Karlsruher Institut für Technologie

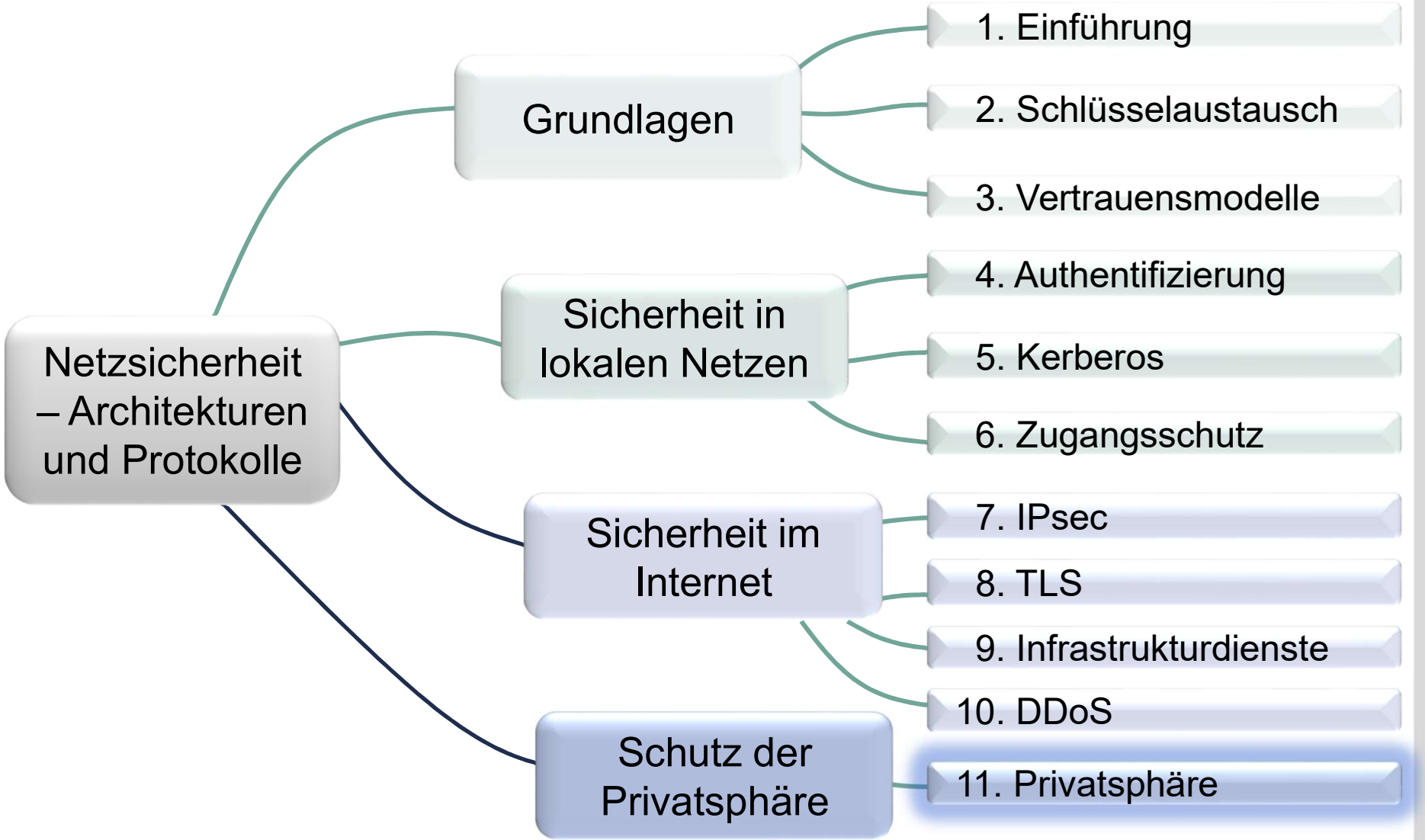
Vorlesung Netzsicherheit
Kapitel 11 – Privatsphäre

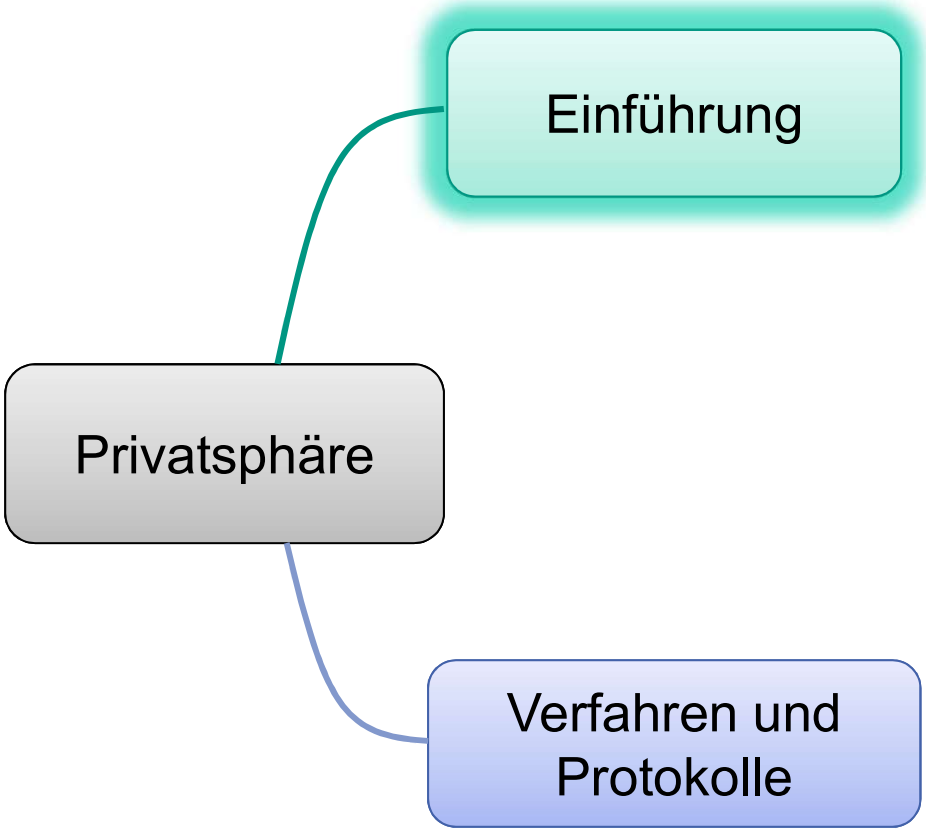
PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Institut für Telematik, Prof. Zitterbart

© Peter Baumung

Inhalte der Vorlesung




Einführung
Privatsphäre
Verfahren und Protokolle

Motivation

- Können wir unsere Privatsphäre im Internet überhaupt noch schützen?

Geburtsdatum

Wohnort

Arbeitgeber

Soziale Kontakte

Kalender

Fotoalben

Emails

Chatnachrichten

Gekaufte Bücher, Filme, Musik, …

Bewegungsprofile

Einführung - Diskussion

Wie definieren Sie Privatsphäre?

Was bedeutet für Sie Schutz der Privatsphäre?

Definition Privatsphäre/Datenschutz

- 1890 Warren/Brandeis
  - Privacy is the right to be let alone
- 1948 Universal Declaration of Human Rights
  - No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks
- 1967 Alan Westin
  - Privacy is the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others
- 1984 Ferdinand Schoeman
  - Privacy is the right to determine what (personal) information is communicated to others or the control an individual has over information about himself or herself
- 2005 IT-Grundschutzhandbuch des BSI
  - Aufgabe des Datenschutzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht)

Schutz der Privatsphäre (= Datenschutz)

- Schutz des Persönlichkeitsrechts bei der Verarbeitung personenbezogener Daten
  - Recht auf informationelle Selbstbestimmung
- Welche Daten sind schützenswert?
  - Laut BDSG: Personenbezogene Daten
  - Weitreichender: Privacy-relevant data

- Im Kontext von Kommunikationssystemen: auch Metadaten!
  - Wer kommuniziert wann mit wem?
  - Wo hält sich ein Nutzer auf?
  - Wer nutzt einen bestimmten Dienst?

→ Schutz der Metadaten aus technischer Sicht besonders herausfordernd

Säulen zum Schutz der Privatsphäre

- Regulierung (z.B. Datenschutzgesetze)
  - Bundesdatenschutzgesetz
  - Einzelne Regelungen in Telekommunikationsgesetz und Telemediengesetz
  - Landesdatenschutzgesetze
- Selbstregulierung
  - TRUSTe
  - TÜV (Teil von S@ver Shopping)
  - Trusted Shop
- Selbstschutz
  → Privacy Enhancing Technologies (PET)

Spezifische Schutzziele für Privatsphäre

- Unverkettbarkeit
  - Ein System bewahrt Unverkettbarkeit, wenn personenbezogene Daten aus zwei unterschiedlichen Kontexten für einen Angreifer nicht miteinander in Bezug gesetzt werden können
  - Technische Verfahren
    - Datenvermeidung, Anonymisierung, …
- Transparenz
  - Ein System bewahrt Transparenz, wenn die Verarbeitung von personenbezogenen Daten nachvollziehbar und überprüfbar ist
  - Technische Verfahren
    - Erstellung von Logdateien, …
- Intervenierbarkeit
  - Ein System bietet Intervenierbarkeit, wenn betroffene Personen über die Art der Erfassung und Verarbeitung ihrer personenbezogenen Daten selbst bestimmen können
  - Technische Verfahren
    - Schaffung von Wahlmöglichkeiten hinsichtlich der Verarbeitung von Daten, …

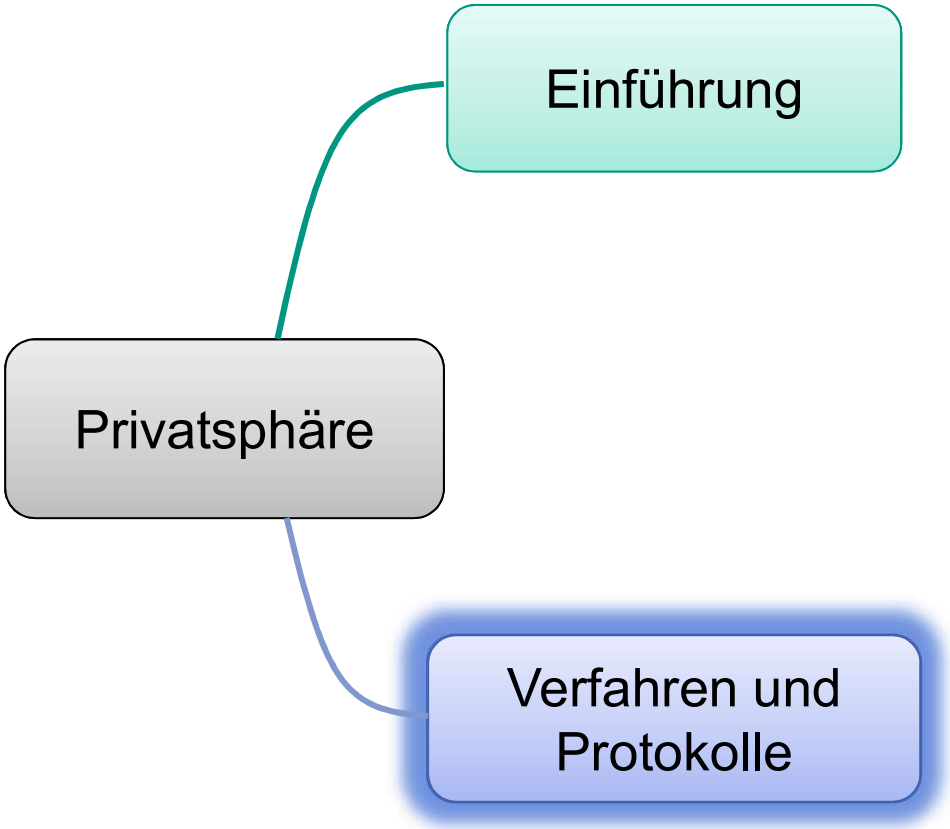
Definitionen

- Anonymität
  - Laut BDSG: Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können
  - Senderanonymität: Benutzer als Sender anonym
  - Empfängeranonymität: Benutzer als Empfänger anonym
- Pseudonymität
  - Laut BDSG: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren

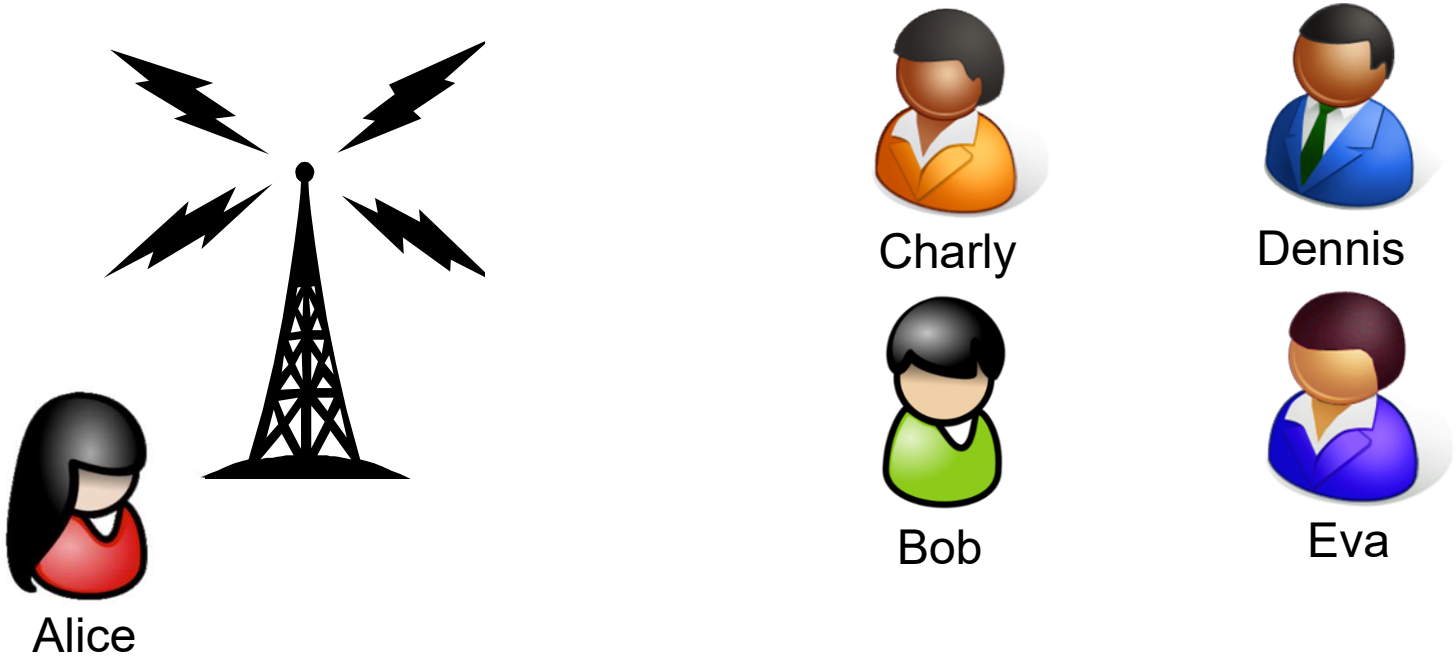
Privacy Enhancing Technologies (PET)

- Was soll geschützt werden?
  - Schutz der Identität eines Benutzers
    - Anonymität, Pseudonymität
    - Unverkettbarkeit
  - Schutz der Herkunft von Daten
    - Anonymität
    - Pseudonymität
  - Schutz personenbezogener Daten
    - Schutz von Vertraulichkeit und Integrität
    - Herstellung von Transparenz
      - Kommunikation mit dem Benutzer
      - Policy-Werkzeuge
    - Filtern personenbezogener Daten aus Netzverkehr

→ Grundprinzip: Datensparsamkeit (data minimization)


Einführung
Privatsphäre
Verfahren und Protokolle

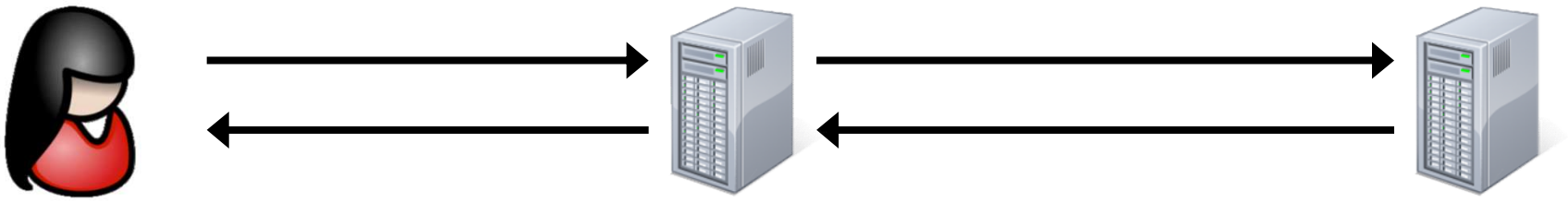
Beispiel 1: Message Broadcast



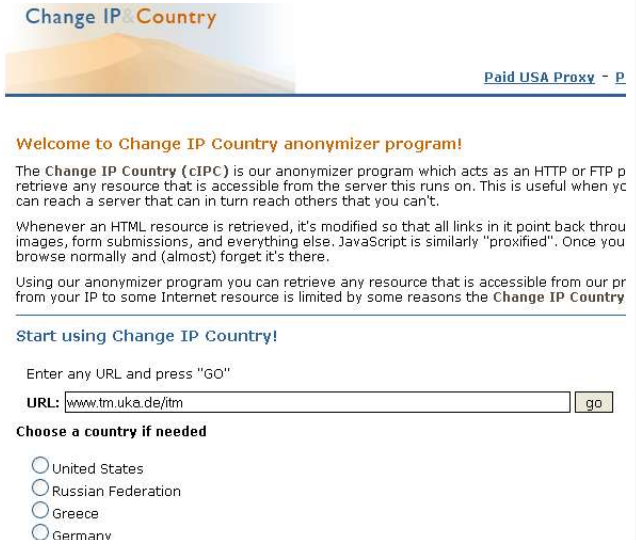
Empfängeranonymität

- Nachteile
  - Keine Senderanonymität
  - Benötigt Broadcast Medium
  - Skaliert nicht

Beispiel 2: Proxy-Ansatz

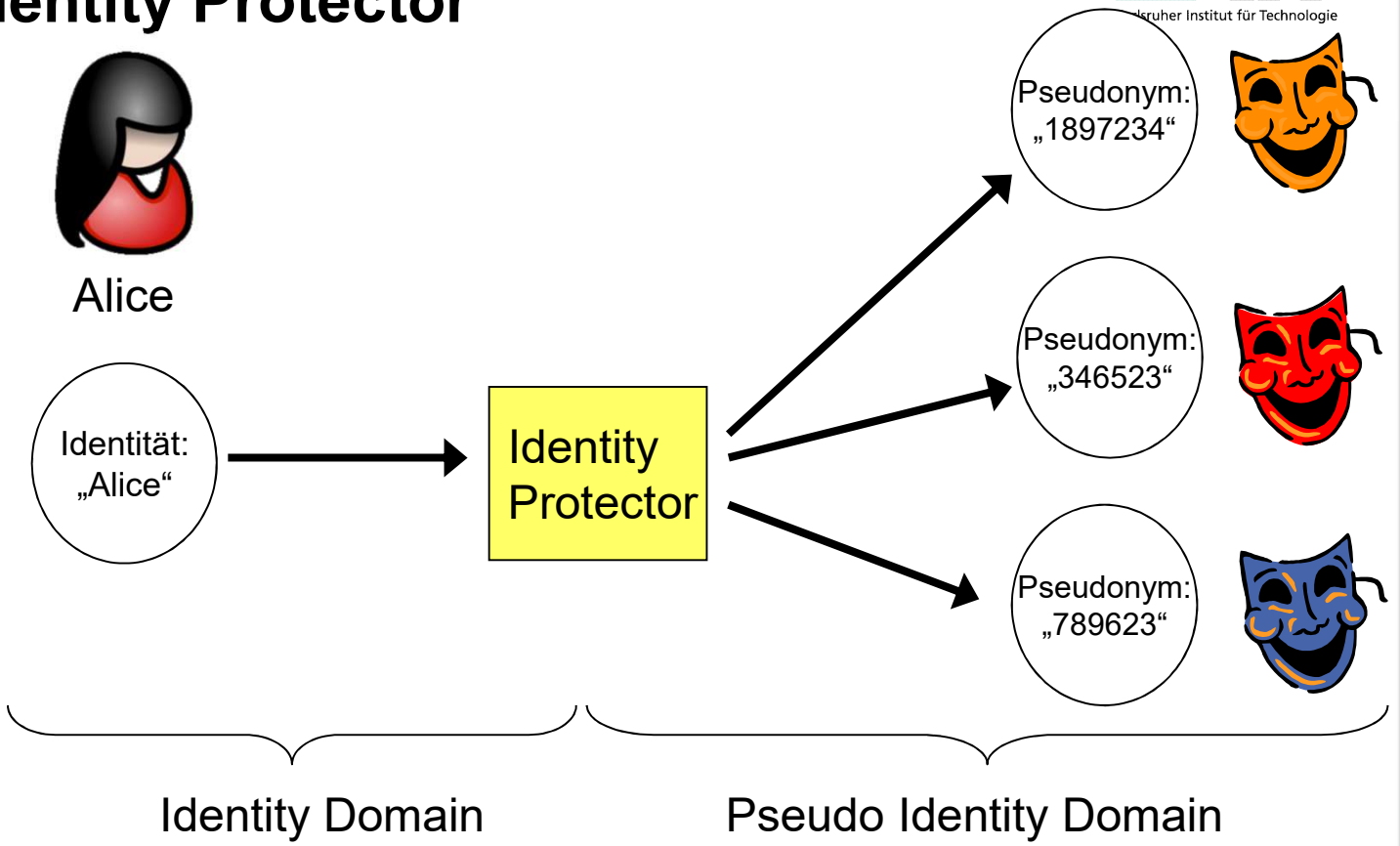


- Proxy (“Anonymizer”) leitet Anfragen weiter und entfernt persönliche Daten
- Senderanonymität
- Nachteile
  - Vertrauen in Anonymizer
  - Verbindung zwischen Alice und Proxy ist kritisch



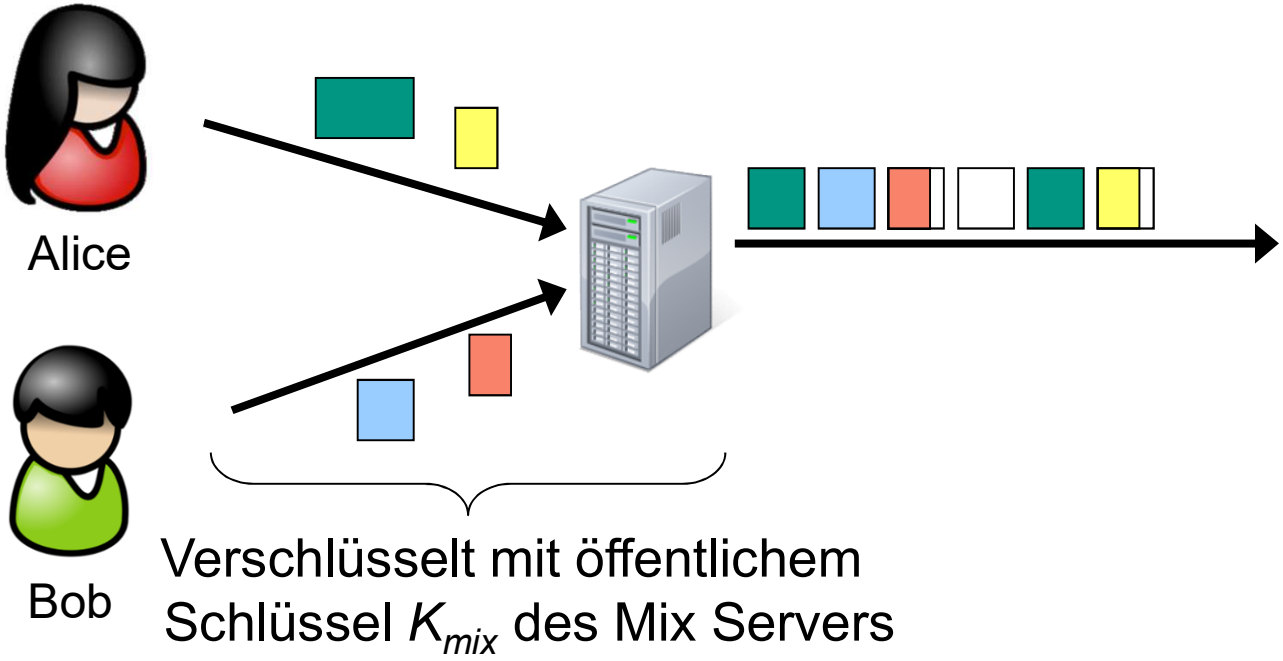
http://anonymizer.nntime.com

Beispiel 3: Identity Protector



- Identity Protector generiert Pseudonyme → Senderpseudonymität
- Nachteile
  - Vertrauen in Identity Protector
  - Wechsel von Pseudonymen darf nicht beobachtbar sein

Beispiel 4: Mixes



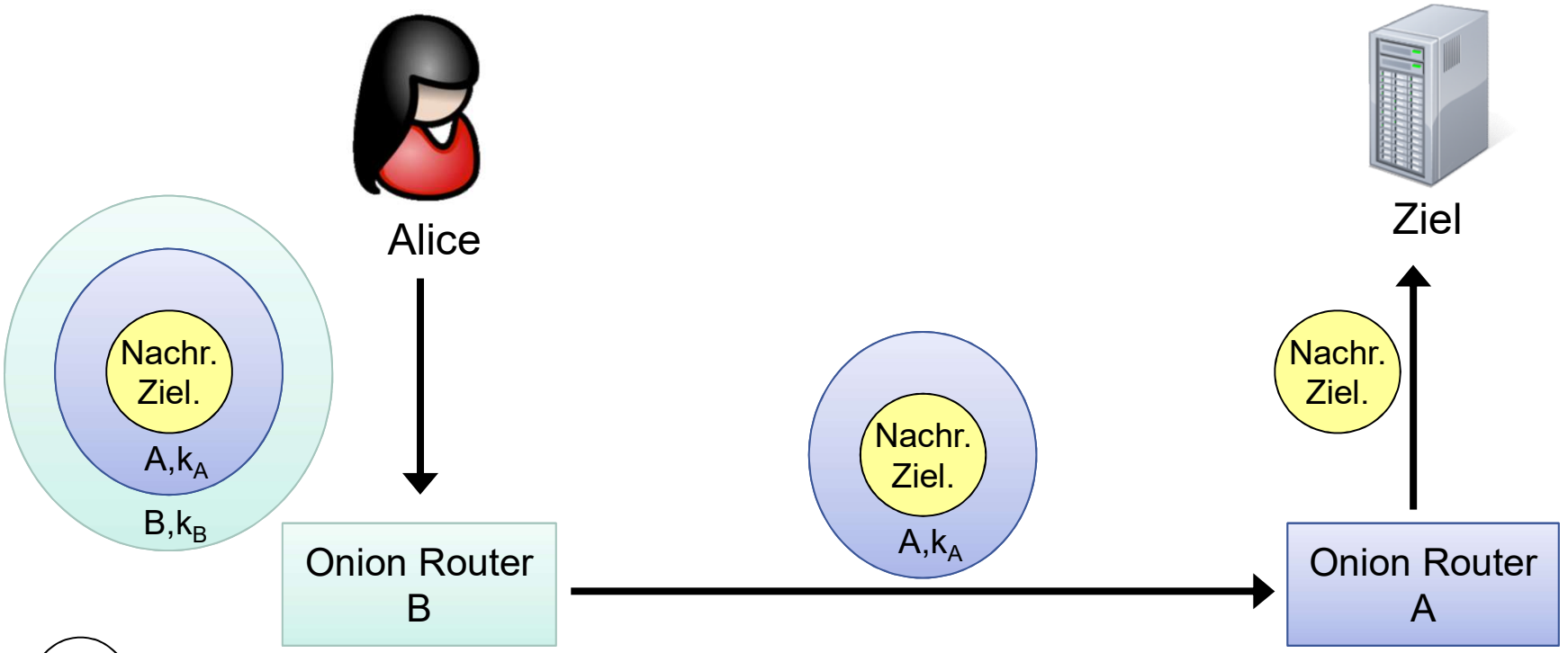
- Mix-Server sammelt, vertauscht, transkodiert eingehende Nachrichten (+ ggf. Löschen von Duplikaten)
- Kaskadierung von Mixes erhöht Sicherheit
  - Sicher, sofern nicht alle Mixbetreiber kooperieren

[Chau81]

Beispiel 4: Mixes - Vor- und Nachteile

- Vorteile
  - Senderanonymität
  - Unverkettbarkeit für alle außer dem Mix selbst
- Nachteile
  - Wartezeiten (v.a. bei Kaskadierung)
  - Speicherbedarf
  - Kommunikationsoverhead (Längenanpassung + Dummy-Verkehr)
  - Mix ist DoS-gefährdet
  - Hoher Aufwand durch Einsatz von Public-Key-Kryptographie
  - Angriffsmöglichkeit: *n-1*-Angriff
    - Mix leitet weiter, sobald *n* Nachrichten im Zwischenspeicher
    - Angreifer schickt Pulk von *n-1* Nachrichten
    - Nächste Nachricht von regulärem Knoten kann beobachtet werden

Beispiel 5: Onion Routing

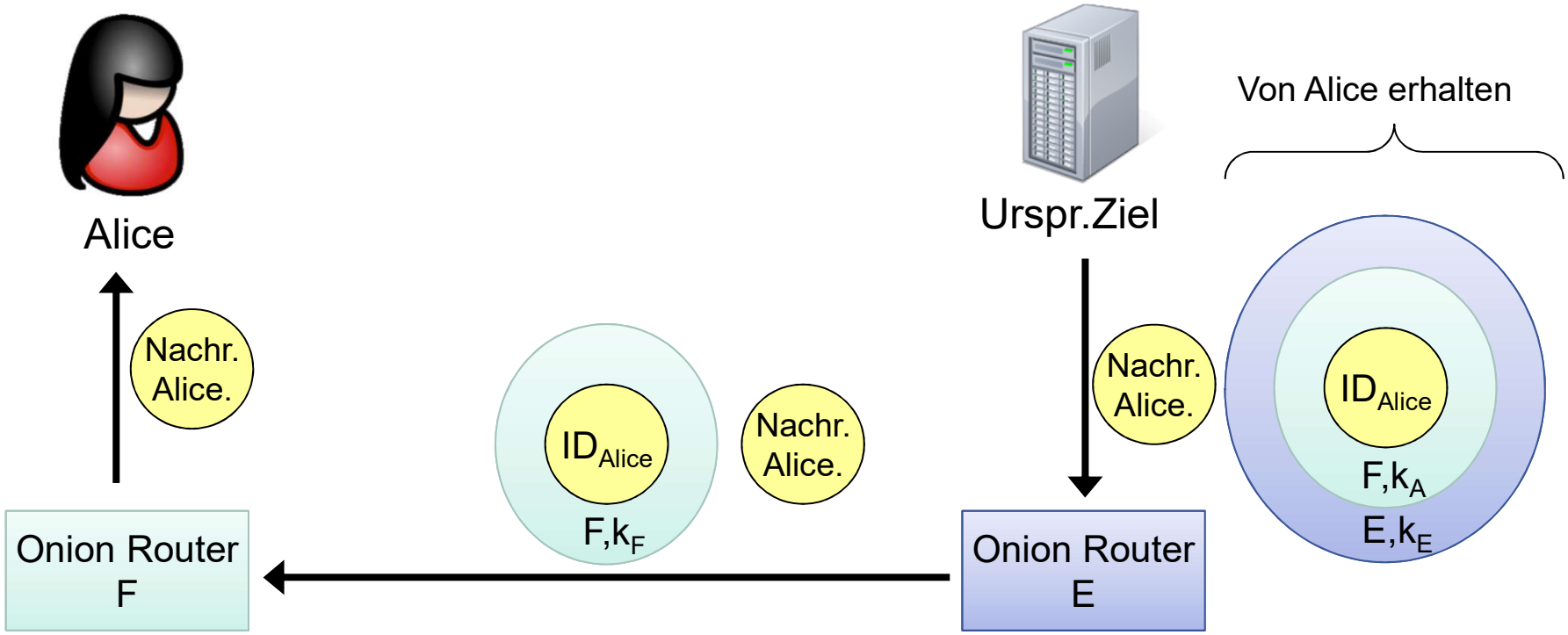


X,k_X = Nachricht an X adressiert und mit öffentlichem Schlüssel k_X verschlüsselt

- Weiterleitung durch zufällig gewählte Reihe von Onion Routern
- Schichtweise Verschlüsselung (“Zwiebel”)

[ReSG98,GoRS99]

Beispiel 5: Onion Routing - Rückkanal



X,k X = Nachricht an X adressiert und mit öffentlichem Schlüssel k X verschlüsselt

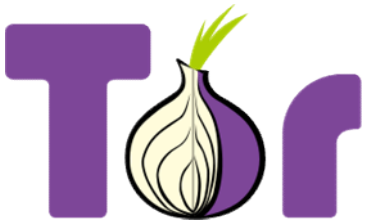
Mix-Kaskaden vs. Onion Routing

- Onion Routing bietet im Gegensatz zu Mix-Kaskaden:
  - Kein Zwischenspeichern und Vertauschen von Nachrichten
  - Neue Pfadwahl für jede Verbindung
  - I.d.R. deutlich mehr Onion Router als Mixes
- Onion Routing bietet keinen Schutz vor starkem Angreifer
  - Angreifer darf nicht das komplette Netz überwachen können
  - Bietet keinen Schutz vor Traffic Confirmation
    - Sobald der Angreifer sowohl Verkehr zum ersten Onion Router sowie Verkehr vom letzten Onion Router beobachten kann, ist Verkettung des Verkehrs (z.B. mittels Timing-Angriff) möglich
  - Mix-Kaskaden bietet hingegen auch bei globalem passiven Angreifer noch (eingeschränkten) Schutz

Beispiel 5: Onion Routing – Vor-/Nachteile

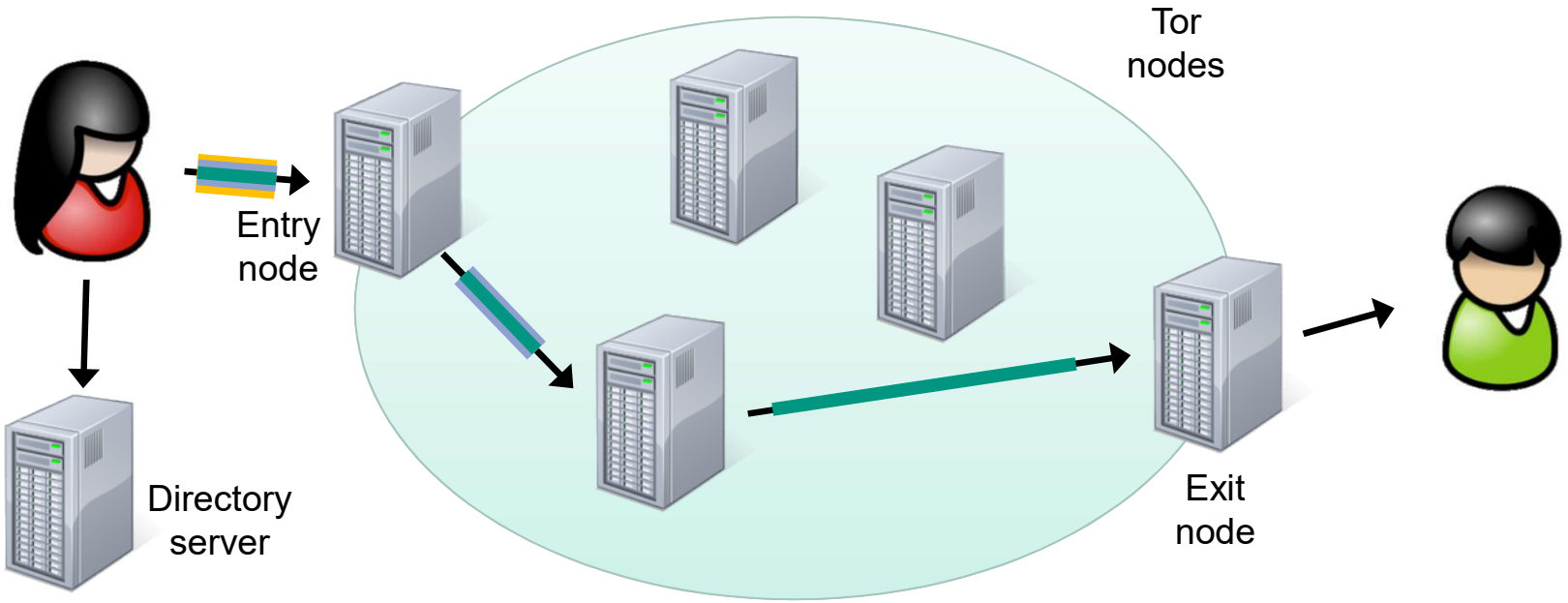
- Vorteile
  - Unverkettbarkeit (sofern Angreifer nur eingeschränkt Verkehr überwachen kann)
  - Geringe Latenz im Vergleich zu Mix-Kaskaden
  - Keine Speicherung der Nachrichten notwendig
  - Für viele Anwendungsprotokolle geeignet, Implementierung als lokaler Proxy-Server möglich
- Nachteile
  - Viele Public-Key-Operationen notwendig (1 pro Nachricht/Router)
    → Optimierung: Jeweils Etablierung eines sicheren Kanals (siehe Tor)
  - Unverkettbarkeit wird nur erreicht, wenn viel Verkehr über die Onion Router
    - Sonst mit hoher Wahrscheinlichkeit Traffic-Analyse möglich
  - Angriffe über Beobachtung der Paketgrößen, Zeitabstände, usw. durch Beobachtung von erstem und letztem Onion Router möglich

Beispiel 5: Onion Routing mit Tor



- Populäre Software für Onion-Routing: Tor (The Onion Routing project)
- Entwickelt seit 2002 mit Unterstützung der US-Regierung
- Finanzielle Unterstützung (Stand 2012)
  - 60% aus Zuwendungen der US-Regierung
  - 40% private Spenden
- Anonymisierung von Verbindungsdaten (IP-Adressen)
- Für Dienste, die auf TCP aufsetzen
  - Web-Browsing
  - Instant Messaging
  - E-Mail
  - SSH
  - …

Beispiel 5: Onion Routing mit Tor



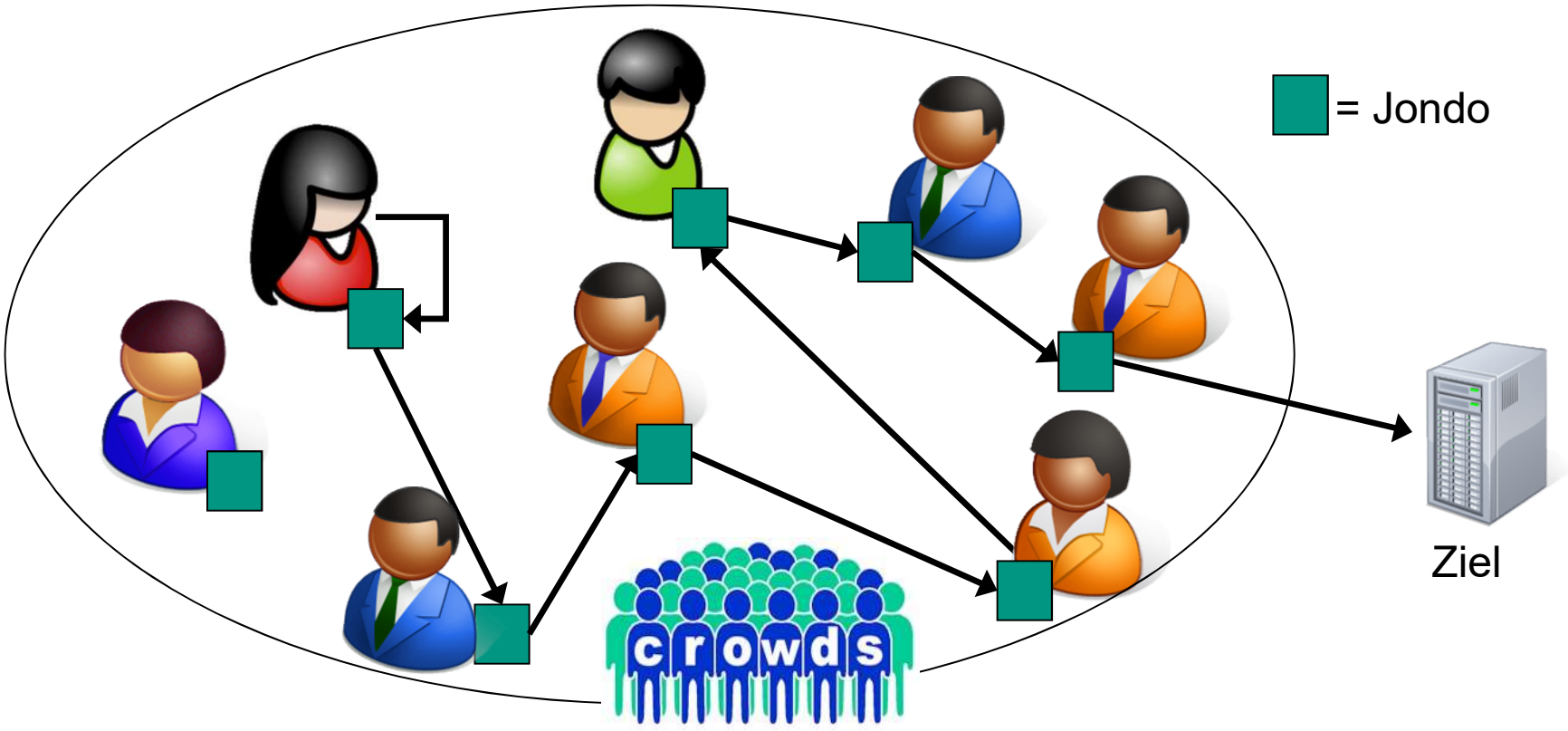
- Ablauf
  - List aller Tor-Knoten von Directory Server abrufen
  - Wahl zufälliger Route über drei Tor-Knoten
  - Aufbau gesicherter Verbindung zu erstem Knoten („entry node“)
  - Über diese Verbindung: Aufbau gesicherter Verbindung zu zweitem Tor-Knoten und schließlich zu exit node
  - Regelmäßig neuer Aufbau der Verbindungen über andere Knoten

Tor: Hidden Services

- Tor bietet zunächst nur Senderanonymität

- Zusätzlich Empfängeranonymität durch Hidden Services
  - Bob (= Dienstanbieter) erstellt Schlüsselpaar (k_E, k_D)
  - Öffentlicher Schlüssel k_E wird mit Liste von Eintrittsknoten auf Verzeichnisserver hinterlegt
  - Hash-Wert des öffentliches Schlüssel identifiziert Dienst
  - Alice baut über Tor Verbindung zu einem Rendevouz-Knoten auf
  - Alice teilt Bob Rendevouz-Knoten mit durch Nachricht an hinterlegten Eintrittsknoten
  - Sofern Bob einverstanden ist, antwortet er an Rendevouz-Knoten und etabliert Verbindung

Beispiel 6: Crowds



- Menge von Benutzern (Crowd) auf deren Knoten „Jondo“ läuft
- Jeder leitet Anfragen zufällig
  - Entweder verschlüsselt an anderes Mitglied der Menge
  - Oder unverschlüsselt an das Ziel weiter

[ReRu98]

Beispiel 6: Crowds - Vor-/Nachteile

- Vorteile
  - Senderanonymität gegenüber Ziel
  - Einige Angreifer in der Crowd können toleriert werden
- Nachteile
  - Jondos können Inhalt mitlesen
  - Längere Antwortzeiten
  - DoS-anfällig
    - Jondos können Nachrichten verwerfen
  - Sicherheitsrisiko Blender
    - Bösartiger Blender könnte auf Anfrage Liste mit Angreifer-Jondos zurückgeben
  - Keine Senderanonymität gegen netzwerkweiten Lauscher

Beispiel 7: Peer-to-Peer-Netz Freenet

- P2P-Filesharing-Netz
- Entwurfsziele
  - Anonymität für Herausgeber und Nutzer von Informationen (entspricht Sender- und Empfängeranonymität)
  - Abstreitbarkeit für den Knoten, der Informationen speichert
  - Sicherheit vor Zensur (Löschen, Zugriffssperren)
  - Effizientes Routing
  - Vollständige Dezentralisierung

Beispiel 7: Freenet - Schutz von Anonymität

- Grundprinzipien
  - Anfragen werden über mehrere Hops weitergeleitet
    - Antworten auf gleichem Weg zurück
    - Jeder Knoten kennt in dieser Kette nur direkten Nachbarn
  - Dokumente werden verschlüsselt gespeichert
    - Speichernder Knoten kennt den Schlüssel nicht
  - Einfügen von Dokumenten funktioniert auf gleichem Pfad wie Suche
- Sender- und Empfängeranonymität i.A. gewährleistet
  - Aber kein Schutz vor Verkehrsanalyse, Unverkettbarkeit nicht garantiert

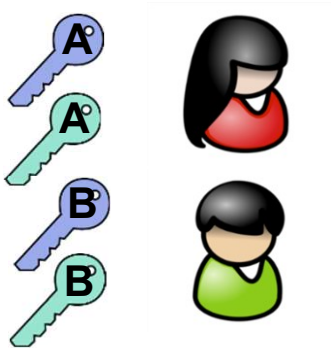
Beispiel 8: Off-the-Record Messaging

Einschub: Sichere Kommunikation mit OpenPGP

- Datenformat zum Verschlüsseln und / oder Signieren von Nachrichten
- Schutzziele können unabhängig voneinander realisiert werden
  - Vertraulichkeit und Integrität von Nachrichten
    - Mit Hilfe von symmetrischem Verfahren
    - Schlüssel muss dazu ausgetauscht werden
  - Authentizität des Absenders
    - Mit Hilfe von asymmetrischem Verfahren
    - Signatur des Absenders unter der Nachricht
    - Abbildung zwischen Signatur und Identität muss überprüft werden
  - Authentizität des Empfängers
    - Mit Hilfe von asymmetrischem Verfahren
    - Durch Verwendung des öffentlichen Schlüssels des Empfängers
    - Abbildung zwischen Identität und Schlüssel muss überprüft werden

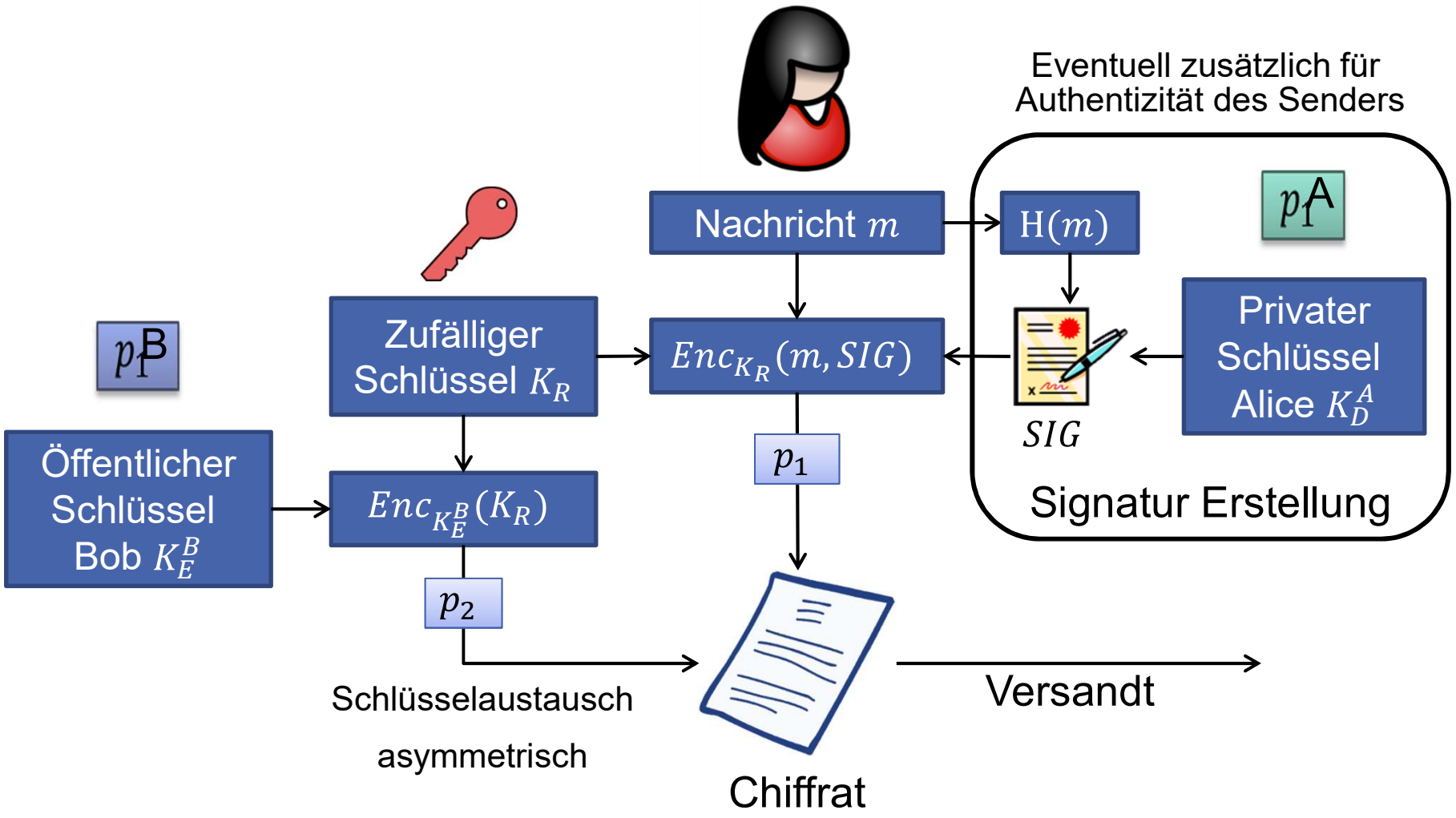
Einschub: OpenPGP

- Nachrichtenversand von Alice an Bob
  - Alice erzeugt
    - Öffentlichen Schlüssel K_E^A
    - Privaten Schlüssel K_D^A
  - Bob erzeugt
    - Öffentlichen Schlüssel K_E^B
    - Privaten Schlüssel K_D^B



- Schutzziel Vertraulichkeit und Integrität der Nachricht
  - Hybrides Verfahren
    - Schlüsselaustausch asymmetrisch, Verschlüsselung symmetrisch
  - Alice
    - Verschlüsselt Nachricht M symmetrisch mit zufälligem Schlüssel K_R
    - Verschlüsselt Schlüssel K_R asymmetrisch mit Bobs öffentlichem Schlüssel K_E^B
    - Sendet Chiffrat der Nachricht und Chiffrat des Schlüssel an Bob
  - Bob
    - Entschlüsselt den Schlüssel K_R asymmetrisch mit privatem Schlüssel K_D^B
    - Entschlüsselt Nachricht M mit symmetrischen Schlüssel K_R

Einschub: OpenPGP



Beispiel 8: Off-the-Record Messaging

Welchen Nachteil hat das Signieren von Nachrichten mit PGP für die alltägliche Kommunikation?

Alle Nachrichten sind *nicht abstreitbar*!

Beispiel 8: Off-the-Record Messaging

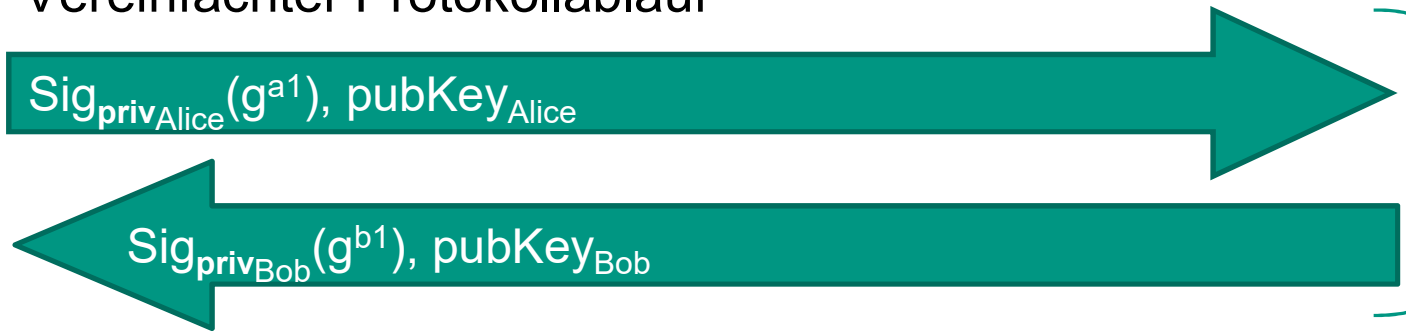
- Ziel: Sicherheit und Datenschutz für Instant Messaging
  - Vertraulichkeit
    - Perfect Forward Secrecy
  - Authentifizierung gegenüber Empfänger
  - Abstreitbarkeit
- Motivation: flüchtigen Charakter verbaler Kommunikation nachbilden
  - Keine späteren Beweise über Gesprächsinhalte
  - Auch bei späterer Kompromittierung eines Hosts
  - Unabhängig vom verwendeten IM-Protokoll (funktioniert mit ICQ, Jabber, MSN, …)

[BoGB04,RaGK05]

Realisierung: Off-the-Record messaging

Entwickelt als Plugin für Pidgin und andere IM Clients

- Vereinfachter Protokollablauf



Sitzungsschlüssel (pro Nachricht neu) → $k_{11} = (g^{b1})^{a1} \bmod n$

Alice

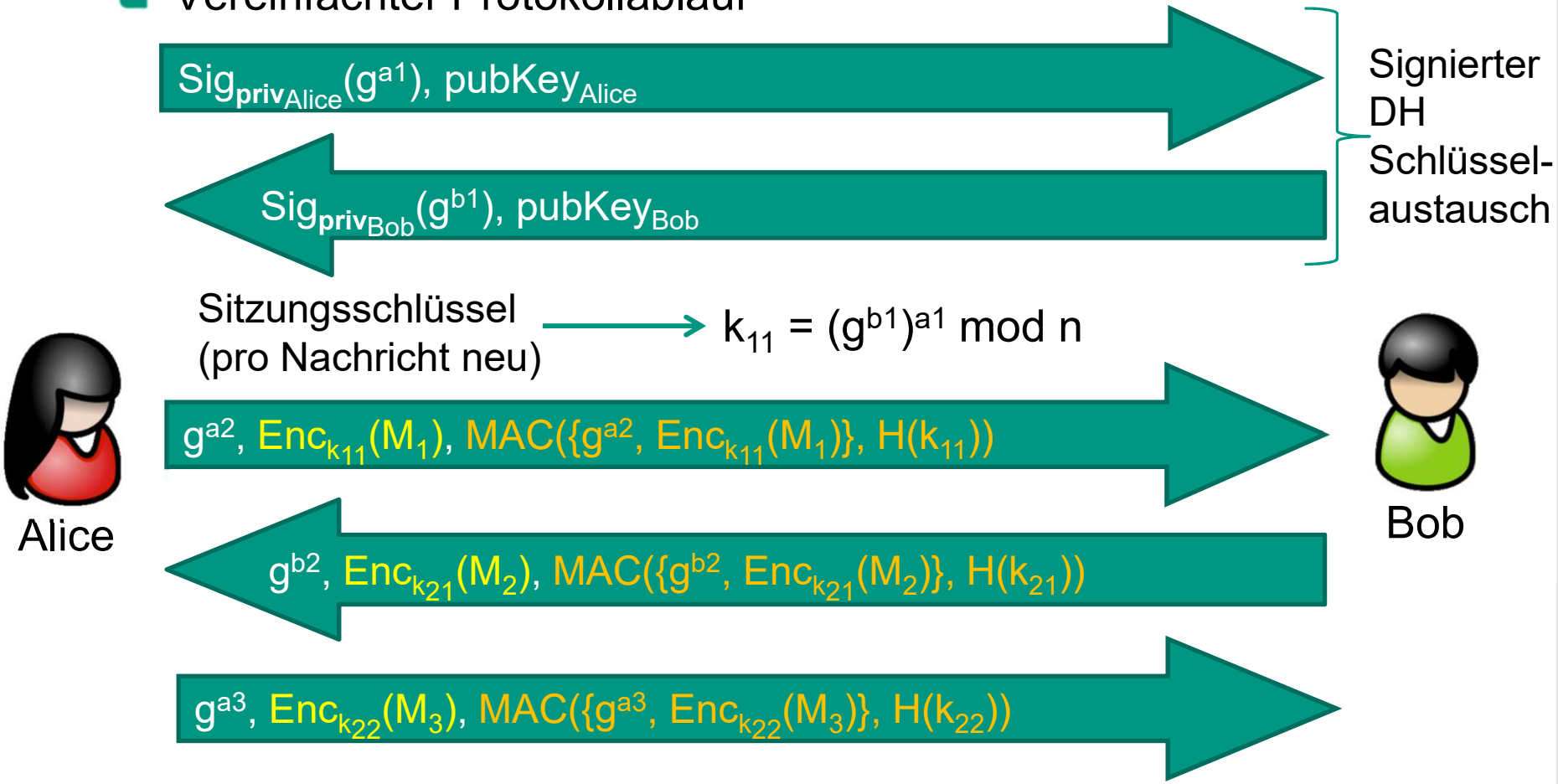
Bob

- Sender wählt pro Nachricht neue Zufallszahl a_i bzw. b_j
- Verschlüsseln der Nachricht mit aktuellem Schlüssel k_{ij}
- HMAC über Nachricht mit $H(k_{ij})$ für Integritätsschutz
- Bei Empfang einer Nachricht: Neuen Sitzungsschlüssel k_{ij} mit Diffie-Hellmann berechnen
- Offenlegung der in Vergangenheit verwendeten $H(k_{ij})$

Realisierung: Off-the-Record messaging

Entwickelt als Plugin für Pidgin und andere IM Clients

- Vereinfachter Protokollablauf



Beispiel 9: Web-Privacy

- Tracking Cookies
  - Server hinterlegt im Browser Cookie mit ID
  - Zuordnung noch möglich, nachdem Nutzer sich beim Dienst abgemeldet hat
  - Verfolgung von Nutzern über Webseiten hinweg (u.a. durch Werbeanbieter)

- Browser-Fingerprinting
  - Eindeutiger Fingerabdruck durch HTTP-Header (u.a. User-Agent, Referer) sowie JavaScript (u.a. Browser-Plugins, Fonts)
  - https://panopticlick.eff.org/
- DNS-Tracking
  - Auflösung von Hostnamen durch DNS-Server des ISP

  → Erstellung eines Nutzerprofils

Kompromittierung der Endsysteme

- Sicherheit aller beschriebenen Verfahren setzt vertrauenswürdige Endsysteme voraus
- Kompromittierung durch Schadsoftware (Malware)
  - Bietet Angreifern u.a. Zugriff auf
    - Tastatur
    - Webcam
    - Mikrofon
    - GPS
    - Dateisystem

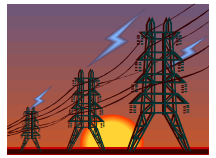
- Einschleusen der Schadsoftware aufgrund von
  - Fehlender Sicherheitsupdates
  - Software aus nicht vertrauenswürdigen Quellen
  - Social Engineering

Forschungsarbeiten zu PETs am Institut

Privatsphäre im…

- …modernen Straßenverkehr (Smart Traffic)
  - Erfassung der aktuellen Verkehrslage
  - Kooperative Routenplanung

- …zukünftigen Stromnetz (Smart Grid)
  - Erfassung von Strombedarf und Einspeisepotential in den einzelnen Haushalten (*Smart Metering*)



- …Haushalt (Smart Home)
  - Immer mehr vernetzte Sensoren und Aktoren im Haushalt

Mehr dazu nächstes Semester in der Vorlesung „Internet of Everything“

Zusammenfassung

- Privacy Enhancing Technologies (PET) bieten technischen (Selbst-)Schutz der Privatsphäre
  - Grundprinzip der Datensparsamkeit
- Ansätze für Anonymität
  - Broadcast
  - Mixes bzw. Mix-Kaskaden
  - Onion-Routing
- Ansätze für Abstreitbarkeit
  - Off-the-record messaging (OTR)

Literatur

[Chau81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM 24(2), Februar 1981

[ReSG98] Michael G. Reed, Paul F. Syverson, David M. Goldschlag: Anonymous Connections and Onion Routing, IEEE Journal on Selected Areas in Communications 16(4), Mai 1998 (sehr ausführliche Darstellung)

[GoRS99] David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections, Communications of the ACM 42(2), Feb. 1999, S. 39-41 (kurzer Überblick, gut zu lesen)

[ReRu98] Michael K. Reiter, Aviel D. Rubin: Crowds: Anonymity for Web Transactions, ACM Transactions on Information and System Security 1(1), Nov. 1998, S. 66-92.

[BoGB04] N. Borisov, I. Goldberg, E. Brewer: Off-the-record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*. 2004. (Vorstellung des OTR-Protokolls)

[RaGK05] M. Di Raimondo, M., R. Gennaro, H. Krawczyk: Secure off-the-record messaging. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. 2005. (Kritik und Verbesserung des OTR-Protokolls)