Anonymous and secure instant messaging

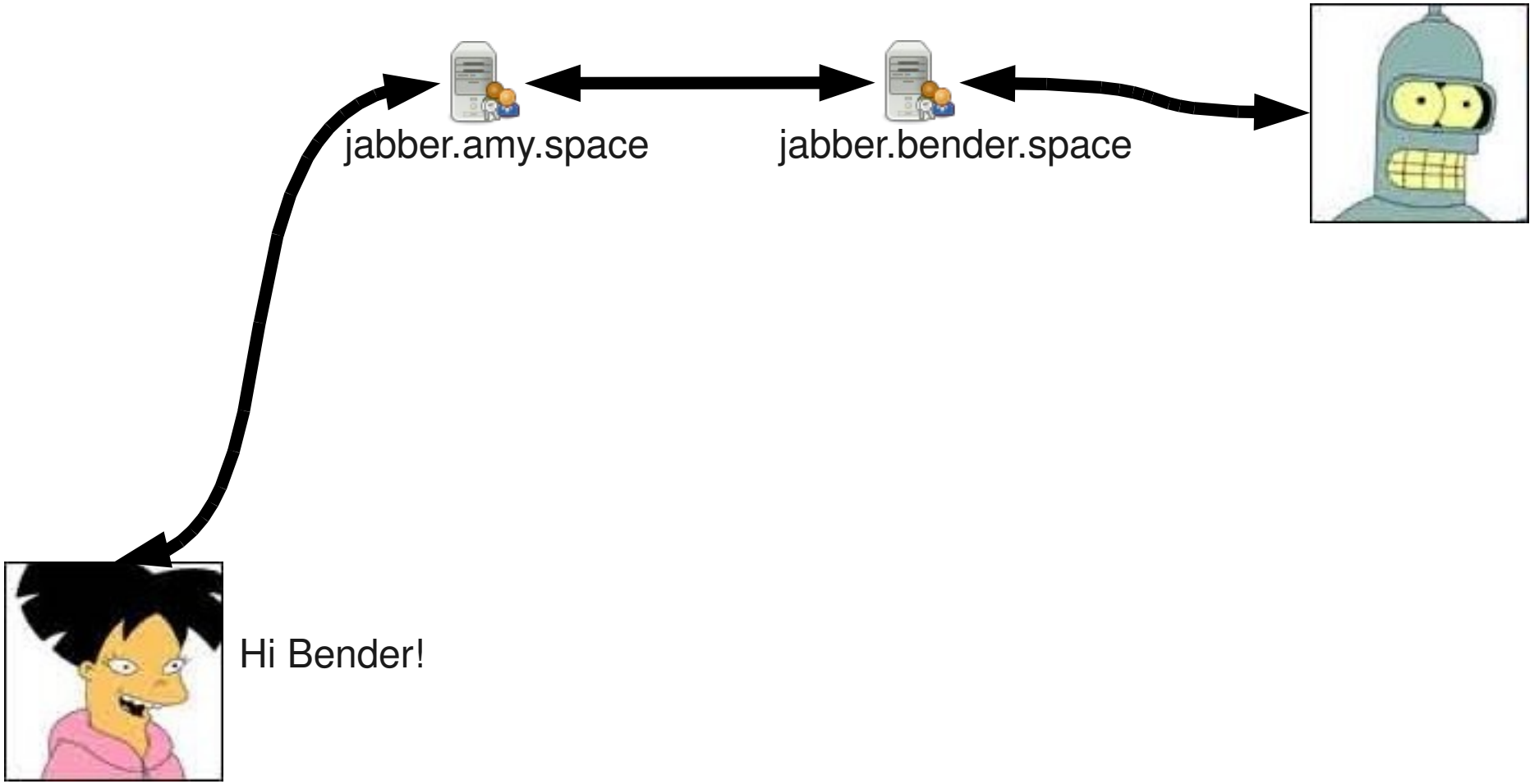
We can neither confirm nor deny the existence or the non-existence of the requested information

Hannes Mehnert; hannes@berlin.ccc.de; Datenspuren 2008

Überblick

- XMPP
- TOR
- TOR Hidden Services
- XMPP mit TOR

XMPP Kommunikation



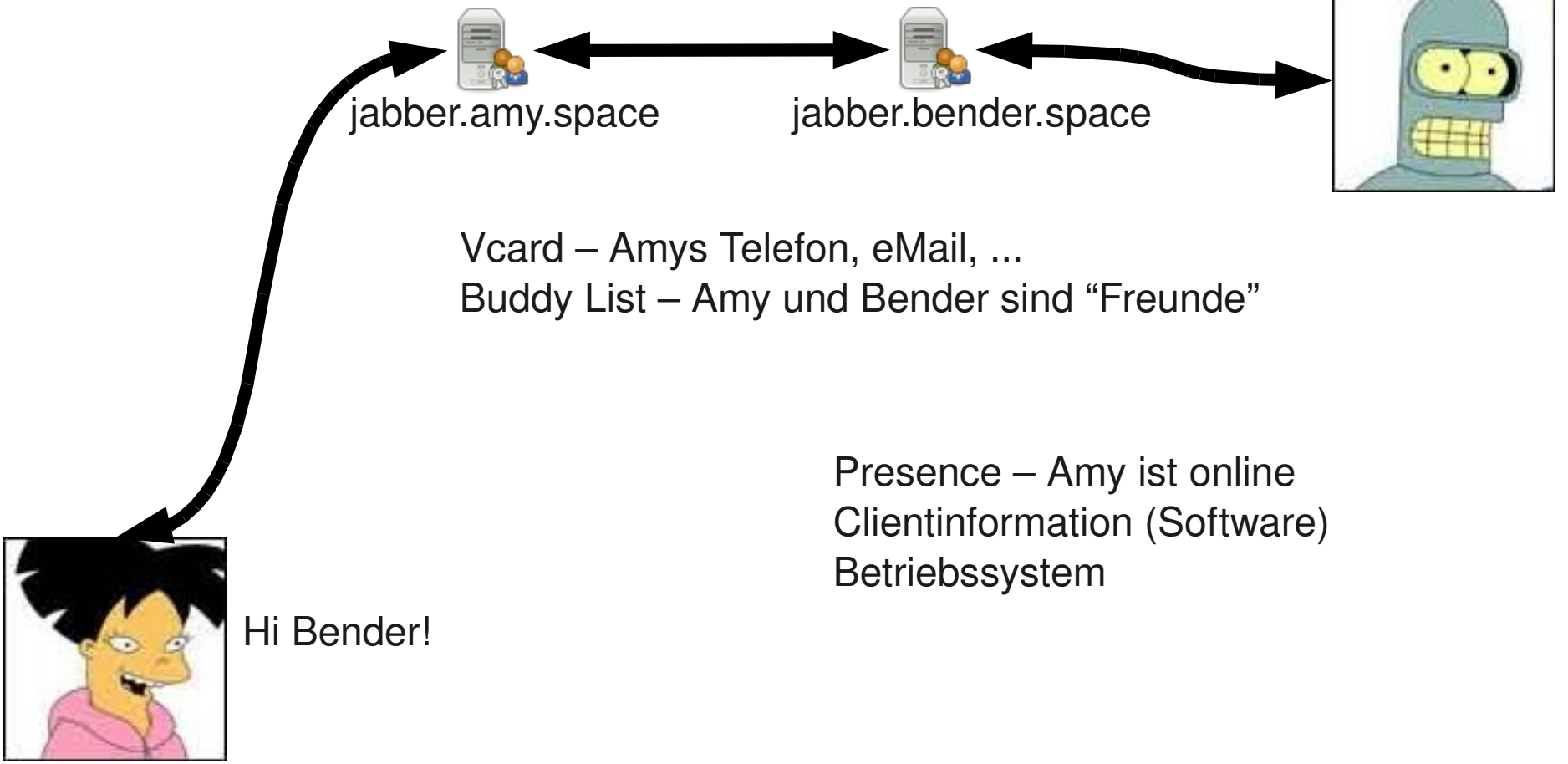
Sicherheitseigenschaften

- Vertraulichkeit – nur Amy und Bender können die Nachricht lesen
- Integrität – die Nachricht kann nicht verfälscht werden
- Authentizität – Bender weiss, dass die Nachricht von Amy kam
- Verbindlichkeit – Amy kann nicht abstreiten, dass sie die Nachricht verfasst hat

XMPP Kommunikation

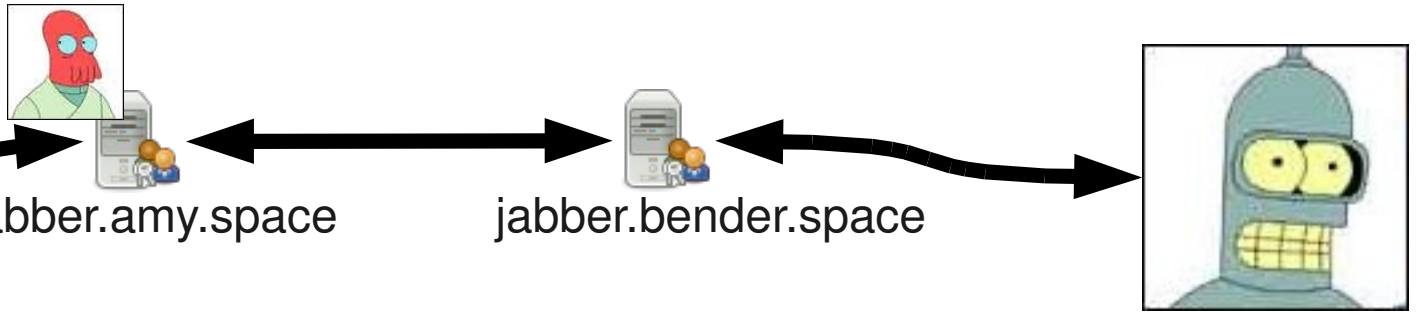
Schützenswerte Daten

- Inhalte der Nachrichten - “Hi Bender!”
- Verbindungsdaten – Amy und Bender chatten



XMPP Kommunikation

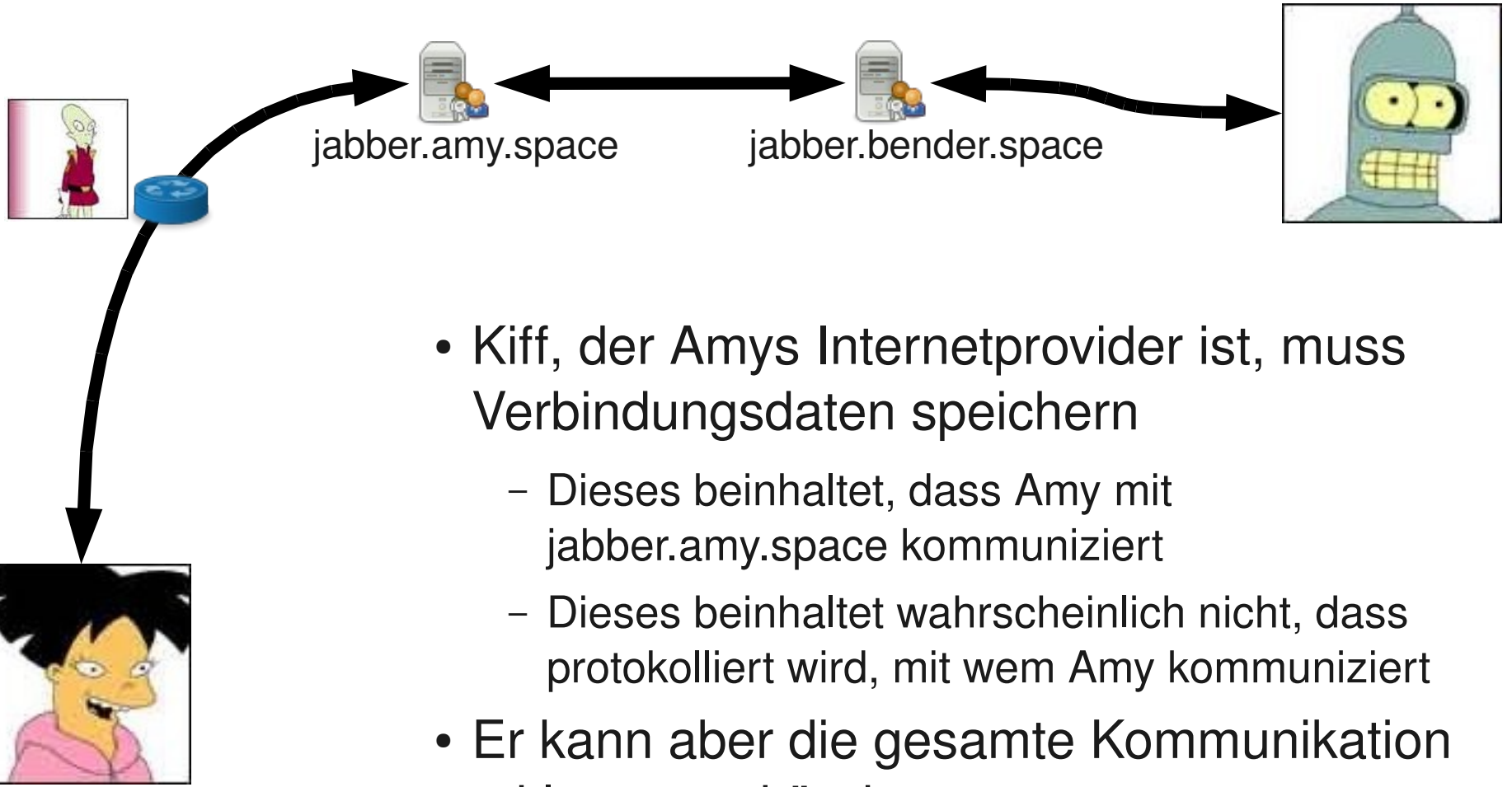
Serverbetreiber



- Zoidberg betreibt den Server von Amy
  - Zugriff auf vcard, Buddy List
  - Kommunikation mitlesen und verändern
  - Arbeitet möglicherweise mit Feinden zusammen
- Server Sicherheit
  - Betriebssystem
  - Server Software

XMPP Kommunikation

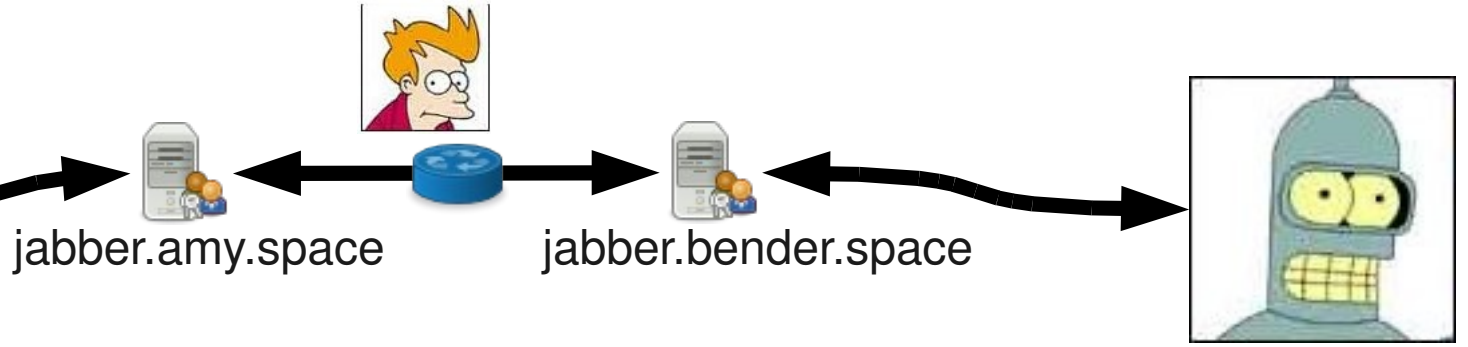
Verbindungsdaten



- Kiff, der Amys Internetprovider ist, muss Verbindungsdaten speichern
  - Dieses beinhaltet, dass Amy mit jabber.amy.space kommuniziert
  - Dieses beinhaltet wahrscheinlich nicht, dass protokolliert wird, mit wem Amy kommuniziert
- Er kann aber die gesamte Kommunikation mitlesen und ändern

XMPP Kommunikation

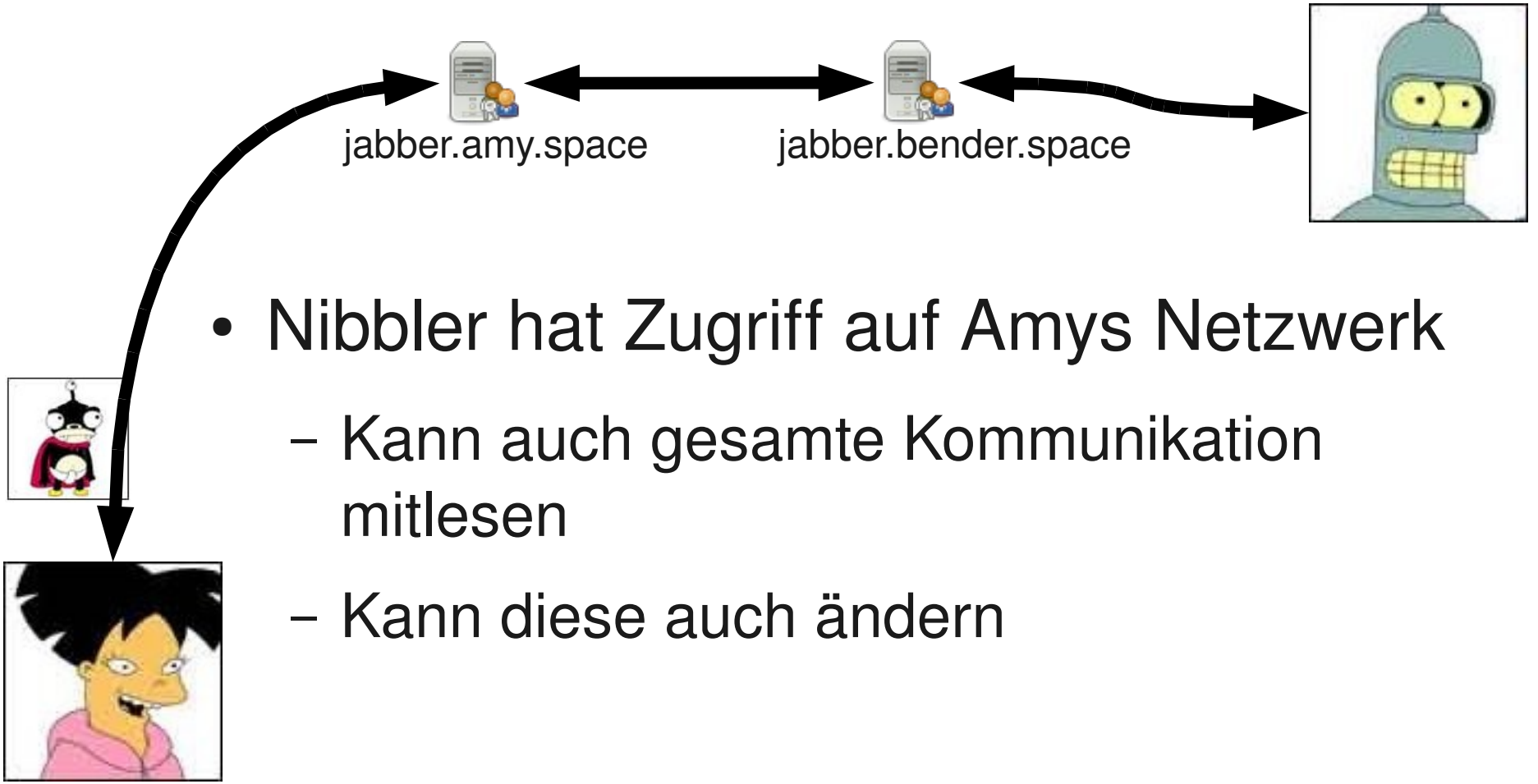
Netzwerk zwischen den Servern



- Fry hat Zugriff auf das Netzwerk zwischen den Jabber Servern
  - Somit kann er auch die Kommunikation lesen
  - Und auch verändern

XMPP Kommunikation

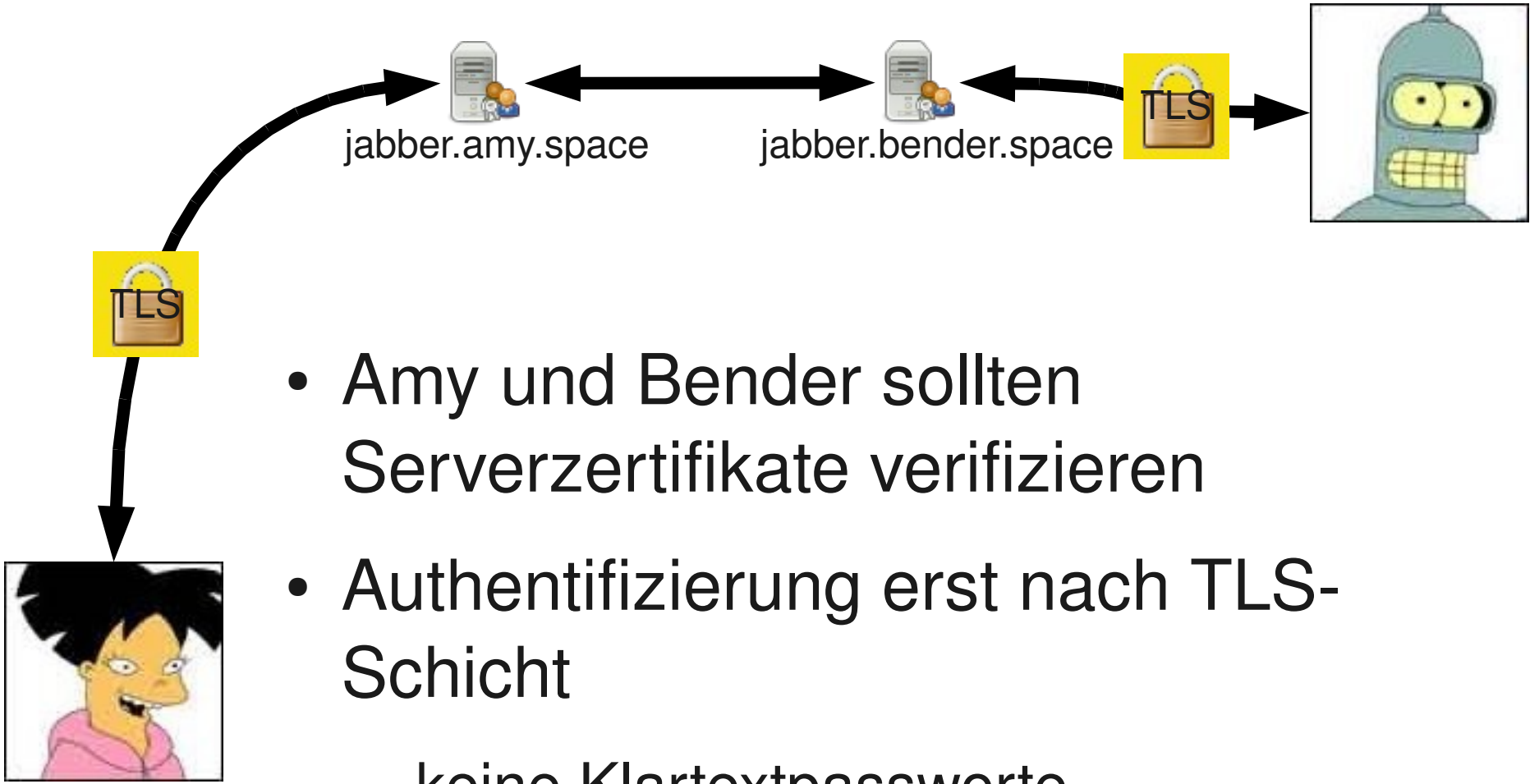
Lokaler Angreifer



- Nibbler hat Zugriff auf Amys Netzwerk
  - Kann auch gesamte Kommunikation mitlesen
  - Kann diese auch ändern

XMPP Kommunikation

Transport Layer Security – Client to Server



- Amy und Bender sollten Serverzertifikate verifizieren
- Authentifizierung erst nach TLS-Schicht
  - keine Klartextpassworte

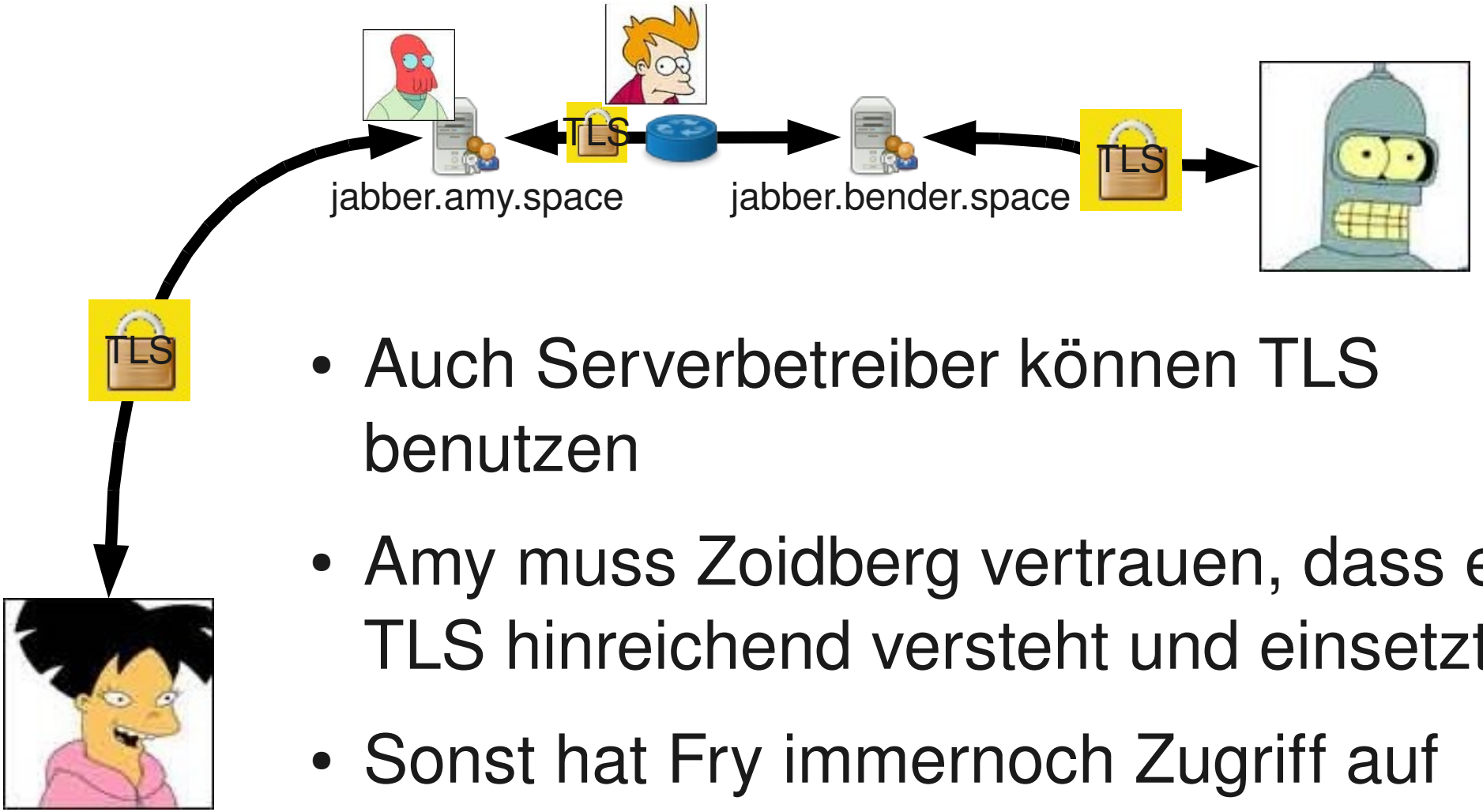
XMPP Kommunikation

Transport Layer Security – Angreifer bei Client to Server

- Zoidberg kann weiterhin Nachrichten lesen
- Nibbler und Kiff
  - Kommunikation von Amy zu jabber.amy.space findet statt
  - Aktiv: Kommunikation verhindern
    - Netzwerkangriffe
    - Man in the middle

XMPP Kommunikation

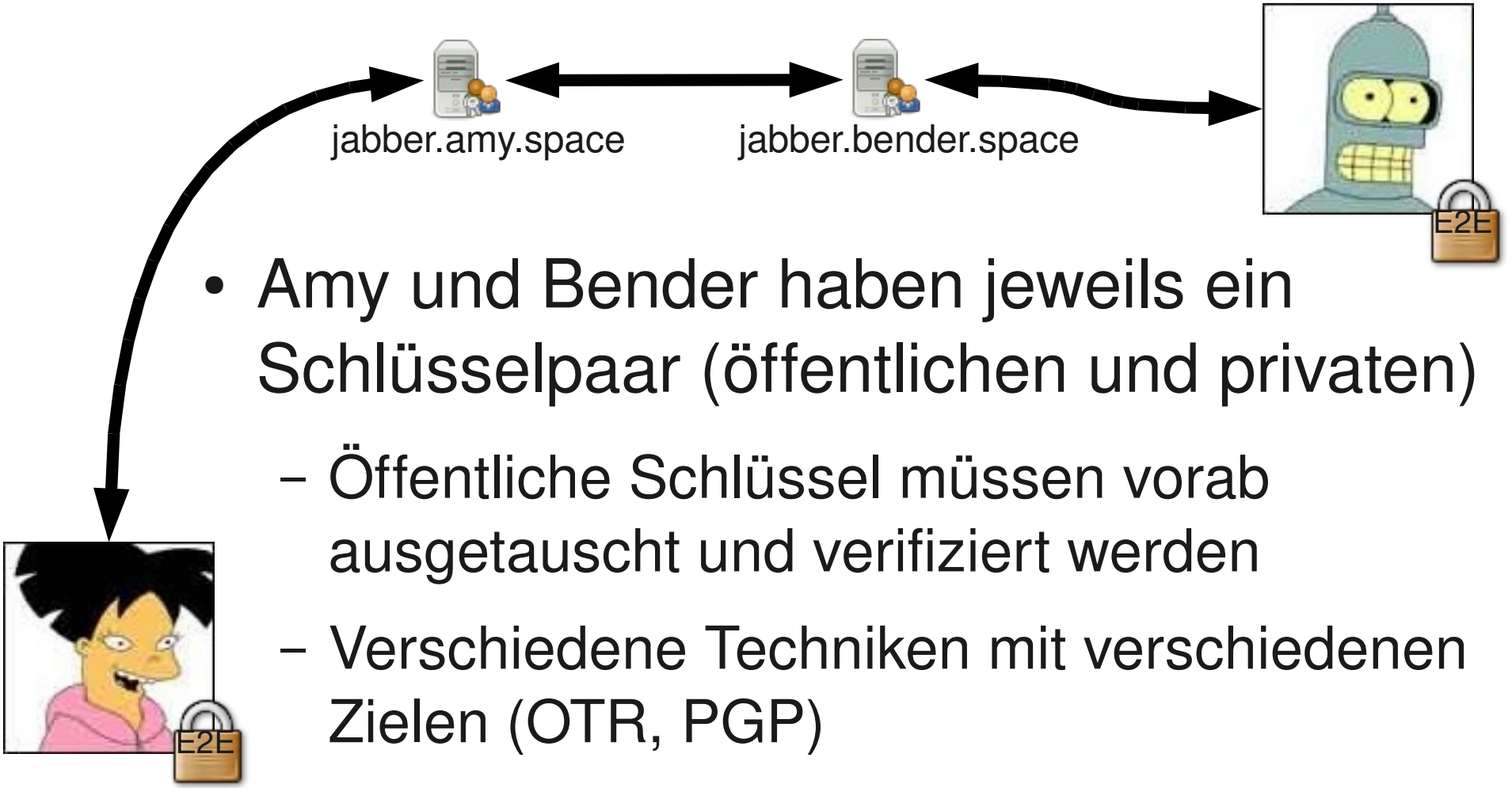
Transport Layer Security – Server to Server



- Auch Serverbetreiber können TLS benutzen
- Amy muss Zoidberg vertrauen, dass er TLS hinreichend versteht und einsetzt
- Sonst hat Fry immernoch Zugriff auf die Kommunikation

XMPP Kommunikation

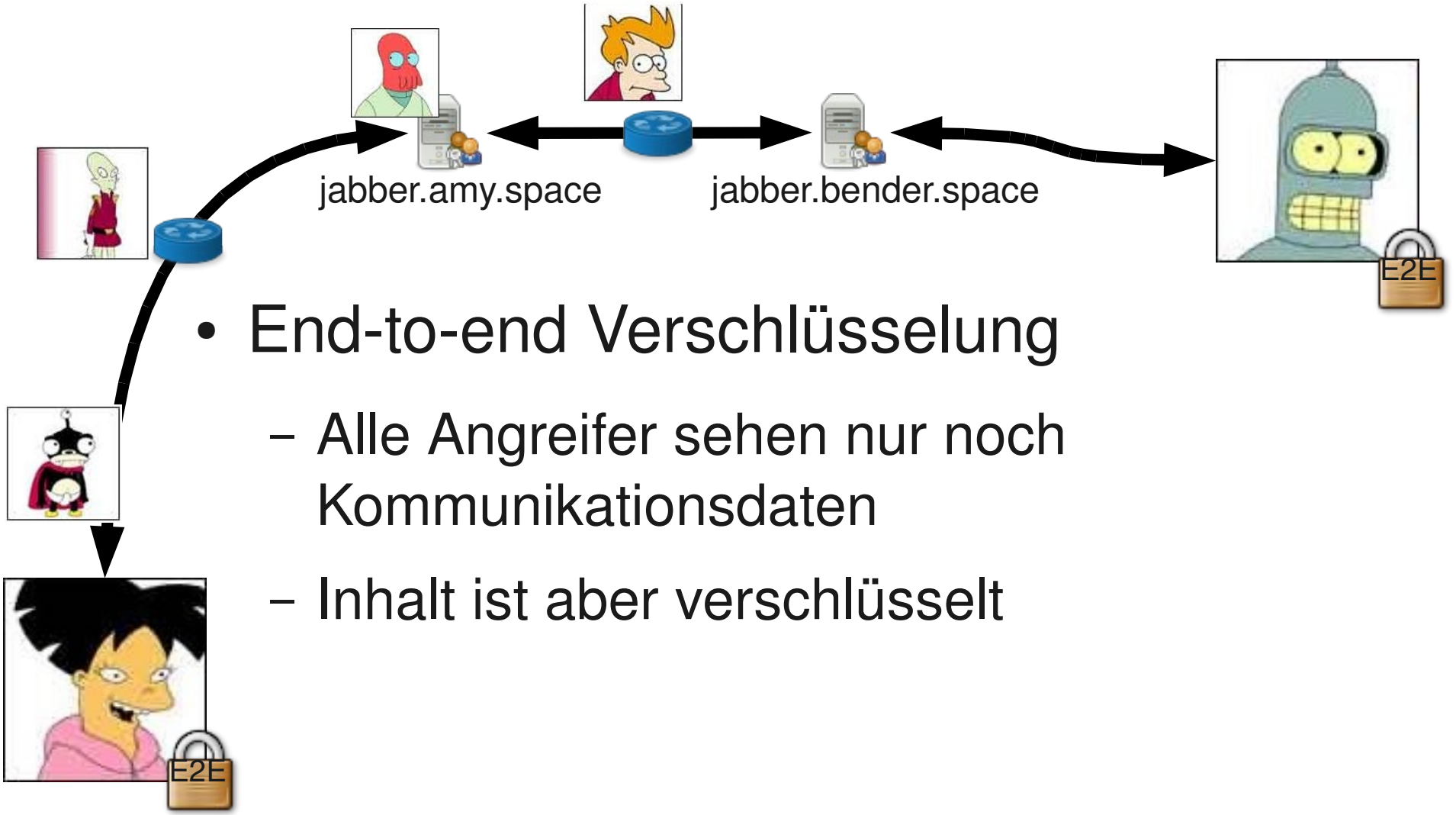
End-to-end Verschlüsselung



- Amy und Bender haben jeweils ein Schlüsselpaar (öffentlichen und privaten)
  - Öffentliche Schlüssel müssen vorab ausgetauscht und verifiziert werden
  - Verschiedene Techniken mit verschiedenen Zielen (OTR, PGP)

XMPP Kommunikation

End-to-end Verschlüsselung - Angreifer



- End-to-end Verschlüsselung
  - Alle Angreifer sehen nur noch Kommunikationsdaten
  - Inhalt ist aber verschlüsselt

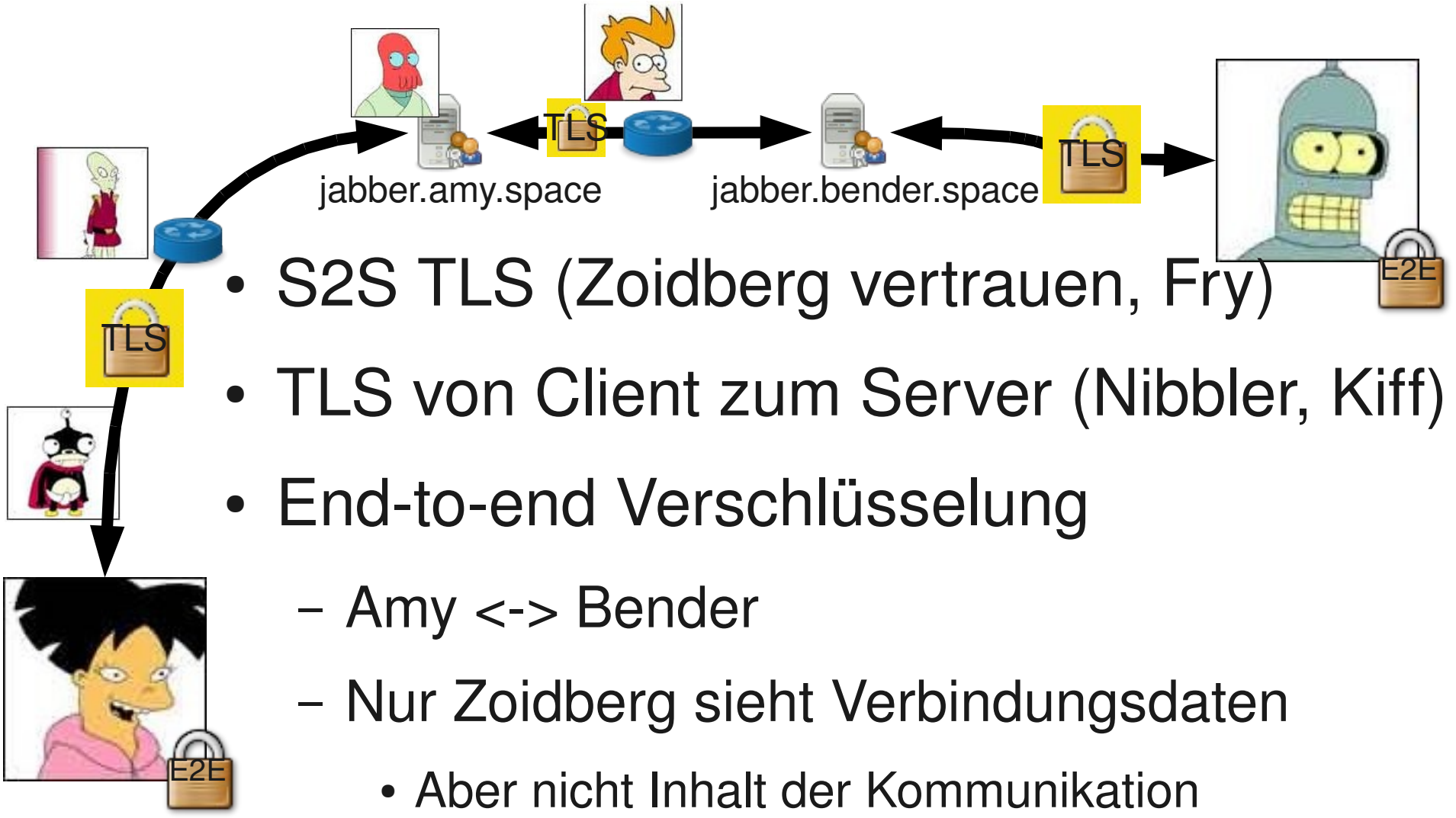
XMPP Kommunikation

End-to-end Verschlüsselung – verschiedene Techniken

- OTR
  - Perfect forward secrecy
  - Malleable encryption
  - Stateful
  - Schlüssel unverschlüsselt
  - Offline storage nur wenn session Key noch da
  - Signiert und verschlüsselt
- PGP
  - Stateless
  - Schlüssel verschlüsselt
  - Offline storage auf dem Server
  - Verschlüsselt (signiert)
  - Nachweisbar (nicht abstreitbar), dass die Nachricht zu Zeitpunkt X geschrieben wurde

XMPP Kommunikation

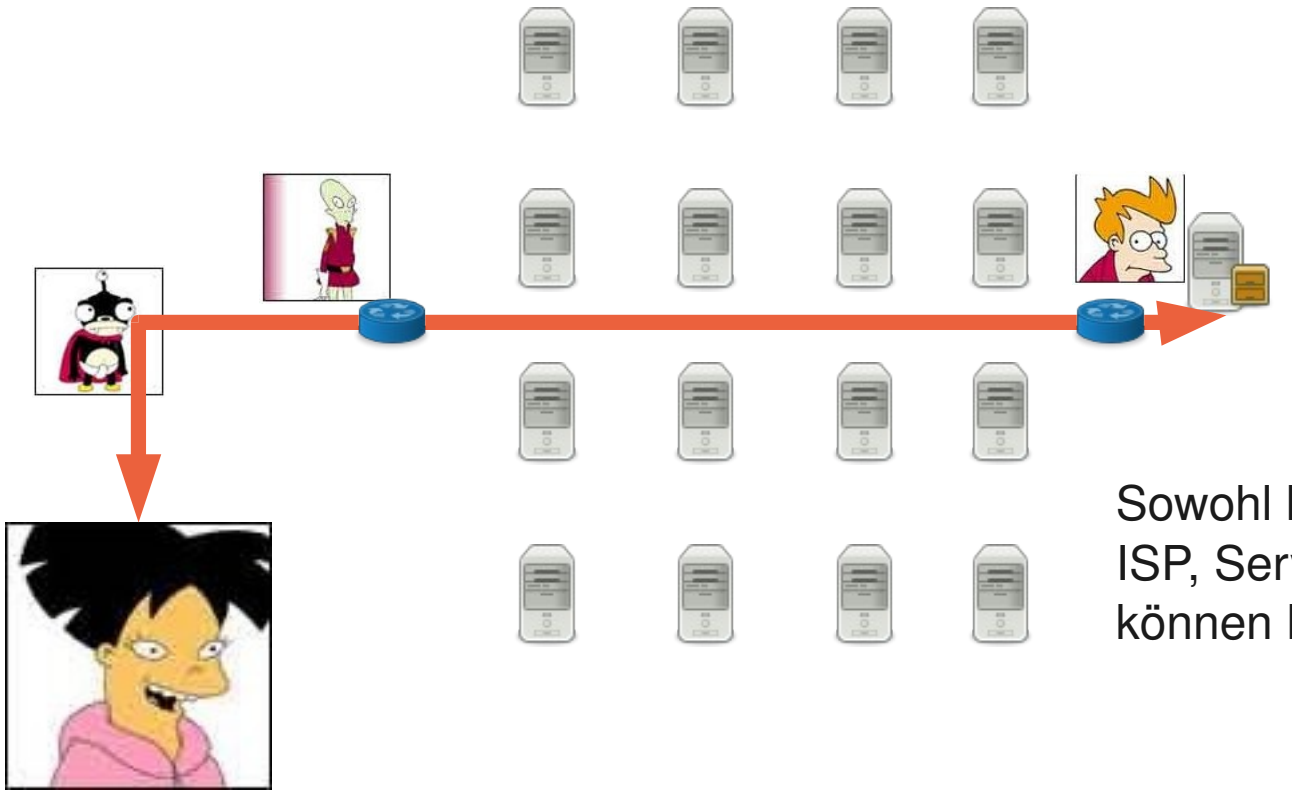
Verschlüsselungsmechanismen - Zusammenfassung



- S2S TLS (Zoidberg vertrauen, Fry)
- TLS von Client zum Server (Nibbler, Kiff)
- End-to-end Verschlüsselung
  - Amy <-> Bender
  - Nur Zoidberg sieht Verbindungsdaten
    - Aber nicht Inhalt der Kommunikation

Zugriff auf einen Rechner

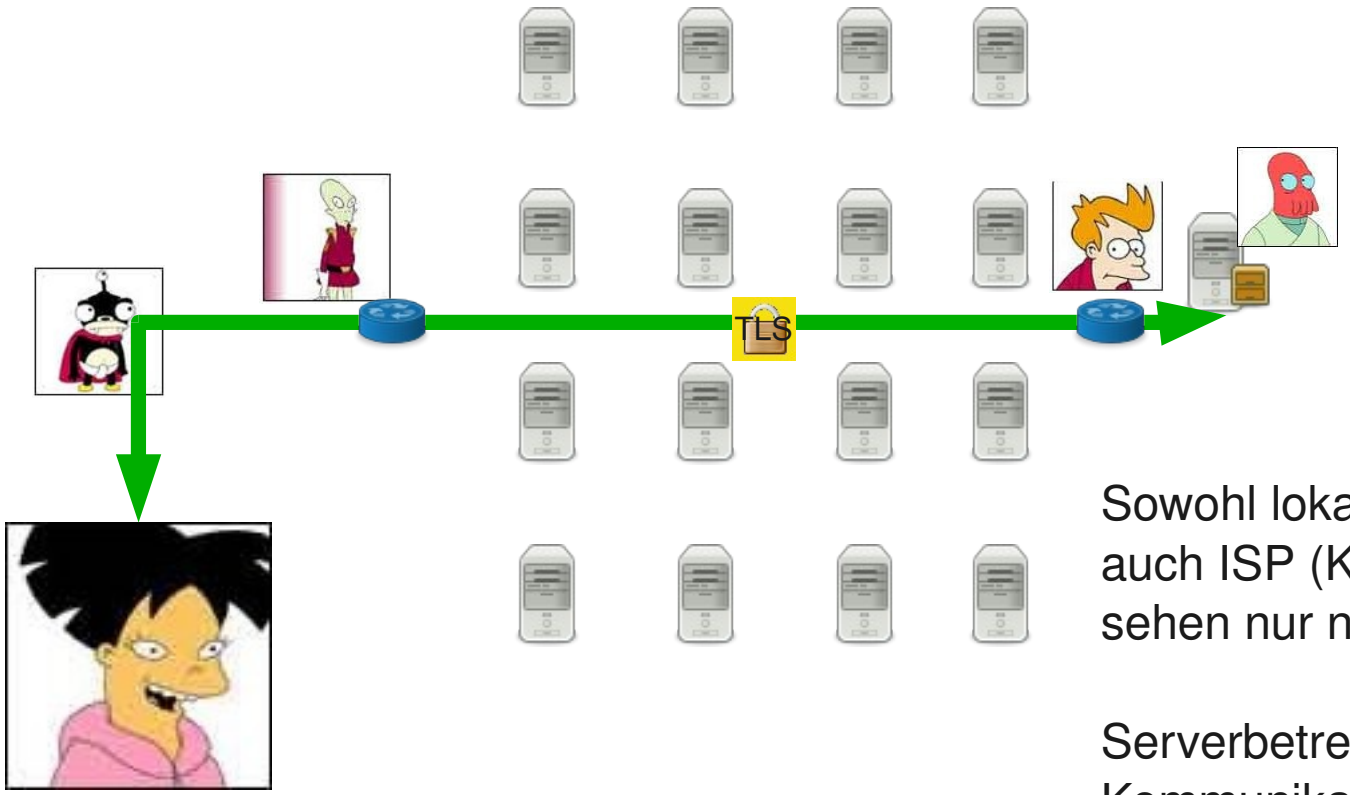
Normale Verbindung, nicht anonym und nicht verschlüsselt



Sowohl lokale Angreifer als auch ISP, Server-ISP, Serverbetreiber können Kommunikation mitlesen

Zugriff auf einen Rechner

Normale Verbindung, nicht anonym aber verschlüsselt

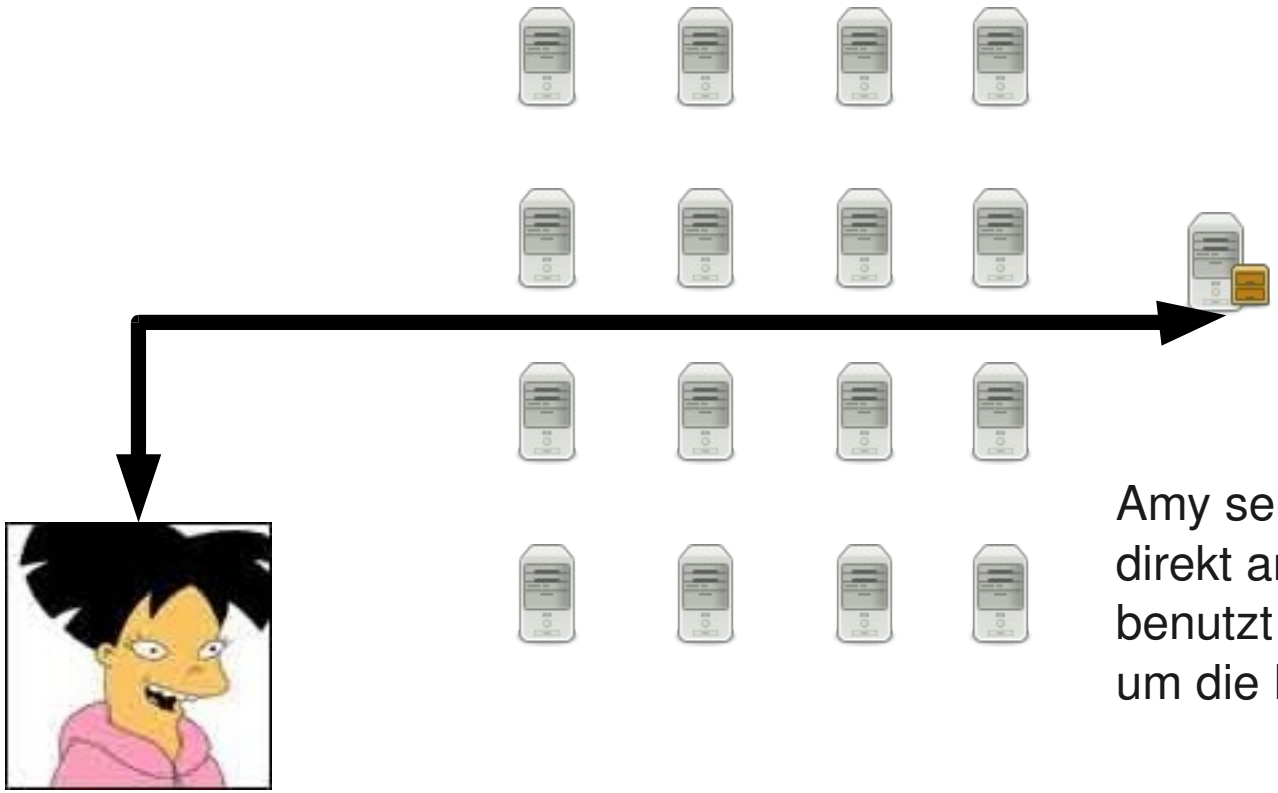


Sowohl lokale Angreifer (Nibbler) als auch ISP (Kiff) und Server-ISP (Fry) sehen nur noch Verbindungsdaten

Serverbetreiber (Zoidberg) können Kommunikation mitlesen

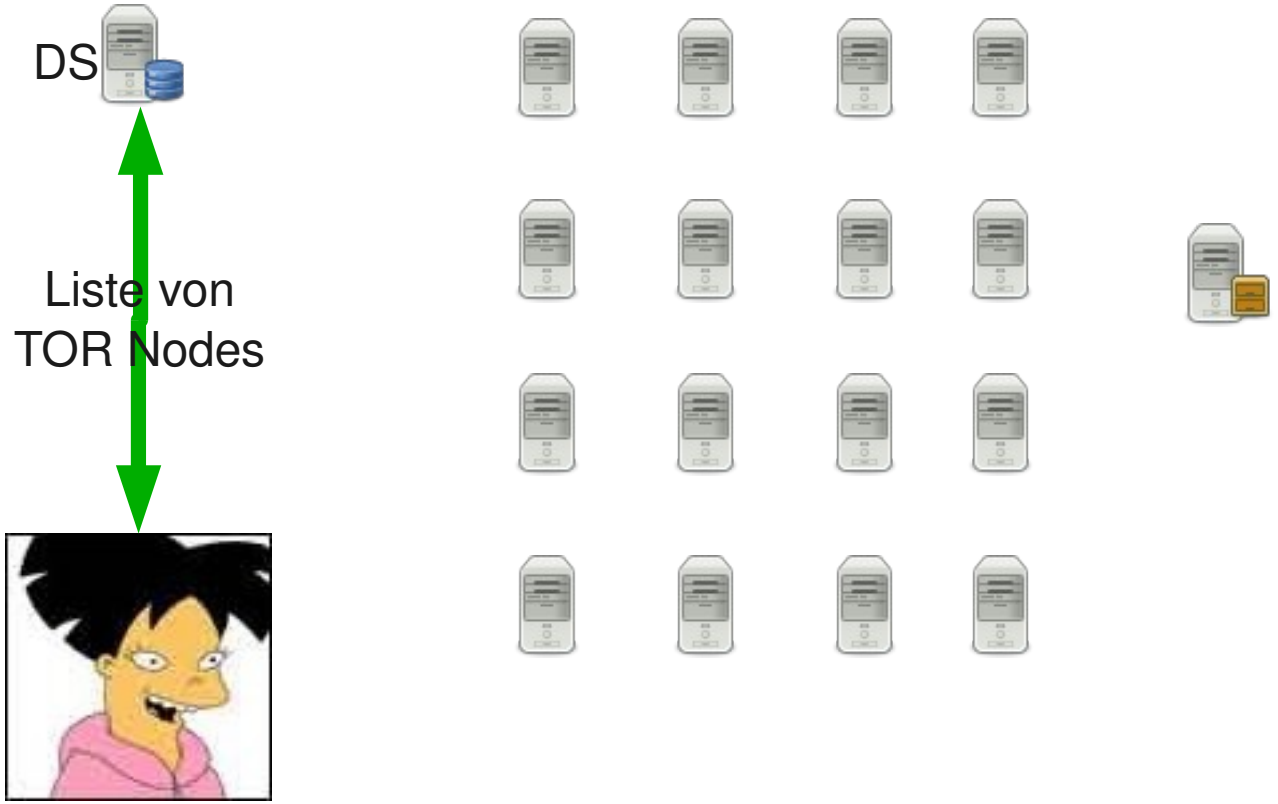
Zugriff auf einen Rechner

Ziel: Verbindung ohne Verbindungsdaten – mit Hilfe von Onion Routing

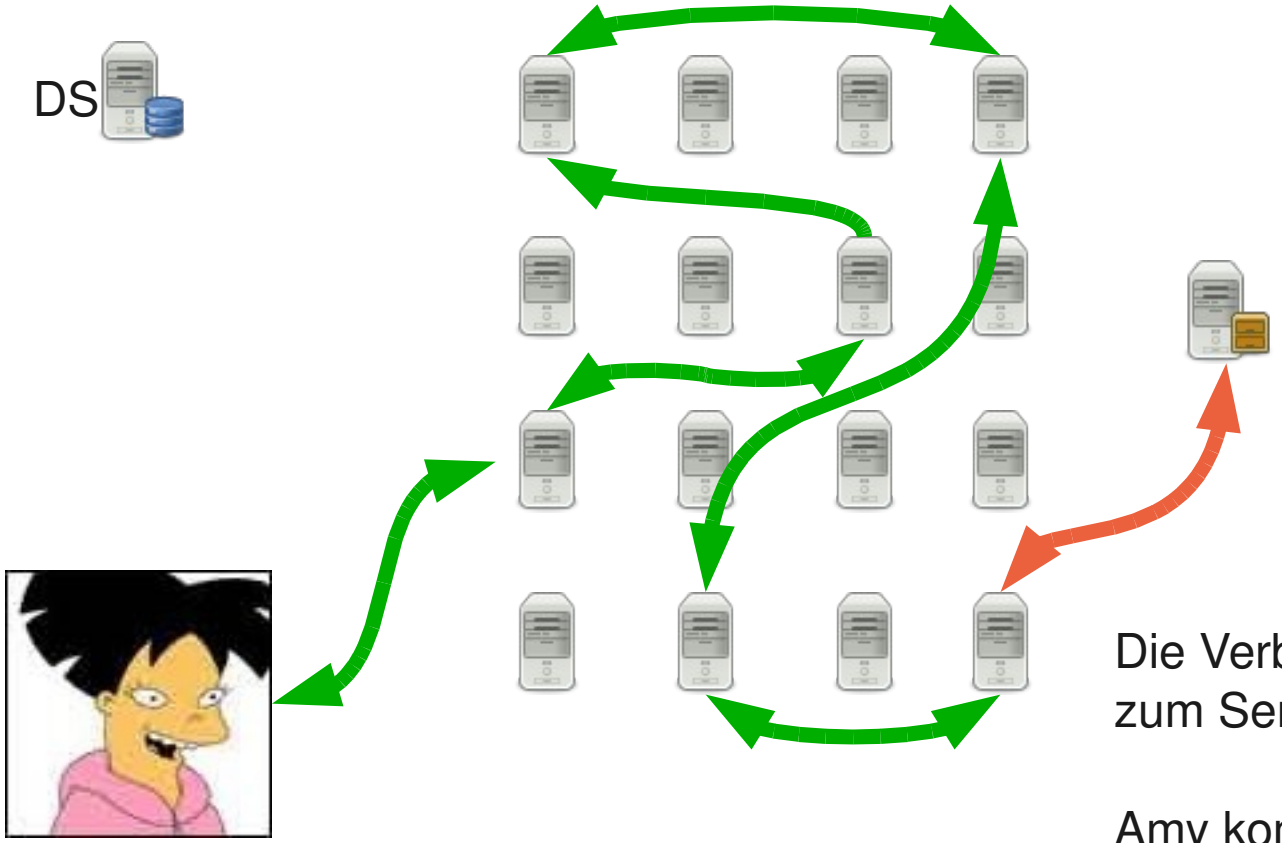


Amy sendet einfach Daten nicht direkt an den Service, sondern benutzt andere Rechner im Internet, um die Herkunft zu verschleiern

TOR – Liste anderer TOR Nodes



TOR – Zugriff auf einen Rechner



Die Verbindung vom Exit Node zum Service ist unverschlüsselt

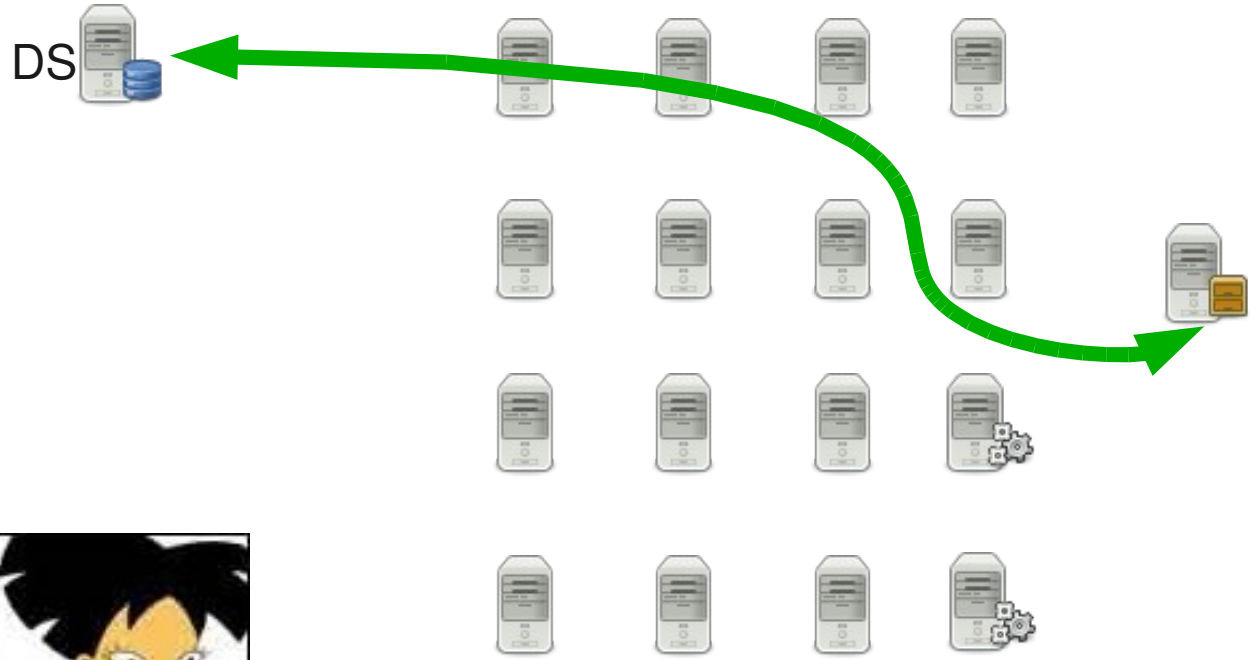
Amy kommuniziert mit dem Service
Der Service wird möglicherweise überwacht

Zugriff auf einen Hidden Service

Hidden Service selektiert Introduction Points

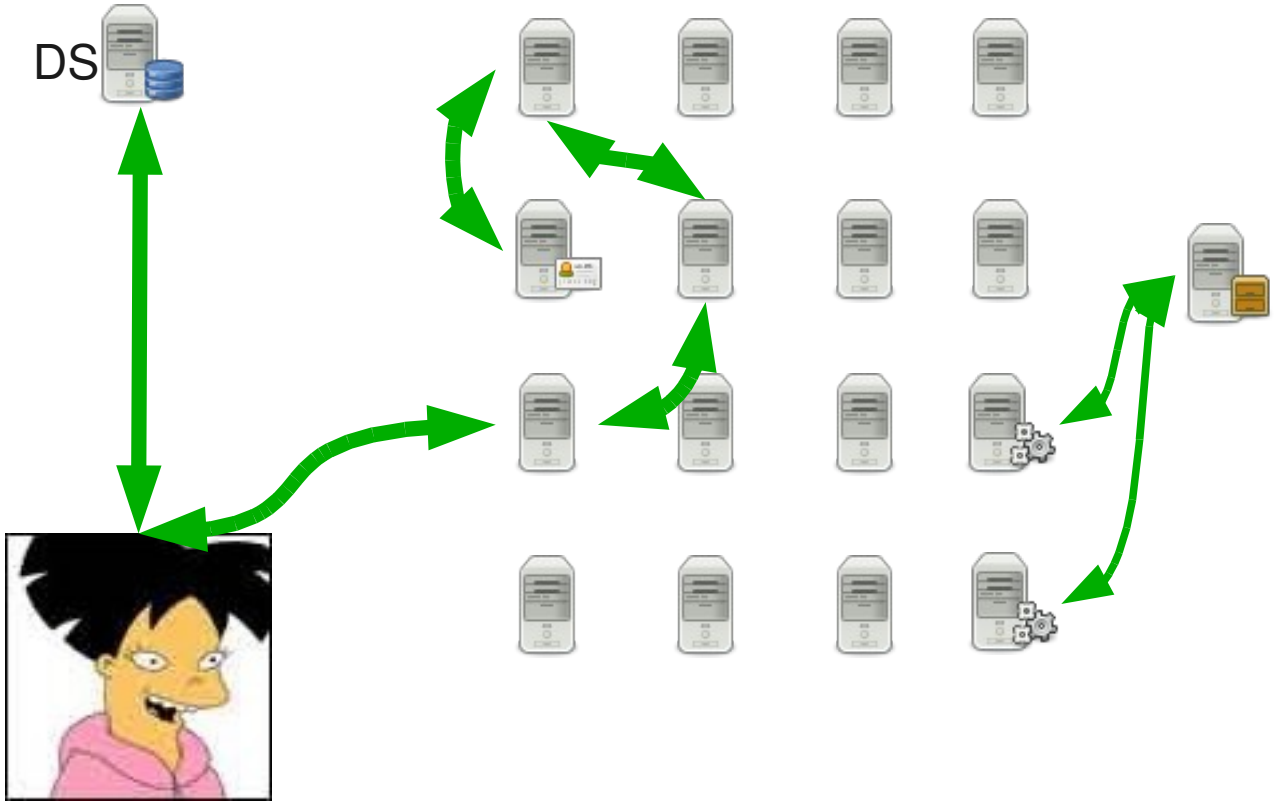
Zugriff auf einen Hidden Service

Hidden Service teilt Directory Server die Introduction Points mit



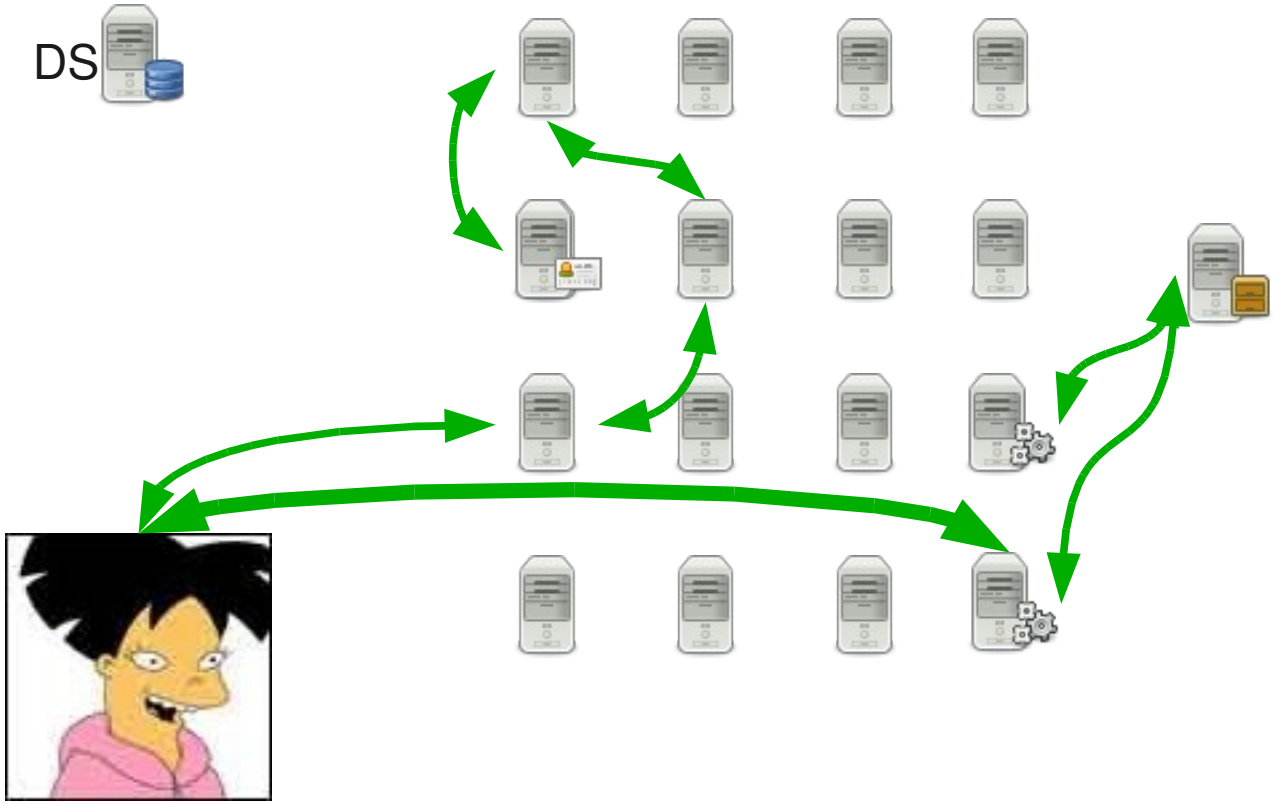
Zugriff auf einen Hidden Service

Amy fragt Directory Server nach Introduction Points vom Hidden Service
Amy wählt Rendezvous Point



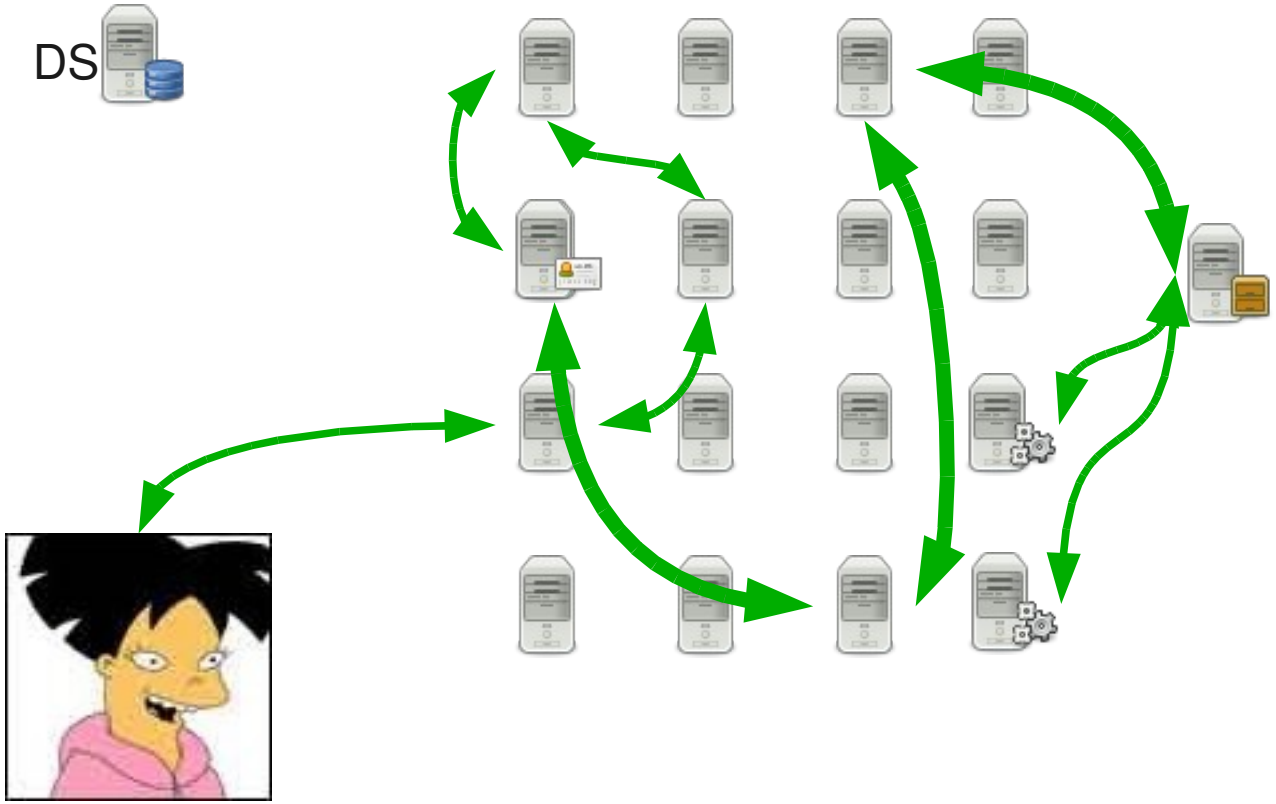
Zugriff auf einen Hidden Service

Amy teilt dem Introduction Point den gewählten Rendezvous Point mit



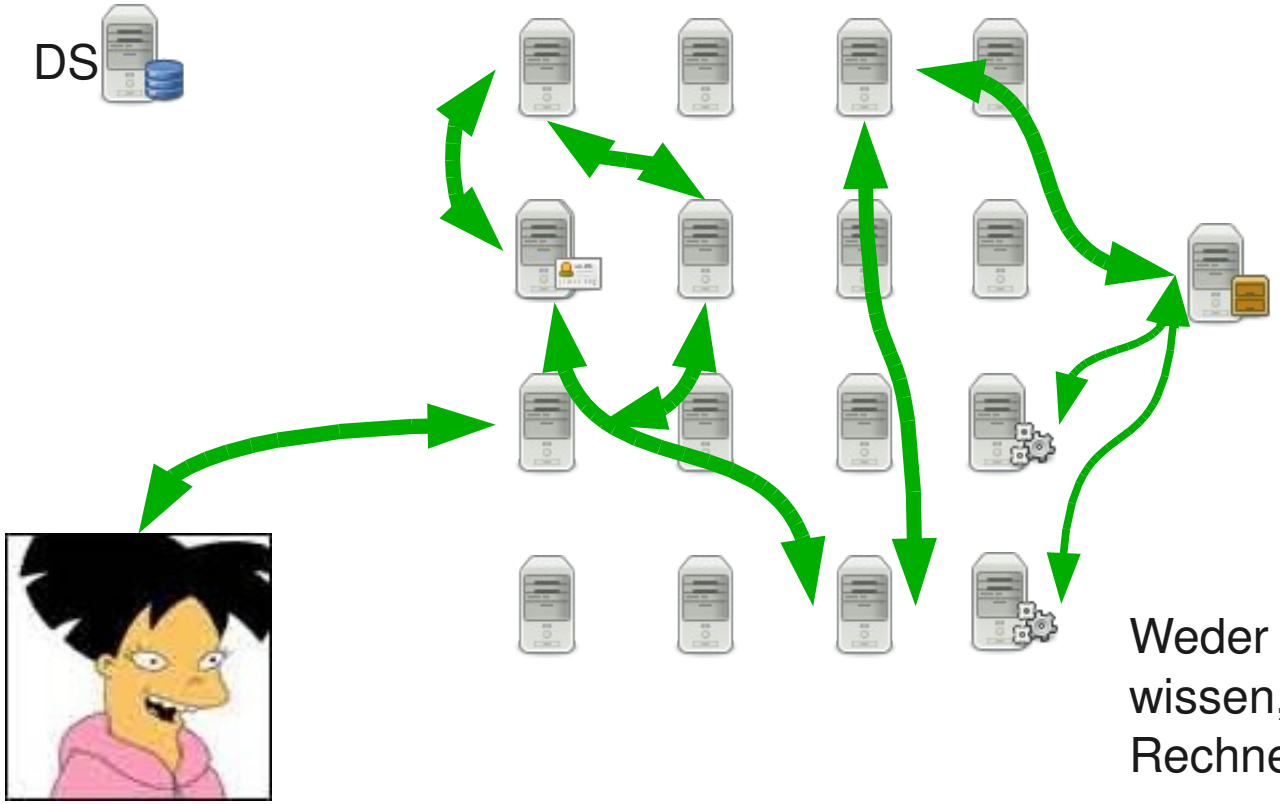
Zugriff auf einen Hidden Service

Hidden Service verbindet sich zum Rendezvous Point



Zugriff auf einen Hidden Service

Amy kann mit dem Hidden Service kommunizieren

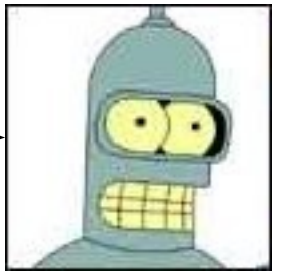


Weder Hidden Service noch Amy wissen, mit welchem realen Rechner sie kommunizieren

XMPP und TOR

ISP und lokale Angreifer sehen nur noch Verbindungen ins TOR Netzwerk

S2S Angreifer sieht immernoch Daten



jabber.bender.space

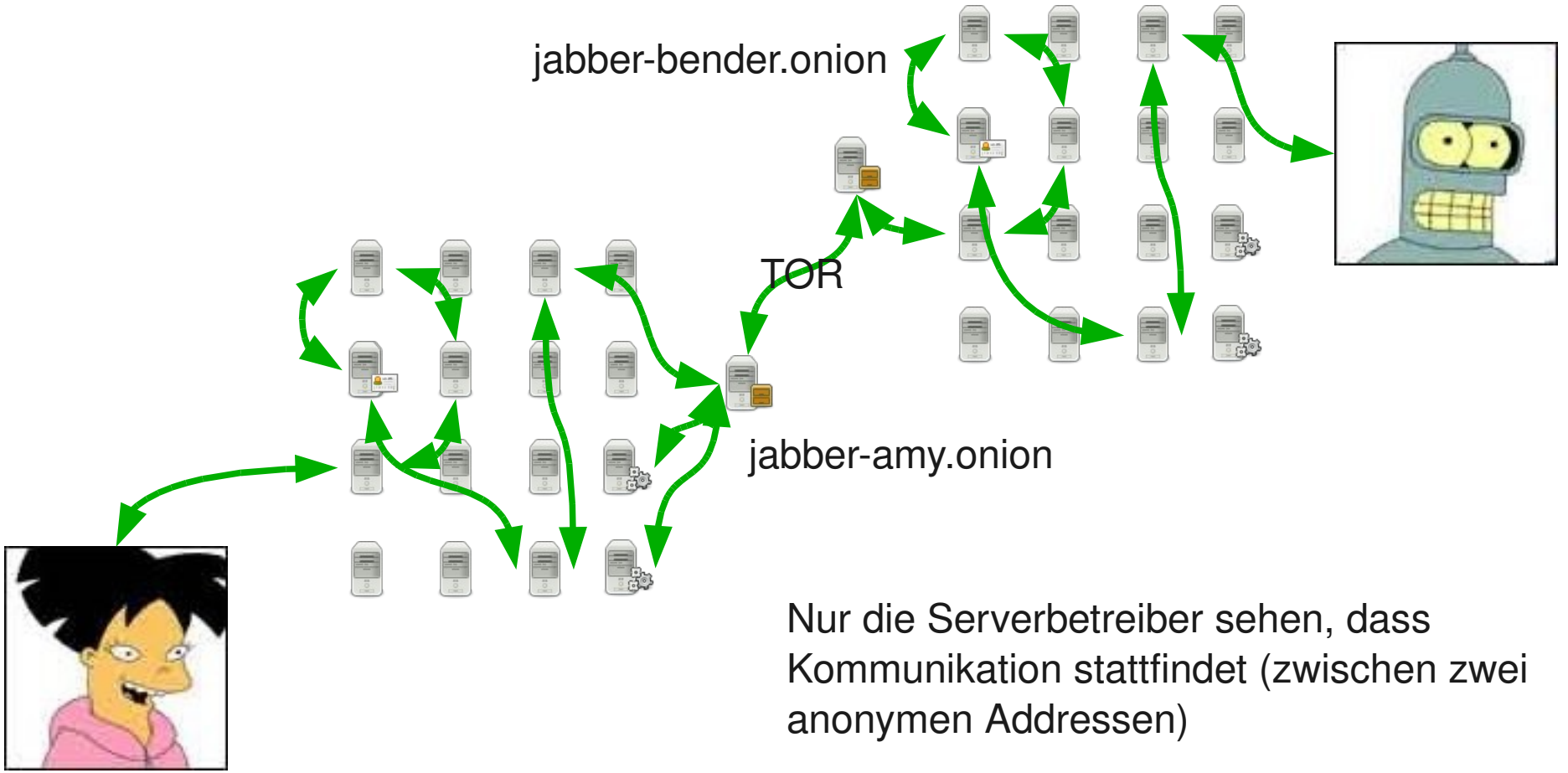
DS

..TOR Exit Node

jabber-amy.onion

Serverbetreiber sieht
(anonyme) Amy loggt sich ein
Kommunikation von Amy zu Bender
ist anonym -> keine Bedarfsträger, die Daten anfragen können

XMPP mit zwei Hidden Services



Nur die Serverbetreiber sehen, dass Kommunikation stattfindet (zwischen zwei anonymen Addressen)

Bei Verwendung von E2E kennen diese auch nur die Verbindungsdaten – und können nicht feststellen, wer sich unterhält

- Anonymes und sicheres Instant Messaging ist möglich, wenn dem Serverbetreiber vertraut wird (oder wenn ein eigener betrieben
- Vcard und Buddy List sind auf dem Server gespeichert
- Andere schützenswerte Daten (Inhalt, Verbindungsdaten, Presence) können gesichert werden
- https://berlin.ccc.de/~hannes/secure-instant-messaging.pdf
- foobar@3khgsei3bkgqvmqw.onion
- foobar@ww7pd547vjnlhdmg.onion

Fragen?