Universität Karlsruhe
Fakultät für Informatik
Institut für Betriebs- und Dialogsysteme
Bereich Einsatz vernetzter Rechensysteme
Prof. Dr.- Ing. Werner Zorn

Universität Karlsruhe, Inst. f. Betriebs- u.
Dialogsysteme, Postfach 6980, 76128 Karlsruhe

Am Fasanengarten 5, Postfach 6980
76128 Karlsruhe
Tel.: (0721) 608 - 3981
Fax: (0721) 96 63 550
zorn@ira.uka.de
www.ira.uka.de/i32

Karlsruhe, den 13.06.2000

Gutachten
zur
vorgelegten Dissertation (Stand 29.08.1999)
mit dem Titel
"Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit"
von
Herrn Dipl. Inform. Hadmut Danisch

1. Problemstellung, Zielsetzung, Beurteilungskriterien

Mit zunehmender Ausbreitung der Kommunikationsnetze, insbesondere offener Netze wie des Internet, und Nutzung für vertrauliche geschäftliche und private Zwecke kommt der Sicherheit ("Security") zentrale Bedeutung zu. Für eine Reihe besonders sensitiver Informationen, z.B. Digitales Geld oder Digitale Unterschriften, ist Kommunikationssicherheit (mit Vertraulichkeit, Integrität, Authentizität, Beweisbarkeit) überhaupt die Grundvoraussetzung für deren technische Realisierung und damit für die Entwicklung von Handel und Wandel ("E-Commerce") in Kommunikationsnetzen. Zum heutigen Zeitpunkt haben die mathematische Sicherheitstheorie und Sicherheitstechnik (Kryptologie und Kryptographie) einen so hohen Stand erreicht, dass diese im Vergleich mit herkömmlichen Sicherheitstechniken bei entsprechender Umsetzung nicht nur als gleichwertig, sondern sogar als überlegen angesehen werden können. Trotz dieser verfügbaren starken Sicherheitstechnologie sind die vorhandenen Kommunikationsnetze und damit auch deren Nutzung potentiell unsicher. Dieses ist vergleichbar mit der Situation eines Gebäudes (z.B. einer Bank), zu dessen Sicherung gegenüber Einbruchdiebstahl es auch nicht ausreicht, die Eingangstür mit Sicherheitsschlössern zu versehen. Entsprechend muss sich der Architekt eines Gebäudes ebenso wie der eines Kommunikationsnetzes überlegen, welche Sicherheitstechnologie er verwendet, um das System gegenüber möglichen Angriffen zu schützen. Dabei können die Angriffe sowohl von Aussen als auch von Innen kommen (letzeres vorzugsweise in Firmen), ebenso wie "von Oben", das von Seiten legitimierter Zugriffsberechtigter wie dem Hausbesitzer, der seinen Schlüsselbund verloren hat, oder der Obrigkeit im Falle von Prävention und Verfolgung von Straftaten oder zum Zwecke der Landesverteidigung (s. Gesetzgebung zum Großen Lauschangriff u. TKÜV- Telekommunikationsüberwachungsverordnung). Mit den zuletzt genannten Anforderungen ist zugleich ein Problembereich angesprochen, in dem rechtliche Randbedingungen, bzw. Auflagen zu berücksichtigen sind, die das legitimierte Ausserkraftsetzen ansonsten gewünschter und erforderlicher Sicherheitsmechanismen ermöglichen. Hierbei werden wiederum Fragen aufgeworfen, inwieweit Technik und Gesetzgebung miteinander in Einklang stehen, bzw. gebracht werden können.

Insgesamt ist mit der von Herrn Danisch behandelten Thematik ein äusserst relevanter Problembereich angesprochen, der mit seinen möglichen Ergebnissen und daraus resultierenden Konsequenzen von grosser Bedeutung sein könnte. Hieraus resultiert eine hohe Anforderung an die Qualität der Problembehandlung, der sich Herr Danisch mit seiner Dissertation stellen muss. Entsprechend der von Herrn Danisch sowohl in seiner Einleitung (Kap. 1) als auch in seiner Zusammenfassung (Kap. 6) formulierten Zielsetzung erhebt er den Anspruch, einen neuen und wichtigen methodischen Beitrag für

die Analyse, Beschreibung und den Entwurf sicherer Kommunikationssysteme zu leisten. Hierbei ist noch zusätzlich der von Herrn Danisch mit dem von ihm gewählten Titel der Arbeit "Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit" gesetzte Anspruch zu berücksichtigen, welcher die Erwartung weckt, dass bei Beachtung der angegebenen Kriterien und Anwendung der angegebenen Methoden Kommunikationssicherheit garantiert zu erlangen ist. Hiermit wird ist ein sehr viel höherer Anspruch als z.B. der einer "Erhöhung von Kommunikationssicherheit" erhoben, mit welcher lediglich eine Verbesserung zugesagt wird. Zusätzlich zu der Garantierbarkeit wird auch nach der Neuigkeit und Originalität der von Herrn Danisch vorgeschlagenen Kriterien und Methoden zu fragen sein. Die zu erlangende Sicherheit kann dabei über eine rein verbale Beschreibung hinaus theoretisch bewiesen ebenso wie hilfsweise an praktischen prototypischen Beispielen demonstriert werden. Hierbei ist nicht nur ein positives Ergebnis von Wert, sondern ebenso das inverse negative in Gestalt der Aussage, dass Kommunikationssicherheit unter gegebenen Randbedingungen nicht garantierbar ist. In diesem Fall würden sich bestimmte Kommunikationsformen oder - dienste aus Sicherheitsgründen verbieten.

2. Durchführung

Im einleitenden Kapitel 1 definiert Herr Danisch den seiner Arbeit zugrundeliegenden Sicherheitsbegriff:

> "Die Sicherheit eines Systems gegen eine bestimmte Bedrohung ist die Fähigkeit des Systems, der böswilligen Herbeiführung der dieser Bedrohung zugrundeliegenden Zustände zu widerstehen oder gegen die daraus potentiell folgenden Schäden resistent zu sein." [S. 4]

"Damit wird Sicherheit relativ zum System und zur Bedrohung definiert. Eine von der Bedrohung abstrahierte, allgemeine Sicherheit gibt es hiernach nicht." [S. 5]

Weiter unten erweitert er das Begriffsgebäude um den Begriff "Feindbild" [S. 45]:

> "Das Feindbild ist die Gesamtheit der Kenntnisse, Annahmen und Vermutungen über den Angreifer."

wobei die Menge der zum Feindbild gehörenden Elemente komplementär zum Freundeskreis definiert wird entsprechend dem Grundsatz:

> "Wer oder was nicht zweifelsfrei zuverlässiger Freund ist, gehört zum Feindbild" [S. 45]

Gegenüber den Mechanismen zur Fehlererkennung und Fehlerbehebung grenzt sich Herr Danisch deutlich ab:

> "Die Absicherung gegen den Fehlerfall ist prinzipiell zwar nicht die Aufgabe der Systemsicherheit (nicht "Security", sondern "Safety"), muss aber bei der Wahl der Sicherungsmethoden berücksichtigt werden und wirkt sich u.a. darauf aus, ob etwa eine Schlüsselhinterlegung vorgenommen werden soll, ob Verschlüsselungsverfahren zu wählen sind, die ..." [S. 41]

Zum Begriff "Safety" steht bereits in der Einleitung [S. 3]

> " 'Safety' wird verwendet, wenn es um den Schutz vor ungewollten Ereignissen wie Unfällen, technischem Versagen usw. geht. Schaden droht hier nicht durch bösen Willen, sondern durch Zufälle, technische Unzulänglichkeiten, Defekte usw."

Eine ebenso deutliche Abgrenzung gegenüber den ebenfalls benachbarten Begriffen "Fehler", "Störung", "Ausfall" ("Mistake", "Error", "Fault", "Denial" u.a.m.) nimmt Herr Danisch nicht vor.

Nach diesen grundlegenden Begriffsdefinitionen und -abgrenzungen, die teilweise auch in späteren Kapiteln vorgenommen werden, gibt Herr Danisch überblicksartige Einführungen in Kryptographie (Abschnitt 1.3), bestehende Kriterien und Maßnahmenkataloge (Abschnitt 1.4), Zertifizierungen und Evaluierungen (Abschnitt 1.5) sowie Grundprobleme Formaler Modelle (Abschnitt 1.6). Mit sämtlichen untersuchten Ansätzen geht Herr Danisch hart ins Gericht:

"Die bestehenden und in der Praxis verwendeten Kriterien- und Maßnahmenkataloge erscheinen vom hier vertretenden Standpunkt der technischen Sicherheit aus betrachtet als unzureichend für den Entwurf und die Analyse von Kommunikationssystemen." [S. 12 unten]

"Diese Art der Sicherheitszertifizierung (Anm.: des BSI) ist nicht überzeugend." [S. 16 oben]

"Diese Anforderung (Anm.: an die Integrität des Servers) ist inadäquat und nicht geeignet, die erforderliche Sicherheit zu gewährleisten" [S. 19 Mitte]

"Die Vorgehensweise der Zertifizierung ist ungeeignet." [S. 20 oben]

"Solchen formalen Modellen ist aber auch gewisse Skepsis entgegenzubringen, was ebenfalls nachfolgend dargelegt wird." [S. 23 unten]
"Der fatale Fehler war [Anm.: s. Quelle [83]], dass man die Existenz des formalen Modells als wichtiger einschätzte als die saubere Erhebung der Interessen, und wohl sogar dem Irrtum unterlag, ersteres könne letzteres ersetzen.
Viel wichtiger als das formale Modell ist daher die Erhebung der Interessen (als Teil der Bedrohungsanalyse) und deren klare und systematische Darstellung anhand der in Kapitel 2 aufgezeigten Kriterien. Wenn sich das dann in ein formales Modell pressen lässt- schön." [S. 24 unten]
- und zahlreiche andere ähnliche Bewertungen.

Die Ausführungen des Kapitels 2 "Die System- und Bedrohungsanalyse" folgen der Vorstellung des bereits zitierten "Feindbildes", zu welchem Herr Danisch einleitend folgendes klarstellt:
"Die System-, Netzwerk- und Kommunikationssicherheit im allgemeinen und die Kryptographie im besonderen sind nicht nur Wissenschaft, sondern auch Kampfkunst; sie haben die Abwehr des Angreifers zum Ziel. Daher bleibt es nicht aus, dass gewisse Gemeinsamkeiten mit den physischen Kampf- und Kriegskünsten bestehen, auch wenn martialische Gepflogenheiten und kriegerische Stilmittel der wissenschaftlichen Vorgehensweise überwiegend fremd sind." [S. 44 unten/S. 45 oben]
Damit unterscheidet Herr Danisch im folgenden neben den "befreundeten" Parteien "Sender" und "Empfänger", sowie ggfls. einem vertrauenswürdigen "Dritten" den feindlichen "Angreifer".
Wichtigstes Merkmal ist dabei die

- räumliche oder zeitliche Position des Angreifers[S. 46 ff]

die bestimmt, an welcher Stelle der Datenkommunikation der Angriff zu erwarten ist [S. 46 Mitte]. Als weitere Kriterien führt Herr Danisch auf:

- Art des Angriffs [S. 49 Mitte]
  - passiv: "abhören" in der Rolle eines unbefugten Empfängers
  - aktiv: "fälschen" in der Rolle eines unbefugten Senders
- befreundete Parteien als Angreifer [S. 49 unten/S. 50 ff]
  - Sender, Empfänger, Dritte Partei
- Angriffszweck [S. 52/ S. 53]
  - Ausspionieren von Inhalten
  - beweisfähige Verwendung gegenüber Dritten
- Aufwand und Kosten des Angriffs [S. 53 unten/S. 54]
  - absolut, relativ

sowie bezogen auf das Schutzobjekt, d.h. die zu schützenden Inhalte als wichtigstes Kriterium den

- Sicherungszweck mit
  - Vertraulichkeit, Integrität, Authentizität, Vollständigkeit (= Echtheit) [S. 54 unten/S. 55 ff]

sowie

- weitere Sicherungsziele [S. 57 ff]
  - (Un-)Beweisbarkeit gegenüber Dritten
  - Verfügbarkeit (resp. "Denial of Service")
  - frühe Angriffserkennung
  - Beweislast (z.B. bei "Telebanking")
  - Fehlerkorrektur und -resistenz
  - Begrenzung der Sender- und Empfängerpositionen

In dem Abschnitt 2.5.3 Komponenten [S. 63 ff] betrachtet Herr Danisch die zu schützenden Kommunikationsinhalte, bzw. deren Träger und unterscheidet diese nach

- Nutzlast, z.B. verschlüsselte Daten
- Hilfslast mit Sender- und Empfängeradressen, bzw. - Identitäten
- Redundanz und Irrelevanz, z.B. Signaturen und Sitzungsschlüssel
- verbergende Umgebung, z.B. für Zwecke der "Steganographie"
- Umfang/Energie
- Ort und Zeit der Übertragung
- Schutz gegen multiple Angriffe (z.B. über "Anonymous Remailer")

- Kosten und Reaktion der Partei

Die Betrachtung von

- Zeitlichen und räumlichen Beschränkungen durch die befugten Parteien selbst
- Schadenserwartung
- Schutzobjekt Sicherungsmaßnahme (z.B. "Stille Alarme")

runden den Kriterienkatalog ab [S. 67 unten/S. 68]. Unter dem zuletzt genannten Kriterium stellt Herr Danisch fest:

"Gegenstand der Betrachtung waren bisher nur Schutzobjekte, die unabhängig von den Sicherungsmaßnahmen sind. Es besteht aber die Gefahr, dass durch Sicherungsmaßnahmen neue Schutzobjekte entstehen, denn Sicherungsmaßnahmen sind meist keine Problemlösungen, sondern Problemverlagerungen (s. Abschnitt 4.3)" [S. S. 68 oben] und leitet damit zum Kapitel 3 über.

Zu Beginn des Kapitels 3. Sicherungsmethoden stellt Herr Danisch begrifflich klar, dass er im vorhandenen Kontext "mit 'Methoden' die verschiedenen Wirkungsweisen bezeichnet, die einen Angriff verhindern oder erschweren sollen, mit 'Maßnahmen' konkrete technische Ausgestaltung von Methoden." [S. 69 oben] In der Übersichtstabelle Tab. 3.1 [S. 70] stellt Herr Danisch für die von ihm betrachteten Angriffs- /Verteidigungsszenarien geeignete GegenMaßnahmen dar. Die Tabelle 3.1 stellt damit gleichzeitig den Katalog der vorgeschlagenen Methoden vor, die im folgenden zusammengefasst und teilweise ergänzt um Auszüge der Original- Erläuterungen aufgelistet werden sollen:

- "3.2 Bewertung und dynamische Auswahlverfahren [S. 70 unten/S. 71 oben]
  Die stärkste Methode zur Abwehr von Angriffen ist die Vermeidung von Situationen, in denen überhaupt erst eine Gefährdung, bzw. ein Schutzbedürfnis entstehen können." [S. 70 unten]
  Bei der technischen Realisierung muss unterschieden werden zwischen Mechanismen, die beim Entwurf festgelegt werden und solchen, die erst zur Laufzeit ausgewählt werden können.
  Hierbei wird wiederum unterschieden zwischen folgenden zwei Methoden:
  - a priori- Bewertung und
  - a posteriori- Bewertung.

  "Diese beiden nichtverhindernden Methoden können damit Teil der verhindernden Methoden für neue Angriffe werden." [S. 71 Mitte]

- 3.3 Spezifikationstreue und Korrektheit [S. 71 Mitte/S. 72]
  "Die empirische Untersuchung von realen Angriffen zeigt, dass ein großer Teil der erfolgreichen Angriffe Systemlücken ausnutzt, die entstanden sind, weil das tatsächliche System von der Spezifikation abweicht (z.B. weil es verändert wurde), spezifikationswidrig verwendet wurde oder schlicht fehlerhaft ist [...]." [S. 71 Mitte]
  ...
  "Deshalb muss gewährleistet werden, dass das System in einem Zustand ist und bleibt, der der Spezifikation entspricht und der dem Entwurf der Sicherheitsmechanismen zugrunde gelegt wird. Das System wird selbst zum Schutzobjekt. Zu unterscheiden ist hier zwischen Beeinträchtigungen aufgrund von Fehlern im System oder Fehlbedienung der befugten Partei und aufgrund von Angriffen. Erstere gehören in den Bereich der Korrektheit und Verifikation, was ausserhalb des Themas der Arbeit liegt. Gegen Angriffe kann das System mit den gleichen Methoden geschützt werden, wie andere Schutzobjekte auch." [S. 72 oben]

- 3.4 Veränderung des Kosten/Nutzenverhältnisses [S. 72 unten/S. 73 f]
  "Eine Anhebung des Angriffsaufwandes, insbesondere eine Verschlechterung des Verhältnisses zum Nutzen des Angriffs für den Angreifer wirkt daher dem Angriff entgegen." [S. 73 oben]

- 3.5 Erschwerung der Angriffsvorbereitung [s. S. 74 unten/S. 75 f]
  "Die Betrachtung erfolgreicher Angriffe zeigt, dass ihnen in vielen Fällen eine Vorbereitung des Angreifers auf den Angriff vorausgeht.
  ...

Da jede Sicherungsmaßnahme letztlich auf eine Erschwerung des Angriffs hinauslaufen soll, ist eine gesonderte Betrachtung erst dann gerechtfertigt, wenn eine Differenzierung zwischen dem Angriff und der Angriffsvorbereitung möglich ist und die Vorbereitung nicht ohne weiteres als Teil des Angriffs angesehen werden kann. Eine Differenzierung ist möglich, wenn der Gegenstand der Vorbereitung der Angriff auf ein anderes Schutzobjekt ist, als es Ziel des Hauptangriffs ist." [S. 74 unten]

- 3.6 Organisatorischen Maßnahmen [S. 76 unten/ S. 77 ff]

  ...

  "Organisatorische Maßnahmen zielen darauf ab, die beabsichtigten, spezifizierten Kommunikationswege so zu legen, dass ein potentieller Angreifer nicht in Kontakt mit dem Schutzobjekt, also den zu schützenden Daten oder Rechnern kommen kann und die tatsächlichen Kommunikationswege möglichst auf die spezifizierten Wege einzuschränken." [S. 77 Mitte]

  ...

  "Beispiel 3.9 [S. 77 unten]
  Paketfilter

  ...

  Ursprünglich gehört das Filtern von Paketen zum Zwecke der Systemsicherheit aber nicht zur Spezifikation von Routern, deren eigentliche Aufgabe nur ist, Datenpakete in Richtung des Empfängers zu transportieren. Es hat daher Router gegeben, die bei hoher Last wegen geringer eigener Rechenleistung nicht mehr in der Lage waren, den normalen Betrieb zu erhalten. Für diesen Fall haben die Router zum Notbetrieb 'auf Durchzug geschaltet und unbesehen jedes Paket durchgereicht. Dies kann im Rahmen ihrer tatsächlichen Spezifikation (nämlich Netzwerkfunktion, nicht Security) durchaus als zulässig angesehen werden. Erst die Zweckentfremdung als Sicherheitselement hat die Spezifikation verschoben und damit zu spezifikationswidrigem Verhalten geführt und die Sicherheit beeinträchtigt." [S. 77 unten/S. 78 oben]

  ...

  "3.6.1.1 Firewalls
  Ein allgemein sehr bekanntes und weit verbreitetes Beispiel für eine organisatorische Sicherungsmaßnahme ist die 'Firewall', mit der Netzsegmente voneinander getrennt werden und so eine der Netztopologie entsprechende Parteienpartition erzeugt wird." [S. 78 Mitte]

  ...

  "3.6.1.2 Zugriffsrechte
  Ein vornehmlich im Betriebssystembereich anzutreffende organisatorische Maßnahme, ..., sind die Zugriffsberechtigungen,..." [S. 78 unten/S.79 oben]

  ...

  "3.6.1.5 Virtuelle Elemente und Umgebungen
  Ein weiteres Beispiel sind die virtuellen Elemente und Umgebungen, die oft eingeführt werden, um eine organisatorische Trennung in Form eines Programms zwischen reale Elemente und unbefugte Parteien zu bringen. Hierzu gehören u.a. auch Postscript- Interpreter, die JAVA Virtual Machine, aber auch Unix- Gerätetreiber und bessere Betriebssysteme."
  [S. 79 Mitte]

  ...

  "3.6.2 Sicherung der Sekundärinformationen
  Eine organisatorische Sicherung ist dann nicht mehr unmittelbar möglich, wenn die Position des Angreifers nicht klar von der Position befugter Empfänger zu trennen ist. Dieses Problem tritt auch beim Schutz der Sekundärinformationen (z.B. IP- Adressen, URLs, Telefonnummern, E- Mail- Adressen) bzw. der Nutzlasten auf, weil diese nicht in beliebiger Weise geschützt werden können. ... Würde man diese Information in der gleichen Weise wie die Primärinformation schützen, könnte der technische Transport nicht mehr funktionieren

oder nur noch dann, wenn jede Transporteinrichtung ihrerseits als befugter Sender und Empfänger behandelt werden würde, was mit zu hohem Aufwand verbunden ist." [S. 79 unten]

...

"3.6.2.1 Verlagerung in höhere Schichten

Jedem Transportmedium haftet eine Abstraktionsebene an, die durch die Trennung zwischen Hilfs- (Anm.: Sekundärinformationen) und Nutzlasten (Anm.: Primärinformationen) indiziert wird." [S. 80 oben]

...

"Diese befugte Transporteinrichtung muss dann auch dafür sorgen, dass die Sekundärinformation 'nach Durchquerung von Feindesland' wieder auf die zugehörige Schicht gebracht wird." [S. 80 Mitte]

- 3.7 Seiteneffektdämpfende Maßnahmen [S. 82 Mitte]

  "In realen Systemen werden Informationen nicht immer nur auf den beabsichtigten, spezifizierten Wegen übertragen. In vielen Fällen gibt es versteckte, aus den verschiedensten Gründen nicht ohne weiteres erkennbare oder vermeidbare 'Informationslecks' durch unbeabsichtigte Seiteneffekte.
  Ziel von Sicherungsmaßnahmen muss es daher sein, diese Effekte möglichst zu vermeiden und damit unspezifizierten Kontakt eines potentiellen Angreifers mit dem Schutzobjekt zu verbinden." [S. 82 Mitte]

  ...

  "Bemerkung 3.17:

  Verhältnis zur Spezifikationstreue und Eingrenzung

  Es besteht ein gewisse Ähnlichkeit zwischen den Maßnahmen zur Dämpfung der Seiteneffekte und zur Sicherstellung der Spezifikationstreue (Abschnitt 3.3). Beide richten sich gegen unerwünschtes Verhalten des Systems.
  Die Maßnahmen zur Sicherstellung der Spezifikationstreue richten sich aber gegen fehlerhaftes Verhalten des Systems und seiner Sicherheitsmechanismen, gehören also vornehmlich zum Themenkreis der Korrektheit.
  Die Dämpfung von Seiteneffekten soll unerwünschte Eigenschaften des Systems verhindern, die nicht spezifikationswidrig sind, weil entweder unsichere Eigenschaften nicht gegen eine Spezifikation verstoßen, die nicht aus Sicherheit ausgelegt ist, oder das System ausserhalb der Spezifikation betrieben wird. Beides ist kein Fehler des Systems im Sinne der Unkorrektheit. Eigenschaften eines Systems ausserhalb seiner Spezifikation zu fordern ist jedoch prinzipiell nicht möglich, weil dies dem Begriff der Spezifikation widerspricht. Sobald man Eigenschaften fordert, hat man sie spezifiziert.
  Ansatzstelle für seiteneffektdämpfende Maßnahmen muss daher die Erweiterung der Spezifikation des Systems sein. Sie gehören damit enger zum Problemkreis der Sicherheit (...)." [S. 83 Mitte]

- 3.8 Kryptographische Maßnahmen [S. 83 unten]

  ...

  "Bemerkung 3.19:

  Schutzobjekt Geheimnis

  Kryptographische Methoden stellen stets eine Problemverlagerung auf das Schutzobjekt Geheimnis dar. Daher ist bei ihrer Anwendung grundsätzlich das Geheimnis als neues Schutzobjekt zu berücksichtigen.

  Bemerkung 3.20:

  Verhältnis zu organisatorischen Maßnahmen

  Wie aus Definition 3.18 hervorgeht, besitzen kryptographische Maßnahmen selbst keine angriffsverhindernde Wirkung. Sie erzeugen lediglich eine Partition, d.h. sie machen Parteien technisch unterscheidbar.

Erst die Konbination mit einer organisatorischen Maßnahme - auch wenn diese dabei trivial ausfallen kann- erbringt die eigentliche Schutzwirkung. So kann etwa durch eine Signatur die Authentizität einer Nachricht bewiesen werden, weil sich der Autor durch die Kenntnis des Geheimnisses vom Angreifer unterscheidet." [S. 84 Mitte]

- 3.9 Verschleiernde Maßnahmen [S. 85 Mitte]

  ...

  "Verschleiernde Maßnahmen sind nicht notwendigerweise 'vollwertige' Sicherungsmaßnahmen, sondern können auch eine leichte Erhöhung der Sicherheit mit geringem Aufwand erlauben, also 'billig' sein. Sie werden zur Unterstützung anderer Maßnahmen eingesetzt. ...
  Verschleiernde Maßnahmen zielen in der Regel darauf ab, den Aufwand des Angreifers zu erhöhen." [S. 85 unten]

  ...

  "Bemerkung 3.22:
  Schutz gegen absichtslose Angriffe
  Durch die Erschwerung der Erfolgsdetektion wirken verschleiernde Maßnahmen gut gegen Angriffe, in deren Erfolgsdetektion nur wenig Energie gesteckt wird oder die erst gar nicht mit einer klaren Vorstellung des Angreifers über den Erfolg betrieben wird.
  Hierzu gehören insbesondere absichtslose und unsystematische Angriffe (z.B. ungezieltes und willkürliches Abhören von Kommunikationseinrichtungen) und Zufallsfunde ('Gelegenheit macht Diebe')." [S. 87 unten]

- 3.10 Schadensbegrenzung [S. 87 unten]

  "Der Nutzen für den Angreifer und der Schaden für den Verteidiger, die durch einen erfolgreichen Angriff entstehen, können, sie müssen aber nicht gleich bzw. von gleichem Umfang sein. Unabhängig von der Senkung des Angriffsnutzens (...) ist daher der mittlere oder maximale Schaden für den Verteidiger zu begrenzen." [S. 87 unten]

  ...

  "3.10.2 Entkopplung der Mechanismen [S. 88 Mitte]
  Werden zur Sicherung eines Systems verschiedene Maßnahmen oder Mechanismen eingesetzt, ist zu untersuchen, inwieweit die Sicherheit eines Mechanismus von der anderer abhängt und ob das Durchbrechen oder Umgehen eines Mechanismus dem Angreifer Vorteile für den Angriff gegen einen anderen bringt." [S. 88 Mitte]

- 3.11 Angriffserkennung und - nachweis [S. 89 ff]

  "Gefährlicher als der Angriff ist der vom Verteidiger unbemerkte (erfolgreiche oder erfolglose) Angriff. Der Verteidiger muss daher auch Maßnahmen ergreifen, um den Angriff zu erkennen und ihn ggfls. sogar Dritten gegenüber nachweisen zu können.
  3.11.1 Implizite Erkennung
  Die implizite Angriffserkennung verwendet nur Merkmale und Eigenschaften, die nicht (oder nicht ausschliesslich) zum Zwecke der Sicherung erzeugt wurden, sondern die für die Funktion des Systems notwendig oder unabhängig vom System vorgegeben sind. Hierzu gehört insbesondere die Plausibilitätsprüfung.
  Bemerkung 3.24:
  Plausibilitätsprüfung
  Grundsätzlich sind alle Adressen, Routen und Protokolle der verwendeten Übertragungseinrichtungen auf ihre Eignung zur Plausibilitätsprüfung zu untersuchen." [S. 89]

  ...

  "3.11.2 Explizite Erkennung
  Angriffserkennende Maßnahmen dienen der frühzeitigen Erkennung des Kontaktes eines Angreifers mit dem Schutzobjekt, auf deren Grundlage geeignete Reaktionen zum Schutz gegen Daten und Maßnahmen gegen den Angreifer eingeleitet werden können, um so weiteren

Schaden zu verhindern oder bereits eingetretenen Schaden zu begrenzen oder wieder zu beheben, allgemein auch um den Angriff Dritten gegenüber nachzuweisen." [S. 90 oben]

...

"Die Erkennung eines Angriffs erfordert Kriterien, anhand derer Angriffe von legalen Aktionen unterschieden werden können. Das bedeutet, dass einer Aktion (und auch deren Ausbleiben) eine gewisse Redundanz innewohnt.

...

Die notwendige Redundanz kann explizit zum Zweck der Sicherung hinzugefügt werden, sie kann aber im Einzelfall auch schon anderweitig hinzugekommen sein (Beispiel: Plausibilitätsprüfung der Pfadangaben bei E-Mail und News)." [S. 90 Mitte/unten]

- 3.12 Reaktionen während und nach dem Angriff [S. 91 Mitte]

  "3.12.1 Objektdestruktive Maßnahmen

  Objektdestruktive Maßnahmen haben zum Ziel, sensible Schutzobjekte im Falle eines Kontaktes mit dem Angreifer zu vernichten, bevor dieser (weiteren) Nutzen aus dem Kontakt ziehen kann. Hierzu gehören auch Negativlisten, wie sie z.B. über gestohlene Kreditkarten geführt werden." [S.01 Mitte]

  ...

  "3.12.1.1 Adaptive Maßnahmen

  Adaptive Maßnahmen sind eine Sonderform der objektdestruktiven Maßnahmen (...). Während die Objektvernichtung auch für den Verteidiger von Nachteil sein kann, liegt der Schwerpunkt hier auf der Anpassung an die Angriffssituation und dem Ziel, das Schutzobjekt nur für den Angreifer, nicht aber für den Verteidiger zu entwerten." [S. 92 oben]

  ...

  "3.12.2 Offensive Maßnahmen

  Offensive Maßnahmen sind den objektdestruktiven Maßnahmen (...) ähnlich; der Unterschied besteht darin, dass die Maßnahme (vornehmlich) gegen den Angreifer gerichtet ist. " [S. 93]

In Kapitel 4 „Bewertung von Sicherheitsmechanismen" betrachtet Herr Danisch die Wirkungsweise einzelner Sicherheitsmechanismen, sowie deren mögliche Umgehungen mit Hilfe des ISO/OSI-Schichtenmodells. In Erweiterung des standardmässigen 7 Schichten umfassenden Modells führt er eine zusätzliche Schicht 8 für den Benutzer (Interessensträger, Partei) ein, für die er als Hauptgrund anführt, dass die im üblichen 7- Schichtenmodell bisher nicht berücksichtigte Instanz „Mensch" die Ursache für eine Vielzahl von Sicherheitsproblemen bilde, die ansonsten nicht geeignet behandelt werden könnten. Im Gegensatz dazu ist jedoch der Anwender üblicherweise auf Schicht 7 angesiedelt, so dass hier nicht nur eine unnötige Modellerweiterung vorliegt, sondern auch offensichtlich ein grundsätzliches Missverständnis des Schichtenmodells.
Um die Art der von Herrn Danisch getroffenen Aussagen besser beurteilen zu können, sei auch an dieser Stelle aus der Arbeit selbst zitiert:
„4.1.2 Schutz der Primär- und Sekundarinformationen [S. 101 Mitte]

...

4.1.2.1 Langfristiger Schutz der Primärinformationen

Je höher eine Sicherungsmaßnahme im Schichtenmodell angeordnet ist, desto langfristiger ist einerseits ihre Wirkung (...), die so auf den obersten Schichten sogar vom Übertragungsvorgang abstrahiert werden kann. Desto geringer ist andererseits aber auch ihre Ausdehnung auf Sekundärinformationen. Eine ‚hohe' Absicherung zur Gewährleistung von Integrität und Authentizität kann u.U. sehr teuer werden, da vor einer Angriffserkennung jeweils der gesamte Stack durchlaugfen werden muss. Bezieht sich eine Signatur auf ein Schicht-7- Paket von erheblicher Größe (E- Mail, Web- Seite usw.), so muss erst das ganze Paket gelesen werden, bevor der Angriff erkannt werden kann. Die Erbringung des Aufwandes zur Abarbeitung der Schichten unterhalb der Sicherung kann Angriffsziel sein.

Durch die größere Ausdehung der Sicherungswirkung können aber auch die Kosten ‚pro Byte' niedriger liegen." [S.101 Mitte]

...

„4.1.2.3 Konsequenz Mehrfachsicherung [S.102 oben]
Wie gezeigt wurde, gibt es keine optimale Schicht für Sicherungsmaßnahmen; sowohl die ‚hohe' als auch die ‚niedrige' Absicherung haben Vor- und Nachteile. Die Konsequenz daraus ist, dass dann, wenn die Eigenschaften verschiedener Schichten genutzt werden müssen, eine mehrfache Absicherung stattfinden muss (...)."

...

„ 4.1.3 Resistenz gegen Umgehung [S. 103 Mitte]
„Jeder Sicherungsmechaismus bleibt wirkungslos, wenn der Angreifer einen Weg findet, der am Mechanismus vorbeiführt. Meist werden solche Umgehungen als ‚verdeckter' Kanal bezeichnet. Mechanismen müssen daher so entworfen und zusammengestellt werden, dass eine Umgehung unmöglich ist. Wie ein Mechanismus umgangen werden kann, lässt sich erschöpfend nur im Einzelfall beurteilen. Gerade im Zusammenhang mit dem Schichtenmodell lassen sich aber Angriffe darstellen, die selbst auf der Ausnutzung des Schichtenaufbaus der Kommunikationseinrichtungen beruhen. Diese Angriffe lassen sich klassifizieren und mit Hilfe dieser Einteilung systematisch ausschliessen.
Das Ausschliessen einer Umgehung bedeutet, dass der Angreifer auf diesem Weg nicht mehr an das Schutzobjekt gelangen kkann, und ist deshalb eine organisatorische Maßnahme. Ist eine Umgehung möglich, dann ist der organisatorische Schutz unzureichend." [S. 103 Mitte]

Hierbei werden folgende Umgehungen genannt und jeweils am Beispiel demonstriert:

- Überspringen (4.1.3.1 [S. 103 unten])
- Unterlaufen (4.1.3.2 [S. 104 Mitte ff])
- Horizontale Protokoll- Umgehung (4.1.3.3 [S. 109 unten f])
- Vertikale Protokoll- Umgehung (4.1.3.4 [S. 110 unten])
- Routen- und Adress- Umgehungen (S. 4.1.3.4 [S. 111 Mitte])
- Mischformen (4.1.3.6 [S. 111 unten])

Zum letzten Punkt sei zitiert:
„Zusätzlich sind auch Mischformen verschiedener Umgehungen möglich und beim Entwurf in Betracht zu ziehen. Beispielsweise ist die kompromittierende Abstrahlung eine Mischform aus Unterlaufen, weil alle Software und Protokollschranken unterlaufen werden, und einer horizontalen Umgehung auf Schicht 1, weil die vermeintliche elektrische Begrenzung des Rechners auf seine äusseren Abmessungen durch elektromagnetische Abstrahlung oder unbeabsichtigte Übertragungen über Stromkabel usw. umgangen wird." [S. 111 unten]

„4.2 Effektivität und Kosten [S. 112 oben]
Sicherungsmechanismen sind nicht immer völlig unüberwindbar; sie sollen und müssen dies oft auch gar nicht sein. Sofern ein geeignetes und zuverlässiges Angreifermodell besteht, genügt es, wenn die absolute oder sogar nur die relative Leistungsfähigkeit des Angreifers den Mechanismus nicht überwinden kann.
Deshalb müssen Beschreibung, Entwurf und Beurteilung von Mechanismen auch deren Stärke und Effektivität, d.h. deren Fähigkeit, einem Angriff zu widerstehen, miteinbeziehen. Dabei ist zu unterscheiden, ob die Angriffskosten den zu erwartenden Gewinn übersteigen oder mit den ihm zur Verfügung stehenden Mitteln nicht erbracht werden können." [S. 112 oben]

Hierbei werden folgende Kriterien betrachtet:

- Erfolg und Erfolgsdetektion (4.2.1 [S. 112 Mitte])
- Theoretische Schranken (4.2.2 [S. 112 unten])
- Angriffskosten (4.2.3 [S. 113 oben])
- Alterung (4.1.4 [S. Alterung])

„4.3 Nebenwirkungen und Anforderungen [S. 114 oben]
Sicherheitsmechanismen und die ihnen zugrunde liegenden Methoden haben nicht notwendigerweise nur die günstigsten Eigenschaften, derentwegen sie eingesetzt werden. Ihre Wirksamkeit hängt regelmäßig auch von der Einhaltung bestimmter Randbedingungen ab und bringt neue Anforderungen mit sich. Sicherheitsmechanismen können daher nur beurteilt und klassifiziert werden, wenn eine genaue Beschreibung auch dieser Eigenschaften vorliegt." [S. 114 oben]

Hierbei werden folgende Randbedingungen betrachtet:

- Abhängigkeit von Systemeigenschaften (4.3.1 [S. 114 Mitte])
- Eingriffstiefe und Nebenwirkungen (4.3.2 [S. 114 unten])
- Übersicherung (4.3.3 [S. 115 Mitte])
- Problemverlagerungen (4.3.4 [S. 116 Mitte])
- Abbildung auf technische Merkmale (4.3.5 [S. 116 unten])

Die Ausführungen zum Punkt „Problemverlagerungen" sollen wegen ihrer Grundsätzlichkeit zum Schluss noch zitiert werden:

„4.3.4 Problemverlagerungen [S. 116 Mitte]
Sicherheitsmechanismen und die ihnen zugrunde liegenden Methoden sind- soweit bisher bekannt- allgemein keine Problemlösungen, sondern Problemverlagerungen. Mit jeder Methode und jedem Mechanismus ergeben sich daher neue Probleme, die – wenn sie nicht schon durch das bestehende System mit den bisher ausgewählten Mechanismen und Methoden gelöst werden – durch neue Mechanismen und Methoden gelöst werden müssen.
Daraus resultieren neue Probleme, die im ursprünglichen System noch nicht gegeben waren und die durch neue Mechanismen und Methoden gelöst werden müssen. So ergibt sich eine Kette von Problemen und Problemlösungen, an deren Ende eine Menge von im Vergleich zum Urproblem leichteren Problemen, die nicht mehr durch technische Mittel lösbar sind, deren Lösung aber ausserhalb der Technik gefunden werden kann.
Bei der Auswahl und Beurteilung von Mechanismen ist eine komplette Beschreibung der gesamten Kette und der verbleibenden Restprobleme zu berücksichtigen."

Abschliessend zu Kapitel 4 gibt es noch Hinweise zu dem genannten nichttechnischen Bereich, die es dann wohl zu berücksichtigen gilt:

„4.4 Nichttechnische Eigenschaften [S. 117 Mitte]
Das Ziel von Sicherheitsmechanismen ist die technische Um- und Durchsetzung, weswegen technische Eigenschaften fraglos im Vordergrund stehen. Es gibt aber auch nichttechnische – hauptsächlich juristische – Randbedingungen, die bei der Beurteilung von Sicherheitsmechanismen zu berücksichtigen sind. Nachfolgend werden einige dieser Aspekte kurz angerissen, weil diese ausserhalb des Themas dieser Arbeit liegen." [S. 117 Mitte]

Hierbei werden im einzelnen genannt:

- Verbot und Gebot von Mechanismen (4.4.1 [S. 117 unten])
- Rechtstreue als Schutzobjekt (4.4.2 [S. 118 oben])
- Verbote und Gebote als Angriff (4.4.3 [S. 118 Mitte])
- Wirksamkeit (4.4.4 [S. 118 unten])

Die in dem sich hieran anschliessenden Kapitel 5 „Besondere Probleme staatlicher Kommunikationsüberwachung" dargelegten Ausführungen waren unter den gegebenen Randbedingungen so wenig nachvollziehbar, dass von einer detaillierteren Widergabe in vorliegenden Abschnitt Abstand genommen wurde.

3. Bewertung

Insgesamt fällt auf, dass von den in Kapitel 1 genannten Kriterien bei der Bewertung der Methoden in Kapitel 4 kaum eines verwendet wird. Weiterhin fällt auf, dass von den in Kapitel 3 genannten 11 Methoden- , bzw. Maßnahmenkategorien in Kapitel 4 nur zwei verwendet werden, nämlich die organisatorischen und die kryptographischen Maßnahmen (3.6 und 3.8). Ebenso fällt auf, dass die zu Beginn des Kapitels 4 als überaus wichtig erachtete zusätzliche 8. Schicht im ISO/OSI-Schichtenmodell nicht weiter verwendet wird.

Über die Kapitel 1 bis 4 hinweg fällt insgesamt auf, dass der gesamte Text aus einem Wechsel von sehr allgemeinen Feststellungen und jeweils sehr speziellen Beispielen dazu besteht. Es gibt keinerlei allgemeingültige Nachweise, geschweige denn Beweise zu irgendeiner Behauptung. Es gibt zahlreiche Hinweise, was denn zu beachten sei, aber was konkret zu tun ist, bleibt offen. Ebenso bleibt fraglich, ob und wie denn Kommunikationssicherheit überhaupt garantiert werden kann. Glaubt man den Ausführungen des Abschnitts „4.3.4 Problemverlagerungen" (s.o. und [S. 116 Mitte]) und so liegen die letztendlich zu suchenden Lösungen im nichttechnischen Bereich. Schaut man dann in dem abschliessenden „Abschnitt 4.4 Nichttechnische Eigenschaften" nach (s.o. und [S. 117 Mitte]), so findet man dort den Hinweis, dass diese Aspekte ausserhalb des Themas der vorgelegten Arbeit liegen. Nachvollziehbare Entwurfsmethodiken einschliesslichlich der notwendigen Diskussion und Lösung von Zielkonflikten („Trade Offs") fehlen vollständig.

Inhaltlich ist Arbeit von Herrn Danisch geprägt von der Modellvorstellung: "Sicherheit ist keine absolute Eigenschaft. Sie wirkt immer relativ gegenüber bestimmten Bedrohungen" [S. 24 oben]. Hierauf gründet sich Ablehnung existierender Ansätze, wie er sie beispielsweise im Abschnitt 1.6.1 "Grundprobleme Formaler Modelle" vorträgt. Deren Defizit sieht er darin, nur idealisierte Modelle zu beschreiben, so dass die zugehörigen formalen Spezifikationen naturgemäß unvollständig sein müssen, sei es, weil die Implementierung des realen Systems nicht konform zu dessen formaler Spezifikation ist, oder dass die formale Spezifikation aus Komplexitätsgründen nicht in der Lage ist, sämtliche möglichen Systemreaktionen unter sämtlichen möglichen Bedingungen zu erfassen. Im Gegensatz dazu schlägt er vor, das Sicherheitsinteresse der Kommunikationsteilnehmer gegenüber möglichen Angreifern als Ausgangspunkt aller Sicherheitsüberlegungen zu wählen. Diesen Ansatz positioniert er in der Einleitung seines Kapitels 2 "Die System- und Bedrohungsanalyse" gegenüber den zuvor kritisierten formalen Modellen wie folgt: "Sicherungsmaßnahmen sollen die Funktion des Systems *innerhalb* seiner Spezifikation möglichst wenig verändern oder beeinträchtigen (also möglichst *transparent* sein), während sie *ausserhalb* der Spezifikation größtmögliche Wirkung entfalten sollen (also *effektiv* sein). Kurz gesagt: Der befugte Benutzer soll möglichst wenig von den Maßnahmen merken, der Angreifer jedoch möglichst wirksam abgewehrt werden." [S. 29 Mitte]

Folgt man diesem Ansatz zunächst, so stellt sich die Frage, inwieweit dieser zum gewünschten Ziel der Arbeit, nämlich "Entwurfskriterien und Methoden zur Erlangung von Kommunikationssicherheit" bereitzustellen, geführt hat. Da ausser der schriftlichen Ausarbeitung keine weiteren Grundlagen für eine Beurteilung vorliegen, kann nur diese herangezogen werden. Hierbei konzentriert sich die Betrachtung zunächst auf das Kapitel 3 "Sicherungsmethoden", in dem die von Herrn Danisch konkret vorgeschlagenen Maßnahmen aufgeführt sind. Folgt man dabei weiterhin der von Herrn Danisch selbst vorgeschlagenen Unterscheidung zwischen "Angriff- nichtverhindernden Methoden" und "Angriff-verhindernden Methoden" [S.71 Mitte] und trifft diese Unterscheidung für den in den Abschnitten 3.2. bis 3.12 beschriebenen Maßnahmenkatalog, so kommt man zu folgendem Ergebnis:

- Angriff- verhindernde Methoden: 3.6 Organisatorische Maßnahmen
  2.8 Kryptographische Maßnahmen (lt. Danisch nur bedingt)
- Angriff- nichtverhindernde Methoden: alle übrigen (d.h. 9 von insgesamt 11)

Damit beantwortet sich die im Gutachten eingangs gestellte Frage nach einer mittels Danischer Methoden garantierbaren Kommunikationssicherheit für die Mehrzahl der Maßnahmen einzeln genommen negativ (wobei die übrigen unter 3.6 und 3.8 aufgeführten sogenannten sicheren Verfahren sämtlich nicht neu sind). Dagegen könnte der Kandidat einwenden, dass es nicht notwendigerweise zu den erklärten Sicherheitsinteressen eines Kommunikationsteilnehmers gehören muss, alle möglichen Angriffe wirksam zu verhindern, solange sich nur die Auswirkungen (z.B. der Schaden) in einem

vorgegebenen Rahmen halten. Hierüber ist in der Arbeit jedoch nichts ausgesagt und ist dieses ohne konkrete Anwendungsumgebung auch kaum möglich.
Herr Danisch hat diesen Anspruch ausser im Titel innerhalb seiner Arbeit auch nirgends erhoben, und dabei mit der Unzulänglichkeit, bzw. Komplexität formaler Spezifikationsmethoden argumentiert (s.o.). In Folge hat er eine Unterscheidung zwischen "Korrektheit" der spezifizierten Systemeigenschaften und "Sicherheit" vorgenommen, welches wegen der grundsätzlichen Bedeutung an dieser Stelle nochmals zitiert sein soll:

> "Zu unterscheiden ist hier zwischen Beeinträchtigung des Systems aufgrund von Fehlern im System oder Fehlbedienung der befugten Partei und aufgrund von Angriffen. Erstere gehören in den Bereich der Korrektheit und Verifikation, was ausserhalb des Themas dieser Arbeit liegt. Gegen Angriffe kann das System mit den gleichen Methoden geschützt werden, wie andere Schutzobjekte auch." [S. 72 oben]

Mit dieser Unterscheidung hat Herr Danisch einen entscheidenden Teil der Sicherheitsproblematik, nämlich die Frage nach der korrekten Funktion der beteiligten Systeme (Rechner- ebenso wie Kommunikationssysteme) ausgeklammert und so versucht, sich das Leben leichter zu machen. Darauf, dass ihm dies wohl nur unvollständig gelungen ist, ist er selbst verschiedentlich gestossen, wie die folgende Textstelle zu erkennen gibt:

> "Bemerkung 3.17:
> Verhältnis zur Spezifikationstreue und Eingrenzung
> Es besteht ein gewisse Ähnlichkeit zwischen den Maßnahmen zur Dämpfung der Seiteneffekte und zur Sicherstellung der Spezifikationstreue (Abschnitt 3.3). Beide richten sich gegen unerwünschtes Verhalten des Systems.
> Die Maßnahmen zur Sicherstellung der Spezifikationstreue richten sich aber gegen fehlerhaftes Verhalten des Systems und seiner Sicherheitsmechanismen, gehören also vornehmlich zum Themenkreis der Korrektheit.
> Die Dämpfung von Seiteneffekten soll unerwünschte Eigenschaften des Systems verhindern, die nicht spezifikationswidrig sind, weil entweder unsichere Eigenschaften nicht gegen eine Spezifikation verstoßen, die nicht aus Sicherheit ausgelegt ist, oder das System ausserhalb der Spezifikation betrieben wird. Beides ist kein Fehler des Systems im Sinne der Unkorrektheit.
> Eigenschaften eines Systems ausserhalb seiner Spezifikation zu fordern ist jedoch prinzipiell nicht möglich, weil dies dem Begriff der Spezifikation widerspricht. Sobald man Eigenschaften fordert, hat man sie spezifiziert.
> Ansatzstelle für seiteneffektdämpfende Maßnahmen muss daher die Erweiterung der Spezifikation des Systems sein. Sie gehören damit enger zum Problemkreis der Sicherheit (...)." [S. 83 Mitte]

wobei der letzte Absatz in die richtige Richtung weist. Statt jedoch spätestens an dieser Stelle zu erkennen, dass sein Ansatz der Unterscheidung zwischen "Korrektheit" und "Sicherheit" nicht durchzuhalten ist und in eine Sackgasse führt, und einen völlig anderen Weg einzuschlagen, versucht Herr Danisch mit Rabulistik, sich dieser Erkenntnis zu entziehen. Ein solcher alternativer Ansatz hätte beispielsweise darin bestehen können, mit erweiterten Systemgrenzen und zunehmend vollständigen Spezifikationen an das Problem heranzugehen, und die ganze martialische Modellwelt von Angreifern und Angegriffenen hinter sich zu lassen. Letztere hätte im übrigen dann ihre Berechtigung gehabt, wenn es um die rechnergestützte Verfolgung von Hackern gegangen wäre (s. [128] Clifford Stoll : "The Cuckoo's Egg"), doch das ist ein vollständig anderes Thema.
Nach obiger Kritik und der Feststellung dieses kapitalen Irrwegs von Herrn Danisch möchte ich mir die Mühe ersparen, alle sonstigen Fehler und Schwächen innerhalb seiner Arbeit aufzulisten. So komme ich zusammenfassend zu der Beurteilung, dass es sich bei dem von Herrn Danisch vorgelegten Entwurf einer Dissertation um eine Arbeit mit fundamentalen gedanklichen und methodischen Fehlern und Schwächen handelt, die ich der Fakultät für Informatik in keinem Fall zur Annahme empfehlen kann.

(Prof. Dr.- Ing. Werner Zorn)
- Zweitgutachter -