

IT-Forensik

– Technologie für Datendetektive

Finden und Auswerten digitaler Spuren verbotener Aktivitäten kann IT-Forensiker vor große Probleme stellen. Wachsende Datenmengen und Spuren verbotener Aktivitäten, die sich auf den ersten Blick nicht von Spuren erlaubter Aktivitäten unterscheiden, lassen die praktische IT-forensische Arbeit zu einer Suche nach der Nadel im Heuhaufen werden. Am CASED entwickelt das Fraunhofer SIT Lösungen, um die Suche und Analyse digitaler Spuren effektiver und effizienter zu machen. Dies erfordert Technologiewissen in unterschiedlichen Bereichen wie Multimedia, Dateisysteme, Data Mining.

► IT Forensics – Technology for Data Detectives

Detection and analysis of digital traces for elucidating forbidden activities that involve IT systems can pose severe problems for IT forensic investigators. Increasing amounts of data and traces of illegal activities that, from a technical perspective, do not differ from traces of day-to-day work make IT forensic investigation often similar to looking for a needle in a haystack. At CASED researchers from Fraunhofer SIT develop solutions that make search and analysis of digital traces more effective and efficient. This requires knowledge in several areas, e.g., multimedia, file systems, data mining.

Martin Steinebach, Markus Schneider, Michael Waidner • Die Forensik umfasst Methoden, die zur Aufklärung und Rekonstruktion von Tathergängen dienen. Hierzu werden Spuren gesucht, untersucht und ausgewertet. Die Ergebnisse der Methoden dienen dazu, Ermittlungshypothesen

Robuste Hashfunktionen

In der Multimediasicherheit werden Alternativen zu den kryptographischen Hashfunktionen entwickelt, die nicht die binäre Gleichheit der Datei zur Erkennung nutzen, sondern die menschliche Wahrnehmung als Ausgangspunkt sehen. Dabei ist das Ziel, verschiedene Ausprägungen eines Werkes, z. B. eines Bildes, welches mit verschiedenen Stärken durch JPEG komprimiert wurde, als gleich zu identifizieren. Andere Werke sollen aber unabhängig von ihrer Ähnlichkeit als nicht gleich erkannt werden. Da diese Funktionen ähnlich wie kryptographische Hashfunktionen eingesetzt werden, aber im Gegensatz zu diesen robust gegen akzeptable Veränderungen sind, werden solche Funktionen robuste Hashfunktionen genannt.

zu unterstützen oder zu widerlegen. Die IT-Forensik umfasst den Teil der Forensik, in der digitale Spuren behandelt werden, die beispielsweise durch den unrechtmäßigen Einsatz von IT-Systemen entstehen, wie Logdaten. Zur IT-forensischen Untersuchung digitaler Spuren sind geeignete Software-Werkzeuge erforderlich. Die IT-Forensik ist nicht mit der computergestützten Forensik zu verwechseln, bei der mittels Computern auch physische Spuren untersucht werden können, z. B. Fingerabdrücke.

IT-Forensik und IT-Sicherheit ergänzen sich beide in sehr sinnvoller Weise, um die Interessen von rechtmäßigen Nutzern bezüglich ihrer Daten oder IT-Systeme zu schützen. Da diese Interessen in der Praxis nicht immer durch Methoden der IT-Sicherheit effektiv geschützt werden können, braucht man Lösungen, um unrechtmäßige Handlungen in IT-Systemen aufzuklären zu können und dem Geschädigten zu seinem Recht zu verhelfen. In der Praxis kann man nicht erwarten, dass IT-Systeme gegen jeden denkbaren Missbrauch geschützt sind, zum Beispiel wegen Sicherheitslücken durch Implementierungsfehler oder durch Fehlkonfigurationen.

So wie für die klassische Forensik beispielsweise mit der Ballistik und der Gentechnik viele unterschiedliche Expertisen notwendig sind, sind auch für die IT-Forensik verschiedene Kompetenzen relevant. Als Beispiele hierfür sind etwa die Technologiebereiche Multimedia, Netzwerke, Email, grafische Datenverarbeitung, Datenbanksysteme, digitale Signalverarbeitung, Data Mining, Speichermedien und Dateisysteme zu nennen.

Zur Verdeutlichung der Relevanz der IT-Forensik sei auf reale Vorfälle verwiesen: Laut Bundeskriminalamt (BKA) wurden 2009 in Deutschland 50.254 Fälle von IT-Kriminalität im engeren Sinn registriert, 2008 wurde in bereits mehr als jedem fünften Fall von Wirtschaftskriminalität das Internet benutzt. Die Gesamtschadenssumme betrug 2008 in Deutschland 3,34 Mrd. Euro. Weitere Herausforderungen ergeben sich durch illegale digitale Inhalte (Kinderpornographie, Gewaltvideos), deren Erstellung und Verbreitung heute technisch sehr einfach möglich und kaum zu verhindern sind.

Hat eine kriminelle Handlung stattgefunden, dann besteht die Aufgabe des IT-Forensikers darin, geeignete Datenquellen zu identifizieren, diese si-

Michael Waidner



herzustellen und zur Rekonstruktion des Tathergangs oder zur Beweisführung Datenspuren zu finden. IT-Forensiker werden jedoch auch aktiv, wenn keine konkreten Hinweise auf verbotene Handlungen vorliegen, zum Beispiel bei routinemäßigen Überprüfungen von Datenbeständen in Unternehmen auf Fälle von Wirtschaftskriminalität. Hierbei ist dem IT-Forensiker bei seiner Arbeit oft nicht klar, wonach genau er suchen soll.

Bei solchen Suchen werden unter anderem statistische Tests eingesetzt, durch die Auffälligkeiten erkannt werden sollen.

Die umfangreichen Mengen an Daten, die bei der Spurensuche zu berücksichtigen sind, treiben die Untersuchungskosten in die Höhe und verlangen nach geeigneten IT-Lösungen. Das Problem bei der automatisierten Herangehensweise besteht jedoch darin, dass Spuren übersehen werden können

Abbildung 1

Digitale Bildforensik kann Unregelmäßigkeiten an Bildmaterial erkennen. So wurde das Original links verändert, indem der Golfball mit einem Kopierstempel mit Rasen übermalt und so gelöscht wurde. Das Ergebnis ist in der Mitte zu sehen. Ein forensisches Verfahren macht sichtbar, dass zwei Bereiche des Rasens identisch sind und weist so auf die Manipulation hin.



(False Negatives) oder zu viele Spuren gefunden werden, die sich als völlig harmlos herausstellen (False Positives). Dies wird in einigen Fällen dadurch erschwert, dass für verbotene Handlungen, die auf Missbrauch von Rechten in IT-Systemen basieren, aus technischer Sicht die gleichen Schrittabfolgen anfallen, wie sie von derselben Person viele Male für unkritische oder erwünschte Handlungen ausgeführt werden.

Im Folgenden werden einige Arbeitsgebiete der IT-Forensik, in denen Fraunhofer SIT am CASED aktiv ist, exemplarisch betrachtet.

Multimedia-Forensik: Erkennung verbotener Inhalte

Im Rahmen der forensischen Untersuchung von Datenbeständen wird unter anderem nach illegalem Bildmaterial gesucht. Hierbei handelt es sich in erster Linie um Kinderpornographie. Die Identifizierung kann auf Sichtung oder auf kryptographischen Hashverfahren beruhen, welche den Hashwert eines Bildes berechnen und diesen mit in einer Datenbank gespeicherten Hashwerten vergleichen. Ein Hashwert ist eine Zeichenfolge, die als eine Art Fingerabdruck für eine Datenmenge berechnet werden kann. Bei kryptographischen Hashverfahren besteht aber immer das Risiko eines Nicht-Identifizierens von entsprechendem Material. Dies ist immer dann der Fall, wenn Dateien nicht identisch kopiert werden, sondern beispielsweise Formatwandlungen unterlaufen. Am CASED werden sogenannte robuste Hashverfahren auf ihre Eignung hin zum automatischen Erkennen von Bildmaterial in forensischen Untersuchungen geprüft.

Kamera-Forensik: Erkennung von Datenquellen

Ein Großteil aller Fotos wird heute mit digitalen Kameras erstellt. Das gilt beispielsweise für Gewaltvideos, die mit Handys aufgezeichnet werden, oder für Kinderpornographie. Dieser Umstand kann helfen, Täter zu überführen, indem Kameras im Besitz der Täter mit aufgefundenem Material in Verbindung gebracht werden. Dies wird durch die Kamera-Forensik ermöglicht. Diese errechnet eine Art Fingerabdruck der Kamera, indem eine Serie von Bildern hinsichtlich eines für die Kamera individuellen Eigenrauschens untersucht wird, welches durch Fertigungsungenauigkeiten des bild erzeugenden CCD Chips bei seiner Herstellung bedingt ist. Dieser Fingerabdruck kann dann als Quellennachweis zu einer Kamera dienen – sogar nach verlustbehafteter Kompression oder dem Ausdrucken und Einscannen.

Test IT-forensischer Werkzeuge

Mit der technologischen Weiterentwicklung ergeben sich immer wieder neue Anforderungen an IT-forensische Methoden und Werkzeuge. Deren Leistungsfähigkeit hängt oftmals von besonderen Rahmenbedingungen ab, unter denen sie eingesetzt werden. Entwickler haben heute oft keine Realdaten, anhand derer sie ihre Ergebnisse testen können. Insbesondere ist es Anwendern und Entwicklern häufig nicht klar, wie sich ihre Werkzeuge unter besonderen Bedingungen verhalten. Deshalb ist es wichtig, die Leistungsfähigkeit der Werkzeuge unter gewünschten Bedingungen testen zu können. Fraunhofer SIT hat mit 3LSPG ein Verfahren entwickelt, mit dem IT-forensische Werkzeuge für gegebene Bedingungen mittels synthetisch erzeugter Datenbestände getestet werden können.

Verbesserung IT-forensischer Werkzeuge

Mit diesen Tests ist es möglich, bestehende IT-forensische Methoden zu untersuchen und sie allgemein oder für bestimmte Bedingungen zu verbessern. So liefert die Benford-Analyse, eine IT-forensische Standardmethode, unter bestimmten Bedingungen (z.B. bei Buchungsgrenzen durch Zugriffsbeschränkung) wegen zu vieler False Positives keine brauchbaren Ergebnisse. Mit seinem Beitrag zur modellgestützten digitalen Analyse ist es Fraunhofer SIT gelungen, die Idee der Benford-Analyse weiter zu entwickeln und zu verbessern, indem von der

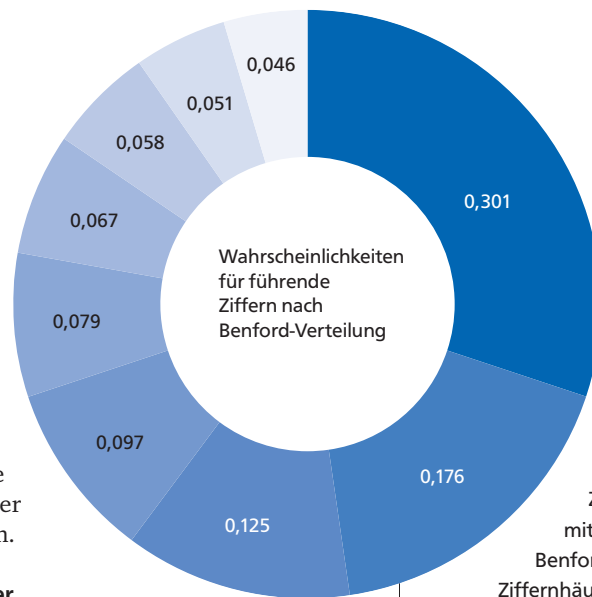
Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Dr.-Ing. Martin Steinebach
Tel. 06151/869-349
E-Mail: martin.steinebach@sit.fraunhofer.de

Dr.-Ing. Markus Schneider
Tel. 06151/869-337
E-Mail: markus.schneider@sit.fraunhofer.de
www.sit.fraunhofer.de

Fachgebiet für Sicherheit in der Informationstechnik

TU Darmstadt / Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Prof. Dr. Michael Waidner
Tel. 06151/869-250
E-Mail: waidner@sit.fraunhofer.de
www.sit.fraunhofer.de



Führende Ziffern

- 1 ■ 2 ■ 3
- 4 ■ 5 ■ 6
- 7 ■ 8 ■ 9

Benfords Gesetz

Dieses Gesetz basiert auf der Beobachtung von S. Newcomb (1881) und F. Benford (1934), dass führende Ziffern in vielen Zahlenlisten nicht gleichverteilt sind. Zahlen mit niedrigerer führender Ziffer treten in vielen Listen öfter auf als Zahlen mit höherer führender Ziffer. Daraus wurde die Benford-Analyse entwickelt: Weichen gemessene Ziffernhäufigkeiten zu stark von der Benford-Verteilung ab, dann ist dies ein Indiz für eine Unregelmäßigkeit.

Benford-Verteilung abweichende und auf die konkreten Bedingungen angepasste Verteilungen verwendet werden. Damit können IT-Forensiker ihre Untersuchungen effektiver und effizienter durchführen.

Entwicklung rechtssicherer Analysemethoden

Zur Entdeckung von Tätern sind oftmals für Plausibilitätschecks, Datenabgleiche oder Anomalie-Erkennung Analysen großer Datenbestände notwendig, bei denen Daten vieler Personen verarbeitet werden. Hier kann die IT-Forensik leicht in Konflikt mit dem Datenschutz geraten (z.B. Datenskandal bei der Deutschen Bahn AG 2009). Zur rechtskonformen und leistungsfähigen IT-forensischen Untersuchung sind somit geeignete Verfahren erforderlich.

Es existieren große Herausforderungen bei der Bekämpfung digitaler Kriminalität. Die IT-Forensik kann hier bei der Bewältigung wichtige Hilfsmittel stellen. Eine Herausforderung besteht in der Entwicklung relevanter neuer Lösungen und in dem Transfer von wissenschaftlichem Beitrag zur praktischen Anwendung. Dies ist am CASED eine der Aufgaben des Fraunhofer SIT.



Martin Steinebach leitet am Fraunhofer SIT den Bereich Information Assurance, der sich unter anderem mit IT Forensik und Multimedia Security beschäftigt. Er ist zudem Principal Investigator des LOEWE-Zentrums CASED.



Markus Schneider koordiniert die CASED-Aktivitäten des Fraunhofer SIT und war am Aufbau der IT-Forensik-Gruppe des Fraunhofer SIT beteiligt.



Michael Waidner ist seit 2010 Professor für Sicherheit in der Informationstechnik an der TU Darmstadt und zugleich Leiter des Fraunhofer SIT am Standort Darmstadt. Er ist zudem stellvertretender Direktor des LOEWE-Zentrums CASED.

—ANZEIGE

Der andere Blickwinkel ist es.

Die perfekte Location für erfolgreiche Seminare und Workshops.

Tel +49 (0)69 696 13 9100
www.lufthansa-seeheim.de

Lufthansa Seeheim