



# Konferenzseminar IT-Sicherheit

SS 2014

Veranstalter: Felix Freiling, Hans-Georg Eßer

Lehrstuhl für IT-Sicherheitsinfrastrukturen  
Univ. Erlangen-Nürnberg

Foliensatz B (23.04.2014)  
Wiss. Arbeiten, Ausarbeitungen und Vorträge

Dieser Foliensatz basiert auf  
Folien von Prof. Felix Freiling





## Inhalte

- Wie lese ich ein Paper?
- Wie schreibe ich eine Seminararbeit?
- Wie halte ich einen Seminarvortrag?



- Was ist das Themengebiet des/der Papers?
- Was ist die zentrale Fragestellung?
  - Welches Problem lösen die Autoren?
  - Wie lösen sie es?
  - Welche Vor-/Nachteile gibt es gegenüber anderen Lösungen (→ die evtl. im Paper erwähnt werden)
- Literaturangaben im Paper auswerten
  - Grundlagen
  - Verwandte Arbeiten (related work)



- Gliederung erstellen
- Typisch:
  - Kap. 1: Einleitung
  - Kap. 2:  (Inhalt)
  - Kap.  $n-1$ : 
  - Kap.  $n$ : Zusammenfassung



- Einleitung besteht aus:
  - Motivation / Themenfeld
    - Welches Themengebiet behandelt die Arbeit
    - Warum ist es relevant?
  - Thema der (Seminar-) Arbeit
    - Fragestellung in dieser Ausarbeitung
    - Bezug auf das Paper / die Papers
    - Welche Lösung wird im Paper vorgeschlagen?
  - Struktur der Arbeit
    - Wie ist diese Arbeit aufgebaut? Roter Faden?



- Leser wollen i. d. R. nicht jedes Dokument vollständig lesen
- Darum: In der Einleitung vollständigen Überblick über die wichtigsten Inhalte der Arbeit geben (→ „Executive Summary“)



- Oft erst ein Kapitel mit Grundlagen
  - (Begriffs-) Definitionen
  - Voraussetzungen
  - Annahmen
  - Eingesetzte Techniken / Verfahren



- In den inhaltlichen Kapiteln kann sich die Grobstruktur der Ausarbeitung wiederholen, also
  - Kap. *i.1*: Einleitung (zu Thema *i*)
    - Worum geht es? ←
    - Roter Faden
    - Anknüpfen an vorangehendes Kapitel
  - Kap. *i.2*: ...
  - Kap. *i.m*: Zusammenfassung
    - Worum ging es? ← Wieder: Roter Faden
    - ggf. Ausblick auf Folgekapitel

Redundanz  
ist OK, hilft bei  
Orientierung





- Kurze Wiederholung der Fragestellung
- Kurze Zusammenfassung der Lösung (Wissen der Arbeit kann jetzt vorausgesetzt werden)
- Falls sinnvoll: Hinweis auf offene Punkte, unbeantwortete Fragen



- Häufiges Problem:  
Paper viel zu lang / Paper viel zu kurz
- Auswahl
- Ergänzung (weitere Papers etc.)
- Seminaarausarbeitung und Vortrag müssen nicht deckungsgleich sein
- Ausarbeitung „in sich geschlossen“ (ohne weitere Literatur verständlich)
- Frage beantworten: Warum sollte man meine Ausarbeitung (statt der Originaltexte) lesen?



- Beim Strukturieren bereits die relevanten Textstellen der Originalliteratur vermerken
  - Welcher Teil der Arbeit bezieht sich auf welchen Teil der Originalliteratur?
- Im Text eine Referenz einbauen falls ...
  - wesentliche Ideen, Zahlen, Bilder, Tabellen usw. übernommen werden
  - ganze Teile wortwörtlich übernommen werden (Zitate)
- Zitate als solche kenntlich machen („...“ [Referenz])
- Referenzen möglichst genau (am besten mit Seitenangabe, vor allem bei Büchern)



- Quellen kritisch bearbeiten
  - Nur weil etwas in einer Quelle steht, muss es nicht richtig sein → kein blindes Vertrauen
  - Problembeschreibungen, Erklärungen und Lösungsvorschlägen kann man auch widersprechen
  - Wenn unklar: Weitere Arbeiten zum selben Thema suchen, vergleichen, gibt es einen Konsens?
  - Kein direkter Zusammenhang zwischen „Zitierfähigkeit“ und Glaubwürdigkeit einer Quelle



- Im Text stehen Referenzen (Verweise) auf das Literaturverzeichnis
  - Referenzen sind meist Kürzel in eckigen Klammern
  - Unterstützung durch LaTeX
  - Nehmt die Papers als Beispiele
- Arten des Zitierens:
  - Aktiv: In [1] wurde gezeigt ... [1, Seite 35]
  - Passiv: Maier und Müller [1] haben gezeigt ...
  - Möglichst für eine Art entscheiden und konsistent verwenden



- Informationen, die (unter Informatikern) allgemein bekannt sind, brauchen keinen Beleg durch Quellenangabe
  - „C ist eine häufig für systemnahe Programmierung verwendete Sprache.“ (ohne Beleg)
  - „Das Betriebssystem ZonkOS wurde nicht in C, sondern in Fortran implementiert [12].“ (mit Beleg)
- Ausführlichkeit des Belegens/Zitierens hängt auch von Zielgruppe ab
  - Informatiker allgemein?
  - Informatiker mit Schwerpunkt IT-Sicherheit?



- Mehrere Referenzen, Seitenangaben
  - [1, 2, 4]
  - [1–3, 5]
  - [4, Seite 15, 6, Seite 34] → besser zerlegen
  - LaTeX macht das automatisch
- Viele Autoren
  - Müller et al.: ab vier Autoren; in engl. Texten ab drei Autoren, vgl. Wikipedia [3]
  - im Literaturverzeichnis aber alle Autoren nennen



- alle verwendeten (und nur die!) Quellen aufführen
  - sortiert nach Nachname des Erstautors, dann nach Datum
- Eintrag enthält
  - Namen der Autoren, Titel der Publikation/des Beitrags
  - ggf. Name der Zeitschrift/Konferenz, Band, Nummer, Seitenzahl / Ort
  - Erscheinungsjahr
  - möglichst genau
- Quellen im Web: Autoren, Titel, URL und Zugriffsdatum (wenn es eine Originalquelle gibt, diese zitieren!)





- Wikipedia: u. U. akzeptable Quelle. Ganz gut für technische Dinge
- Whitepapers von Unternehmen: da fehlen oft wichtige Angaben (z. B. Autoren),  
→ Firma als Hrsg.
- „keinen Schrott zitieren“



- **Negativ-Beispiel**

Bei einem Vergleich forensisch nutzbarer Informationen in Windows-Dateisystemen sieht man u. a., dass FAT [1] nur einen einzigen Zeitstempel pro Datei speichert, während NTFS [2] für jede Datei vier Zeitstempel verwaltet [3]. Ergänzend gibt ...

[1] [http://de.wikipedia.org/wiki/File\\_Allocation\\_Table](http://de.wikipedia.org/wiki/File_Allocation_Table)

[2] <http://de.wikipedia.org/wiki/NTFS>

[3] <http://articles.forensicfocus.com/2013/04/06/interpretation-of-ntfs-timestamps/>

[4] <http://books.google.de/books?id=fummOICB9lgC&pg=PA148&lpg=PA148&dq=ntfs+%22delete+time%22+timestamp&source=bl&ots=FOFB7xD3MY&sig=awkTk3V-f1dR3E6ivx46-Gc7xs4&hl=en&sa=X&ei=loFXU6mOC4LNtQbLuwE&ved=0CDwQ6AEwAg#v=onepage&q=ntfs%20%22delete%20time%22%20timestamp&f=false>



Bei einem Vergleich forensisch nutzbarer Informationen in Windows-Dateisystemen sieht man u. a., dass FAT [1] nur einen einzigen Zeitstempel pro Datei speichert, während NTFS [2] für jede Datei vier Zeitstempel (create, modify, access, change) verwaltet [3]. Der vierte Zeitstempel (change) wird für gelöschte Dateien auch als delete-Timestamp betrachtet [4, S. 148].

- [1] Microsoft: Microsoft EFI FAT32 File System Specification, 2000, Whitepaper, <http://download.microsoft.com/download/1/6/1/161ba512-40e2-4cc9-843a-923143f3456c/fatgen103.doc>, Onlineabruf am 23.04.2014
- [2] Microsoft: NTFS Technical Reference, 2003, <http://technet.microsoft.com/en-us/library/cc758691%28WS.10%29.aspx>, Onlineabruf am 23.04.2014
- [3] wpathulin: „Interpretation of NTFS Timestamps“, Forensic Focus, 2013, <http://articles.forensicfocus.com/2013/04/06/interpretation-of-ntfs-timestamps/>, Onlineabruf am 23.04.2014
- [4] Greg Gogolin: *Digital Forensics Explained*, Auerbach Publications, 2012, ISBN: 1-4398-7495-6

Positiv-Beispiel



- In eigenen Worten formulieren
- Keine Textblöcke aus dem Paper übernehmen, auch keine Wort-für-Wort-Übersetzung
- kein Copy & Paste
  - Plagiat, ist in Prüfungs- und Seminararbeiten ein Grund für Nichtbestehen; an einigen Hochschulen sogar für offizielle Rügen oder Exmatrikulation (Abschlussarbeiten)
  - fällt auf (Stilbruch etc.) und wird geprüft
  - Reines Umformulieren von Satz für Satz ist aber genauso Plagiat!



- Vorsicht bei Formulierungen wie „**Ich/wir** habe/n gezeigt / herausgefunden / analysiert“ etc., wenn es tatsächlich die Autoren der Originalquellen waren
- Eigene Beiträge kennzeichnen (wenn Ihr z. B. eigene Messungen, Tests etc. macht)
- Stil: Passivkonstruktionen, Substantivierungen meiden



- Copy & Paste (wortwörtliche Wiedergabe)
- Paraphrasierung (Wiedergabe mit eigenen Worten),
- Übersetzungsplagiat
- Strukturplagiat
- „Shake and Paste“ [1]

[1] [http://plagiat.htw-berlin.de/ff/schule/3\\_2/wie](http://plagiat.htw-berlin.de/ff/schule/3_2/wie)



- Jedes Bild hat eine Bildunterschrift
  - beschreibt das Bild – ohne den restlichen Text vorauszusetzen
  - ist keine Kopie eines Satzes aus dem Text
- Für Tabellen gilt dasselbe analog



- Konsistent sein
  - beim Zitieren
  - bei der Verwendung von Fachbegriffen
- Sich an die (deutsche) Sprache halten
  - englische Wörter übersetzen und (wenn nötig) den Originalbegriff beim ersten Mal nennen
  - steht das Wort im Duden? Dann ist es deutsch
  - Fachbegriffe wie Botnet, Malware sind ok (1x erklären)
  - teilweise Geschmacksache („I/O“ oder „E/A“?)
- Sparsame Typographie
  - LaTeX hilft da auch (inhaltliche Auszeichnung)





- Beschwerden, dass der Stoff zu umfangreich ist. Aus jedem Thema lässt sich problemlos ein 10-, 20- oder 60-minütiger Vortrag gestalten. Das ist eben die Vortragskunst.
- Eine Motivation wird vernachlässigt.
- Sich nicht mit dem roten Faden oder der „Message“ auseinanderzusetzen.
- Es werden Dinge vorausgesetzt, die bei Teilen des Publikums nicht bekannt sind.
- Fachbegriffe werden nicht erklärt, Abkürzungen nicht ausgeführt.

Quelle: Weicker & Weicker, Lehrstuhl 4, Univ. Erl.-Nbg. [5]



- Gliederung wird anhand von Stichworten erstellt, die dann in jeweils ein bis zwei Sätzen ausgeführt werden. Meist geht hierbei der rote Faden verloren: die Arbeit wirkt abgehackt und unverständlich
- Gliederung der Folien für den Vortrag oder Gliederung des Vortrags für die Ausarbeitung verwenden
- Zu viel Zeit auf Folien verwenden, aber das Gesprochene improvisieren
- Den Folieninhalt nur vorlesen oder sich an den Folien entlang zu hangeln ohne den Vortrag lebendig werden zu lassen
- Mit Powerpoint-Effekten über inhaltliche Defizite hinwegtäuschen

Quelle: Weicker & Weicker, Lehrstuhl 4, Univ. Erl.-Nbg. [5]



- [1] Marcus Deininger, Horst Lichter, Jochen Ludewig, Kurt Schneider: Studienarbeiten. Ein Leitfaden zur Vorbereitung, Durchführung und Betreuung von Studien-, Diplom-, Abschluss- und Doktorarbeiten am Beispiel Informatik. vdf, 5. Auflage, 2005.
- [2] Albers et al.: Gute wissenschaftliche Praxis für das Verfassen wissenschaftlicher Qualifikationsarbeiten, [http://www.hochschulverband.de/cms1/uploads/media/Gute\\_wiss.\\_Praxis\\_Fakultaetentage.pdf](http://www.hochschulverband.de/cms1/uploads/media/Gute_wiss._Praxis_Fakultaetentage.pdf), Juli 2012.
- [3] Wikipedia zu „et al.“: [http://de.wikipedia.org/wiki/Et\\_al.](http://de.wikipedia.org/wiki/Et_al.)
- [4] Peter Rechenberg: Technisches Schreiben. Hanser, 2. Auflage, 2003.
- [5] Karsten Weicker, Nicole Weicker: Seminarrichtlinien am Lehrstuhl 4, [https://www4.cs.fau.de/Lehre/SS11/PS\\_KVBK/info/Weicker.pdf](https://www4.cs.fau.de/Lehre/SS11/PS_KVBK/info/Weicker.pdf)
- [6] Markus Rath: Leitfaden zur Anfertigung von Seminar-, Studien- und Diplomarbeiten, [http://www.wi-inf.uni-duisburg-essen.de/FGFrank/documents/Lehre/Leitfaden\\_WissArbeit.pdf](http://www.wi-inf.uni-duisburg-essen.de/FGFrank/documents/Lehre/Leitfaden_WissArbeit.pdf)