Analyse von Gutachten

beauftragt durch

Kanzlei Hubrig
Frau Beata-Konstanze Hubrig
Gaudystraße 6

10437 Berlin

verfasst von

Mirko Vogt
Zossener Str. 51
10961 Berlin

Version 1.2.1

zuletzt aktualisiert am 1. Februar 2017

Betrachtete Gutachten

verfasst von

Sachverständigen-Büro für Computerwesen
Prof. Dr. Pausch & Partner

im Privatauftrag für

GuardaLey Ltd.
Herrn Perino
Donauring 71
76344 Eggenstein-Leopoldshafen

120222/04
Gutachten über die sachegerechte Aufzeichnung von Torrent-Daten mit dem System ,,Observer"

141117/04
Gutachten zur korrekten Ermittlung von IP-Adressen eines BitTorrent-Systems

120424/04
Stellungnahme über die Nachfrage des Gerichts bezüglich des Systems ,,Observer"

Inhaltsverzeichnis

Der Sachverständige und Autor dieses Dokuments wurde mit der Betrachtung oben genannter Gutachten – mit Fokus auf folgende Fragestellungen – beauftragt:

- Lässt das vorliegende Gutachten genug Rückschlüsse auf Architektur und Implementierung der Software zu?
- Wenn nein, welche Teile fehlen, sind diese für eine lückenlose Beweisführung essentiell?
- Unter Vorbehalt der destillierbaren Informationen:
  - Entsprechen Architektur und Implementierung der Software dem Stand der Technik?
  - Worin unterscheidet sich die Software von der anderer Anbieter am Markt? Was sind Stärken und Schwächen?
- Fand eine kritische Auseinandersetzung mit der begutachteten Software statt?
- Entspricht das Gutachten qualitativen Anforderungen? Kann eine Aussage getroffen werden, ob alle Fragen an den Gutachter korrekt beantwortet wurden?

Im Folgenden wird der Verfasser dieses Dokuments als *Sachverständiger* und der Verfasser betrachteter Gutachten als *Gutachter* bezeichnet.

Da dem Sachverständigen selbst weder Quelltext der Software noch die Software selbst vorliegt, wird dieser bei der Betrachtung genannter Gutachten bzgl. des Systems ,,Oberserver" die vom Gutachter zusammengestellten Informationen über die Software als korrekt erachten, sofern das Gutachten keine Widersprüche oder Unklarheiten aufweist.

Der Sachverständige konnte den Gutachten inhaltlich und technisch problemlos folgen und hat keine Anlässe das technische Verständnis des Gutachters anzuzweifeln.

Im Folgenden werden - mit Fokus auf vom Auftraggeber gegebene Fragestellungen - dem Sachverständigen unklare bzw. zweifelhafte Passagen angeführt und kommentiert.

1 120222/04: Gutachten über die sachegerechte Aufzeichnung von Torrent-Daten mit dem System ,,Observer"

Der Sachverständige hält das Gutachten für plausibel und fundiert, vermisst jedoch eine für fehlerfreie und sichere Datenaufzeichnung notwendige Betrachtung des Gesamtbildes des Aufbaus, auch wenn sich der gutachtliche Auftrag auf die ausschließliche Betrachtung der Komponente ,,Observer" bezieht.

1.1 Race Conditions

Eine Untersuchung der Software auf für Applikationen dieser Art typische Probleme, z.B. sog. *Race Conditions*, wären aus Sicht des Sachverständigen relevant und fehlen. *Race Conditions* sind Situationen, in welchen ein durch parallelle Ausführung bedingtes, unerwartetes, im Normalbetrieb nicht auftretendes, aber nicht gänzlich unwahrscheinliches Ereignis, einen Programmablauf schwer vorhersehbar beeinträchtigen kann.

Ein typisches Beispiel sind zwei Programme, die parallel laufen, auf die selbe Ressource (z.B. eine Datei) zugreifen und wo die Zugriffe nicht abgestimmt werden. Beide Programmenteile werden in dem Beispiel meist nacheinander, aber unter bestimmten Umständen auch exakt zeitgleich ausgeführt. In dem Beispiel schreiben beide Programmteile einzeln Buchstabe für Buchstabe zwei Wörter in eine Datei. Obwohl in den meisten Fällen beide Wörter nacheinander geschrieben werden (z.B. ,,Welt" und ,,Frieden"), kann es auch zu dem ungewünschten Resultat ,,WeFlrtieden" kommen.

Ein weiteres Beispiele wäre der Test auf die Existenz einer Datei, sowie die anschließende Anlegung dieser, sofern sie zuvor nicht existierte. Oder die Erstellung eines Datenbankeintrags, sofern ein vorheriger Test auf die Existenz eines ggf. bereits existierenden Eintrags negativ ausfällt.

In allen Fällen besteht auf modernen Betriebssystemen die Möglichkeit, dass bei paralleler Ausführung unter Zugriff auf die selben Ressourcen, es zu solchen *Race Conditions* kommen kann und es damit zu schwer determinierbaren Programmverläufen und korrumpierten Daten kommt.

Race Conditions treten ebenfalls häufig bei der Verwendung zentraler Speichersysteme, auf welche mehrere Komponenten parallel und in nicht definierten Reihenfolgen zugreifen, auf.

Heutige Computersysteme sind auf Grund mehrzähliger verbauter Prozessoren für den Parallelbetrieb von Applikationen ausgelegt; um diese auszunutzen und die eigene Applikation von Anfang an skalierbar zu gestalten, ist es üblich, bestimmte Programmroutinen – auch innerhalb ein und derselben Applikation – parallel auszuführen. Diese Technik ist ohne explizites Treffen geeigneter Gegenmaßnahmen sehr anfällig für beschriebene *Race Conditions*, ist aber für performancekritische Applikationen ein enormer Mehrwert.

Die Erwähnung mehrerer geladene Module und der Verteilung von Aufgaben des Brokers auf eben jene (Seite 17., Zeile 19ff, Seite 29, 19ff), sowie der Verwendung einer zentralen Datenbank, lässt den Sachverständigen vermuten, dass hier von paralleler Ausführung Gebrauch gemacht wird.

Insofern vermisst der Sachverständige hier Hinweise auf eine Untersuchung auf *Race Conditions* bzw. paralleler Ausführung von Applikationen, Teilen ihrer bzw. getroffene Gegenmaßnahmen für einen determinierten Ausführungsfluss.

Race conditions können für die Datenverarbeitung fatale Folgen haben, da hier die Synchronisation und Abtimmung der einzelnen parallel ausgeführten Komponenten nicht gewährleistet ist und somit keine Annahmen darüber getroffen werden können, ob noch andere Komponenten zeitgleich auf entsprechende Datensätze zugreifen oder diese zunächst unerkannt verändern.

Unter Einbeziehung des Verwendungszwecks der Applikation „Observer" und der von ihr gespeicherten Daten, muss sichergestellt werden, dass Programmroutinen hier atomar und frei von *Race Conditions* sind.

Eine solche Prüfung fand durch den Gutachter anscheinend nicht statt.

1.2 SQL-Operatoren

Der Sachverständige wurde stutzig bei den auf Seite 27, Zeile 6ff. gelisteten, von der Applikation implementierten, SQL-Operatoren:

- INSERT
- DELETE
- UPDATE
- SELECT

Die Listung der Operatoren *INSERT* und *SELECT* erscheint schlüssig, da diese zum Eintragen und Auslesen von entsprechenden Datensätzen verwendet werden. Die Aufführung der *UPDATE*- und *DELETE*-Operatoren ist dem Sachverständigen jedoch nicht plausibel, da diese für die *Abänderung* bereits gespeicherter Datensätze verwendet werden.

In Anbetracht dessen, dass das Gesamtsystem die nachträgliche Manipulation einmal gespeicherter Datensätze verhindern soll, erscheint vorallem die Implementierung des *UPDATE*-Operators fragwürdig.

Auch wenn der Gutachter schreibt, dass hier nur *INSERT* und *SELECT* Verwendung finden, vermisst der Sachverständige eine Erklärung für die Existenz einer Implementierung von *UPDATE*-Routinen.

1.3 Aussagekraft einer einzelnen Messung

Um den Internetanschlussinhaber, konkret den Herunterladenden, zu bestimmen, werden die die Internetanschlüsse bereitstellenden Institutionen (*ISPs*) angefragt, den Anschlussinhaber zu der durch den ,,Observer" ermittelten IP-Adresse zu ermitteln.

Nach dem letzten Stand des Sachverständigen geben die ISPs diese Daten jedoch explizit unter Vorbehalt und ohne Garantie auf Korrektheit heraus. Dem Sachverständigen sind mehrere Fälle bekannt, wo der zu einer IP-Adresse ermittelte Abschlussinhaber den fragwürdigen Aufruf/Download nicht getätigt haben kann (z.B. Anschlussinhaber und ausschließlicher Nutzer des Anschlusses war zu dieser Zeit verreist).

Auch wenn die Applikation ,,Observer" anscheinend Vorkehrungen trifft, um das Risiko einer falschen Zuordnung zwischen Anschlussinhaber und IP-Adresse zu reduzieren – z.B. indem es Mindestzeiten offener Verbindungen vor und nach der Messung voraussetzt – gilt dem Sachverständigen die Assoziation zwischen Anschlussinhaber und IP-Adresse als nicht gesichert. Dies trifft vor allem zu, wenn nur eine Messung vorgenommen wird und dementsprechend nur einmal die entsprechende IP-Adresse protokolliert wird.

Andere Applikationen sehen eine ermittelte IP-Adresse erst als verwertbar an, wenn mehrere Messungen ergeben, dass ein Klient mit der selben IP-Adresse, von der selben Gegenseite, Teile der selben Datei runterlädt. Auch wenn mehrere Messungen das Risiko der nicht eindeutigen Assoziation zwischen IP-Adresse und Anschlussinhaber nicht beheben können, so erhöht dieses Verfahren doch die Wahrscheinlichkeit, dass die Zuordnung korrekt ist.

Zudem stellt sich dem Sachverständigen die Frage, inwiefern der Download eines Bruchteils einer Datei (erst Daten kleiner als 1KB werden verworfen) ausreichend ist, um davon auszugehen, dass der Herunterladende zu irgendeinem Zeitpunkt die gesamte Datei heruntergeladen haben wird. Dies ist auf Grund der zugrunde liegenden Technik für die Applikation ,,Observer" nämlich zu keinem Zeitpunkt nachprüfbar.

Der Gutachter scheint sehr akribisch bei der Analyse des Vorgangs zur Erstellung verwertbarer Datensätze vorgegangen zu sein. Er erklärt die Funktionsweise der Applikation ,,Observer" detailliert und schildert nachvollziehbar, wie ungültige Datensätze erkannt, verworfen und damit schlussendlich nicht verwendet werden.

Jedoch kann der Sachverständige nur den Teil der in dem Gutachten behandelten Komponente ,,Observer" bewerten - eine Gesamteinschätzung wäre erst möglich,

wenn die Funktionsweise und das Zusammenspiel aller Komponenten bekannt wäre.

Das Gutachten bezieht sich ausschließlich auf das Programm „Observer“, jedoch sind offensichtlich noch weitere Komponenten involviert, welche Daten abgreifen, bearbeiten und speichern, sodass der Sachverständige keine abschließende Einschätzung über die korrekte Erfassung und Speicherung entsprechender Daten treffen kann.

Ausschließich auf den „Observer“ bezogen hat der Sachverständige nach Studium des Gutachtens keinen Grund zu der Annahme, dass in diesem Programmteil Datensätze fälschlicherweise als verwertbar deklariert werden.

2 141117/04: Gutachten zur korrekten Ermittlung von IP-Adressen eines BitTorrent-Systems

Der Sachverständige erkennt Überschneidungen bzgl. Fragen und Erkenntnissen in den Gutachten 141117/04 sowie 120222/04 und wird hier nur auf abweichende Fragestellungen Bezug nehmen.

In Hinblick auf die Frage des Gerichts „*Lädt das System die komplette von einem anderen Computer ‚angebotene' Datei herunter?*" teilt der Sachverständige nur bedingt die Auffassung des Gutachters.

Wie der Gutachter kommt auch der Sachverständige zu dem Schluss, dass eine am BitTorrent-Netzwerk partizipierende Partei in aller Regel nicht sicher feststellen kann, dass eine Datei von einem anderen Klienten komplett heruntergeladen wurde.

Die Applikation „Observer" erstellt und speichert bereits einen Eintrag, wenn mit dem Download eines anscheinend relevanten Teils (*Piece*) begonnen wurde. Relevant gelten bereits Daten ab der Größe von 1KB. Zudem muss auf Grund der Architektur von BitTorrent davon ausgegangen werden, dass zumindest Teile der angefragten Datei auch von anderen Seedern angeboten und bereitgestellt werden. Je mehr Klienten also Teile einer Datei haben, desto parallelisierter werden Teile von unterschiedlichen Seedern – und damit weniger von nur einem Seeder – heruntergeladen.

Auf diesen Gründen – Verteilung eines Downloads auf soviele Seeder wie möglich auf Grund der Architektur des BitTorrent-Netzwerkes sowie den Abbruch einer Verbindung durch den „Observer" schon nach Download eines Bruchteils der angefragen Datei – hält es der Sachverständige für praktisch nicht möglich, dass durch den „Observer" sichergestellt werden kann, dass eine Datei von einem Klienten komplett heruntergeladen wurde.

Inwiefern der Gutachter auf Grund dessen zu dem Schluss kommt, dass es nur „eine Frage der Zeit [ist,] bis er die komplette Datei heruntergeladen hätte", erschließt sich dem Sachverständigen nicht. Technisch gibt es für diese Schlussfolgerung keine Grundlage. Auch wenn die Wahrscheinlichkeit gegeben ist, dass der Herunterladende die Datei komplett herunterlädt oder dies bereits getan hat, ist dies weder nachprüfbar, noch zwingend der Fall.

Es gibt diverse Gründe, wieso ein Klient nur einen Teil einer Datei herunterlädt - darunter fallen offensichtliche Gründe, wie Abbruch des Downloads durch den Benutzer. Ein Abbruch der *peer-to-peer*-Verbindung ist auch aus anderen Gründen nicht unwahrscheinlich, z.B. weil eine Partei, welche derzeit als einzige ein be-

stimmtes *Piece* einer Datei im BitTorrent-Netzwerk bereitstellt, die Verbindung unterbricht.

Die Annahme, dass der herunterladende Klient irgendwann eine vollständige Kopie dieser Datei hat, ist begründet, aber nicht gesichert.

3 120424/04: Stellungnahme über die Nachfrage des Gerichts bezüglich des Systems ,,Observer”

In der o.g. Stellungnahme bekräftigt der Gutachter seine schon in dem Gutachten 141117/04 erklärte Annahme, dass ein Klient, welcher nur einen Bruchteil einer Datei über das BitTorrent heruntergeladen hat, im Besitz einer vollständigen Kopie der Datei ist oder sein wird.

Da BitTorrent so aufgebaut ist, dass von möglichst vielen Klienten (*Seedern*) parallel unterschiedliche Teile einer Datei heruntergeladen werden und unter Einbeziehung, dass die Software ,,Observer“ anscheinend Verbindungen trennt, nachdem sie feststellte, dass bereits ein Bruchteil einer Datei geladen wurde, hält es der Sachverständige für nicht möglich, dass für die überwachten Dateien nachweisbar ist, dass diese komplett heruntergeladen wurden.

Der Gutachter beschreibt dies als ,,berechtigte Annahme” (Seite 4, Zeile 7ff.), für ihn ,,erscheint es nahezu ausgeschlossen, dass der vom ,,Observer” aufzeichnete Client [..] nicht die vollständige Datei zur Verfügung hat.”.

Der Sachverständige kann diese Schlussfolgerung auf Grund der schon zuvor genannten Szenarien, in welchen der Klient keine vollständige Kopie der Datei herunterlädt, nicht nachvollziehen.