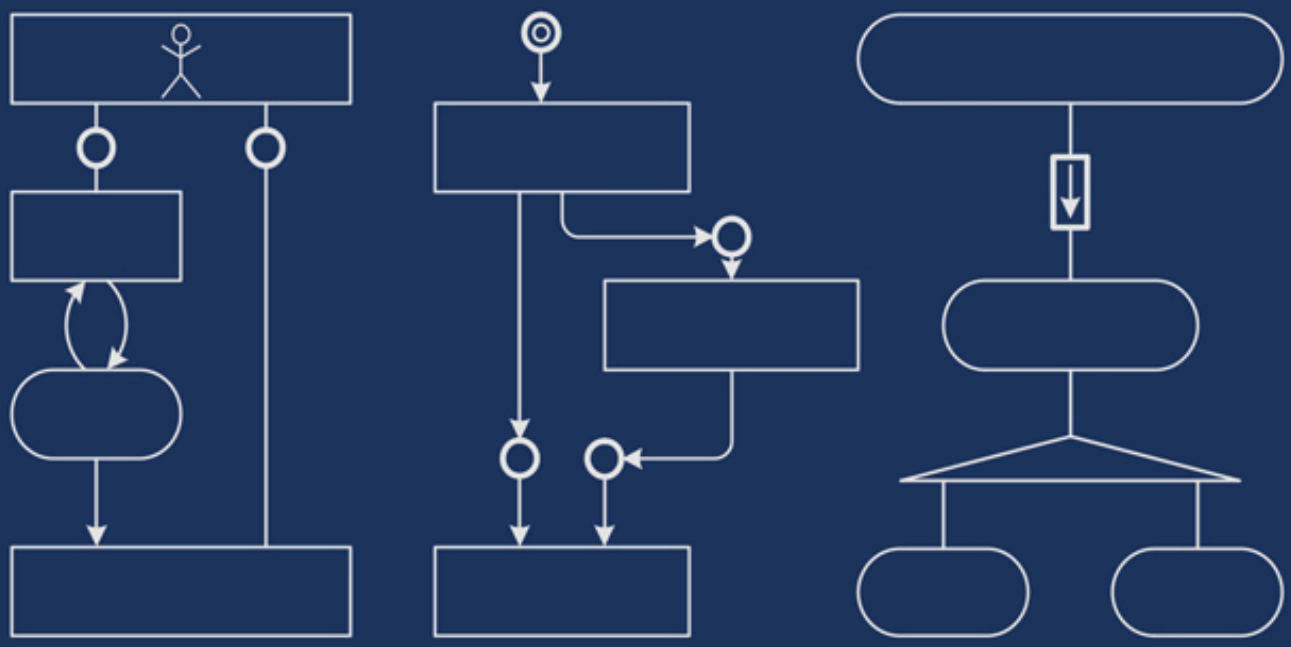
Marco Siegert

Forensisches Reverse Engineering

Entwurf eines Teilgebietes der digitalen Forensik unter besonderer Berücksichtigung der Systemmodellierung



2. Auflage

MsT.

Marco Siegert, geboren 1978 in Lutherstadt Wittenberg. 1996 Abitur am Albert-Schweitzer-Gymnasium in Coswig (Anhalt). 1997 bis 2000 Studium an der Fachhochschule der Polizei des Landes Brandenburg im Studiengang für den gehobenen Polizeivollzugsdienst. Abschluss als Diplom-Verwaltungswirt. 2002 bis 2006 Studium am Hasso-Plattner-Institut für Softwaresystemtechnik der Universität Potsdam. Abschluss als Bachelor of Science in Software Engineering. 2011 bis 2016 Studium im Masterstudiengang Digitale Forensik an der Hochschule Albstadt-Sigmaringen. Abschluss als Master of Science in Digitale Forensik. 2005 bis 2011 Projektleiter für die Internetwache der Polizei des Landes Brandenburg. 2012 bis 2013 Sachbearbeiter im Landeskriminalamt der Polizei des Landes Brandenburg mit dem Arbeitsschwerpunkt Mobilfunkforensik. Seit 2014 Sachbearbeiter im Bundespolizeipräsidium für Grundsatzangelegenheiten und Systementwicklung in der digitalen Forensik.

Inhalt

Abstract

Polizeibehörden setzen in der digitalen Forensik im zunehmenden Maße auch Reverse Engineering ein. Auf den ersten Blick scheint hierbei der Fokus auf der Analyse von Schadsoftware und dem Aufspüren und Ausnutzen von systemseitigen Fehlern und Schwachstellen zu liegen. Hierbei wird jedoch übersehen, dass sich mittels Reverse Engineering auch forensische Erkenntnisse über Softwaresysteme und digitale Spuren in solchen Systemen gewinnen lassen. Reverse Engineering ist für die digitale Forensik daher von fundamentaler Bedeutung. In der Arbeit wird die These vertreten, dass sich ein entsprechendes Fachgebiet *Forensisches Reverse Engineering* abgrenzen lässt. Es wird herausgearbeitet, dass sich aus einem forensisch motivierten Reverse Engineering eine Reihe von besonderen Herausforderungen ergeben. Analog zur Softwaretechnik zeigen sich diese insbesondere bei der Modellierung, Beschreibung und Kommunikation über Softwaresysteme. Die Arbeit befasst sich auch mit der Rolle der Systemmodellierung bei der Bewältigung dieser Herausforderungen. Im ersten Teil der Arbeit werden zunächst die erforderlichen Grundlagen der Systemmodellierung, der klassischen Forensik und des Reverse Engineerings aufbereitet. Hierbei wird auf eine bewährte Systemtheorie für programmierte digitale Systeme und eine allgemeine Modelltheorie zurückgegriffen. Die Grundlage für die klassische Forensik bilden deren Einbettung in das deutsche Strafverfahren sowie eine Theorie über klassische Spuren. Im zweiten Teil der Thesis wird ein eigener Ansatz zur Abgrenzung eines Fachgebietes *Forensisches Reverse Engineering* entwickelt. Auf der Basis

einer erweiterten Theorie über digitale Spuren wird nicht nur den Gegenstand des Fachgebietes präzisiert, sondern auch dessen innere Systematik. Hierbei bilden die zuvor eingeführte Systemtheorie, Modelltheorie und die klassische Spurentheorie den begrifflichen und konzeptionellen Rahmen. Die Bezüge zur Systemmodellierung, zur klassischen Forensik sowie zum Reverse Engineering werden hergestellt und die kommunikativen Herausforderungen beschrieben. Abschließend wird herausgearbeitet, wie Systemmodellierung bei deren Bewältigung helfen kann.

Danksagung

Nachdem ich im Oktober 2011 das berufsbegleitende Masterstudium „Digitale Forensik“ an der Hochschule Albstadt-Sigmaringen begonnen hatte, wurde mir sehr schnell bewusst, dass dieses Vorhaben weniger mit einem „Kurzstreckenlauf“, sondern vielmehr mit einem „Marathon“ vergleichbar ist. Meine Vermutungen haben sich bestätigt. Nach nunmehr fünf interessanten sowie anregenden, jedoch auch aufopferungsvollen und entbehrungsreichen Jahren lege ich mit dieser Arbeit nun zum Abschluss des Studiums meine Masterthesis vor.

Dass mir die hierfür erforderlichen Ressourcen und Freiräume zur Verfügung standen, wodurch die Unternehmung letzten Endes auch nur gelingen konnte, verdanke ich vielen Menschen in meinem familiären, persönlichen und beruflichen Umfeld. Den größten Dank schulde ich meiner Frau Stephanie, die mich bereits seit 20 Jahren bei meinen „Projekten“ unterstützt und mit der ihr eigenen selbstlosen und sehr liebenswerten Art den Rücken stärkt. Ich kann mir keinen anderen Menschen vorstellen, der über einen so langen Zeitraum so viel Geduld aufbringt. Ich danke auch meinem Sohn Maximilian, der häufig auf seinen Vater verzichten musste. Gleiches gilt für meine Familie sowie meine Freunde und Bekannte, die mich in dieser Zeit nicht so häufig zu Gesicht bekamen. Ich bedanke mich zudem bei meinen ehemaligen und aktuellen Vorgesetzten, die dem berufsbegleitenden Studium aufgeschlossen gegenüberstanden und Verständnis für die Mehrbelastung aufbrachten.

Ohne die richtige Ausbildung und ohne entsprechende geistige Anregung hätte ich das Thema meiner Thesis nicht finden und bearbeiten können. Mein besonderer Dank geht an Siegfried Wendt und Peter Tabeling, die meine Lehrer am Hasso-Plattner-Institut der Universität Potsdam waren. Sie haben mir eine Sichtweise auf Softwaresysteme vermittelt, die mir bei der Bewältigung des Themas sehr geholfen hat. Darüber hinaus danke ich Peter Tabeling, dass er sich bereiterklärt hat, für die Thesis die Rolle des zweiten Prüfers zu übernehmen. Bei der Bearbeitung des Themas hat er mir stets mit seinem Fachwissen und seiner Erfahrung in der Systemmodellierung zur Seite gestanden.

Weiterer Dank geht an Felix Freiling, Andreas Dewald und Werner Massonne, die meine Lehrer an der Friedrich-Alexander-Universität Erlangen-Nürnberg waren. Felix Freiling und Andreas Dewald haben ganz wesentliche Beiträge zur theoretischen Fundierung der digitalen Forensik geleistet und das Fachgebiet in der deutschen Hochschullandschaft etabliert. Ohne diese Vorarbeiten würden meiner Thesis ganz wesentliche Grundlagen fehlen. Felix Freiling danke ich, dass er für die Thesis die Rolle des ersten Prüfers übernommen hat. Mein besonderer Dank gilt Werner Massonne, der sich von einer Idee begeistern ließ und mich bei der theoretischen Ausrichtung der Thesis unterstützt sowie während der Bearbeitungszeit in der ihm eigenen ruhigen und freundlichen Art betreut hat.

Durch Felix Freiling wurde meine Arbeit für den „Zukunftspreis Polizeiarbeit 2017“ vorgeschlagen, der jährlich im Rahmen des Europäischen Polizeikongresses vergeben wird. Durch die Mitglieger der Expertenjury wurde die Arbeit zusammen mit fünf weiteren Abschlussarbeiten (3x Bachelor, 3x Master) in die engere Auswahl für die Preisverleihung genommen. Leider konnte sich meine Arbeit bei der Expertenjury nicht gegen die Konkurrenz

durchsetzen. Bemerkenswert bleibt jedoch, dass im Bereich der Masterarbeiten alle Abschlussarbeiten aus dem berufsbegleitenden Masterstudiengang „Digitale Forensik“ der Hochschule Albstadt-Sigmaringen eingereicht wurden. Ich freue mich für die Preisträger 2017 und spreche Ihnen meine Anerkennung für ihre Leistung und ihren wissenschaftlichen Beitrag aus.

Die deutschen Polizei- und Sicherheitsbehörden tun sich mit der dienstlichen Unterstützung von berufsbegleitenden Studiengängen derzeit noch immer schwer. Aus Gesprächen weiß ich, dass nur einige wenige Kommilitonen aus dem öffentlichen Dienst von ihren Arbeitgebern finanzielle und zeitliche Unterstützung erhalten. Auf der anderen Seite suchen die gleichen Arbeitgeber auf einem stark umworbenen Arbeitsmarkt händeringend IT-Spezialisten für die digitale Forensik. Liegt es da nicht auf der Hand, die dienstlichen Rahmenbedingungen für berufsbegleitende Studiengänge und engagierte Mitarbeiterinnen und Mitarbeiter zu verbessern?

Marco Siegert

Geleitworte

Niemand versteht mehr, wie komplexe Softwaresysteme genau funktionieren. Wenn wir wissen wollen, wie es zu einem bestimmten Systemverhalten kam, dann beginnt die Spurensuche am und im System: Mit Methoden des „Reverse Engineering“ werden die internen Wirkzusammenhänge der Softwaresysteme offengelegt. Je komplexer das System, desto mühseliger ist die Aufgabe – heute mehr Kunst als Handwerk. Wenn jedoch die untersuchten Systeme Beweismittel in Gerichtsverfahren sind, dann muss man systematisch und nachvollziehbar vorgehen. Und man muss die Ergebnisse angemessen dokumentieren und kommunizieren können. Wie das geht, zeigt auf eindrucksvolle Art und Weise das vorliegende Buch von Marco Siegert. Das Werk ist außerordentlich gehaltvoll. Es vereinigt lehrbuchartige Übersichten dreier Gebiete (Systemmodellierung, Forensik, Reverse Engineering) und entwickelt mit dem Ansatz des *Forensischen Reverse Engineering* eine zentrale Grundlage für die Polizeiarbeit im digitalen Zeitalter – denn ein präzises, nachvollziehbares und dokumentiertes Verständnis für die Funktionsweise technischer Geräte ist die Voraussetzung für qualifizierte Einsichten und Hilfestellung im Rahmen der Strafverfolgung. Praktikern rate ich dazu, dieses Werk in moderaten Häppchen zu konsumieren, denn die Menge an Definitionen, Konzepten und Literaturverweisen mag nach anfänglicher Lektüre schwer verdaulich wirken. Jedoch lassen sich die Kapitel durchaus auch einzeln lesen; umfangreiche Querverweise und ein hilfreiches Register erleichtern zudem die Navigation, einem Nachschlagewerk gleich. So wird mit zunehmender Seitenzahl das (auch wiederholte) Lesen zum

Genuss voller differenzierter Einsichten. Ein Buch, das dem Gebiet der digitalen Forensik guttut.

Felix C. Freiling

Miss Marple hatte es leicht. Um ein Verbrechen aufzuklären und den Täter zu überführen genügten ihr scharfer Verstand und ihre Sinne. Der Tatort war meist die Stelle, an der man das arme Opfer vorgefunden hat. Die Spur, mit der man den Täter überführen konnte, zeigte sich als Abdruck seines Stiefels. Das mögliche Tatwerkzeug, z. B. eine in der Nähe gefundene Flinte, war als solches schnell zu erkennen. In der heutigen modernen Welt hätte es die berühmte Detektivin sicherlich schwerer. Der Fortschritt der Digitalisierung und Vernetzung hat neue Formen der Kriminalität ermöglicht, bei denen die Tat im virtuellen Raum der Rechner und Datenströme stattfindet. Der „Einbruch“ in einen Server hinterlässt keinen Stiefelabdruck. Hier sind die Beweismittel nicht mehr „handfest“ im wörtlichen Sinne, sondern nur mit profunden Kenntnissen der Informationstechnik und den geeigneten Werkzeugen zu finden. Für die digitale Forensik stellen sich damit grundsätzliche Fragen. Sind Begriffe und Methoden übertragbar, die aus einer Zeit stammen, als das Internet noch in den Kinderschuhen steckte? Welche Bedeutung haben z. B. „Tatort“ oder „Spur“ in einer digitalen Umgebung, die weltweit vernetzt ist und in der Informationen beliebig kopiert oder verändert werden können - und bestenfalls deren kryptisches, binäres Abbild in Speichern von Computersystemen physisch nachweisbar ist? Marco Siegert findet Antworten auf diese Fragen, indem er Begriffe und Methoden des Reverse Engineering und der klassischen Forensik aufgreift und zusammenführt. Mit beeindruckender Sorgfalt und Gründlichkeit zeigt er nicht nur die Relevanz und Nützlichkeit des Reverse Engineering für ein Gebiet auf, das im Ursprung gar nicht dessen

Gegenstand war. Er findet darüber hinaus erweiterte (Be-)Deutungen für die bewährten Konzepte der Forensik, sodass diese ihre Anwendbarkeit behalten - auf einem Feld, wo es heute umso wichtiger ist. Entsprechend seinem wissenschaftlichen Anspruch geht Marco Siegert jedoch weiter und benennt mit dem *Forensischen Reverse Engineering* einen neuen Schwerpunkt für Forschung und Lehre, für den er auch die sich ergebenden Fragestellungen aufzeigt. Für ihn als Polizeibeamten gehört dazu natürlich die Frage, wie das Forensische Reverse Engineering seine Ergebnisse am effektivsten in die Praxis einbringen kann. Er schlägt vor, auf bewährte Methoden der Systemmodellierung zurückzugreifen. Diese gäben dem Forensiker die nötigen Mittel an die Hand, um seine Erkenntnisse verständlich und präzise aufzubereiten, etwa bei gutachterlichen Tätigkeiten in Gerichtsverfahren.

Peter Tabeling

Abkürzungen

ASCII	American Standard Code for Information Interchange
BSI	Bundesamt für Sicherheit in der Informationstechnik
BtMG	Betäubungsmittelgesetz
CD	Compact Disc
CF	CompactFlash
DFRWS	Digital Forensic Research Workshop
DNA	Deoxyribonucleic acid
DVD	Digital Versatile Disc
EMRK	Europäische Menschenrechtskonvention
ER-Modell	Entity-Relationship-Modell
FMC	Fundamental Modeling Concepts
GG	Grundgesetz
HTML	Hypertext Markup Language
IEEE	Institute of Electrical and Electronics Engineers
I.e.S.	Im engeren Sinne
I.w.S.	Im weiteren Sinne
IP	Internet Protocol (Internetprotokoll)
IT	Informationstechnik
IuK	Information und Kommunikation
MAC	Media Access Control
NAS	Network Attached Storage
RAM	Random-Access Memory
ROM	Read-Only Memory
SD	Secure Digital
StGB	Strafgesetzbuch

StPO	Strafprozessordnung
TAM	Technical Architecture Modeling
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UML	Unified Modeling Language
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time (Koordinierte Weltzeit)
VM	Virtuelle Maschine

Abbildungen

Tabellen

Definitionen

1 Einleitung

Inhalt

1.1 Motivation für die Thesis

Als Bestandteil des Masterstudiengangs „Digitale Forensik“ der Hochschule Albstadt-Sigmaringen habe ich 2013 im Rahmen einer Hausarbeit im Modul „Reverse Engineering“ ein Windows Binärprogramm analysiert. Dabei waren mir weder der Hochsprachen-Quelltext noch die Dokumentation des analysierten Programms bekannt. Das Programm forderte als Eingabe eine Seriennummer und prüfte diese auf Gültigkeit. Ich habe das Programm mittels IDA[1] analysiert und den Prüfalgorithmus für die Seriennummer ermittelt. Des Weiteren habe ich meine Vorgehensweise dokumentiert und die von mir über das Programm gewonnenen Erkenntnisse auf der Grundlage von Assembler-Quelltext erläutert sowie mittels der Fundamental Modeling Concepts (vgl. *Knöpfel* et al. 2005; *Tabeling* 2006, S. 253-321) modelliert.

Im Rahmen der Hausarbeit wurden durch mich ca. 170 Zeilen Assemblercode analysiert und dokumentiert. Die zu

Grunde liegende Programmdatei war knapp 9 Kilobyte groß und kann somit als „kleines“ Programm bezeichnet werden. Die Funktionsweise des Programms zu verstehen, bewerte ich im Nachgang als beherrschbare Herausforderung. Obwohl beherrschbar, war die Erstellung der Hausarbeit für mich dennoch mit einem verhältnismäßig hohen Aufwand verbunden. Dieser Aufwand ergab sich nicht aus der eigentlichen Analysetätigkeit, sondern vielmehr aus der geforderten Dokumentation der Vorgehensweise und der Ergebnisse sowie dem Anspruch, das mittels Reverse Engineering gewonnene Wissen über das System angemessen zu kommunizieren.

Bei der Hausarbeit hat mir u.a. auch mein Wissen über Softwaresysteme und ihre Modellierung geholfen, welches mir im Rahmen meines Studiums der „Softwaresystemtechnik“ am Hasso-Plattner-Institut der Universität Potsdam insbesondere durch Prof. Dr.-Ing. *Siegfried Wendt* und Dr.-Ing. *Peter Tabeling* vermittelt wurde. Speziell bei der Dokumentation und der Modellierung konnte ich hinsichtlich der Anforderungen einige Parallelen zur Softwaretechnik erkennen. Die Hausarbeit hat für mich einige grundsätzliche Fragen aufgeworfen:

1. Welche Bedeutung hat Reverse Engineering für die digitale Forensik?
2. Welche forensisch relevanten Informationen können mittels Reverse Engineering gewonnen werden?
3. Kann Reverse Engineering als Methode der Softwaretechnik unverändert für forensische Zwecke übernommen werden?
4. Ist der Aufwand für Dokumentation, Modellierung und Kommunikation in der Praxis gerechtfertigt?
5. Wie können Erkenntnisse im Reverse Engineering angemessen modelliert, beschrieben und kommuniziert

werden?

6. Können etablierte Methoden und Techniken aus der Softwaretechnik und insbesondere aus der Systemmodellierung bei der Modellierung, Beschreibung und Kommunikation helfen?
7. Lässt sich eine Verbindung zwischen der Systemtheorie der Softwaretechnik und der Theorie über digitale Spuren herstellen?

Auf Grund meiner beruflichen Tätigkeit[2] war mir bekannt, dass durch die deutschen Sicherheitsbehörden in der Praxis bereits Methoden und Techniken des Reverse Engineering für forensische Zwecke (unabhängig von der Schadsoftwareanalyse oder der Umgehung von Sicherheitsmechanismen) eingesetzt werden. Nach meiner persönlichen Einschätzung wird der Bedarf an Reverse Engineering und entsprechend ausgebildeten Spezialisten in den kommenden Jahren zunehmen. Eine theoretische Fundierung des Reverse Engineering innerhalb der digitalen Forensik erscheint mir daher nicht nur aus wissenschaftlicher Sicht, sondern auch für die Strafverfolgungspraxis der deutschen Sicherheitsbehörden relevant. Bei einer groben Sichtung der Fachliteratur stellte ich Folgendes fest:

1. Reverse Engineering als eine grundlegende Methode aufzufassen, mittels der forensisch relevante Information über digitale Systeme gewonnen werden können (beispielsweise Erkenntnisse über digitale Spuren), ist nicht verbreitet.
2. Innerhalb der digitalen Forensik wird Reverse Engineering derzeit überwiegend als Methode für die Analyse von Schadsoftware und zur Umgehung von Sicherheitsmechanismen eingesetzt.

3. In der digitalen Forensik ist die Anwendung von Methoden und Techniken der Systemmodellierung und eine damit einhergehende systemorientierte Sichtweise nicht verbreitet.

Aus den vorgenannten Gründen habe ich mich dazu entschlossen, die Anwendung von Reverse Engineering in der digitalen Forensik unter besonderer Berücksichtigung der Systemmodellierung als Gegenstand meiner Masterthesis zu wählen.

1.2 Eingrenzung des Themas

Unter dem Begriff „Reverse Engineering“ werden üblicherweise Methoden und Techniken zur Analyse von Systemen zusammengefasst. Die Ziele von Reverse Engineering bestehen im Allgemeinen darin, die inneren Strukturen eines Systems und deren wechselseitige Abhängigkeiten zu identifizieren sowie eine Repräsentation des betrachteten Systems in einer anderen Form oder auf einem anderen Abstraktionsniveau zu gewinnen. Innerhalb der Softwaretechnik wird Reverse Engineering überwiegend der Softwarewartung zugerechnet und als Vorstufe zum Reengineering gesehen. Daher wird Reverse Engineering in diesem Anwendungsbereich primär durch die Perspektive eines Ingenieurs bestimmt, der für einen Auftraggeber ein neues System erstellen oder ein bereits bestehendes System modifizieren soll. Die Systemmodellierung stellt dabei entsprechende Methoden, Verfahren und Standards zur Beschreibung und Modellierung von Systemen bereit. Sie hat sich in der Softwaretechnik insbesondere als Hilfsmittel zur Komplexitätsbeherrschung, Dokumentation, Kommunikation und Arbeitsteilung bewährt.

In der digitalen Forensik werden Methoden der Informatik zur gerichtsfesten Sicherung und Auswertung digitaler

Beweismittel angewendet. Forensiker greifen dabei in ihrer praktischen Arbeit auch auf Methoden und Techniken aus dem Bereich des Reverse Engineering zurück. Im Gegensatz zur Sichtweise eines konstruierenden Ingenieurs wird dieser Anwendungsbereich durch die Perspektive eines analysierenden Forensikers bestimmt. Dessen Aufgabe besteht in der Regel darin, spezielle forensische Problemstellungen zu lösen bzw. forensische Fragestellungen eines juristisch oder kriminalistisch motivierten Auftraggebers zu beantworten. In Abgrenzung zur Softwaretechnik reichen die Einsatzszenarien für Reverse Engineering hierbei von der Unterstützung der Kryptoanalyse, der Überwindung von Sicherheitsmechanismen und der Schadsoftwareanalyse über die Analyse unbekannter Dateiformate, Datenbankstrukturen und Netzwerkprotokolle bis hin zu umfangreichen Untersuchungen „regulärer“ System- und Anwendungssoftware.

Nach eigenen Erfahrungen ist die praktische Vorgehensweise im Reverse Engineering aktuell dadurch gekennzeichnet, dass forensisch relevante Systeme und Datenstrukturen in der Regel durch einzelne Spezialisten analysiert werden. Eine Kommunikation über Analyseergebnisse mit anderen Spezialisten sowie Außenstehenden ist die Ausnahme. Wenn eine Kommunikation stattfindet, erfolgt diese üblicherweise sehr nahe an der technischen Realisierung (Assemblersprachen und hexadezimale Repräsentationen). Eine systematische und strukturierte Modellierung und Beschreibung findet man selten. In den Anwendungsbereichen Kryptoanalyse, Überwindung von Sicherheitsmechanismen und Schadsoftwareanalyse werden zielgerichtet statische und dynamische Analysemethoden eingesetzt und Systeme häufig als „Whitebox“ untersucht. Bei der Analyse regulärer System- und Anwendungssoftware zur Ermittlung forensisch

relevanter digitaler Spuren hingegen dominiert die „Blackbox“-Methodik. In einigen wenigen Anwendungsgebieten, beispielsweise in der Mobilfunk- und Netzwerkforensik, ist bereits vereinzelt ein arbeitsteiliges Vorgehen zwischen einzelnen Spezialisten und auch zwischen verschiedenen Sicherheitsbehörden zu beobachten.

Als eine mögliche Folge der gesellschaftlichen und technologischen Veränderungen ist es nach eigener Bewertung nicht unwahrscheinlich, dass der Bedarf für Reverse Engineering in der digitalen Forensik zunehmen wird. So wird beispielsweise der herkömmliche stationäre Computer mit einer überschaubaren Anzahl von klassischen Anwendungsprogrammen zunehmend durch mobile und smarte Endgeräte mit einer unüberschaubaren Masse an mobilen Anwendungen („Apps“) verdrängt. Dadurch vervielfacht sich die Anzahl der forensisch relevanten Software. Zugleich ist Anwendungssoftware „kleiner“ geworden, die Innovations- und Entwicklungszyklen haben sich verkürzt und die Anzahl der Entwickler erhöht. Auf der anderen Seite ermöglichen die wachsenden Speichergrößen sowie zunehmende Prozessorleistungen und Netzwerkbandbreiten größere und komplexere Systemsoftware sowie die Realisierung komplexer und verteilter Anwendungen.

Die Hersteller von forensischen Werkzeugen können mit diesen Veränderungen sowie der Dynamik nur schwer Schritt halten. In der Folge nehmen die Defizite bei der werkzeuggestützten und automatisierten forensischen Arbeit zu. Die Sicherheitsbehörden versuchen diese Defizite mit eigenem Personal, Fachwissen und einer Arbeitsteilung bei der Analyse forensisch relevanter Systeme und Anwendungen auszugleichen. Die steigende Nachfrage nach sicheren Systemen und Verschlüsselung erhöht die

Komplexität und den Aufwand für forensische Analysen zunehmend. Die zuvor beschriebenen Aspekte und Zusammenhänge lassen sich grundsätzlich auch auf den Bereich der Schadsoftwareanalyse übertragen.

Aus der forensischen Perspektive ergeben sich eine Reihe spezieller Anforderungen an das Reverse Engineering. So müssen forensische Erkenntnisse auf einer wissenschaftlichen Vorgehensweise beruhen sowie objektiv nachprüfbar und ggf. auch wiederholbar sein. Dies gilt grundsätzlich auch für Erkenntnisse, die mittels Reverse Engineering gewonnen werden. Des Weiteren muss ein Forensiker in der Lage sein, über seine Analyseerkenntnisse sowohl mit anderen Spezialisten als auch mit seinen Auftraggebern zu kommunizieren. Hierfür bedarf es geeigneter Dokumentations- und Kommunikationsmöglichkeiten.

Die aus den gesellschaftlichen und technologischen Veränderungen resultierenden Herausforderungen für das Reverse Engineering machen zukünftig unter Umständen eine noch intensivere Arbeitsteilung erforderlich. In diesem Fall wäre ein weiterer Anstieg des Aufwandes für Modellierung, Beschreibung und Kommunikation zu erwarten. Erschwerend kommt hinzu, dass im forensischen Kontext häufig sehr wenige Informationen als Ausgangspunkt für eine Analyse vorliegen. So kann in der Regel nicht auf einen kommentierten Quellcode in einer Hochsprache oder Systemdokumentation zurückgegriffen werden.

Mit den aktuellen Ansätzen der Praxis (und hier insbesondere die nur unzureichend ausgeprägten Fähigkeiten zur Modellierung, Beschreibung und Kommunikation) können nach eigener Einschätzung die beschriebenen Herausforderungen langfristig nicht

zufriedenstellend bewältigt werden. Die für die Zwecke der Softwaretechnik entwickelten Methoden und Standards der Systemmodellierung könnten entsprechende Lösungsansätze liefern.

Die Hauptthesen der Arbeit werden wie folgt formuliert:

1. Innerhalb der digitalen Forensik kann ein Teilgebiet „Forensisches Reverse Engineering“ mit spezifischen Merkmalen abgegrenzt werden.
2. Im forensischen Reverse Engineering bestehen besondere Herausforderungen bei der Modellierung, Beschreibung und Kommunikation über Strukturen von programmierten digitalen Systemen.
3. Diese Herausforderungen lassen sich durch die Anwendung von Systemmodellierung beherrschen.

Das Ziel der vorliegenden Arbeit besteht darin, entsprechende Beziehungen zwischen Systemmodellierung, Reverse Engineering und digitaler Forensik aufzuzeigen. Des Weiteren sollen charakterisierende Merkmale von forensisch motivierten Reverse Engineering herausgearbeitet werden. Die Abbildung 1.2-1 zeigt schematisch die Einordnung des Themas in eine Struktur der Wissenschaften. Die Teilgebiete, die im Fokus dieser Arbeit stehen, wurden mit grauer Schattierung hervorgehoben.

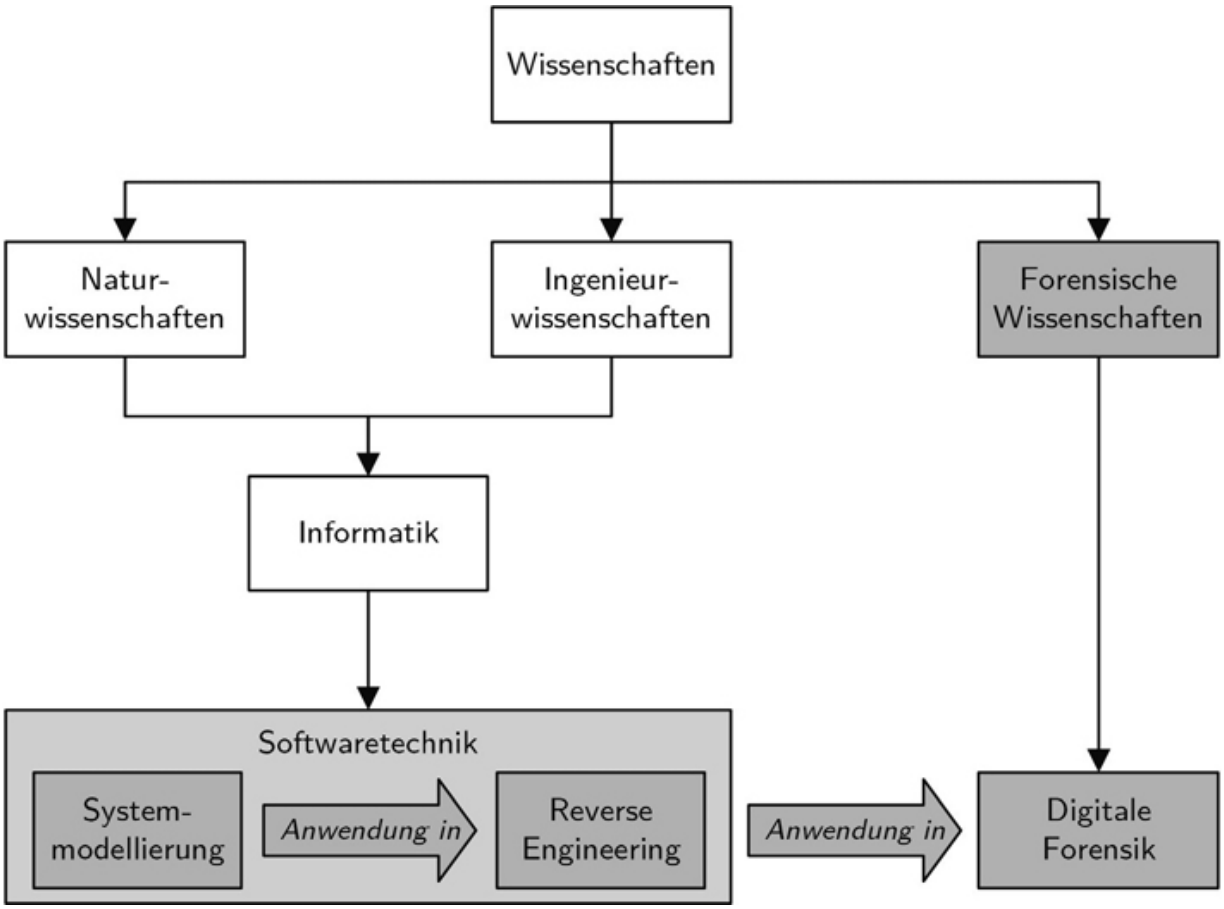


Abbildung 1.2-1: Einordnung des Themas

1.3 Abgrenzung des Themas

Die Masterthesis ist als theoretische sowie interdisziplinäre Literaturarbeit angelegt. Zu den im Abschnitt 1.1 aufgeworfenen Problem- und Fragestellungen sollen allgemeingültige Antworten und Lösungen erarbeitet werden. Hierzu erfolgen grundlegende Betrachtungen zur Systemmodellierung (inklusive Systemtheorie), zur klassischen und digitalen Forensik (inklusive Spurentheorie) und zum Reverse Engineering. Zwischen den verschiedenen Gebieten werden Zusammenhänge aufgezeigt und neue Verknüpfungen hergestellt. Die nachfolgenden Punkte umfassen Aspekte, die im Rahmen der Masterthesis nicht betrachtet werden:

1. In den Themenbereichen Systemmodellierung, klassische Forensik, digitale Forensik und Reverse Engineering erfolgen keine historischen Ausführungen. Historische Zusammenhänge werden nur in dem Maße erörtert, wie sie für das Grundverständnis erforderlich sind.
2. Da die Masterthesis als theoretische Arbeit konzipiert wurde, erfolgt keine Betrachtung von Werkzeugen und ausführlichen Beispielen zur Systemmodellierung und zum Reverse Engineering. Die Ausführungen zur Systemmodellierung werden möglichst unabhängig von bestimmten Modellierungsansätzen oder Modellierungssprachen gehalten.
3. Die Betrachtungen konzentrieren sich auf die Klasse der „programmierten digitalen Systeme“. Reverse Engineering von nicht programmierten Systemen bildet keinen Schwerpunkt.
4. Bei den Einsatzszenarien für Reverse Engineering erfolgt eine Beschränkung auf solche mit forensischem Hintergrund aus dem Bereich der staatlichen Strafverfolgung. Hierbei wird das Thema im Wesentlichen aus der Perspektive deutscher Polizei- bzw. Sicherheitsbehörden betrachtet.

1.4 Überblick über die Thesis

Neben der Einleitung (im aktuellen **Kapitel 1**) und dem abschließenden Fazit (**Kapitel 6**) besteht die Arbeit im Kern aus den folgenden vier Kapiteln:

Kapitel 2 – Systemmodellierung: In diesem Kapitel werden die erforderlichen Grundlagen der Systemmodellierung vermittelt. Auf der Basis einer bewährten Systemtheorie über programmierte digitale Systeme sowie einer allgemeinen Modelltheorie werden

zentrale Grundbegriffe eingeführt und Zusammenhänge zwischen den Begriffen erörtert. Einen Schwerpunkt bilden hierbei klassische Methoden und Vorgehensweisen zur Modellierung solcher Systeme sowie deren Anwendung in der Softwaretechnik.

Kapitel 3 – Klassische Forensik: Anschließend werden wesentliche Grundlagen der Forensik ausgeführt, wobei der Fokus auf der klassischen (nicht-digitalen) Forensik liegt. Danach werden auf der Basis eines eigenen Entity-Relationship-Modells zentrale Grundbegriffe, Konzepte und Zusammenhänge einer klassischen Spurentheorie eingeführt. Abschließend werden die Funktion der Forensik im Strafverfahren sowie die klassischen forensischen Methoden erläutert.

Kapitel 4 – Reverse Engineering: Im letzten Grundlagenkapitel liegt der Schwerpunkt auf den für die Arbeit erforderlichen Grundlagen des Reverse Engineering aus der Sichtweise der Softwaretechnik. Hierbei bilden die im Kapitel 0 eingeführte System- und Modelltheorie das begriffliche Fundament. In einem ersten Schritt wird der Begriff Reverse Engineering herausgearbeitet und vom Forward Engineering und Reengineering abgegrenzt. Anschließend konzentrieren sich die Ausführungen auf die Programm- und Softwareanalyse, die eine Reihe von Basismethoden und -techniken für das Reverse Engineering bereitstellen. Darauf aufbauend erfolgt dann die Beschreibung der Kernmethoden des Reverse Engineerings.

Kapitel 5 – Forensisches Reverse Engineering: Dieses Kapitel bildet den inhaltlichen Schwerpunkt der vorliegenden Arbeit. Zuerst wird ein eigener Ansatz zur Abgrenzung eines Fachgebietes *Forensisches Reverse Engineering* innerhalb der digitalen Forensik präsentiert. Als Gegenstand des Fachgebiets werden auf der Basis eines

eigenen Entity-Relationship-Modells zentrale Grundbegriffe, Konzepte und Zusammenhänge einer digitalen Spurentheorie eingeführt. Hierbei bilden insbesondere die System- und Modelltheorie aus Kapitel 2 sowie die klassische Spurentheorie aus Kapitel 3 die konzeptionelle und begriffliche Grundlage. Darauf aufbauend wird das Fachgebiet definiert und Möglichkeiten zu seiner Binnenstrukturierung sowie Außenabgrenzung vorgestellt. Einen weiteren Schwerpunkt bilden die Bezüge zur klassischen Forensik, zum Reverse Engineering und zur Systemmodellierung. Schließlich werden die für das forensische Reverse Engineering prägenden Kommunikationsaspekte und -herausforderungen beschrieben und es wird aufgezeigt, wie die Systemmodellierung bei deren Bewältigung helfen kann.

1.5 Gestaltung und Form

Die Kapitel gliedern sich in Abschnitte und Unterabschnitte. Diese dreistufige numerische Basisgliederung der Arbeit bildet die Grundlage für Querverweise im Text. Als ergänzende Orientierungshilfe dienen nach Bedarf weitere Zwischenüberschriften.

Jedem Kapitel wird ein eigenes Inhaltsverzeichnis vorangestellt, welches neben der dreistufigen Basisgliederung auch die Zwischenüberschriften umfasst. Um eine bessere Orientierung zu ermöglichen, werden die Kapitel und Abschnitte jeweils mit einer kurzen Inhaltsbeschreibung eingeleitet.

Da der Text viele Definitionen enthält, wurde zusätzlich zum Abbildungs- und Tabellenverzeichnis ein eigenes Definitionsverzeichnis erstellt. Definitionen werden im Text zusätzlich durch einen umschließenden Rahmen optisch hervorgehoben.