

Systemverschlüsselung unter Linux/Android mit LUKS

Lars Beckers

Open Source Software AK
Fachschaft Mathematik / Physik / Informatik

16.01.2014 / Cryptoparty

Gliederung

Einleitung

Warum will man seinen Computer verschlüsseln?

Wie will man die Verschlüsselung erreichen?

Linux

Linux Unified Key Setup

Linux verschlüsseln

Android

LUKS unter Android verwenden

Android verschlüsseln

Zusammenfassung

Ziel erreicht?

Ziel nicht erreicht?

Motivation

Warum will man seinen Computer verschlüsseln?

Pro

- Daten sollen privat bleiben.
- Notebooks haben sonst keinen Schutz.
- Diebstahl, Durchsuchung, ...

Contra

- Einrichtungsaufwand
- ein weiteres Passwort, bei jedem Start
- Daten bleiben sicher.

Motivation

Warum will man seinen Computer verschlüsseln?

Pro

- Daten sollen privat bleiben.
- Notebooks haben sonst keinen Schutz.
- Diebstahl, Durchsuchung, ...

Contra

- Einrichtungsaufwand
- ein weiteres Passwort, bei jedem Start
- Daten bleiben sicher.

Zielsetzung

Wie will man die Verschlüsselung erreichen?

Linux Unified Key Setup

- Standardwerkzeug unter Linux: LUKS
- einfaches Interface für starke Verschlüsselung
- unterstützt beliebige *devices*
- für mehrere Benutzer geeignet

Systemverschlüsselung

- Nutzdaten sichern
- Systemdaten sichern
- Programme und Metadaten im System sichern
- Daten sollen die Verschlüsselung nicht verlassen.

Zielsetzung

Wie will man die Verschlüsselung erreichen?

Linux Unified Key Setup

- Standardwerkzeug unter Linux: LUKS
- einfaches Interface für starke Verschlüsselung
- unterstützt beliebige *devices*
- für mehrere Benutzer geeignet

Systemverschlüsselung

- Nutzdaten sichern
- Systemdaten sichern
- Programme und Metadaten im System sichern
- **Daten sollen die Verschlüsselung nicht verlassen.**

LUKS

Linux Unified Key Setup

Wichtig vorab zu wissen

- One-Way.
- Backup machen!

Anforderungen

- Systemverschlüsselung bei Installation
- Sicherheit hängt an sicherem Passwort
- Auswahl eines geeigneten Algorithmus
- Einrichtung über Kommandozeile

LUKS

Linux Unified Key Setup

Wichtig vorab zu wissen

- One-Way.
- Backup machen!

Anforderungen

- Systemverschlüsselung bei Installation
- Sicherheit hängt an sicherem Passwort
- Auswahl eines geeigneten Algorithmus
- Einrichtung über Kommandozeile

Installation

Linux verschlüsseln

Einrichten

1. `apt-get install cryptsetup lvm2`
2. `modprobe dm-crypt`
3. Partitionierung:
unverschlüsselte Bootpartition,
Rest verschlüsselt (mit lvm2 aufteilen)
4. `cryptsetup -c aes-xts-plain64 -s 512 luksFormat /dev/sdX2`
5. `cryptsetup luksOpen /dev/sdX2 lukslvm`
6. `pvcreate /dev/mapper/lukslvm`
7. `vgcreate vgubuntu /dev/mapper/lukslvm`
8. `lvcreate -l 100%FREE -n root vgubuntu`
9. `mkfs.ext4 /dev/mapper/vgubuntu-root`

Installation

Linux verschlüsseln

Einrichten

10. In das verschlüsselte System wechseln. Software installieren.
11.

```
printf "lukslvm\tUUID=\"%s\"\tnone\tluks\n" \  
"$(cryptsetup luksUUID /dev/sdX2)" \  
| tee -a /etc/crypttab
```
12.

```
echo "dm-crypt" » /etc/modules
```
13. Bootloader umkonfigurieren.
14. Aus dem verschlüsselten System rausgehen. Neustarten.

Installation

Linux verschlüsseln

Einrichten

- Anleitung während des Installierens lesen.
- http://wiki.ubuntuusers.de/System_verschlüsseln

Schlüssel austauschen

- `cryptsetup luksAddKey /dev/sdX2`
- `cryptsetup luksRemoveKey /dev/sdX2`

Installation

Linux verschlüsseln

Einrichten

- Anleitung während des Installierens lesen.
- http://wiki.ubuntuusers.de/System_verschlüsseln

Schlüssel austauschen

- `cryptsetup luksAddKey /dev/sdX2`
- `cryptsetup luksRemoveKey /dev/sdX2`

Android

LUKS unter Android verwenden

Wichtig vorab zu wissen

- One-Way.
- Backup machen!
- nicht geeignet für mehrere Benutzer

Anforderungen

- seit Version 2.3.4 verfügbar
- oft keine Hardwareunterstützung
- Erstverlüsselung nicht unterbrechen
- Akku voll laden und am Strom lassen
- Verwendung von Passwort/PIN

Android

LUKS unter Android verwenden

Wichtig vorab zu wissen

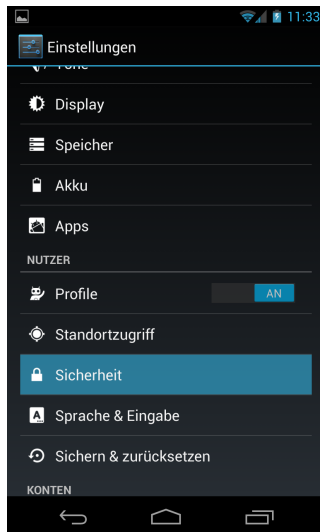
- One-Way.
- Backup machen!
- nicht geeignet für mehrere Benutzer

Anforderungen

- seit Version 2.3.4 verfügbar
- oft keine Hardwareunterstützung
- Erstverlüsselung nicht unterbrechen
- Akku voll laden und am Strom lassen
- Verwendung von Passwort/PIN

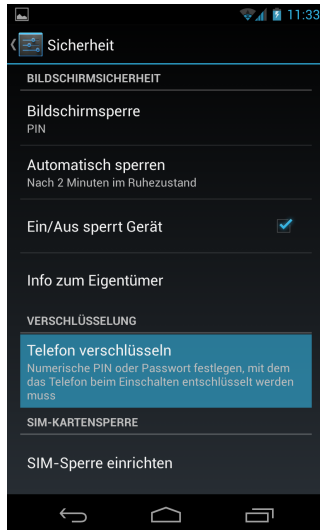
Installation

Android verschlüsseln



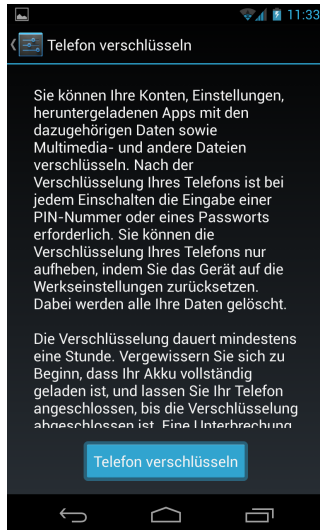
Installation

Android verschlüsseln



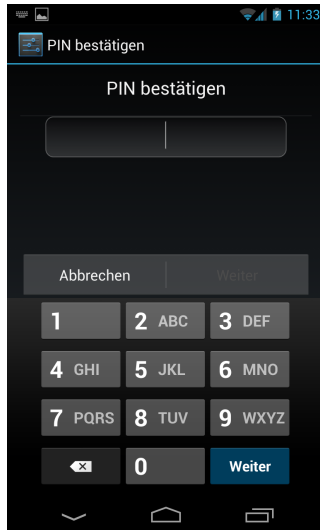
Installation

Android verschlüsseln



Installation

Android verschlüsseln



Zusammenfassung

Ziel erreicht?

Linux

- Programme und Daten verschlüsselt
- mit sicherem Algorithmus
- mit hoffentlich sicherem Passwort
- System nur noch unverschlüsselt angreifbar.

Android

- Automatische Einrichtung
- PIN/Passwort zur Entschlüsselung notwendig
- hoffentlich sicheres Passwort

Zusammenfassung

Ziel erreicht?

Linux

- Programme und Daten verschlüsselt
- mit sicherem Algorithmus
- mit hoffentlich sicherem Passwort
- System nur noch unverschlüsselt angreifbar.

Android

- Automatische Einrichtung
- PIN/Passwort zur Entschlüsselung notwendig
- hoffentlich sicheres Passwort

Ausblick

Ziel nicht erreicht?

Linux

- unverschlüsselte Passwortabfrage
- Besonderheiten SSDs/Flashspeicher
- Sicherheit des Masterkeys hängt am Passwort

Android

- Linux-Problematiken gelten ebenfalls
- Was machen Apps?

Ausblick

Ziel nicht erreicht?

Linux

- unverschlüsselte Passwortabfrage
- Besonderheiten SSDs/Flashspeicher
- Sicherheit des Masterkeys hängt am Passwort

Android

- Linux-Problematiken gelten ebenfalls
- Was machen Apps?