TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur, Professur Datenschutz & Datensicherheit

BEISPIELAUSARBEITUNG FÜR DAS PROSEMINAR

Mickey Mouse

1. April 2016

ABSTRACT

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

INHALTSVERZEICHNIS

1 EINLEITUNG

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

1.1 ÜBERSCHRIFT

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Das hier ist der zweite Absatz. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Und nun folgt – ob man es glaubt oder nicht – der dritte Absatz. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte

möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Nach diesem vierten Absatz beginnen wir eine neue Zählung. Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

1.2 ÜBERSCHRIFT

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

1.3 ÜBERSCHRIFT

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

2 ÜBERSCHRIFT AUF EBENE 0 (CHAPTER)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

2.1 ÜBERSCHRIFT AUF EBENE 1 (SECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

2.1.1 ÜBERSCHRIFT AUF EBENE 2 (SUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

ÜBERSCHRIFT AUF EBENE 3 (SUBSUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Überschrift auf Ebene 4 (paragraph) Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

2.2 LISTEN

2.2.1 BEISPIEL EINER LISTE (ITEMIZE)

- Erster Listenpunkt, Stufe 1
- Zweiter Listenpunkt, Stufe 1
- Dritter Listenpunkt, Stufe 1
- Vierter Listenpunkt, Stufe 1
- Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ITEMIZE)

- Erster Listenpunkt, Stufe 1
  - Erster Listenpunkt, Stufe 2
    - Erster Listenpunkt, Stufe 3
      - Erster Listenpunkt, Stufe 4
      - Zweiter Listenpunkt, Stufe 4
    - Zweiter Listenpunkt, Stufe 3
  - Zweiter Listenpunkt, Stufe 2
- Zweiter Listenpunkt, Stufe 1

2.2.2 BEISPIEL EINER LISTE (ENUMERATE)

1. Erster Listenpunkt, Stufe 1
2. Zweiter Listenpunkt, Stufe 1
3. Dritter Listenpunkt, Stufe 1
4. Vierter Listenpunkt, Stufe 1
5. Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ENUMERATE)

1. Erster Listenpunkt, Stufe 1
    a) Erster Listenpunkt, Stufe 2
        i. Erster Listenpunkt, Stufe 3
            A. Erster Listenpunkt, Stufe 4
            B. Zweiter Listenpunkt, Stufe 4
        ii. Zweiter Listenpunkt, Stufe 3
    b) Zweiter Listenpunkt, Stufe 2
2. Zweiter Listenpunkt, Stufe 1

2.2.3 BEISPIEL EINER LISTE (DESCRIPTION)

Erster Listenpunkt, Stufe 1

Zweiter Listenpunkt, Stufe 1

Dritter Listenpunkt, Stufe 1

Vierter Listenpunkt, Stufe 1

Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*DESCRIPTION)

Erster Listenpunkt, Stufe 1

Erster Listenpunkt, Stufe 2

Erster Listenpunkt, Stufe 3

Erster Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 3

Zweiter Listenpunkt, Stufe 2

Zweiter Listenpunkt, Stufe 1

3 ÜBERSCHRIFT AUF EBENE 0 (CHAPTER)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

3.1 ÜBERSCHRIFT AUF EBENE 1 (SECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

3.1.1 ÜBERSCHRIFT AUF EBENE 2 (SUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

ÜBERSCHRIFT AUF EBENE 3 (SUBSUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Überschrift auf Ebene 4 (paragraph) Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

3.2 LISTEN

3.2.1 BEISPIEL EINER LISTE (ITEMIZE)

- Erster Listenpunkt, Stufe 1
- Zweiter Listenpunkt, Stufe 1
- Dritter Listenpunkt, Stufe 1
- Vierter Listenpunkt, Stufe 1
- Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ITEMIZE)

- Erster Listenpunkt, Stufe 1
  - Erster Listenpunkt, Stufe 2
    - Erster Listenpunkt, Stufe 3
      - Erster Listenpunkt, Stufe 4
      - Zweiter Listenpunkt, Stufe 4
    - Zweiter Listenpunkt, Stufe 3
  - Zweiter Listenpunkt, Stufe 2
- Zweiter Listenpunkt, Stufe 1

3.2.2 BEISPIEL EINER LISTE (ENUMERATE)

1. Erster Listenpunkt, Stufe 1
2. Zweiter Listenpunkt, Stufe 1
3. Dritter Listenpunkt, Stufe 1
4. Vierter Listenpunkt, Stufe 1
5. Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ENUMERATE)

1. Erster Listenpunkt, Stufe 1
    a) Erster Listenpunkt, Stufe 2
        i. Erster Listenpunkt, Stufe 3
            A. Erster Listenpunkt, Stufe 4
            B. Zweiter Listenpunkt, Stufe 4
        ii. Zweiter Listenpunkt, Stufe 3
    b) Zweiter Listenpunkt, Stufe 2
2. Zweiter Listenpunkt, Stufe 1

3.2.3 BEISPIEL EINER LISTE (DESCRIPTION)

Erster Listenpunkt, Stufe 1

Zweiter Listenpunkt, Stufe 1

Dritter Listenpunkt, Stufe 1

Vierter Listenpunkt, Stufe 1

Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*DESCRIPTION)

Erster Listenpunkt, Stufe 1

Erster Listenpunkt, Stufe 2

Erster Listenpunkt, Stufe 3

Erster Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 3

Zweiter Listenpunkt, Stufe 2

Zweiter Listenpunkt, Stufe 1

4 ÜBERSCHRIFT AUF EBENE 0 (CHAPTER)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

4.1 ÜBERSCHRIFT AUF EBENE 1 (SECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

4.1.1 ÜBERSCHRIFT AUF EBENE 2 (SUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

ÜBERSCHRIFT AUF EBENE 3 (SUBSUBSECTION)

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Überschrift auf Ebene 4 (paragraph) Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

4.2 LISTEN

4.2.1 BEISPIEL EINER LISTE (ITEMIZE)

- Erster Listenpunkt, Stufe 1
- Zweiter Listenpunkt, Stufe 1
- Dritter Listenpunkt, Stufe 1
- Vierter Listenpunkt, Stufe 1
- Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ITEMIZE)

- Erster Listenpunkt, Stufe 1
  - Erster Listenpunkt, Stufe 2
    - Erster Listenpunkt, Stufe 3
      - Erster Listenpunkt, Stufe 4
      - Zweiter Listenpunkt, Stufe 4
    - Zweiter Listenpunkt, Stufe 3
  - Zweiter Listenpunkt, Stufe 2
- Zweiter Listenpunkt, Stufe 1

4.2.2 BEISPIEL EINER LISTE (ENUMERATE)

1. Erster Listenpunkt, Stufe 1
2. Zweiter Listenpunkt, Stufe 1
3. Dritter Listenpunkt, Stufe 1
4. Vierter Listenpunkt, Stufe 1
5. Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*ENUMERATE)

1. Erster Listenpunkt, Stufe 1
    a) Erster Listenpunkt, Stufe 2
        i. Erster Listenpunkt, Stufe 3
            A. Erster Listenpunkt, Stufe 4
            B. Zweiter Listenpunkt, Stufe 4
        ii. Zweiter Listenpunkt, Stufe 3
    b) Zweiter Listenpunkt, Stufe 2
2. Zweiter Listenpunkt, Stufe 1

4.2.3 BEISPIEL EINER LISTE (DESCRIPTION)

Erster Listenpunkt, Stufe 1

Zweiter Listenpunkt, Stufe 1

Dritter Listenpunkt, Stufe 1

Vierter Listenpunkt, Stufe 1

Fünfter Listenpunkt, Stufe 1

BEISPIEL EINER LISTE (4*DESCRIPTION)

Erster Listenpunkt, Stufe 1

Erster Listenpunkt, Stufe 2

Erster Listenpunkt, Stufe 3

Erster Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 4

Zweiter Listenpunkt, Stufe 3

Zweiter Listenpunkt, Stufe 2

Zweiter Listenpunkt, Stufe 1

QUELLENVERZEICHNIS

LITERATUR

[2006/24/EG] EG-Richtlinie: *Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Richtlinie über die Vorratsdatenspeicherung)*, Amtsblatt der Europäischen Union, L 105/54, veröffentlicht am 13. April 2006, Inkrafttreten am 3. Mai 2006, 54–60.

[A5-0264/2001] EU-Parlament: *A5-0264/2001 Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) (2001/2098(INI))*, beschlossen am 5. September 2001, Amtsblatt der Europäischen Union, C 72 E, 21. März 2002, 221–230.

[Abe_98] Masayuki Abe: *Universally verifiable mix-net with verification work independent of the number of mix-servers*; Proc. Advances in Cryptology – EUROCRYPT 1998, Springer, Heidelberg / Berlin, LNCS 1403, 1998, 437–447.

[ABHN_06] Luis von Ahn, Andrew Bortz, Nicholas J. Hopper, Kevin O'Neil: *Selectively Traceable Anonymity*; Proc. of Privacy Enhancing Technologies Workshop (PET 2006), LNCS 4258, Springer, Berlin / Heidelberg, 2006, 208–222.

[Acco_05] Rafael Accorsi: *Towards a secure logging mechanism for dynamic systems*; Proc. of the 7th IT Security Symposium, São José dos Campos, Brasilien, November 2005.

[AcDS_03] Alessandro Acquisti, Roger Dingledine, Paul F. Syverson: *On the Economics of Anonymity*; Proc. Financial Cryptography 2003, LNCS 2742, Springer, Berlin / Heidelberg, 1997, 84–102.

[ANSI X9.44-2007] ANSI/X9: *Key Establishment Using Integer Factorization Cryptography*; Accredited Standards Committee X9 Incorporated, 24. August 2007.

[BaCL_04] Endre Bangerter, Jan Camenisch, Anna Lysyanskaya: *Cryptographic Framework for the Controlled Release Of Certified Data*; Proc. of Twelfth International Workshop on Security Protocols, LNCS 3957, Springer, Berlin / Heidelberg, 2004, 20–42.

[BaNe_99] Matthias Baumgart, Heike Neumann: *Bezahlen von Mix-Netz-Diensten*; Verläßliche Informationssysteme (VIS 1999), IT-Sicherheit an der Schwelle des neuen Jahrtausends, Vieweg, Wiesbaden, 1999, 19–33.

[Bara_64] Paul Baran: *On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations*; Memorandum RM-3765-PR, August 1964, The Rand Corporation, 1700 Main St, Santa Monica, California, 90406, http://www.rand.org/pubs/research_memoranda/2006/RM3765.pdf (abgerufen am 25. Oktober 2009), nachgedruckt in: Lance J. Hoffman (ed.): Security and Privacy in Computer Systems; Melville Publishing Company, Los Angeles, California, 1973, 99–123.

[BaYa_60] Paul Baran, Frank Yates: *A Non.Synchronous Digital Data Link Transmission System Using Randomly Surviving Relay Points*; The RAND Corporation, 25. Mai 1960.

[BDDKP_05] Rainer Böhme, George Danezis, Claudia Díaz, Stefan Köpsell, Andreas Pfitzmann: *On the PET Workshop Panel "Mix Cascades Versus Peer-to-Peer: Is One Concept Superior?"*; Proc. of Privacy Enhancing Technologies Workshop (PET 2004), Springer, Berlin / Heidelberg, LNCS 3424, 2005, 243–255, http://citeseer.ist.psu.edu/cache/papers/cs/32954/http:zSzzSzwww.inf.tu-dresden.dezSz~rb21zSzpetpanelzSzpaper.pdf/mix-cascades-vs-peer.pdf, abgerufen am 25. Oktober 2009.

[BeBK_08] Stefan Berthold, Rainer Böhme, Stefan Köpsell: *Data Retention and Anonymity Services*; Proc. The Future of Identity in the Information Society – Challenges for Privacy and Security, FIDIS/IFIP Internet Security & Privacy Fourth International Summer School, Springer, Boston, IFIP Advances in Information and Communication Technology, volume 298, 2009, 92–106.

[BeFK_00] Oliver Berthold, Hannes Federrath, Stefan Köpsell: *Web MIXes: A System for Anonymous and Unobservable Internet Access*; Proc. of Privacy Enhancing Technologies Workshop (PET 2000), Springer, Berlin / Heidelberg, LNCS 2009, Juli 2000, 115–129.

[BeFK_01] Oliver Berthold, Hannes Federrath, Stefan Köpsell: *Praktischer Schutz vor Flooding-Angriffen bei Chaumschen Mixen*; in: Patrick Horster (Hrsg.): Kommunikationssicherheit im Zeichen des Internet. DuD-Fachbeiträge, Vieweg, Wiesbaden, 2001, 235–249.

[BeGr_03] Krista Bennett, Christian Grothoff: *GAP – Practical Anonymous Networking*; Proc. Privacy Enhancing Technologies workshop (PET 2003), Springer, Berlin / Heidelberg, LNCS 2760, 2003, 141–160.

[BeGR_98] Mihir Bellare, Juan A. Garay, Tal Rabin: *Fast Batch Verification for Modular Exponentiation and Digital Signatures*; Proc. Advances in Cryptology – EUROCRYPT 1998, Springer, Heidelberg / Berlin, LNCS 1403, 1998, 236–250.

[BeGS_03] Oliver Berthold, Claudia Golembiewski, Sandra Steinbrecher: *Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes*; in: IT-Sicherheit im verteilten Chaos, Tagungsband zum 8. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI), SecuMedia Verlags GmbH, Ingelheim, 2003, 203.

[BeLa_03] Oliver Berthold, Heinrich Langos: *Dummy Traffic against Long Term Intersection Attacks*; Proc. of Privacy Enhancing Technologies Workshop (PET 2002), Springer, Berlin / Heidelberg, LNCS 2482, 2003, 199–203.

[BePS_00] Oliver Berthold, Andreas Pfitzmann, Ronny Standke: *The disadvantages of free MIX routes and how to overcome them*; Proc. of Privacy Enhancing Technologies Workshop (PET 2000), Springer, Berlin / Heidelberg, LNCS 2009, Juli 2000, 30–45, http://www.springerlink.com/content/89lyh41089kl40jy/fulltext.pdf, abgerufen am 26. Oktober 2009.

[Bert_99] Oliver Berthold: *Effiziente Realisierung von Dummy Traffic zur Gewährleistung von Unbeobachtbarkeit im Internet*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Theoretische Informatik, 13. Dezember 1999.

[Bert_03] Oliver Berthold: *Analyse moderner Mixschemata in offenen Umgebungen*; Proc. of D-A-CH Security, IT-Verlag, 2003.

[BeYe_97] Mihir Bellare, Bennet S. Yee: *Forward integrity for secure audit logs*; Technischer Bericht, University of California at San Diego, Dept. of Computer Science & Engineering, 1997.

[BGGMM_97] Daniel Bleichenbacher, Eran Gabber, Phillip B. Gibbons, Yossi Matias, A. Mayer: *On personalized yet anonymous interaction*; Technical report, Bell Laboratories, April 1997.

[BKA_02] Bundeskriminalamt KI 11 – SKA: *Notwendigkeiten, Möglichkeiten und Perspektiven der Bekämpfung von Internet-Kriminalität*; Abschlussbericht zum Projekt der Strategischen Kriminalitätsanalyse (SKA) im Bundeskriminalamt, überarbeitete Fassung vom Juni 2002.

[Bloo_70] Burton H. Bloom: *Space/time trade-offs in hash coding with allowable errors*; Communications of the ACM, vol. 13, Nr. 7, ACM, New York, Juli 1970, 422–426.

[BoBo_90] Jurjen Bos, Bert den Boer: *Detection of Disrupters in the DC Protocol*; Proc. Advances in Cryptology – EUROCRYPT 1989, Springer, Berlin / Heidelberg, LNCS 434, 1990, 320–327.

[Böhm_08] Rainer Böhme: *Improved Statistical Steganalysis using Models of Heterogeneous Cover Signals*, Dissertation, Technische Universität Dresden, Fakultät Informatik, Dresden, 2008.

[BoMa_03] Colin Boyd, Anish Mathuris: *Protocols for Authentication and Key Establishment*; Springer, Berlin / Heidelberg, 2003.

[Bund_07] Bundesregierung: *Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*; Bundesdrucksache 275/07, Bundesanzeiger, 27. April 2007, `http://www.bmj.bund.de/media/archive/2603.pdf`, abgerufen am 25. Oktober 2009.

[Bund_07a] Bundestag: *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007*; Bundesgesetzblatt, Bonn, 2007, 3198–3211.

[CaGJ_99] Ran Canetti, Rosario Gennaro, Stanislaw Jarecki: *Adaptive Security for Threshold Cryptosystems*; Proc. Advances in Cryptology – CRYPTO '99, LNCS 1666, Springer, Berlin / Heidelberg, 1999, 98–115.

[CaGr_04] Jan Camenisch, Jens Groth: *Group Signatures: Better Efficiency and New Theoretical Aspects*; Proc. of Security in Communication Networks (SCN 2004), LNCS 3352, Springer, Berlin / Heidelberg, 2004, 120–133.

[CaKW_04] Jan Camenisch, Maciej Koprowski, Bogdan Warinschi: *Efficient Blind Signatures without Random Oracles*, Proc. of Security in Communication Networks (SCN 2004), Springer, Berlin / Heidelberg, LNCS 3352, 2004, 134–148.

[CaLy_04] Jan Camenisch, Anna Lysyanskaya: *Signature Schemes and Anonymous Credentials from Bilinear Maps*; Proc. Advances in Cryptology – CRYPTO 2004, LNCS 3152, Springer, Berlin / Heidelberg, 2004, 56–72.

[CCRT_90] Robert B. Cleveland, William S. Cleveland, Jean E. McRae, Irma Terpenning: *STL: A Sesonal-Trend Decomposition Procedure Based on Loess*; Journal of Official Statistics, vol. 6, Nr. 1, 1990, 3–73.

[Chau_81] David Chaum: *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*; Communications of the ACM 24/2, 1981, 84–88.

[Chau_85] David Chaum: *Security Without Identification: Transaction Systems to Make Big Brother Obsolete*; Communications of the ACM, vol. 28, Nr. 10, Oktober 1985, 1030–1044.

[Chau_88] David Chaum: *The dining cryptographers problem: Unconditional sender and recipient untraceability*; Journal of Cryptology, Springer, New York, vol. 1, Nr. 1, Januar 1988, 65–75.

[Clau_07] Sebastian Clauß: *Towards Quantification of Privacy Within a Privacy-Enhancing Identity Management System*, Dissertation, Technische Universität Dresden, Fakultät Informatik, Dresden, 2007.

[ClDí_03] Joris Claessens, Claudia Díaz, Svetla Nikova, Vincent Naessens, Bart De Win, Caroline Goemans, Stefaan Seys, Mieke Loncke, Jos Dumortier, Bart De Decker, Bart Preneel: *APES, Anonymity and Privacy in Electronic Services, Deliverable 10, Technologies for controlled anonymity*; September 2003, 34–40, `https://www.cosic.esat.kuleuven.be/publications/article-105.pdf`, abgerufen am 26. Oktober 2009.

[ClOA_07] Jeremy Clark, Paul C. van Oorschot, Carlisle Adams: *Usability of anonymous web browsing: an examination of Tor interfaces and deployability*; Proc. 3rd Symposium On Usable Privacy and Security (SOUPS 2007), ACM International Conference Proceeding Series, vol. 229, ACM, New York, 2007, 41–51.

[ClSc_06] Sebastian Clauß, Stefan Schiffner: *Structuring anonymity metrics*; Proc. Workshop on Digital Identity Management (DIM 2006), ACM, New York, 2006, 55–62.

[CrGa_05] Lorrie F. Cranor, Simson Garfinkel (Editoren): *Security and Usability: Designing Secure Systems that People Can Use*; O'Reilly, 1. Auflage, August 2005.

[Dane_03] George Danezis: *Mix-Networks with Restricted Routes*; Proc. of Privacy Enhancing Technologies Workshop (PET 2003), Springer, Berlin / Heidelberg, LNCS 2760, März 2003, 1–17, `http://research.microsoft.com/en-us/um/people/gdane/papers/ExpMix.pdf`, abgerufen am 25. Oktober 2009.

[Dane_03a] George Danezis: *Statistical disclosure attacks: Traffic confirmation in open environments*; Proc. of Security and Privacy in the Age of Uncertainty (SEC 2003), Kluwer, 2003, 421–426.

[Dane_05] George Danezis: *The Traffic Analysis of Continuous-Time Mixes*; Proc. of Privacy Enhancing Technologies Workshop (PET 2004), Springer, Berlin / Heidelberg, LNCS 3424, 2005, 35–50.

[DaCl_06] George Danezis, Richard Clayton: *Route Fingerprinting in Anonymous Communications*; Proc. Sixth IEEE International Conference on Peer-to-Peer Computing, IEEE Computer Society, 2006, 69–72.

[DaLa_07] George Danezis, Ben Laurie: *Minx: a simple and efficient anonymous packet format*; Proc. of the 2004 ACM workshop on Privacy in the electronic society, ACM, New York, 2004, 59–65.

[DaSe_04] George Danezis, Andrei Serjantov: *Statistical Disclosure or Intersection Attacks on Anonymity Systems*; Proc. of Information Hiding Workshop (IH 2004), Springer, Berlin / Heidelberg, LNCS 3200, 2004, 293–308.

[DeKu_00] Yvo Desmedt, Kaoru Kurosawa: *How to break a practical mix and design a new one*; Proc. Advances in Cryptology – EUROCRYPT 2000, Springer, Berlin /Heidelberg, LNCS 1807, 2000, 557–572.

[DeRi_98] Thomas Demuth, Andreas Rieke: *Anonym im World Wide Web? Janus – Schutz von Inhalteanbietern im WWW*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 11, November 1998, 623–627.

[DeRi_99] Thomas Demuth, Andreas Rieke: *On Securing the Anonymity of Content Providers in the World Wide Web*; Proc. of SPIE, vol. 3657, April 1999, 494–502.

[DiMS_04] Roger Dingledine, Nick Mathewson, Paul F. Syverson: *Tor: The Second-Generation Onion Router*; Proc. of the 13th USENIX Security Symposium, August 2004, 303–320, `http://www.usenix.org/publications/library/proceedings/sec04/tech/full_papers/dingledine/dingledine.pdf`, abgerufen am 25. Oktober 2009.

[DIN EN ISO 9000:2005] Normenausschuss Qualitätsmanagement, Statistik und Zertifizierungsgrundlagen (NQSZ) im DIN: *DIN EN ISO 9000: Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2005); Dreisprachige Fassung EN ISO 9000:2005*; DIN Deutsches Institut für Normung e. V., Berlin, Dezember 2005.

[DíPr_04a] Claudia Díaz, Bart Preneel: *Reasoning About the Anonymity Provided by Pool Mixes That Generate Dummy Traffic*; Proc. of Information Hiding Workshop (IH 2004), Springer, Berlin / Heidelberg, LNCS 3200, 2004, 309–325.

[DíPr_04b] Claudia Díaz, Part Preneel: *Taxonomy of Mixes and Dummy Traffic*; Proc. I-NetSec04 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems, in: Information Security Management, Education and Privacy, Kluwer, 2004, 217–232.

[DíSD_04] Claudia Díaz, Len Sassaman, Evelyne Dewitte: *Comparison Between Two Practical Mix Designs*; Proc. of ESORICS 2004, Springer, Berlin / Heidelberg, LNCS 3193, 2004, 141–159.

[DíSe_03] Claudia Díaz, Andrei Serjantov: *Generalising Mixes*; Proc. of Privacy Enhancing Technologies Workshop (PET 2003), Springer, Berlin / Heidelberg, LNCS 2760, 2003, 18–31.

[DiSS_05] Roger Dingledine, Vitaly Shmatikov, Paul F. Syverson: *Synchronous Batching: From Cascades to Free Routes* ; Proc. of Privacy Enhancing Technologies Workshop (PET 2004), Springer, Berlin / Heidelberg, LNCS 3424, 2005, 186–206.

[Doch_08] Sebastian Dochow: *Blockresistenz unter Benutzung von Skype*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, September 2008.

[Douc_02] John R. douceur: *The Sybil Attack*; Proc. of 1st Intl. Workshop on Peer-to-Peer Systems, Springer Berlin / Heidelberg, LNCS 2429, 2002, 251–260.

[DSCP_03] Claudia Díaz, Stefaan Seys, Joris Claessens, Bart Preneel: *Towards Measuring Anonymity*; Proc. of Privacy Enhancing Technologies Workshop (PET 2002), Springer, Berlin / Heidelberg, LNCS 2482, 2003, 184–188.

[EiFr_08] Birgit van Eimeren, Beate Frees: *Internetverbreitung: Größter Zuwachs bei Silver-Surfern*, Ergebnisse der ARD/ZDF-Onlinestudie 2008, Media Perspektiven, Heft 7, ARD-Werbung SALES & SERVICES GmbH, Frankfurt am Main, Juli 2008, 330–344, http://www.media-perspektiven.de/uploads/tx_mppublications/Eimeren_I.pdf, abgerufen am 10. März 2009.

[ETSI TS 102 656] ETSI: *Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data*; Version 1.2.1, European Telecommunications Standards Institute (ETSI), Technische Spezifikation, TS 102 656, Dezember 2008.

[ETSI TS 102 657] ETSI: *Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data*; Version 1.2.1, European Telecommunications Standards Institute (ETSI), Technische Spezifikation, TS 102 657, Juni 2009.

[ETSI TR 102 661] ETSI: *Lawful Interception (LI); Security framework in Lawful Interception and Retained Data environment*; Version 1.1.1, European Telecommunications Standards Institute (ETSI), Technischer Bericht, TR 102 661, November 2008.

[Fede_05] Hannes Federrath: *Privacy Enhanced Technologies: Methods — Markets — Misuse*; Proc. Trust, Privacy and Security in Digital Business (TrustBus 2005), Springer, Berlin / Heidelberg, LNCS 3592, 2005, 1–9.

[FeGo_04] Hannes Federrath, Claudia Golembiewski: *Speicherung von Nutzungsdaten durch Anonymisierungdienste im Internet. Welche strafprozessualen Vorschriften zur Überwachung der Telekommunikation sind auf Anonymisierungsdienste anwendbar?*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 8, August 2004, 486–490.

[FeKL_02] Hannes Federrath, Stefan Köpsell, Heinrich Langos: *Anonyme und unbeobachtbare Kommunikation im Internet*; Proc. GI-Jahrestagung 2002, Informatik bewegt, Lecture Notes in Informatics (P-19), Köllen, Bonn 2002, 481–488.

[FePö_08] Hannes Federrath, Wolfgang Pöppl: *Detektion von anonym abgerufenen rechtswidrigen Inhalten mit einem hashwertbasierten Datenscanner*; in Ammar Alkassar, Jörg H. Siekmann (Eds.): SICHERHEIT 2008, Sicherheit – Schutz und Zuverlässigkeit, Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V., LNI P-128, Gesellschaft für Informatik, Bonn, 2008, 59–70.

[FGBZ_03] Xinwen Fu, Bryan Graham, Riccardo Bettati, Wei Zhao: *On Effectiveness of Link Padding for Statistical Traffic Analysis Attacks*; Proc. 23rd International Conference on Distributed Computing Systems, IEEE Computer Society, 2003, 340–??.

[FIPS 180-2] NIST: *Federal Information Processing Standards Publication 180-2: Specifications for the SECURE HASH STANDARD*; U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), 1. August 2002, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf, abgerufen am 16. Februar 2009.

[FIPS 197] NIST: *Federal Information Processing Standards Publication 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES)*; U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), 26. November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, abgerufen am 16. Februar 2009.

[FlashEB 225] Flash Eurobarometer: *Data Protection in the European Union – Citizens' perceptions – Analytical Report*; Flash Eurobarometer 225, Europäische Kommission, 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf, abgerufen am 10. März 2009.

[FrJe_98] Elke Franz, Anja Jerichow: *A Mix-Mediated Anonymity Service and Its Payment*; ESORICS '98 (5th European Symposium on Research in Computer Security), LNCS 1485, Springer, Berlin, 1998, 313–327.

[FrJW_98] Elke Franz, Anja Jerichow, Guntram Wicke: *Payment Scheme for Mixes Providing Anonymity*; IFIP Working Conference on Electronic Commerce 98, LNCS 1402, Springer, Berlin, 1998, 94–108.

[FrMo_02] Michael J. Freedman, Robert Morris: *Tarzan: a peer-to-peer anonymizing network layer*; Proc. 9th ACM Conference on Computer and Communications Security (CCS 2002), ACM, New York, 2003, 193–206.

[FSCM_02] Michael J. Freedman, Emil Sit, Josh Cates, Robert Morris: *Introducing Tarzan, A Peer-to-Peer Anonymizing Network Layer*; Proc. of 1st Intl. Workshop on Peer-to-Peer Systems, Springer Berlin / Heidelberg, LNCS 2429, 2002, 121–129.

[FuTI_06] Kazuyoshi Furukawa, Masahiko Takenaka, Kouichi Itoh: *A Fast RSA Implementation on Itanium 2 Processor*; Proc. Information and Communications Security 2006, LNCS 4307, Springer, Berlin, 2006, 507–518.

[GeTi_03] Rainer W. Gerling, Marie-Theres Tinnefeld: *Anonymität im Netz. Einige Gedanken zum Heft 3/2003*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 5, Mai 2003, 305.

[Ger_04] Marco Gercke: *Die Protokollierung von Nutzerdaten. Zu den Ermittlungsmaßnahmen gegen JAP nach § 100 g/h StPO*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 4, April 2004, 210–214.

[Gerd_04] Daniela Gerd tom Markotten: *Benutzbare Sicherheit in informationstechnischen Systemen*; Rhombos Verlag, März 2004.

[GGMM_97] Eran Gabber , Phillip B. Gibbons, Yossi Matias, Alain Mayer: *How to make personalized web browsing simple, secure, and anonymous*; Proc. Financial Cryptography 1997, LNCS 1318, Springer, Berlin / Heidelberg, 1997, 17–31.

[GHCP_04] Dennis F. Galletta, Raymond Henry, Scott McCoy, Peter Polak: *Web Site Delays: How Tolerant are Users?*; Journal of the Association for Information Systems, vol. 5, Nr. 1, Januar 2004, 1–28.

[GiSc_07] Rotraud Gitter, Christoph Schnabel: *Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das nationale Recht*; Multimedia und Recht (MMR), Zeitschrift für Informations-, Telekommunikations- und Medienrecht, C. H. Beck, München, Heft 7, Juli 2007, 411–416.

[Glob_06] GlobalPlatform: *Card Specifiaction*; Version 2.2, März 2006, `http://www.globalplatform.org/specificationscard.asp`, abgerufen am 5. Dezember 2008.

[Gol_03] Claudia Golembiewski: *Das Recht auf Anonymität im Internet – Gesetzliche Grundlagen und praktische Umsetzung*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 3, März 2003, 129–133.

[Gol_03a] Claudia Golembiewski: *AN.ON: Der Staatsanwalt hat geklingelt*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 10, Oktober 2003, 596.

[Go_05] Philippe Gollé: *Reputable Mix Networks*; Proc. of Privacy Enhancing Technologies Workshop (PET 2004), Springer, Berlin / Heidelberg, LNCS 3424, 2005, 51–62.

[GoJu_04] Philippe Golle, Ari Juels: *Dining Cryptographers Revisited*; Proc. Advances in Cryptology – EUROCRYPT 2004, Springer, Berlin /Heidelberg, LNCS 3027, 2004, 456–473.

[GoRS_96] David M. Goldschlag, Michael G. Reed, Paul F. Syverson: *Hiding Routing Information*; Proc. of Information Hiding Workshop (IH 1996), Springer, Berlin / Heidelberg, LNCS 1174, 1996, 137–150.

[GPSS_06] Martin Geppert (Herausgeber), Hermann-Josef Piepenbrock (Herausgeber), Raimund Schütz (Herausgeber), Fabian Schuster (Herausgeber): *Beck'scher TKG-Kommentar: Telekommunikationsgesetz*; 3. Auflage, Beck Juristischer Verlag, September 2006.

[GrVi_05] David A. McGrew, John Viega: *The Security and Performance of the Galois/Counter Mode (GCM) of Operation*; Proc. of Progress in Cryptology – INDOCRYPT 2004, Springer, Berlin / Heidelberg, LNCS 3348, 2005, 343–355.

[GTDP_08] Benedikt Gierlichs, Carmela Troncoso, Claudia Diaz, Bart Preneel, Ingrid Verbauwhede: *Revisiting A Combinatorial Approach Toward Measuring Anonymity*; Proc. Workshop on Privacy in the Electronic Society (WPES 2008), ACM, New York, 2008, 111–116.

[Guer_09] Shay Gueron: *Intel's New AES Instructions for Enhanced Performance and Security*; Proc. Fast Software Encryption, Springer Berlin / Heidelberg, LNCS 5665, 2009, 51–66.

[GZFB_05] Bryan Graham, Ye Zhu, Xinwen Fu, Riccardo Bettati: *Using Covert Channels to Evaluate the Effectiveness of Flow Confidentiality Measures*; Proc. 11th International Conference on Parallel and Distributed Systems, IEEE Computer Society, 2005, 57–63.

[Hams_01] Martin Gregor Hamsch: *Entwurf und Implementierung einer Infrastruktur zur Durchsetzung der Schutzziele Integrität und Zurechenbarkeit für die Metainformationen eines Anonymisierungsdienstes*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, Dezember 2001.

[HåNå_04] Johan Håstad, Mats Nåslund: *The security of all RSA and discrete log bits*; Journal of the ACM, vol. 51, Nr. 2, März 2004, 187–230.

[Herr_08] Dominik Herrmann: *Analyse von datenschutzfreundlichen Übertragungstechniken hinsichtlich ihres Schutzes vor Datenverkehrsanalysen im Internet*; Diplomarbeit, Universität Regensburg, Wirtschaftswissenschaftliche Fakultät, Institut für Wirtschaftsinformatik, 19. März 2008.

[Hill_03] Ulf Hillig: *Blockungsresistente anonyme Webzugriffe*; Diplomarbeit, Hochschule für Technik und Wirtschaft Dresden (FH), Fachbereich Elektrotechnik, August 2003.

[HoDi_00] John A. Hoxmeier, Chris DiCesare: *System Response Time and User Satisfaction: An Experimental Study of Browser-based Applications*, Proc. Americas Conference on Information Systems (AMCIS 2000), Long Beach California, August 2000, 140–145.

[HOII_05] Osamu Honda, Hiroyuki Ohsaki, Makoto Imase, Mika Ishizuka, Junichi Murayama: *Understanding TCP over TCP: Effects of TCP Tunneling on End-to-End Throughput and Latency*; Proc. of SPIE, vol. 6011, 60110H, 24. Oktober 2005,

[IEEE 1363a-2004] IEEE Computer Society: *1363a™ IEEE Standard Specification for Public-Key Cryptography–Amendment 1: Additional Techniques*; IEEE Computer society, New York, USA, 2. September 2004, `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1335427\&isnumber=29460`, abgerufen am 16. Februar 2009.

[ISO/IEC 10118-3:2004] ISO/IEC JTC 1/SC 27: *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*, ISO/IEC International Standard, ISO/IEC 10118-3:2004, 2004.

[ISO/IEC 11770-3:2008] ISO/IEC JTC 1/SC 27: *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*; ISO/IEC International Standard, ISO/IEC 11770-3:2008, 15. Juli 2008.

[ISO/IEC 14882:1998] ISO/IEC JTC 1/SC 22: *Programming Language – C++*; ISO/IEC International Standard, ISO/IEC 14882:1998, 1. September 1998.

[ISO/IEC 18033-2:2006] ISO/IEC JTC 1/SC 27: *Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers*; ISO/IEC International Standard, ISO/IEC 23001-1:2006, 8. Mai 2006.

[ISO/IEC 23001-1:2006] ISO/IEC JTC 1/SC 29: *Information technology – MPEG systems technologies – Part 1: Binary MPEG format for XML*; ISO/IEC International Standard, ISO/IEC 23001-1:2006, 24. März 2006.

[ISO/IEC 25000:2005] ISO/IEC JTC 1/SC 7: *Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE*; ISO/IEC International Standard, ISO/IEC 25000:2005, 1. August 2005.

[ITU-T X.690] ITU-T: *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*; Telecommunication Standardization Sector of ITU, ITU-T Recommendation X.690, Juli 2002, `http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf`, abgerufen am 11. Februar 2009.

[Jak_98] Markus Jakobsson: *A practical mix*; Proc. Advances in Cryptology – EUROCRYPT 1998, Springer, Heidelberg / Berlin, LNCS 1403, 1998, 448–461.

[Jak_99] Markus Jakobsson: *Flash mixing*; Proc. of Eighteenth ACM Symposium on Principles of Distributed Computing (PODC 99), ACM, New York, 1999, 83–89.

[Jak_99b] Markus Jakobsson: *On Quorum Controlled Asymmetric Proxy Re-encryption*; Proc. of the Second International Workshop on Practice and Theory in Public Key Cryptography, Springer, Berlin / Heidelberg, LNCS 1560, 1999, 112–121.

[JSR-056] Andy Herrick (Editor): *Java™ Network Launching Protocol & API Specification (JSR-56) Version 6.0.10*; Java Specification Request 56, Sun Microsystems, Inc., 18. August 2008.

[KeEB_98] Dogan Kesdogan, Jan Egner, Roland Büschkes: *Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System*; Proc. of Information Hiding Workshop (IH 1998), Springer, Berlin / Heidelberg, LNCS 1525, 1998, 83–98.

[KePi_04] Dogan Kesdogan, Lexi Pimenidis: *The Hitting Set Attack on Anonymity Protocols*; Proc. of Information Hiding Workshop (IH 2004), Springer, Berlin / Heidelberg, LNCS 3200, 2004, 326–339.

[Klei_08] Andreas Klein: *Attacks on the RC4 stream cipher*; Designs, Codes and Cryptography, vol. 48, Nr. 3, Springer Netherlands, September 2008, 269–286.

[Koç_94] Çetin Kaya Koç: *High-Speed RSA Implementation*; Technischer Bericht TR 201, RSA Laboratories, RSA Data Security, Inc., November 1994, `ftp://ftp.rsasecurity.com/pub/pdfs/tr201.pdf`, abgrufen am 20. Mai 2009.

[KöFH_03] Stefan Köpsell, Hannes Federrath, Marit Hansen: *Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 3, März 2003, 139–141.

[KöHi_04] Stefan Köpsell, Ulf Hillig: *How to achieve blocking resistance for existing systems enabling anonymous web surfing*; in Vijay Atluri, Paul F. Syverson, Sabrina De Capitani di Vimercati (Eds.): Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, WPES 2004, Washington, DC, USA, 28. Oktober 2004, ACM, 2004, 47–58.

[KöMi_05] Stefan Köpsell, Tobias Miosga: *Strafverfolgung trotz Anonymität – Rechtliche Rahmenbedingungen und technische Umsetzung*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Heft 7, Juli 2005, 403–409.

[KöMü_03] Stefan Köpsell, Andreas Müller: *Bezahlsystem für einen Mixkaskaden-basierten Anonymisierungsdienst*; in Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Eds.): INFORMATIK 2003 – Mit Sicherheit Informatik, Schwerpunkt „Sicherheit – Schutz und Zuverlässigkeit", 29. September – 2. Oktober 2003 in Frankfurt am Main, LNI P-36, Gesellschaft für Informatik, Bonn, 2003, 305–316.

[Köps_06] Stefan Köpsell: *Low Latency Anonymous Communication — How Long Are Users Willing to Wait?*; Emerging Trends in Information and Communication Security (ETRICS 2006), Springer, Berlin / Heidelberg, LNCS 3995, 2006, 221–237.

[Köps_06a] Stefan Köpsell: *Vergleich der Verfahren zur Verhinderung von Replay-Angriffen der Anonymisierungsdienste AN.ON und Tor*; in Jana Dittmann (Ed.): SICHERHEIT 2006, Sicherheit – Schutz und Zuverlässigkeit, Konferenzband der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V., LNI P-77, Gesellschaft für Informatik, Bonn, 2006, 183–187.

[KöWF_06] Stefan Köpsell, Rolf Wendolsky, Hannes Federrath: *Revocable Anonymity*; Emerging Trends in Information and Communication Security (ETRICS 2006), Springer, Berlin / Heidelberg, LNCS 3995, 2006, 206–220.

[KöŠv_09] Stefan Köpsell, Petr Švenda: *Secure logging of retained data*; Proc. Privacy and Identity Management for Life, PrimeLife/IFIP Internet Security & Privacy Fith International Summer School, 2009.

[Lies_05] Stefan Lieske: *Strafverfolgung und Blockungsresistenz*; Belegarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, November 2005.

[LRWW_04] Brian N. Levine, Michael K. Reiter, Chenxi Wang, Matthew Wright: *On the Economics of Anonymity*; Proc. Financial Cryptography 2004, LNCS 3110, Springer, Berlin / Heidelberg, 2004, 251–265.

[Lütt_98] Thomas Lüttig: *Dummy Traffic zur Gewährleistung von Unbeobachtbarkeit im Internet*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Theoretische Informatik, 31. Dezember 1998.

[MaDi_05] Nick Mathewson, Roger Dingledine: *Practical Traffic Analysis: Extending and Resisting Statistical Disclosure*; Proc. of Privacy Enhancing Technologies Workshop (PET 2004), Springer, Berlin / Heidelberg, LNCS 3424, 2005, 17–34.

[MaKh_08] Alexander Maximov, Dmitry Khovratovich: *New State Recovery Attack on RC4*; Proc. CRYPTO 2008, Springer, Berlin / Heidelberg, LNCS 5157, 2008, 297–316.

[MaTs_09] Di Ma, Gene Tsudik: *A new approach to secure logging*; ACM Transactions on Storage (TOS), vol. 5, Nr. 1, ACM, New York, März 2009.

[May_09] Christoph Mayer: *Pflicht zur Vorratsdatenspeicherung bei unentgeltlichen E-Mail-Diensten? Die Definition des Telekommunikationsdienstes gem. § 3 Nr. 24 TKG und ihre Auswirkungen auf die Vorratsdatenspeicherung*; Kommunikation & Recht, Heft 5, Jahrgang 2009, Verlag Recht und Wirtschaft, Frankfurt a. M., Mai 2009, 313–317.

[MeOV_96] Alfred J. Menezes, Paul C. van Oorschot, Scoot A. Vanstone: *Handbook of applied cryptograhpy*; 1. Auflage, CRC Press, 1996.

[Mill_68] Robert B. Miller: *Response time in man-computer conversational transaction*, Proc. of AFIPS Fall Joint Computer conference, vol. 33, ACM, New York, 1968, 267–277.

[Müll_02] Andreas Müller: *Entwurf und Implementierung einer Zahlungsfunktion für einen Mix-basierten Anonymisierungsdienst unter Berücksichtigung mehrseitiger Sicherheitsanforderungen*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, Dezember 2002.

[Murd_07] Steven J. Murdoch: *Covert channel vulnerabilities in anonymity systems*; Technical Report Nr. 706, University of Cambridge, Großbritannien, Computer Laboratory, Dezember 2007.

[Nah_04] Fiona Fui-Hoon Nah: *A study on tolerable waiting time: how long are Web users willing to wait?*; Behaviour & Information Technology, Special Issue on HCI in MIS; vol. 23, Nr. 3, Taylor and Francis Ltd, 2004, 153–163.

[Niel_93] Jakob Nielsen: *Response Times: The Three important Limits*, in: Usability Engineering, Kapitel 5.5, Academic Press, 1993, 134–138.

[Nol_00] Inge Margaretha van der Nol: *datenbanken in mix-systemen*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut für Theoretische Informatik, Delft University of Technology, Faculteit van Informatietechnologie en Systemen, Subfaculteit Technische Informatica, 3. November 2000.

[OhAb_00] Miyako Ohkubo, Masayuki Abe: *A Length-Invariant Hybrid Mix*; Proc. Advances in Cryptology – ASISACRYPT 2000, Springer, Berlin /Heidelberg, LNCS 1976, 2000, 440–444.

[OKST_97] Wakaha Ogata, Kaoru Kurosawa, Kazue Sako, Kazunori Takatani: *Fault tolerant anonymous channel*; Proc. First International Conference on Information and Communications Security, Springer, Berlin /Heidelberg, LNCS 1334, 1997, 440–444.

[OzSc_06] Andy Ozment, Stuart E. Schechter: *Bootstrapping the Adoption of Internet Security Protocols* ; Proc. Fith Workshop on the Economics of Information Security (WEIS 2006), Juni, 2006, `http://weis2006.econinfosec.org/docs/46.pdf`, abgerufen am 24. Oktober 2009.

[PfHa_08] Andreas Pfitzmann, Marit Hansen: *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. A Consolidated Proposal for Terminology*; in: René Balzer, Stefan Köpsell, Horst Lazarek (Hg.): Fachterminologie Datenschutz und Datensicherheit Deutsch – Russisch – Englisch; FGI – Forschungsgesellschaft Informatik, Technische Universität Wien, Wien, `http://dud.inf.tu-dresden.de/Anon\_Terminology.shtml`, Februar 2008, 111–144.

[Pfitz_85] Andreas Pfitzmann: *How to implement ISDNs without user observability – Some remarks*; Institut für Informatik IV, Universität Karlsruhe, Interner Bericht 14/85, 1985.

[Pfitz_90] Andreas Pfitzmann: *Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz*; Informatik-Fachberichte, 234, Springer, Berlin / Heidelberg, 1990.

[PfPf_90] Birgit Pfitzmann, Andreas Pfitzmann: *How to Break the Direct RSA-Implementation of MIXes*; Proc. Advances in Cryptology – EUROCRYPT 1989, Springer, Berlin /Heidelberg, LNCS 434, 1990, 373–381.

[PfPW_89] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: *Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2·64 + 16)-kbit/s-Teilnehmeranschluß*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 12, Dezember 1989, 605–622.

[PfPW_91] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: *ISDN-MIXes: Untraceable Communication with very small Bandwidth Overhead*; Proc. Kommunikation in verteilten Systemen, Informatik-Fachberichte 267, Springer Berlin / Heidelberg, 1991, 451–463.

[PfWa_86] Andreas Pfitzmann, Michael Waidner: *Networks without User Observability – Design Options*; Proc. Advances in Cryptology – EUROCRYPT 1985, Springer, Berlin /Heidelberg, LNCS 245, 1986, 245–253.

[PiKo_08] Lexi Pimenidis, Eleni Kosta: *The impact of the retention of traffic and location data on the internet user – A critical discussion*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 2, Februar 2008, 92–97.

[Pime_05] Lexi Pimenidis: *A practical approach to transparent und usable anonymity networks*; in Hannes Federrath (Eds.): SICHERHEIT 2005, Sicherheit – Schutz und Zuverlässigkeit, Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V., LNI P-62, Gesellschaft für Informatik, Bonn, 2005, 305–316.

[PKCS#1 v2.1] RSA Laboratories: *PKCS#1 v2.1: RSA Cryptography Standard*; RSA Security Inc., 14. Juni 2002, `ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf`, abgerufen am 5. Dezember 2008.

[Pöpp_06] Wolfgang Pöppl: *Integration eines Datenscanners in den Anonymisierungsdienst AN.ON*; Diplomarbeit, Universität Regensburg, Wirtschaftswissenschaftliche Fakultät, Institut für Wirtschaftsinformatik, 27. September 2006.

[Putn_08] Markus Putnings: *Untersuchung des Medienechos zum Internet-Anonymisierer JAP*; Diplomarbeit, Universität Regensburg, Wirtschaftswissenschaftliche Fakultät, Institut für Wirtschaftsinformatik, 13. Oktober 2008.

[Ra_03] Oliver Raabe: *Die rechtliche Einordnung zweier Web-Anonymisierungsdienste*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 3, März 2003, 134–138.

[Rab_78] M. Rabin: *Digital signatures*; in: Foundations of Secure Computation, R. DeMillo, D. Dobkin, A.Jones, R.Lipton (Herausgeber), Academic Press, New York, 1978, 155–168.

[RaBP_98] J. Ramsay, A. Barbesi, J. Preece: *A psychological investigation of long retrieval times on the world wide web*, Interacting with Computers, The interdisciplinary journal of Human-Computer Interaction, vol. 10, Nr. 1, Elsevier, 1998, 77–86.

[Renn_04] Marc rennhard: *MorphMix A Peer-to-Peer-based System for Anonymous Internet Access*, Shaker Verlag, 1. Auflage, 2004.

[RePl_02] Marc Rennhard, Bernhard Plattner: *Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection*; Proc. Workshop on Privacy in the Electronic Society (WPES 2002), ACM , New York, 2002, 91–102.

[RePl_04] Marc Rennhard, Bernhard Plattner: *Practical Anonymity for the Masses with MorphMix* ; Proc. Financial Cryptography, 8th International Conference (FC 2004), Springer, Berlin / Heidelberg, LNCS 3110, 2004, 233–250.

[ReRu_98] Michael K. Reiter, Aviel D. Rubin: *Crowds: Anonymity for Web Transactions*; ACM Transactions on Information and System Security, vol. 1, Nr. 1, November 1998, 66–92.

[ReSG_98] Michael G. Reed, Paul F. Syverson, David M. Goldschlag: *Anonymous Connections and Onion Routing*; IEEE Journal on Selected Areas in Communication, vol. 16, Nr. 4, IEEE Communications Society, Mai 1998, 474–481.

[Rock_03] Ivo Rockstuhl: *„Zero-Footprint" – Technologie für Sicherheitsanwendungen*; Zeitschrift OBJEKTspektrum, SIGS-DATACOM GmbH, Ausgabe 4, 2003, 56–63, `http://www.sigs.de/publications/os/2003/04/ruckstuhl_OS_04_03.pdf`, abgerufen am 26. Oktober 2009.

[RoES_03] Gregory M. Rose, Roberto Evaristo, Detmar W. Straub: *Culture and Consumer Responses to Web download Time: A Four-Continent Study of Mono and Polychronism*; IEEE Transactions on Engineering Management, 50(1), 2003, 31–44.

[RoSt_01] Gregory M. Rose, Detmar W. Straub: *The Effect of Download Time on Consumer Attitude Toward the e-Service Retailer*, e-Service Journal, vol. 1, Nr. 1, Indian University Press, August 2001, 55–76.

[Scho_09] Jens Schomburg: *Anonymity Techniques – Usability tests of Major Anonymity Networks*; Proc. Fourth Privacy enhancing Technologies Convention (PET-CON 2009.1), Technischer Bericht, TUD-FI09-04-April 2009, Technische Berichte, Technische Universität Dresden, Fakultät Informatik, April 2009, 49–58, `http://ftp.inf.tu-dresden.de/berichte/tud09-04.pdf`, abgerufen am 13. Juli 2009.

[Schu_04] Sebastian Schumann: *Implementierung des Verfahrens Flash Mix*; Belegarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, Dezember 2004.

[ScKe_99] Bruce Schneier, John Kelsey: *Secure Audit Logs to Support Computer Forensics*; ACM Transactions on Information and System Security (TISSEC), vol. 2, Nr. 2, 1999, 159–176.

[ScRi_06] Steffen Schoenwiese, Matthias Riedel: *Entwurf und Implementierung von Erweiterungen zur Vereinfachung der Administration von Mixen*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, November 2006.

[SeDa_03] Andrei Serjantov, George Danezis: *Towards an Information Theoretic Metric for Anonymity*; Proc. of Privacy Enhancing Technologies Workshop (PET 2002), Springer, Berlin / Heidelberg, LNCS 2482, 2003, 259–263.

[SeDS_03] Andrei Serjantov, Roger Dingledine, Paul Syversion: *From a Trickle to a Flood: Active Attacks on Several Mix Types*; Proc. of Information Hiding Workshop (IH 2002), Springer, Berlin / Heidelberg, LNCS 2578, 2003, 36–52.

[Serj_07] Andrei Serjantov: *A Fresh Look at the Generalised Mix Framework*; Proc. of Privacy Enhancing Technologies Symposium (PET 2007), Springer, Berlin / Heidelberg, LNCS 4776, 2007, 17–29.

[SeNe_03] Andrei Serjantov, Richard E. Newman: *On the anonymity of timed pool mixes*; Proc. of the Workshop on Privacy and Anonymity Issues in Networked and Distributed Systems, Athens, Greece, May 2003, Kluwer, 427–434.

[SiNo_08] Ulrich Sieber, Malaika Nolde: *Sperrverfügungen im Internet: nationale Rechtsdurchsetzung im globalen Cyberspace?*; Schriftenreihe des Max-Planck-Instituts für Ausländisches und Internationales Strafrecht, Reihe S, Strafrechtliche Forschungsberichte, Band 113, Verlag Duncker & Humblot, Berlin, 2008.

[Shne_84] Ben Shneiderman: *Response time and display rate in human performance with computers*, ACM Computing Surveys, vol. 16, Nr. 3, ACM, New York, September 1984, 265–285.

[ShSH_08] Erik Shimshock, Matt Staats, Nick Hopper: *Breaking and Provably Fixing Minx*; Proc. of Privacy Enhancing Technologies Symposium (PET 2008), Springer, Berlin / Heidelberg, LNCS 5134, 2008, 99–114.

[SP 800-38D] Morris Dworkin: *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*; U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), November 2007, `http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf`, abgerufen am 1. Dezember 2008.

[SP 800-38A] Morris Dworkin: *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*; U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), Dezember 2001, `http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf`, abgerufen am 16. Februar 2009.

[Spie_03] Sahra Spiekermann: *Die Konsumenten der Anonymität — Wer nutzt Anonymisierungsdienste?*; Datenschutz und Datensicherheit (DuD), Vieweg & Sohn, Wiesbaden, Heft 3, März 2003, 150–154.

[Spie_05] Sahra Spiekermann: *The Desire for Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services*; International Journal of Technology and Human Interaction, vol. 1, Nr. 1, Januar 2005, 74–83.

[Spie_07] Sahra Spiekermann: *Protecting One's Privacy: Insights into the Views and Nature of the Early Adopters of Privacy Services*; in: Issues and Trends in Technology and Human Interaction, IRM Press, Hershey, 2007, 84–95.

[Stev_94] W. Richard Stevens: *TCP/IP Illustrated, Volume 1 – The Protocols*; Addison-Wesley, 1994.

[StKM_08] Vassilios Stathopoulosa, Panayiotis Kotzanikolaoua, Emmanouil Magkosc: *Secure log management for privacy assurance in electronic communications*; Computers & Security, vol. 27, Nr. 7-8, Elsevier, Dezember 2008, 298–308.

[StKö_03] Sandra Steinbrecher, Stefan Köpsell: *Modelling Unlinkability*; Proc. Privacy Enhancing Technologies workshop (PET 2003), Springer, Berlin / Heidelberg, LNCS 2760, 2003, 32–47.

[SUN_06] Sun Microsystems, Inc.: *Java Card Specification*; Version 2.2.2, März 2006, `http://java.sun.com/javacard/specs.html`, abgerufen am 5. Dezember 2008.

[SyGR_97] Paul F. Syverson, David M. Goldschlag, Michael G. Reed: *Anonymous Connections and Onion Routing*; Proc. IEEE Symposium on Security and Privacy, IEEE Computer Society, 1997, 44–54.

[Tan_98] Andrew S. Tanenbaum: *Computernetzwerke*; 3., revidierte Auflage, Prentice Hall, 1998.

[TGPV_08] Carmela Troncoso, Benedikt Gierlichs, Bart Preneel, Ingrid Verbauwhede: *Perfect Matching Disclosure Attacks*; Proc. of Privacy Enhancing Technologies Symposium (PET 2008), Springer, Berlin / Heidelberg, LNCS 5134, 2008, 2–23.

[TóHV_04] Gergely Tóth, Zoltán Hornák, Ferenc Vajda: *Measuring Anonymity Revisited*; Proc. Nordic Workshop on Secure IT-systems (Nordsec 2004), 2004, `http://freehaven.net/anonbib/cache/THV04.pdf`, abgerufen am 1. November 2009.

[Uhli_06] Thomas Uhlig: *Entwurf und Implementierung einer Erweiterung zur anonymen Kommunikation für den Web-Browser Firefox*; Diplomarbeit, Technische Universität Dresden, Fakultät Informatik, Institut Systemarchitektur, Lehrstuhl Datenschutz und Datensicherheit, 27. Oktober 2006.

[ULD_06] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Abschlussbericht für das Projekt AN.ON – Juristische Arbeitspakete –*; Abschlußbericht des AN.ON Projektes, Förderkennzeichen 01 MS 917, 9. Oktober 2006.

[WaBr_1890] Samuel D. Warren, Louis D. Brandeis: *The Right to Privacy*; Harvard Law Review, vol. IV, Nr. 5, 15. Dezember 1890, 193–220.

[Waid_90] Michael Waidner: *Unconditional Sender and Recipient Untraceability in Spite of Active Attacks*; Proc. Advances in Cryptology – EUROCRYPT 1989, Springer, Berlin /Heidelberg, LNCS 434, 1990, 302–319.

[WaPf_89] Michael Waidner, Birgit Pfitzmann: *The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability*; Universität Karlsruhe 1989, Abstract in: Proc. Advances in Cryptology – EUROCRYPT 1989, Springer, Berlin /Heidelberg, LNCS 434, 1990, 690.

[WeHF_07] Rolf Wendolsky, Dominik Herrmann, Hannes Federrath: *Performance Comparison of Low-Latency Anonymisation Services from a User Perspective*; Proc. of Privacy Enhancing Technologies Workshop (PET 2007), Springer, Berlin / Heidelberg, LNCS 4776, 2007, 233–253.

[WSBL_08] Karel Wouters, Koen Simoens, Danny Lathouwers, Bart Preneel: *Secure and Privacy-Friendly Logging for eGovernment Services*; Proc. of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008, 1091-1096.

ZEITUNGEN UND ZEITSCHRIFTEN

[NYT_05] James Risen, Eric Lichtblau: *Bush Lets U.S. Spy on Callers Without Courts*; The New York Times, The New York Times Company, New York, USA, 16. Dezember 2005. `http://www.nytimes.com/2005/12/16/politics/16program.html?adxnnl=1\&adxnnlx=1134991970-aCBSv4Ws4mUI/nAkFqEBZQ`, abgerufen am 26. Oktober 2009.

[NYT_06] Eric Lichtblau, James Risen: *BANK DATA SIFTED IN SECRET BY U.S. TO BLOCK TERROR*; The New York Times, The New York Times Company, New York, USA, 23. Juni 2006. `http://select.nytimes.com/gst/abstract.html?res=F40F1FFE3D540C708EDDAF0894DE404482`, abgerufen am 26. Oktober 2009.

[USA TODAY_06] Leslie Cauley: *NSA has massive database of Americans' phone calls*; USA Today, Gannett Company, Inc., USA, 5. Oktober 2006, `http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm`, abgerufen am 11. Februar 2009.

INTERNET

RFCS[1]

[RFC 791] Jonathan B. Postel (Editor): *Internet Protocol*; September 1981, Standard, http://www.rfc-editor.org/rfc/rfc791.txt.

[RFC 821] Jonathan B. Postel: *Simple Mail Transfer Protocol*; August 1982, Standard, http://www.rfc-editor.org/rfc/rfc821.txt.

[RFC 959] Jonathan B. Postel, Joyce Reynolds: *File Transfer Protocol*; Oktober 1985, Standard, http://www.rfc-editor.org/rfc/rfc959.txt.

[RFC 1122] Robert Braden (Editor): *Requirements for Internet Hosts – Communication Layers*; Oktober 1989, Standard, http://www.rfc-editor.org/rfc/rfc1122.txt.

[RFC 1928] Marcus Leech, Matt Ganis, Ying-Da Lee, Ron Kuris, David Koblas, LaMont Jones: *SOCKS Protocol Version 5*; März 1996, Proposed Standard, http://www.rfc-editor.org/rfc/rfc1928.txt.

[RFC 1945] Tim Berners-Lee, Roy T. Fielding, Henrik Frystyk: *Hypertext Transfer Protocol – HTTP/1.0*; Mai 1996, Informational, http://www.rfc-editor.org/rfc/rfc1945.txt.

[RFC 2246] Tim Dierks, Christopher Allen: *The TLS Protocol Version 1.0*; Januar 1999, Proposed Standard, http://www.rfc-editor.org/rfc/rfc2246.txt.

[RFC 2616] Roy T. Fielding, Jim Gettys, Jeffrey Mogul, Henrik Frystyk, Larry Masinter, Paul Leach, Tim Berners-Lee: *Hypertext Transfer Protocol – HTTP/1.1* ; Juni 1999, Draft Standard, http://www.rfc-editor.org/rfc/rfc2616.txt.

[RFC 3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*; August 2001, Proposed Standard, http://www.rfc-editor.org/rfc/rfc3161.txt.

[RFC 3279] Larry Bassham, William Tim Polk, Russell Housley: *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, April 2002, Proposed Standard, http://www.rfc-editor.org/rfc/rfc3279.txt.

[RFC 3280] Russell Housley, William Tim Polk, Warwick Ford, David Solo: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*; April 2002, Proposed Standard, http://www.rfc-editor.org/rfc/rfc3280.txt.

[RFC 3439] Randy Bush, David Meyer: *Some Internet Architectural Guidelines and Philosophy*; Dezember 2002, Informational, http://www.rfc-editor.org/rfc/rfc3439.txt.

[RFC 3986] Tim Berners-Lee, Roy T. Fielding, Larry Masinter: *Uniform Resource Identifier (URI): Generic Syntax*; Januar 2005, Standard 66, http://www.rfc-editor.org/rfc/rfc3986.txt.

[RFC 4346] Tim Dierks, Eric Rescorla: *The Transport Layer Security (TLS) Protocol Version 1.1*; April 2006, Proposed Standard, http://www.rfc-editor.org/rfc/rfc4346.txt.

[RFC 4634] Donald E. Eastlake 3rd, Tony Hansen: *US Secure Hash Algorithms (SHA and HMAC-SHA)*; Juli 2006, Informational, http://www.rfc-editor.org/rfc/rfc4634.txt.

[1] Alle RFC-URLs zuletzt abgerufen am 6. November 2009.

[RFC 5321] John C. Klensin: *Simple Mail Transfer Protocol*; Oktober 2008, Draft Standard, http://www.rfc-editor.org/rfc/rfc5321.txt.

[RFC 5322] Peter W. Resnick (Editor): *Internet Message Format*; Oktober 2008, Draft Standard, http://www.rfc-editor.org/rfc/rfc5322.txt.

WIKIPEDIA

[Wikipedia:Geek] Artikel *Geek*. In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 26. Februar 2006, 20:40 UTC. URL: http://de.wikipedia.org/w/index.php?title=Geek\&oldid=14090532, abgerufen am 17. März 2006.

SONSTIGE WEB-SEITEN UND VERÖFFENTLICHUNGEN

[WWW:AN.ON_03] AN.ON Projekt: *Erklärung der Partner des Projektes „AN.ON – Anonymität.Online" zum zukünftigen Umgang mit Strafverfolgungsbehörden*; September 2003, http://anon.inf.tu-dresden.de/strafverfolgung/policy.pdf, abgerufen am 12. September 2008.

[WWW:Anon_06] Anonymizer Inc. Press Release: *Anonmyizer's chief scientist Lance Cotrell to present at FOSE 2006*; http://www.anonymizer.com/consumer/media/press_releases/03062006.html, abgerufen am 8. November 2007.

[WWW:Bach_08] Daniel Bachfeld: *Präparierte Webseite schaltet Firewall im Router aus*; Artikel in heise Security vom 11. Januar 2008, http://www.heise.de/security/Praeparierte-Webseite-schaltet-Firewall-im-Router-aus--/news/meldung/101641, abgerufen am 15. Juli 2009.

[WWW:Bach_08a] Daniel Bachfeld: *Ungewollte Fernkonfiguration für Heim-Router [Update]*; Artikel in heise Security vom 15. Januar 2008, http://www.heise.de/security/Ungewollte-Fernkonfiguration-fuer-Heim-Router-Update--/news/meldung/101799, abgerufen am 15. Juli 2009.

[WWW:Bach_08b] Daniel Bachfeld: *Erste aktive Angriffe auf DSL-Router [Update]*; Artikel in heise Security vom 23. Januar 2008, http://www.heise.de/security/Erste-aktive-Angriffe-auf-DSL-Router-Update--/news/meldung/102281, abgerufen am 15. Juli 2009.

[WWW:BaGS_01] Adam Back, Ian Goldberg, Adam Shostack: *Freedom 2.1 Security Issues and Analysis*, White Paper, Zero-Knowledge Systems, Inc., 3. Mai 2001, http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/Freedom_Security2-1.pdf, abgerufen am 20. November 2007.

[WWW:BrEl_01] David Bratzer, Andrew Elkin: *Freedom 2.2 Abuse Issues and Analysis*; White Paper, Zero-Knowledge Systems, Inc., 14. Juni 2001, http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/freedom_abuse2-2.pdf, abgerufen am 13. August 2008.

[WWW:Brey_08] Patrick Breyer: *Keine Vorratsdatenspeicherung für unentgeltliche Dienste [6. Ergänzung]*; Version vom 23. November 2008, 18.03 Uhr, http://www.daten-speicherung.de/index.php/keine-vorratsdatenspeicherung-fuer-unentgeltliche-dienste/, abgerufen am 25. Mai 2009.

[WWW:BoGS_00] Philippe Boucher, Ian Goldberg, Adam Shostack: *Freedom System 2.0 Architecture*; Zero-Knowledge Systems, Inc., White Paper, 18. Dezember 2000, http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/Freedom_System_2_Architecture.pdf, abgerufen am 5. September 2009.

[WWW:Cot_94] Lance Cottrell: *Mixmaster & Remailer Attacks*; Essay, 1994, http://web.archive.org/web/19961112194057/http://www.obscura.com/~loki/remailer/remailer-essay.html, abgerufen am 16. November 2007.

[WWW:Cot_07] Lance Cottrell: *Slashdot | Web-based Anonymizer Discontinued*; Blog-Eintrag im „/the privacy blog/", 31. Juli 2007, http://www.theprivacyblog.com/?p=29, abgerufen am 9. Januar 2008.

[WWW:Dai_95] Wai Dai: *link encryption and anonymous interactivity (Was: "Subway" remai*; Nachricht auf der Cypherpunk Mailingliste, 26. Januar 1995, http://cypherpunks.venona.com/date/1995/01/msg01348.html, abgerufen am 22. November 2007.

[WWW:Dai_98a] Wai Dai: *PipeNet description*; Nachricht auf der Cypherpunk Mailingliste, 19. Januar 1998, http://cypherpunks.venona.com/date/1998/01/msg00878.html, abgerufen am 22. November 2007.

[WWW:Dai_98b] Wai Dai: *PipeNet 1.1 and b-money*; Nachricht auf der Cypherpunk Mailingliste, 26. November 1998, http://cypherpunks.venona.com/date/1998/11/msg00941.html, abgerufen am 22. November 2007.

[WWW:Dai_98c] Wai Dai: *PipNet 1.1*; http://www.weidai.com/pipenet.txt, abgerufen am 22. November 2007.

[WWW:Ding_05] Roger Dingledine: *Research questions for Tor*; Internationale Begegnungs- und Forschungszentrum für Informatik (IBFI) Schloß Dagstuhl, Seminar 05411: Anonymous Communication and its Applications, Schloß Dagstuhl, Deutschland, 9.-14. Oktober 2005, http://freehaven.net/\%7Earma/slides-dagstuhl05.pdf, abgerufen am 11. März 2008.

[WWW:ECRYPT_08] Mats Näslund (Editor): *ECRYPT Yearly Report on Algorithms and Keysizes (2007-2008)*; Revision 1.1, ECRYPT Projekt (IST-2002-507932), 31. Juli, 2008, http://www.ecrypt.eu.org/ecrypt1/documents/D.SPA.28-1.1.pdf, abgerufen am 9. Februar 2009.

[WWW:ErKu_07] Monika Ermert, Jürgen Kuri: *Europaratsempfehlung zu Internet-Filtern geplant*; in heise online vom 15. November 2007, http://www.heise.de/netze/Europaratsempfehlung-zu-Internet-Filtern-geplant--/news/meldung/99032, abgerufen am 13. August 2008.

[WWW:Feder_00] Hannes Federrath: *Flaw in anonymity systems found*; Arbeitsnotiz, 18. Februar 2000, aktualisiert am 6. Mai 2000, http://www-sec.uni-regensburg.de/publ/2000/aproxies/indexe.html, abgerufen am 9. November 2007.

[WWW:FUD_03] Captain FUD: *JAP compromised, privacy community panics*, Beitrag in der News-Gruppe alt.privacy.anon-server vom 28. Juli 2003, http://groups.google.com/group/alt.privacy.anon-server/msg/c5ee4bb5a0161f9e, abgerufen am 14. August 2008.

[WWW:Glea_05] Mike Gleason: *The File Transfer Protocol (FTP) and Your Firewall / Network Address Translation (NAT) Router / Load-Balancing Router*; Version 1.1.1, 18. April 2005, http://www.ncftp.com/ncftpd/doc/misc/ftp_and_firewalls.html, abgerufen am 26. Februar 2009.

[WWW:GNET] Christian Grothoff, Ioana Patrascu, Krista Bennett, Tiberiu Stef, Tzvetan Horozov: *GNET*; White Paper, Version 0.5.2, 13. Juni 2002, http://www.gnunet.org/download/main.pdf, abgerufen am 20. Juli 2009.

[WWW:GNUnet] Deutschsprachige Web-Seite des GNUnet Projektes. http://www.gnunet.org/?xlang=German, abgerufen am 20. Juli 2009.

[WWW:Gold_01] Ian Goldberg: *ZeroKnowledge to Discontinue Anonymity Service*; Mitteilung auf Slashdot®; http://slashdot.org/comments.pl?cid=2388977\&sid=22261\&tid=158, abgerufen am 6. Februar 2008.

[WWW:GoSh_99a] Ian Goldberg, Adam Shostack: *Freedom Network 1.0 Architecture*; White Paper, Zero-Knowledge Systems, Inc., 29. November 1999 ; http://web.archive.org/web/20000815223339/www.freedom.net/info/freedompapers/Freedom-Architecture.pdf, abgerufen am 5. September 2009.

[WWW:GoSh_99b] Ian Goldberg, Adam Shostack: *Freedom Network 1.0 Architecture and Protocols*; White Paper, Zero-Knowledge Systems, Inc., 29. November 1999 ; http://web.archive.org/web/20000815223347/www.freedom.net/info/freedompapers/Freedom-Architecture-Protocols.pdf, abgerufen am 5. September 2009.

[WWW:IBM_00] International Business Maschines: *Web guidelines – Final Testing*, archivierte Version vom 18. August 2000, http://web.archive.org/web/20000818063332/http://www-3.ibm.com/ibm/easy/eou_ext.nsf/Publish/609, abgerufen am 10. März 2009.

[WWW:Intel_08] Shay Gueron: *Advanced Encryption Standard (AES) Instructions Set*; White Paper, Intel Mobility Group Israel Development Center, Israel, Juli 2008, http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf, abgerufen am 16. Februar 2009.

[WWW:Intel_09] Intel Corporation: *Introduction to Intel's 32nm Process Technology*; White Paper, Intel Corporation, erstellt am 9. Februar 2009, http://download.intel.com/pressroom/kits/32nm/westmere/Intel_32nm_Overview.pdf, abgerufen am 16. Februar 2009.

[WWW:Kaps_07] Reik Kaps: *Update beseitigt Lücke in Anonymisierungsdienst Tor* ; Artikel in heise online vom 4. August 2007, http://www.heise.de/newsticker/Update-beseitigt-Luecke-in-Anonymisierungsdienst-Tor--/meldung/93853, abgerufen am 15. Juli 2009.

[WWW:KrSt_09] Stefan Krempl, Ingo T. Storm: *Hansenet speichert TK-Daten weiterhin nicht auf Vorrat*; Artikel in heise online vom 31. Oktober 2009, http://www.heise.de/newsticker/meldung/Hansenet-speichert-TK-Daten-weiterhin-nicht-auf-Vorrat-847214.html, abgerufen am 31. Oktober 2009.

[WWW:Klei_01] Torsten Kleinz: *Eine marktbezogene Entscheidung*; Telepolis, Heise Zeitschriften Verlag, München, 6. Oktober 2001, http://www.heise.de/tp/r4/artikel/9/9734/1.html, abgerufen am 6. Februar 2008.

[WWW:Kra_04] Henry Krasemann: *Besprechung des Beschlusses des Landgerichts Frankfurt am Main vom 15.09.2003 (Az.: 5/6 Qs 47/03) und des Beschlusses des Landgerichts Frankfurt am Main vom 21.10.2003 (Az.: 5/8 Qs 26/03)*; JurPC Web-Dok. 140/2004, Abs. 1 - 5, http://www.jurpc.de/aufsatz/20040140.htm, abgerufen am 14. August 2008.

[WWW:Ko_04] Axel Kossel: *eBay-Passwortklau: Zugangsdaten stehlen mittels präparierter Auktionen*; in heise online vom 15. Dezember 2004, http://www.heise.de/security/eBay-Passwortklau--/artikel/54271, abgerufen am 13. August 2008.

[WWW:Ko_08] Axel Kossel: *eBay: Phishing und kein Ende*; in heise online vom 22. Januar 2008, http://www.heise.de/newsticker/eBay-Phishing-und-kein-Ende--/meldung/102247, abgerufen am 13. August 2008.

[WWW:Ku_07] Jürgen Kuri: *Musikindustrie fordert EU-weites Filtern des Internetverkehrs*; in heise online vom 22. Dezember 2007, http://www.heise.de/newsticker/meldung/101020, abgerufen am 13. August 2008.

[WWW:LGFra_03] Landgericht Frankfurt am Main: *Beschluss in der Strafsache gegen ... und weiterer unbekannter Täter wegen Verdachts einer Straftat nach § 184 StGB*; Aktenzeichen: 5/6 Qs 47/03; JurPC Web-Dok. 326/2003, http://www.jurpc.de/rechtspr/20030326.htm, 15. September 2003, abgerufen am 18. August 2008.

[WWW:LGFra_03a] Landgericht Frankfurt am Main: *Beschluss*; Aktenzeichen 5/8 Qs 26/03, JurPc Web-Dok. 134/2004, http://www.jurpc.de/rechtspr/20040134.htm, 30. Oktober 2003, abgerufen am 18. August 2008.

[WWW:Luck_99] Norbert Luckhardt: *Falsche Fährten im Internet*; Artikel in heise online vom 13. Dezember 1999, http://www.heise.de/newsticker/meldung/7259, abgerufen am 6. Februar 2008.

[MaPG_03] Brian A. Malloy, James F. Power, Tanton H. Gibbs: *C++ Compilers & ISO Conformance*; Dr. Dobb's Portal, 1. November 2003, http://www.ddj.com/cpp/184405483, abgerufen am 26. Februar 2008.

[WWW:MaxMind_05] Web-Site of MaxMind LLC. http://www.maxmind.com/, 2005.

[WWW:Me_07] Ingrid Melander: *Web search for bomb recipes should be blocked: EU*; Reuters Meldung vom 10. September 2007, http://www.reuters.com/article/internetNews/idUSL1055133420070910, abgerufen am 13. August 2008.

[WWW:minFraud] MaxMind: *Fraud Detection through IP Address Reputation and a Mutual Collaboration Network*; White Paper, http://www.maxmind.com/minFraudWhitePaper.pdf, abgerufen am 12. August 2008.

[WWW:Niel_95] Jakob Nielsen: *Jakob Nielsen's Alertbox for December 1995: Guidelines for multimedia on the web*, Dezember 1995, http://www.useit.com/alertbox/9512.html, abgerufen am 10. März 2009.

[WWW:Niel_96] Jakob Nielsen: *Jakob Nielsen's Alertbox for May 1996: Top ten mistakes in Web design*, Mai 1996, http://www.useit.com/alertbox/9605.html, abgerufen am 10. März 2009.

[WWW:Niel_97] Jakob Nielsen: *Jakob Nielsen's Alertbox for March 1, 1997: The Need for Speed*; März, 1997, http://www.useit.com/alterbox/9703a.html, abgerufen am 15. Januar 2009.

[WWW:Niel_08] Jakob Nielsen: *Jakob Nielsen's Alertbox for March 31, 2008: Middle-Aged Users' Declining Web Performance*; März, 2008, http://www.useit.com/alertbox/middle-aged-users.html, abgerufen am 10. März 2009.

[WWW:Onion_07] Onion-Info: *Onion Routing: Brief Selected History*; http://www.onion-router.net/History.html, abgerufen am 26. November 2007.

[WWW:R_08] R Development Core Team (2008): *R: A language and environment for statistical computing*; R Foundation for Statistical Computing, Wien, Österreich, http://www.R-project.org/.

[WWW:RSF_05] Reporters sans frontières: *Saudi Arabia - 2005 annual report*; http://www.rsf.org/article.php3?id_article=13312, 2005, abgerufen am 8. Dezember 2008.

[WWW:SaHa_00] Russell Samuels, Ed Hawco: *Untracable Nym Creation on the Freedom 2.0 Network™*; White Paper, Zero-Knowledge Systems, Inc., 1. November 2000, http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/Freedom-NymCreation.pdf, abgerufen am 21. Januar 2008.

[WWW:Sc_05] Jürgen Schmidt: *eBay-Seiten helfen beim Phishen*; in heise online vom 9. März 2005, http://www.heise.de/newsticker/eBay-Seiten-helfen-beim-Phishen--/meldung/57240, abgerufen am 13. August 2008.

[WWW:Selv_99] Paula Selvidge: *How Long is* Too Long *to Wait for a Website to Load?*, Usability News, vol. 1, Nr. 2, Software Usability Research Laboratory, Wichita State University, Juli 1999, http://www.surl.org/usabilitynews/12/time_delay.asp, abgerufen am 10. März 2009.

[WWW:Shou_01] Victor Shoup: *A proposal for an ISO standard for public key encryption*; Version 2.1, 20. Dezember 2001, http://www.shoup.net/papers/iso-2_1.pdf, abgerufen am 28. Juli 2009.

[WWW:Sper_94] Simon E. Spero: *Analysis of HTTP Performance problems* ; Juli 1994, http://www.w3.org/Protocols/HTTP/1.0/HTTPPerformance.html, abgerufen am 26. Februar 2009.

[WWW:ULD_03] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Erster Teilerfolg für AN.ON*; Pressemitteilung, 27. August 2003, https://www.datenschutzzentrum.de/material/themen/presse/anonip2.htm, abgerufen am 18. August 2008.

[WWW:ULD_04] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Der Fall BKA vs. AN.ON (Anonymität Online) jährt sich und dauert.*; Pressemitteilung, 30. Juni 2004, https://www.datenschutzzentrum.de/material/themen/presse/20040702-bkavsanon.htm, abgerufen am 18. August 2008.

[WWW:WaSt_01] Thomas Wagner, Wolfgang Stieler: *TU-Software schützt vor Datenschnüfflern*; in heise online vom 10. Januar 2007, http://www.heise.de/newsticker/TU-Software-schuetzt-vor-Datenschnuefflern--/meldung/14374, abgerufen am 20. August 2009.

[WWW:WBXML] Wireless Apllication Protocol Forum, Ltd: *Binary XML Content Format Specification*; Wireless Application Protocol, WAP-192-WBXML-20010725-a, Version 1.3, 25. Juli 2008, http://www.openmobilealliance.org/tech/affiliates/wap/wap-192-wbxml-20010725-a.pdf, abgerufen am 23. Juni 2008.

[WWW:WWW_07] DEranged Security: *Time to reveal...*; Blog-Eintrag, 10. September 2007, http://www.derangedsecurity.com/time-to-reveal.../, abgerufen am 9. November 2007.

[WWW:WWW_08] Onion-Router Web-Seite (http://www.onion-router.net/Prototype.html) in der Version vom 12. Dezember 1999, abgerufen aus dem Web-Archiv (http://www.webarchive.org/) am 13. Januar 2008.

[WWW:XMLEnc] Takeshi Imamura, Blair Dillaway, Ed Simon: *XML Encryption Syntax and Processing*; W3C Recommendation, 10. Dezember 2002, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, abgerufen am 23. Juni 2008.

[WWW:XMLEXI] John Schneider, Takuki Kamiya (Editoren): *Efficient XML Interchange (EXI) Format 1.0*; W3C Working Draft, 3rd working draft, 26. März 2008, http://www.w3.org/TR/2008/WD-exi-20080326/, abgerufen am 23. Juni 2008.

[WWW:XMLSchema Part 1] Henry S. Thompson, David Beech, Murray Maloney, Noah Mendelsohn (Editoren): *XML Schema Part 1: Structures Second Edition*; W3C Empfehlung, 28. Oktober 2004, http://www.w3.org/TR/xmlschema-1/, abgerufen am 17. April 2009.

[WWW:XMLSchema Part 2] Paul V. Biron, Kaiser Permanente, Ashok Malhotra (Editoren): *XML Schema Part 2: Datatypes Second Edition*; W3C Empfehlung, 28. Oktober 2004, http://www.w3.org/TR/xmlschema-2/, abgerufen am 17. April 2009.

[WWW:XMLSig] Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon: *XML Signature Syntax and Processing (Second Edition)*; W3C Recommendation, 10. Juni 2008, http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/, abgerufen am 23. Juni 2008.

[WWW:XSLT] James Clark (Editor): *XSL Transformations (XSLT) Version 1.0*; W3C Recommendation, 16. November 1999 , http://www.w3.org/TR/1999/REC-xslt-19991116/, abgerufen am 11. September 2009.

[WWW:Zona_99] Zona Research Inc.: *The Economic Impacts of Unacceptable Web-Site Download Speeds*, White Paper, April 1999, http://www.webperf.net/info/wp_downloadspeed.pdf, abgerufen am 10. März 2009.