Tutorium Fortgeschrittene

ubuntu

Übersicht

- Sicherheit
  - GPG
  - TOR
  - OTR
  - ...

GPG

ubuntu

GPG

- GPG = GNU Privacy Guard
- Freies Kryptographiesystem
- Verwendet keine patentierten Algorithmen
- Ver- und Entschlüsseln von Daten
- Erzeugen und prüfen von elektronischen Signaturen

GPG

- Gründe für GPG:
  - E-Mails sind von jedem lesbar und veränderbar (wie Postkarten)
  - Passwörter, private Daten,... sind nicht sicher
  - Identität des Absenders ist nicht sichergestellt

GPG

- Schlüssel erstellen
  - Terminal: gpg –gen-key
  - GUI: ”Gnu Privacy Assistant”, ”Seahorse”

- Hinweis: Man sollte seinen Richtigen und vollen Namen angeben

GPG

- Web of Trust
  - Gegenseitiges signieren der Schlüssel
  - Je mehr Signaturen umso wahrscheinlicher ist die Echtheit der Person
  - Zertifizierungsstellen (z.B. ”c't Zeitschrift”), Kontrolle des Personalausweises
  - Vergleich des digitalen Fingerabdrucks

GPG

- E-Mails signieren/verschlüsseln
  - Öffentlicher Schlüssel des Empfängers muss bekannt sein
  - Eigener öffentlicher Schlüssel muss dem Empfänger bekannt sein
  - Mail-Programm mit GPG-Unterstützung (Evolution, Thunderbird, Claws,...)

GPG

- Fazit
  - Erst durch signieren und verschlüsseln werden E-Mails sicher
  - Unverschlüsselte E-Mails sollten immer kritisch hinterfragt werden

TOR

TOR

- Anonymisierungsdienst
  - Anfragen des Nutzers werden über 3 Server (Nodes) geleitet (”Zwiebelprinzip”)
  - Erst der letzte Node (Exit-Node) entschlüsselt die Daten vollständig und sendet sie an die gewünschte Adresse

TOR

- Vorteile:
  - Anonymisierung da IP-Adresse versteckt wird
  - Lässt sich mit vielen Programmen kombinieren (Browser, IM, Mail,...)

TOR

- Nachteile:
  - Exit-Nodes könnten Daten mitschneiden
  - Nur wirksam bei sinnvoller Verwendung
  - langsam

TOR

- Fazit
  - TOR ist eine relativ gute Lösung um anonym zu surfen
  - Man sollte aber wissen, wann die Verwendung von TOR sinnvoll ist und wann nicht
  - DNS-Leaks müssen zusätzlich unterbunden werden

OTR

ubuntu

OTR

- Off-the-Record Messaging
- Verschlüsselung für Instant Messenger
- Unabhängig vom Protokoll

ubuntu

OTR

- Eckpfeiler:
  - Verschlüsselung = Nachrichten können nicht von anderen gelesen werden
  - Authentifizierung = man kann sicher sein, mit wem man spricht
  - Abstreitbarkeit = die Nachrichten tragen keine digitale Signatur und könnten im NACHHINEIN manipuliert worden sein
  - Folgenlosgikeit = verliert man die Kontrolle über seinen privaten Schlüssel sind davon keine vorherigen Unterhaltungen betroffen

OTR

- Durch OTR können Unterhaltungen über IM-Dienste nicht mehr von Dritten mitgelesen werden
- Man geht damit unschönen Lizensbestimmungen vieler IM-Betreiber aus dem Weg

Lokale Sicherheit

Lokale Sicherheit

- Auch wenn der Rechner im Netz gut abgesichert ist sind die Daten nicht sicher wenn andere Personen Zugang zum PC haben
- Weitere Maßnahmen zur Absicherung sind nötig

Lokale Sicherheit

- Kann der Computer von einer Live-CD gestartet werden gelangt man meist an die Daten auf der Festplatte
- Gegenmaßnahmen:
  - Bootreihenfolge im BIOS ändern
  - BIOS mit Passwort schützen
- Probleme
  - Masterpasswörter beim BIOS
  - BIOS-Reset Jumper

Lokale Sicherheit

- Über den GRUB gelangt man in eine Rescue-Shell, in der man Root-Rechte besitzt. Außerdem kann man GRUB Parameter übergeben um root-Rechte zu bekommen
- Gegenmaßnahmen
  - GRUB mit Passwort versehen
  - Recovery-Modus nicht auflisten
- Probleme
  - Wiederherstellen des GRUB wird umständlich

Lokale Sicherheit

- Ubuntu hat kein root-Passwort. Dadurch könnte es passieren, dass der Benutzer an eine root-shell gelangt
- Gegenmaßnahmen
  - Passwort für root-User einrichten
- Probleme
  - Ubuntu-Konfiguration ist nicht darauf ausgelegt

Lokale Sicherheit

- Die Festplatte könnte einfach ausgebaut werden um an die Daten zu kommen
- Gegemaßnahmen
  - Verschlüsselung (z.B. Mit TrueCrypt oder LUKS)
  - Abschließbare PC-Gehäuse
- Probleme
  - Passwörter müssen sicher sein (und nicht vergessen werden!)

Fragen?!

ubuntu

Hinweise

- Bei Problemen sofort nachfragen
- Linux-Stammtisch (Jeden 2. Mittwoch im Monat um 19 Uhr)
- Dr. Tux – Die Sprechstunde für Linux-Interessierte
  - Sprechzeiten Mittwochs

    15.00 bis 17.00 Uhr
  - Ort: Database Competence

    Center (Raum F0001)

ubuntu