
# Verschlüsselte Kommunikation: Warum und wie.

Festival:progressive 2017

# <Eigenwerbung>

# Wer sind wir?

- Hochschulgruppe an der TU (gegründet 2014, ca. 10 P.)
- Studierende (TU, HTW) und andere Leute
- Hochschulen als Zielgruppe (Multiplikationswirkung) und Arbeitsfeld (Räume, Strukturen)

# Wer sind wir?

- Hochschulgruppe an der TU (gegründet 2014, ca. 10 P.)
- Studierende (TU, HTW) und andere Leute
- Hochschulen als Zielgruppe (Multiplikationswirkung) und Arbeitsfeld (Räume, Strukturen)

- Bisherige Projekte
  - Linux-Install-Party, Linux-Presentation-Day
  - Verschlüsselungsgewinnspiel
  - Monatliche Sprechstunde zu LaTeX u.a.
  - Formulierung eines Programmpapiers
  - „Uni-Stick“: 80 × 8 GB mit freier Software

# Warum machen wir das? Aus Überzeugung!

- *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)

# Warum machen wir das? Aus Überzeugung!

- *Überzeugung 1*: freie und quelloffene Software ist (oft) besser (technische + nicht technische Argumente)
- *Überzeugung 2*: öffentlich finanzierte wissenschaftliche Inhalte (AutorInnen, GutachterInnen) sollten nicht von öffentlich finanzierten Bibliotheken für horrende Summen von Zeitschriften-Verlagen gekauft werden müssen

# Projekt Uni-Stick

- **4000** Flyer in Ersti-Tüten: **Gutscheine** für 8 GB Stick mit freier Software fürs Studium, 550 € vom TU-StuRa für 80 Stk.
- Live-Linux / freie Windows-Programme

# Projekt Uni-Stick

- **4000** Flyer in Ersti-Tüten: **Gutscheine** für 8 GB Stick mit freier Software fürs Studium, 550 € vom TU-StuRa für 80 Stk.
- Live-Linux / freie Windows-Programme
- Hat viel Arbeit gemacht

# Projekt Uni-Stick

- **4000** Flyer in Ersti-Tüten: **Gutscheine** für 8 GB Stick mit freier Software fürs Studium, 550 € vom TU-StuRa für 80 Stk.
- Live-Linux / freie Windows-Programme
- Hat viel Arbeit gemacht
- Ist gut angekommen (ca. 250 TN)


# Projekt Uni-Stick

- **4000** Flyer in Ersti-Tüten: **Gutscheine** für 8 GB Stick mit freier Software fürs Studium, 550 € vom TU-StuRa für 80 Stk.
- Live-Linux / freie Windows-Programme
- Hat viel Arbeit gemacht
- Ist gut angekommen (ca. 250 TN)


- Accessibility:
  - brltty
  - gnome-orca (Screenreader)
  - ...
  - WIP!

# Zukunftsideen

- Fortführung „Uni-Stick“
- Studierende zum Nutzen/Verbessern freier Software animieren
  - Mehr Blog-Beiträge
  - Kurse (LaTeX/ Python / Git / Inkscape / . . . )
  - Ansible-Infrastruktur-Stipendium
  - OpenSource-Wettbewerb/Preis
  - . . .
- Aufmerksamkeit erzeugen / Lobby-Arbeit
- Vernetzung mit anderen Städten

# Weitere Informationen

https://fsfw-dresden.de/

- uni-stick
- blog
- newsletter
- mitmachen
- fork

</Eigenwerbung>

# Gliederung

- Einführung
- Sammlung von Argumenten und Diskussion („Ich habe doch nichts zu verbergen“)
- Theoretischer Hintergrund und Begriffsklärungen
- Unterstützung bei Installation und Einrichtung (Zeit?)
  - GPG-Enigmail (Thunderbird)
  - Mailvelope (Webmail)

# Einführung

In der Geschichte der Menschheit...

- ... kein Mangel an Beispielen für **rücksichtslosen Egoismus**
- Ausnutzung von Macht zu persönlichem Vorteil

# Einführung

In der Geschichte der Menschheit...

- ... kein Mangel an Beispielen für **rücksichtslosen Egoismus**
- Ausnutzung von Macht zu persönlichem Vorteil
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

# Einführung

In der Geschichte der Menschheit...

- ... kein Mangel an Beispielen für **rücksichtslosen Egoismus**
- Ausnutzung von Macht zu persönlichem Vorteil
- „Wissen ist Macht“

$\Rightarrow$ sensibler Umgang mit Informationen empfehlenswert

- Digitalisierung verstärkt das Problem:
- E-Mail[1] ist wie Postkarte: unterwegs[2] lesbar
- E-Mail ist schlimmer als Postkarte:
  - automatisiert auswertbar
  - unbemerkt kopierbar
  - unbemerkt veränderbar (inkl. Absender)

1: E-Mail = Beispielmedium  2: ggf. um die ganze Welt

# Einführung 2

Schutzziele sicherer Kommunikation:

- ☐ Vertraulichkeit
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität

# „Ich habe doch nichts zu verbergen“

10min freie Diskussion

- je 2-5 Personen
- verschiedene Perspektiven (Bürgerrechtler*in, Innenminister*in)
- Argumente aufschreiben

# „Ich habe doch nichts zu verbergen“

10min freie Diskussion

- je 2-5 Personen
- verschiedene Perspektiven (Bürgerrechtler*in, Innenminister*in)
- Argumente aufschreiben

Stichworte:

- Kriminalität (Einbruch, Erpressung, ...)
- Privatsphäre
- Selbstzensur (analog: Kamera-Attrappen)
- Demokratie
- Journalismus
- Whistleblowing
- Erstarken totalitärer Strukturen

# Begriffe

- asymmetrisches Verfahren
- Privater Schlüssel
- Öffentlicher Schlüssel
- Verschlüsseln
- Signieren / Signatur
- Schlüsselserver
- Web of Trust
- Widerrufszertifikat
- Cryptoparty
- Fingerabdruck
- Metadaten
- GPG vs PGP vs S/MIME
- Enigmail vs Mailvelope

# Hintergrundwissen 1

- Schlüsselverteilungsproblem

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren

- $\exists$ **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel
- sehr große zufällige Zahlen (dargestellt als Zeichensalat)

# Hintergrundwissen 1

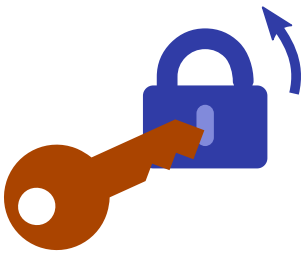
- Schlüsselverteilungsproblem

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren

  - $\exists$ **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel
  - sehr große zufällige Zahlen (dargestellt als Zeichensalat)

- ÖS: zum Verschlüsseln

- PS: zum Entschlüsseln



# Hintergrundwissen 1

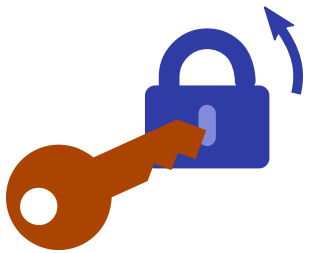
- Schlüsselverteilungsproblem

$\Rightarrow$ asymmetrisches Verschlüsselungsverfahren

  - $\exists$ **ö**ffentlicher **S**chlüssel und **p**rivater **S**chlüssel
  - sehr große zufällige Zahlen (dargestellt als Zeichensalat)

- ÖS: zum Verschlüsseln

- PS: zum Entschlüsseln



Oft eingesetzt: `GPG` (**G**nu**P**rivacy**G**uard) = Freie Software

Vorläufer: `PGP` (**P**retty **G**ood **P**rivacy) $\neq$ Freie Software, Namensgeber des Verfahrens

S/MIME: anderes Verfahren, hier nicht weiter behandelt

# Hintergrundwissen 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → Keyserver auf hochladen

    Bsp: `http://pgp.mit.edu` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?

# Hintergrundwissen 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → Keyserver auf hochladen

    Bsp: `http://pgp.mit.edu` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?
- Privater Schlüssel („private key“)
  - Benötigt zum Entschlüsseln
  - Darf nicht verloren gehen
    → Entschlüsseln wäre dann unmöglich
  - Darf nicht in fremde Hände kommen
    → andere können meine Mails entschlüsseln
  - Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

# Hintergrundwissen 2

- Öffentlicher Schlüssel („public key“)
  - Benötigt zum Verschlüsseln
  - Sollten alle haben, von denen man verschlüsselte Mails empfangen möchte
  - kann/sollte man weitergeben → Keyserver auf hochladen

    Bsp: `http://pgp.mit.edu` Bedenkenswert: Nicht löschen, nur Widerrufen → Anonymität?
- Privater Schlüssel („private key“)
  - Benötigt zum Entschlüsseln
  - Darf nicht verloren gehen
    → Entschlüsseln wäre dann unmöglich
  - Darf nicht in fremde Hände kommen
    → andere können meine Mails entschlüsseln
  - Typischerweise nochmal zusätzlich mit einem Passwort verschlüsselt

  ⇒ Sicheres Backup wichtig

# Hintergrundwissen 3

Was wird verschlüsselt?

- Text
- Anhänge Format-Empfehlung: `PGP/MIME` nicht: `Inline PGP`

Was wird nicht Verschlüsselt?

- Metadaten
  - Absender*in, Empfänger*in, **Betreff!**, ...

Umsetzung:

- Enigmail (GPG-Plugin für Thunderbird)
- Mailvelope (GPG-Plugin für Firefox / Chrome → Webmail)

# Hintergrundwissen 4

Schutzziele sicherer Kommunikation:

- Vertraulichkeit $\rightarrow$ Verschlüsselung
- Integrität (keine Veränderung)
- Anonymität

# Hintergrundwissen 4

Schutzziele sicherer Kommunikation:

- ☑ Vertraulichkeit $\rightarrow$ Verschlüsselung
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität

# Hintergrundwissen 4

Schutzziele sicherer Kommunikation:

- ☑ Vertraulichkeit $\rightarrow$ Verschlüsselung
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität

Integrität durch Signieren

- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

$\Rightarrow$ Man muss dem öffentlichen Schlüssel vertrauen

# Hintergrundwissen 4

Schutzziele sicherer Kommunikation:

- ☑ Vertraulichkeit → Verschlüsselung
- ☐ Integrität (keine Veränderung)
- ☐ Anonymität

Integrität durch Signieren

- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

⇒ Man muss dem öffentlichen Schlüssel vertrauen

- Schlüssel signieren bei persönlichem Treffen → „Web of trust“
- Fingerabdruck-Bsp: `214E 4E9D B193 6AF2 CFDC 68DF 13AD 3604 9D3E F6BF`

# Hintergrundwissen 4

Schutzziele sicherer Kommunikation:

- ☑ Vertraulichkeit → Verschlüsselung
- ☑ Integrität (keine Veränderung)
- ☐ Anonymität

Integrität durch Signieren

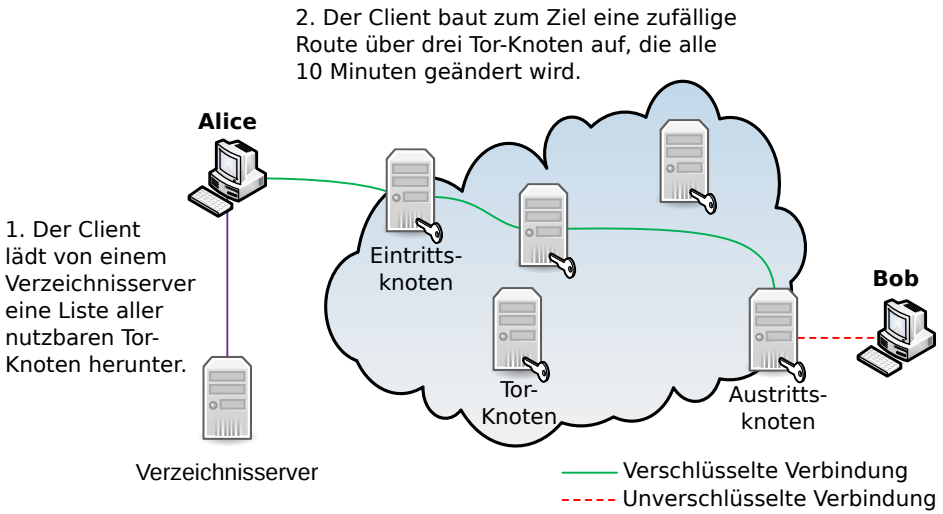
- Prinzip: mit PS verschlüsselte Prüfsumme der Nachricht
- Überprüfen = Entschlüsseln mit ÖS

⇒ Man muss dem öffentlichen Schlüssel vertrauen

- Schlüssel signieren bei persönlichem Treffen → „Web of trust“
- Fingerabdruck-Bsp: `214E 4E9D B193 6AF2 CFDC 68DF 13AD 3604 9D3E F6BF`

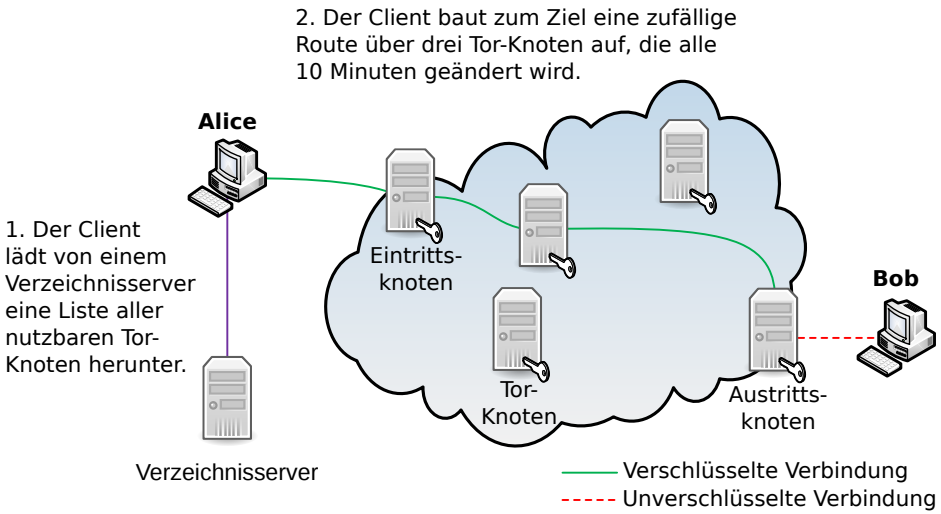
# Hintergrundwissen 5

- Anonymität mittels Tor (Ehem. **T**he **O**nion **R**outer)



# Hintergrundwissen 5

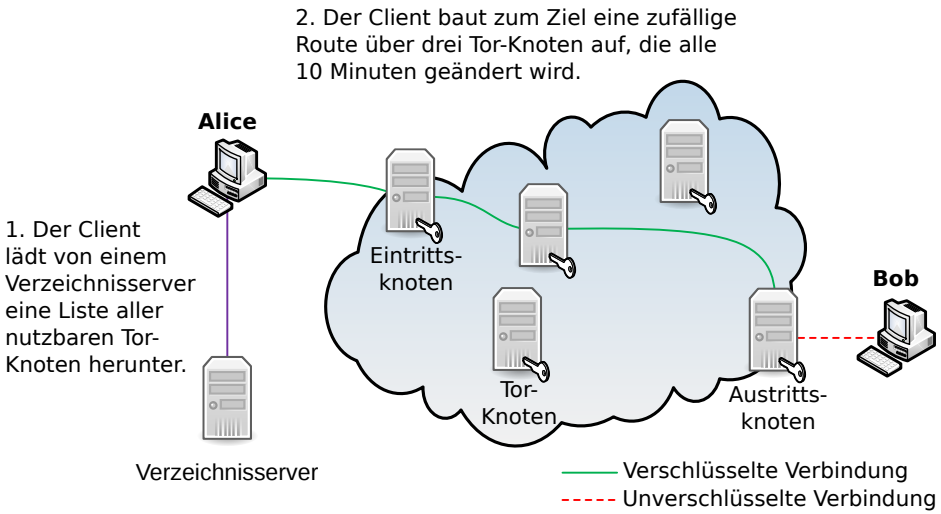
- Anonymität mittels Tor (Ehem. **T**he **O**nion **R**outer)




- https://www.torproject.org/projects/torbrowser.html
- Nachteile: Geschwindigkeit

# Hintergrundwissen 5

☑ Anonymität mittels Tor (Ehem. **T**he **O**nion **R**outer)




- https://www.torproject.org/projects/torbrowser.html
- Nachteile: Geschwindigkeit

# Begriffe

- asymmetrisches Verfahren
- Privater Schlüssel
- Öffentlicher Schlüssel
- Verschlüsseln
- Signieren / Signatur
- Schlüsselserver
- Web of Trust
- Widerrufszertifikat
- Cryptoparty
- Fingerabdruck
- Metadaten
- GPG vs PGP vs S/MIME
- Enigmail vs Mailvelope

„Paranoia und Resignation sollte man denen überlassen, die sich damit [IT-Sicherheit] auskennen.“

# Links

PGP-Verschlüsselung in Thunderbird (Plugin „Enigmail“)

- https://fsfw-dresden.de/gpg

PGP-Verschlüsselung für Webmail

- https://vimeo.com/178702500 (Screencast)
- Anleitung von Posteo

Allgemeine Infos

- https://virtual-privacy.org/

Cryptopartys

- https://www.cryptoparty.in/; | https://de.wikipedia.org/wiki/CryptoParty

Videos

- G. Greenwald: *Why privacy matters* | J. Oliver + E. Snwoden (lustig)

# Und jetzt?

- Fragen?

- Unterstützung jetzt bei Installation
  - Enigmail (Plugin für Thunderbird)
  - Mailvelope (Browserplugin für Webmail)
  - ⚠ Zeit?

# Und jetzt?

- Fragen?

- Unterstützung jetzt bei Installation
  - Enigmail (Plugin für Thunderbird)
  - Mailvelope (Browserplugin für Webmail)
  - ⚠ Zeit?

- Unterstützung später (im Rahmen unserer Möglichkeiten):
  - `https://fsfw-dresden.de/gpg` (diese Vortragsfolien)
  - `https://fsfw-dresden.de/sprechstunde`
  - `kontakt@fsfw-dresden.de`

# Und jetzt?

- Fragen?

- Unterstützung jetzt bei Installation
  - Enigmail (Plugin für Thunderbird)
  - Mailvelope (Browserplugin für Webmail)
  - ⚠ Zeit?

- Unterstützung später (im Rahmen unserer Möglichkeiten):
  - `https://fsfw-dresden.de/gpg` (diese Vortragsfolien)
  - `https://fsfw-dresden.de/sprechstunde`
  - `kontakt@fsfw-dresden.de`

- Verschlüsselung regelmäßig nutzen, Erfahrung sammeln
- Selber aktiv werden „Wer, wenn nicht wir? Wann, wenn nicht jetzt?“