KRYPROGRAPHIE FÜR LINUX ADMINS

STEFAN MIETHKE & CARSTEN STROTMANN

Created: 2025-09-11 Thu 06:39

AGENDA

1. Grundlagen der Computersicherheit
2. Kryptografie für Linux-Systemadministratoren

GRUNDLAGEN DER COMPUTERSICHERHEIT

Sicherheitseinstellungen von Linux-Systemen sollten sich an der Gefährdung des Systems orientieren

- Wer ist der Angreifer
- Was sind die Ziele von Angreifer
- Was kann angegriffen werden (Daten, Ressourcen, Personen, Infrastruktur …)

LEBENSDAUER VON SYSTEMEN

Bei der Planung von Sicherheitssystemen muss die Lebensdauer dieser Systeme berücksichtigt werden

- Sind heute sichere System auch in 5,10,15 Jahren noch sicher?
- Die Lebenszeit von Computersystemen verlängert sich
  - Embedded Systeme (IoT)
  - Virtualisierung (Hardware wird erneuert, die VMs werden umgezogen)
  - 'Enterprise'-Distribution mit langer Wartung (10+ Jahre)

KOMPLEXITÄT VS. SICHERHEIT

- Unix-Systeme und Netzwerke sind komplex. Spezielle Sicherheitseinstellungen entfernen das System von der vom Hersteller gelieferten Grund-Konfiguration.
- Die Komplexität des Systems und der Systemadministration erhöht sich.

KOMPLEXITÄT VS. SICHERHEIT

- Spezielle Sicherheitseinstellungen sollten automatisiert eingerichtet und (regelmäßig) getestet werden. 'Configuration Orchestration' Werkzeuge können dabei helfen:
  - Ansible
  - SaltStack
  - Puppet
  - Chef
  - cfengine
- Dabei sollte das Werkzeug keine neuen Sicherheitslücken erzeugen!

KRYPTOGRAPHIE FÜR LINUX-SYSTEMADMINISTRATOREN

Eine kleine Einführung in Begriffe und Kryptographische Algorithmen, welche bei der Arbeit als Systemadmin vorkommen

1. Kryptographische Hashes (Fingerprints)
2. Hashed Message Authentication Codes (HMAC)
3. Symmetrische Verschlüsselung
4. Asymmetrische Verschlüsselung
5. Digitale Signaturen

FUNKTIONEN VON KRYPTOGRAPHIE

1. Authentisierung - die Antwort auf die Frage "wer?"
2. Integrität - die Antwort auf die Frage "wurden Daten geändert?"
3. Geheimhaltung - Daten Verschlüsseln so das nur der/die Empfänger die Daten lesen kann
4. Verbindlichkeit/Nichtabstreitbarkeit - "Sage nicht Du hast es nicht geschrieben"

KRYPTOGRAPHISCHE HASHES

Kryptographische Hashes sind spezielle mathematische Funktionen, welche aus beliebigen Eingabe-Daten einen digitalen Fingerabdruck fester Länge erstellen.

KRYPTOGRAPHISCHE HASHES

Kryptografische Hash-Funktionen haben dabei vier Hauptmerkmale:

- Die Berechnung des Hash-Wertes sollte einfach (nicht rechenintensiv) sein
- Die Hash-Funktion darf nicht umkehrbar sein, d.h. es darf nicht möglich sein nur aus dem Hash-Wert die ursprünglichen Daten wiederherzustellen
- Bei leichten Änderungen in den Eingabewerten muss sich der Hash komplett ändern
- Es muss unmöglich sein, zwei Eingabewerte zu finden welche in den gleichen Hash-Wert resultieren

Kryptographische Hash-Funktionen werden auch **Message Digest** genannt.

BEKANNTE KRYPTOGRAPHISCHE HASH-FUNKTIONEN

- MD5 (unsicher)
- RIPEMD160
- SHA1 (nicht mehr empfohlen)
- SHA256
- SHA512
- SHA3 (Keccak)

BENUTZUNG VON KRYPTOGRAFISCHEN HASH-FUNKTIONEN

- Integritätsprüfung von Dateien und Nachrichten (z.B. nach Download)
- Password-Prüfung (Datei `/etc/shadow`)
- 'Proof-of-Work', Beweis das der Anfrager eine Arbeit geleistet hat (z.B. Bitcoin Mining)
- Datei/Versions-ID (Beispiel 'git')

BENUTZUNG VON KRYPTOGRAFISCHEN HASH-FUNKTIONEN

Kryptografische Hash-Funktionen haben keine Authentisierungs-Funktion. Das prüfen von MD5-, SHA1- oder andern Hash-Werten nach dem Download einer Datei über ungesicherte Netzwerke gibt keine Auskunft über die Quelle der Daten!

BEISPIELE DER BENUTZUNG VON KRYPTOGRAFISCHEN HASH-FUNKTIONEN

```
# echo "Hallo" | md5sum
3290ec3c19a8a39362f7d70043f15627  -

# echo "Hallo" | sha1sum
6ce3fe1479a10edb2f1bdd6d181a5b0e210abe1a  -

# echo "Hallo" | openssl dgst -sha1
(stdin)= 6ce3fe1479a10edb2f1bdd6d181a5b0e210abe1a

# echo "Hallo" | openssl dgst -sha256
(stdin)= 5891b5b522d5df086d0ff0b110fbd9d21bb4fc7163af34d08286a2e846

# echo "Hello" | openssl dgst -sha256
(stdin)= 66a045b452102c59d840ec097d59d9467e13a3f34f6494e539ffd32c1b
```

HMAC - HASH-BASED MESSAGE AUTHENTICATION CODES

- HMAC-Funktionen verbinden eine kryptografische Hash-Funktion mit einem geteilten Geheimnis (pre shared secret, PSK).
- Ein HMAC liefert Authentisierung (die Daten kommen von einem Ersteller des HMAC mit dem PSK) und Integrität (die Daten wurden seit Erstellung des HMAC nicht verändert).
- HMACs sind symmetrische kryptografische Signaturen.
- HMAC-Funktionen werden z.B. SSH und DNS (TSIG) benutzt.

HMAC ALGORITHMEN

- HMAC-MD5 (siehe RFC 6151 "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms")
- HMAC-SHA1
- HMAC-SHA256
- HMAC-SHA512
- HMAC-RIPEMD160

WEITERE MAC-ALGORITHMEN

- UMAC-32/64/96/128 (OpenSSH)
- SKEIN-256/512 (SHA3-Finalist)
- Keccak/SHA3 (SHA3-Gewinner)
- Poly1305-AES (RFC 7539, TLS, OpenSSH)

BEISPIELE: HMAC-SHA1 MIT OPENSSL

```
echo –n "nachricht" | openssl sha1 –hmac "geheimnis"
```

SYMMETRISCHE VERSCHLÜSSELUNG

- Bei symmetrischer Verschlüsselung kommt sowohl beim Verschlüsseln als auch beim Entschlüsseln der identische Schlüssel zur Anwendung (Preshared Secret Key, PSK).
- Symmetrische Verschlüsselung ist in der Regel um ein vielfaches schneller als asymmetrische Verschlüsselung

SYMMETRISCHE VERSCHLÜSSELUNGS-ALGORITHMEN

- DES (veraltet, unsicher)
- 3DES (unsicher)
- AES-128/256 (Rijndael)
- Twofish (AES Finalist, OpenSSH)
- Serpent (AES Finalist)
- RC4 (unsicher)
- Salsa20/ChaCha20 (RFC 7539, benutzt in OpenSSL/Android/Chrome/OpenSSH)

BEISPIEL: SYMMETRISCHE VERSCHLÜSSELUNG MIT OPENSSL: RC4

- RC4 (schnell, aber ggf. nicht sicher genug)

```
echo "Hallo LinuxHotel" | openssl enc -e -rc4 -a
enter rc4 encryption password:
Verifying - enter rc4 encryption password:
U2FsdGVkX1+/19xWWHObEzgY8tNP8MCQUrqOO83ylzzy

echo "U2FsdGVkX1+/19xWWHObEzgY8tNP8MCQUrqOO83ylzzy" \
  | openssl enc -d -rc4 -a
```

BEISPIEL: SYMMETRISCHE VERSCHLÜSSELUNG MIT OPENSSL: AES

```
% echo "Hallo LinuxHotel" | openssl enc -e -aes256 -a
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
U2FsdGVkX186OZf2oJrGRtSOHtSusHEZSapzohhY2JtlbDAdBXSYUlAVFX1UFtnM

echo "U2FsdGVkX186OZf2oJrGRtSOHtSusHEZSapzohhY2JtlbDAdBXSYUlAVFX1UFtnM" \
    | openssl enc -d -aes256 -a
```

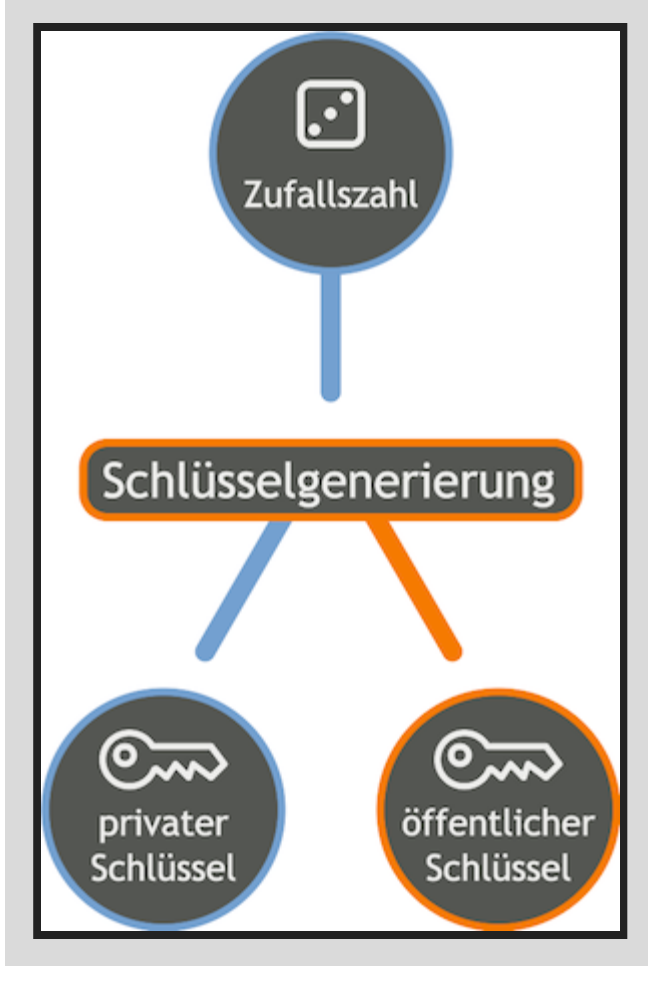
ASYMMETRISCHE VERSCHLÜSSELUNG

- Bei der asymmetrischen Verschlüsselung kommen Schlüsselpaare, bestehend aus öffentlichen und privaten Schlüsseln zum Einsatz.
- Daten, welche mit dem privaten Schlüssel verschlüsselt wurden, können nur mit dem öffentlichen Schlüssel wieder entschlüsselt werden (Digitale Signatur).
- Daten, welche mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem privaten Schlüssel entschlüsselt werden.

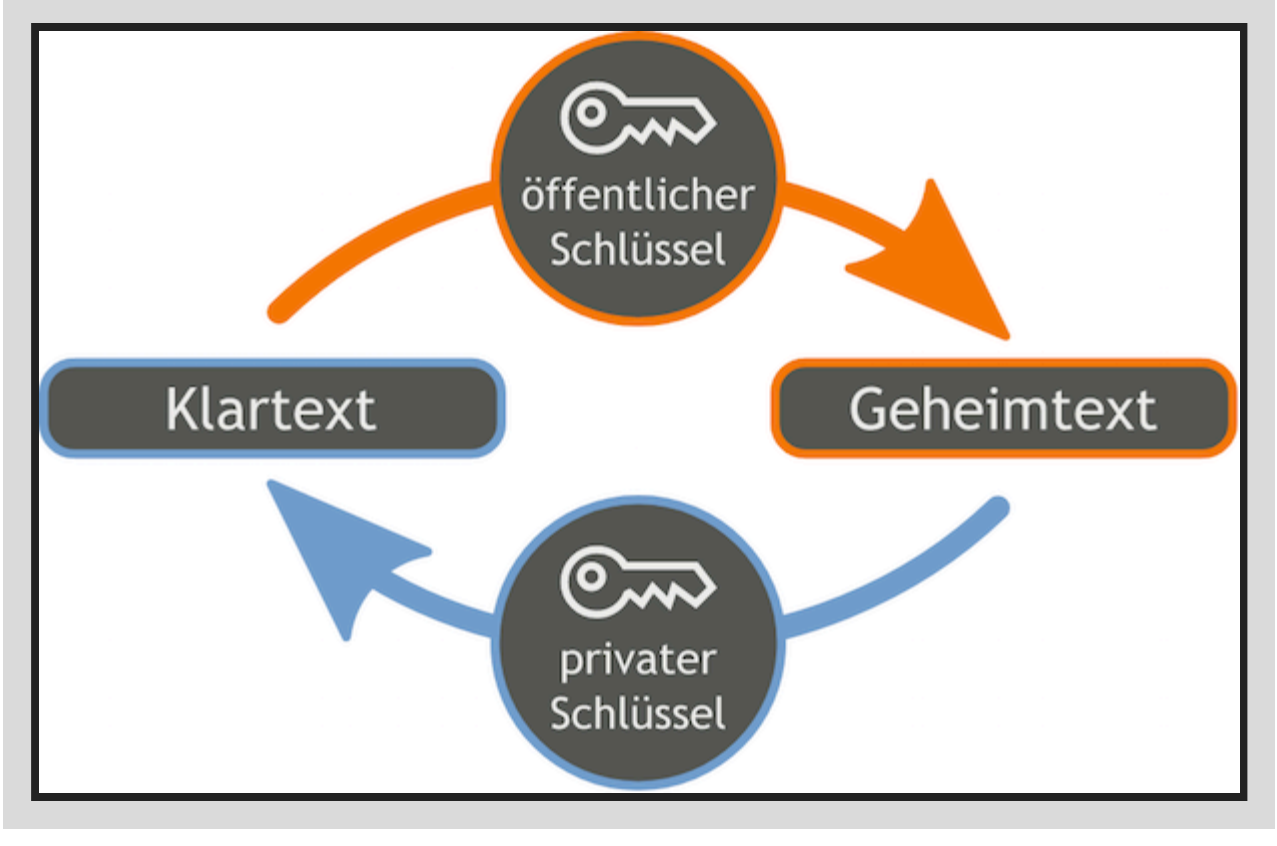
ASYMMETRISCHE VERSCHLÜSSELUNGSALGORITHMEN

- RSA
- Elliptische Kurven (ECDSA, ED25519, ED448 …)
- Elgamal
- McEliece (Post-Quantum-Safe)

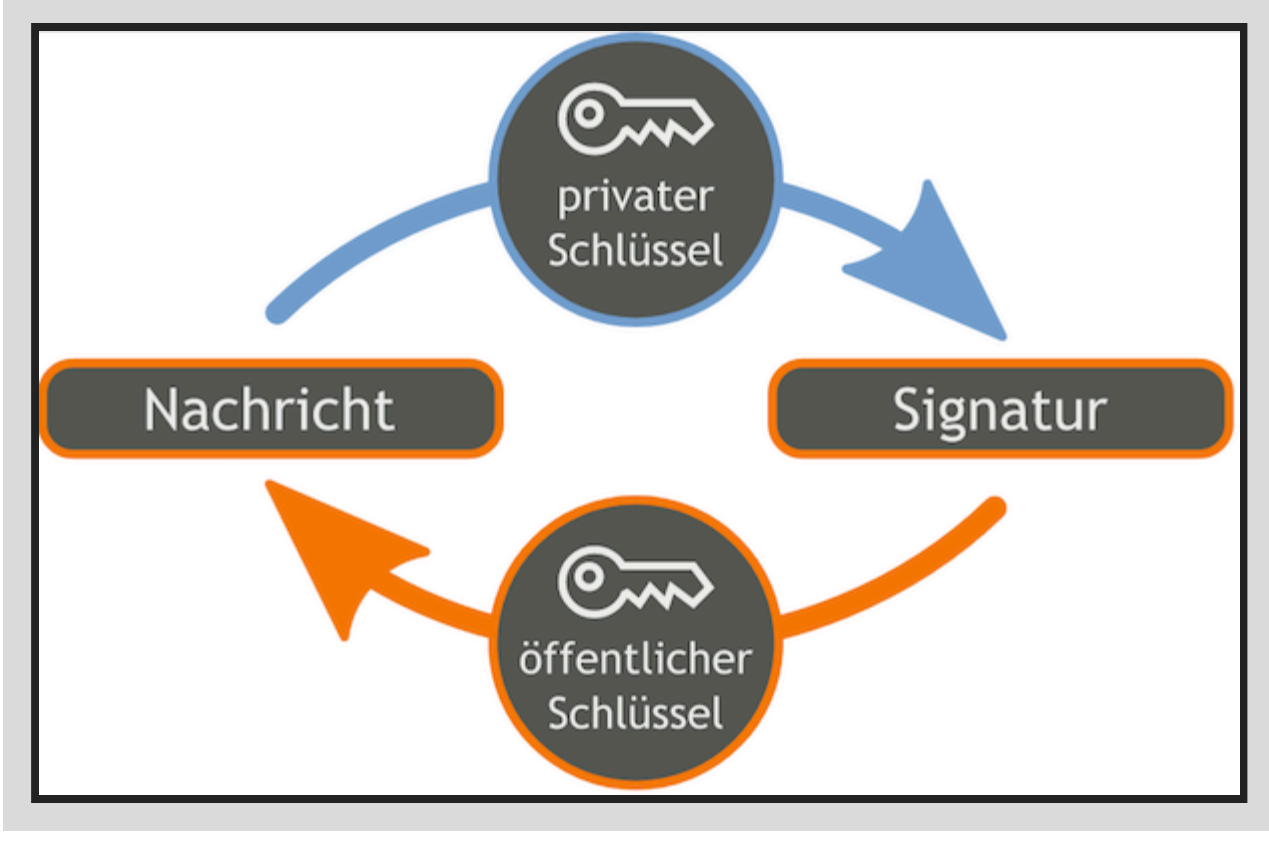
ASYMMETRISCHE VERSCHLÜSSELUNG



ASYMMETRISCHE VERSCHLÜSSELUNG



ASYMMETRISCHE DIGITALE SIGNATUR



BEISPIEL ASYMMETRISCHE VERSCHLÜSSELUNG MIT OPENSSL (1/3)

```
# einen neuen privaten RSA Schlüssel erstellen
openssl genpkey -algorithm RSA -out key.pem
# den privaten Schlüssel mit AES 256bit verschlüsseln
openssl pkey -in key.pem -aes256 -out keyaes.pem
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
rm key.pem
```

BEISPIEL ASYMMETRISCHE VERSCHLÜSSELUNG MIT OPENSSL (2/3)

```
# den öffentlichen Schlüssel erzeugen
openssl pkey -in keyaes.pem -pubout -out pubkey.pem
# Daten mit dem öffentlichen Schlüssel verschlüsseln
echo "Hallo LinuxHotel" > plain.txt
openssl pkeyutl -in plain.txt -out cipher.txt -encrypt \
    -pubin -inkey pubkey.pem
cat cipher.txt | od -x -a
```

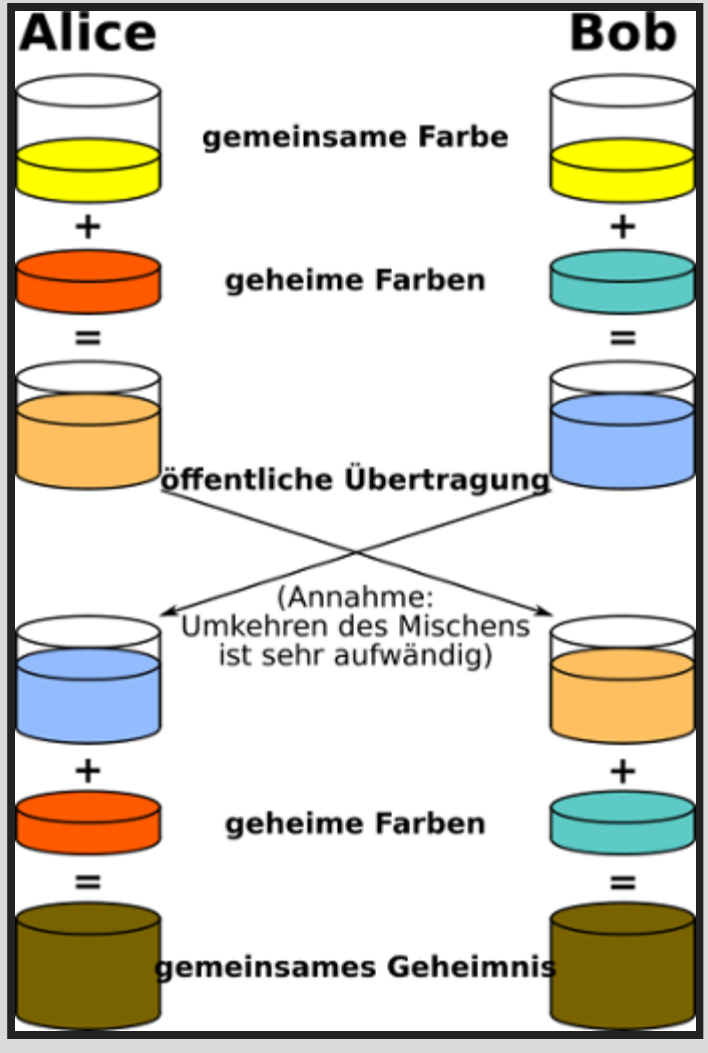
BEISPIEL ASYMMETRISCHE VERSCHLÜSSELUNG MIT OPENSSL (2/3)

```
# Daten mit dem privaten Schlüssel entschlüsseln
openssl pkeyutl -in cipher.txt -out plain2.txt \
  -decrypt -inkey keyaes.pem
Enter pass phrase for keyaes.pem:
cat plain2.txt
Hallo LinuxHotel
```

SCHLÜSSELAUSTAUSCH-PROTOKOLLE

- In verschlüsselten Kommunikationsverbindungen müssen die Kommunikationsparter oft einen gemeinsamen, geheimen Schlüssel aushandeln.
- Das Diffie-Hellman-Verfahren erlaubt es, einen gemeinsamen geheimen Schlüssel zu errechnen, ohne das ein Angreifer mit Zugriff auf die Kommunikation diesen Schlüssel auch errechnen kann.
    - Diffie-Hellman-Schlüsselaustausch
    - Ephemeral Diffie-Hellman (Forward-Secrecy)
    - Elliptic Curve Diffie-Hellman (ECDH)
- **Achtung**: Schlechte DH-Parameter vermeiden: https://weakdh.org/

DIFFIE-HELLMANN-SCHLÜSSELAUSTAUSCH


Alice
Bob
gemeinsame Farbe
+
+
geheime Farben
=
=
öffentliche Übertragung
(Annahme:
Umkehren des Mischens
ist sehr aufwändig)
+
+
geheime Farben
=
=
gemeinsames Geheimnis

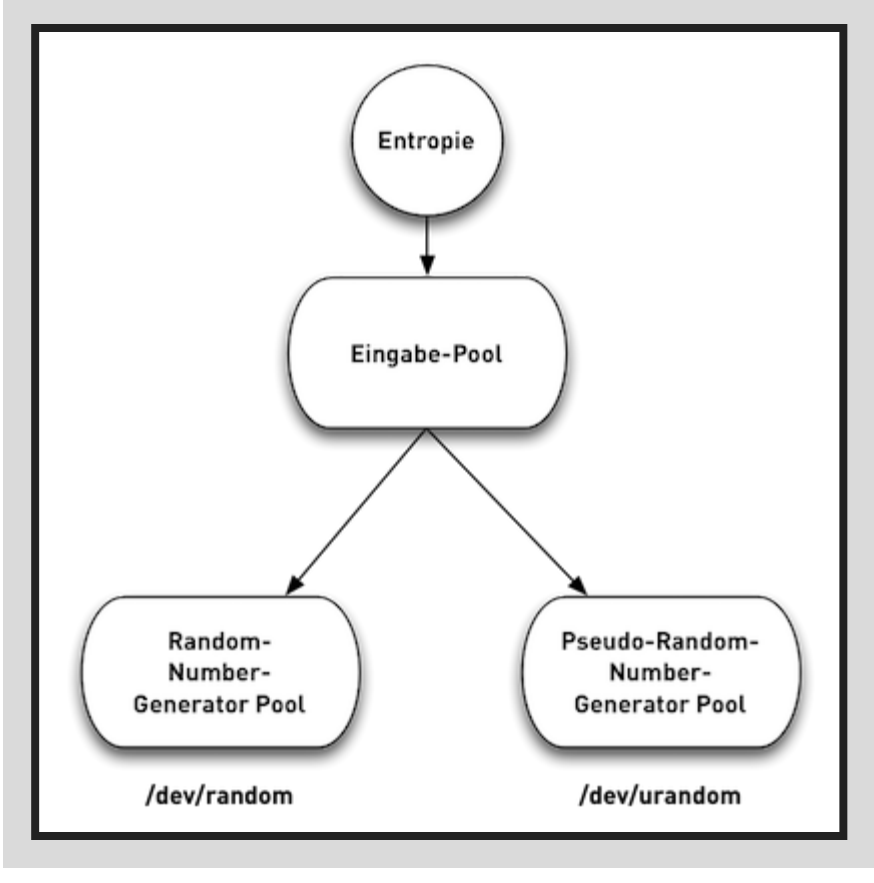
ZUFALLSZAHLEN UND LINUX

- Einige kryptografische Protokolle benötigen qualitativ hochwertige (== statistisch zufällige) Zufallszahlen.
- Die Erzeugung von echtem Zufall in einem Computersystem ist schwierig.
- In Linux werden Zufallszahlen im Kernel per Software Cryptographically secure pseudorandom number generator (CSPRNG) erzeugt
- Quelle für den CSPRNG sind dabei Ereignisse aus der *echten Welt* (Tastatur-Anschlägen des Benutzers, Interrupts der Netzwerkkarte etc)

ZUFALLSZAHLEN UND LINUX

- Der Linux-Kernel bietet zwei Geräte-Schnittstellen als Quelle für Zufallszahlen:
  - `/dev/random` - liefert Zufallsereignisse aus dem CSPRNG und kann blockieren
  - `/dev/urandom` - liefert Zufall aus dem CSPRNG und blockiert nicht

ZUFALLSZAHLEN UND LINUX



ZUFALLSZAHLEN, VIRTUELLE MASCHINEN UND LINUX (1/2)

- In virtuellen Maschinen, aber auch auf echter Hardware (embedded Systemen, Raspberry-Pi, günstigen Routern), kann es vorkommen, das nicht genügend Entropie (Zufall) im Linux-System vorhanden ist.
- Effekt ist, das Programme mit kryptografischen Funktionen (z.B. RSA-Schlüsselerzeugung) sehr lange laufen.

ZUFALLSZAHLEN, VIRTUELLE MASCHINEN UND LINUX (2/2)

- In solchen Situationen muss für mehr Entropie im System gesorgt werden (in absteigender Reihenfolge):
  - Einen Hardware Zufallszahlen-Generator benutzen
  - Eine CPU mit Zufallszahlen-Generator verwenden (Intel RDRAND)
  - Bei KVM/QEmu `/dev/random` oder `/dev/urandom` per VirtIO Gerät in die VM durchreichen
  - In der VM einen Entropie-Gathering-Daemon (EGD) benutzen Ein bekannter EGD für Mehr-Kern-CPU-Systeme is `haveged`. Der Nutzen und die Sicherheit von EGD ist umstritten.

PSEUDO-ZUFALLSZAHLEN PER OPENSSL ERZEUGEN (1/2)

- Auch OpenSSL kann Zufallszahlen erzeugen.
- Ein Zufallszahlengenerator welcher ausserhalb des Kernels läuft kann jedoch von Angreifern einfacher manipuliert werden und sollte nur in Aussnahmefällen benutzt werden (z.B. wenn die Benutzung von `/dev/urandom` nicht möglich ist)

PSEUDO-ZUFALLSZAHLEN PER OPENSSL ERZEUGEN (2/2)

- Der nachfolgende Befehl gibt 10 Pseudo-Zufallszahlen im hexadezimaler Format aus. Der Pseudo-Zufallszahlen-Genertator wird hierbei aus der Datei `~/.rnd` und `/dev/urandom` initialisiert ("seeding"):

```
openssl rand -rand /dev/urandom -hex 10
% ls -l ~/.rnd
-rw-------. 1 nutzer nutzer 1024 Nov 22 22:12 /home/cas/.rnd
```

- OpenSSL legt in der Datei `~/.rnd` Entropie für spätere Aufrufe ab.