



Grenzen des Schutzes der Vertraulichkeit in IT-Systemen

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
<http://svs.informatik.uni-hamburg.de/>



Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

Dresden, 17. Juli 2013

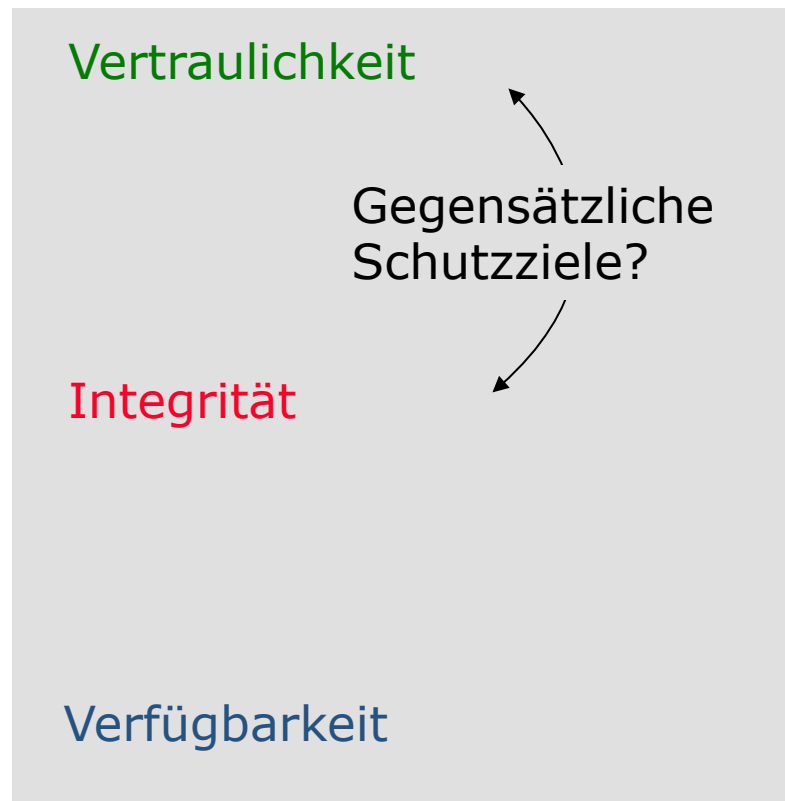
Gliederung des Vortrages

- Schutzziele
- Mehrseitige Sicherheit
- Vertraulichkeit
 - Verfahren und Algorithmen
- Beobachtungen zum Monotonieverhalten
- Fallbeispiele
 - One-Time-Pad
 - DC-Netz und Schnittmengenangriffe
 - Umkodierende Mixe und praktische Verkettungsangriffe
- Schlussbemerkungen

Schutzziele

Voydock, Kent 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.



unbefugter Informationsgewinn

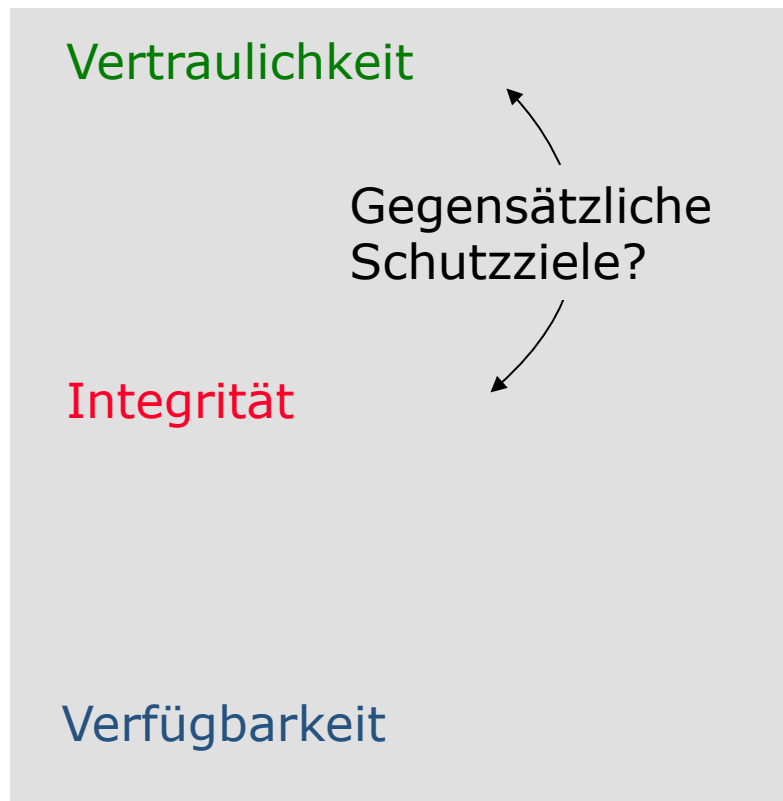
unbefugte Modifikation

unbefugte Beeinträchtigung der Funktionalität

Mehrseitige Sicherheit

Müller et. al. 1997

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.



- Voraussetzung
 - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
 - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Vertraulichkeit: Schutzziele und Angreifermodell

Inhaltsdaten

Vertraulichkeit
Verdecktheit

Inhalte

Verkehrsdaten

Anonymität
Unbeobachtbarkeit

Sender

Ort

Empfänger

- Outsider
 - Abhören auf Kommunikationsleitungen
 - Verkehrsanalysen
- Insider
 - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
 - Staatliche Organisationen (insb. fremde)

Vertraulichkeit: Verfahren und Algorithmen

Verfahren

Algorithmen

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES,
RSA, ElGamal, ...

Verdecktheit

Steganographie

Inhalte + Existenz

F5, ...

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer,
Remailer, anonyme
Zahlungssysteme

Pseudonyme, Proxies,
umkodierende Mixe, DC
Netz, Private Information
Retrieval, ...

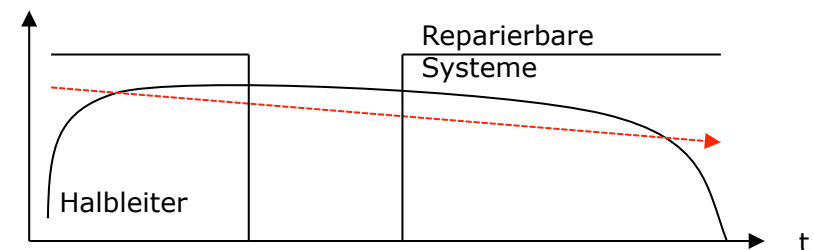
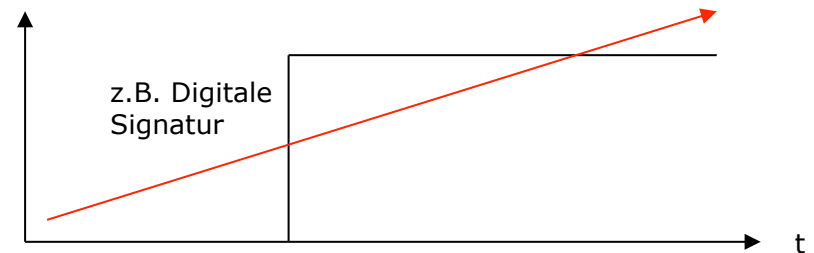
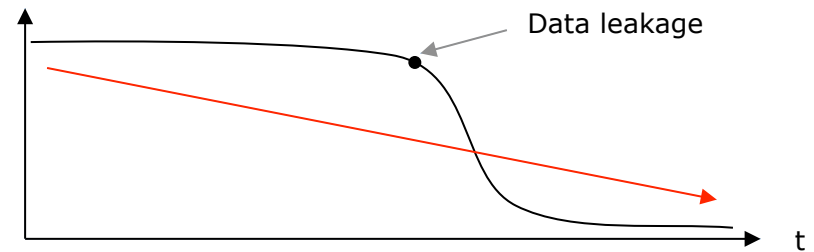
Beobachtungen zum Monotonieverhalten

- Das Monotonieverhalten von Schutzzielen gibt Hinweise auf die Prioritäten bei der Umsetzung von Schutzzielen und das praktisch erreichbare Schutzniveau.

Vertraulichkeit

Integrität

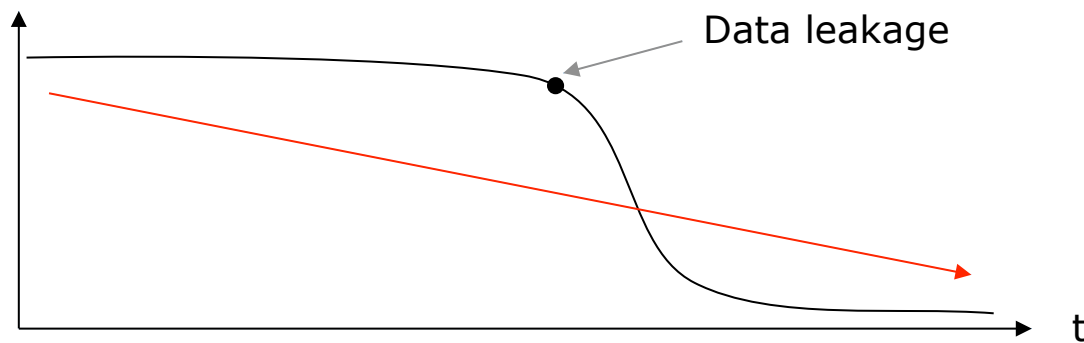
Verfügbarkeit



Beobachtungen zum Monotonieverhalten

- Vertraulichkeit, Verdecktheit, Anonymität und Unbeobachtbarkeit können nur geringer werden.

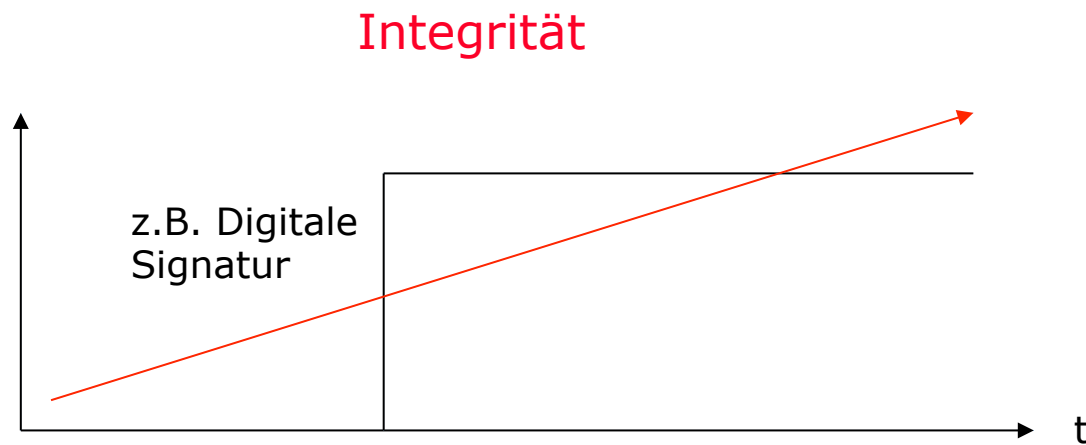
Vertraulichkeit



Sensible Daten müssen besonders sorgsam und mit hoher Priorisierung geschützt werden.

Beobachtungen zum Monotonieverhalten

- Integrität, Zurechenbarkeit und Rechtsverbindlichkeit können nur größer werden.

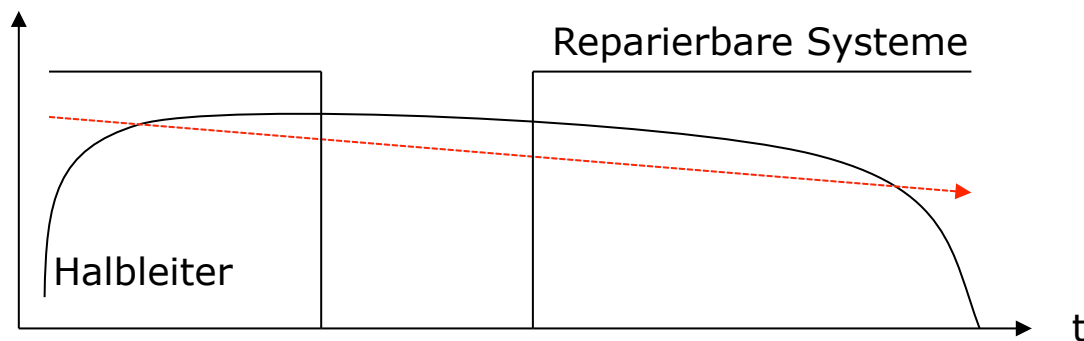


Ist einmal die Authentizität von Daten (auf technischer Ebene) festgestellt, geht sie nicht mehr verloren.

Beobachtungen zum Monotonieverhalten

- Verfügbarkeit und Erreichbarkeit verhalten nicht monoton (häufig unstetig und doch langfristig meist regressiv).

Verfügbarkeit



Es sind stets nur probabilistische Aussagen zur Verfügbarkeit möglich.

Grenzen der Vertraulichkeit

- Monotonie der Vertraulichkeit: Vertraulichkeit, Verdecktheit, Anonymität und Unbeobachtbarkeit können nur geringer werden.

Vertraulichkeit
Verdecktheit

Inhalte

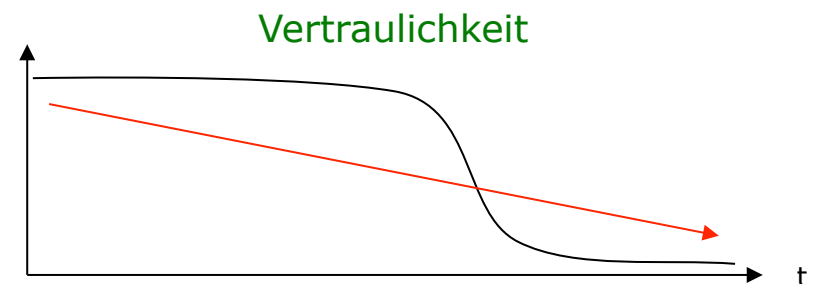
Anonymität
Unbeobachtbarkeit

Sender

Ort

Empfänger

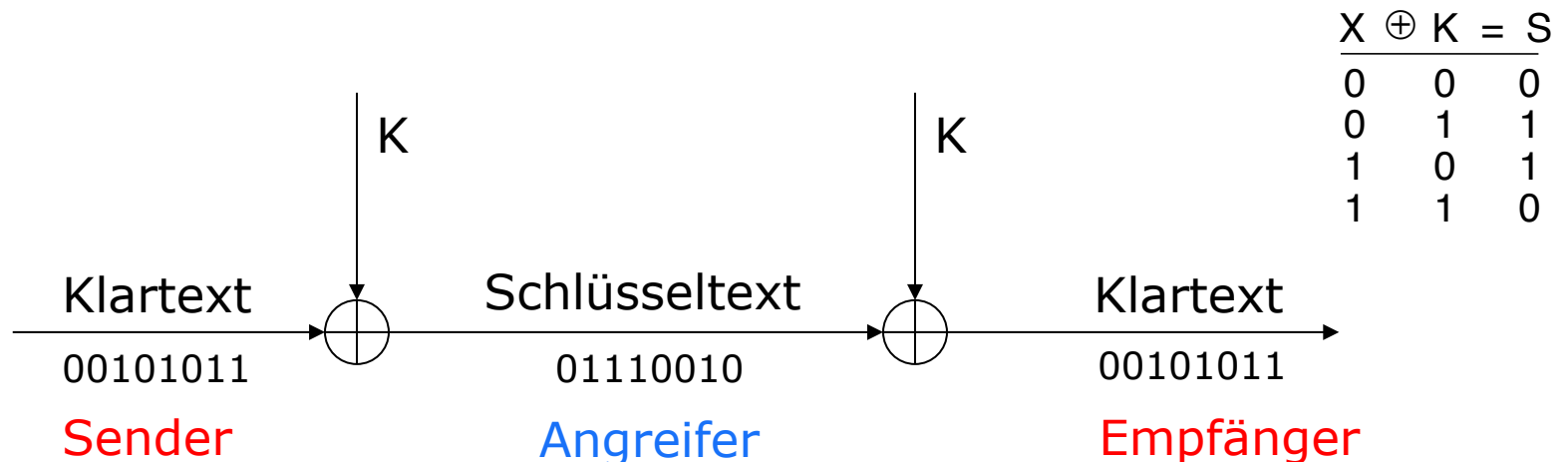
- Fallbeispiele
 - One-Time-Pad
 - DC-Netz und Schnittmengenangriffe
 - Umkodierende Mixe und praktische Verkettungsangriffe



One-Time-Pad (mod 2)

Inhalte

- **Randbedingungen**
 - Jedes Schlüsselbit darf nur einmal verwendet werden
 - Bits von K sind zufällig und unabhängig
 - Schlüssel genauso lang wie Klartext
- **Erreichbare Sicherheit**
 - Angreifer kann alle Varianten durchrechnen, erhält dadurch aber keine zusätzliche Information über den Klartext
 - Wahrscheinlichkeit, den Klartext richtig zu erraten, verändert sich durch die Beobachtung des Schlüsseltextes nicht



One-Time-Pad (mod 2)

Inhalte

- **Randbedingungen**
 - Jedes Schlüsselbit darf nur einmal verwendet werden
 - Bits von K sind zufällig und unabhängig
 - Schlüssel genauso lang wie Klartext
- **Erreichbare Sicherheit**
 - Angreifer kann alle Varianten durchrechnen, erhält dadurch aber keine zusätzliche Information über den Klartext
 - Wahrscheinlichkeit, den Klartext richtig zu erraten, verändert sich durch die Beobachtung des Schlüsseltexes nicht

Informationstheoretische Sicherheit

- Nicht im Modell: Angreifer erfährt: Länge des Klartextes

01110010

↔ Länge l ↔

DC-Netz

Chaum, 1988

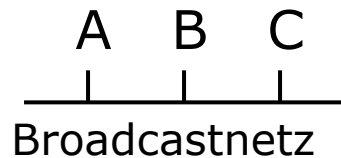
• Randbedingungen

- Jedes Schlüsselbit darf nur einmal verwendet werden
- Bits von K sind zufällig und unabhängig
- Schlüssel genauso lang wie Klartext
- Rundenbasiertes Protokoll

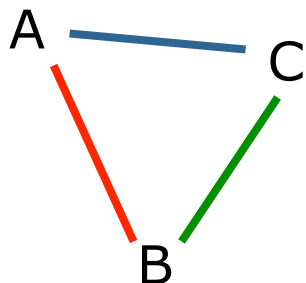
Sender

$$X \oplus K = S$$

0	0	0
0	1	1
1	0	1
1	1	0



Schlüsselgraph



Echte Nachricht von A	00110101
Schlüssel mit B	00101011
Schlüssel mit C	<u>00110110</u>
Summe	00101000

A sendet 00101000

Leere Nachricht von B	00000000
Schlüssel mit A	00101011
Schlüssel mit C	<u>01101111</u>
Summe	01000100

B sendet 01000100

Leere Nachricht von C	00000000
Schlüssel mit A	00110110
Schlüssel mit B	<u>01101111</u>
Summe	01011001

C sendet 01011001

Summe = Echte Nachricht von A 00110101

DC-Netz

- **Randbedingungen**
 - Jedes Schlüsselbit darf nur einmal verwendet werden
 - Bits von K sind zufällig und unabhängig
 - Schlüssel genauso lang wie Klartext
 - Rundenbasiertes Protokoll
- **Erreichbare Sicherheit**
 - Perfekte Unbeobachtbarkeit des Sendens
 - Jede Nachricht ist innerhalb der Teilnehmer unbeobachtbar, die durch zusammenhängenden Schlüsselgraph bilden.

Sender

Informationstheoretische Sicherheit

- Nicht im Modell: Wechselnde Benutzergruppen ermöglichen Schnittmengenangriffe

DC Netz und Schnittmengenangriffe

- Angreifer beobachtet:

Sender

- zu t_1 Nachrichten von 3 Sendern A,B,C an 3 Empfänger S,T,U
- zu t_2 Nachrichten von 3 Sendern C,D,E an 3 Empfänger T,V,W

$$t_1: \{A,B,C\} \rightarrow \{S,T,U\}$$

$$t_2: \{C,D,E\} \rightarrow \{T,V,W\}$$

$X \rightarrow Y$ bedeutet: Jeweils ein Teilnehmer aus der Menge X kommuniziert mit genau einem Teilnehmer aus der Menge Y.

- Schnittmengenbildung:

$$\{A,B,C\} \cap \{C,D,E\} \rightarrow \{S,T,U\} \cap \{T,V,W\} = \{C\} \rightarrow \{T\}$$

- Interpretation:

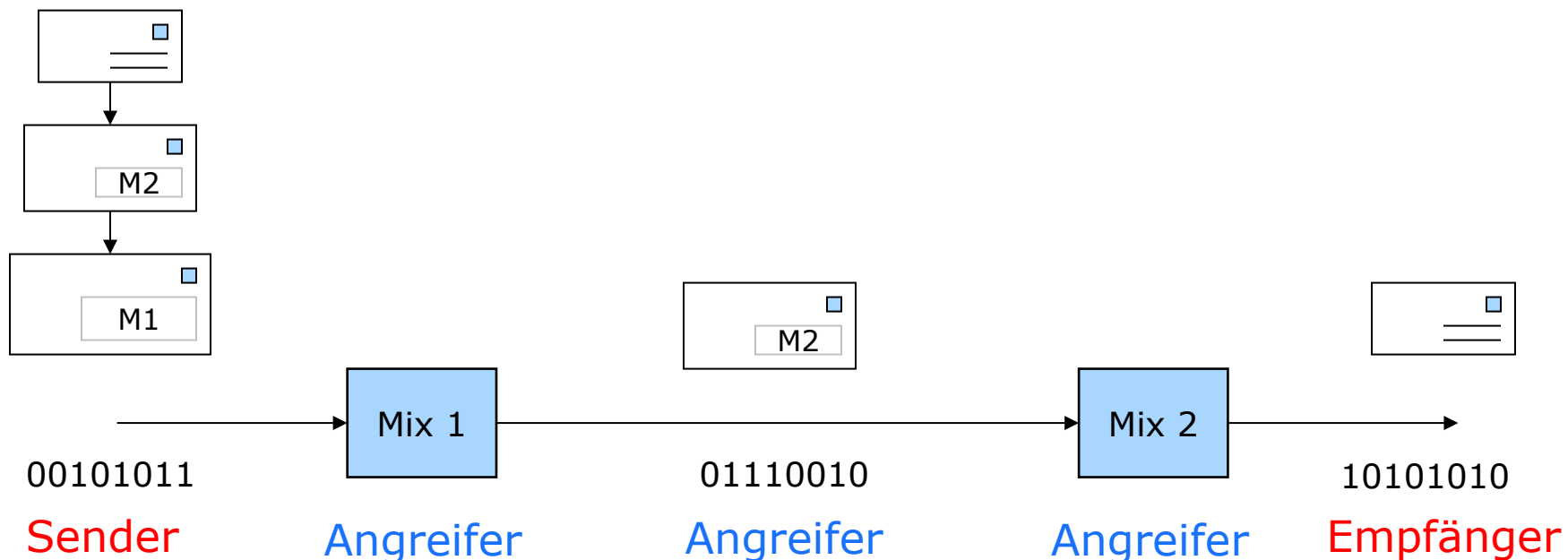
- reduzierte Anonymitätsgruppe $\{C,T\}$
- Wenn T angreift, weiß T sofort, dass C der Sender ist

Umkodierende Mixe

Chaum, 1981

- Grundidee:
 - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
- Randbedingungen
 - Alle Nachrichten haben die gleiche Länge.
 - Mehr als einen Mix verwenden.
 - Wenigstens ein Mix darf nicht angreifen.

Kommunikationsbeziehung

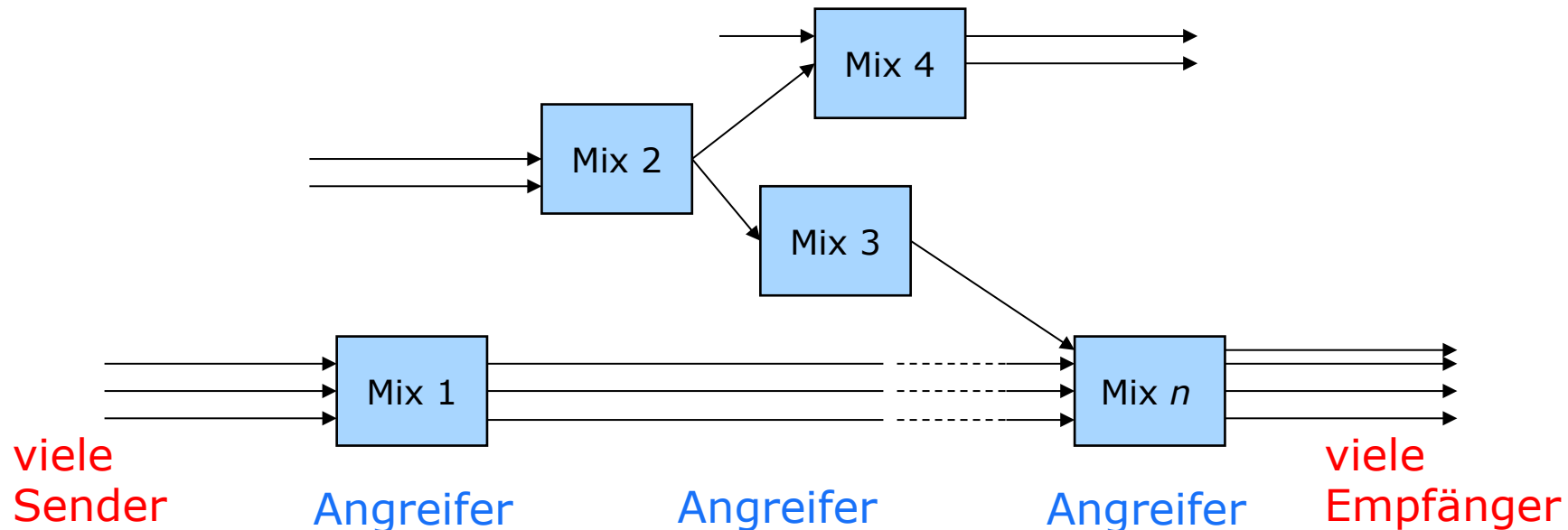


Umkodierende Mixe

Chaum, 1981

- Grundidee:
 - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
- Randbedingungen
 - Alle Nachrichten haben die gleiche Länge.
 - Mehr als einen Mix verwenden.
 - Wenigstens ein Mix darf nicht angreifen.

Kommunikationsbeziehung



Umkodierende Mixe und praktische Verkettungsangriffe

- Grundidee: Kommunikationsbeziehung
 - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
- Randbedingungen
 - Alle Nachrichten haben die gleiche Länge.
 - Mehr als einen Mix verwenden.
 - Wenigstens ein Mix darf nicht angreifen.
- Erreichbare Sicherheit
 - Unverkettbarkeit der Kommunikationsbeziehung gegen Insider und Outsider; solange kryptographische Verfahren nicht gebrochen sind:

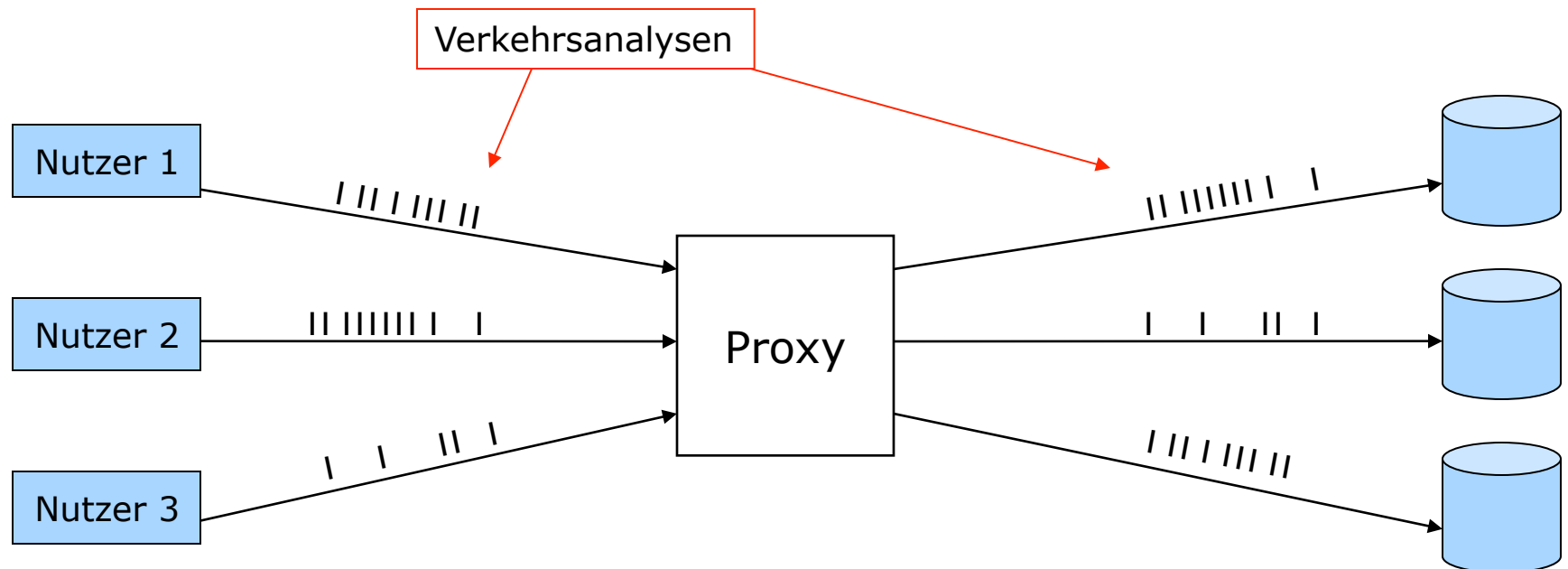
Komplexitätstheoretische Sicherheit

- Nicht im Modell: Schutz durch Dummy Traffic
- Schlimmer noch: schlechte Skalierbarkeit führt zu praktisch schwächer implementierten Verfahren

Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
 - trotz Verschlüsselung:
 - kein Schutz gegen Verkehrsanalysen
 - Verkettung über Nachrichtenlängen
 - zeitliche Verkettung

Kommunikationsbeziehung



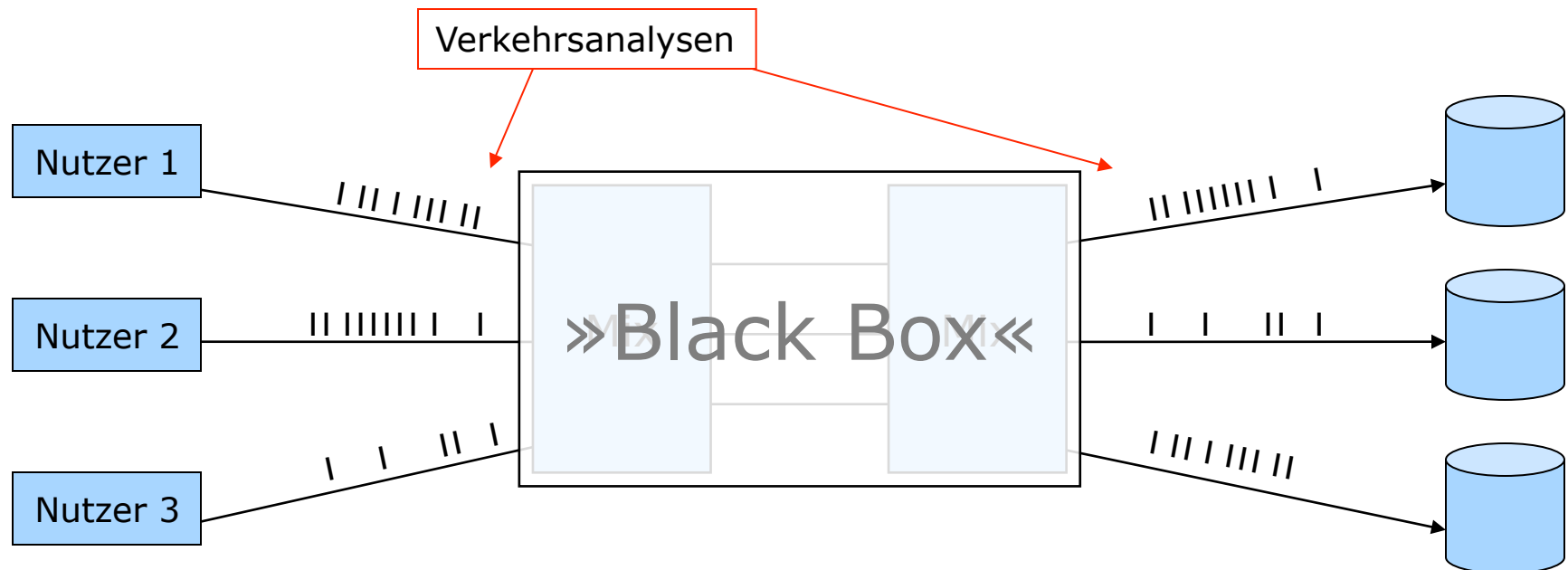
Umkodierende Mixe und praktische Verkettungsangriffe

- Erreichbare Sicherheit

Kommunikationsbeziehung

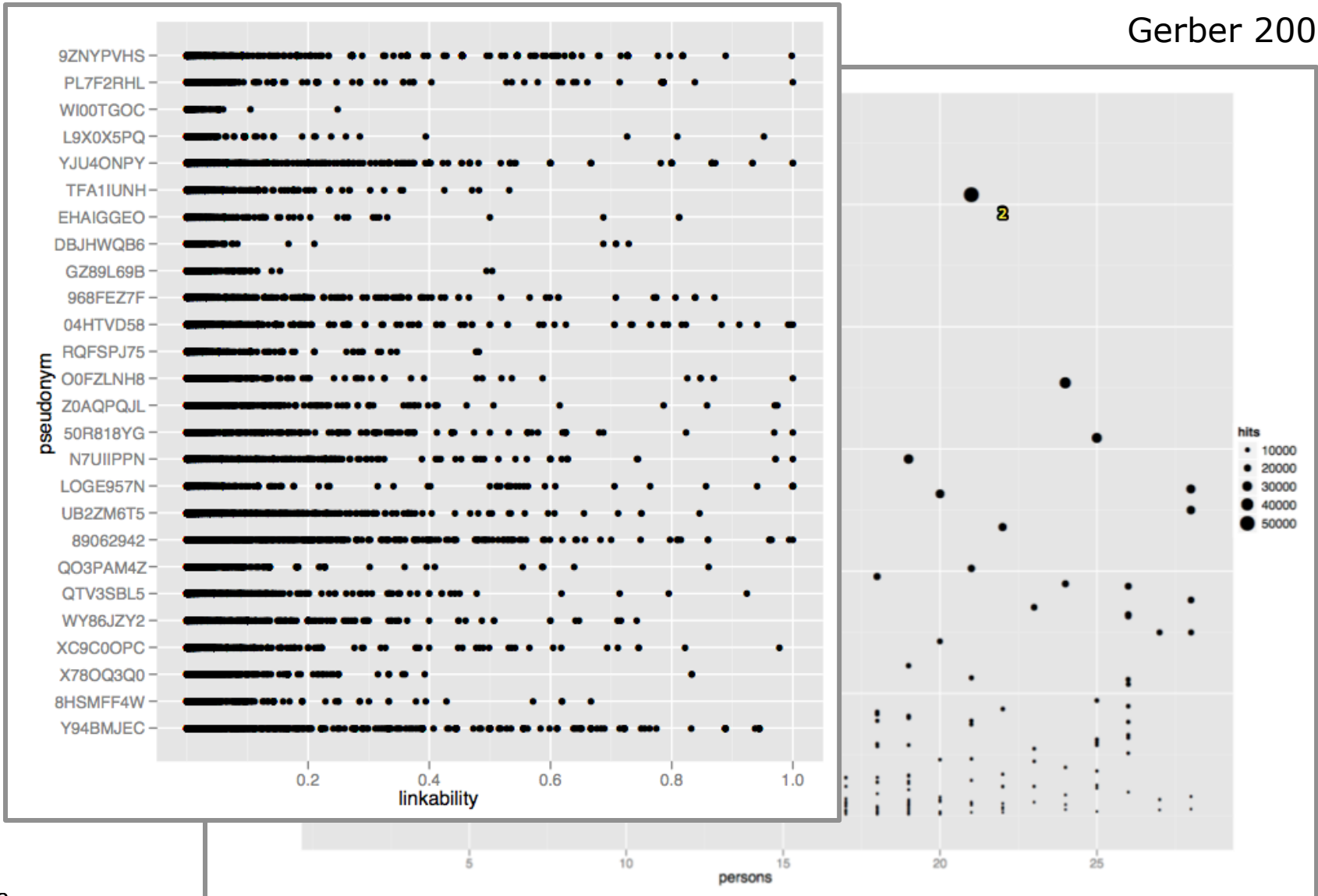
- für einzelne Runde: perfekt (atomare Betrachtung)
- über längere Zeit und mit Kontextinformation
 - Abhängigkeit vom Benutzerverhalten
 - Abhängigkeit von Verkehrssituation

- Beachte: Angreifer ist stets gleich stark



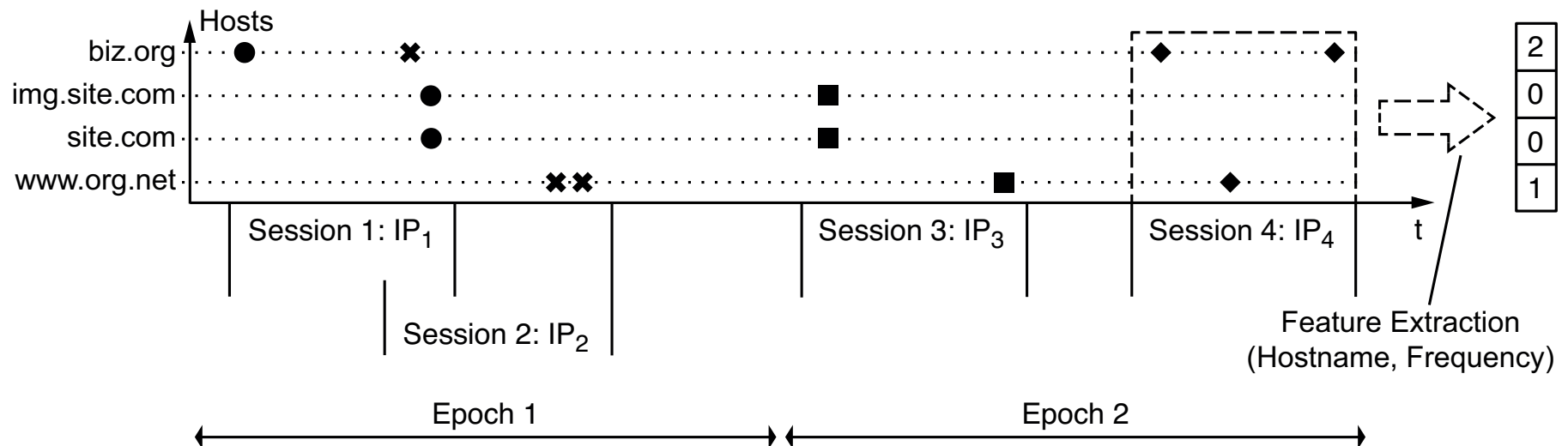
Website- und DNS-Fingerprinting

Gerber 2009



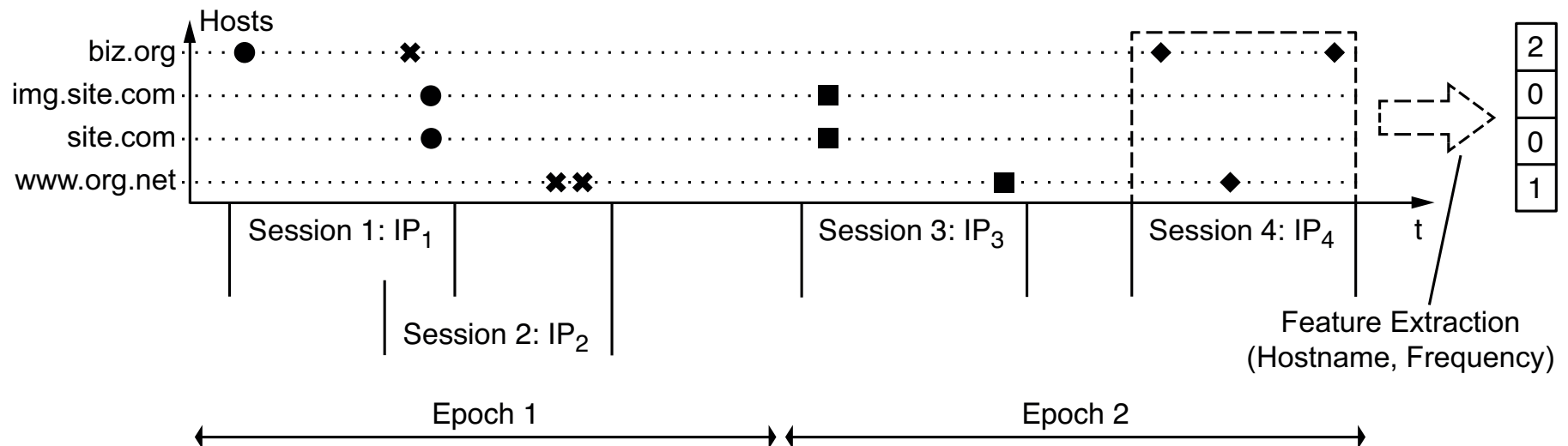
Praktischer Verkettungsangriff auf DNS Black Box

- Annahme
 - Benutzer wechseln täglich ihre IP-Adresse ($t=24h$)
- Hypothese
 - Nutzer können anhand der Menge der angefragten Hostnamen innerhalb einer Session wiedererkannt werden



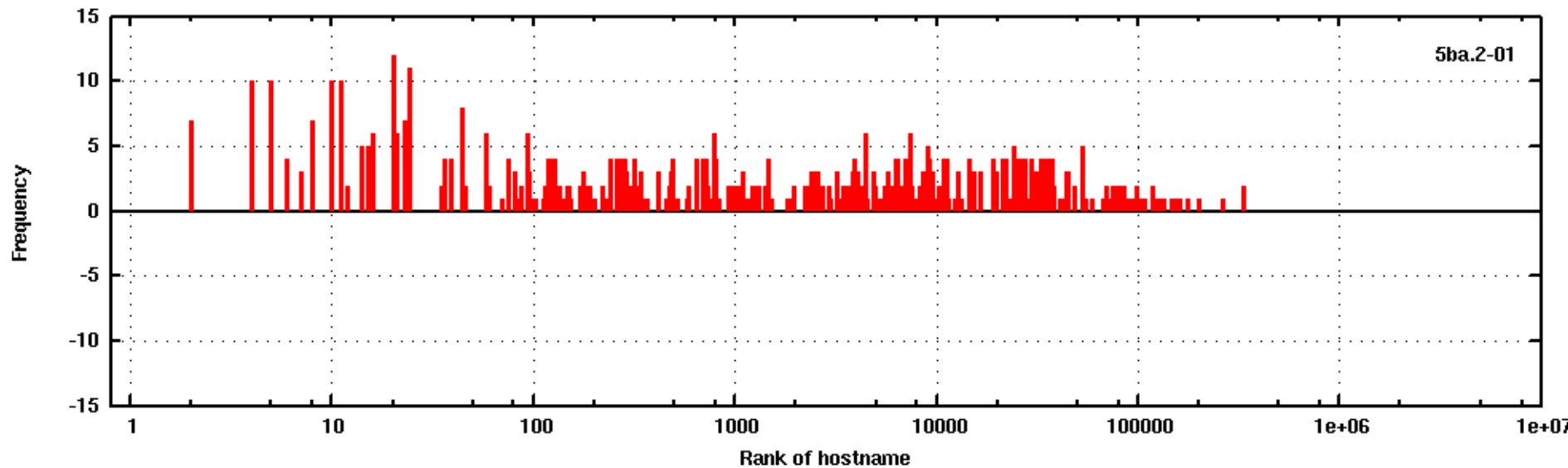
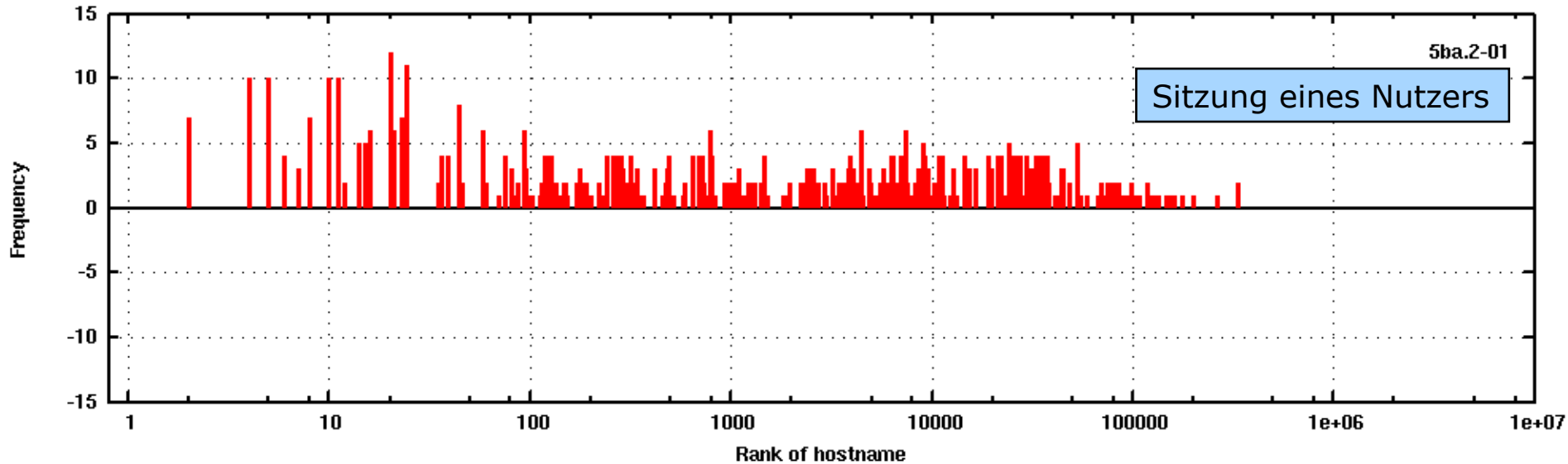
Praktischer Verkettungsangriff auf DNS Black Box

- Annahme
 - Benutzer wechseln täglich ihre IP-Adresse ($t=24h$)
- Hypothese
 - Nutzer können anhand der Menge der angefragten Hostnamen innerhalb einer Session wiedererkannt werden

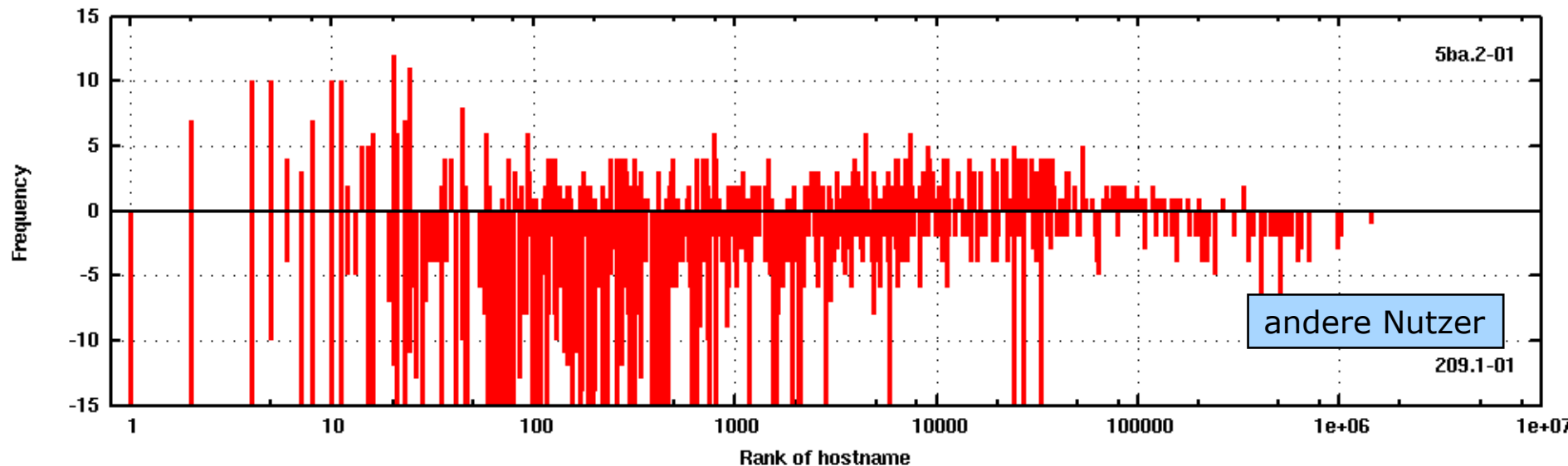
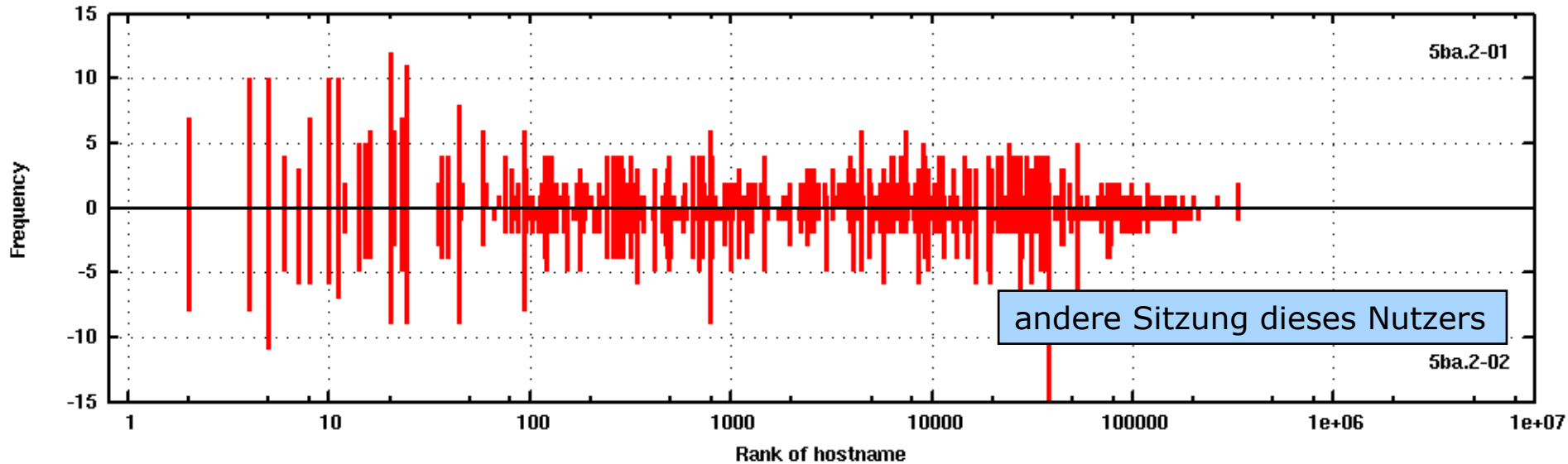


- Datenlage
 - DNS-Anfragen (hostnames) von 4153 Nutzern mit statischen IP-Adressen; Simulation Adresswechsel durch Black Box ($t=24h$)

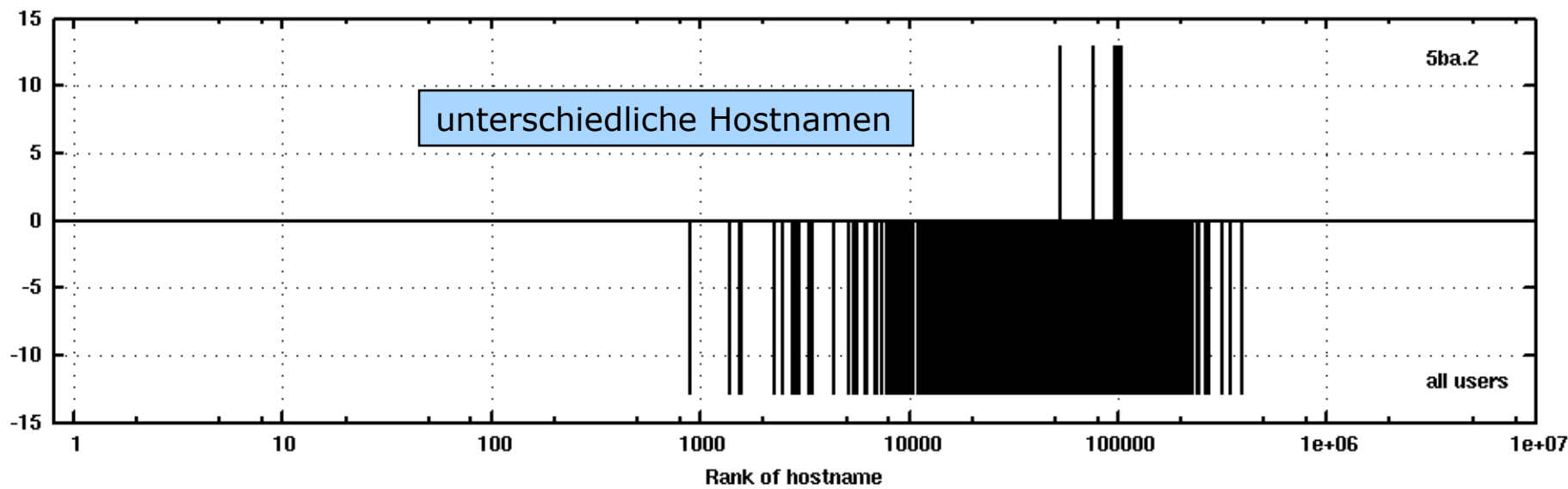
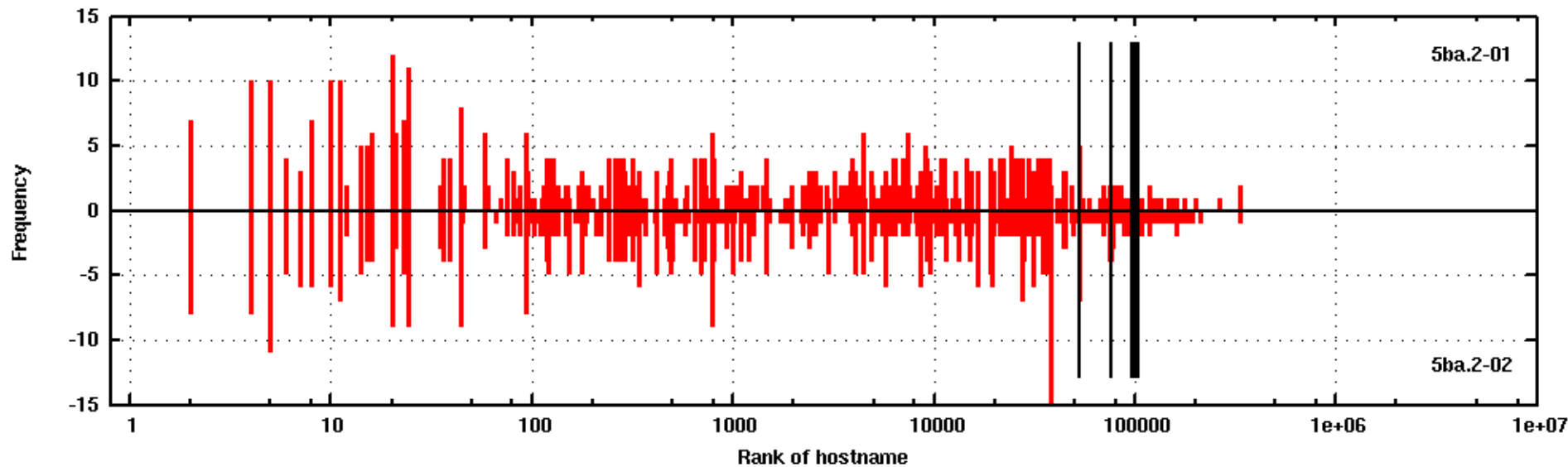
Praktischer Verkettungsangriff auf DNS Black Box



Praktischer Verkettungsangriff auf DNS Black Box

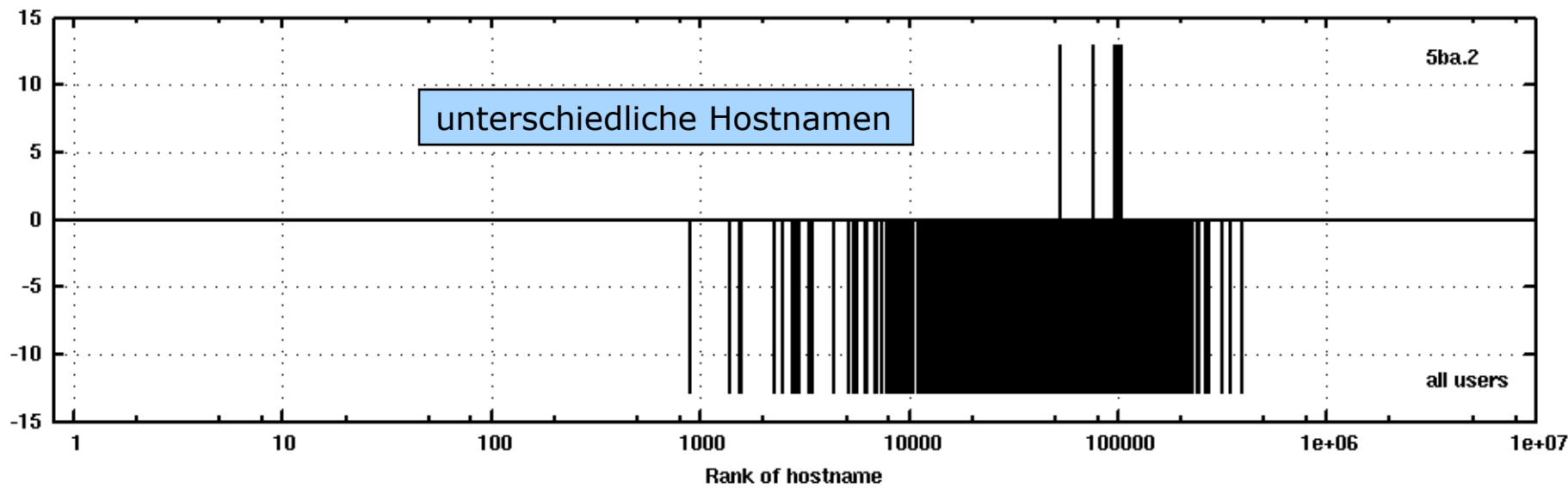


Praktischer Verkettungsangriff auf DNS Black Box



Praktischer Verkettungsangriff auf DNS Black Box

- Ergebnis mit $t=24h$
 - Bis zu 88 Prozent der Nutzer werden (wenigstens einmal) korrekt wiedererkannt ($t=24$).
 - Bis zu 35 Prozent der Nutzer sind ununterbrochen verkettbar (alle Sessions).
- Interessant
 - Mit $t=1h$ halbiert sich jeweils die Erkennungsrate.



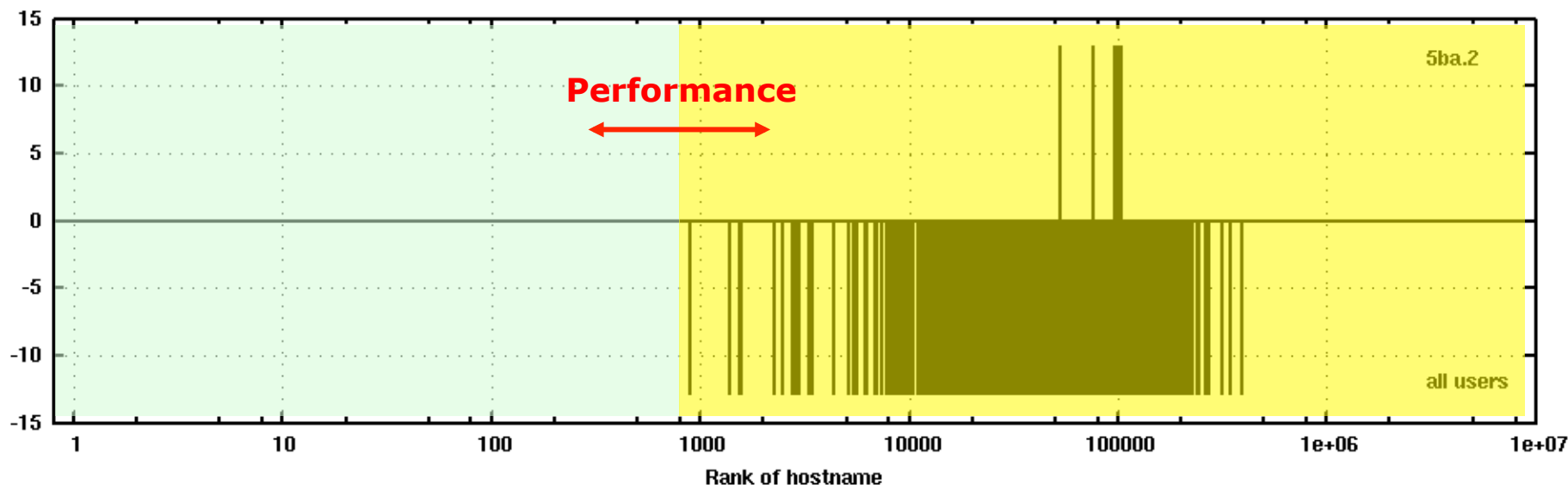
Praktischer Verkettungsangriff auf DNS Black Box

- Zipf's law:
 - Eine geringe Anzahl von Sites erzeugt den Großteil des Datenverkehrs

- Idee:

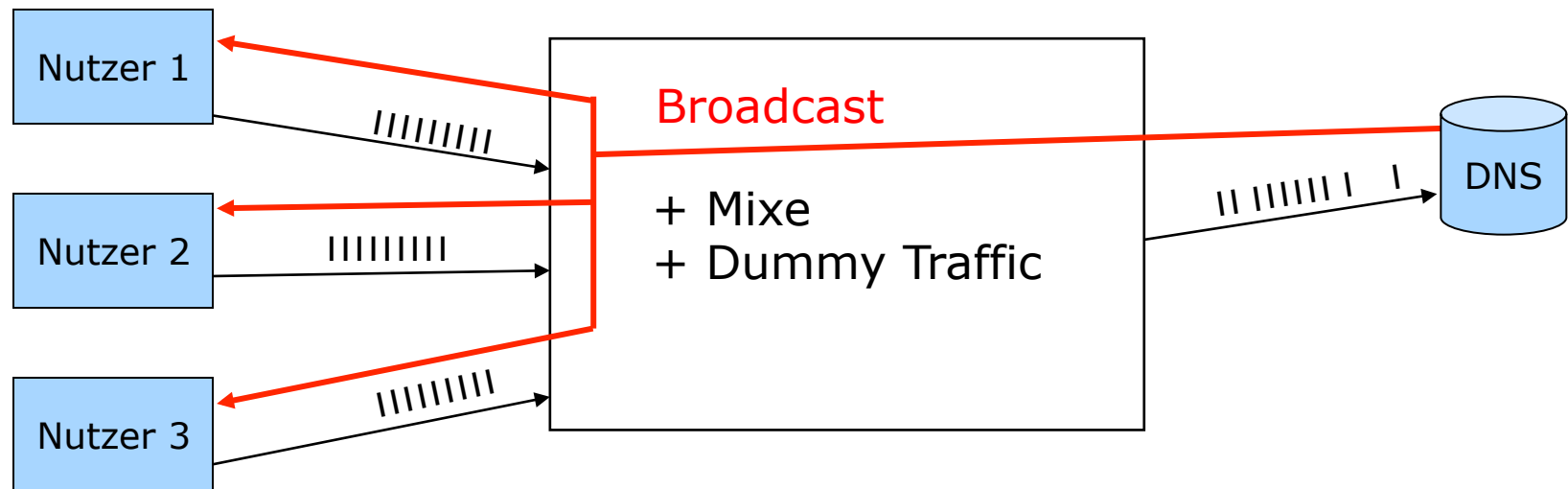
Populärste DNS-Anfragen werden vorab per Broadcast übermittelt (perfekte Unbeobachtbarkeit)

Andere DNS-Anfragen werden über umkodierende Mixe (inkl. Dummy Traffic!) abgefragt.



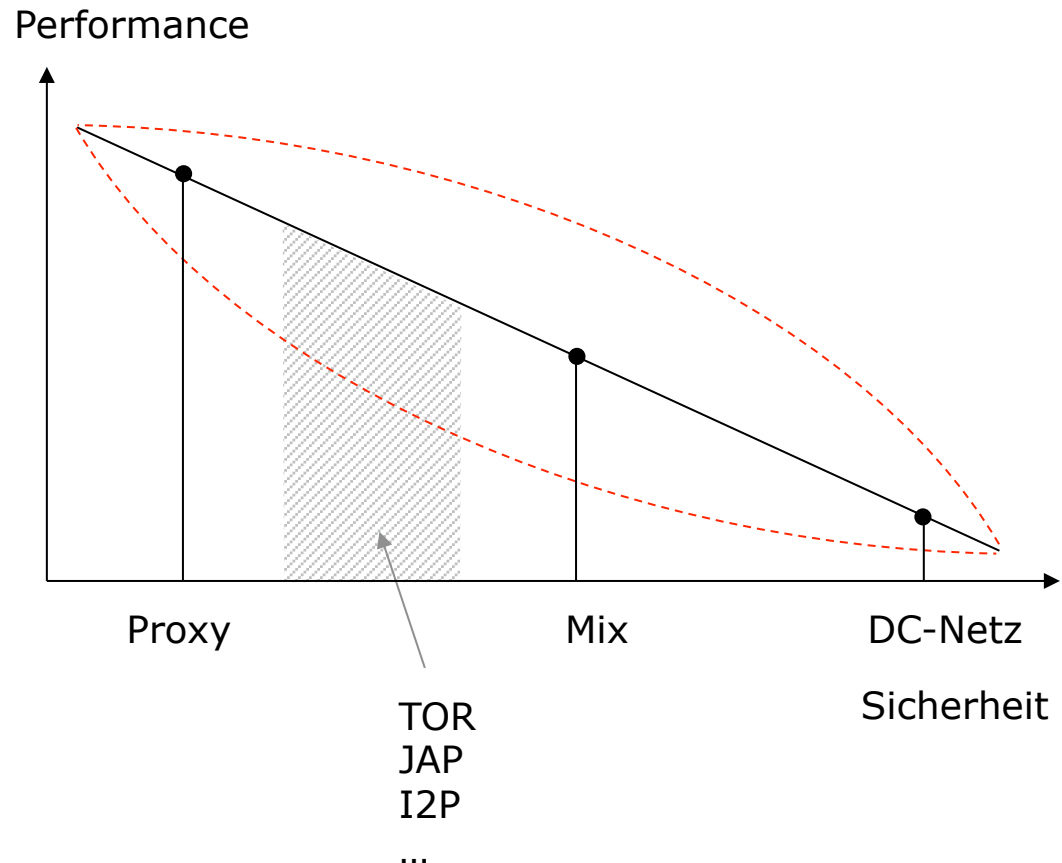
Praktische Unbeobachtbarkeit von DNS

- Mehr als ein Verfahren nutzen Kommunikationsbeziehung
 - Populärste DNS-Anfragen werden vorab per Broadcast übermittelt (perfekte Unbeobachtbarkeit)
 - Andere DNS-Anfragen werden über umkodierende Mixe (inkl. Dummy Traffic!) abgefragt.



Tradeoff zwischen Sicherheit und Performance

- Messbarkeit
 - analytisch
 - simulativ
- Wo liegt das Optimum?
 - technische
 - normative
 - soziale
- Welche sinnvollen Kombinationen der Verfahren existieren?
- Ist das überhaupt ein Tradeoff?
 - Wenig Benutzer = geringe Anonymität



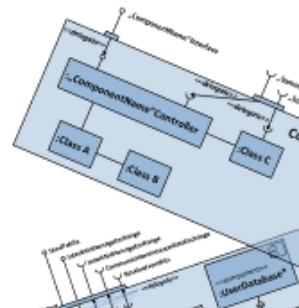
Tradeoff zwischen Sicherheit und Performance

- Messbarkeit
 - analytisch
 - simulativ
 - Wo liegt das
 - technische
 - normative
 - soziale
- Optimum?

- Welche sinnvollen Kombinationen der Verfahren existieren?
- Ist das überhaupt ein Tradeoff?
 - Wenig Benutzer = geringe Anonymität

gMix: A generic Open Source Framework for Mixes

Home Implementations Tutorials People Publications Current Activities Get Involved FAQ



Home

The gMix framework is an [open source \(GPLv3\)](#) Java software framework for [Mix](#) implementations. It is structured in abstraction layers and uses a plug-in mechanism to load individual mix implementations, i.e., it allows to build **Custom Mixes** out of individual plug-ins. gMix is targeted at researchers who want to evaluate and compare their proposals as well as developers interested in building practical mix systems. It contains several **Evaluation Tools** to support these tasks.

In particular, the project **Goals** are to

<http://svs.informatik.uni-hamburg.de/gmix/>



Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

<http://svs.informatik.uni-hamburg.de>