Cryptoparty
u23 2015

Florob

Chaos Computer Club Cologne e.V.
https://koeln.ccc.de

Cologne
2015-10-04

Regeln

- keine Wörter
- Sonderzeichen
- angemessene Länge (Moore’s Law 😒)
- anderes Passwort pro Anwendung
- Passwort-Manager verwenden
- z. B. KeePass (`http://keepass.info`)

- Software zum verschlüsseln/signieren von Daten (insb. E-Mails)
- PGP (1991) von Phil Zimmermann
- OpenPGP (1998) IETF-standartisierte Variante von PGP 5
- GnuPG (1999) freie Implementation von OpenPGP

Schlüssel

Ein OpenPGP Schlüssel besteht aus (mindestens) 2 Teilen:

1. Verschlüsselungs Schlüsselpaar
2. Signatur Schlüsselpaar

	Private Key	**Public Key**
Encryption Pair	Entschlüsseln	Verschlüsseln
Signature Pair	Signieren	Verifizieren

Schlüssel

```
pub   rsa4096/64BD2C9E 2014-02-01 [verfällt: 2016-02-01]
  Schl.-Fingerabdruck = 9B59 97A7 D96A 07AD 1881
                        1C83 97A1 6A80 64BD 2C9E
uid        [  ultimativ] Florian Zeitz <florob@babelmonkeys.de>
sub   rsa4096/76ADA3AD 2014-02-01 [verfällt: 2016-02-01]
```

Keyserver

- öffentliche Schlüssel werden über Keyserver verteilt
- veröffentliche Schlüssel können nicht gelöscht werden
- jeder kann Schlüssel mit beliebigen Daten hochladen

⇒ Verifizierung nötig

Web of Trust

- Nutzer signieren von ihnen geprüfte Schlüssel
- Echtheit von Schlüsseln durch ein verteiltes Netz verifizieren
- Vertrauen etabliert über Pfade im Netz
- “Jeder kennt jeden über 5 Ecken”

Schlüssel verifizieren

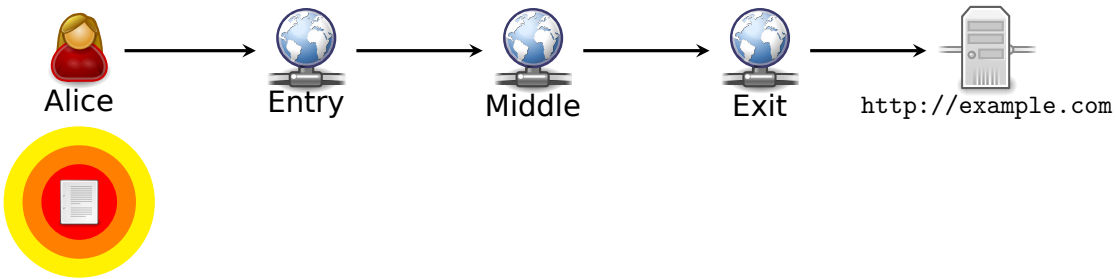
1. Personennamen prüfen (Ausweis)
2. Fingerprint vergleichen
3. Schlüssel signieren

- Windows: `http://gpg4win.org/`
- MacOS X: `https://gpgtools.org/`
- Thunderbird (`https://www.mozilla.org/de/thunderbird/`) + Enigmail

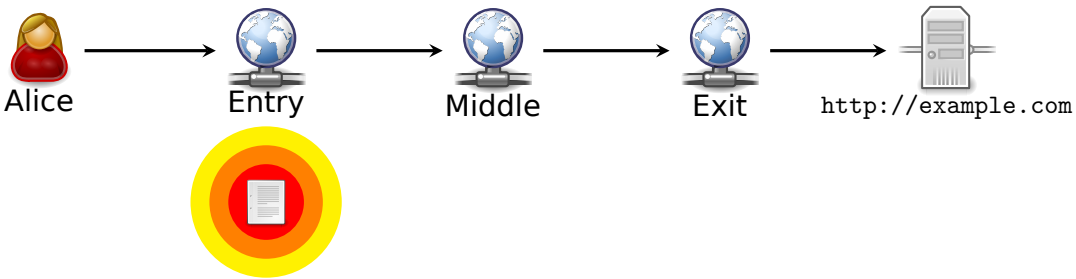
Florob <florob@babelmonkeys.de>

- `https://www.torproject.org/`
- Anonymisierung
- Umgehen von Zensurmaßnahmen

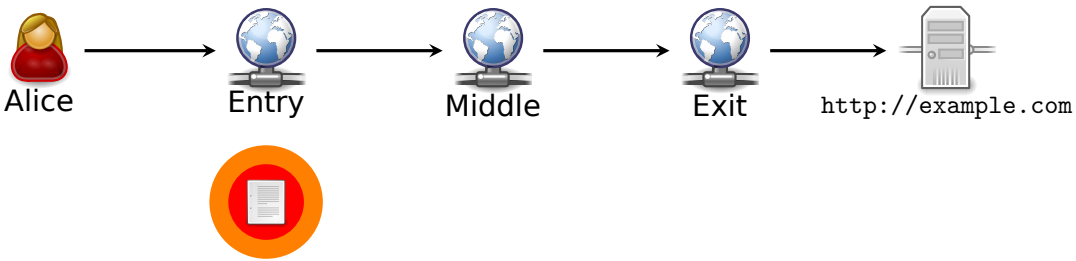
Onion Routing



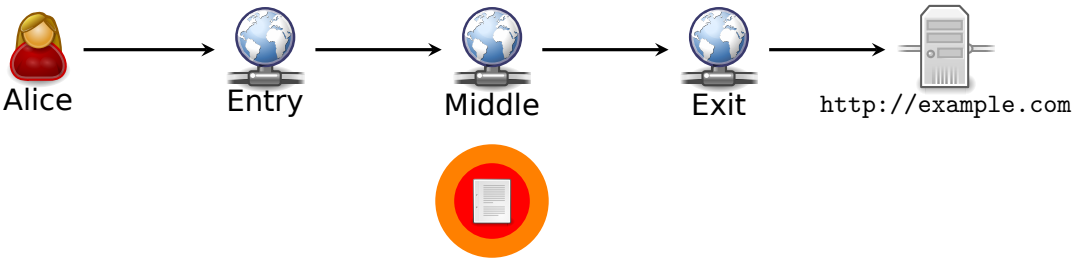
Onion Routing



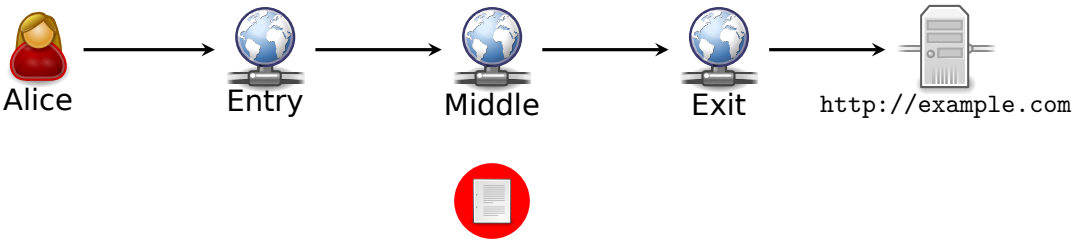
Onion Routing



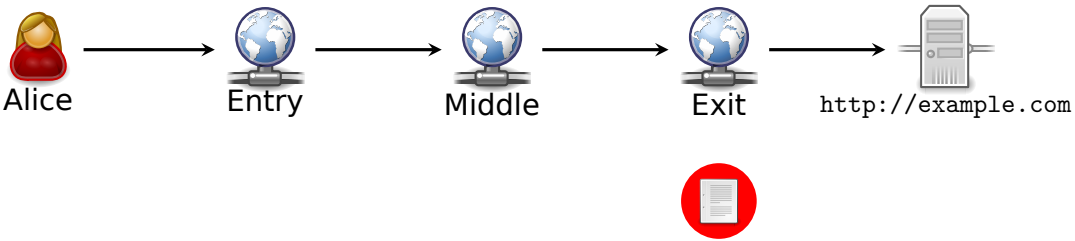
Onion Routing



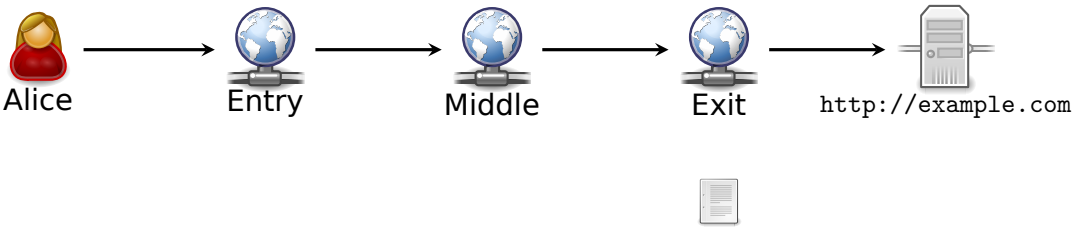
Onion Routing



Onion Routing



Onion Routing



Onion Routing

Onion Routing

Schwachstellen

- aktiver Inhalt
- Browser-Fingerprinting
- Nutzer

Anonymität durch Proxy-IP

- `https://panopticlick.eff.org/`
- die meisten Browser sind eindeutig Erkennbar
- Vergleich mit Tor Browser
- `https://www.torproject.org/`

Florob <florob@babelmonkeys.de>

OTR

- Off-the-Record Messaging
- sicheres Instant Messaging
- entworfen um mit beliebigen IM Protokollen zu funktionieren
- Überprfen des öffentlichen Schlüssels wie bei OpenPGP nötig

(Perfect) Forward Secrecy

- Das ermitteln eines langlebigen Schlüssels kompromittiert nicht alle bisherigen Gespräche
- Sitzungs-/Nachrichtenschlüssel berechnen sich nicht sofort aus dem private Key
- Schlüssel werden rotiert

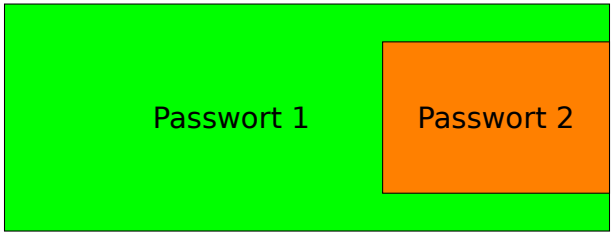
(Non-)Repudiation

- repudiation/plausible deniability: Im Nachhinein ist nicht prüfbar wer eine Nachricht erstellt hat
- für rechtliche Angelegenheiten (z. B. in Firmen) ist oft non-repudiation wünschenswert
- der Empfänger sollte trotzdem zum Zeitpunkt des Empfanges wissen wer der Absender war

- https://otr.cypherpunks.ca/
- https://pidgin.im/

- Werkzeug zur Datenträgerverschlüsselung
- physikalische Laufwerke
- virtuelle Laufwerke (Container)
- Keyfiles

Hidden Volumes



- https://veracrypt.codeplex.com/