Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.)

IT-Incident Management & IT-Forensics

Erste Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik

24. – 25. November 2003 in Stuttgart, Deutschland

Gesellschaft für Informatik 2003

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-39

ISBN 3-88579-368-7
ISSN 1617-5468

Volume Editors
Jens Nedon
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, D-49716 Meppen
Nedon@consecur.de
Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, D-70569 Stuttgart
Sandra.Frings@iao.fhg.de
Oliver Göbel
RUS-CERT (Universität Stuttgart)
Breitscheidstr. 2, D-70174 Stuttgart
Goebel@CERT.Uni-Stuttgart.DE

printed by Köllen Druck+Verlag GmbH, Bonn

Integrationsplattform zur systemübergreifenden Erfassung und forensischen Analyse von Spurenträgern

Christoph Fischer

BFK edv-consulting GmbH
Durlacher Allee 47
D-76131 Karlsruhe
cfischer@bfk.de

Abstract: Die Integrationsplattform soll eine Basis zum Erfassen, Auswerten und Dokumentieren von digitalen Spuren auf unterschiedlichsten elektronischen Geräten und IT-Systemen dienen. Die IT-Welt ändert sich so rasant, dass nur ein modulares und skalierbares Konzept langfristig Bestand haben kann. Das Paper beschäftigt sich mit der prinzipiellen Architektur und den Designparadigmen.

1 Zielsetzungen

Ziel des Projekts ist es einen holistischen Ansatz für eine 'workbench' zu entwickeln, die die Arbeit beim Sammeln, Erfassen, Auswerten, Bewerten und Dokumentieren von digitalen Spuren vereinfacht und standardisiert. Die den gesamten Vorgang begleitenden Maßnahmen bestehen aus beratenden Funktionen, Arbeitserleichterungen, Unterstützung von Gruppenarbeit, so wie Automatisierung mechanisch ablaufender Vorgänge. Die Entlastung bzw. Unterstützung der Ermittler und die Reduzierung der Fehlermöglichkeiten sollen zu einer zeitnaheren und qualitativ verbesserten Bearbeitung der Spuren führen.

2 Digitale Spuren

2.1 Definition der Spurenquellen

Durch die zunehmende Verbreitung von lokaler Intelligenz in allen nur erdenklichen Geräten kann heute selbst eine Waschmaschine zur interessanten Spurenquelle werden. Die geradezu explosionsartige Entwicklung der Speicherkapazität bei gleichzeitigem Verfall der Preise erlaubt es selbst in unscheinbaren Geräten Betriebsstatistiken oder andere Daten zu speichern. Eine saloppe Definition von digitalen Spurenquellen wäre: 'Alles was Strom verbraucht'.

Beispiele für beiläufigen Spuren sind:

- Playlists in komfortablen Audio/Video Geräten, hier ist meist eine Historie der Benutzung abgespeichert.
- Re-dial-Speicher eines Telephons zeigt nicht nur die letzten gerufenen Nummern an, sondern auch Datum und Uhrzeit des Rufes.
- Alarmanlagen haben eine Historie der ausgelösten Alarme und der Scharf- bzw. Unscharf-Schaltungen.
- Moderne Faxgeräte haben nicht nur eine Journalfunktion, sondern lassen auch ein Auslesen der letzten Faximile zu.
- Beispiele für 'kreative Nutzung' von Speicherkapazität sind:
- Halbleitermedien für digitale Kameras. Diese Medien können von Rechnern wie normale Dateisysteme beschrieben werden. In den Kameras bleiben aber fremde Datenformate meistens verborgen.
- Mobilfunkgeräte der oberen Leistungsklasse verfügen über große Speicherkapazität und verschiedene Kommunikationsmöglichkeiten, wie IrDA und Bluetooth.

2.2 Erfassung

Die Generationswechsel bei 'Gadgets' sind rapide, dies bedeutet für die Werkzeuge, die in die Plattform eingebaut werden einen sehr kurzen lifecycle. Begleitend mit den Softwareanpassungen sind auch technische Elemente elektrischer bzw. mechanischer Natur an die Neuerungen anzupassen. Um all diese Möglichkeiten auszunutzen sollte das Personal detaillierte Beschreibungen und Schritt für Schritt Anweisungen zur korrekten Erhebung und Sicherung der Spuren erhalten. Die Beschreibungen der Einzelschritte sind mit Photos, und Graphiken angereichert und forcieren in ihrem Ablauf die Einhaltung vorgegebener Prozeduren und generiert die erforderliche Dokumentation während des Erfassungsprozesses.

Die Menge der zu erfassenden Daten stellt hohe Anforderungen an Kapazität und Schreibgeschwindigkeit der Medien, die zur Sicherung verwendet werden. Allen Entwicklungen voran ist die Kapazität von Festplatten zu erwähnen. 1983 bei der Einführung des Personal Computer auf Basis des Intel 8088 wurden 5 MB Platten ausgeliefert, heute 2003 werden von Lebensmitteldiscounter PCs mit 180GB angeboten. Dies bedeutet in nur 20 Jahren eine 36-fache Kapazitätsvergrößerung. Die klassischen Back-Up Medien wie Wechselplatten und Magnetbänder haben weder bei der Kapazität noch bei der Transfergeschwindigkeit ein nur annähernd vergleichbaren Zuwachs aufzuzeigen. Im Bereich der ‚write-once'-Medien, die wegen der Authentizitätsfrage in der Forensik besonders interessant wären liegen weit abgeschlagen.

Zusätzliche Herausforderungen entstehen durch minimal invasive Verfahren des Hakkings. Diese neuen Werkzeuge, die keine Änderung auf der Festplatte bewirken und sich nur in dem Hauptspeicher einnisten stellen bei der Erfassung der Spuren ein besonderes Problem dar, da ihre Dokumentation mit Eingriffen in das betroffene System verbunden sind. Hier ist eine fundierte Triage und ein extrem sorgfältiges Vorgehen und extrem genaues Dokumentationsverfahren notwendig. Hier sind besonders die sogenannten ‚kernel root-kits' zu erwähnen, die durch einen Neustart des Systems spurlos vernichtet würden. Eine genaue Analyse ist nur in einem Hauptspeicherdump zu erreichen und somit nur durch einen Eingriff, der andere Spuren im System beeinträchtigt.

2.3 Auswertung

Die enorme Datenmengen stellen besondere Anforderungen an die Speicherkapazität und Rechenleistung der Auswertesysteme. Um das Konzept 'überlebensfähig' zu halten wurde besonderer Wert auf die Skalierbarkeit und Modularität gelegt.

Jegliche automatisierbare Auswertefunktion soll mit minimalstem Benutzeraufwand anwendbar sein. Die gefundenen Auffälligkeiten werden über ein Punktesystem priorisiert zur manuellen Bewertung sortiert. Die Priorisierung ist von mehreren Faktoren abhängig und wird auch durch die generelle Kategorisierung eines Falles beeinflusst. Ein Erpressungsfall zeigt andere Spezifika als ein Industriespionagefall oder ein Betrugsfall.

Eine halbautomatische Dokumentationsfunktion erlaubt eine schnelle Erzeugung von Einzel- und Gesamtreports. Die auf dynamischen HTML-Funktionen basierenden Dokumentationsmodule stellen parametrisierte Rohtexte dar, die vom Auswerter angepasst und ergänzt werden. Eine multilinguale Dokumentationserstellung ist bereits in den Vorprojekten implementiert worden. Die Ausgabe der Dokumente erfolgt via Renderingmodule als elektronisches Dokument, druckfreundliche Formate und als CD/DVD Authoring.

Die einzelnen Auswertemodule verfügen über Rohdatendarstellungen, anwendungstypische ‚views', graphische Visualisierungen und Exportfunktionen, die externe Anwendungen einbindbar machen. Beispielhaft sind hier Speicherdumps von Handheld Computern zu nennen. Diese sind von der Komplexität, Vielfalt und Kurzlebigkeit her nicht vollständig integrierbar. Die meisten Hersteller bieten aber virtuelle Versionen ihrer Systeme für z.B. Laptops an. Ein anderes Beispiel sind Audiodaten, die in Recorderfunktionen von Mobiltelephonen gespeichert sind. Diese Daten sollten in optimaler Qualität wiedergegeben oder überspielt werden, um Sprachanalysen bzw. Vergleiche oder Veröffentlichungen bei Fahndungen zu erlauben

2.4 Realisierung

Die Realisierung des derzeitigen Prototypen basiert auf einem RAID Array, auf den mehrere Agenten zugreifen. Ein zentrales System übernimmt die Aufgabe des Scheduling und bildet die Benutzerschnittstelle via Web-Interface. Die nächste Generation (Abbildung 2.2) des Projekts wird auf NAS-Technologie basieren, um eine höhere Geschwindigkeit und bessere Skalierbarkeit zu erzielen. Die einzelnen Agentensysteme übernehmen Teilaufgaben des automatisierten und manuellen Auswertens. Das Schedu-

ling kann mehrere Fälle parallel bearbeiten und priorisiert dabei die Aufgaben nach geschätztem Aufwand und vorhandener Rechenleistung.

Generation 1:

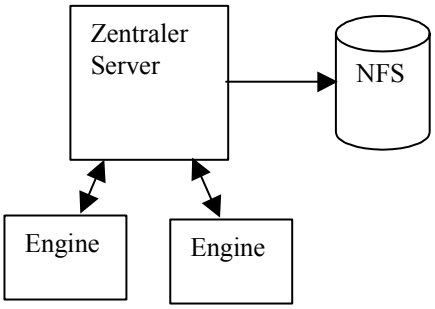

Abbildung 2.1: Generation 1

Generation 2:

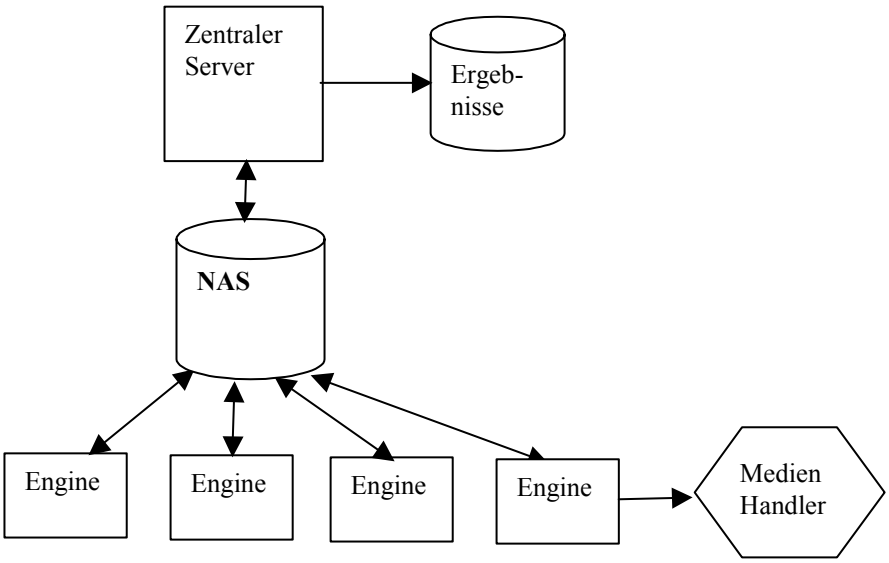

Abbildung 2.2: Generation 2

Die explosionsartige Entwicklung bei den Datenmengen hat den Wechsel zu einer schnelleren Anbindung und größeren Speicherkapazitäten erzwungen. Der zentrale Server ist weiterhin für die Darstellung beim Anwender und die Koordination zuständig. Die engines führen die einzelnen Such- und Analyseaufgaben durch, deren Ergebnisse in der Datenbank des Servers abgelegt werden.

Die einzelnen Anwender greifen über einen normalen Browser auf den auf dem zentralen Servers laufenden Webserver zu. Die Auswertekomponenten sollten, bis auf wenige Ausnahmen auf dem Gesamtsystem laufen und nicht als Applikationen auf der Client-Seite. Dies integriert die einzelnen Schritte und erlaubt eine stringente Kontrolle und Protokollierung der Zugriffe auf die Asservate, was unter vielen Gesetzgebungen eine extrem wichtige Rolle spielt.

Die Architektur wurde sehr offen gehalten, um möglichst einfach externe Module und fremde Werkzeuge einzubinden. Die Kommunikation zwischen zentralem Server und Engines basiert auf SOAP und XML. Beispiele für integrierte Funktionen sind TCT ein rudimentäres Analysetool für Festplatteninhalte. Die ‚known good' Datenbank des NIST (National Institute of Standards and Technology), die Hashwerte für bekannte Softwareprodukte auf derzeit vier CD-ROM vertrieben wird in eine Art ‚Aschenputtel' Funktion eingebettet.

Weitere Module dienen zur Automatisierung von manuellen Aufgaben, wie z.B. das Einlesen von großen Mengen von Datenträgern, wie Disketten, CD-ROM und DVD. Hier kommen Duplizierroboter zum Einsatz, deren Interface durch ein reservierten Engine bedient wird.

Ein typischer Ablauf beinhaltet die folgenden Schritte:

Eröffnung des Falles: Es werden die Grunddaten und Zuständigkeiten eingegeben.

Erfassung von Daten: Hier werden die einzelnen Spurenträger erfasst und ausgelesen.

Initialauswertung: Alle automatisierbaren Standardaufgaben werden vom Scheduling erfasst.

Sichtung und Bewertung: Die vom System gefundenen und priorisierten Auffälligkeiten werden manuell gesichtet und bewertet.

Dokumentation: Aus den Bewertungen werden tempates erzeugt, angepasst und in ein Gesamtdokument integriert.

Alle Schritte können iterativ wiederholt werden und sich in multiplen Fassungen und verschiedenen Typen von Dokumenten wiederspiegeln.

3 Vorführung des Prototypen

Die Vorführung des transportablen Prototypen wird durch einen fiktiven Fall anhand einiger exemplarischer Schritte im Laufe des Vortrags durchgeführt.

Die einzelnen Schritte sollen den Ablauf von Erfassung, Auswertung und Dokumentation vorführen. Wegen der zeitlichen Limitierung sind die einzelnen Schritte vorgefertigt und werden in den einzelnen Phasen dargestellt und diskutiert.

4 Quellen

Vortrag: C. Fischer EECTF European Electronic Crime Task Force, Mailand 11. Juni 2003
Interne Dokumente BFK: BFTK BFK Forensic Toolkit
Softwaredokumentation: TCT The Coroner's Toolkit, Wietse Venema und Dan Farmer
Vortrag: C. Fischer CTOSE Workshop, Stuttgart 6. Mai 2003