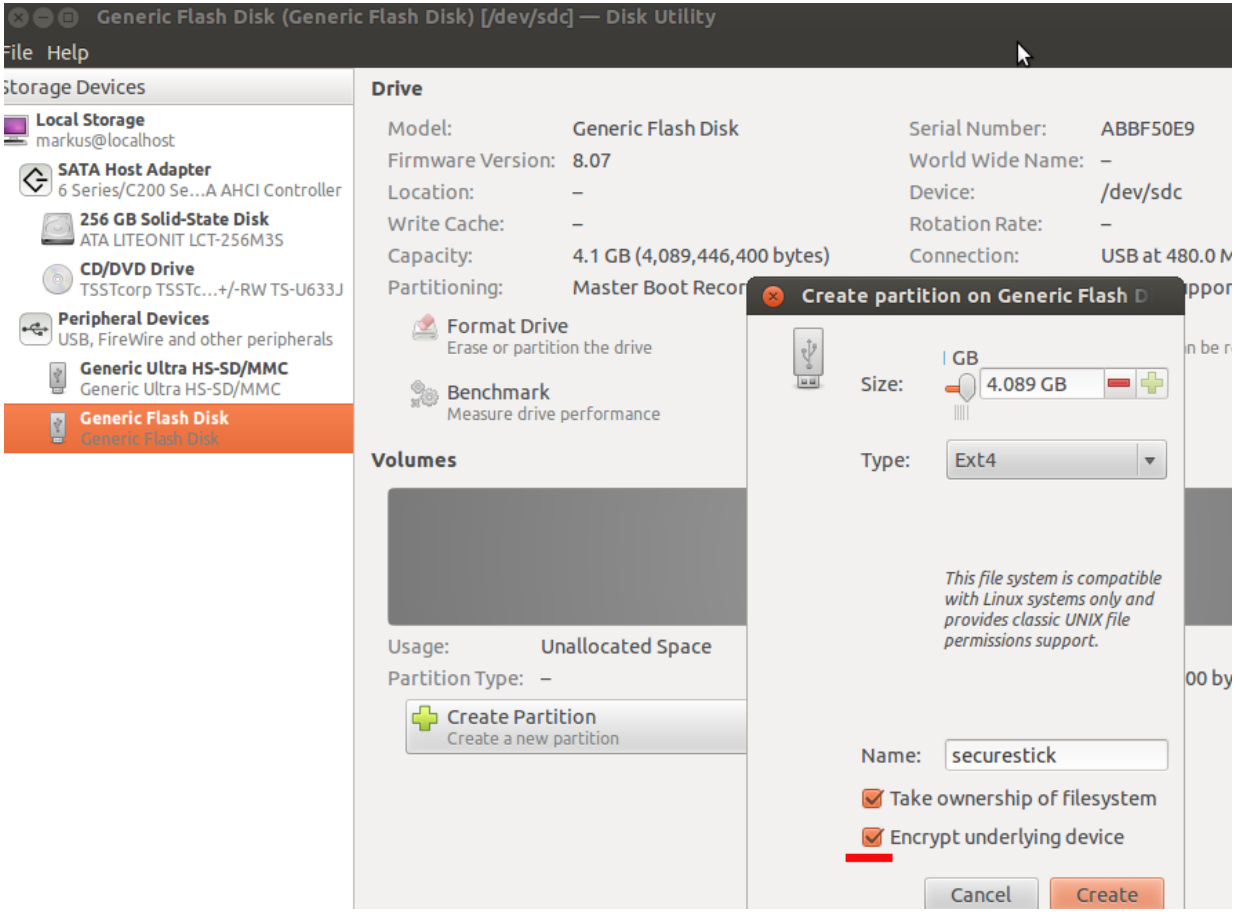
# Disk Utility Beispiel 1



# Disk Utility Beispiel 2



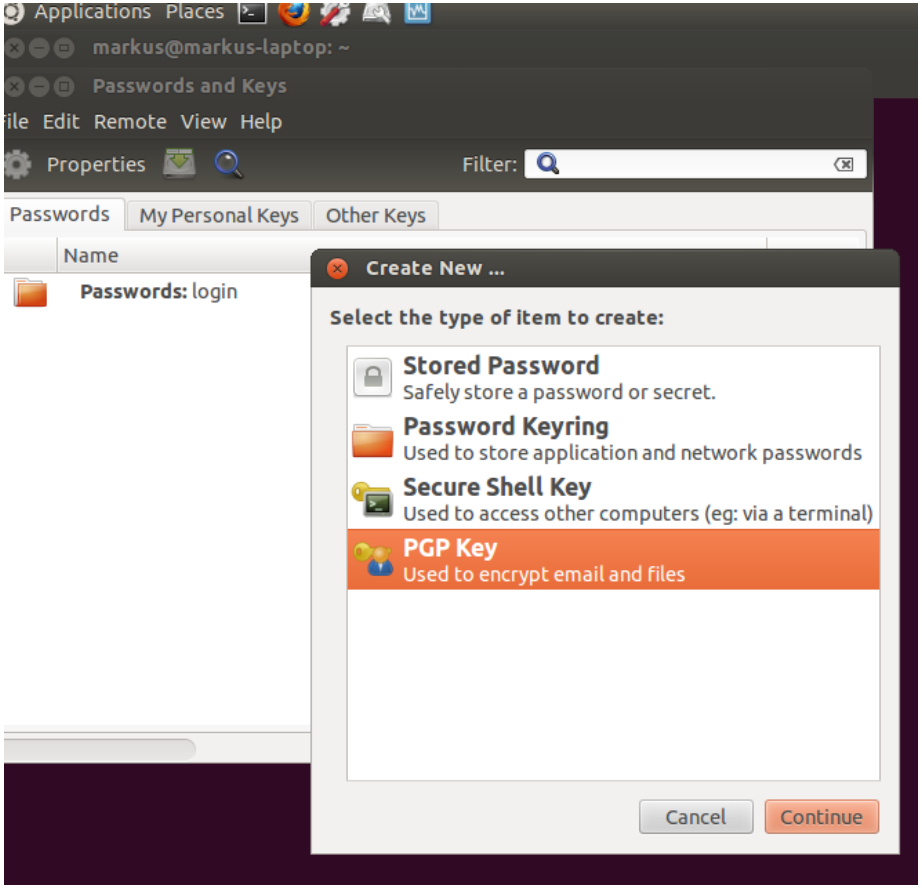
# Disk Utility Beispiel 3



# Email verschlüsseln und signieren

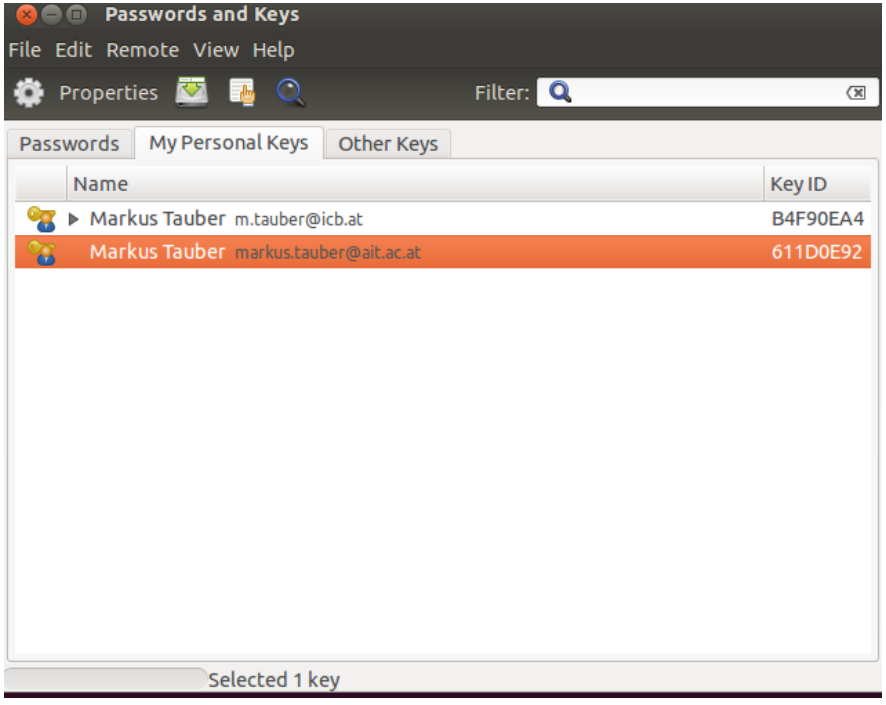
- Public/Private Key System
  - Public Key - darf öffentlich gemacht werden (website, pgp sever,..)
  - Nachrichten die mit öffentlichem Schlüssel verschlüssel wurden können nur mit dazugehörigem privatem Schüssel entschlüsselt werden.
- Thunderbird plugin: enigmail
- PGP, GPG, sMime

# PGP - Schüsselgenerierung



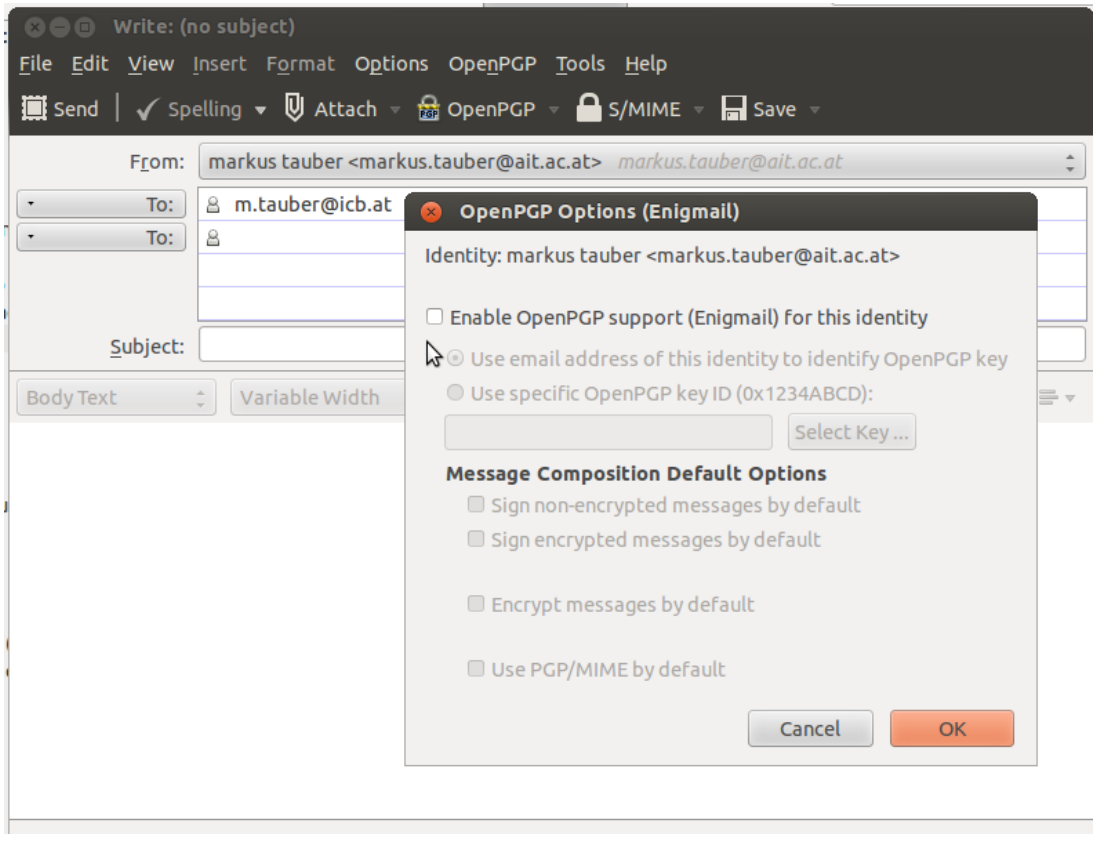

- Applications -> Preferences -> Password and Keys
- Strg + N

# PGP - Schlüsselverwaltung

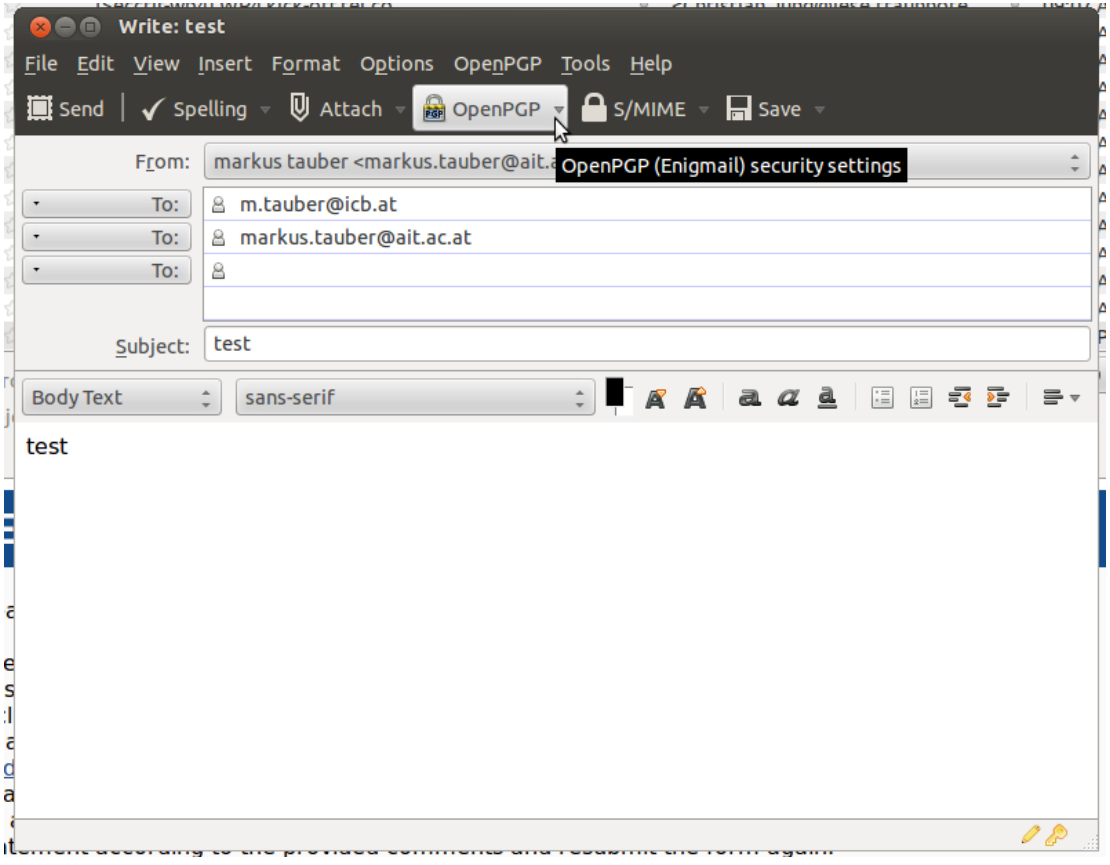



- export public key
- share it on key servers
- look for other keys on key servers

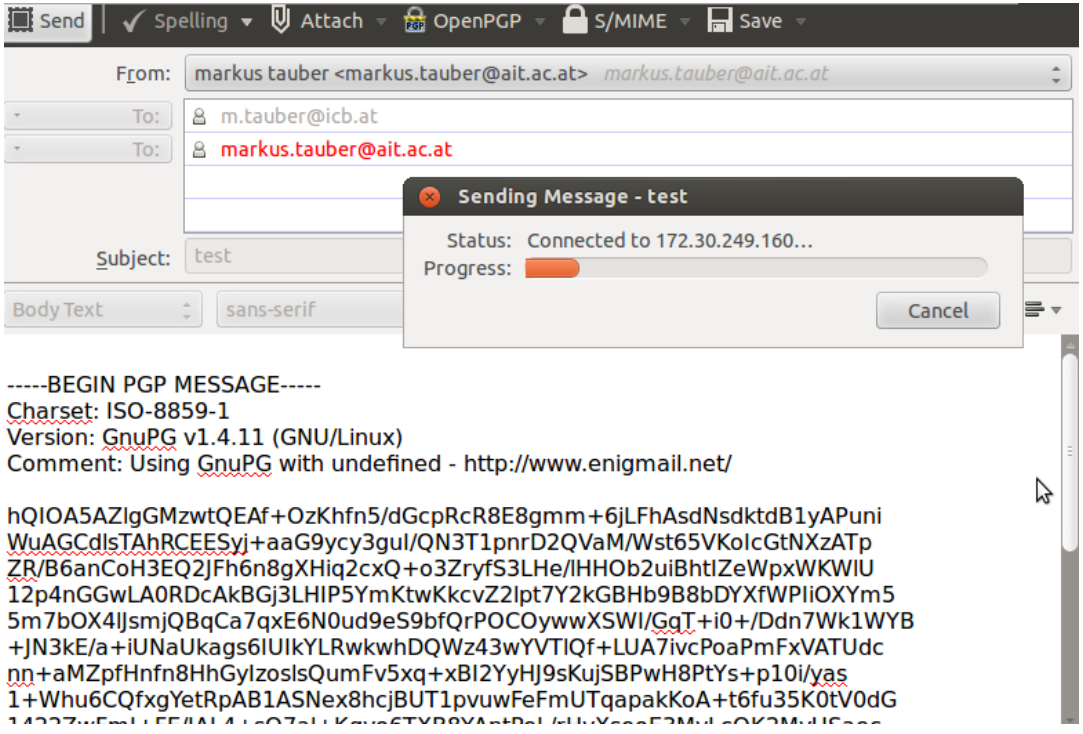
# PGP - Schlüsselverwendung



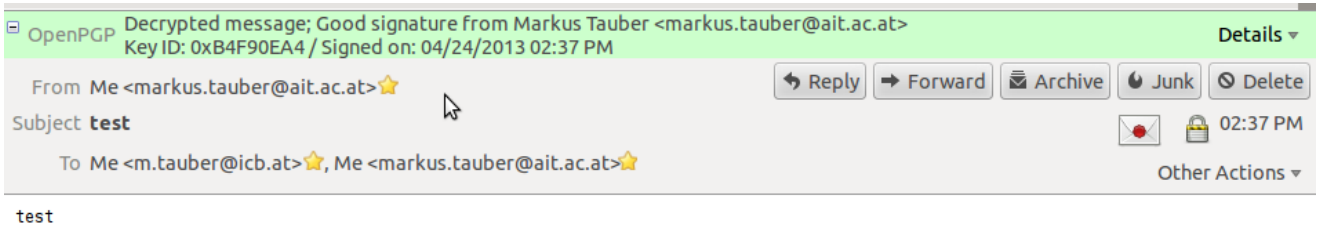
# PGP - Email Signatur und Verschlüsselung



# PGP - Verschüsselter Text



# PGP - Entschlüsselter Text



AUSTRIAN INSTITUTE OF TECHNOLOGY

## Ende

# Linux Anwender-Security

Dr. Markus Tauber

markus.tauber@ait.ac.at

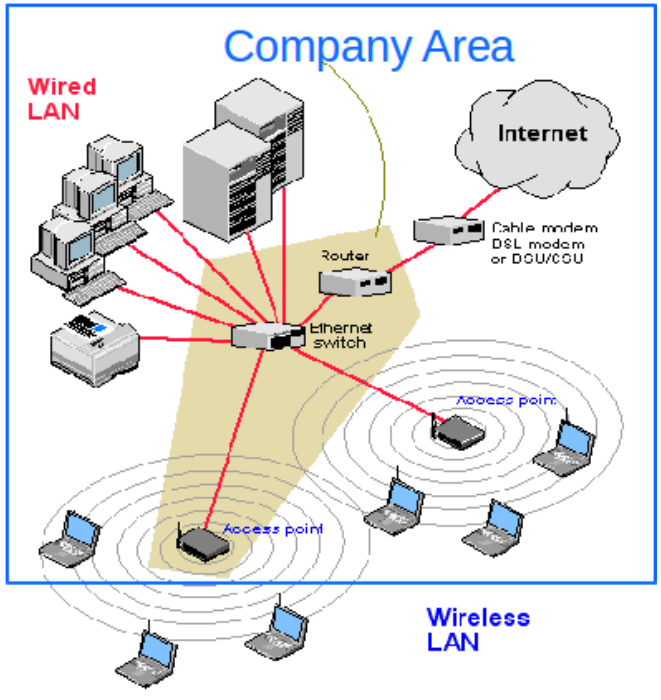
26/04/2013

Oder doch nicht?..:)

# Bonus Slides

# Everyone has WLAN

- WEP is outdated
- Hide SSID (private vs. enterprise)
- Provide conectivity only where needed



AUSTRIAN INSTITUTE OF TECHNOLOGY

# Using a nonstandard desktop is worth its weight in gold

Not only do the alternative desktops (Enlightenment, Blackbox, Fluxbox, etc.) give you a whole new look and feel for your PC, they offer simple security from prying eyes you may never have thought of. I have deployed Fluxbox on kiosk machines when I wanted a machine that could do one thing: Browse the network. How do you do that? Simple. Create a single mouse menu (or desktop icon) for the application you want to use. Unless the user knows how to get back to the command line (by logging out or hitting Ctrl-Alt-F*, where * is a desktop other than the one you are using), they will not be able to start up any application other than the one offered. Since most users have no idea how to move around in these desktops anyway, they aren't going to have the slightest idea how to get to your files. Simple pseudo-security.

AUSTRIAN INSTITUTE OF TECHNOLOGY

# Installing virus protection is actually useful in Linux

Believe it or not, virus protection in Linux has its place. Of course, the chances of a virus causing problems on YOUR Linux machine are slim to none. But those e-mails you forward to others' Windows machines could cause problems. With a good virus protection (like ClamAV), you can ensure that e-mail going out of your machine doesn't contain anything nasty that could come back to haunt you (or your company).

AUSTRIAN INSTITUTE OF TECHNOLOGY

# Creating /home in a separate partition is safer

The default Linux installation places your /home directory right in the root of your system. Sure, this is fine, but 1) it's standard, so anyone gaining access to your machine knows right where your data is and 2) if your machine goes down for good, your data might be gone. To solve this problem, you can place /home on a different hard drive or partition all together (making it a partition in and of itself). This is not a task for the weak of heart, but it is one worth employing if you're uber-concerned about your data.

AUSTRIAN INSTITUTE OF TECHNOLOGY

# Installing file-sharing applications is a slippery slope

I know many Linux users are prone to file sharing. If you want to run that risk at home, that's your call. But when at work, you not only open yourself (or your company) up to lawsuits, you open your desktop machine up to other users who might have access to sensitive data on your work PC. So as a rule, do not install file-sharing tools.

# The end

Really the very end.