Strafverfolgung trotz Anonymität

Stefan Köpsell, TU Dresden, Institut Systemarchitektur

- Anonyme Kommunikation im Internet: AN.ON
- Rechtliche Bewertung von anonymer Kommunikation
- Erfahrungen im Bezug auf Strafverfolgung
- Verfahren zur Deanonymisierung ex nunc
- Ausblick

Das *AN.ON* Projekt

- soll Anonymität auch gegen starke Angreifer gewährleisten, die z. B. Daten auf allen Leitungen abhören und verändern können
- besteht aus lokal zu installierender Client-Software (JAP) und Servern (Mixen)
- Idee beruht auf dem Mix-Verfahren von David Chaum (1981)
- Gefördert durch die DFG im Rahmen des Schwerpunktes „Sicherheit“ und das BMWA
- Zusammenarbeit mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und der Universität Regensburg
- Testversion unter: http://anon.inf.tu-dresden.de/

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

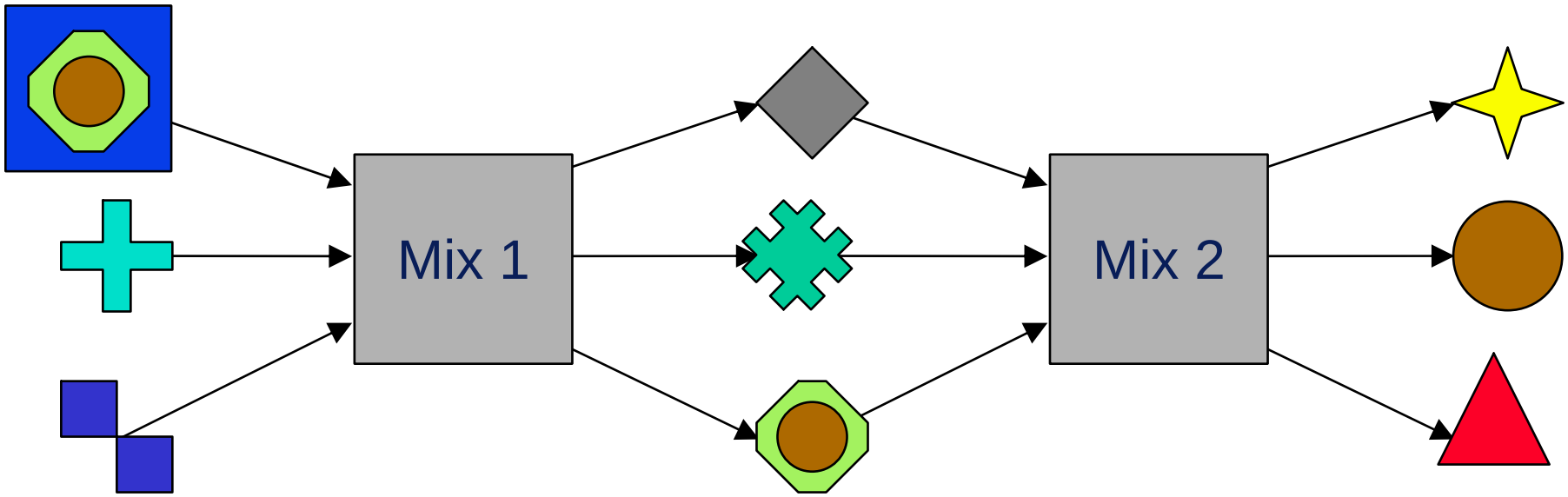
Funktionsweise

„ JAP“ wird als Proxy für den WWW-Browser eingetragen

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Das Mix-Verfahren

Idee: Unverkettbarkeit zwischen ein- und ausgehenden Nachrichten erzeugen



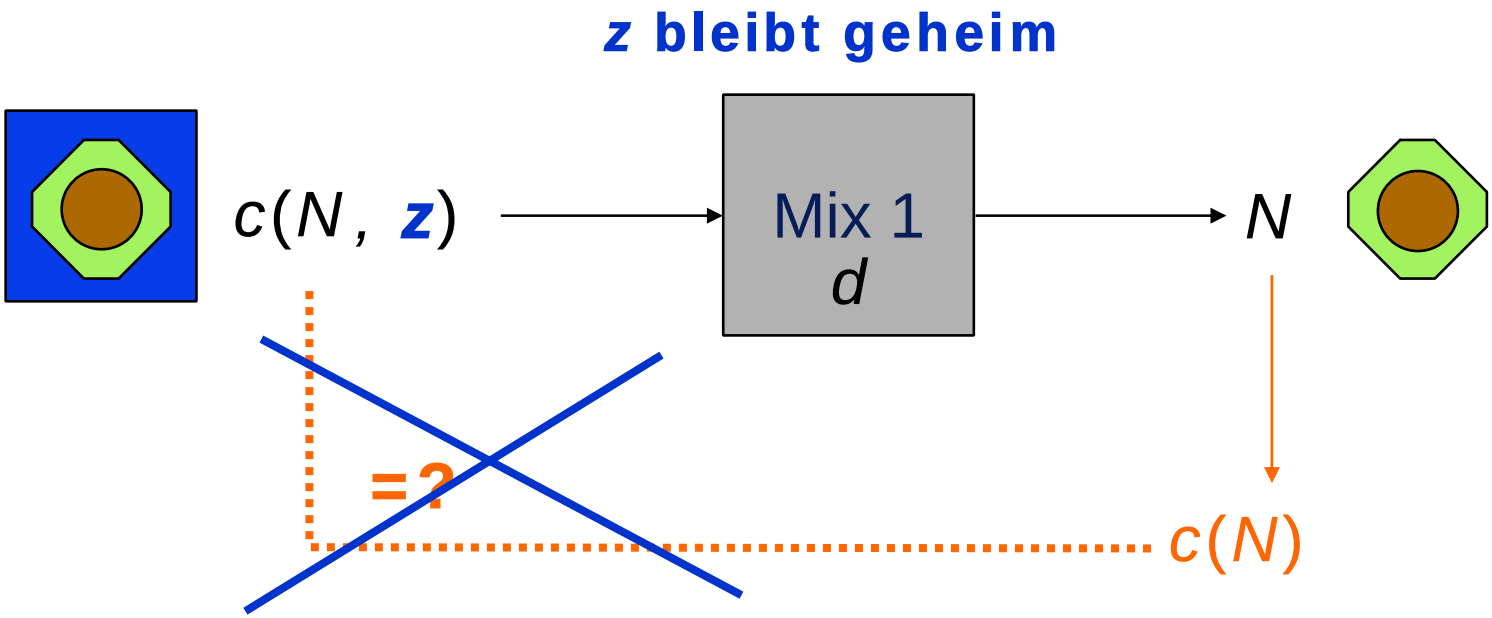
Ein Mix sammelt Nachrichten, kodiert sie um und gibt sie umsortiert wieder aus.

Alle Mixe müssen zusammenarbeiten, um den Weg einer Nachricht zurückverfolgen zu können.

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

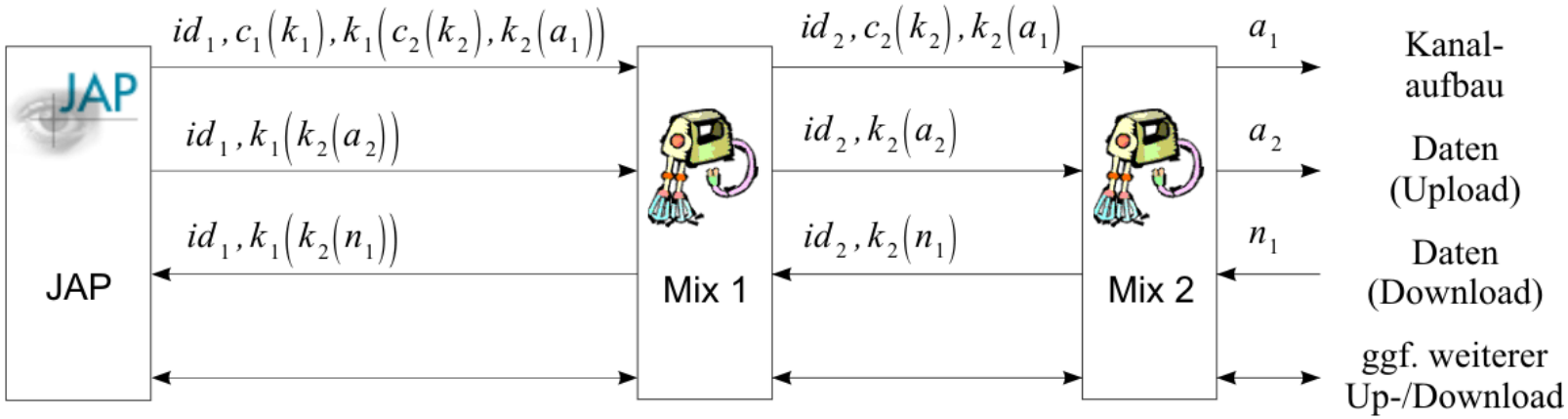
Mixe: Ein wenig Kryptographie

- Umkodierung erfolgt mittels asymmetrischer Verschlüsselungsverfahren
- jeder Mix besitzt einen geheimen Schlüssel *d* und veröffentlich den dazu passenden Verschlüsselungsschlüssel *c*
- Nachrichten *N* werden schrittweise für jeden Mix verschlüsselt – beginnend mit dem letzten Mix



Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Anonyme Kommunikations-Kanäle



ID	Schlüssel M_1	Schlüssel M_2
id_1	k_1	k_2
id_2	k_3	k_6
id_3	k_4	k_7
id_4	k_5	k_8

in	Schlüssel	out
id_1	k_1	id_2
id_3	k_3	id_4
id_5	k_4	id_6
id_7	k_5	id_8

Verbindungs-tabellen

- „Schalten“ von Kanälen geschieht durch die Übermittlung eines symmetrischen Schlüssels k_i und eines Kanalkennzeichens id_j an jeden Mix
- zu übertragende Daten werden durch den Mix mit Hilfe eines symmetrischen Kryptoverfahrens umkodiert

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

- ✓ Anonyme Kommunikation im Internet: AN.ON
- ▶ **Rechtliche Rahmenbedingungen**
  - Erfahrungen im Bezug auf Strafverfolgung
  - Verfahren zur Deanonymisierung ex nunc

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Vielzahl von Vorschriften ist zu berücksichtigen

- Grundgesetz (GG)
- Außenwirtschaftsgesetz (AWG)
- Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (G10-Gesetz)
- Strafprozeßordnung (StPO)
- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- Mediendienste-Staatsvertrag (MDStV)
- Teledienstegesetz (TDG)
- Telekommunikationsüberwachungsverordnung (TKÜV)
- Telekommunikations-Datenschutzverordnung (TDSV)
- Teledienstedatenschutzgesetz (TDDSG)
- EU Datenschutz Direktive (95/46/EC)
- EU Verfassung
- ...

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Welche Art von Dienst ist AN.ON ?

- Telekommunikationsdienste
  - Anknüpfungspunkt: Datentransport und Signalverarbeitung
  - Gesetzliche Regelung: TKG
  - Beispiele: Telefonkabel, Mobilfunk, Access-Provider, E-Mail
    - Speicherpflicht für Strafverfolgung

- Teledienste
  - Anknüpfungspunkt: Inhalt der Kommunikation
  - Gesetzliche Regelung: TDG / TDDSG
  - Beispiele: Websites / Datendienste / Online Banking / **AN.ON**
    - Keine Verpflichtung zur Vorratsdatenspeicherung

- Mediendienste
  - Anknüpfungspunkt: Inhalt mit redaktionellem Hintergrund
  - Gesetzliche Regelung: MDStV
  - Beispiele: Spiegel-Online, Heise etc.

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Rechtliche Rahmenbedingungen

- Volkszählungs-Urteil (BVerfGE 65,1 - 15. Dezember 1983)

  „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."

- Bundesdatenschutzgesetz (BDSG) [§ 3a]:

  „Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Teledienstedatenschutzgesetz

- Teledienstedatenschutzgesetz (TDDSG) [§ 4 Absatz 6]:

  „Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“

- Teledienstedatenschutzgesetz (TDDSG) [§ 6 Abs. 1]:

  „Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne Einwilligung nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten).“

- TDDSG wurde zum 1. Januar 2002 umfassend novelliert.
  - Der Wortlaut des § 4 Abs. 6 TDDSG blieb unverändert.
  - anonyme oder pseudonyme Möglichkeit der Inanspruchnahme von Telediensten weiterhin wichtiges Anliegen des Gesetzgebers

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Strafprozeßordnung

- §§ 100 a, b und §§ 100 g, h relevant für Überwachungsmaßnahmen

- §§ 100 g, h
  - Auskunftsersuchen ist auf Daten beschränkt, die nach bestehenden Regelungen zulässigerweise erhoben und gespeichert werden und insoweit bereits vorliegen
  - gemäß Vorgaben des TDDSG werden bei AN.ON keine Daten gespeichert
  - Paragraphen nicht anwendbar

- §§ 100 a, b
  - Aufzeichnung personenbezogener Daten für die Zukunft kann angeordnet werden
  - Vorraussetzung:
    - Verdacht auf Straftat gemäß Katalog
    - richterliche Anordnung (maximal für drei Monate)
    - bei Gefahr im Verzug auch Staatsanwalt (maximal für drei Tage)
  - relevant für AN.ON

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Schlußfolgerungen

⌘ der Betrieb des Anonymisierungsdienstes in seiner angebotenen Form steht im Einklang mit den geltenden gesetzlichen Regelungen

⌘ Vorratsspeicherung von Nutzungsdaten bezüglich des Dienstes zum Zwecke der Strafverfolgung ist nicht vorgeschrieben; vielmehr wäre im Gegenteil die Speicherung dieser Daten rechtswidrig

⌘ im Einzelfall kann eine Überwachung einer Kommunikationsbeziehung durch richterlichen bzw. staatsanwaltschaftlichen Beschluß angeordnet werden

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

- ✓ Anonyme Kommunikation im Internet: AN.ON
- ✓ Rechtliche Rahmenbedingungen
- ▶ **Erfahrungen im Bezug auf Strafverfolgung**
  - Verfahren zur Deanonymisierung ex nunc

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Erfahrungen aus dem Betrieb von AN.ON

- Test Version verfügbar: http://anon.inf.tu-dresden.de/
  - veröffentlicht und kostenlos nutzbar: seit September 2000
  - > 1.000.000 Downloads
  - geschätzt:
    - mehr als 50 000 Nutzer
    - 2 500 gleichzeitig
  - pro Monat:
    - > 4 TByte Daten
    - >200 Million URLs

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Mißbrauch von AN.ON

- Mißbrauchs bezogene Anfragen (1. Januar – 30. Juni 2004)
  - insgesamt: 32 Anfragen
  - 22 Anfragen von Strafverfolgungsbehörden (Polizei, Staatsanwalt, Richter)
    - bezogen auf strafrechtlich relevanten Anfangsverdacht.
    - 14 x Betrug (3 x eBay)
    - 5 x Beleidigung
  - 10 Anfragen von Privatpersonen und Firmen
    - Spam-Email
    - Beleidigungen
    - Urheberrechtsverletzungen
    - Angriffe auf Webseiten (gestohlene eBay Paßwörter)

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Mißbrauch verhinderbar?

- „künstliche“ Beschränkung der unterstützten Protokolle
  - keine TCP/IP Verbindungen möglich
    - implementiert aber deaktiviert
  - nur HTTP (Web)
  - nur bekannte HTTP Ports (80, 443, 8080)
  - Begrenzung der Größe von POST-Anfragen (Uploads)
- Webseitenbetreiber können Sperrung beantragen
- Mißbrauch aber generell nicht verhinderbar:
  - Zugriffe die in einem Land zulässig sind können in einem anderen ALnd verboten sein
  - Computer sind generell nicht in der Lage zu entscheiden ob ein Zugriff “gut” oder “böse” ist

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Beispiel für Anfrage und Antwort bei Mißbrauch

Polizeidirektion XY
Kommissariat 3

Berlin, den 25.02.2005

Ermittlungsverfahren gegen Unbekannt wegen des Verdachtes auf Computerbetrug

Sehr geehrte Damen und Herren, im Rahmen des oben genannten Ermittlungsverfahrens wurde festgestellt, daß dem Täter eine IP-Adresse zugeordnet werden kann, die durch Sie verwaltet wird:

IP-Adresse: 141.76.1.121 Datum/Uhrzeit (Ortszeit): 25.06.2004, 09:05:46 Uhr

Sie werden nun gebeten alle Ihnen bekannten Verbindungs- und Nutzungsdaten, die oben genannte IP-Adresse und Zeitpunkt betreffen mitzuteilen. Es wird auch um Mitteilung gebeten, falls keine Daten zum Beispiel auf Grund der bereits verstrichenen Zeit vorliegen

... Der von Ihnen genannten Server ist Teil eines Forschungsprojektes. Ziel des Projektes ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren. Dabei geht es darum, die Vorschriften des Teledienstedatenschutzgesetzes umzusetzen. Dabei wird bereits auf technischer Ebene die Zuordnung von IP-Adressen zu einzelnen Nutzern oder sonstigen identifizierenden Merkmalen vermieden. Aus diesem Grunde liegen keine Daten vor, über die (bei Vorliegen eines richterlichen Beschlusses) Auskunft gegeben werden könnte.
Es tut mir leid, Ihnen insoweit nicht weiterhelfen zu können. ...

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Der BKA Fall

- 03.07.2003: Beschluß des Amtsgerichts Frankfurt/Main
  - Grundlage: §§ 100g, 100h StPO
  - Speicherung / Auskunft von Zugriffen auf eine bestimmte IP
  - ULD legt Beschwerde ein (keine aufschiebende Wirkung)
- Einbau / Aktivierung der Strafverfolgungsfunktion
  - Aufzeichnung eines einzelnen Datensatzes
- 11.07.2003: Landgericht Frankfurt setzt Vollziehung aus
  - Mitteilung an ULD erst 26.08.2003
  - Bestätigung endgültig 15.09.2003
- 29.08.2003: AG Frankfurt ordnet Durchsuchung der Räume der TU Dresden und Beschlagnahme an
  - Auskunftsverpflichtung war schon ausgesetzt
  - Protokolldatensatz wird unter Protest herausgegeben
- 21.10.2003: LG Frankfurt bestätigt Rechtsauffassung des ULD
  - Durchsuchungsanordnung und Beschlagnahme waren rechtswidrig
- Löschung des Datensatzes erweist sich als schwierig

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

- ✓ Anonyme Kommunikation im Internet: AN.ON
- ✓ Rechtliche Rahmenbedingungen
- ✓ Erfahrungen im Bezug auf Strafverfolgung
- ▶ **Verfahren zur Deanonymisierung ex nunc**

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Anforderungen an die Deanonymisierung

- gemäß §§ 100 a, b StPO muß eine Deanonymisierung im Einzelfall auf entsprechende Anordnung unter Angabe der zu überwachenden Kennung ex nunc (von jetzt an) möglich sein

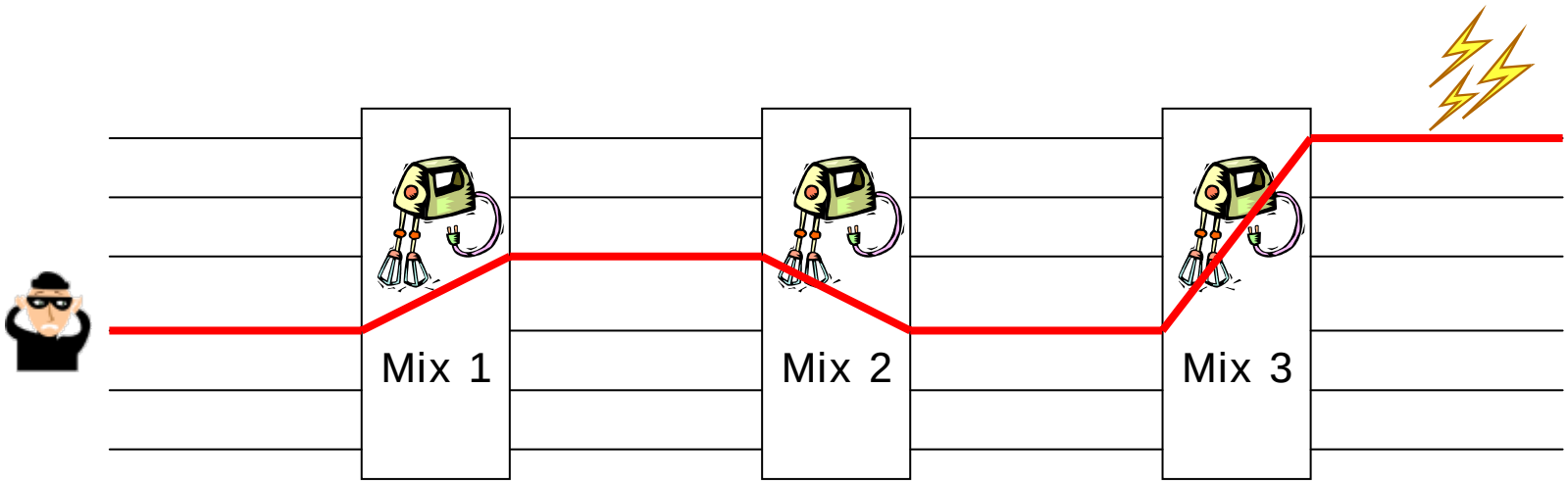
- die Anonymität der nicht überwachten Teilnehmer muß gewahrt bleiben, d. h. daß bei *n* Teilnehmern und Durchführung einer Überwachung die Kardinalität der verbleibenden Anonymitätsmenge *n*-1 beträgt

- das Vertrauensmodell des Anonymisierungsdienstes muß erhalten bleiben, d. h. die Deanonymisierung erfordert die Mitarbeit *aller* Mixe einer Kaskade

- es sollen Audit-Daten gespeichert werden, um die Häufigkeit von durchgeführten Deanonymisierungen durch externe Stellen kontrollieren zu können

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Idee



- Schrittweise Aufdecken beginnend beim ersten bzw. letzten Mix
- Jeder Mix muß überprüfen, daß:
  - die von ihm umkodierten Daten eines Kanals zu der in einer Anordnung genannten Kennung führen
    - Offenlegung der bei der asymmetrisch Verschlüsselung verwendeten Zufallszahl
  - er genau diese Daten an den nachfolgenden Mix gesandt hat
    - Mix speichert Hashwert der übertragenen Daten bzw.
    - Anhängen eines symmetrischen Authentikationskodes an die Daten

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Details

- ... findet man im Papier ☺

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA

Ausblick

- Nachteil des vorgestellten Verfahrens: erster Mix erfährt im Falle einer Deanonymisierung, wer welche Anfrage gestellt hat
  - Wie läßt sich das verhindern?

- Viele offene Fragen bezüglich des konkreten Ablaufs einer Überwachung
  - Wer ist verantwortlich für die Überwachungsmaßnahme? Der letzte Mix?
  - Erhält jeder Mix eine Überwachungsanweisung?

Stefan Köpsell
sk13@inf.tu-dresden.de
TU Dresden, Inst.SyA