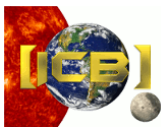


Linux Anwender-Security

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

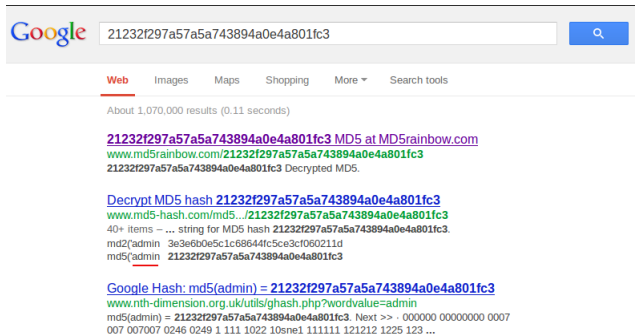
- Sicheres Passwort
 - > 8 Zeichen
 - Buchstaben, Zahlen, Sonderzeichen
- Keine automatische Anmeldung
- Bildschirmschoner

Warum? - Wie sieht ein Passwort aus?

Host	User	Password
any	admin	21232f297a57a5a743894a0e4a801fc3

Host	User	Password
any	fritz	xxj31ZMTZzkVA

"Entschlüsselung" mit Google



Google

[Web](#) [Images](#) [Maps](#) [Shopping](#) [More ▾](#) [Search tools](#)

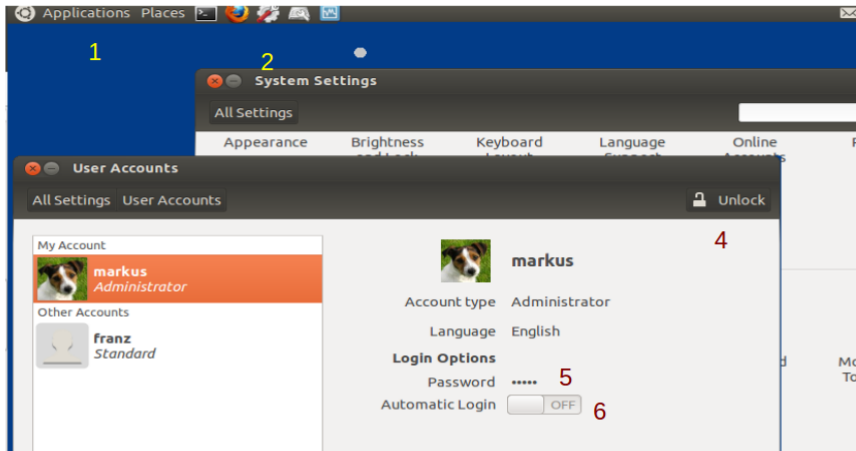
About 1,070,000 results (0.11 seconds)

[21232f297a57a5a743894a0e4a801fc3 MD5 at MD5rainbow.com](#)
www.md5rainbow.com/21232f297a57a5a743894a0e4a801fc3
21232f297a57a5a743894a0e4a801fc3 Decrypted MD5.

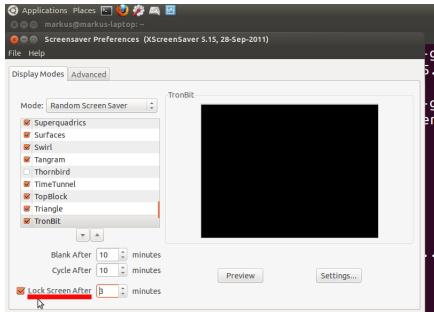
[Decrypt MD5 hash 21232f297a57a5a743894a0e4a801fc3](#)
www.md5-hash.com/md5.../21232f297a57a5a743894a0e4a801fc3
 40+ items - ... string for MD5 hash **21232f297a57a5a743894a0e4a801fc3**.
 md2{admin} 3e3e6b0e5c1c68644fc5ce3cf060211d
 md5{admin} **21232f297a57a5a743894a0e4a801fc3**

[Google Hash: md5\(admin\) = 21232f297a57a5a743894a0e4a801fc3](#)
www.nth-dimension.org.uk/utills/ghash.php?wordvalue=admin
 md5(admin) = **21232f297a57a5a743894a0e4a801fc3**. Next >> · 000000 00000000 0007
 007 007007 0246 0249 1 111 1022 10sne1 1111111 121212 1225 123 ...

Authentifizierung-Konfiguration



Bildschirmschoner



The screenshot shows the 'ScreenSaver Preferences' window for XScreenSaver 5.15, 28-Sep-2011. The 'Advanced' tab is active, showing a list of screen saver modes. The 'TronBit' mode is selected. Below the list, there are settings for 'Blank After' (10 minutes), 'Cycle After' (10 minutes), and 'Lock Screen After' (1 minutes). A mouse cursor is pointing at the 'Lock Screen After' setting.

```

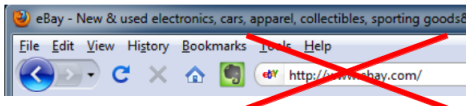
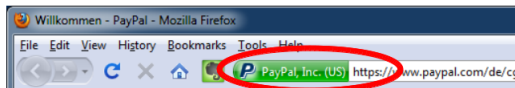
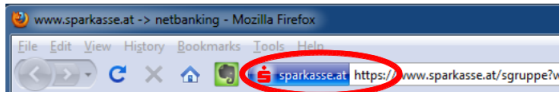
ldconfig deferred processing now taking place
markus@markus-laptop:~$ xscreensaver
xscreensaver                xscreensaver-getimage-fil
xscreensaver-command       xscreensaver-getimage-vid
xscreensaver-demo          xscreensaver-gl-helper
xscreensaver-getimage      xscreensaver-text
markus@markus-laptop:~$ xscreensaver-demo

```


Sichere Websites

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

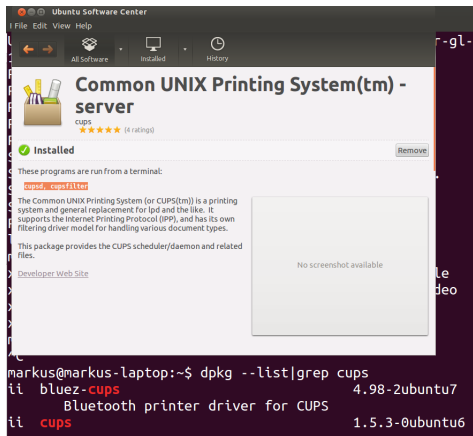
https Beispiele



Welche Software?

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

Was ist cups und welche version version verwende ich?



Ubuntu Software Center

File Edit View Help

All Software Installed History

Common UNIX Printing System(tm) - server

cups
★★★★☆ (4 ratings)

Installed Remove

These programs are run from a terminal:

`cupsd, cupsfilter`

The Common UNIX Printing System (or CUPS(tm)) is a printing system and general replacement for lpd and the like. It supports the Internet Printing Protocol (IPP), and has its own filtering driver model for handling various document types.

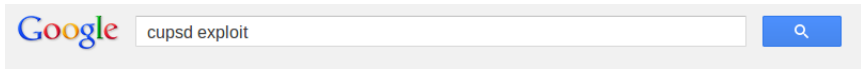
This package provides the CUPS scheduler/daemon and related files.

[Developer Web Site](#)

No screenshot available

```
markus@markus-laptop:~$ dpkg --get-architecture cups
ii bluez-cups 4.98-2ubuntu7
Bluetooth printer driver for CUPS
ii cups 1.5.3-0ubuntu6
```

Ist meine Version gefährdet?



Web Images Maps Shopping More Search tools

About 45,400 results (0.31 seconds)

[CUPS < 1.3.8-4 \(pstopdf filter\) Privilege Escalation Exploit](#)

www.exploit-db.com/exploits/7550/

Dec 22, 2008 – Note: * * This **exploit** only works under the (rare) conditions that **cupsd** executes * external filters as a privileged user, a printer on the system ...

[CUPS Cupsd Request Method Denial Of Service Vulnerability](#)

www.securityfocus.com/bid/7637/exploit

SecurityFocus is designed to facilitate discussion on computer security related topics, create computer security awareness, and to provide the Internet's largest ...

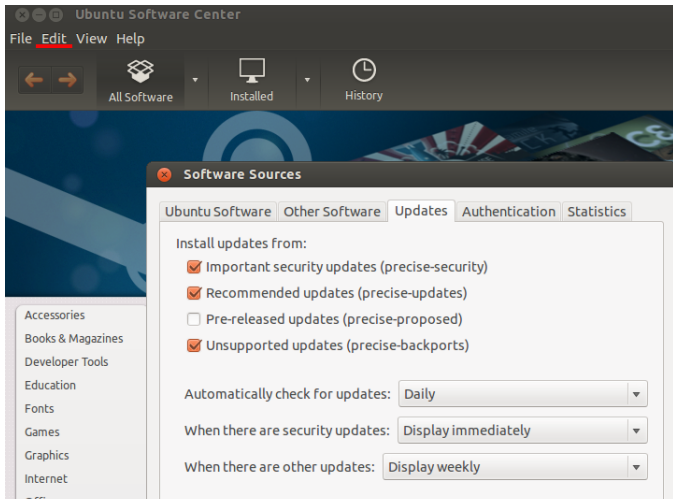
[ISS X-Force Database: cups-cupsd-code-execution\(62882\): CUPS ...](#)

xforce.iss.net/xforce/xfdb/62882

Oct 28, 2010 – ... corruption error in the CUPS daemon (**cupsd**). By sending a specially-crafted IPP request, a remote attacker could **exploit** this vulnerability to ...

[CUPS Integer Overflow Exploit - SecurityFocus.com](#)

Software Updates - HowTo

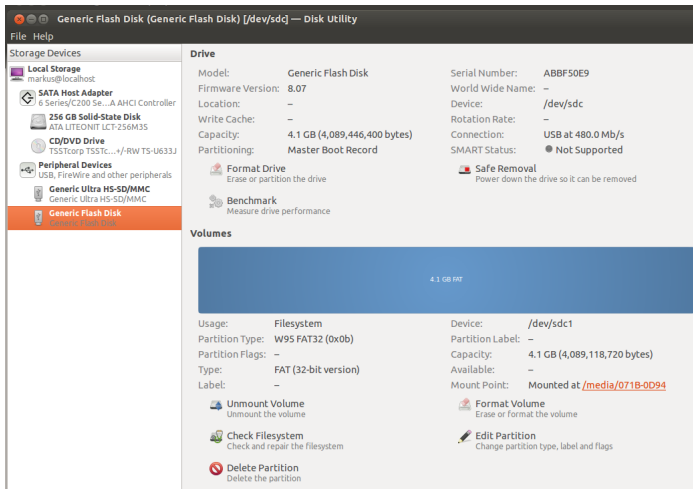


Festplatten Verschlüsselung

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



Disk Utility Beispiel 1



Generic Flash Disk (Generic Flash Disk) [/dev/sdc] — Disk Utility


File Help


Storage Devices


- Local Storage
 - markus@localhost
 - SATA Host Adapter
 - 6 Series/C200 Se...A AHCI Controller
 - 256 GB Solid-State Disk
 - ATA LITEONIT LCT-256M35
 - CD/DVD Drive
 - TSSTcorp TSSTC...+/RW TS-U633J
 - Peripheral Devices
 - USB, FireWire and other peripherals
 - Generic Ultra HS-SD/MMC
 - Generic Ultra HS-SD/MMC
 - Generic Flash Disk**

Drive

Model:	Generic Flash Disk	Serial Number:	ABBF50E9
Firmware Version:	8.07	World Wide Name:	–
Location:	–	Device:	/dev/sdc
Write Cache:	–	Rotation Rate:	–
Capacity:	4.1 GB (4,089,446,400 bytes)	Connection:	USB at 480.0 Mb/s
Partitioning:	Master Boot Record	SMART Status:	● Not Supported

 **Format Drive**
Erase or partition the drive


 **Safe Removal**
Power down the drive so it can be removed


 **Benchmark**
Measure drive performance


Volumes


4.1 GB FAT


Usage:	Filesystem	Device:	/dev/sdc1
Partition Type:	W95 FAT32 (0x0b)	Partition Label:	–
Partition Flags:	–	Capacity:	4.1 GB (4,089,118,720 bytes)
Type:	FAT (32-bit version)	Available:	–
Label:	–	Mount Point:	Mounted at /media/071B-0D94

 **Unmount Volume**
Unmount the volume

 **Format Volume**
Erase or format the volume

 **Check Filesystem**
Check and repair the filesystem

 **Edit Partition**
Change partition type, label and flags

 **Delete Partition**
Delete the partition

Disk Utility Beispiel 2

Generic Flash Disk (Generic Flash Disk) [/dev/sdc] — Disk Utility

File Help

Storage Devices

- Local Storage**
markus@localhost
- SATA Host Adapter**
6 Series/C200 Se...AHCI Controller
- 256 GB Solid-State Disk**
ATA LITEONIT ICT-256M3S
- CD/DVD Drive**
TSSSTcorp TSSSTc...+/-RW TS-U633J
- Peripheral Devices**
USB, FireWire and other peripherals
- Generic Ultra HS-SD/MMC**
Generic Ultra HS-SD/MMC
- Generic Flash Disk**
Generic Flash Disk

Drive

Model:	Generic Flash Disk	Serial Number:	ABBF50E9
Firmware Version:	8.07	World Wide Name:	–
Location:	–	Device:	/dev/sdc
Write Cache:	–	Rotation Rate:	–
Capacity:	4.1 GB (4,089,446,400 bytes)	Connection:	USB at 480.0 Mb/s
Partitioning:	Master Boot Record	SMART Status:	● Not Supported

Format Drive
Erase or partition the drive

Safe Removal
Power down the drive so it can be removed

Benchmark
Measure drive performance

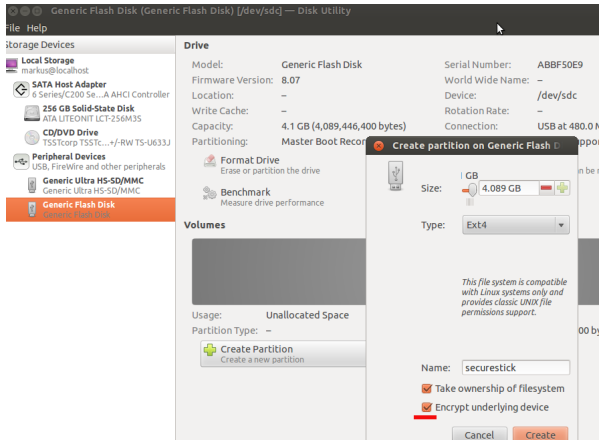
Volumes

Free
4.1 GB

Usage: **Unallocated Space** Device: /dev/sdc
 Partition Type: – Capacity: 4.1 GB (4,089,446,400 bytes)

Create Partition
Create a new partition

Disk Utility Beispiel 3



The screenshot shows the Disk Utility application window titled "Generic Flash Disk (Generic Flash Disk) [/dev/sdc] — Disk Utility". The main window displays drive information for the selected "Generic Flash Disk":

- Model: Generic Flash Disk
- Firmware Version: 8.07
- Location: -
- Write Cache: -
- Capacity: 4.1 GB (4,089,446,400 bytes)
- Partitioning: Master Boot Record
- Serial Number: ABBF50E9
- World Wide Name: -
- Device: /dev/sdc
- Rotation Rate: -
- Connection: USB at 480.0 M

The "Volumes" section shows "Unallocated Space" with a "Create Partition" button. A modal dialog box titled "Create partition on Generic Flash Disk" is open, showing the following configuration:

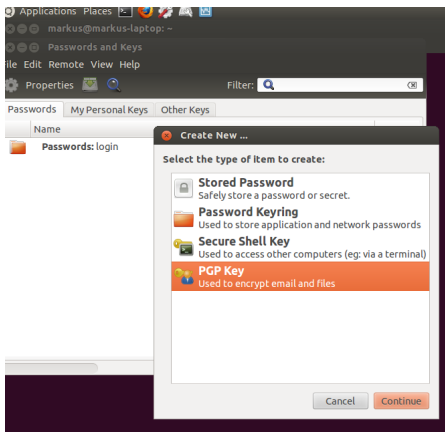
- Size: 4.089 GB
- Type: Ext4
- Name: securestick
- Take ownership of filesystem
- Encrypt underlying device

Buttons for "Cancel" and "Create" are visible at the bottom of the dialog.

Email verschlüsseln und signieren

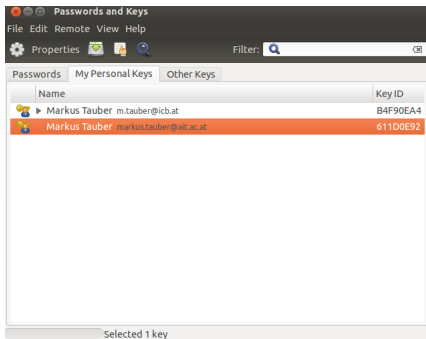
- Public/Private Key System
 - Public Key - darf öffentlich gemacht werden (website, pgp sever,..)
 - Nachrichten die mit öffentlichem Schlüssel verschlüsselt wurden können nur mit dazugehörigem privatem Schlüssel entschlüsselt werden.
- Thunderbird plugin: enigmail
- PGP, GPG, sMime

PGP - Schlüsselgenerierung



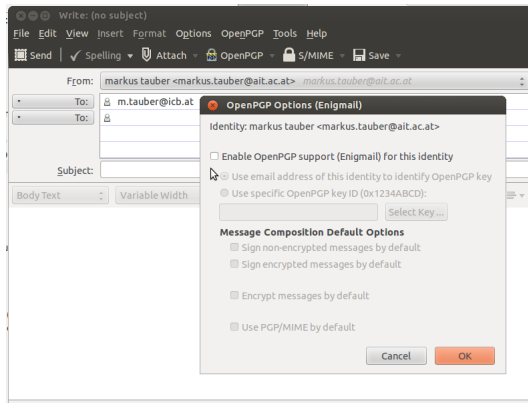
- Applications -> Preferences -> Password and Keys
- Strg + N

PGP - Schlüsselerwaltung

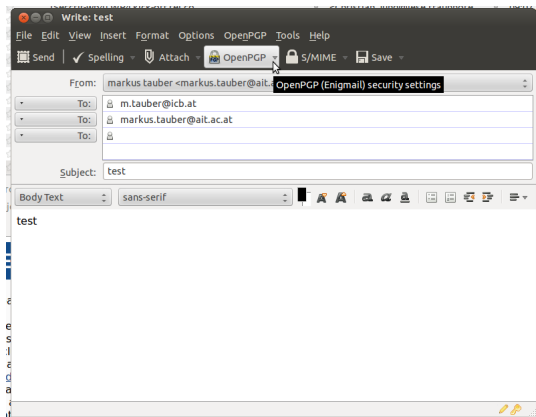


- export public key
- share it on key servers
- look for other keys on key servers

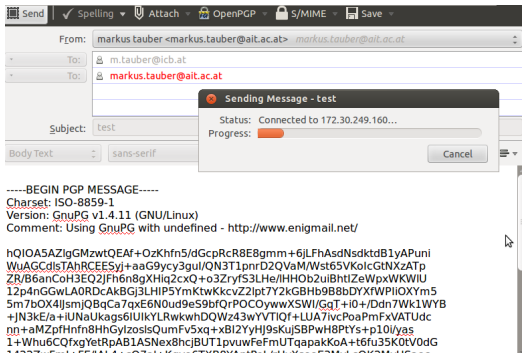
PGP - Schlüsselerwendung



PGP - Email Signatur und Verschlüsselung



PGP - Verschlüsselter Text



Send Spelling Attach OpenPGP S/MIME Save

From: markus tauber <markus.tauber@ait.ac.at> markus.tauber@ait.ac.at

To: m.tauber@icb.at

To: markus.tauber@ait.ac.at

Subject: test

Body Text sans-serif

Sending Message - test

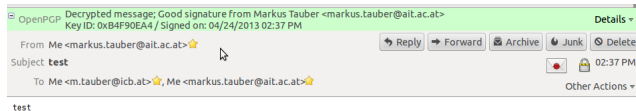
Status: Connected to 172.30.249.160...

Progress:

Cancel

-----BEGIN PGP MESSAGE-----
 Charset: ISO-8859-1
 Version: GnuPG v1.4.11 (GNU/Linux)
 Comment: Using GnuPG with undefined - http://www.enigmail.net/
 hQIOASAZIlgMzwtQEAF+OzKhfn5/dGcpcR8E8gmm+6jLFhAsdNsdktdB1yAPuni
 WuAGCdIsTAhRCEESyj+aaG9ycy3gul/QN3T1pnrD2QVaM/Wst65VKolcGtNxzATp
 ZR/B6anCoH3EQ2JFh6n8gXHIq2cxQ+o3ZryfS3LHe/IHHOb2uiBhtIzeWpxWKWIU
 12p4nGGwLA0RDcAkBGj3LHIP5YmKtwKkcVZ2lpt7Y2kGBHb9B8bDYXFWPIIOXYm5
 5m7bOX4IjsmjQBqCa7qxEN0ud9eS9bfQrPOCOywwXSWI/GgT+i0+/Ddn7Wk1WYB
 +JN3kE/a+iUNaUkags6IUIkYLRkwwhDQWz43wYTIQf+LUA7ivcPoaPmFxFVATUdc
 nn+aMZpfHfn8HhGylzosisQumFv5xq+xBi2YyH9sKujSBPwH8PtYs+p10I/yas
 1+Whu6CQfxgYtRpAB1ASNex8hcjBUT1pvuwFeFmUTqapakKoA+t6fu35K0tV0dG
 14337uFmU...

PGP - Entschlüsselter Text



Ende

Linux Anwender-Security

Dr. Markus Tauber
markus.tauber@ait.ac.at

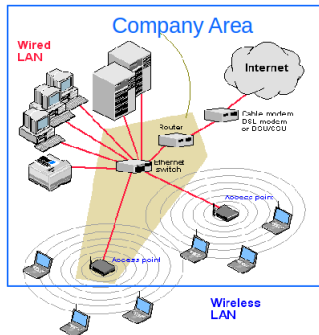
26/04/2013

Oder doch nicht?...:)

Bonus Slides

Everyone has WLAN

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



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.

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).

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.

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.